z/OS
Version 2.Release 4

Cryptographic Services ICSF Trusted Key Entry Workstation User's Guide

SEE RESOURCE LINK FOR THE LATEST COPY OF THIS BOOK



SC14-7511-09

Note

Before using this information and the product it supports, read the information in “Notices” on page 399.

This edition applies to TKE 9.2 and Version 2 Release 4 of z/OS® (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

Last updated: 2021-04-06

© Copyright International Business Machines Corporation 2000, 2021.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures ..... **xi**

Tables ..... **xxvii**

About this information ..... **xxix**
Who should read this information xxix
How to use this information xxix
Where to find more information xxx

How to send your comments to IBM ..... **xxxi**
If you have a technical problem xxxi

Summary of changes ..... **xxxiii**
Changes made in z/OS Version 2 Release 4 (V2R4) xxxiii
Changes made in z/OS Version 2 Release 3 (V2R3) xxxv
Changes made in z/OS Version 2 Release 3 (V2R3) xxxvi
Changes made in z/OS Version 2 Release 2 (V2R2) xxxvii

Chapter 1. Overview **1**
Trusted Key Entry components 1
TKE hardware 1
TKE software 2
Supported host cryptographic adapters 3
Host crypto module 3
TKE concepts and mechanisms 3
Integrity 4
PCI-HSM overview 4
Authorities 5
Crypto module OA signature key 7
Command signatures 7
Key-exchange protocol 9
Domain controls and domain control points 9
Domain modes 9
TKE operational considerations 10
Logically partitioned (LPAR) mode considerations 10
Multiple hosts 10
Multiple TKE workstations 10
Defining your security policy 10
TKE enablement 11
Trusted Key Entry console 11
Trusted Key Entry console navigation 15
TKE workstation crypto adapter roles and profiles 16
Authority checking on the TKE 16
Types of profiles 16
Initializing a TKE workstation crypto adapter 17
Roles and profiles definition files 20
System-supplied role access control points (ACPs) 23
Blue smart cards (00RY790) 37
TKE security policy wizards 38

Chapter 2. Using smart cards with TKE.....41
Terminology..... 41
Preparation and planning..... 42
Using the IDENTIV smart card reader..... 42
Using the OmniKey smart card reader.....43
Using the Gemalto smart card reader.....43
Things to consider..... 44
Smart card compatibility issues.....44
Zone concepts 49
Authentication and secure communication.....49
Zone creation 49
Multiple zones..... 50
Enrolling an entity.....51
TKE smart cards..... 51
EP11 smart cards..... 52
Steps to set up a smart card installation..... 52
Moving TKE and EP11 smart card data to smart cards in a new zone..... 53
Moving data from a TKE smart card in a 1024-bit zone to a blue smart card.....53

Chapter 3. TKE upgrade and migration actions..... 55
Considerations before upgrading a TKE or copying data from an existing TKE..... 55
DVD-RAM is not supported on a TKE 7.2 or later system..... 55
Copying files to the TKE 7.0 or TKE 7.1 hard drive.....55
Copying files to a USB flash memory drive while on a TKE 7.0 or TKE 7.1 system.....56
Preparing for a new TKE local crypto adapter..... 58
Upgrading an existing TKE workstation to TKE 9.2.....60
Moving data from a TKE Version 5.*x*, 6.0, 7.*x*, 8.0, or 9.*x* to a new workstation at TKE 9.2..... 62
Identifying data to be copied from the source TKE to the target TKE..... 62
Copying customer data from the source TKE to USB memory in a form that the target TKE can read.....66
On the Target TKE, copying data from USB memory onto the TKE's hard drive.....67
Loading TKE local adapter roles and profiles..... 69
Recovery installation..... 70

Chapter 4. TKE setup and customization..... 73
TKE TCP/IP setup.....73
TKE host transaction program setup.....74
Cancel the TKE server..... 77
TKE workstation setup and customization.....77
The TKE Workstation Setup wizard.....78
Configuring TCP/IP..... 81
Customize console date and time.....83
Initializing the TKE workstation crypto adapter.....84
TKE workstation crypto adapter post-initialization tasks..... 85

Chapter 5. TKE up and running.....97
Crypto adapter logon: passphrase or smart card..... 97
Passphrase and passphrase group logon..... 97
Smart card and smart card group logon..... 99
Automated crypto module recognition..... 102
Authenticating host crypto modules.....102
Initial authorities..... 103
Backing up files.....103
Host file to back up..... 104

Chapter 6. Main window..... 105

Working with hosts ... 106
Creating a new host ... 106
Changing host entries ... 107
Deleting host entries ... 107
Logging on to a host ... 107
Closing a host ... 108
Specify auto-accept for all hosts ... 108
Understanding crypto modules and domain groups ... 108
Copy and paste domains using a create or change domain group screen ... 109
Working with crypto modules ... 112
Working with domain groups ... 112
Creating a domain group ... 114
Changing a domain group ... 116
Viewing a domain group ... 118
Checking domain group overlap ... 119
Comparing groups ... 121
TKE functions supporting domain groups ... 122
Crypto module groups ... 122
Function menu ... 122
Load signature key ... 122
Unload signature key ... 124
Display signature key information ... 124
Define transport key policy ... 124
Exit ... 125
Exit and logoff ... 126
Utilities menu ... 126
Manage workstation DES keys ... 126
Manage workstation PKA keys ... 127
Manage workstation AES keys ... 129
Manage smart card contents ... 129
Copy smart card contents ... 131
Copy key part from binary file to smart card ... 132
Create CCA key parts ... 133
Duplicate TKE and EP11 smart card ... 134
Generate EP11 master key parts ... 134
TKE customization ... 134

Chapter 7. Using the Crypto Module Notebook to administer CCA crypto modules 137
Notebook mode ... 137
Crypto Module Notebook function menu ... 138
Tabular pages ... 139
Crypto Module Notebook General tab ... 139
Intrusion latch ... 140
Crypto Module Notebook Details tab ... 141
Crypto Module Notebook Roles tab ... 142
Dual-signature commands ... 143
Domain access ... 143
Creating or changing a role ... 144
Deleting a role ... 145
View a role ... 145
Using Guided Create Roles ... 145
Setup Module Policy ... 146
Crypto Module Notebook Authorities tab ... 146
Generating authority signature keys ... 147
Create authority ... 150
Change authority ... 154
Delete authority ... 154

Using Guided Create Authorities ... 155
Setup Module Policy ... 155
Crypto Module Notebook Domains tab ... 155
Domain General page ... 156
Domain Keys page ... 158
Operational keys ... 170
RSA keys ... 183
Domain Controls pages ... 187
Domain Decimalization Tables page ... 190
Domain Restricted PINs page ... 192
Domain Certificates page ... 193
Domain Roles page ... 194
Domain Authorities page ... 195
Domain Audit Log page ... 195
Crypto Module Notebook Co-Sign tab ... 196
Host crypto module index values ... 196
Placing a domain in PCI-compliant mode ... 197
Required dual controls ... 197
Configuring a domain to be in PCI-compliant mode ... 197

Chapter 8. Using the Crypto Module Notebook to administer EP11 crypto modules ... 209
Notebook mode ... 210
Imprint mode ... 210
Crypto Module Notebook Function menu ... 211
Tabular pages ... 212
Crypto Module Notebook Module General tab ... 212
Intrusion latch ... 213
Crypto Module Notebook Module Details tab ... 214
Crypto Module Notebook Module Administrators tab ... 215
Generate signature key ... 216
Add administrator ... 217
Remove administrator ... 217
Setup Module Policy ... 217
Crypto Module Notebook Module Attributes tab ... 217
Crypto Module Notebook Domains tab ... 219
Domain General page ... 220
Domain Administrators page ... 221
Domain Attributes page ... 221
Domain Keys page ... 223
Domain Control Points page ... 225

Chapter 9. Auditing ... 227
TKE Audit Configuration utility ... 227
Service Management auditing functions ... 229
View security logs ... 230
Audit and log management ... 231
Archive security logs ... 235
TKE Security Events Viewer ... 236
TKE Audit Record Upload Configuration utility ... 238
Starting the TKE Audit Record Upload Configuration utility ... 238
Configure TKE for audit data upload ... 239
Uploading audit records ... 240
Enabling and disabling automatic audit record upload ... 240

Chapter 10. Managing keys using TKE and ICSF ... 243
Changing master keys ... 243

Adding host crypto modules after ICSF initialization ... 244
Loading operational keys to the CKDS ... 245
Installing RSA keys in the PKDS from a data set ... 248

Chapter 11. Cryptographic Node Management utility (CNM) ... 251
Crypto adapter logon ... 251
File menu ... 252
Crypto Node menu ... 252
TKE crypto adapter clock-calendar ... 252
Access Control menu ... 253
Initialize ... 253
Managing profiles ... 254
Managing roles ... 264
Save user roles and profiles ... 270
Load user roles and profiles ... 270
Check TKE crypto adapter group profiles ... 271
Load TKEGRPMB role ... 271
TKE Workstation Logon Profile Wizard ... 271
Master Key menu ... 271
Auto Set and Create Random Master Key ... 272
Clear new ... 272
Parts — Loading a new master key from clear key parts ... 273
Smart card parts — generating master key parts to a smart card ... 274
Smart card parts — loading master key parts from a smart card ... 276
Set — setting the master key value ... 277
Verify — verifying the master key ... 277
Key Storage menu ... 279
Reenciphering key storage ... 279
Smart card menu ... 280
Change PIN ... 281
Generate TKE crypto adapter logon key ... 282
Display smart card details ... 282
Manage smart card contents ... 283
Copy smart card ... 285
CNM common errors ... 288

Chapter 12. Smart Card Utility Program (SCUP) ... 291
General information ... 291
Starting point for all the TKE policy wizards ... 293
Gemalto smart card reader considerations ... 293
File menu functions ... 294
Display smart card information ... 294
Display smart card key identifiers ... 296
TKE zone wizard ... 298
TKE Smart Card wizard ... 298
CA smart card menu functions ... 299
Initialize and personalize a CA smart card ... 299
Create a backup CA smart card ... 301
Change the CA smart card PINs ... 302
TKE smart card menu functions ... 302
Initialize and enroll a smart card ... 302
Personalize a smart card ... 303
Unblock PIN on a smart card ... 303
Change PIN of a smart card ... 304
Enroll smart card in an alternate zone ... 304
Remove alternate zone from smart card ... 304
EP11 smart card menu functions ... 304

Crypto adapter menu functions 305
Enroll a TKE cryptographic adapter in a primary zone 305
View current zone for the crypto adapter 310
Remove current zone from the crypto adapter 310

Appendix A. Secure key part entry 311
Steps for secure key part entry 311
Steps for secure key part entry for a TKE smart card 311
Steps for secure key part entry for a EP11 smart card 316
Entering a key part on the smart card reader 318

Appendix B. LPAR considerations 321

Appendix C. Trusted Key Entry - workstation crypto adapter initialization 323
Cryptographic Node Management Batch Initialization 323
CCA CLU (Code Load utility) 324
CLU processing 324
Checking coprocessor status 327
Loading coprocessor code 327
Validating coprocessor code 327
Checking system status 327
Resetting coprocessor 328
Removing coprocessor CCA code and zeroizing CCA 328
Help menu 328

Appendix D. Clear RSA key format 329

Appendix E. Trusted Key Entry applications and utilities 331
Using USB flash memory drives with TKE applications and utilities 333
Begin Zone Remote Enroll Process 333
CCA CLU 333
Complete Zone Remote Enroll Process 333
Configure Displayed Hash Size 334
Enhanced Password Encryption Policy 334
EP11 Transport Wrapping Key Policy 334
Configure Printers 335
Cryptographic Node Management batch initialization 335
Cryptographic Node Management utility 335
Edit TKE files 336
Add Access Control Points utility 339
Smart Card Utility Program 339
TKE Audit Configuration utility 340
TKE Audit Record Upload Configuration utility 340
TKE File Management utility 340
TKE workstation code information 343
Configuration migration 343
Migrate Host Crypto Module Public Configuration Data 344
Configuration migration tasks 345
Signature collection 346
Window actions 347
Instructions for migrating key material 349
OA proxy 349
Smart card applet level for configuration migration 350
Restriction on CCA User Defined Extensions (UDXs) 350
Service Management tasks 350
Analyze console internal code 351
Archive security logs 351

Authorize internal code changes ... 351
Backup critical console data ... 351
Change console internal code ... 352
Change password ... 353
Customize scheduled operations ... 353
Format media ... 358
Audit and log management ... 360
Hardware messages ... 360
Lock console ... 362
Manage print screen files ... 362
Network diagnostic information ... 363
Rebuild vital product data ... 363
Offload virtual RETAIN data to removable media ... 363
Password protect console ... 364
Save/restore customizable console data ... 364
Save upgrade data ... 364
Shutdown or restart ... 365
Transmit console service data ... 366
Users and tasks ... 368
View console events ... 369
View console information ... 370
View console service history ... 371
View console tasks performed ... 373
View licenses ... 374
View security logs ... 375

Appendix F. TKE best practices ... 377
Checklist for loading a TKE machine - passphrase ... 377
Checklist for loading a TKE machine - smart card ... 379

Appendix G. TKE hardware support and migration information ... 383
TKE release and feature codes available by CEC levels ... 383
Smart card readers and smart cards orderable by TKE release ... 383
TKE (LIC) upgrade paths ... 385
Host cryptographic modules managed by TKE ... 386

Appendix H. Hardware Security Module (HSM) event log entries that CCA version 6.0.3 supports ... 387

Appendix I. Multi-Factor Authentication (MFA) and the TKE ... 393

Appendix J. Accessibility ... 395
Accessibility features ... 395
Consult assistive technologies ... 395
Keyboard navigation of the user interface ... 395
Dotted decimal syntax diagrams ... 395

Notices ... 399
Terms and conditions for product documentation ... 400
IBM Online Privacy Statement ... 401
Policy for unsupported hardware ... 401
Minimum supported hardware ... 401
Trademarks ... 402

Index ... 403

Figures

1. TKE Console - initial panel 12

2. TKE Console - pre-login panel 13

3. Log on with other privileged mode access console user names 13

4. Trusted Key Entry for ADMIN - categorized 14

5. Service Management – No Privileged Mode Access 15

6. Multiple primary zones 50

7. Entry example 74

8. Example of reserving a port 74

9. Format of AUTHCMD 74

10. Assign a user ID to CSFTTKE in FACILITY class 75

11. Assign a User ID to CSFTTKE in APPL Class 75

12. Assign a user ID to a started task 75

13. Sample startup procedure 76

14. Start the TKE server 77

15. Cancel the TKE server 77

16. Login with ADMIN user name 78

17. The TKE Workstation Setup wizard Welcome window 78

18. Customize Network Settings - Identification Tab 81

19. Customize Network Settings LAN Adapters Tab 81

20. Local Area Network 82

21. Customize Network Settings - Name Services Tab 82

22. Network Diagnostic Information Task 83

23. Customize Console Date and Time Window 83

24. Configure NTP settings..... 84
25. Add Network Time Server..... 84
26. Add Access Control Points utility..... 89
27. Configure 3270 Emulators..... 93
28. Add 3270 Emulator Session..... 93
29. Start or Delete a 3270 Emulator Session..... 94
30. Manage trusted signing certificates..... 94
31. Import remote certificate..... 95
32. Confirm import..... 95
33. Manage trusted signing certificates..... 95
34. Configure 3270 emulators..... 96
35. Add 3270 emulator session..... 96
36. Configure 3270 emulators: Start at console startup..... 96
37. Crypto Adapter logon window with passphrase profiles..... 97
38. Enter passphrase for logon..... 98
39. Change logon passphrase..... 98
40. Crypto Adapter group logon window with passphrase profiles..... 98
41. Enter passphrase for logon..... 99
42. Crypto Adapter Group logon window with passphrase profile ready..... 99
43. Crypto Adapter Logon Window with smart card profiles..... 100
44. Insert the smart card..... 100
45. Enter smart card PIN..... 100
46. Crypto Adapter Group logon window with smart card profiles..... 101
47. Insert the smart card..... 101
48. Crypto Adapter Group logon window with smart card profile ready..... 101

49. Authenticate Crypto Module 103

50. TKE Preferences 105

51. Create Host 106

52. Host Logon window 108

53. Example of a copy 110

54. Example of a paste into an individual module 111

55. Example of a paste into all the modules in a host 111

56. Main window 112

57. Main window - working with domain groups 113

58. Create New CCA Domain Group 115

59. Change CCA Domain Group 117

60. View CCA Domain Group 118

61. Check Domain Group Overlap 119

62. Duplicate Domains Not Allowed 120

63. Domain Group Overlap Details 120

64. Compare Group 121

65. Select Authority Signature Key Source 123

66. Specify Authority Index 123

67. Load Signature Key 124

68. Select Transport Key Policy 125

69. TKE Workstation DES Key Storage Window 127

70. TKE Workstation PKA Key Storage Window 128

71. TKE Workstation AES Key Storage window 129

72. Smart card contents (for TKE smart cards) 130

73. Smart card contents (for EP11 smart cards) 130

74. Select keys to copy..... 132
75. Copy binary file key part utility..... 133
76. Create CCA key parts..... 134
77. Crypto Module Notebook for CCA - General Page 137
78. Window to Release Crypto Module..... 138
79. Set clock..... 140
80. Dual Validation..... 142
81. Create New Role page..... 144
82. Guided Create Roles page..... 145
83. Authorities Page..... 147
84. Completed generate signature key window 148
85. Save authority signature key..... 149
86. Generate signature key..... 149
87. Key saved status message..... 150
88. Select source of authority signature key..... 150
89. Create new authority..... 151
90. Load Signature Key from binary file..... 152
91. Create New Authority with Role Container..... 153
92. Change Authority 154
93. Guided Create Authorities page..... 155
94. Domain General page - Normal mode..... 156
95. Select mode panel for IMPRINT mode..... 157
96. Select mode panel for PCI-COMPLIANT mode..... 157
97. Select mode panel for PCI-COMPLIANT mode, key migration allowed..... 157
98. Domain in IMPRINT mode..... 158

99. Domain Keys page....159
100. Enter number of keys to be generated....164
101. Select source of new AES Master Key part....165
102. Select key part from TKE smart card....165
103. Warning message....165
104. Key part information panel....166
105. Enter Key Value - Blind Key Entry....166
106. Enter Key Value....167
107. Specify Key File....167
108. Generate Operational Key - predefined EXPORTER key type....171
109. Generate Operational Key - USER DEFINED....172
110. Generate Operational Key panel - AES MAC operational key....172
111. AES MAC Key Attributes panel....173
112. Key part information - first DES key part....174
113. Key part information - first DES key part PCI-compliant....175
114. DES key part register information....175
115. Enter key value - keyboard source for predefined EXPORTER key type....176
116. DES Key part information - add part....177
117. Complete DES Operational Key Part Register - predefined EXPORTER key type....177
118. DES Key part register information - predefined EXPORTER key type in Complete state....178
119. Key Part Information panel for an AES operational key other than DATA....178
120. Key Part Register Information panel for an AES operational key other than DATA....179
121. View Operational Key Part Register panel - AES CIPHER operational key....180
122. Key Part Register Information panel - AES CIPHER operational key....180
123. Clear Operational Key Part Register panel -- AES CIPHER operational key....181

124. Install IMP-PKA Key Part in Key Storage 182
125. Install AES IMPORTER Key Part in Key Storage 183
126. Generate RSA Key 184
127. Encipher RSA Key 185
128. Load RSA Key to PKDS 186
129. Load RSA Key to Dataset 187
130. Domain Controls page 188
131. Decimalization tables page 190
132. Table entry options 191
133. Enter new decimalization table value 191
134. Domain Restricted PINs page 192
135. Domain certificates 194
136. Domain audit log 195
137. PCI-HSM smart card wizard 199
138. PCI-HSM smart card wizard - Welcome screen 199
139. TKE smart card wizard 199
140. TKE smart card wizard - Welcome screen 200
141. TKE smart card wizard - Creation screen 200
142. Enter imprint mode 202
143. Select source for signature key for command 202
144. Setup PCI Environment 203
145. Setup PCI Environment - Welcome screen 204
146. Setup domain-specific roles 204
147. Setup PCI environment 204
148. Setup domain specific authorities 205

149. Setup domain specific authorities - Summary....205
150. Move an imprint mode domain to compliant mode....206
151. Authority error message....207
152. Select source....207
153. Enter PCI mode - Co-sign....207
154. Co-sign pending....208
155. PCI-compliant mode....208
156. Crypto Module Notebook for EP11 - Module General page....209
157. Window to release crypto module....211
158. Module Administrators page....216
159. Generate Signature Key....216
160. Module Attributes page....218
161. Domain General page....221
162. Domain Attributes page....222
163. Domain Keys page....224
164. Domain Control Points page....226
165. Default settings for auditing....228
166. Auditing is off....228
167. Example of expanded auditing points....229
168. Set heartbeat interval....229
169. Viewing the security logs....230
170. Viewing additional details of the security logs....231
171. Audit and Log Management dialog....232
172. Audit and Log Management dialog (security log data selected)....233
173. Security Log....234

174. Export Data..... 235

175. Archiving the security logs..... 236

176. TKE Security Events..... 237

177. TKE Audit Record Upload Configuration utility..... 238

178. Specify Host Information dialog..... 239

179. Other hosts and associated timestamps..... 239

180. Specify Host Login Information..... 240

181. ICSF primary menu panel..... 246

182. Coprocessor Management panel..... 246

183. Operational Key Load panel..... 247

184. Operational Key Load panel..... 248

185. Operational Key Load Panel - ENC-ZERO and CV values displayed..... 248

186. Operational Key Load Panel - AES -VP displayed..... 248

187. Selecting the TKE option on the ICSF primary menu panel..... 249

188. PKA Direct Key Load..... 249

189. CNM main window..... 251

190. CNM main window — Crypto Node Time sub-menu..... 252

191. Current Coprocessor Clock 253

192. Sync time with host window..... 253

193. Profile Management window listing the profiles on the TKE's local crypto adapter..... 255

194. From the CCA Node Management Utility's Profile Management window, click on the New push button..... 256

195. Select profile type..... 256

196. Select profile and click Edit..... 257

197. From the CCA Node Management Utility's Profile Management window, click on the Open push button..... 257

198. Specify file to open dialog..... 258

199. Profile Management window for passphrase profiles..... 259

200. Profile Management window for smart card profiles.....261

201. Profile Management window for group profiles.....262

202. Role Management window listing the roles on the TKE workstation crypto adapter..... 265

203. From the CCA Node Management Utility's Role Management window, click on the New push button..... 266

204. Select role and click Edit..... 266

205. From the CCA Node Management Utility's Role Management window, click on the Open push button..... 267

206. Specify file to open dialog..... 268

207. Role Management window modifying role attributes.....269

208. CNM main window — Master Key pull-down menu..... 272

209. Clear New Master Key Register — confirm clearing.....273

210. Clear New Master Key Register — register cleared.....273

211. Load Master Key from Clear Parts.....273

212. Load Master Key from Clear Parts — key part randomly generated.....274

213. Load Master Key from Clear Parts — key part successfully loaded.....274

214. Smart Card Master Key Parts panel..... 275

215. Smart Card Master Key Parts panel — key part description prompt..... 275

216. Smart Card Master Key Parts panel — key part generated.....276

217. Master Key Part Smart Card panel — loading a Crypto Adapter key part from a smart card..... 277

218. Master key part successfully loaded.....277

219. Master Key Verify sub-menu..... 278

220. Master Key Register Verification panel - verification pattern is displayed..... 278

221. Master Key Register VP compare successful.....279

222. CNM main window — Key Storage pull-down menu.....279

223. Key Storage Management Panel – key labels list..... 280

224. CNM main menu — Smart Card pull-down menu..... 281
225. Change PIN — insert smart card prompt..... 281
226. Change PIN — enter current PIN prompt..... 281
227. Change PIN — enter new PIN prompt..... 281
228. Generate Crypto Adapter Logon Key — insert smart card..... 282
229. Generate Crypto Adapter Logon Key — PIN prompt..... 282
230. Generate Crypto Adapter Logon Key — User ID prompt..... 282
231. Generate Crypto Adapter Logon Key — key generated..... 282
232. Display Smart Card Details — insert smart card prompt..... 282
233. Display Smart Card Details — public information displayed..... 283
234. Manage Smart Card contents — contents of smart card are displayed..... 284
235. Manage Smart Card contents — confirm delete prompt..... 284
236. Manage Smart Card contents..... 285
237. Copy Smart Card — insert first smart card..... 286
238. Copy Smart Card — asked for the TKE or EP11 smart card..... 286
239. Copy Smart Card — smart card contents are displayed..... 286
240. Copy Smart Card — highlight object to copy and direction..... 287
241. Copy Smart Card — first smart card PIN prompt..... 287
242. Copy Smart Card — second smart card PIN prompt..... 287
243. Establishing a secure session between the two smart cards..... 287
244. Objects are copied to the target smart card..... 287
245. Copy Smart Card — objects are copied to the target container..... 288
246. First screen of TKE Smart Card Utility Program (SCUP) with 2 readers..... 292
247. First screen of TKE Smart Card Utility Program (SCUP) with more than 2 readers..... 293
248. Display smart card information..... 295

249. Display of smart card key identifiers....297
250. First step for initialization and personalization of the CA smart card....299
251. Zone key length window....299
252. Message if card is not empty....300
253. Initialization message for CA smart card....300
254. Enter first PIN for CA smart card....300
255. Enter second PIN twice for CA smart card....300
256. Enter zone description for CA smart card....300
257. Enter card description for CA smart card....300
258. Building a CA smart card....301
259. Begin creation of backup CA smart card....301
260. Initialization of backup CA smart card....301
261. Continue creation of backup CA smart card....301
262. Establish secure connection for backup CA smart card....301
263. Building backup CA smart card....302
264. Select first CA PIN....302
265. Initialize and enroll TKE smart card....303
266. Initializing TKE smart card....303
267. Building TKE smart card....303
268. Personalizing TKE smart card....303
269. Enroll TKE smart card in alternate zone....304
270. View current zone for a TKE cryptographic adapter....305
271. Select local zone....305
272. Certifying request for local Crypto Adapter enrollment....306
273. Message for successful Crypto Adapter enrollment....306

274. View current zone after Crypto Adapter enrollment....306
275. View current zone after crypto adapter enrollment.... 310
276. Choosing secure key part entry from the domains keys panel.... 311
277. Enter description panel for secure key part entry.... 312
278. DES USER DEFINED operational key for secure key part entry.... 312
279. AES non-DATA operational key for secure key part entry.... 313
280. Secure key part entry — insert TKE smart card into reader....313
281. Secure key part entry — enter key part digits.... 313
282. Secure key part entry card identification....314
283. Secure key part entry — enter key part digits.... 314
284. Secure key part entry — DES key part information for a master key....315
285. Secure key part entry — AES key part information for a master key....315
286. Secure key part entry — DES key part information for operational key.... 315
287. Secure key part entry — AES DATA operational key.... 316
288. Secure key part entry — AES non-DATA key.... 316
289. Secure key part entry — message for successful execution....316
290. Choosing secure key part entry from the domain keys window....317
291. Secure key part entry card identification....317
292. Secure key part entry -- enter key part digits....318
293. Secure key part entry -- key part information window....318
294. An example of TKE host and TKE target LPARs without domain sharing....322
295. An example of TKE host and TKE target LPARs with domain sharing....322
296. Cryptographic Node Management Batch Initialization task window....323
297. Cryptographic Node Management Batch Initialization task output window.... 324
298. CLU command check boxes....324

299. CLU View menu 325
300. Output log file 325
301. CLU command history 326
302. Successful completion of CLU commands 326
303. CLU File menu 327
304. Configure Displayed Hash Size task window 334
305. Enhanced Password Encryption Policy window 334
306. EP11 Transport Wrapping Key Policy window 335
307. Edit TKE Files task window 336
308. Editor - File menu items 337
309. Editor - Edit menu items 338
310. Editor - Style Menu Items 339
311. TKE File Management Utility task window 341
312. TKE File Management - directory options 342
313. Delete confirmation window 342
314. Window for inputting a filename 342
315. TKE Workstation Code Information window 343
316. Configuration Migration Tasks panel 345
317. Backup Critical Console Data -- select backup destination 352
318. Backup Critical Console Data -- in progress 352
319. Backup Critical Console Data -- final status 352
320. Customize Scheduled Operations task window 353
321. Customize Scheduled Operations - Add a Scheduled Operation window 354
322. Customize Scheduled Operations - Set Date and Time window 355
323. Customize Scheduled Operations - Set repetition of operation 356

324. Completion window for Adding Scheduled Operation..... 356

325. Customize Scheduled Operations..... 357

326. Details view of scheduled operation..... 358

327. New time range window for scheduled operation..... 358

328. Format Media dialog..... 359

329. Select Media Device..... 360

330. Hardware Messages window..... 361

331. Hardware Messages - details window..... 361

332. Prompt for password..... 362

333. Prompt to unlock console..... 362

334. Virtual RETAIN Data Offload window..... 363

335. Successful offload of data..... 363

336. Virtual RETAIN Data Offload incorrect media error 364

337. Save Upgrade window..... 364

338. Save upgrade success window..... 365

339. Shutdown or Restart task window..... 365

340. Confirmation window..... 366

341. Transmit Console Service Data..... 366

342. Transmit Console Service Data - successful completion..... 367

343. Update problem number for virtual RETAIN file..... 367

344. Select the virtual RETAIN files..... 368

345. Copying data to selected media..... 368

346. Users and Tasks window..... 369

347. View Console Events window..... 369

348. View Console Information window..... 370

349. Internal Code Change Details window....371

350. View Console Service History window....372

351. Problem summary....372

352. Problem Analysis....373

353. View Console Tasks Performed window....374

354. View Licenses window....375

Tables

1. CAA code loaded for specific releases of TKE....17

2. Definition files and their corresponding role or profile....20

3. System-supplied role definition files for passphrase roles....21

4. System-supplied role definition files for smart card roles....21

5. System-supplied profile definition files for passphrase profiles....22

6. ACPs assigned to the SCTKEADM role....24

7. ACPs assigned to the SCTKEUSR role....25

8. ACPs assigned to the TKEGRPMB role....27

9. ACPs assigned to the DEFAULT role when initialized for use with smart card profiles....28

10. ACPs assigned to the TKEADM role....32

11. ACPs assigned to the TKEGRPMB role....33

12. ACPs assigned to the TKEUSER role....34

13. ACPs assigned to the KEYMAN1 role....35

14. ACPs assigned to the KEYMAN2 role....36

15. ACPs assigned to the DEFAULT role when initialized for use with passphrase profiles....37

16. Prerequisite TKE wizard: TKE Smart Card Wizard....40

17. TKE security policy implementation wizards....40

18. Applet version by TKE release....44

19. Applet version by TKE release....46

20. CA smart card usage....47

21. TKE smart card usage....48

22. Smart card task checklist....52

23. TKE feature code changes....60

24. TKE Data Directory....62
25. CNM Data Directory (system-supplied files)....63
26. CNM Data Directory (Customer-named files)....64
27. Configuration Data Directory....64
28. CCA Audit Log Data Directory....65
29. Summary of data to be copied from the source TKE....65
30. TKE management system task checklist....73
31. Key types and actions for the supported crypto modules....159
32. Module index type displayed on the TKE....196
33. Smart cards....201
34. Smart cards and purpose....205
35. Smart card migration actions....294
36. Decimal to Hexadecimal Conversion Table....319
37. Tasks, applications and utilities accessible by console user name....331
38. Allowable labels when formatting USB flash memory....359
39. TKE release and feature codes available by CEC level....383
40. Smart card readers and smart cards orderable by TKE release....384
41. Summary of when a TKE workstation can be upgraded....385
42. Host cryptographic modules managed by TKE LIC....386
43. Hardware Security Module (HSM) event log entries....387

About this information

This information introduces Version 9.2 of the Trusted Key Entry (TKE) customized solution for ICSF.

It includes information to support these tasks for the solution:

- Planning
- Installing
- Administering
- Customizing
- Using

Who should read this information

This information is for technical professionals who will be installing, implementing and administering Version 9.2 of the Trusted Key Entry product. It is intended for anyone who manages cryptographic keys, usually a security administrator.

To understand this information you should be familiar with z/OS, OS/390®, RACF®, ICSF, VTAM®, and TCP/IP. You should also be familiar with cryptography and cryptographic terminology.

The information provided with ICSF provides the background information you need to manage cryptographic keys. For more information, see *z/OS Cryptographic Services ICSF Overview* and *z/OS Cryptographic Services ICSF Administrator's Guide*.

How to use this information

The major topics are:

Chapter 1, “Overview,” on page 1, gives a high-level explanation of the TKE workstation, its relationship to ICSF and the environment it requires for operation.

Chapter 2, “Using smart cards with TKE,” on page 41, gives an explanation of the smart card support for the TKE workstation.

Chapter 3, “TKE upgrade and migration actions,” on page 55, provides details on migrating from previous versions of TKE.

Chapter 4, “TKE setup and customization,” on page 73, provides information about using TCP/IP and the host files needed by TKE. It also explains how to configure the TKE workstation for TCP/IP and initialize the TKE workstation.

Chapter 5, “TKE up and running,” on page 97, provides preliminary setup and initialization tasks that are necessary for operation.

Chapter 6, “Main window,” on page 105, explains the beginning window of the TKE program and the functions and utilities accessible from it.

Chapter 7, “Using the Crypto Module Notebook to administer CCA crypto modules,” on page 137, explains how to work with CCA crypto modules. The status of the master keys and key parts are displayed. This window is where the keys can be generated, loaded and cleared. The domain controls are set here. The zeroize domain function is accessed from here. RSA handling is described here.

Chapter 8, “Using the Crypto Module Notebook to administer EP11 crypto modules,” on page 209 explains how to work with EP11 crypto modules.

Chapter 9, “Auditing,” on page 227, provides information on auditing.

© Copyright IBM Corp. 2000, 2021

Chapter 10, “Managing keys using TKE and ICSF,” on page 243, explains how ICSF is used when loading and importing keys to a host crypto module on IBM® S/390®, IBM System z10, IBM zEnterprise® 196 or IBM zSeries hardware.

Chapter 11, “Cryptographic Node Management utility (CNM),” on page 251, provides information on the CNM utility tasks.

Chapter 12, “Smart Card Utility Program (SCUP),” on page 291, provides information on the SCUP tasks.

Appendix A, “Secure key part entry,” on page 311, provides information on secure entry of a known key part onto a TKE or EP11 smart card.

Appendix B, “LPAR considerations,” on page 321, discusses host setup considerations for managing host crypto modules across multiple logical partitions.

Appendix C, “Trusted Key Entry - workstation crypto adapter initialization,” on page 323, provides information on the TKE Workstation Cryptographic Adapter Initialization.

Appendix D, “Clear RSA key format,” on page 329, provides information on the format of RSA-entered keys.

Appendix E, “Trusted Key Entry applications and utilities,” on page 331, provides information on TKE console applications and utilities and Service Management tasks.

Appendix F, “TKE best practices,” on page 377, provides information on Checklists for Loading a TKE Machine for both passphrase and smart card.

Appendix G, “TKE hardware support and migration information,” on page 383, provides information on TKE release and feature codes available by CEC levels, smart card readers and smart cards orderable by TKE release, TKE (LIC) upgrade paths, and host cryptographic modules managed by TKE.

Appendix H, “Hardware Security Module (HSM) event log entries that CCA version 6.0.3 supports,” on page 387, provides information on all the possible Hardware Security Module (HSM) event log entries that CCA version 6.0.3 supports.

Appendix J, “Accessibility,” on page 395, provides information on accessibility features that help a user who has a physical disability to use software products successfully.

“Notices” on page 399, provides information on notices, programming interface information, and trademarks.

Where to find more information

The information in this book is supported by other books in the ICSF library and other system libraries. These books include:

- *z/OS Cryptographic Services ICSF Administrator's Guide*
- *z/OS Cryptographic Services ICSF System Programmer's Guide*
- *z/OS Cryptographic Services ICSF Application Programmer's Guide*
- *z/OS Cryptographic Services ICSF Overview*
- *z/OS Cryptographic Services ICSF Messages*
- *Z Service Guide for TKE Workstations*, GC28-6980
- *PR/SM Planning Guide*, SB10-7153

How to send your comments to IBM

We invite you to submit comments about the z/OS product documentation. Your valuable feedback helps to ensure accurate and high-quality information.

Important: If your comment regards a technical question or problem, see instead “If you have a technical problem” on page xxxi.

Submit your feedback by using the appropriate method for your type of comment or question:

Feedback on z/OS function
If your comment or question is about z/OS itself, submit a request through the IBM RFE Community (www.ibm.com/developerworks/rfe/).

Feedback on IBM Knowledge Center function
If your comment or question is about the IBM Knowledge Center functionality, for example search capabilities or how to arrange the browser view, send a detailed email to IBM Knowledge Center Support at ibmkc@us.ibm.com.

Feedback on the z/OS product documentation and content
If your comment is about the information that is provided in the z/OS product documentation library, send a detailed email to mhvrcfs@us.ibm.com. We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

To help us better process your submission, include the following information:

- Your name, company/university/institution name, and email address
- The following deliverable title and order number: z/OS Cryptographic Services ICSF TKE Workstation User's Guide, SC14-7511-09
- The section title of the specific information to which your comment relates
- The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive authority to use or distribute the comments in any way appropriate without incurring any obligation to you.

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem

If you have a technical problem or question, do not use the feedback methods that are provided for sending documentation comments. Instead, take one or more of the following actions:

- Go to the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

© Copyright IBM Corp. 2000, 2021

Summary of changes

This information includes terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations for the current edition are indicated by a vertical line to the left of the change.

Changes made in z/OS Version 2 Release 4 (V2R4)

This document contains information previously presented in *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SC14-7511-08.

The most recent updates are listed at the top of each section.

New

November 2020 refresh

The following features are available on TKE 9.2 if the active level of your TKE Tower Code is 7 or above. If you need to upgrade your tower code, ask IBM to install P46690.007 on your TKE 9.2 system.

Note: To check the active level of your TKE Tower Code, open the 'View console information' application. This application is in the 'Service Management' area of the IBM Trusted Key Entry Console. For more information, see “View console information” on page 370.

- When you bring up the pop-up menu in the host container, there is a new option that allows you to add the auto-accept option to all existing host definitions.
- There is now a copy and paste capability available when you create or change domain groups.
- The 'load all new master keys' feature has been changed. It now asks you for the number of master key parts that your master keys have.
- There is a new feature in the Smart Card Utility program that allows you to remove a TKE workstation from a zone.
- The copy binary key parts files to smart card feature now allows you to select more than file at a time.
- If mismatches are found during a compare group operation, the results may now be saved to a file.
- The CCA Setup Module Policy Wizard now allows you to use the TKE workstation Manager 1 and 2 smart cards as the CCA module administrators.
- The TKE Workstation Logon Profile Wizard now allows you to create a second group profile with TKE workstation manager 1 and 2 profiles for use when opening the TKE application.
- The Cryptographic Node Management utility now has a feature that allows you to produce a TKE local crypto adapter role and profile report.
- A new compare group feature has been added to the TKE. You can now run a compare that only includes module-wide settings.

Prior to the November 2020 refresh

- You can use TKE 9.2 to manage Express 7 modules that are running in Common Cryptographic Architecture (CCA) or IBM Enterprise PKCS #11 (EP11) mode. You can also use the wizards found in the Configuration Migration Tasks application to collect data from older Crypto Express modules and apply the data to new Crypto Express 7 modules.

  Note: Crypto Express 7 is available on IBM z15 and TKE 9.2 is the minimum level of TKE that can be used to manage the Crypto Express 7 modules.

© Copyright IBM Corp. 2000, 2021

- With TKE 9.2, you can use AT-TLS connections between the TKE workstation and the host that is running the TKE host transaction program. If you configure the TCP/IP port that the host transaction program is using to use AT-TLS, you must select the new check box in your TKE workstation host definition to specify you are using a TLS connection.
- There are new features in some Common Cryptographic Architecture (CCA) firmware levels that can be exploited from TKE 9.2:
  - Some CCA firmware levels support a new flag that marks AES operational key parts as PCI-compliant. When you generate new AES operational key parts on TKE 9.2, you can turn the PCI-compliant tag on when you create the parts. Tagged key parts can be put in binary files, print files, and on blue smart cards that were initialized on TKE 9.2. When you load an AES operational key, all the parts must have the same PCI-compliant tag value.
  - Some CCA firmware levels keep track of when Access Control Point (ACP) tracking is turned on and off. If you display ACP tracking information from TKE 9.2 and CCA provides tracking interval information, the information is included in your ACP tracking report. The report tells you when tracking was turned on, if or when tracking was turned off, and the number of times tracking was turned off and back on from the last time tracking data was cleared. For additional information, see “Access Control Tracking” on page 189.
  - Some new levels of Common Cryptographic Architecture (CCA) firmware provide the ability to display the ENC-ZERO or CMAC verification patterns for master keys. TKE 9.2 allows you to select which type of verification pattern is displayed if ENC-ZERO and CMAC are available.
- Beginning in TKE 9.2, you can use the IBM Enterprise PKCS #11 (EP11) Transport Wrapping Key Policy to select the EP11 Transport Wrapping Key strength. You would select this policy if you require the EP11 transport wrapping key to be a true 256-bit AES key. If the policy is selected, the transport wrapping key is derived using Diffie-Hellman Key Exchange of 521-bit Elliptic Curve (EC) public keys between the TKE and the host crypto module running IBM Enterprise PKCS#11 (EP11). You can only select this policy when:
  - All your EP11 smart cards are at the minimum part level 00RY790 (Blue Smart cards).
  - All your EP11 smart cards are at the minimum applet version V0.6 (The minimum applet support first appeared in TKE 9.2).
  - All your host IBM Enterprise PKCS #11 modules are at API version 7.04 or later.

  Note: If the policy is not selected, EC-320 Diffie-Hellman Key Exchange is used and a 256-bit AES key with the effective strength of 128-bits is derived.

  For additional information, see “EP11 Transport Wrapping Key Policy” on page 334.
- TKE 9.2 has new usability enhancements that simplify existing management tasks:
  - Beginning in TKE 9.2, you can configure your host definition so that it automatically accepts modules that are successfully authenticated. If, for example, you created and open a new host that has 4 modules, you do not have to explicitly accept each module after they are authenticated. You can select the option to automatically accept modules when you create a host definition or add the option to existing host definitions through the change host function.
  - Beginning in TKE 9.2, the utility that allows you to copy key parts in binary files onto smart cards allows you to select more than one file at a time. This simplifies the process of moving from binary key part files to smart card key part management. For additional information, see “Copy key part from binary file to smart card” on page 132.
  - Beginning in TKE 9.2, when you attempt to delete a Role or Authority from a Common Cryptographic Architecture (CCA) mode host crypto module from inside of a TKE domain group, the delete is attempted on every module included in the group. Previously, the operation stopped the first time the role or authority was not found on a module in the group.
  - When TKE 9.2 detects that a LINUX host supports long user IDs, you are able to enter user IDs with up to 32 characters.
  - Beginning in TKE 9.2, the TKE Workstation Logon Wizard includes a new step that encourages you to remove excess authority from the DEFAULT role after your TKE Workstation administrator

profiles have been created. For additional information, see “TKE Workstation Logon Profile Wizard” on page 271.

Deleted

No content was removed from this information.

Changes made in z/OS Version 2 Release 3 (V2R3)

This document contains information previously presented in *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SC14-7511-07.

The most recent updates are listed at the top of each section.

New

- A new smart card part, 00RY790, was shipped with TKE 9.1. In addition to having the part number printed on it, the card is blue. The blue smart card supports 521-bit Elliptic Curve (EC) cryptography and has more memory than the previous TKE smart card. For additional information, see “Blue smart cards (00RY790)” on page 37.
- TKE 9.1 provides six wizards that work together to implement a comprehensive set of security policies for managing access to the TKE workstation and managing host crypto modules and their domains. All of the policies require that something be stored on a smart card. Therefore, the first wizard, TKE Smart Card Wizard, creates all the smart cards the other wizards need. The TKE provides five additional wizards that setup the minimum recommended security policies for managing administrators responsible for specific tasks. For additional information, see “TKE security policy wizards” on page 38.
- With TKE 9.1, you have access to a new type of domain group compare. This function performs the same module-wide comparisons as the Compare Group function. When doing the domain-specific comparisons, this function only compares domains that have the same index value on all crypto modules in the group. In other words, domain 0 on crypto module A is compared only with domain 0 on all other crypto modules, domain 1 is compared with all other domain 1's, and so on. This group compare only has value if there is more than one module in the group.
- Beginning in TKE 9.1, there is a Duplicate TKE or EP11 Smart Card feature available from the TKE Utilities pull down menu. This utility is used to delete existing content from a target smart card and then copy data from a source smart card to the target smart card. Once the duplicate feature has determined you can copy the contents of a source smart card to a target smart card, there are two types of duplicate functions that you can do:

  Duplicate an entire smart card
  The target smart card becomes a complete copy of the source smart card. All the current content of the target smart card is deleted and then all the content of the source smart card is copied to the target smart card.

  Only duplicate master and operational key parts
  Any signature keys that are on the target smart card stay on the target smart card. Only the current master and operational key parts on the target smart card are deleted and then all of the master and operational key parts from the source smart cards are copied to the target smart cards.

  Note: You can only use the duplicate feature if the target smart card is at the same or newer applet version as the source smart card and the primary zone of the source smart card matches the primary or alternate zone of the target smart card.

  For additional information, see “Moving TKE and EP11 smart card data to smart cards in a new zone” on page 53 and “Moving data from a TKE smart card in a 1024-bit zone to a blue smart card” on page 53.

Changed

- TKE 9.1 supports the generation of 24-byte DES operational keys parts. There is no change to key load process.
- TKE 9.1 supports new key usage values, which are available in CCA 5.4 and CCA 6.1. You select the key usage values when the key parts are created.
- Beginning in TKE 9.1, audit records are saved and displayed in human-readable form when retrieved from the Download EP11 Audit Data task. You no longer have to run the data through a user created utility to parse the data.

Deleted

No content was removed from this information.

Changes made in z/OS Version 2 Release 3 (V2R3)

This document contains information previously presented in *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SC14-7511-06.

The most recent updates are listed at the top of each section.

New

- "Using the IDENTIV smart card reader" on page 42 is added.
- "Using the Gemalto smart card reader" on page 43 is added.
- "Things to consider" on page 44 is added.
- "Gemalto smart card reader considerations" on page 293 is added.
- TKE 9.0 adds support for dual validation of the crypto module. This can be found on the host crypto module's details tab.
- TKE 9.0 adds support for allowing key material to be copied from smart cards in one TKE zone to smart cards in another zone through assigning smarts cards to alternate zones.
- TKE 9.0 adds the ability to create key parts without opening a host to allow the key administrators to create key parts while offline or to prepare key parts before a host is defined.
- TKE 9.0 adds a TKE Security Event Viewer application that is available for the Privileged Mode Access ID of AUDITOR. It provides an alternate means of working with the TKE audit log, with save-to-file and print capabilities, simple text search, and the ability to limit the displayed entries to a specific time and date range.
- TKE 9.0 provides every TKE with TKE 9.0 a heartbeat audit record. Heartbeat audit records are records that get written if no audit events occur during a specific interval. The heartbeat audit cannot be turned off, but its interval can be changed.
- TKE 9.0 adds a step in the TKE Workstation Setup wizard to change the role of a TKE workstation group profile MEMBER to TKEGRPMB if it is set to the DEFAULT role.
- The number of commands that are needed to Load, Set, or Clear commands in a Domain Group are significantly reduced with TKE 9.0 with CCA version 5.3. Depending on the size of a domain group, users might experience an improvement when they are doing a Load, Set, or Clear operation from inside a domain group.
- TKE 9.0 EP11 smart card applet now supports secure key entries of EP11 master key parts.
- TKE 9.0 adds support for the CEX6C crypto module, including support for working with domain certificates and support for a mode of operation that is designed to be compliant with the *Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM)* standard, Version 3.0, dated June 2016 (PCI-compliant mode). PCI-HSM support includes the following features:

  - Each domain can exist in either normal mode, imprint mode, or PCI-compliant mode.
  - The host crypto module clock can be set from TKE.
  - For each domain in imprint mode or PCI-compliant mode, an audit log on the crypto module is exposed and active. The audit log can hold a maximum of 512 audit records. These must be downloaded to file periodically. Most TKE administrative actions to the domain are prevented from executing when the domain audit log on the crypto module is full.
  - Each domain in imprint mode or PCI-compliant mode has a set of domain-specific roles and authorities that are used to administer the domain.
- "Placing a domain in PCI-compliant mode" on page 197 is new.
- "TKE Security Events Viewer" on page 236 is new.
- Appendix H, "Hardware Security Module (HSM) event log entries that CCA version 6.0.3 supports," on page 387 is new.

Changed

- "Gemalto smart card reader considerations" on page 293 is updated.
- "TKE hardware" on page 1 is updated.
- "Domain modes" on page 9 is updated.
- "Smart card readers and smart cards orderable by TKE release" on page 383 is updated.
- TKE 9.0 adds the ability for TKE data to be saved to, or restored from, removable media in the same directory structure they are found on the TKE. Previously, data copied to be removed was placed in the base directory of the removable media. When you would copy data from one TKE to another, you had to remember which directory each file went into.
- TKE 9.0 adds a usability improvement to the Cryptographic Node Management utility (CNM). Previously, when you created a new profile, the default activation period was one day. With TKE 9.0, the default activation period is one year.

Deleted

No content was removed from this information.

Changes made in z/OS Version 2 Release 2 (V2R2)

This document contains information previously presented in *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SC14-7511-04.

New

- Download EP11 Audit Data was added to "Crypto Module Notebook Function menu" on page 211.
- TKE 8.1 adds TKE support for the coordinated change master key function. Previously this function could be performed only using ICSF panels.
- TKE 8.1 adds support for domain-only apply. This allows configuration settings from a single source domain to be applied to one or more target domains without changing module-level configuration settings or non-target domains.
- TKE 8.1 adds several wizard-like features to create roles and authorities, create the smart cards used to implement a TKE zone, and create the smart cards needed to implement a migration zone.
- TKE 8.1 adds support for HMAC operational keys.
- TKE 8.1 supports a new option on domain groups to clear and load operational key registers for all domains in the group rather than for just the master domain.

- TKE 8.1 adds support for access control tracking. Access control tracking identifies what access control points are referenced as applications run in a domain.
- TKE 8.1 supports a new function to copy a key part from a binary file to a smart card.
- TKE 8.1 supports new administrative settings to require enhanced password encryption for host connections and to disable TKE console automatic logon.

Changed

- The ICSF primary menu panel and the Coprocessor Management panel in “Loading operational keys to the CKDS” on page 245 have been updated.

Deleted

No content was removed from this information.

Chapter 1. Overview

The ICSF Program Product provides secure, high-speed cryptographic services in the z/OS and OS/390 environment. By using cryptographic keys on the Integrated Cryptographic Service Facility (ICSF), you can perform functions such as protecting data, verifying messages, generating and verifying signatures, and managing personal identification numbers (PINs). Cryptographic systems use cryptographic keys. A cryptographic key instructs the cryptographic function in its operation. The security of the cryptographic service and its results depend on safeguarding the cryptographic keys.

Cryptographic systems use a variety of keys that must be securely managed. ICSF uses a hierarchical key management approach and provides one or more master keys to protect all the other keys that are active on your system.

Trusted Key Entry (TKE) is an optional hardware feature of IBM Z® that provides a management tool for Z host cryptographic coprocessors. The main features provided by TKE are:

- Compliance-level, hardware-based, master key management for Z host cryptographic coprocessors.

  Notes:

  – Key material can be kept on smart cards. This provides an additional level of data confidentiality and security. The use of smart card is required to meet some compliance requirements.

  – The same key management mechanisms are also available for many types of Common Cryptographic Architecture (CCA) operational keys.
- Highly secure management of the configuration of the Z host cryptographic coprocessors.
- Highly secure and speedy method to collect configuration data from one Z host cryptographic coprocessor and apply the data to another host cryptographic coprocessor. This feature is used for card cloning in the case of new hardware deployments or recovery situations.
- Grouping support is provided so that multiple Z host cryptographic coprocessors and multiple domains on Z host cryptographic coprocessors can be managed together.
- The TKE provides separation of duties mechanisms to require multiple security officers to perform critical operations.

TKE works together with ICSF:

- The TKE manages Z cryptographic coprocessors through a network-connected Z. The ICSF TKE host transaction program must be started.
- Key registers are loaded from the TKE, but keys are set from ICSF. This requires an active Time Sharing Option/Extended (TSO/E) session on the TKE workstation or another workstation located nearby. The ICSF panels are used to load operational keys from key part registers, set master keys, and initialize or reencipher the CKDS (Cryptographic Key Data Set), PKDS (Public Key Data Set), and TKDS (PKCS #11 Token Data Set). The TSO/E session is also required to disable and enable PKA services so that the Public Key Algorithm (PKA) master keys can be reset and changed and the PKDS can be initialized, reenciphered, and refreshed.

Trusted Key Entry components

The Trusted Key Entry feature is a combination of workstation hardware and software network-connected to zSeries, System z9, System z10, and zEnterprise hardware and software.

TKE hardware

- TKE Workstation.
- IBM 4768 Cryptographic adapter.

© Copyright IBM Corp. 2000, 2021

The cryptographic adapter, which is the TKE workstation engine and has key storage for DES, AES, and PKA keys, supports a broad range of DES, AES, and public-key cryptographic processes.

Available with a TKE 9.2 workstation is:

- Feature 0900: 10 IBM part number 00RY790 smart cards.
- Feature 0891: 2 smart card readers and 20 IBM part number 00RY790 smart cards.

Notes:

1. You can carry your smart card readers from feature code 0885 or 0891 forward. Existing smart cards can be used on TKE 9.2 with these readers.
2. With Gemalto smart card readers, you must press the green Enter button after you enter the PIN or a character during the secure key entry process.
3. IDENTIV smart card readers do not have a display window. When you press on the pad, a tone comes from the reader that indicates that the pad was pressed. When the PIN is fully entered, a different pitched tone plays, signaling that the PIN is complete.
4. To manage EP11 host crypto modules, EP11 smart cards are required. Only IBM part numbers 74Y0551 and 00JA710 can be used to create EP11 smart cards.
5. Kobil smart card readers are not supported and not usable with TKE 7.0 or later.
6. DataKey smart cards are no longer usable with TKE 7.0 or later.
7. Older smart cards must be reinitialized on TKE 7.0 or later to be able to store ECC (APKA) master keys.

Two USB flash memory drives are shipped with TKE:

- Use one USB drive for saving and backing up TKE-related files in the TKE data directories.
- Use the other USB drive for backing up critical console data only.

TKE software

The following software is preinstalled on the TKE workstation:

- IBM Cryptographic Coprocessor Support Program Release 6.0.
- Trusted Key Entry Version 9.2 - FC 0879.

Notes:

1. TKE software should not be changed without instructions from IBM Service.
2. TKE 6.0 software, FC 0858, can be installed only on TKE workstations FC 0859, FC 0839, or FC 0840.
3. TKE 7.0 software, FC 0860, can be installed only on a TKE 7.0 workstation, FC 0841.
4. TKE 7.1 software, FC 0867, can be installed only on a TKE 7.0 workstation, FC 0841.
5. TKE 7.2 software, FC 0850, can be installed only on a TKE 7.0 workstation, FC 0841.
6. TKE 7.3 software, FC 0872, can be installed only on a TKE 7.0 workstation, FC 0841 or FC 0842.
7. TKE 8.0 software, FC 0877, can be installed only on a TKE 8.0 workstation, FC 0847.
8. TKE 8.1 software, FC 0878, can be installed only on a TKE 8.0 workstation, FC 0847 or FC 0097.
9. TKE 9.0 software, FC 0879, can be installed on a TKE workstation, FC 0842, FC 0847, FC 0097, FC 0098, FC 0849, FC 0080, FC 0081, FC 0085, or FC 0086.

   Note:

   - When TKE 9.0 is installed on FC 0842 or FC 0847, the workstation feature code becomes 0849.
   - When TKE 9.0 is installed on FC 0097, the workstation becomes feature code becomes 0080.
   - When TKE 9.0 is installed on FC 0098, the workstation becomes feature code becomes 0081.
10. You can only upgrade your TKE workstation to TKE 9.1 software, FC 0880, if your workstation is assigned to a z13 or later.

11. You can only upgrade your TKE workstation to TKE 9.2 software, FC0881, if your workstation is assigned to a z14 or later.

Supported host cryptographic adapters

The host cryptographic adapters supported by TKE 9.2 are:

- Crypto Express2 adapter (CEX2C).
- Crypto Express3 adapter (CEX3C).
- Crypto Express4 CCA adapter (CEX4C).
- Crypto Express4 PKCS #11 adapter (CEX4P).
- Crypto Express5S CCA adapter (CEX5C).
- Crypto Express5S PKCS #11 adapter (CEX5P).
- Crypto Express6S CCA adapter (CEX6C).
- Crypto Express6S PKCS #11 adapter (CEX6P).
- Crypto Express7S CCA adapter (CEX7C).
- Crypto Express7S PKCS #11 adapter (CEX7P).

These host cryptographic adapters:

- Provide a secure processing environment with hardware to provide DES, AES, TDES, RSA, SHA-1, and SHA-256 cryptographic services with secure key management and finance-industry special function support.
- Perform random number generation and modular math functions for RSA and similar public-key cryptographic algorithms.
- Include sensors to protect against attacks that involve probe penetration, power sequencing, radiation, and temperature manipulation.

CEX2C, CEX3C, CEX4C, CEX5C, CEX6C, and CEX7C adapters implement the IBM Common Cryptographic Architecture and are referred to as CCA coprocessors.

CEX4P, CEX5P, CEX6P, and CEX7P adapters implement the IBM Enterprise PKCS #11 architecture and are referred to as EP11 coprocessors.

Host crypto module

The supported host cryptographic card is the host system hardware device performing the cryptographic functions, referred to as the *host crypto module* or, simply, the *crypto module*.

When a host crypto module is manufactured, a unique 8-byte Crypto-Module ID (CMID) is generated and permanently stored on the crypto module. The CMID is returned in all reply messages sent from the host crypto module to the TKE workstation.

TKE concepts and mechanisms

The TKE program uses the following terms on its window displays:

Host
Refers to the name of the currently-defined logical partition or single image.

Host crypto module
Performs the cryptographic functions and is identified by the crypto module index.

Domain
Holds master keys and may hold operational keys. Host crypto modules may contain up to 85 domains (0-84).

Authority
For CCA host crypto modules, a person or TKE workstation that is able to issue signed commands to the host crypto module. All administration of host CCA crypto modules is done by authorities. Authorities do not apply to EP11 host crypto modules.

Role
Privileges assigned to one or more authorities. Roles apply only to CCA host crypto modules and not to EP11 crypto modules.

Administrator
For EP11 host crypto modules, the owner of a smart card who is able to issue signed commands to the host crypto module.

Integrity

TKE security consists of separate mechanisms to provide integrity and secrecy. At initialization time, security is built up in stages: first, integrity of the host crypto module, then integrity of the authorities and administrators. Finally, these integrity mechanisms are used as part of the process to establish secrecy.

The authenticity of the commands issued by an authority or administrator at the TKE workstation to a host crypto module is established by means of digitally signing the command. The command is signed by the TKE workstation using the private key of the authority or administrator. It is verified by the host crypto module using the public key of the authority or administrator previously loaded into the host crypto module.

In the same way, the authenticity of the reply from the host crypto module to the TKE workstation is established. The reply is signed by the host crypto module using its private OA signature key and verified by the TKE workstation using the public OA signature key of the host crypto module.

In order to eliminate the possibility of an attacker successfully replaying a previously signed command, sequence numbers are included in all signed commands. A command with an invalid sequence number is rejected.

PCI-HSM overview

PCI standards are developed by the PCI (Payment Card Industry) Security Standards Council to ensure security in the payment card industry. The PCI Security Standards Council defines their standards as “a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment”.

Compliance with the PCI-HSM (PCI Hardware Security Module) standard has a great deal of value for customers, particularly those who are in the banking and finance industry. There are two fundamental reasons that this certification is important to customers.

1. Compliance is increasingly becoming mandatory.
2. The requirements in PCI-HSM make your system more secure.

This topic includes:

- “Industry requirements for PCI-HSM compliance” on page 4.
- “Improved security through use of PCI-HSM” on page 5.
- “PCI-HSM features for IBM Crypto Express” on page 5.

Industry requirements for PCI-HSM compliance

The PCI organization itself has no power to require compliance with its standards. Compliance with PCI standards is enforced by the payment card brands: Visa, MasterCard, American Express, JCB International, and Discover. If you are a bank, acquirer, processor, or other participant in the payment card systems, the card brands have the ability to impose requirements on you if you want to process their cards. One set of requirements they have been increasingly enforcing are the PCI standards.

The card brands work with the PCI Security Standards Council to develop the PCI standards. The standards that they developed first were the ones they considered most important, particularly the PCI Data Security Standard (PCI-DSS). Other standards were added over time, and PCI-HSM is one of the latest to be developed. In addition, many of the standards have been changed over time to make security requirements stronger and to make requirements mandatory that were optional before.

In general, the trend is for the card brands to enforce more of the PCI standards and to enforce them more rigorously. The trend in the standards themselves is to impose more and stricter requirements in each successive version. The net result is that companies subject to these requirements can expect that they will eventually have to comply with all of them.

Improved security through use of PCI-HSM

PCI-HSM was developed to improve security in payment card systems. It imposes requirements in key management, HSM API functions, device physical security, controls during manufacturing and delivery, device administration, and a number of other areas. It prohibits many things that were in common use for many years, but are no longer considered secure.

The result of these requirements is that applications and procedures often must be updated because they used some of the things that are now prohibited. While this is inconvenient and imposes some costs, it does truly increase the resistance of the systems to attacks of various kinds. Updating a system to use PCI-HSM compliant HSMs reduces the risk of loss for both the institution and its customers.

PCI-HSM features for IBM Crypto Express

In response to the PCI-HSM standards and adoption trends in the industry, CCA version 6.0.3 was designed to meet the Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM), Version 3.0, June 2016 standard. In addition, IBM is in evaluation to certify compliance with this standard. The features and enhancements in CCA 6.0.3 provide you:

- The ability to simultaneously support PCI-HSM compliant applications and non-compliant applications.
- Features to help you determine what parts of your current system need to be changed to be compliant.
- Required dual control for sensitive operations.
- Separate logical key spaces to support both compliant and non-compliant workloads.
- Secure auditing of sensitive operations.
- Key usage restrictions for keys that are used in PCI-HSM compliant applications.
- Cryptographically protected information about firmware versions in the HSM, which can be viewed from a remote administration workstation.

These features and this environment have been provided to support your needs when working with applications subject to PCI standards. For more information on PCI Security Standards Council and PCI standards, see PCI Security Standards (www.pcisecuritystandards.org).

Authorities

An authority is an entity that is able to issue signed commands to the host crypto module. Authorities are used to manage CCA host crypto modules.

All administration of host CCA crypto modules is done with authorities. An authority is identified to the host crypto module or domain by the *authority index*. For module-wide authorities, indexes 00-99 are used. Beginning with CEX6C, each domain can also have authorities, with indexes 100-999 to be used for domain-specific authorities.

If your system has multiple crypto modules, it is convenient to assign authorities the same index on each of your host crypto modules. This will give each authority the ability to update all host crypto modules on the system after loading its signature key. If an authority has a different index on each host crypto module, it has to change its index as it works with different crypto modules.

In addition to the ease of use from crypto module to crypto module, if you intend to create domain groups, then everything relating to the host crypto modules (authority index, authority signature keys, signing requirements, roles, and so on) within the group needs to be the same.

Authority signature key

An authority signs commands by using the private key of its signature key pair, and the host crypto module verifies the signature by using the public key of the same key pair.

Beginning with the CEX5C, authority signature keys can be either RSA keys or ECC keys. For prior CCA crypto modules, only RSA authority signature keys are supported. The public exponent of RSA authority signature keys is always 65537 and the public key is identified by just the modulus.

Before signing and verifying command signatures, the signature key pair must be generated and the public key sent to the host crypto module.

1024-bit, 2048-bit, and 4096-bit RSA authority signature keys can be saved to key storage or binary files. 1024-bit and 2048-bit RSA authority signature keys and BP-320 ECC authority signature keys can be saved to smart cards.

Note: For authority indexes in the range 100 to 999, the associated signature key must reside on a smart card and must be either a 2048-bit RSA key or a 320-bit ECC key.

Authority default signature key

During the crypto module initialization, the public key of a default signature key pair is loaded into the host crypto module. The private key of the default signature key pair is known to the TKE workstation and used until valid authority signature keys are generated and made known to the host crypto module. You are able to reload the public key of a default signature key pair to the host crypto module.

For all crypto module types, a default authority with index 0 is created on the crypto module when it is manufactured or reinitialized. Starting with the CEX6C, a default authority with index 99 is created at the same time as the default authority with index 0. The default authority for index 0 uses a 1024-bit RSA key. The default authority for index 99 uses a 512-bit Brainpool ECC key. In future crypto modules, the default authority with index 0 will no longer be created and users will need to use the default authority with index 99 for initial setup. The default authorities with index 0 and 99 are module-wide authorities.

Also, starting with the CEX6C, a default authority with index 100 is created when a domain enters imprint mode. This default authority is a domain-specific authority and is used to create extra domain-specific authorities and their associated roles for administering a domain in PCI-compliant mode. The default authority with index 100 also uses a 512-bit Brainpool ECC signature key.

Roles

Each authority has an associated role, which specifies what signed commands the authority can issue or co-sign and what domains the authority can change.

When segments 2 and 3 of a CCA host crypto module are loaded for the first time, or when ownership of segments 2 and 3 is surrendered and the segments are reloaded, an initial authority with index 00 is created. This authority is assigned the INITADM role, which is created at the same time. The INITADM role allows the authority to create, change, and delete authorities and roles.

Roles are not supported on EP11 host crypto modules.

Administrators

An administrator is another entity that is able to issue signed commands to a host crypto module. Administrators manage EP11 host crypto modules.

Because EP11 host crypto modules use a different architecture than CCA host crypto modules, the administration is different. Administrative commands to a EP11 host crypto module can be signed by up to eight administrators. The exact number of signatures required depends on the specific command, the target of the command, and the crypto module or domain attributes set by the user.

Administrators are represented in a EP11 host crypto module as an X.509 certificate containing an administrator name (up to 30 characters) and the public part of an ECC signature key. The signature key pair is stored on a smart card, which must be inserted in a smart card reader for commands to be signed.

The concepts of authority index and signature key index are not used when managing EP11 host crypto modules. Panels for managing administrators display the administrator name and a 32-byte Subject Key Identifier, which is a hash of the public part of the signature key. EP11 host crypto modules identify administrators using the Subject Key Identifier. The ability to specify an administrator name is provided as a usability feature. Users are strongly encouraged to assign meaningful, unique names for each administrator signature key created, but this is not required. Both the administrator name and the Subject Key Identifier are written to audit records when commands are signed.

Administrator signature keys are 320-bit Brainpool ECC keys. Administrator signature keys cannot be saved to key storage or to binary files.

Crypto module OA signature key

Host crypto modules sign replies to the TKE workstation using a special OA signature key.

The type of OA signature key depends on the type of host crypto module:

- For the CEX2C, the OA signature key is a 1024-bit RSA key.
- For the CEX3C, CEX4C, and CEX4P, the OA signature key is a 4096-bit RSA key.
- For the CEX5C, CEX5P, CEX6C, CEX6P, CEX7C, and CEX7P, the OA signature key is a P521 ECC key.

When a host crypto module is manufactured, a random RSA or ECC key pair, known as the device key, is generated. The public part of the key is exported and is incorporated into a device key certificate. The certificate is signed by an IBM Class Root key. This certificate validates that the host crypto module was manufactured by IBM.

As code is loaded into segments 1, 2, and 3 of the host crypto module, additional keys and certificates are generated, forming a certificate chain based on the IBM Class Root key and the crypto module device key certificate.

The crypto module OA signature key is the final key in this chain. The process of validating the signature on a reply, and retrieving and validating the certificates in the chain, is known as Outbound Authentication (OA).

When TKE connects to a host, it queries the attached crypto modules. If a new Crypto-Module ID is discovered, TKE fetches the OA certificate chain for the crypto module and verifies it ends with a certificate signed by the IBM Class Root key. When defining or changing a host, there is a check box option that if checked, TKE automatically accepts any crypto modules that are currently attached to the host when opening it. If the box is left unchecked, the TKE displays the Crypto-Module ID and asks the user to accept or reject the crypto module. If a crypto module is accepted, TKE saves the public part of the crypto module OA signature key and uses it to validate all future signed replies from the crypto module.

Command signatures

The number of signatures required on commands to a host crypto module depends on the host crypto module type.

Command signatures for CCA host crypto modules

All commands to CCA host crypto modules are signed. Depending on the command and the setup, the command is either executed immediately or is pending (waiting to be co-signed by other authorities before being executed). Commands requiring more than one signature are called dual-signature commands.

The following single-signature commands deal with master key management and disabling the host crypto module:

- Clear old master key (DES, AES, RSA, or ECC (APKA))

- Clear new master key (DES, AES, RSA, or ECC (APKA))
- Load/combine new master key parts (DES, AES, RSA, or ECC (APKA))
- Set master key (RSA master key only)
- Set master key, immediate (DES, AES, RSA, or ECC (APKA))
- Disable crypto module

The dual-signature commands always require two signatures. These commands deal with:

- Access Control
- Zeroize Domain
- Enable Crypto Module
- Domain Controls
- Domain Mode Transitions

The single-signature commands for operational keys are:

- Load first key part (DES or AES)
- Load additional key part (DES or AES)
- Complete key (DES or AES)
- Clear operational key register (DES or AES)

Command signatures for EP11 host crypto modules

Commands to EP11 host crypto modules require up to eight signatures. The number of required signatures depends on the specific command, the target of the command, and the crypto module or domain attributes set by the user.

If the EP11 host crypto module or the target domain is in imprint mode, no command signatures are required, but only a limited subset of administrative commands can be executed. (See "Imprint mode" on page 210 for more information.) Otherwise, the number of required signatures depends on the command type and on the signature threshold and revocation signature threshold attributes set by the user for the host crypto module or target domain.

The following commands to EP11 host crypto modules require a single signature, regardless of how the signature threshold is set:

- Generate IMPORTER key
- Load new master key
- Clear new master key
- Clear current master key

The following commands require up to eight signatures, depending on how the signature threshold or revocation signature threshold attributes are set:

- Add administrator
- Remove administrator
- Commit master key
- Set attributes
- Enable Crypto Module
- Disable Crypto Module

The following commands can be configured to either require a single signature or require the number of signatures specified by the signature threshold:

- Set control points
- Zeroize domain

- Zeroize crypto module

Key-exchange protocol

TKE provides a Diffie-Hellman key-exchange protocol that permits an authority to set up a transport key between the workstation and the host crypto module. One or more key parts can then be encrypted under the transport key.

Domain controls and domain control points

Domain controls (CCA host crypto modules) and domain control points (EP11 host crypto modules) enable or restrict the cryptographic capabilities of a particular domain. Your installation should consider the ramifications of various implementations.

Domain modes

Beginning with the CEX6C crypto module, the domains of a crypto module can exist in various modes or distinct operational states. These modes support setting up a domain for PCI-compliant operation, running PCI-compliant applications, and converting non-compliant key tokens into PCI-compliant key tokens.

There are three main domain modes:

Normal mode
The legacy state of a domain. Domains on crypto modules before the CEX6C exist in what is called normal mode on the CEX6C and later crypto modules. After a domain is zeroized, it reverts to normal mode. Module-wide roles and authorities are used to administer domains in normal mode.

Imprint mode
Used to create the domain-specific roles and authorities that are needed to administer a domain for PCI-compliant operation. When a domain enters imprint mode, a default domain-specific role and authority with index 100 are created. The default authority uses a default signature key whose private part is known to the TKE workstation. The default role and authority can be used to create other domain-specific roles and authorities for administering the domain in PCI-compliant mode. Most other administrative actions are prohibited in imprint mode.

PCI-compliant mode
After a set of domain-specific roles and authorities is created in imprint mode, the domain can move to PCI-compliant mode. The transition to PCI-compliant mode deletes the default authority if it still uses the default signature key. PCI-compliant mode operations that use PCI-compliant key tokens are allowed. In both imprint mode and PCI-compliant mode, only domain-specific roles and authorities for the domain can be used to run administrative commands to the domain.

PCI-compliant mode was designed to meet the security requirements of the *Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM)* standard, Version 3.0, dated June 2016. IBM is in evaluation to certify compliance with this standard. On future IBM host crypto modules, additional compliance modes may be supported.

Applications that use non-compliant key tokens can run in all domain modes, but applications that use PCI-compliant key tokens can run only in PCI-compliant mode.

To convert non-compliant key tokens to PCI-compliant key tokens, a fourth domain mode is supported which is a sub-mode of PCI-compliant mode. This mode is described as **PCI-compliant mode, key migration allowed** on the Domain General page. In this mode, applications that are running on the host are permitted to re-encipher the secret key in key tokens by using the effective master key for PCI-compliant mode and mark the key token as PCI-compliant. Only key tokens that contain DES operational keys can be marked as PCI-compliant. A TKE workstation is required to enable this sub-mode and while this mode is active, PCI-compliant key tokens cannot be used by applications.

Note: This sub-mode can be explicitly disabled, or it automatically ends if no non-compliant key tokens are converted to PCI-compliant key tokens in the last 30 minutes. If automatically disabled, in order to

see the mode change on the TKE workstation, the crypto module notebook must be refreshed by using the Refresh Notebook option on the function menu.

TKE operational considerations

The TKE workstation can manage CEX2C, CEX3C, CEX4C, CEX4P, CEX5C, CEX5P, CEX6C, CEX6P, CEX7C, and CEX7P crypto modules attached to a Z host.

Logically partitioned (LPAR) mode considerations

When you activate a logical partition, you can prepare it for running software products that work with supported host crypto modules. These supported crypto modules can be shared among several Processor Resource/Systems Manager (PR/SM) logical partitions, provided unique domains are assigned to each LPAR.

When you run in LPAR mode, each logical partition can have its own master keys, CKDS, PKDS, and TKDS.

When you activate a logical partition, you prepare it for being a TKE host or a TKE target. For details, refer to Appendix B, “LPAR considerations,” on page 321.

Multiple hosts

One TKE workstation can be connected to several hosts. Each host connection will have a unique transport key, which is used to protect any key material sent over the connection.

Multiple TKE workstations

Several users on different TKE workstations can have sessions with one host simultaneously. Whenever a user attempts to work with a host crypto module, the system checks to determine whether another user is working with that module. The first user has a reserve on the host crypto module. All other users open the host crypto module in read-only mode until either:

- The first user releases the host crypto module by closing the notebook.
- A user in read-only mode forces the release of the crypto module using the **Release Crypto Module** function from within the notebook.

Defining your security policy

Each installation should have its own unique policies. These policies should be documented in a security plan. Security officers should periodically review their corporate security policy and their current key management system.

The security plan might include these areas:

- General
  - How many security officers does your organization have?
  - How often is the master key changed?
  - Who is authorized to enter master key parts?
  - Do the key parts you enter from the keyboard need to be masked?
  - Who has access to the secure computer facility?
  - What are the policies for working with service representatives?
  - Will you be using smart card support?
- Workstation Considerations
  - Who will use the TKE workstation?
  - Where will your workstation be located?
  - Is it only accessible to the security administrators or security officers?

  - How many workstations will there be?
  - Will you use group logon?
  - Who will backup the workstations?
  - Where will the passwords of the security officers be saved?
- Command Considerations
  - Which commands require multiple signatures?
  - Which crypto modules should be grouped together?
  - How many signatures will be required?
  - Will this affect the availability of the system?
  - Which commands require a single signature?
  - Who will make these decisions?

TKE enablement

A support element is a dedicated workstation used for monitoring and operating Z hardware. TKE commands must be permitted on the Support Element before any commands issued by the TKE workstation can be executed.

For CCA crypto modules the default setting for TKE Commands is **Denied**. The setting must be changed to **Permitted** before the TKE workstation can be used to manage the crypto module.

For EP11 crypto modules, only a TKE workstation can perform certain management functions, so the setting is always shown as **Permitted** on the Support Element.

If TKE commands are not permitted on the Support Element, the following Details Error is displayed on the TKE Workstation when an attempt is made to open the Host ID:

```
Error Message: Program CSFPCIX Interface
Error Type 2
Return Code 12
Reason Code 2073

Detail Message "The Crypto Coprocessor has been disabled on the Support Element.
It must be enabled on the Support Element before TKE can access it."
```

An authorized user can permit TKE commands on the Support Element, using the Support Element Console Application. For more information, see the help files that are provided with the Support Element.

Note: A global zeroize issued from the Support Element returns the state of TKE Commands to the default value of **Denied** for CCA host crypto modules.

Trusted Key Entry console

The Trusted Key Entry Console automatically loads on start up with a set of commonly used tasks. The console is shipped with several predefined console user names. Your first logon is with the console user name.

Most tasks require an additional logon to the TKE workstation crypto adapter. You log on with your TKE workstation crypto adapter profile. The profile is defined for your workstation when TKE is configured and customized.

At start up, you are logged in with the default user name TKEUSER. The user names determine the applications and utilities that can be run during the console session. The predefined console user names are:

- TKEUSER -- default console user name.
- ADMIN -- provides access to administrative functions, such as migration utilities, the code load utility, and the crypto adapter initialization utility.

- AUDITOR -- provides access to audit functions, such as the Audit Configuration Utility, the Audit Record Upload Configuration Utility, and utilities to view and archive security logs.
- SERVICE -- provides access to service functions, such as managing the console code level, setting the date and time, and saving upgrade data.

The ADMIN, AUDITOR, and SERVICE console user names require a password when logging on the console. The default TKEUSER console user name may optionally require a password. See "Password protect console" on page 364 for more information.

Appendix E, "Trusted Key Entry applications and utilities," on page 331 describes the applications and utilities available to each console user name.

After starting the TKE console, the initial Trusted Key Entry Console panel appears.

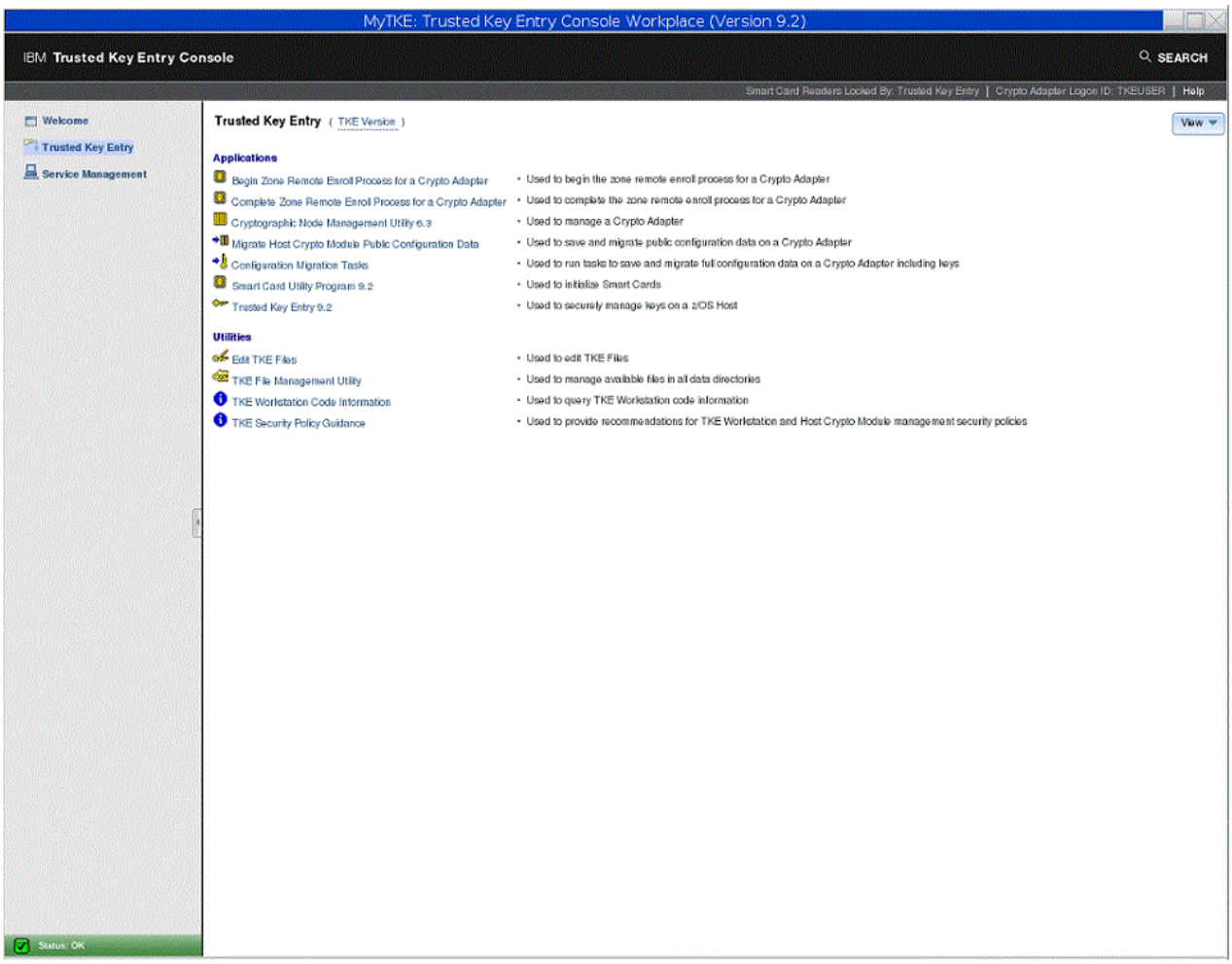


Figure 1. TKE Console - initial panel

This initial panel provides access to applications and utilities that are available when you are using the default TKEUSER console user name.

- Clicking **Trusted Key Entry** provides access to the main TKE window, the Smart Card Utility Program, the Cryptographic Node Management Utility, and other commonly used applications and utilities.
- Clicking **Service Management** provides access to service functions, such as locking, shutting down, or restarting the console.
- Clicking **Status Bar** displays the current status of the TKE Hardware.

When it is necessary to log on to the TKE console using a different user name, for example, ADMIN, AUDITOR or SERVICE, close this panel by clicking the **X** in the upper right corner. The Trusted Key Entry Console pre-login panel appears.

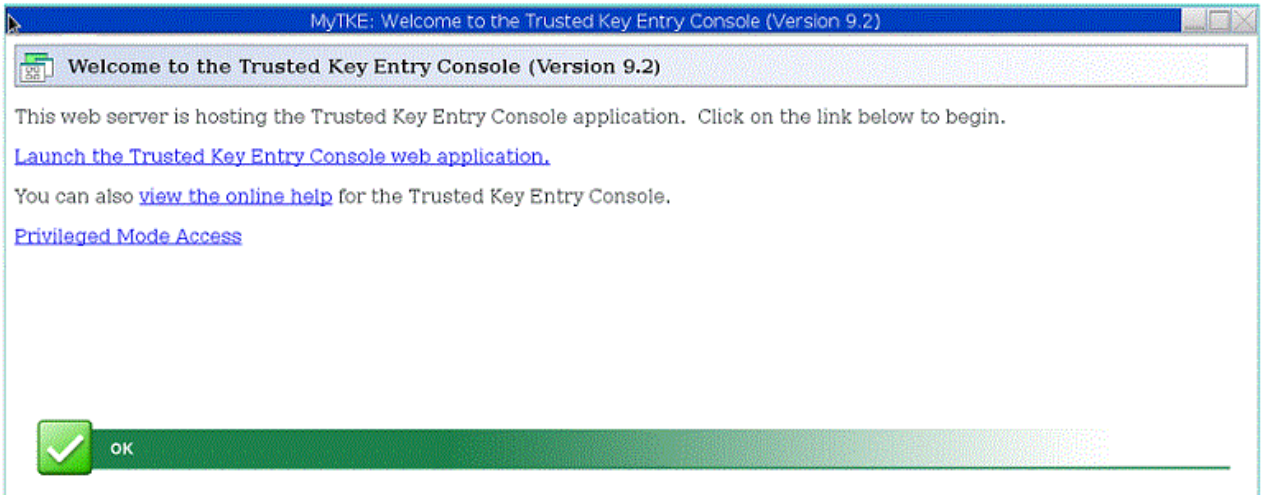


Figure 2. TKE Console - pre-login panel

Clicking **Launch the Trusted Key Entry Console web application**, starts a console session using the default TKEUSER console user name. It returns you to the initial panel.

Clicking **view the online help** opens an IBM help window. You can navigate to the help information for the TKE panels.

Clicking **Privileged Mode Access** displays a logon panel. You can log on as any of the following privileged mode access user IDs: AUDITOR, ADMIN, SERVICE.

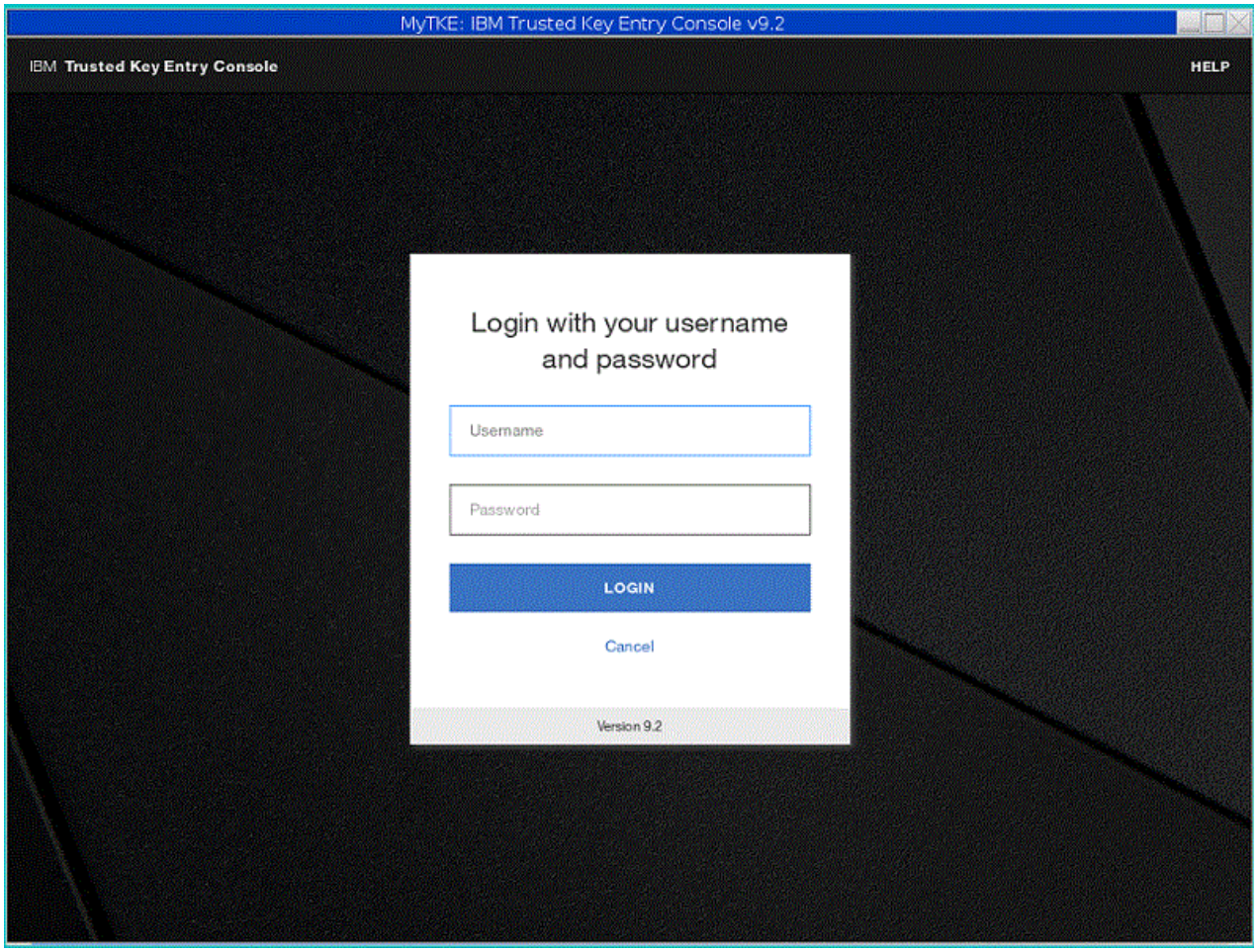


Figure 3. Log on with other privileged mode access console user names

Fill in the user name field with one of the following:

- ADMIN - the default password is PASSWORD
- AUDITOR - the default password is PASSWORD
- SERVICE - the default password is SERVMODE

After logging on with the new user name, an initial panel appears. In the upper-right corner, to the left of the word Help, the privileged mode access id is displayed. This initial panel provides access to applications and utilities when you are using a console user name. It is identical to the TKEUSER initial panel with the same options:

- Clicking **Trusted Key Entry** provides access to the applications and utilities available with the console user name you used to log on.
- Clicking **Service Management** provides access to service functions available with the console user name you used to log on.
- Clicking **Status Bar** displays the current status of the TKE Hardware.

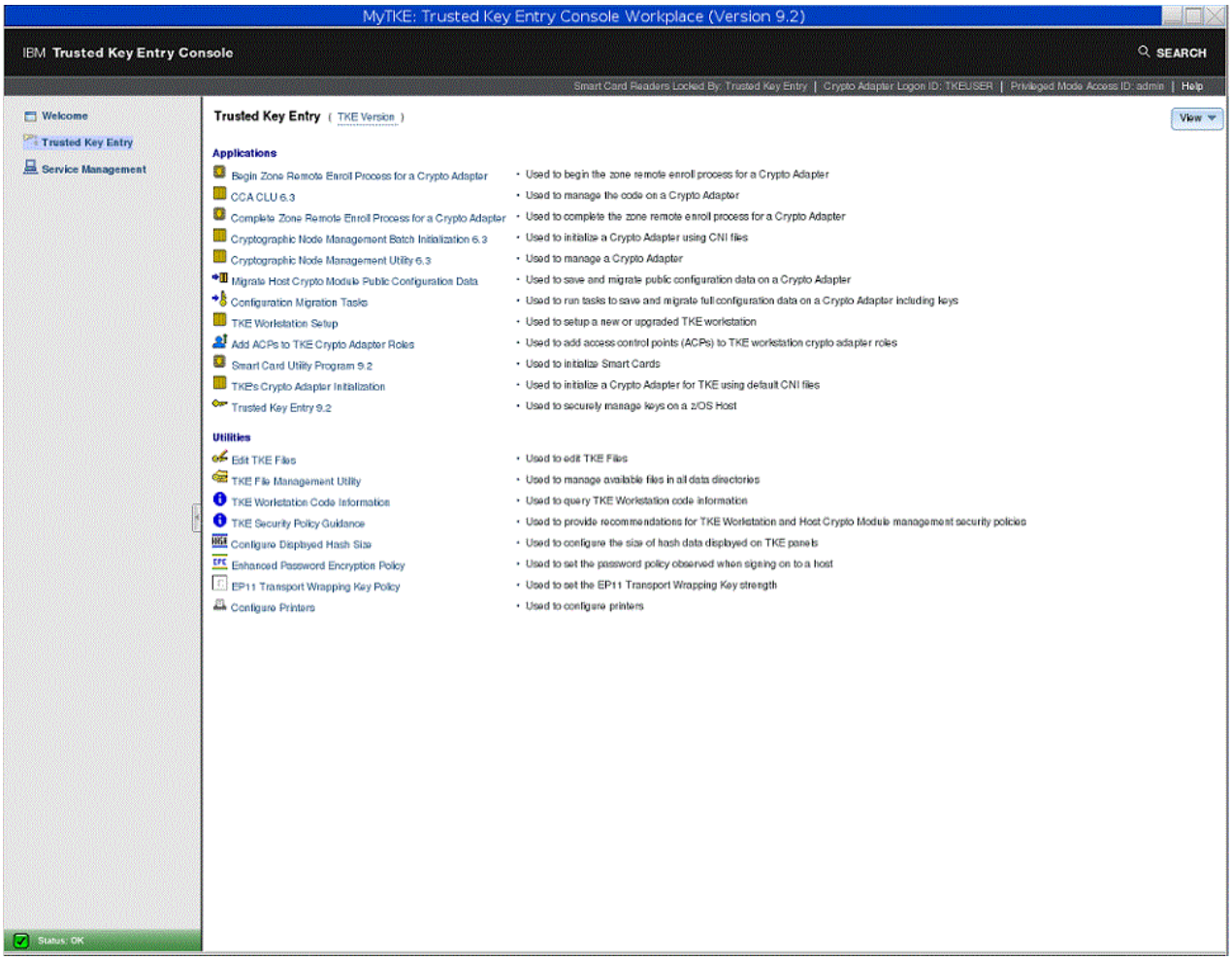


Figure 4. Trusted Key Entry for ADMIN - categorized

The Trusted Key Entry console message bar can contain three types of status messages to the left of the word Help:

- **Privileged Mode Access ID** is displayed if the console user is logged on as a privileged mode access user.
- **Crypto Adapter Logon ID** is displayed when the user of a TKE application is logged on to the Crypto Adapter.

- **Smart Card Readers Locked By** is displayed when a TKE application has a lock on the smart card readers.

Guideline: After you log in the first time, change the password with the Change Password task. See “Change password ” on page 353.

Trusted Key Entry console navigation

When the TKE console initially comes up it consists of a navigation area on the left side and a Welcome page on the right side. The navigation area contains links to the Trusted Key Entry and Service Management categories. The Welcome page displays a brief description of these categories and a link to where the *TKE Workstation User's Guide* can be accessed. When clicking on the Trusted Key Entry and Service Management categories, a list of tasks and utilities will be displayed on the right side of your TKE console.

There are three presentation options:

- Detail (the way things are shown in the screen shots).
- Icon (looks similar to icons on a desktop).
- Tile (looks similar to the Icon view).

Each Category can be displayed in two different views, alphabetical and categorized. The categorized view for Trusted Key Entry contains the sub categories Applications and Utilities. The alphabetical view allows a user to display all tasks, uncategorized, in a flat alphabetized list. A user can select either the Alphabetical or Categorized Link at the top of the window to change the view.

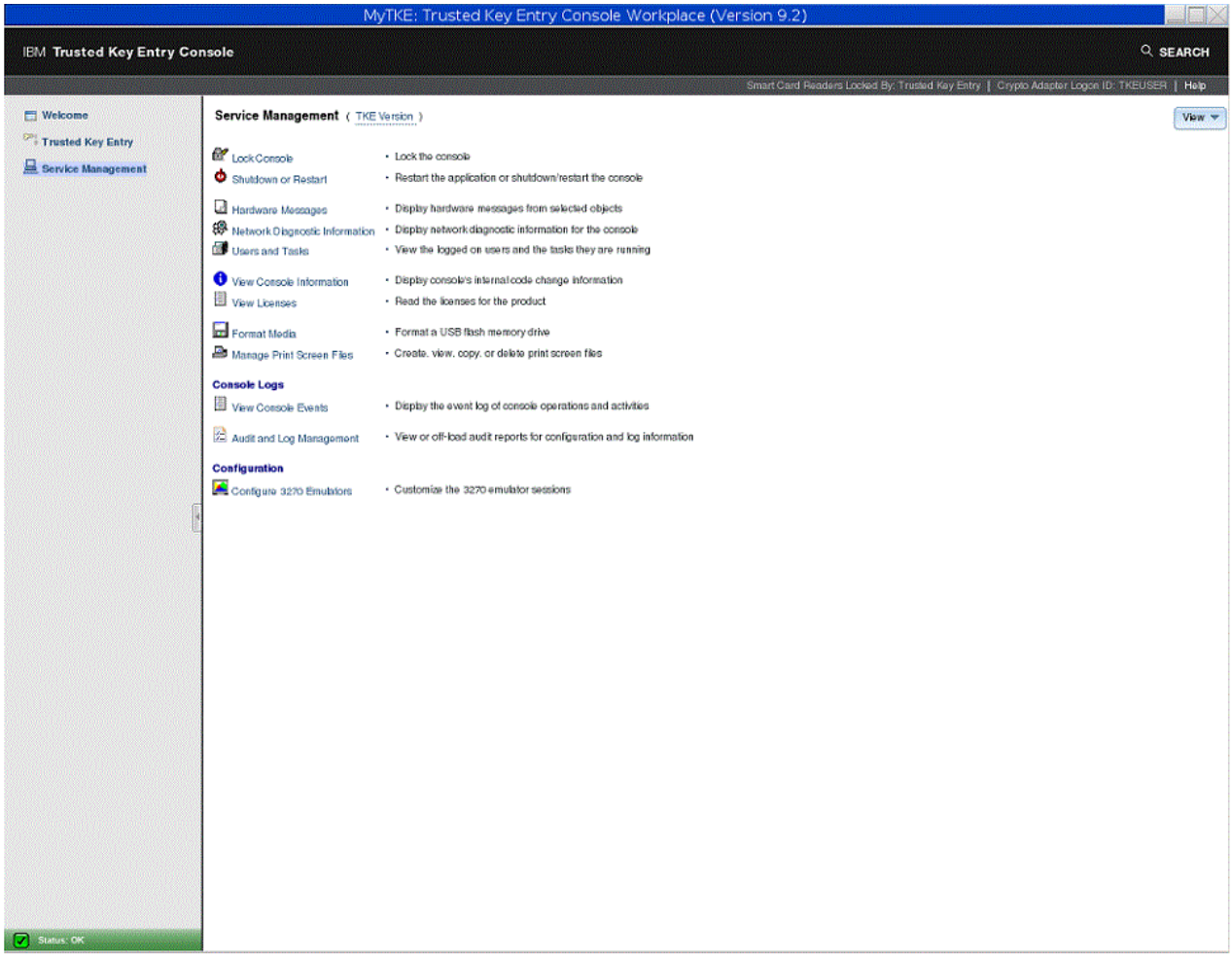


Figure 5. Service Management – No Privileged Mode Access

TKE workstation crypto adapter roles and profiles

This information describes how the roles and profiles on the TKE workstation crypto adapter are used to control access to the TKE applications and the cryptographic services on the adapter.

Roles and profiles are placed on a TKE workstation crypto adapter when you:

- Run the TKE Crypto Adapter Initialization application to initialize the adapter for use with smart card or passphrase profiles. This application loads system-supplied roles and profiles onto the adapter.
- Explicitly load roles and profiles onto the adapter through the Cryptographic Node Management Utility.

Every profile must have a role. Each role contains a list of Access Control Points (ACPs) in its permitted operations list. The list of permitted operations in a role determines what a profile with the role is allowed to do.

When a user signs onto the TKE workstation crypto adapter, the profile and its associated role become the adapter's current profile and current role. All the authority checks are done against the current role.

There is always a current role in effect.

- If you are explicitly signed on to TKE, the profile and its role became the current profile and current role when you signed on.
- If you are not explicitly signed on to TKE, there is no current profile. However, there is a default current role. This is only valuable if you have also signed onto the TKE in Privileged Access Mode.

Authority checking on the TKE

Every time a TKE application is started, an authority check is done. The following describes the basic tests that are done:

- Is there a current profile?
  - NO: Present a logon screen. Only profiles with roles that have enough authority to start the application are presented on the logon screen.
  - YES: Does the current role have the necessary ACPs to start the application?
    - YES: The application is started.
    - NO: The user is given the option to log off and be presented with a new logon screen. Only profiles with roles that have enough authority to start the application are presented on the logon screen.

Every time a cryptographic service on the TKE workstation crypto adapter is attempted, an authority check is done to determine if the current role has the required ACP to perform the cryptographic service. If the role has the ACP, the operations will be done. If not, the operation will not be performed.

Types of profiles

A TKE workstation crypto adapter supports 3 types of profiles:

- **Passphrase Profiles:** A profile that requires the user to provide the correct passphrase during the authentication process.
- **Smart Card Profiles:** A profile that requires the user to have the correct crypto adapter logon key on a smart card during the authentication process. In addition, the user must know the PIN number of the smart card that has the logon key.
- **Group Profiles:** A profile designed to require a specific number of people to sign on to their individual profiles before the logon process for the group profile is complete. The following characteristics apply to group profiles:
  - A group profile has a set of 1 to 10 members.
  - A group member is an individual passphrase or smart card profile that must exist when the group profile is created.
  - All the members of a group profile must be the same type, either passphrase or smart card.

  - A group profile contains an attribute that defines how many people must sign on before the group logon is complete. The number is a value between 1 and the total number of members of the group.
  - A group profile has a role. Normally the group's role is more powerful than the roles given to each individual group member.

A TKE workstation crypto adapter can contain all types of profile at the same time:

- Passphrase profiles
- Smart card profiles
- Group profiles with passphrase profile members
- Group profiles with smart card profile members

For instructions on creating or changing roles and profiles, refer to Chapter 11, "Cryptographic Node Management utility (CNM)," on page 251.

Initializing a TKE workstation crypto adapter

This information describes how to initialize a TKE workstation crypto adapter.

Rule: The user must be logged on to the TKE Workstation console through Privileged Mode Access as ADMIN to initialize a TKE workstation crypto adapter.

Initial adapter conditions

Before you can start to use your TKE workstation, the crypto adapter must meet the following conditions:

- It must have the correct CCA level of code.
- The Function Control Vector must be loaded.

Initial adapter conditions on new TKE workstations

Every TKE workstation comes with a cryptographic adapter. The following steps should have been performed before the adapter was shipped with the TKE workstation:

- The proper level of CCA code was loaded onto the TKE workstation crypto adapter. Specific releases of CCA are associated with specific releases of TKE.

Table 1. CAA code loaded for specific releases of TKE

TKE Release	**CCA Release**
TKE 5.3	CCA 3.4
TKE 6.0	CCA 3.5
TKE 7.0	CCA 4.1
TKE 7.1	CCA 4.2
TKE 7.2	CCA 4.3
TKE 7.3	CCA 4.4
TKE 8.0	CCA 5.0
TKE 8.1	CCA 5.2
TKE 9.0	CCA 6.0
TKE 9.1	CCA 6.1
TKE 9.2	CCA 6.3

- The Function Control Vector (FCV) was loaded onto the TKE workstation crypto adapter.

  Notes:

1. During the process of loading the CCA code and the FCV, the card was initialized for use with passphrase profiles. The system-supplied roles and profiles might still be on the adapter.
2. Beginning in 7.2, every time a TKE application is opened, a check is done to make sure that the TKE workstation has the correct level of CCA code. If not, a message tells you to reload the CCA code onto the adapter.

Initial adapter conditions on upgraded TKE workstations

When you upgrade an existing TKE workstation to a new level of TKE, the upgrade process states:

- You must go into the CCA CLU utility and load the new CCA code onto your TKE workstation crypto adapter. The CLU utility can only be accessed through Privileged Mode Access by a user logged onto the TKE Workstation console as ADMIN.
- You might have to load a new Function Control Vector onto your TKE workstation crypto adapter. The Installation Instructions for your upgrade will tell you if this is required.

Verify current crypto adapter settings

You can check the state of the TKE workstation crypto adapter at any time using the following utilities.

- You can determine the CCA level by running the **Check Coprocessor Status** command from the CCA CLU utility. (To access the CCA CLU utility you must log on to the TKE Workstation console through Privileged Access Mode as ADMIN.)
- You can determine if the FCV is loaded by pressing the “export control” button on the **Crypto Node -> Status** screen in the Cryptographic Node Management (CNM) utility.
- You can determine if there are any roles on the adapter by looking at the **Access Control –Roles** screen in the CNM utility.
- You can determine if there are any roles on the adapter by looking at the **Access Control –Profiles** screen in the CNM utility.

System-supplied roles and profiles on TKE workstation crypto adapters:

The TKE provides an initial set of system-supplied roles and profiles based on whether you intend to use passphrase or smart card profiles. Prior to initializing your TKE workstation crypto adapter, you must decide if you want to sign on to the adapter using passphrase profiles, smart card profiles, or both types of profiles.

Guideline: Use smart card profiles whenever possible. They provide the highest level of security.

Once you have decided what type of profiles you will use, you need to initialize the TKE workstation crypto adapter for use with those kinds of profiles. The initialization is done through the TKE Crypto Adapter Initialization application. To start this application you must be logged on as ADMIN through Privileged Mode Access. When you start this application, you are asked:

```
Would you like to prepare your cryptographic coprocessor for Smart Card
or Pass Phrase use?
```

Guidelines: Make your choice following these guidelines:

- Select “s”, smart card if you will use smart card profiles exclusively.
- Select “p”, pass phrase, if you will use passphrase profiles exclusively.
- Select “p”, pass phrase if you will use a combination of pass phrase and smart card profiles.

Initializing for use with smart card profiles

When you initialize a TKE workstation crypto adapter for use with smart card profiles, the following system-supplied roles and profiles will be created:

- System-supplied roles:

DEFAULT
Intended for use during the migration process or initial setup of the roles and smart card profiles on the TKE.

SCTKEADM
Intended for use with customer-defined smart card profiles. The role is designed to provide the authority to manage the TKE.

SCTKEUSR
Intended for use with customer-defined smart card profiles. The role is designed to provide the authority to manage host cryptographic modules.

TKEGRPMB
Intended for use by members of a group profile. Has the minimum required authority. When logging on as a group, the role for each member is ignored. Once the group logon completes, the role for the group profile controls what operations are allowed.

- System-supplied profiles:

None
No system-supplied smart card profiles are provided by the TKE.

Initializing for use with passphrase profiles

When you initialize a TKE workstation crypto adapter for use with passphrase profiles, the following system-supplied roles and profiles will be created:

- System-supplied roles:

DEFAULT
Intended for use during the migration process or initial setup of the roles and smart card profiles on the TKE.

TKEADM
Intended for use with system-supplied and customer-defined passphrase profiles. The role is designed to provide the authority to manage the TKE.

TKEUSER
Intended for use with system-supplied and customer-defined passphrase profiles. The role is designed to provide the authority to manage host crypto modules.

KEYMAN1
Intended for use with the system-supplied passphrase profile KEYMAN1. The role is designed to provide users authority to clear the TKE crypto adapter new master key register and load first master key parts.

KEYMAN2
Intended for use with the system-supplied passphrase profile KEYMAN2. The role is designed to provide users authority to load any middle and last master key parts to the TKE crypto adapter new master key register, set the master key and reencipher key storage.

TKEGRPMB
Intended for use by members of a group profile. Has the minimum required authority. When logging on as a group, the role for each member is ignored. Once the group logon completes, the role for the group profile controls what operations are allowed.

- System-supplied profiles:

TKEADM
Intended for a person with the responsibility of initially setting up a TKE, completing migration tasks, or managing the TKE.

TKEUSER
Intended for a person with the responsibility of managing host crypto modules.

KEYMAN1
Intended for a person with the responsibility to clear the TKE crypto adapter new master key register and load first master key parts.

KEYMAN2
Intended for a person with the responsibility to load any middle and last master key parts to the TKE crypto adapter new master key register, set the master key and reencipher key storage.

Roles and profiles definition files

Files can be created that contain enough information to create or update roles and profiles on a TKE workstation crypto adapter. These are called role definition files and profile definition files. Definition files can be stored on the TKE workstation's hard drive or on removable media. The files can be used to create or update roles and profiles in the following instances:

- The TKE workstation crypto adapter is initialized.
- Migration is being done.
- Recovery is being done.

Definition files and their corresponding role or profile might or might not be synchronized. The following table shows all of the possible relationships.

Table 2. Definition files and their corresponding role or profile

Role or profile definition file exists	Corresponding role or profile exists on TKE workstation crypto adapter	File attributes equal adapter's attributes
Yes	Yes	Yes
Yes	Yes	No
Yes	No	N/A
No	Yes	N/A

Role definition files

A role definition file contains enough information to create or replace a role on a TKE workstation crypto adapter. The file contains the following information:

- Role name.
- Comment field.
- Required Authentication Strength. Only applies to passphrase profiles with the role.
- Valid times a user with the role can use the TKE.
- Permitted operations list. The list of capabilities a profile with the role is allowed to use.

All system-supplied roles have corresponding system-supplied role definition files. When you create a role, you can also create a corresponding role definition file for the role.

System-supplied role definition files

The TKE comes with system-supplied role definition files for each of the system-supplied roles that can be created on a TKE. When a TKE workstation crypto adapter is initialized, the system-supplied roles are created from the system-supplied definition files.

Guideline: To preserve the ability to restore system-supplied roles to their default settings, do not update system-supplied role definition files.

Passphrase roles

When a TKE workstation crypto adapter is initialized for use with passphrase profiles, six roles are created. The following table shows the names of the system-supplied role definition files that are used to create the roles.

Table 3. System-supplied role definition files for passphrase roles

TKE Release	DEFAULT	KEYMAN1	KEYMAN2	TKEADM	TKEUSER	TKEGRPMB (Cannot see or modify the file)
TKE 5.0 to 6.0	default.rol	keyman1.rol	keyman2.rol	tkeadm50.rol	tkeuser42.rol	N/A
TKE 7.0	default_70.rol	keyman1_70.rol	keyman2_70.rol	tkeadm_70.rol	tkeusr_70.rol	N/A
TKE 7.1	default_71.rol	keyman1_71.rol	keyman2_71.rol	tkeadm_71.rol	tkeusr_71.rol	N/A
TKE 7.2	default_72.rol	keyman1_72.rol	keyman2_72.rol	tkeadm_72.rol	tkeusr_72.rol	N/A
TKE 7.3	default_73.rol	keyman1_73.rol	keyman2_73.rol	tkeadm_73.rol	tkeusr_73.rol	N/A
TKE 8.0	default_80.rol	keyman1_80.rol	keyman2_80.rol	tkeadm_80.rol	tkeusr_80.rol	N/A
TKE 8.1	default_81.rol	keyman1_81.rol	keyman2_81.rol	tkeadm_81.rol	tkeuser_81.rol	tkegrpmb_81.rol
TKE 9.0	default_90.rol	keyman1_90.rol	keyman2_90.rol	tkeadm_90.rol	tkeusr_90.rol	tkegrpmb_90.rol
TKE 9.1	default_91.rol	keyman1_91.rol	keyman2_91.rol	tkeadm_91.rol	tkeusr_91.rol	tkegrpmb_91.rol
TKE 9.2	default_92.rol	keyman1_92.rol	keyman2_92.rol	tkeadm_92.rol	tkeusr_92.rol	tkegrpmb_92.rol

Notes:

- Beginning in TKE 7.0, release-specific system-supplied role definition files were shipped with the TKE workstation.
- If there are any tkegrpmb_*xx*.rol files in the CNM Data Directory, they are not used by TKE and may be deleted.

Smart card roles

When a TKE workstation crypto adapter is initialized for use with smart card profiles, four roles are created. The following table shows the names of the system-supplied role definition files that are used to create the roles.

Table 4. System-supplied role definition files for smart card roles

TKE Release	DEFAULT	SCTKEADM	SCTKEUSR	TKEGRPMB (Cannot see or modify the file)
TKE 5.0 to 6.0	tempdefault.rol	sctkeadm50.rol	sctkeusr.rol	N/A
TKE 7.0	tempdefault_70.rol	sctkeadm_70.rol	sctkeusr_70.rol	N/A
TKE 7.1	tempdefault_71.rol	sctkeadm_71.rol	sctkeusr_71.rol	N/A
TKE 7.2	tempdefault_72.rol	sctkeadm_72.rol	sctkeusr_72.rol	N/A
TKE 7.3	tempdefault_73.rol	sctkeadm_73.rol	sctkeusr_73.rol	N/A
TKE 8.0	tempdefault_80.rol	sctkeadm_80.rol	sctkeusr_80.rol	N/A
TKE 8.1	tempdefault_81.rol	sctkeadm_81.rol	sctkeusr_81.rol	tkegrpmb_81.rol
TKE 9.0	tempdefault_90.rol	sctkeadm_90.rol	sctkeusr_90.rol	tkegrpmb_90.rol
TKE 9.1	tempdefault_91.rol	sctkeadm_91.rol	sctkeusr_91.rol	tkegrpmb_91.rol
TKE 9.2	tempdefault_92.rol	sctkeadm_92.rol	sctkeusr_92.rol	tkegrpmb_92.rol

Notes:

- Beginning in TKE 7.0, release-specific system-supplied role definition files were shipped with the TKE workstation.
- If there are any tkegrpmb_*xx*.rol files in the CNM Data Directory, they are not used by TKE and may be deleted.

Customer-defined role definition files

You can create your own roles on your TKE's local crypto adapter. When you create a role, an associated definition file is not automatically created. You must explicitly create the definition file.

Guidelines: Follow these guidelines for creating customer-defined roles:

- Create role definition files for your customer-defined roles. These files can be used for recovery or migration purposes if necessary.
- Use the file naming convention "*role_name*.rol".
- When you update a role on the TKE's local crypto adapter, make the same change to the associated definition file. Remember, the definition file is not automatically updated when you make a change to a role.

For Instructions on creating or changing role definition files, refer to Chapter 11, "Cryptographic Node Management utility (CNM)," on page 251.

Profile definition files

A profile definition file contains enough information to create or replace a profile on a TKE local crypto adapter. The file contains the following information:

- Profile Name
- Comment field
- Activation and deactivation dates
- Role
- For passphrase profiles, the passphrase and passphrase expiration date for the profile.
- For smart card profiles, the public modulus of the crypto adapter logon key for the profile.

All system-supplied profiles have a corresponding system-supplied profile definition files. When you create your own profiles, they can also create a corresponding profile definition file for the profile.

System-supplied profile definition files

The TKE comes with system-supplied profile definition files for each of the system-supplied profiles that can be created on a TKE. When a TKE workstation crypto adapter is initialized, the system-supplied profiles are created from the system-supplied definition files. Profiles do not change between releases of TKE. The definition file names are the same in each release of the TKE.

To preserve the ability to restore system-supplied profiles to their default settings, including the default passwords, do not update system-supplied profile definition files.

Passphrase profiles: When a TKE workstation crypto adapter is initialized for use with Passphrase profiles, four profiles are created using their system-supplied profiles definition files. The following table shows the profiles and the definition files used to create them:

Table 5. System-supplied profile definition files for passphrase profiles

Profile	Definition File
TKEADM	tkeadm.pro
TKEUSER	tkeuser.pro
KEYMAN1	keyman1.pro
KEYMAN2	keyman2.pro

Smart card profiles: No profiles are created when the TKE workstation crypto adapter is initialized for use with smart card profiles.

Customer-defined profile definition files

You can create your own profiles on your TKE workstation crypto adapter. When you create a profile an associated definition file is not automatically created. You must explicitly create the definition file.

Guidelines: Follow these guidelines for creating customer-defined profiles:

- Create profile definition files for your customer-defined profiles. These files can be used for recovery or migration purposes if necessary.
- Use the file naming convention "*profile_name*.pro".
- When you update a profile on the TKE workstation crypto adapter, make the same change to the associated definition file. Remember, the definition file is not automatically updated when you make a change to a profile.

For instructions on creating or changing profile definition files, refer to Chapter 11, "Cryptographic Node Management utility (CNM)," on page 251.

System-supplied role access control points (ACPs)

The primary purpose of any role is to define the capabilities of a user with the role. Each role has a list of permitted operations, also called access control points (ACPs), which define the capabilities of the user.

ACP considerations for user-defined roles

There are many cryptographic services the TKE uses during normal operation which the user is not aware of. To use these services, the user's role must contain the appropriate list of ACPs in its "permitted operations" list. If you are going to create user-defined roles, it is difficult to know what cryptographic services will be used by your target users. Therefore, selecting the correct list of ACPs is difficult.

Guideline: If you are going to create roles, use one of the following system-supplied roles as the basis for your new role.

- TKE workstation crypto adapter initialized for passphrase profile use:
  - TKEUSER
  - TKEADM
- TKE workstation crypto adapter initialized for smart card profile use:
  - SCTKEUSR
  - SCTKEADM

ACPs assigned to system-supplied roles

The following tables show the ACPs that are assigned to each of the system-supplied roles.

Note:

- Beginning in TKE 7.1, the ACP "TKE USER, X'8002'" is no longer used. This ACP was replaced with more granular access control checking. The new ACPs that are checked are ACPs X'1000' through X'100E'.
- Beginning with TKE 8.0, TKE supports a USB-attached printer. To print files, the X'1010' (print files) ACP must be enabled. This ACP is not enabled by default in any system-supplied role.
- Beginning with TKE 8.1:
  - To copy a key part that is stored in a binary file to a smart card, the X'1011' (Copy binary file key part to smart card) ACP must be enabled.
  - To invoke from the TKE workstation an ICSF function that coordinates the setting of one or more master keys with the updating of key storage on a host system, the X'1012' (Coordinated change master key and KDS) ACP must be enabled.

  These ACPs are not enabled by default in any system-supplied role.

Roles for use with smart card profiles

The following roles are created when a TKE workstation crypto adapter is initialized for use with smart card profiles:

- SCTKEADM
- SCTKEUSR
- TKEGRPMB
- DEFAULT

SCTKEADM

Table 6. ACPs assigned to the SCTKEADM role

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 5.2	Enabled in release TKE 5.3, TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0, TKE 8.1	Enabled in release TKE 9.0, TKE 9.1, TKE 9.2
Required 0047 Change Own Passphrase	X'0047'						x	x
Required 008E Generate Key	X'008E'	x	x	x	x	x	x	x
Required 0100 PKA96 Digital Signature Generate	X'0100'			x	x	x	x	x
Required 0103 PKA96 Key Generate	X'0103'		x	x	x	x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x	x	x	x
Required 011F RSA Decipher Clear Key	X'011F						x	x
Required 012A Encipher Data Using AES	X'012A'						x	x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'			x	x	x	x	x
Required 0203 Delete Retained Key	X'0203'		x	x	x	x	x	x
Required 027D Permit Regeneration Data	X'027D'						x	x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'			x	x	x	x	x
Load First Master Key Part	X'0018'	x	x	x	x	x	x	x
Combine Master Key Parts	X'0019'	x	x	x	x	x	x	x
Set Master Key	X'001A'	x	x	x	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x	x	x
Clear New Master Key Register	X'0032'	x	x	x	x	x	x	x
Reencipher to Current Master Key	X'0090'	x	x	x	x	x	x	x
Reencipher to Current Master Key2	X'00F1'					x	x	x
PKA96 Key Token Change	X'0102'	x	x	x	x	x	x	x
One-Way Hash, SHA-1	X'0107'	x	x	x	x	x	x	x
Reset Intrusion Latch	X'010F'	x	x	x	x	x	x	x
Set Clock	X'0110'	x	x	x	x	x	x	x
Reinitialize Device	X'0111'	x	x	x	x	x	x	x
Initialize Access-Control System	X'0112'	x	x	x	x	x	x	x
Change User Profile Expiration Date	X'0113'	x	x	x	x	x	x	x
Change User Profile Authentication Data	X'0114'	x	x	x	x	x	x	x
Reset User Profile Logon-Attempt-Failure Count	X'0115'	x	x	x	x	x	x	x
Delete User Profile	X'0117'	x	x	x	x	x	x	x
Delete Role	X'0118'	x	x	x	x	x	x	x

Table 6. ACPs assigned to the SCTKEADM role (continued)

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 5.2	Enabled in release TKE 5.3, TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0, TKE 8.1	Enabled in release TKE 9.0, TKE 9.1, TKE 9.2
Load Function-Control Vector	X'0119'	x	x	x	x	x	x	x
Clear Function-Control Vector	X'011A'	x	x	x	x	x	x	x
Clear AES New Master Key Register	X'0124'					x	x	x
Load First AES Master Key Part	X'0125'					x	x	x
Load Middle/Last AES Master Key Parts	X'0126'					x	x	x
Set AES Master Key	X'0128'					x	x	x
Unrestrict Combine Key Parts	X'027A'	x	x	x	x	x	x	x
RNX access control point	X'02A2'	x	x	x	x	x	x	x
Session Key Primary	X'02A3'	x	x	x	x	x	x	x
Session Key Secondary	X'02A4'	x	x	x	x	x	x	x
Import Card Device Certificate	X'02A5'		x	x	x	x	x	x
Import CA Public Certificate	X'02A6'		x	x	x	x	x	x
Master Key Extended	X'02A7'	x	x	x	x	x	x	x
Delete Device Retained Key	X'02A8'		x	x	x	x	x	x
Export Card Device Certificate	X'02A9'		x	x	x	x	x	x
Export CA Public Certificate	X'02AA'		x	x	x	x	x	x
Reset Battery Low Indicator	X'030B'	x	x	x	x	x	x	x
Clear APKA New Master Key Register	X'031F'							x
Load First APKA Master Key Part	X'0320'							x
Load Middle/Last APKA Master Key Parts	X'0321'							x
Set APKA Master Key	X'0322'							x
Open Begin Zone Remote Enroll Process	X'1000'				x	x	x	x
Open Complete Zone Remote Enroll Process	X'1001'				x	x	x	x
Open Cryptographic Node Management Utility	X'1002'				x	x	x	x
Open Smart Card Utility Program	X'1005'				x	x	x	x
Open Edit TKE Files	X'100D'				x	x	x	x
Open TKE File Management Utility	X'100E'				x	x	x	x
TKE USER	X'8002'		x	x				

SCTKEUSR

Table 7. ACPs assigned to the SCTKEUSR role

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2	Enabled in release TKE 7.3	Enabled in release TKE 8.0, TKE 8.1, TKE 9.0, TKE 9.1, TKE 9.2
Required 0047 Change Own Passphrase**	X'0047'						x
Required 008E Generate Key**	X'008E'	x	x	x	x	x	x
Required 0100 PKA96 Digital Signature Generate**	X'0100'	x	x	x	x	x	x
Required 0103 PKA96 Key Generate**	X'0103'	x	x	x	x	x	x

Table 7. ACPs assigned to the SCTKEUSR role (continued)

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2	Enabled in release TKE 7.3	Enabled in release TKE 8.0, TKE 8.1, TKE 9.0, TKE 9.1, TKE 9.2
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x	x	x
Required 011F RSA Decipher Clear Key	X'011F'						x
Required 012A Encipher Data Using AES	X'012A'						x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'		x	x	x	x	x
Required 0203 Delete Retained Key	X'0203'			x	x	x	x
Required 027D Permit Regeneration Data	X'027D'						x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'			x	x	x	x
Encipher	X'000E'	x	x	x	x	x	x
Decipher	X'000F'	x	x	x	x	x	x
Reencipher to Master Key	X'0012'	x	x	x	x	x	x
Reencipher from Master Key	X'0013'	x	x	x	x	x	x
Load First Key Part	X'001B'	x	x	x	x	x	x
Combine Key Parts	X'001C'	x	x	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x	x
Compute CMACZERO Verification Pattern for AES	X'0022'						x (TKE 9.2 only)
Compute CMACZERO Verification Pattern for DES	X'0023'						x (TKE 9.0, 9.1, and 9.2 only)
Generate Key Set	X'008C'	x	x	x	x	x	x
PKA96 Digital Signature Verify	X'0101'	x	x	x	x	x	x
PKA96 Key Import	X'0104'	x	x	x	x	x	x
PKA Clone Key Generate	X'0204'	x	x	x	x	x	x
PKA Clear Key Generate	X'0205'	x	x	x	x	x	x
Load Diffie-Hellman Key mod/gen	X'0250'	x	x	x	x	x	x
Combine Diffie-Hellman Key part	X'0251'	x	x	x	x	x	x
Clear Diffie-Hellman Key values	X'0252'	x	x	x	x	x	x
Unrestrict Combine Key Parts	X'027A'	x	x	x	x	x	x
Import First AES Key Part (min of 2)	X'0298'				x	x	x
Import Last Required AES Key Part	X'029B'				x	x	x
Import Optional AES Key Part	X'029C'				x	x	x
Complete AES Key Import	X'029D'				x	x	x
Process cleartext ICSF key parts	X'02A0'	x	x	x	x	x	x
Process enciphered ICSF key parts	X'02A1'	x	x	x	x	x	x
RNX access control point	X'02A2'	x	x	x	x	x	x
Session Key Primary	X'02A3'	x	x	x	x	x	x
Session Key Secondary	X'02A4'	x	x	x	x	x	x
Export Card Device Certificate	X'02A9'	x	x	x	x	x	x
OA Proxy Key Generate	X'0344'		x	x	x	x	x
OA Proxy Signature Return	X'0345'		x	x	x	x	x

Table 7. ACPs assigned to the SCTKEUSR role (continued)

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2	Enabled in release TKE 7.3	Enabled in release TKE 8.0, TKE 8.1, TKE 9.0, TKE 9.1, TKE 9.2
Open Migrate Host Crypto Module Public Configuration Data	X'1003'			x	x	x	x
Open Configuration Migration Tasks	X'1004'			x	x	x	x
Open Smart Card Utility Program	X'1005			x	x	x	x
Open Trusted Key Entry	X'1006'			x	x	x	x
Create Domain Group	X'1007'			x	x	x	x
Change Domain Group	X'1008'			x	x	x	x
Delete Domain Group	X'1009'			x	x	x	x
Create Crypto Module Group	X'100A'			x	x	x	x
Change Crypto Module Group	X'100B'			x	x	x	x
Delete Crypto Module Group	X'100C'			x	x	x	x
Open Edit TKE Files	X'100D'			x	x	x	x
Open TKE File Management Utility	X'100E'			x	x	x	x
Manage Host List	X'100F'					x	x
TKE USER	X'8002'	x	x				

TKEGRPMB

Table 8. ACPs assigned to the TKEGRPMB role

ACP - Current description	Numeric value	Enabled in release TKE 8.1, TKE 9.0, TKE 9.1, TKE 9.2
Required 0047 Change Own Passphrase**	X'0047'	x
Required 008E Generate Key**	X'008E'	x
Required 0100 PKA96 Digital Signature Generate**	X'0100'	x
Required 0103 PKA96 Key Generate**	X'0103'	x
Required 0116 Read Public Access-Control Information**	X'0116'	x
Required 011F RSA Decipher Clear Key**	X'011F	x
Required 012A Encipher Data Using AES**	X'012A'	x
Required 012B Symmetric Algorithm Decipher - secure AES keys**	X'012B'	x
Required 0203 Delete Retained Key**	X'0203'	x
Required 027D Permit Regeneration Data**	X'027D'	x
Required 027E Permit Regeneration Data For Retained Keys**	X'027E'	x

DEFAULT

DEFAULT role when initialized for use with smart card profiles

Table 9. ACPs assigned to the DEFAULT role when initialized for use with smart card profiles

ACP	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0 to TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0, TKE 8.1	Enabled in release TKE 9.0, TKE 9.1, TKE 9.2
*****Required*** 0047 Change Own Passphrase**	X'0047'				x	x
*****Required*** 008E Generate Key**	X'008E'	x	x	x	x	x
*****Required*** 0100 PKA96 Digital Signature Generate**	X'0100'	x	x	x	x	x
*****Required*** 0103 PKA96 Key Generate**	X'0103'	x	x	x	x	x
*****Required*** 0116 Read Public Access-Control Information**	X'0116'	x	x	x	x	x
*****Required*** 011F RSA Decipher Clear Key**	X'011F'	x	x	x	x	x
*****Required*** 012A Encipher Data Using AES**	X'012A'				x	x
*****Required*** 012B Symmetric Algorithm Decipher - secure AES keys**	X'012B'		x	x	x	x
*****Required*** 0203 Delete Retained Key**	X'0203'	x	x	x	x	x
*****Required*** 027D Permit Regeneration Data**	X'027D'				x	x
*****Required*** 027E Permit Regeneration Data For Retained Keys**	X'027E'		x	x	x	x
Encipher	X'000E'	x	x	x	x	x
Decipher	X'000F'	x	x	x	x	x
Generate MAC	X'0010'	x	x	x	x	x
Verify MAC	X'0011'	x	x	x	x	x
Reencipher to Master Key	X'0012'	x	x	x	x	x
Reencipher from Master Key	X'0013'	x	x	x	x	x
Load First Master Key Part	X'0018'	x	x	x	x	x
Combine Master Key Parts	X'0019'	x	x	x	x	x
Set Master Key	X'001A'	x	x	x	x	x
Load First Key Part	X'001B'	x	x	x	x	x
Combine Key Parts	X'001C'	x	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x
Translate Key	X'001F'	x	x	x	x	x
Generate Random Master Key	X'0020'	x	x	x	x	x
Clear New Master Key Register	X'0032'	x	x	x	x	x
Clear Old Master Key Register	X'0033'	x	x	x	x	x
Generate Diversified Key (CLR8-ENC)	X'0040'	x	x	x	x	x
Generate Diversified Key (TDES-ENC)	X'0041'	x	x	x	x	x
Generate Diversified Key (TDES-DEC)	X'0042'	x	x	x	x	x
Generate Diversified Key (SESS-XOR)	X'0043'	x	x	x	x	x
Enable DKG Single Length Keys and Equal Halves for TDES-ENC, TDES-DEC	X'0044'	x	x	x	x	x
Load First Asymmetric Master Key Part	X'0053'	x	x	x	x	x
Combine PKA Master Key Parts	X'0054'	x	x	x	x	x
Set Asymmetric Master Key	X'0057'	x	x	x	x	x
Clear New Asymmetric Master Key Buffer	X'0060'	x	x	x	x	x
Clear Old Asymmetric Master Key Buffer	X'0061'	x	x	x	x	x
Generate MDC	X'008A'	x	x	x	x	x
Generate Key Set	X'008C'	x	x	x	x	x
Reencipher to Current Master Key	X'0090'	x	x	x	x	x

Table 9. ACPs assigned to the DEFAULT role when initialized for use with smart card profiles (continued)

ACP	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0 to TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0, TKE 8.1	Enabled in release TKE 9.0, TKE 9.1, TKE 9.2
Generate Clear 3624 PIN	X'00A0'	x	x	x	x	x
Generate Clear 3624 PIN Offset	X'00A4'	x	x	x	x	x
Verify Encrypted 3624 PIN	X'00AB'	x	x	x	x	x
Verify Encrypted German Bank Pool PIN	X'00AC'	x	x	x	x	x
Verify Encrypted VISA PVV	X'00AD'	x	x	x	x	x
Verify Encrypted InterBank PIN	X'00AE'	x	x	x	x	x
Format and Encrypt PIN	X'00AF'	x	x	x	x	x
Generate Formatted and Encrypted 3624 PIN	X'00B0'	x	x	x	x	x
Generate Formatted and Encrypted German Bank Pool PIN	X'00B1'	x	x	x	x	x
Generate Formatted and Encrypted InterBank PIN	X'00B2'	x	x	x	x	x
Translate PIN with No Format-Control to No Format-Control	X'00B3'	x	x	x	x	x
Reformat PIN with No Format-Control to No Format-Control	X'00B7'	x	x	x	x	x
Generate Clear VISA PVV Alternate	X'00BB'	x	x	x	x	x
Encipher Under Master Key	X'00C3'	x	x	x	x	x
Lower Export Authority	X'00CD'	x	x	x	x	x
Translate Control Vector	X'00D6'	x	x	x	x	x
Generate Key Set Extended	X'00D7'	x	x	x	x	x
Encipher/Decipher Cryptovariable	X'00DA'	x	x	x	x	x
Replicate Key	X'00DB'	x	x	x	x	x
Generate CVV	X'00DF'	x	x	x	x	x
Verify CVV	X'00E0'	x	x	x	x	x
Unique Key Per Transaction, ANSI X9.24	X'00E1'	x	x	x	x	x
Reencipher to Current Master Key2	X'00F1'			x	x	x
PKA96 Digital Signature Verify	X'0101'	x	x	x	x	x
PKA96 Key Token Change	X'0102'	x	x	x	x	x
PKA96 Key Import	X'0104'	x	x	x	x	x
Symmetric Key Export PKCS-1.2/OAEP	X'0105'	x	x	x	x	x
Symmetric Key Import PKCS-1.2/OAEP	X'0106'	x	x	x	x	x
One-Way Hash, SHA-1	X'0107'	x	x	x	x	x
Data Key Import	X'0109'	x	x	x	x	x
Data Key Export	X'010A'	x	x	x	x	x
Compose SET Block	X'010B'	x	x	x	x	x
Decompose SET Block	X'010C'	x	x	x	x	x
PKA92 Symmetric Key Generate	X'010D'	x	x	x	x	x
NL-EPP-5 Symmetric Key Generate	X'010E'	x	x	x	x	x
Reset Intrusion Latch	X'010F'	x	x	x	x	x
Set Clock	X'0110'	x	x	x	x	x
Reinitialize Device	X'0111'	x	x	x	x	x
Initialize Access-Control System	X'0112'	x	x	x	x	x
Change User Profile Expiration Date	X'0113'	x	x	x	x	x

Table 9. ACPs assigned to the DEFAULT role when initialized for use with smart card profiles (continued)

ACP	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0 to TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0, TKE 8.1	Enabled in release TKE 9.0, TKE 9.1, TKE 9.2
Change User Profile Authentication Data	X'0114'	x	x	x	x	x
Reset User Profile Logon-Attempt-Failure Count	X'0115'	x	x	x	x	x
Delete User Profile	X'0117'	x	x	x	x	x
Delete Role	X'0118'	x	x	x	x	x
Load Function-Control Vector	X'0119'	x	x	x	x	x
Clear Function-Control Vector	X'011A'	x	x	x	x	x
Force User Logoff	X'011B'	x	x	x	x	x
Set EID	X'011C'	x	x	x	x	x
Initialize Master Key Cloning	X'011D'	x	x	x	x	x
RSA Encipher Clear Key	X'011E'	x	x	x	x	x
Generate Random Asymmetric Master Key	X'0120'	x	x	x	x	x
SET PIN Encrypt with IPINENC	X'0121'	x	x	x	x	x
SET PIN Encrypt with OPINENC	X'0122'	x	x	x	x	x
Clear AES New Master Key Register	X'0124'			x	x	x
Load First AES Master Key Part	X'0125'			x	x	x
Load Middle/Last AES Master Key Parts	X'0126'			x	x	x
Set AES Master Key	X'0128'			x	x	x
PKA Register Public Key Hash	X'0200'	x	x	x	x	x
PKA Public Key Register with Cloning	X'0201'	x	x	x	x	x
PKA Public Key Register	X'0202'	x	x	x	x	x
PKA Clone Key Generate	X'0204'	x	x	x	x	x
PKA Clear Key Generate	X'0205'	x	x	x	x	x
Clone-info (share) Obtain 1	X'0211'	x	x	x	x	x
Clone-info (share) Obtain 2	X'0212'	x	x	x	x	x
Clone-info (share) Obtain 3	X'0213'	x	x	x	x	x
Clone-info (share) Obtain 4	X'0214'	x	x	x	x	x
Clone-info (share) Obtain 5	X'0215'	x	x	x	x	x
Clone-info (share) Obtain 6	X'0216'	x	x	x	x	x
Clone-info (share) Obtain 7	X'0217'	x	x	x	x	x
Clone-info (share) Obtain 8	X'0218'	x	x	x	x	x
Clone-info (share) Obtain 9	X'0219'	x	x	x	x	x
Clone-info (share) Obtain 10	X'021A'	x	x	x	x	x
Clone-info (share) Obtain 11	X'021B'	x	x	x	x	x
Clone-info (share) Obtain 12	X'021C'	x	x	x	x	x
Clone-info (share) Obtain 13	X'021D'	x	x	x	x	x
Clone-info (share) Obtain 14	X'021E'	x	x	x	x	x
Clone-info (share) Obtain 15	X'021F'	x	x	x	x	x
Clone-info (share) Install 1	X'0221'	x	x	x	x	x
Clone-info (share) Install 2	X'0222'	x	x	x	x	x
Clone-info (share) Install 3	X'0223'	x	x	x	x	x

Table 9. ACPs assigned to the DEFAULT role when initialized for use with smart card profiles (continued)

ACP	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0 to TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0, TKE 8.1	Enabled in release TKE 9.0, TKE 9.1, TKE 9.2
Clone-info (share) Install 4	X'0224'	x	x	x	x	x
Clone-info (share) Install 5	X'0225'	x	x	x	x	x
Clone-info (share) Install 6	X'0226'	x	x	x	x	x
Clone-info (share) Install 7	X'0227'	x	x	x	x	x
Clone-info (share) Install 8	X'0228'	x	x	x	x	x
Clone-info (share) Install 9	X'0229'	x	x	x	x	x
Clone-info (share) Install 10	X'022A'	x	x	x	x	x
Clone-info (share) Install 11	X'022B'	x	x	x	x	x
Clone-info (share) Install 12	X'022C'	x	x	x	x	x
Clone-info (share) Install 13	X'022D'	x	x	x	x	x
Clone-info (share) Install 14	X'022E'	x	x	x	x	x
Clone-info (share) Install 15	X'022F'	x	x	x	x	x
List Retained Key	X'0230'	x	x	x	x	x
Generate Clear NL-PIN-1 Offset	X'0231'	x	x	x	x	x
Verify Encrypted NL-PIN-1	X'0232'	x	x	x	x	x
PKA92 Symmetric Key Import	X'0235'	x	x	x	x	x
PKA92 Symmetric Key Import with PIN keys	X'0236'	x	x	x	x	x
ZERO-PAD Symmetric Key Generate	X'023C'	x	x	x	x	x
ZERO-PAD Symmetric Key Import	X'023D'	x	x	x	x	x
ZERO-PAD Symmetric Key Export	X'023E'	x	x	x	x	x
Symmetric Key Generate PKCS-1.2/OAEP	X'023F'	x	x	x	x	x
Load Diffie-Hellman Key mod/gen	X'0250'	x	x	x	x	x
Combine Diffie-Hellman Key part	X'0251'	x	x	x	x	x
Clear Diffie-Hellman Key values	X'0252'	x	x	x	x	x
Unrestrict Reencipher from Master Key	X'0276'	x	x	x	x	x
Unrestrict Data Key Export	X'0277'	x	x	x	x	x
Add Key Part	X'0278'	x	x	x	x	x
Complete Key Part	X'0279'	x	x	x	x	x
Unrestrict Combine Key Parts	X'027A'	x	x	x	x	x
Unrestrict Reencipher to Master Key	X'027B'	x	x	x	x	x
Unrestrict Data Key Import	X'027C'	x	x	x	x	x
Generate Diversified Key (DALL with DKYGENKY Key Type)	X'0290'	x	x	x	x	x
Generate CSC-5, 4 and 3 Values	X'0291'	x	x	x	x	x
Verify CSC-3 Values	X'0292'	x	x	x	x	x
Verify CSC-4 Values	X'0293'	x	x	x	x	x
Verify CSC-5 Values	X'0294'	x	x	x	x	x
Process cleartext ICSF key parts	X'02A0'	x	x	x	x	x
Process enciphered ICSF key parts	X'02A1'	x	x	x	x	x
RNX access control point	X'02A2'	x	x	x	x	x
Session Key Primary	X'02A3'	x	x	x	x	x

Table 9. ACPs assigned to the DEFAULT role when initialized for use with smart card profiles (continued)						
ACP	**Numeric value**	**Enabled in release TKE 5.0 to TKE 6.0**	**Enabled in release TKE 7.0 to TKE 7.1**	**Enabled in release TKE 7.2, TKE 7.3**	**Enabled in release TKE 8.0, TKE 8.1**	**Enabled in release TKE 9.0, TKE 9.1, TKE 9.2**
Session Key Secondary	X'02A4'	x	x	x	x	x
Import Card Device Certificate	X'02A5'	x	x	x	x	x
Import CA Public Certificate	X'02A6'	x	x	x	x	x
Master Key Extended	X'02A7'	x	x	x	x	x
Delete Device Retained Key	X'02A8'	x	x	x	x	x
Export Card Device Certificate	X'02A9'	x	x	x	x	x
Export CA Public Certificate	X'02AA'	x	x	x	x	x
Reset Battery Low Indicator	X'030B'	x	x	x	x	x
Clear APKA New Master Key Register	X'031F'					x
Load First APKA Master Key Part	X'0320'					x
Load Middle/Last APKA Master Key Parts	X'0321'					x
Set APKA Master Key	X'0322'					x
OA Proxy Key Generate	X'0344'					x
OA Proxy Signature Return	X'0345'					x

Roles for use with passphrase profiles

The following roles are created when a TKE workstation crypto adapter is initialized for use with passphrase profiles:

- TKEADM
- TKEGRPMB
- TKEUSER
- KEYMAN1
- KEYMAN2
- DEFAULT

TKEADM

Table 10. ACPs assigned to the TKEADM role						
TKEADM - Current description	**Numeric value**	**Enabled in release TKE 5.0 to TKE 5.2**	**Enabled in release TKE 5.3, TKE 6.0**	**Enabled in release TKE 7.0**	**Enabled in release TKE 7.1, TKE 7.2, TKE 7.3**	**Enabled in release TKE 8.0, TKE 8.1, TKE 9.0, TKE 9.1, TKE 9.2**
*****Required*** 0047 Change Own Passphrase**	X'0047'					x
*****Required*** 008E Generate Key**	X'008E'					x
*****Required*** 0100 PKA96 Digital Signature Generate**	X'0100'			x	x	x
*****Required*** 0103 PKA96 Key Generate**	X'0103'		x	x	x	x
*****Required*** 0116 Read Public Access-Control Information**	X'0116'	x	x	x	x	x
*****Required*** 011F RSA Decipher Clear Key**	X'011F'					x
*****Required*** 012A Encipher Data Using AES**	X'012A'					x
*****Required*** 012B Symmetric Algorithm Decipher - secure AES keys**	X'012B'			x	x	x

Table 10. ACPs assigned to the TKEADM role (continued)

TKEADM - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 5.2	Enabled in release TKE 5.3, TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1, TKE 7.2, TKE 7.3	Enabled in release TKE 8.0, TKE 8.1, TKE 9.0, TKE 9.1, TKE 9.2
Required 0203 Delete Retained Key	X'0203'		x	x	x	x
Required 027D Permit Regeneration Data	X'027D'					x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'			x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x
One-Way Hash, SHA-1	X'0107'	x	x	x	x	x
Reset Intrusion Latch	X'010F'	x	x	x	x	x
Set Clock	X'0110'	x	x	x	x	x
Reinitialize Device	X'0111'	x	x	x	x	x
Initialize Access-Control System	X'0112'	x	x	x	x	x
Change User Profile Expiration Date	X'0113'	x	x	x	x	x
Change User Profile Authentication Data	X'0114'	x	x	x	x	x
Reset User Profile Logon-Attempt-Failure Count	X'0115'	x	x	x	x	x
Delete User Profile	X'0117'	x	x	x	x	x
Delete Role	X'0118'	x	x	x	x	x
Load Function-Control Vector	X'0119'	x	x	x	x	x
Clear Function-Control Vector	X'011A'	x	x	x	x	x
Import Card Device Certificate	X'02A5'		x	x	x	x
Import CA Public Certificate	X'02A6'		x	x	x	x
Delete Device Retained Key	X'02A8'		x	x	x	x
Export Card Device Certificate	X'02A9'		x	x	x	x
Export CA Public Certificate	X'02AA'		x	x	x	x
Reset Battery Low Indicator	X'030B'	x	x	x	x	x
Open Begin Zone Remote Enroll Process	X'1000'				x	x
Open Complete Zone Remote Enroll Process	X'1001'				x	x
Open Cryptographic Node Management Utility	X'1002'				x	x
Open Smart Card Utility Program	X'1005'				x	x
Open Edit TKE Files	X'100D'				x	x
Open TKE File Management Utility	X'100E'				x	x
TKE USER	X'8002'		x	x		

TKEGRPMB

Table 11. ACPs assigned to the TKEGRPMB role

ACP - Current description	Numeric value	Enabled in release TKE 8.1, TKE 9.0, TKE 9.1, TKE 9.2
Required 0047 Change Own Passphrase	X'0047'	x
Required 008E Generate Key	X'008E'	x
Required 0100 PKA96 Digital Signature Generate	X'0100'	x

Table 11. ACPs assigned to the TKEGRPMB role (continued)

ACP - Current description	Numeric value	Enabled in release TKE 8.1, TKE 9.0, TKE 9.1, TKE 9.2
Required 0103 PKA96 Key Generate	X'0103'	x
Required 0116 Read Public Access-Control Information	X'0116'	x
Required 011F RSA Decipher Clear Key	X'011F	x
Required 012A Encipher Data Using AES	X'012A'	x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'	x
Required 0203 Delete Retained Key	X'0203'	x
Required 027D Permit Regeneration Data	X'027D'	x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'	x

TKEUSER

Table 12. ACPs assigned to the TKEUSER role

TKEUSER - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2	Enabled in release TKE 7.3	Enabled in release TKE 8.0, TKE 8.1	Enabled in release TKE 9.0, TKE 9.1, TKE 9.2
Required 0047 Change Own Passphrase	X'0047'						x	x
Required 008E Generate Key	X'008E'	x	x	x	x	x	x	x
Required 0100 PKA96 Digital Signature Generate	X'0100'	x	x	x	x	x	x	x
Required 0103 PKA96 Key Generate	X'0103'	x	x	x	x	x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x	x	x	x
Required 011F RSA Decipher Clear Key	X'011F'						x	x
Required 012A Encipher Data Using AES	X'012A'						x	x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'		x	x	x	x	x	x
Required 0203 Delete Retained Key	X'0203'			x	x	x	x	x
Required 027D Permit Regeneration Data	X'027D'						x	x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'			x	x	x	x	x
Encipher	X'000E'	x	x	x	x	x	x	x
Decipher	X'000F'	x	x	x	x	x	x	x
Reencipher to Master Key	X'0012'	x	x	x	x	x	x	x
Reencipher from Master Key	X'0013'	x	x	x	x	x	x	x
Load First Key Part	X'001B'	x	x	x	x	x	x	x
Combine Key Parts	X'001C'	x	x	x	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x	x	x
Computer CMACZERO Verification Pattern for DES	X'0023'							x
Generate Key Set	X'008C'	x	x	x	x	x	x	x
PKA96 Digital Signature Verify	X'0101'	x	x	x	x	x	x	x
PKA96 Key Import	X'0104'	x	x	x	x	x	x	x
PKA Clone Key Generate	X'0204'	x	x	x	x	x	x	x
PKA Clear Key Generate	X'0205'	x	x	x	x	x	x	x

Table 12. ACPs assigned to the TKEUSER role (continued)

TKEUSER - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2	Enabled in release TKE 7.3	Enabled in release TKE 8.0, TKE 8.1	Enabled in release TKE 9.0, TKE 9.1, TKE 9.2
Load Diffie-Hellman Key mod/gen	X'0250'	x	x	x	x	x	x	x
Combine Diffie-Hellman Key part	X'0251'	x	x	x	x	x	x	x
Clear Diffie-Hellman Key values	X'0252'	x	x	x	x	x	x	x
Unrestrict Combine Key Parts	X'027A'	x	x	x	x	x	x	x
Import First AES Key Part (min of 2)	X'0298'				x	x	x	x
Import Last Required AES Key Part	X'029B'				x	x	x	x
Import Optional AES Key Part	X'029C'				x	x	x	x
Complete AES Key Import	X'029D'				x	x	x	x
Process cleartext ICSF key parts	X'02A0'	x	x	x	x	x	x	x
Process enciphered ICSF key parts	X'02A1'	x	x	x	x	x	x	x
RNX access control point	X'02A2'	x	x	x	x	x	x	x
Session Key Primary	X'02A3'	x	x	x	x	x	x	x
Session Key Secondary	X'02A4'	x	x	x	x	x	x	x
Export Card Device Certificate	X'02A9'	x	x	x	x	x	x	x
OA Proxy Key Generate	X'0344'		x	x	x	x	x	x
OA Proxy Signature Return	X'0345'		x	x	x	x	x	x
Open Migrate Host Crypto Module Public Configuration Data	X'1003'			x	x	x	x	x
Open Configuration Migration Tasks	X'1004'			x	x	x	x	x
Open Smart Card Utility Program	X'1005'			x	x	x	x	x
Open Trusted Key Entry	X'1006'			x	x	x	x	x
Create Domain Group	X'1007'			x	x	x	x	x
Change Domain Group	X'1008'			x	x	x	x	x
Delete Domain Group	X'1009'			x	x	x	x	x
Create Crypto Module Group	X'100A'			x	x	x	x	x
Change Crypto Module Group	X'100B'			x	x	x	x	x
Delete Crypto Module Group	X'100C'			x	x	x	x	x
Open Edit TKE Files	X'100D'			x	x	x	x	x
Open TKE File Management Utility	X'100E'			x	x	x	x	x
Manage Host List	X'100F'					x	x	x
TKE USER	X'8002'	x	x					

KEYMAN1

Table 13. ACPs assigned to the KEYMAN1 role

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0, TKE 8.1	Enabled in release TKE 9.0, TKE 9.1, TKE 9.2
*****Required*** 0047 Change Own Passphrase**	X'0047'					x	x
*****Required*** 008E Generate Key**	X'008E'		x	x	x	x	x
*****Required*** 0100 PKA96 Digital Signature Generate**	X'0100'		x	x	x	x	x

Table 13. ACPs assigned to the KEYMAN1 role (continued)

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0, TKE 8.1	Enabled in release TKE 9.0, TKE 9.1, TKE 9.2
Required 0103 PKA96 Key Generate	X'0103'		x	x	x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x	x	x
Required 011F RSA Decipher Clear Key	X'011F'					x	x
Required 012A Encipher Data Using AES	X'012A'					x	x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'		x	x	x	x	x
Required 0203 Delete Retained Key	X'0203'		x	x	x	x	x
Required 027D Permit Regeneration Data	X'027D'					x	x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'		x	x	x	x	x
Load First Master Key Part	X'0018'	x	x	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x	x
Clear New Master Key Register	X'0032'	x	x	x	x	x	x
Clear AES New Master Key Register	X'0124'				x	x	x
Load First AES Master Key Part	X'0125'				x	x	x
Clear APKA New master Key Register	X'031F'						x
Load First APKA Master Key Part	X'0320'						x
Open Cryptographic Node Management Utility	X'1002'			x	x	x	x

KEYMAN2

Table 14. ACPs assigned to the KEYMAN2 role

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0, TKE 8.1	Enabled in release TKE 9.0, TKE 9.1, TKE 9.2
Required 0047 Change Own Passphrase	X'0047'					x	x
Required 008E Generate Key	X'008E'	x	x	x	x	x	x
Required 0100 PKA96 Digital Signature Generate	X'0100'		x	x	x	x	x
Required 0103 PKA96 Key Generate	X'0103'		x	x	x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x	x	x
Required 011F RSA Decipher Clear Key	X'011F'					x	x
Required 012A Encipher Data Using AES	X'012A'					x	x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'		x	x	x	x	x
Required 0203 Delete Retained Key	X'0203'		x	x	x	x	x
Required 027D Permit Regeneration Data	X'027D'					x	x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'		x	x	x	x	x
Combine Master Key Parts	X'0019'	x	x	x	x	x	x
Set Master Key	X'001A'	x	x	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x	x
Reencipher to Current Master Key	X'0090'	x	x	x	x	x	x
Reencipher to Current Master Key2	X'00F1'				x	x	x
PKA96 Key Token Change	X'0102'	x	x	x	x	x	x

Table 14. ACPs assigned to the KEYMAN2 role (continued)							
ACP - Current description	**Numeric value**	**Enabled in release TKE 5.0 to TKE 6.0**	**Enabled in release TKE 7.0**	**Enabled in release TKE 7.1**	**Enabled in release TKE 7.2, TKE 7.3**	**Enabled in release TKE 8.0, TKE 8.1**	**Enabled in release TKE 9.0, TKE 9.1, TKE 9.2**
Load Middle/Last AES Master Key Parts	X'0126'				x	x	x
Set AES Master Key	X'0128'				x	x	x
Load Middle/Last APKA Master Key Parts	X'0321'						x
Set APKA Master Key	X'0322'						x
Open Cryptographic Node Management Utility	X'1002'			x	x	x	x

DEFAULT

DEFAULT role when initialized for use with passphrase profiles

Table 15. ACPs assigned to the DEFAULT role when initialized for use with passphrase profiles				
ACP - Current description	**Numeric value**	**Enabled in release TKE 5.0 to TKE 6.0**	**Enabled in release TKE 7.0, TKE 7.1, TKE 7.2, TKE 7.3**	**Enabled in release TKE 8.0, TKE 8.1, TKE 9.0, TKE 9.1, TKE 9.2**
Required 0047 Change Own Passphrase**	X'0047'			x
Required 008E Generate Key**	X'008E'			x
Required 0100 PKA96 Digital Signature Generate**	X'0100'		x	x
Required 0103 PKA96 Key Generate**	X'0103'		x	x
Required 0116 Read Public Access-Control Information**	X'0116'	x	x	x
Required 011F RSA Decipher Clear Key**	X'011F'			x
Required 012A Encipher Data Using AES**	X'012A'			x
Required 012B Symmetric Algorithm Decipher - secure AES keys**	X'012B'		x	x
Required 0203 Delete Retained Key**	X'0203'		x	x
Required 027D Permit Regeneration Data**	X'027D'			x
Required 027E Permit Regeneration Data For Retained Keys**	X'027E'		x	x
Compute Verification Pattern	X'001D'	x	x	x
Reinitialize Device	X'0111'	x	x	x
Export Card Device Certificate	X'02A9'	x	x	x

Blue smart cards (00RY790)

Smart card part, 00RY790, was shipped with TKE 9.1. In addition to having the part number printed on it, the card is blue. The blue smart card supports 521-bit Elliptic Curve (EC) cryptography and has more storage than the previous TKE smart card. Because of the stronger encryption and increase in storage, the following important features were added to TKE 9.1:

- With a blue smart card, you can create a TKE zone (defined when you initialize and personalize a Certificate Authority (CA) smart card) or a Migration zone (defined when you initialize and personalize a Migration Certificate Authority (MCA) smart card) with a zone strength of 521-bit EC. All the smart cards in any type of 521-bit EC zone must also be blue smart cards.

- If your Migration Zone (MCA) strength is 521-bit EC, you can collect and apply data from domains that are in Imprint or PCI compliant mode. With the older smart cards, it was not possible to collect or apply the settings of domains in these two states.
- When a new Local Adapter Logon key is generated on a blue smart card, the strength is 521-bit EC.
- When an Authority Signature Key or Administrator Signature key is generated on a blue smart card, you can select 521-bit EC as the key strength. You would only select this strength if the host crypto module that you will manage also has 521-bit EC support.
- Blue smart cards can hold up to 85 key parts. This is an increase of 35 key parts.

Things to know about the blue smart card:

- TKE 9.1 is the minimum supported release for the blue smart card. You may not use the blue smart card on any TKE below TKE 9.1.
- IMPORTANT RESTRICTIONS: The blue smart card is configured to run in FIPS mode. Therefore, the smart card hardware prohibits the generation of any 1024-bit RSA keys. This has the following significant implications:

  1. When you initialize a Certificate Authority (CA) smart card using a blue smart cart, the zone strength may not be 1024-bit RSA. The zone strength can be set to 2048-bit RSA or 521-bit EC.
  2. When you are making a backup CA smart card from an existing CA smart card, you may not use a blue smart card to make a backup of a 1024-bit RSA CA smart card.
  3. A blue smart card may not have a 1024-bit RSA alternate zone. This means that you must use a special procedure to move (migrate) key material from one 1024-bit RSA zone TKE smart card onto a blue TKE smart card, which must be in a different, stronger zone.

     Note: The process for moving data onto a blue smart card is described in “Moving data from a TKE smart card in a 1024-bit zone to a blue smart card” on page 53.
  4. You may not create an Authority Signature Key for managing a Crypto Express 2 host crypto module onto a blue smart card. The Crypto Express 2 only supports 1024-bit RSA signature keys.

     Note: You can copy an existing 1024-bit RSA Authority Signature Key or 1024-bit RSA local adapter logon key onto a blue smart card and use these keys.

     Recommendations:

     – Only continue to use 1024-bit RSA Authority Signature Keys if you are still managing Crypto Express 2 modules. This is a very weak key strength and it is recommended that you move to stronger keys.
     – You should stop using 1024-bit RSA local adapter logon keys. The strength is too weak. If you generate a local adapter logon key onto a blue smart card, the strength of the key will be 521-bit EC.

TKE security policy wizards

Strictly defined security policies are important in order to govern who can do the following TKE workstation activities:

Manage the TKE workstation
Activities include setting up access to the TKE workstation and managing your smart card environment.

Manage host crypto modules running in Common Cryptographic Architecture (CCA) mode
Activities include setting up access to the module, managing general purpose settings, and master key wrapping management.

Manage host crypto modules running in IBM Enterprise PKCS11 (EP11) mode
Activities include setting up access to the module, managing general purpose setting, and master key wrapping management.

All of these activities, including signing onto the TKE workstation, are security-relevant administrative actions and should only be done by a small set of trusted administrators with a high degree of accountability.

TKE 9.1 and later provides six TKE security policy wizards that work together to implement a comprehensive set of security policies for managing access to the TKE workstation and managing host crypto modules and their domains. All of the TKE security policies require that something be stored on a smart card so use the **TKE Smart Card Wizard** to create all the smart cards that the other TKE wizards need. See the **TKE Smart Card Wizard** in Table 16 on page 40 for additional information. Five additional wizards setup the minimum recommended security policies for managing administrators responsible for specific tasks. See Table 17 on page 40 for additional information.

TKE security policy guidance

Before using the TKE security policy wizards, analyze your environment and decide which of the policies you need to implement:

Controlling who has access to your TKE workstation
: This policy should be on your list because you need to control who has access to your TKE workstation. See the **TKE Workstation Logon Profile Wizard** in Table 17 on page 40 for additional information.

Controlling who can manage CCA legacy settings
: Analyze your host cryptographic environment managed from the TKE workstation to determine if this policy applies to you. See the **Setup Module Policy Wizard** in Table 17 on page 40 for additional information.

Controlling who can manage CCA PCI-compliant domain settings
: Analyze your host cryptographic environment managed from the TKE workstation to determine if this policy applies to you. See the **Setup PCI Environment Wizard** in Table 17 on page 40 for additional information.

Controlling who can manage EP11 module-wide settings
: Analyze your host cryptographic environment managed from the TKE workstation to determine if this policy applies to you. See the **Setup Module Policy Wizard** in Table 17 on page 40 for additional information.

Controlling who can manager EP11 domain-specific settings
: Analyze your host cryptographic environment managed from the TKE workstation to determine if this policy applies to you. See the **Setup Domain Policy Wizard** in Table 17 on page 40 for additional information.

TKE security policy wizards

Once you know which set of TKE security policies you need, use the **TKE Smart Card Wizard** to create the smart cards you need for the rest of the TKE security policy wizards. Table 16 on page 40 provides a summary of the **TKE Smart Card Wizard**. Table 17 on page 40 provides a summary of the security policy implementation wizards.

Note: There is a link to wizard-specific information and guidance provided on the welcome screen of all six of the wizards.

Table 16. Prerequisite TKE wizard: TKE Smart Card Wizard

Required activity	TKE security policy wizard name	TKE security policy wizard purpose	Where the TKE security policy wizard is found
Manage smart card environment.	TKE Smart Card Wizard	To create all the smart cards needed by the other TKE security policy wizards. You can also create a new TKE zone, enroll the TKE in a zone, or both.	Smart Card Utility Program (SCUP) in the **File** pull down menu.

Table 17. TKE security policy implementation wizards

Policy purpose	TKE security policy wizard name	TKE security policy wizard purpose	Where the TKE security policy wizard is found
Control access to the TKE workstation.	TKE Workstation Logon Profile Wizard	To create TKE local crypto adapter smart card profiles that control access to the TKE workstation.	Cryptographic Node Management (CNM) Utility in the **Access Control** pull down menu.
Control who can manage CCA legacy settings.	Setup Module Policy Wizard	To create CCA module-wide roles and authorities to control administrative access for managing module-wide and normal mode domain-specific settings.	Trusted Key Entry (TKE) application in Open a host or CCA domain group on the module's **General** tab.
Control who can manage CCA PCI-compliant domain settings.	Setup PCI Environment Wizard	To create CCA domain-specific roles and authorities to control administrative access for managing the domain-specific settings in IMPRINT and PCI-COMPLIANT domains.	Trusted Key Entry (TKE) application in Open a host or CCA domain group on the domain's **General** tab (only available while in imprint mode).
Control who can manage EP11 module-wide settings.	Setup Module Policy Wizard	To add administrators to the EP11 module-wide list and take the modules out of imprint mode to control administrative access for managing EP11 module-wide settings.	Trusted Key Entry (TKE) application in Open the host of EP11 domain group on the **Module General** tab (only available while in imprint mode).
Control who can manage EP11 domain-specific settings.	Setup Domain Policy Wizard	To add administrators to the EP11 domain-specific list and take the domains out of imprint mode to control administrative access for managing EP11 domain-specific settings.	Trusted Key Entry (TKE) application in Open the host or EP11 domain group on **Domain General** tab (only available while in imprint mode).

Chapter 2. Using smart cards with TKE

Companies aiming for a high level of data confidentiality and integrity are likely to install a hardware-based cryptographic system, such as one provided by the Trusted Key Entry (TKE) workstation. It allows you to keep your cryptographic keys secret and protected from unauthorized access. When properly installed and administered, using smart cards with the TKE workstation provides a high level of security.

Smart card support gives the user the ability to keep all key parts, authority and administrator signature keys, and crypto adapter logon keys from ever appearing in the clear.

Terminology

There are several terms you should be familiar with to understand the smart card support.

Certificate authority (CA) smart card
An entity that establishes a zone using the Smart Card Utility Program (SCUP). Protected by two 6-digit PINs.

CNI
Cryptographic Node Batch Initialization utility. The CNI Editor is a utility within CNM that is used to create CNI scripts to automate some of the functions of CNM. CNI scripts can be used for additional setup of the TKE workstation crypto adapter.

CNM
Cryptographic Node Management utility. This utility is a Java™ application that provides a graphical user interface to initialize and manage the TKE workstation crypto adapter. See Chapter 11, “Cryptographic Node Management utility (CNM),” on page 251.

Entity
A member of a zone. Entities can be a CA smart card, one or more TKE or EP11 smart cards, and one or more TKE workstation cryptographic adapters.

EP11 smart card
Used for storing keys and key parts. Can hold a maximum of 50 key parts, a TKE crypto adapter logon key, and an administrator signature key. Protected by a 6-digit PIN. EP11 smart cards support EP11 host crypto modules.

Group logon
Allows multiple users to co-sign the logon to the TKE workstation crypto adapter. A group may have a minimum of one member and a maximum of ten members.

Injection authority (IA) smart card
Used for approving the application of a data to a target host crypto module using the Configuration Migration Tasks application's Apply Configuration Data wizard. Protected by a 6-digit PIN.

Key part holder (KPH) smart card
Used for decrypting a specific piece of the encryption key used to protect the data that is migrated to a host crypto module using the Configuration Migration Tasks application's Apply Configuration Data wizard. Protected by a 6-digit PIN.

Migration certificate authority (MCA) smart card
An entity that establishes a migration zone using the Configuration Migration Tasks application. Protected by two 6-digit PINs.

PIN prompt
PIN prompts appear as pop-ups from the application and also on the smart card reader. The smart card reader expects a PIN to be entered promptly; otherwise a timeout condition occurs.

SCUP
Smart Card Utility Program. Performs maintenance operations, such as the creation/initialization and personalization of CA, TKE, and EP11 smart cards and zone enrollment of the TKE workstation crypto adapter. See Chapter 12, “Smart Card Utility Program (SCUP),” on page 291.

© Copyright IBM Corp. 2000, 2021

Smart card reader
Hardware where the PIN protecting the smart card is entered. Also, where the key parts are entered with secure key entry. Two, three, or four smart card readers may be attached to the TKE workstation.

TKE smart card
Used for storing keys and key parts. Can hold a maximum of 50 key parts, a TKE crypto adapter logon key and a TKE authority key. Protected by a 6-digit PIN. TKE smart cards support CCA host crypto modules.

Zone
A security concept ensuring that only members of the same zone can exchange key parts. A zone is established by a CA smart card. See “Zone creation ” on page 49.

Preparation and planning

Before beginning a smart card implementation, consider these questions:

- How many users will be using smart cards?
- Will you be using group logon?
- How many members will be in the group?
- How many members in the group will be required to sign a logon?
- What role will the group have?
- What type of roles will users have?
- Are there procedures requiring special security considerations?
- Which tasks will have dual control?
- Who should be involved in security, auditing, and operation procedures in a test environment?
- Who should be involved in security, auditing, and operation procedures in a production environment?
- How many TKE and EP11 smart cards will you have?
- How many backup CA smart cards will you have?
- Where will you keep backup CA smart cards?
- How many users will have access to the CA smart cards? Who will know the two CA PIN numbers? Where will the CA smart card and backups be secured?
- If you have more than one TKE workstation, will they be in the same zone?

Using the IDENTIV smart card reader

TKE 9.0 and later supports IDENTIV smart card readers.

The IDENTIV smart card reader does not have a display window and all the necessary information is signaled by sound from the smart card reader. The IDENTIV smart card reader has:

A PIN pad
When you press on the PIN pad, a tone comes from the reader that indicates that the pad was pressed. When the PIN is fully entered, a different pitched tone plays, signaling that the PIN is complete. On the PIN pad, TKE supports the numeric buttons (0-9), the red cancel button, the yellow clear button, and the green enter button. The yellow clear button is a backspace button so if you press the wrong button, you can clear it by using the yellow button.

Two LED indicators (green and yellow)
When the green LED indicator is on, the smart card is present in the reader. If the green LED indicator is flashing or not on, the smart card is not detected to be in the reader or has timed out.

When the yellow LED indicator is flashing, the PIN operation is in progress. If the PIN operation is not in progress, the yellow LED indicator is not on.

Only one smart card application can be opened at a time. If more than one is opened, you get an error message that indicates that smart card functions are not available or smart card readers are not available, depending on the application.

The smart card has a gold plated contact. Insert the gold plated contact so that it faces you and pointed down into the smart card reader.

Using the OmniKey smart card reader

The smart card reader has a PIN pad and a display window. On the PIN pad, TKE supports the numeric buttons (0-9), the red X cancel button, and the yellow <- backspace button.

The display is blank if the reader is not attached. When attached, a USB plug symbol displays. A microprocessor chip symbol displays after you insert a smart card.

Only one smart card application may be opened at a time. If more than one is opened, you will get an error message indicating that smart card functions are not available or smart card readers are not available, depending on the application.

The smart card has a gold plated contact. Insert the gold plated contact facing you and pointing down into the smart card reader.

When prompted to insert a smart card, push the smart card all the way in until a microprocessor chip symbol displays. If a USB plug symbol displays, you have not inserted the smart card correctly

When prompted for a PIN, enter your PIN using the numeric buttons on the PIN pad. If a PIN is not entered promptly, the PIN prompt will time out and a timeout message will be issued from the application. You must restart the task.

The <- is a backspace button; if you press the wrong button, you can backspace using <-.

The other buttons on the PIN pad are not operational.

Using the Gemalto smart card reader

TKE 9.0 and later supports Gemalto smart card readers.

Important: Gemalto CT700 readers only work with smart cards that have applets that are loaded from TKE 8.1 or later. Therefore, you must carry Omnikey Cardman 3821 smart card readers forward to use smart cards with pre-TKE 8.1 applets on TKE 9.0 and later. See Table 35 on page 294 for the actions that are required to move to smart cards that work in Gemalto smart card readers.

The smart card reader has a PIN pad, a display window, and some LED indicators. On the PIN pad, TKE supports the numeric buttons (0-9), the red cancel button, the yellow clear button, and the green Enter button.

The display is blank if the reader is not attached. When attached, the display shows 'Insert Card' and the green LED flashes. When you insert a smart card, the display goes blank and the green LED goes to a solid color.

Only one smart card application can be opened at a time. If more than one is opened, you get an error message that indicates that smart card functions are not available or smart card readers are not available, depending on the application.

The smart card has a gold plated contact. Insert the gold plated contact so that it faces you and pointed down into the smart card reader.

When prompted to insert a smart card, insert the smart card until the green LED light stops flashing. If the display still shows 'Insert Card', the smart card was not inserted correctly.

When prompted for a PIN, enter your PIN by using the numeric buttons on the PIN pad and press Enter. If a PIN is not entered promptly, the PIN prompt times out and a timeout message is displayed for the application. You must then restart the task.

The Clear button works like a backspace button. If you press the wrong button when you are entering your PIN, you can backspace a character or characters by pressing the clear button.

The Cancel button can be used to cancel the task anytime while you are completing a smart card operation.

The other buttons on the PIN pad are not operational.

For information on the procedures that must be followed if you want to use smart cards that are supported by Gemalto smart card readers, see Chapter 3, “TKE upgrade and migration actions,” on page 55.

Things to consider

- You can carry your HID/OMNIKEY smart card readers from older TKEs forward to your TKE 9.0 and later systems.
- If you use HID/OMNIKEY smart card readers on your TKE 9.0 or later system, any previously initialized smart cards can be used on TKE 9.0 or later. Any smart card limitations that existed for the smart cards on TKE 8.1 also apply to TKE 9.0 and later.
- Any smart card that is initialized and personalized on TKE 9.0 or later can be used in either the HID/OMNIKEY, Gemalto, or IDENTIV smart card readers.
- TKE 9.0 and later supports a combination of HID/OMNIKEY, Gemalto, and IDENTIV smart card readers at the same time. Gemalto and IDENTIV smart card readers can be used only with smart cards that were initialized on TKE 8.1 or later.
- If you experience issues after you unplugged and plugged a combination of smart card readers in, you might restart the workstation.

Smart card compatibility issues

Features added in recent TKE releases (such as support for ECC authority signature keys in TKE 8.0) have required changes to the smart card applets. Because of these changes, there are restrictions on which smart cards can be used with a particular TKE release.

Applet version

When a new smart card is created, an applet is loaded onto the smart card. This occurs when initializing and personalizing CA or MCA smart cards, when creating a backup CA or MCA smart card, or when initializing and enrolling TKE, EP11, IA, or KPH smart cards in a zone. The applet version depends on the TKE release and type of smart card used, as shown in the following tables.

Table 18. Applet version by TKE release

	CA smart card	**TKE smart card**	**EP11 smart card**	**Smart card part**
TKE 5.2 or earlier	applet version = 0.3	applet version = 0.3	Not supported	Any supported card
TKE 5.3	applet version = 0.3	applet version = 0.4	Not supported	Any supported card
TKE 6.0	applet version = 0.4	applet version = 0.5	Not supported	Any supported card
TKE 7.0	applet version = 0.4	applet version = 0.6	Not supported	Any supported card
TKE 7.1	applet version = 0.4	applet version = 0.7	Not supported	Any supported card
TKE 7.2	applet version = 0.4	applet version = 0.8	Not supported	45D3398
TKE 7.2	applet version = 0.4	applet version = 0.8	applet version = 0.1	74Y0551

Table 18. Applet version by TKE release (continued)				
	CA smart card	**TKE smart card**	**EP11 smart card**	**Smart card part**
TKE 7.3	applet version = 0.4	applet version = 0.8	Not supported	45D3398
TKE 7.3	applet version = 0.5	applet version = 0.9	applet version = 0.2	74Y0551
TKE 8.0	applet version = 0.4	applet version = 0.8	Not supported	45D3398
TKE 8.0	applet version = 0.5	applet version = 0.10	applet version = 0.2	74Y0551
TKE 8.0	applet version = 0.5	applet version = 0.10	applet version = 0.2	00JA710
TKE 8.1	applet version = 0.6	applet version = 0.11 [1]	Not supported	45D3398
TKE 8.1	applet version = 0.7	applet version = 0.12 [2]	applet version = 0.3[3]	74Y0551
TKE 8.1	applet version = 0.7	applet version = 0.12[2]	applet version = 0.3[3]	00JA710
TKE 9.0	applet version = 0.6	applet version = 0.15[4]	Not supported	45D3398
TKE 9.0	applet version = 0.7	applet version = 0.16[5]	applet version = 0.4[6]	74Y0551
TKE 9.0	applet version = 0.7	applet version = 0.16[5]	applet version = 0.4[6]	00JA710
TKE 9.1 and TKE 9.2	applet version = 0.6	applet version = 0.17	Not supported	45D3398
TKE 9.1 and TKE 9.2	applet version = 0.7	applet version = 0.18	applet version = 0.5	74Y0551
TKE 9.1 and TKE 9.2	applet version = 0.7	applet version = 0.18	applet version = 0.5	00JA710
TKE 9.1	applet version = 0.8	applet version = 0.19	applet version = 0.6	00RY790
TKE 9.2	applet version = 0.8	applet version = 0.20	applet version = 0.7	00RY790

Notes:

1. A PTF available on TKE 8.1 changes the applet version to 0.13. The PTF adds support for an alternate zone when copying smart card contents.
2. A PTF available on TKE 8.1 changes the applet version to 0.14. The PTF adds support for an alternate zone when copying smart card contents.
3. A PTF available on TKE 8.1 changes the applet version to 0.4. The PTF adds support for an alternate zone when copying smart card contents.
4. A PTF available on TKE 9.0 changes the applet version to 0.17. The PTF modifies support for using an alternate zone when copying smart card contents.

5. A PTF available on TKE 9.0 changes the applet version to 0.18. The PTF modifies support for using an alternate zone when copying smart card contents.
6. A PTF available on TKE 9.0 changes the applet version to 0.5. The PTF modifies support for using an alternate zone when copying smart card contents.

Table 19. Applet version by TKE release

	MCA smart card	**IA smart card**	**KPH smart card**	**Smart card part**
TKE 7.0 to TKE 7.2	applet version = 0.1	applet version = 0.1	applet version = 0.1	Any supported card
TKE 7.3	applet version = 0.1	applet version = 0.1	applet version = 0.1	45D3398
TKE 7.3	applet version = 0.2	applet version = 0.2	applet version = 0.2	74Y0551
TKE 8.0	applet version = 0.1	Not supported	Not supported	45D3398
TKE 8.0	applet version = 0.2	applet version = 0.3	applet version = 0.3	74Y0551
TKE 8.0	applet version = 0.2	applet version = 0.3	applet version = 0.3	00JA710
TKE 8.1, TKE 9.0, TKE 9.1, and TKE 9.2	applet version = 0.3	Not supported	Not supported	45D3398
TKE 8.1, TKE 9.0, TKE 9.1, and TKE 9.2	applet version = 0.4	applet version = 0.4	applet version = 0.4	74Y0551
TKE 8.1, TKE 9.0, TKE 9.1, and TKE 9.2	applet version = 0.4	applet version = 0.4	applet version = 0.4	00JA710
TKE 9.1 and TKE 9.2	applet version = 0.5	applet version = 0.5	applet version = 0.5	00RY790

Notes:

1. In general, smart cards that are created on a particular TKE release cannot be used on TKE workstations that are at prior release levels. TKE 5.2 applets are not usable on TKE 7.1 and later because they can only be installed on DataKey smart cards, and DataKey smart cards are not supported.
2. If you are collecting data that will be applied to a Crypto Express 5 or later:
   - The KPH certificates must come from smart cards at the minimum applet version 0.3. This applet version was first available in TKE 8.0.
   - The collect must be done from a TKE 8.0 or later.
3. If you are applying data to a Crypto Express 5 or later, you must use IA smart cards that are at applet version 0.3 or later. This applet version was first available in TKE 8.0.
4. If you are using Gemalto CT700 smart card readers:
   - MCA smart cards must be at the minimum applet version 0.4. This applet version was first available in TKE 8.1.
   - IA smart cards must be at the minimum applet version of 0.4. This applet version was first available in TKE 8.1.

- KPH smart cards must be at the minimum applet version of 0.4. This applet version was first available in TKE 8.1.

5. If you want to collect data from a Common Cryptographic Architecture (CCA) module that has domains configured to run in PCI-compliant mode, all of your smart cards (the MCA, IA, and KPH smart cards):
   - Must be initialized and personalized on TKE 9.1 or later.
   - Must be the minimum part number of 00RY790 (the blue smart card).
   - The Migration Zone (MCA smart card) must have EC-521 strength zones.

Zone key type and length

TKE uses smart cards and establishes zones for two categories of operations: normal crypto module administration, which includes loading keys and key parts and signing commands to a crypto module, and configuration migration. CA, TKE, and EP11 smart cards are created for normal crypto module administration, and MCA, IA, and KPH smart cards are created for configuration migration. Support for configuration migration was added in TKE 7.0.

Zone keys establish secure communication between entities in a zone. Entities include smart cards and the TKE workstation crypto adapter.

Prior to TKE 6.0, zones for normal crypto module administration use 1024-bit RSA keys. Beginning in TKE 6.0, customers can select either 1024-bit RSA keys or 2048-bit RSA keys as the zone key type.

When support for configuration migration was added in TKE 7.0, the zone key type for configuration migration was restricted to 2048-bit RSA keys. Similarly, when support for EP11 crypto modules was added in TKE 7.2, a zone key type of 2048-bit RSA keys was required to create an EP11 smart card.

Beginning in TKE 9.1, zones based on P521 ECC keys are supported for both normal crypto module administration and configuration migration. You must use 00RY790 smart cards for this zone type. The zone key type and size is selected when initializing and personalizing a CA or an MCA smart card.

Smart card usage

Table 20 on page 47 indicates in more detail where CA smart cards created in different releases can be used. Usage means employing a CA smart card to create TKE smart cards, creating a backup CA smart card, or enrolling a TKE workstation cryptographic adapter in the zone. OmniKey smart card readers are required to use CA smart cards with a zone key length of 2048-bits.

Table 20. CA smart card usage

	Use on TKE 5.2 or earlier	**Use on TKE 5.3**	**Use on TKE 6.0**	**Use on TKE 7.0 and later**
Created on TKE 5.2 or before	Yes	Yes	Yes	No
Created on TKE 5.3	No	Yes	Yes	Yes[1]
Created on TKE 6.0, 1024-bit zone key	No	Yes	Yes	Yes[1]
Created on TKE 6.0, 2048-bit zone key	No	No	Yes	Yes
Created on TKE 7.0 and above	No	No	No	Yes

[1] You must use smart cards associated with part number 45D3398 or 74Y0551 in this release of TKE. Datakey smart cards are not supported in TKE 7.0 and above.

Table 21 on page 48 indicates in more detail where TKE smart cards created in different releases can be used. Usage means employing a TKE smart card to store or load key parts or to generate and retain an authority signature key or a crypto adapter logon key, to copy keys and key parts from one smart card to another, to log on to the TKE workstation crypto adapter, or to create a profile for the TKE workstation crypto adapter. The TKE smart card must be enrolled in the zone where it is used, although this is not required to use the authority signature key or crypto adapter logon key on the smart card. The authority signature key and the crypto adapter logon key are not subject to zone constraints.

Table 21. TKE smart card usage

	Use on TKE 5.2 or before	**Use on TKE 5.3**	**Use on TKE 6.0**	**Use on TKE 7.0 and above**
Created on TKE 5.2 or before	Yes	Yes	Yes	No
Created on TKE 5.3	No	Yes	Yes	Yes[2]
Created on TKE 6.0, 1024-bit zone key	No	Yes[1]	Yes	Yes[2]
Created on TKE 6.0, 2048-bit zone key	No	No	Yes	Yes
Created on TKE 7.0 and above	No	No	No	Yes

[1] This smart card could contain:

- Key parts.
- A 1024-bit or 2048-bit authority signature key.
- A 1024-bit or 2048-bit cryptographic adapter logon key.

In TKE 5.3, 2048-bit keys are not supported. Only the key parts and 1024-bit keys could be used in TKE 5.3.

[2] You must use smart cards associated with part number 45D3398 or 74Y0551 in this release of TKE. Datakey smart cards are not supported in TKE 7.0 or later.

When creating an EP11 smart card on TKE 8.1, you must use a smart card associated with part numbers 74Y0551 or 00JA710.

Datakey card usage

Support for Datakey smart cards was withdrawn in TKE 7.0. You can make a backup of an existing Datakey CA smart card onto a more current smart card part number or copy key parts from an existing Datakey TKE smart card onto a more current smart card part number, but you cannot otherwise use Datakey smart cards on TKE 7.0 or later.

Use the Smart Card Utility program to backup an existing Datakey CA smart card. This allows the zone of the Datakey CA smart card to continue to be used on TKE 7.0 or later. Use the *Backup CA smart card* option in the *CA Smart Card* pull-down menu to backup a CA smart card.

Copy key parts from an existing Datakey TKE smart card using the Cryptographic Node Management Utility. The target TKE smart card must be in the same zone as the source TKE smart card. This allows key parts from the Datakey TKE smart card to be used on TKE 7.0 or later. Use the *Copy Smart Card* option in the *Smart Card* pull-down menu to copy keys and key parts from one TKE smart card to another. The *Smart Card* pull-down menu is displayed only when smart card readers are enabled under the *File* pull-down menu.

Zone concepts

Smart card support provides the ability to store key parts and the ability to enter key parts directly by using the card reader key pad. Key parts can also be transferred between the TKE crypto adapter and the smart card, or between two smart cards securely. Smart card support for TKE is designed around the concept of a zone. This is done to ensure the secure transfer of key parts.

These are members of a zone:

- CA smart card
- TKE workstation crypto adapter
- TKE smart cards
- EP11 smart cards

A member of a zone is referred to as an entity. Entities must be in the same zone before they can exchange key information.

The zone ID is checked only when exchanging key parts. Other functions using TKE smart cards (TKE crypto adapter logon key, TKE authority signature key) do not check the zone ID of the TKE smart card against the zone ID of the TKE workstation crypto adapter. In other words, a TKE smart card from a different zone may be used to logon to the TKE workstation crypto adapter in another zone, but the key parts on the TKE smart card cannot be exchanged in this zone (because the TKE smart card is enrolled in another zone).

Beginning with TKE 9.0, TKE and EP11 smart cards can be created that support both a primary zone and an alternate zone. The primary zone is established when the TKE or EP11 smart card is initialized and enrolled by using the Smart Card Utility Program. The primary zone cannot be changed. The primary zone is used when you load key parts from the smart card to a host crypto module and when you generate a key part on the TKE workstation crypto adapter and transfer it to the smart card.

An optional alternate zone can also be established by using the Smart Card Utility Program. The alternate zone allows key parts that are saved on smart cards in one primary zone to be copied to smart cards with a different primary zone. Without the alternate zone, these copies would not be possible. Keys and key parts can be copied from one smart card to another whenever the primary zone on the source smart card matches either the primary or the alternate zone on the target smart card. An alternate zone can be removed when it is no longer needed or changed to a different alternate zone.

Alternate zone support was added to allow you to upgrade from a zone based on a 1024-bit RSA key to a zone based on a 2048-bit RSA key and to copy existing keys and key parts from the old smart cards to the new smart cards. A PTF for TKE 8.1 makes alternate zone support available on that TKE release.

Authentication and secure communication

The entity authentication and generation of session keys is established through a public key exchange process between entities. Session keys are symmetric keys that are exchanged between entities and are protected by encryption with a public key that was previously received from the intended recipient. Session keys are used for both encryption and decryption of key parts between entities. In order to have a secure line for communication, the session keys are established between any two entities.

Export of sensitive information (from TKE smart cards or TKE workstation crypto adapters) is only done when encrypted under a session key. An entity will only establish a connection with other entities that are members of the same zone as itself. This prevents sensitive information from being used outside the zone.

Zone creation

A zone is created when you use the Smart Card Utility Program (SCUP) to create a CA smart card. The CA smart card issues a root certificate for itself and has the ability to issue certificates to other TKE entities. A zone can have only one CA smart card (plus optional backup smart cards). In other words, a zone is defined by a CA smart card.

CA smart cards

The CA smart card is protected by two six-digit PINs. To ensure dual control, the two PINs should belong to different people. Both PINs must be entered for all functions requiring a CA smart card. A CA smart card is only used by the SCUP application. If either of the PINs of a CA smart card is entered incorrectly 5 times, the CA smart card will be permanently blocked. A CA smart card cannot be unblocked. You will be unable to unblock any blocked TKE smart cards – which means you will be unable to retrieve key parts from the blocked TKE smart card; nor will you be able to enroll TKE workstation crypto adapters in the zone.

We strongly recommend that you have backups of the CA smart card available. CA backup smart cards are necessary in case the original CA smart card is misplaced, destroyed or blocked.

Zone description

When a CA smart card is created, the user is prompted to enter an optional zone description. The zone description can be up to twelve characters in length and cannot be changed.

When you enroll an entity (a TKE smart card, EP11 smart card, or a TKE workstation crypto adapter), the entity inherits the zone description from the CA smart card performing the enrollment. Similarly, when you backup a CA smart card, the zone description will be the same for both cards.

Zone identifier (ID)

When a CA smart card is created, the system will generate an 8-digit zone number, a zone ID. The zone ID has similar properties to the zone description. The main difference is that the zone ID is created by the system. It is derived from the system clock of the workstation that created the CA smart card.

The TKE application uses the zone ID to check if two cards belong to the same zone. The zone ID acts as an 'early warning' that an illegal action is being attempted; if this check fails, the entities themselves will eventually detect and stop the illegal operation.

Multiple zones

It may be desirable to use multiple primary zones, especially if you have multiple TKE workstations. In fact, it is recommended that separate zones be created for testing and production systems. This prevents keys from getting intermixed.

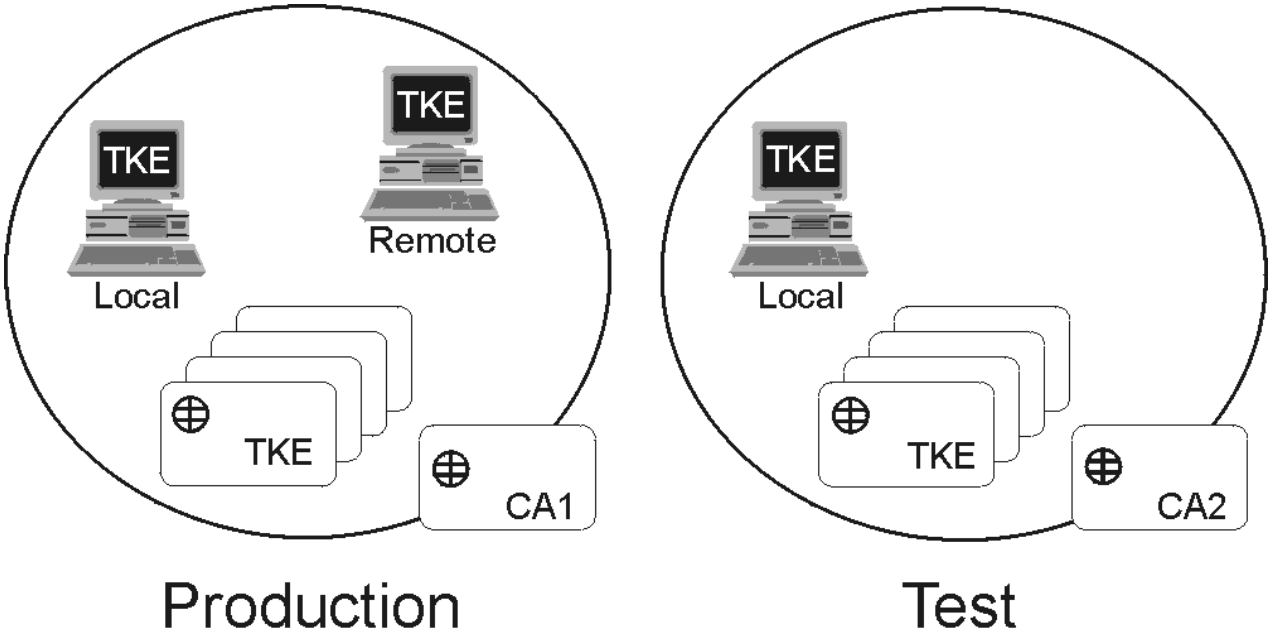


Figure 6. Multiple primary zones

Figure 6 on page 50 shows multiple primary zones for a production and test system. The production system has a remote TKE workstation enrolled; the test system does not. There are separate CA smart cards associated with each system.

Enrolling an entity

To enroll an entity into a zone, you need the CA smart card for the zone. Entities that the CA smart card enrolls are:

- TKE workstation crypto adapters.
- TKE smart cards.
- EP11 smart cards.

For TKE workstation crypto adapters, there are local and remote enrollments. Your primary TKE workstations and any local backups use local enrollment. Any offsite TKE workstations that do not have direct access to the CA use remote enrollment.

During enrollment, the entity receives and stores the root certificate of the CA smart card. The root certificate is then used to verify other entities that are enrolled in the same zone.

Additionally, the CA issues a certificate for the entity, enabling the entity to:

- Prove to other entities that it has been enrolled into the zone.
- Allow a session key to be encrypted by the public key included in the entity certificate in order to exchange key parts.

The certificate that was issued to the TKE workstation crypto adapter by the CA is destroyed if you initialize the adapter.

Cryptographic connections can be established only between entities that share a common zone. The TKE workstation crypto adapter supports only a primary zone. TKE and EP11 smart cards that are created on TKE 9.0 or later support both a primary zone and an optional alternate zone. The alternate zone on TKE and EP11 smart cards can be used only for copying keys and key parts from one smart card to another.

TKE smart cards

TKE smart cards support CCA host crypto modules. They can hold:

- A maximum of 50 key parts for non-blue smart cards or 85 key parts for blue smart cards:
  - ICSF master key parts
  - ICSF operational key parts
  - TKE workstation crypto adapter master key parts
- One TKE crypto adapter logon key. TKE crypto adapter logon keys generated on TKE 7.0 and later are 2048-bits long. TKE crypto adapter logon keys generated on earlier versions of the TKE workstation may be 1024-bits long.
- One authority signature key. When generating an authority signature key and saving it to a smart card, you select the key type and size. 1024-bit and 2048-bit RSA keys and BP-320 ECC keys are supported.

After the TKE smart card is initialized, enrolled in a zone, and personalized, it can be used for the storage and exchange of key parts.

A TKE smart card initialized using TKE 7.0 (applet version 0.6 or later) is protected by a 6-digit PIN. Smart cards initialized on earlier versions of TKE are protected by a 4-digit PIN. Enter this PIN when prompted to access the TKE smart card. If the PIN of a TKE smart card is entered incorrectly 3 times, the TKE smart card will be blocked. It is possible to unblock a TKE smart card using SCUP and a CA smart card in the same zone. The unblocking process resets the PIN failure counter on the TKE smart card. It does not reset or change the PIN value.

The zone environment is the primary security feature of the TKE smart cards (not the PIN). Even if an attacker gets access to several TKE smart cards containing all key parts for a certain key and manages to

get access to the PIN's of those smart cards, there will not be any access to the key parts. The TKE smart card will only export its key parts to other entities in the same zone and the key parts will always be encrypted during such transfers.

Before a TKE smart card can be used for logging onto a TKE workstation, a TKE crypto adapter logon key must be generated on the TKE smart card and the TKE administrator must create a user profile for the user.

During the personalization of a TKE smart card, a PIN and an optional 20 character card description can be entered. The description can be changed if the TKE smart card is personalized again. The description can be used to distinguish between TKE smart cards.

EP11 smart cards

EP11 smart cards support EP11 host crypto modules. They can hold:

- A maximum of 50 key parts for non-blue smart cards or 85 key parts for blue smart cards. These can be:
  - ICSF P11 master key parts
  - TKE workstation crypto adapter master key parts
- One TKE crypto adapter logon key. This is a 2048-bit RSA key.
- One administrator signature key. This is a 320-bit Brainpool ECC key.

EP11 smart cards are protected by a 6-digit PIN. If you enter the PIN incorrectly three times in a row, the smart card is blocked and cannot be used. To unblock the smart card, run the Smart Card Utility Program and select the Unblock EP11 smart card option in the EP11 Smart Card menu. You will need a CA smart card for the zone to do this. Unblocking the smart card does not change the PIN value.

An optional description for an EP11 smart card can be entered when the smart card is personalized, the same as for TKE smart cards.

Steps to set up a smart card installation

Before using TKE smart card support, a number of hardware and software components must be installed and initialized correctly.

Notes:

1. This setup is done in conjunction with Table 30 on page 73. The tasks defined here replace task 9: *Customize the TKE workstation crypto adapter*.
2. You must be logged in as ADMIN for this task.

Table 22. Smart card task checklist

Task	Person responsible	Where	Completed
1. Attach the smart card readers	IBM CE	TKE workstation	
2. Initialize the TKE workstation crypto adapter for smart card use; see “Initializing the TKE workstation crypto adapter for use with smart card profiles” on page 85.	TKE Administrator	TKE workstation	
3. Create CA smart card (zone); see “Initialize and personalize a CA smart card” on page 299.	TKE Administrator	TKE workstation	

Table 22. Smart card task checklist (continued)			
Task	**Person responsible**	**Where**	**Completed**
4. Backup the CA smart card; see "Create a backup CA smart card" on page 301.	TKE Administrator	TKE workstation	
5. Initialize and enroll TKE smart cards into the zone; see "Initialize and enroll a smart card" on page 302.	TKE Administrator	TKE workstation	
6. Personalize TKE smart cards; see "Personalize a smart card" on page 303.	TKE Administrator	TKE workstation	
7. Enroll the local TKE workstation crypto adapter (and any remote TKE workstation crypto adapters) in the zone; see "Enroll a TKE cryptographic adapter in a primary zone" on page 305.	TKE Administrator	TKE workstation	
8. CNM utility - generate TKE workstation crypto adapter logon keys; define and load profiles; reset default role. see Chapter 11, "Cryptographic Node Management utility (CNM)," on page 251.	TKE Administrator	TKE workstation	

Moving TKE and EP11 smart card data to smart cards in a new zone

To move data from a TKE or EP11 smart card onto a corresponding TKE or EP11 smart card in a different zone, either because you want to move to a stronger zone or because you want to consolidate data from multiple zones into one zone, do the following:

1. Using the Smart Card Utility Program (SCUP) **TKE Smart Card -> Enroll TKE smart card in alternate zone** function, enroll all the target smart cards in the alternate zone of the source smart card. The alternate zone must be the same as the primary zone of the source smart card.

   Note: Alternate zones are only supported on smart cards that were initialized and personalized on TKE 8.1 or later.
2. Using any of the copy smart card or duplicate smart card content features found in the Cryptographic Node Management (CNM) or Trusted Key Entry (TKE) applications, copy the contents from the source smart cards to their corresponding target smart cards.

   Note: If the source TKE smart card is in a 1024-bit RSA zone, you must use a special process to move data onto a blue smart card. See "Moving data from a TKE smart card in a 1024-bit zone to a blue smart card" on page 53 for additional information.

Moving data from a TKE smart card in a 1024-bit zone to a blue smart card

Because blue smart cards run in FIPS mode, the blue smart card cannot have primary or alternate zones that have 1024-bit RSA strength. Therefore, data cannot be moved directly from a TKE smart card that is

enrolled in 1024-bit RSA zone onto a blue TKE smart card. In this case, the following steps must be taken to move data from a 1024-bit zone TKE smart card onto a blue smart card:

Note: This process only applies to TKE smart cards. EP11 smart cards were never allowed to be in a 1024-bit RSA strength zone.

1. In order to copy data from the source 1024-bit zone TKE smart card to a non-blue intermediate TKE smart card, you first need to create the intermediate TKE smart card by using the Smart Card Utility Program **File -> TKE zone wizard** function. Do one of the following:
   - If the target blue smart card is enrolled in an EC 521-bit zone, use the wizard to create an intermediate 2048-bit RSA strength Certificate Authority (CA) smart card. Once you have the new 2048-bit zone CA smart card, use the wizard to create one non-blue intermediate TKE smart card.
   - If the target blue smart card is enrolled in a 2048-bit zone, you do not need to create a CA smart card. Use the wizard, with the existing CA smart card, to create one non-blue intermediate TKE smart card.

   The non-blue intermediate TKE smart card must:
   - Not be a blue smart card.
   - Be enrolled in a 2048-bit zone.
   - Have the alternate zone equal to the source smart card's 1024-bit zone primary zone.
2. If necessary, enroll all the target blue smart cards in the alternate zone of the non-blue intermediate TKE smart card. You only need to do this step if the non-blue intermediate and target blue smart cards are not enrolled in the same zone. Using the Smart Card Utility Program **TKE Smart Card -> Enroll TKE smart card in alternate zone** function, enroll all the target blue smart cards in the alternate zone.
3. Using any of the copy smart card or duplicate smart card content features found in the Cryptographic Node Management (CNM) or Trusted Key Entry (TKE) applications, copy the contents from the source 1024-bit RSA zone TKE smart card to the non-blue intermediate 2048-bit RSA zone TKE smart card.

   Note: Repeat this step for each source and target smart card pair.
4. Using any of the copy smart card or duplicate smart card content features found in the Cryptographic Node Management (CNM) or Trusted Key Entry (TKE) applications, copy the contents from the non-blue intermediate TKE smart card to the target blue TKE smart card. The target smart card must have the primary zone equal to the non-blue intermediate smart card's primary zone or have the alternate zone equal to the non-blue intermediate smart card's primary zone.

   Note: Repeat this step for each source and target smart card pair.

Chapter 3. TKE upgrade and migration actions

When you upgrade an existing TKE to TKE 9.2 or when you want to copy data from one TKE to another, there are some things to consider:

- When you upgrade a TKE from one version to another, do not install the new TKE licensed internal code (LIC) or replace the TKE local crypto adapter if a new adapter is required. These tasks are done by an IBM Customer Engineer (CE). However, during an upgrade process, there are decisions and actions you need to take part in. Those actions are discussed in this topic.
- If you purchased a new TKE, this new TKE might be a replacement for an existing TKE or it might be a backup to an existing TKE. In either case, you want to copy data from the existing TKE and place it on the new TKE. The processes for copying the data on the source TKE and applying the data to the target TKE are discussed in this topic.

The topic includes:

- "Considerations before upgrading a TKE or copying data from an existing TKE" on page 55
- "Upgrading an existing TKE workstation to TKE 9.2" on page 60
- "Moving data from a TKE Version 5.x, 6.0, 7.x, 8.0, or 9.x to a new workstation at TKE 9.2" on page 62

Considerations before upgrading a TKE or copying data from an existing TKE

- "DVD-RAM is not supported on a TKE 7.2 or later system" on page 55
- "Copying files to the TKE 7.0 or TKE 7.1 hard drive" on page 55
- "Copying files to a USB flash memory drive while on a TKE 7.0 or TKE 7.1 system" on page 56
- "Preparing for a new TKE local crypto adapter" on page 58

DVD-RAM is not supported on a TKE 7.2 or later system

Important: If you are still using DVD-RAM on a pre-TKE 7.2 system, DVD-RAM is not supported on TKE 7.2 or later systems. If you want to continue to use files that are on your DVD-RAM on a TKE 7.2 or later, you must remove the data from the DVD-RAM before your move to the TKE 7.2 or later system.

Beginning with TKE 7.2, you can no longer read files from a DVD-RAM. Therefore, if you have a DVD-RAM that is formatted for TKEDATA (TKEDATA DVD-RAM) and you want to use the files from the TKEDATA DVD-RAM on a TKE 7.2 or later system, do one of the following procedures:

- Copy the files from the TKEDATA DVD-RAM to the TKE's hard drive before upgrading the TKE to version 7.2 or later. For more information, see "Copying files to the TKE 7.0 or TKE 7.1 hard drive" on page 55.
- Copy the files from the TKEDATA DVD-RAM to a USB flash memory drive that is formatted for TKEDATA from a TKE 7.0 or TKE 7.1 system. For more information, see "Copying files to a USB flash memory drive while on a TKE 7.0 or TKE 7.1 system" on page 56.

Copying files to the TKE 7.0 or TKE 7.1 hard drive

Because DVD-RAM is no longer supported on TKE 7.2 or later systems, perform the following steps if you do not need to use removable media in the future. To copy any files you have on a TKEDATA DVD-RAM to the TKE's hard drive on the TKE 7.0 or TKE 7.1 system before upgrading to TKE 7.2 or later:

1. From the Trusted Key Entry Console on your TKE 7.0 or TKE 7.1 system, open the Trusted Key Entry window pane.
2. Perform the following setup steps for the source DVD-RAM:
   a. Insert the TKEDATA DVD-RAM into the DVD drive.

© Copyright IBM Corp. 2000, 2021

b. Open the TKE Media Manager utility.

   Note: The TKE Media Manager is in the Utilities list on the Trusted Key Entry window pane.

c. Select “Activate read only CD/DVD inserted in DVD drive” and press OK.

   Note: When complete, the “DVD Drive Status” is “Active (Read Only)”.

d. Press Cancel to close the TKE Media Manager.

e. Press OK to close the informational warning message. Remember, the DVD drawer will not open until the DVD drive is deactivated.

3. Perform the following steps to copy the files from the DVD-RAM to the TKE 7.0 or TKE 7.1 hard drive:

   a. Open the TKE File Management Utility.

      Note: The TKE File Management Utility is in the Utilities list on the Trusted Key Entry window.

   b. On the left side of the File Management Utility window, select the CD/DVD Drive radio button.

   c. On the right side of the File Management Utility window, select the Local Hard Drive radio button.

   d. Select the files from the CD/DVD Drive file list and use the “Copy ->” button to copy files from the CD/DVD Drive to the local hard drive.

      Note: In general, store each file from the TKEDATA DVD-RAM into the directory that the file originally came from. General information about the three most common types of files that are saved on TKEDATA DVD-RAM include:

      - Key part files should be stored in the TKE Data Directory.
      - Profile and role definition files should be stored in the CNM Directory.
      - Data from either of the host migration wizards should be stored in the Configuration Data Directory.

      Note: After the files are saved on the TKE 7.0 or TKE 7.1 system, the files are included in the data that is saved and applied when the TKE system is upgraded to TKE 7.2 or later.

4. Perform the following clean-up steps:

   a. Close the File Management Utility by selecting either “Exit” or “Exit and logoff” to close the TKE application window.

   b. Open the TKE Media Manager utility.

      Note: The TKE Media Manager is in the Utilities list on the Trusted Key Entry window pane.

   c. Select “Deactivate media inserted into DVD drive” and press OK. When complete, the “DVD Drive Status” is “Deactivated”.

   d. Remove the TKEDATA DVD-RAM from the DVD drive.

Copying files to a USB flash memory drive while on a TKE 7.0 or TKE 7.1 system

Because DVD-RAM is no longer supported on TKE 7.2 or later systems, perform the following steps if you want to use removable media on a TKE 7.2 or later system. To copy your TKEDATA DVD-RAM files to a USB flash memory drive that is formatted for TKEDATA from a TKE 7.0 or TKE 7.1 system:

1. From the Trusted Key Entry Console on your TKE 7.0 or TKE 7.1 system, open the Trusted Key Entry window pane.
2. Perform the following setup steps for the source DVD-RAM:

   a. Insert the TKEDATA DVD-RAM into the DVD drive.

   b. Open the TKE Media Manager utility.

      Note: The TKE Media Manager is in the Utilities list on the Trusted Key Entry window pane.

   c. Select “Activate read only CD/DVD inserted in DVD drive” and press OK.

Note: When complete, the "DVD Drive Status" is "Active (Read Only)".

d. Press Cancel to close the TKE Media Manager.

e. Press OK to close the informational warning message. Remember, the DVD drawer will not open until the DVD drive is deactivated.

3. Perform the following setup steps for the new USB flash memory removable media:

a. Insert the USB flash memory drive into any open USB port on the TKE 7.0 or TKE 7.1 workstation and wait for the "USB Device Status" message to appear.

Note:

- It can take up to 1 minute for the message to appear.
- You can press OK to close the "USB Device Status" message or wait for it to close in 10 seconds.

b. Perform the following steps only if you want to format the USB flash memory drive. Proceed to Step "4" on page 57 if you do not want to format the USB flash memory drive.

The USB flash memory drive must be formatted if:

- The drive is not formatted for TKEDATA.
- You want to remove any existing data from the USB flash memory drive before you copy your files.

You can use a USB flash memory drive that was formatted for TKEDATA on a TKE 7.2 or later system. To format the USB flash memory drive:

i) From the Trusted Key Entry Console on your TKE 7.0 or TKE 7.1 system, open the Service Management window pane.

ii) Open the Format Media application.

iii) Select the "Trusted Key Entry Data" radio button and press the FORMAT button.

iv) Select the radio button for the USB flash memory drive device you want to format and press OK.

v) You might receive the "file system setting" window before the confirm format message. If you do, take the default setting and press the FORMAT button.

vi) Press YES to confirm that you want to format the media.

vii) Press OK to close the completion message.

4. Perform the following steps to copy the files from the TKEDATA DVD-RAM to the USB flash memory drive:

a. From the Trusted Key Entry Console on your TKE 7.0 or TKE 7.1 system, open the Trusted Key Entry window pane.

b. Open the TKE File Management Utility.

Note: The TKE File Management Utility is in the Utilities list on the Trusted Key Entry window.

c. On the left side of the File Management Utility window, select the CD/DVD Drive radio button.

d. On the right side of the File Management Utility window, select the USB Flash Memory Drive radio button.

e. Select the files from the CD/DVD Drive file list and use the "Copy ->" button to copy files from the CD/DVD Drive to the USB flash memory drive.

Important: The directory pull-down menu does not apply to the USB flash memory drive. Do not change the directory or it will also select the Local Hard Drive radio button.

Note: After all the files are stored on the USB flash memory drive:

- The USB flash memory drive can be used as removable media on any TKE 7.0 or later system.
- You can remove the USB flash memory drive at any time.

5. Perform the following clean-up steps:

a. Close the File Management Utility by selecting either "Exit" or "Exit and logoff" to close the TKE application window.

b. Open the TKE Media Manager utility.

   Note: The TKE Media Manager is in the Utilities list on the Trusted Key Entry window pane.

c. Select “Deactivate media inserted into DVD drive” and press OK. When complete, the “DVD Drive Status” is “Deactivated”.

d. Remove the TKEDATA DVD-RAM from the DVD drive.

Preparing for a new TKE local crypto adapter

All TKEs have a local crypto adapter. After a TKE has been configured according to your TKE security policy, the TKE local crypto adapter will contain user-defined profiles and sometimes user-defined roles. You might want to configure a new TKE local crypto adapter with an existing set of user-defined roles and user-defined profiles if:

- Your TKE is given a new TKE local crypto adapter as part of an upgrade. For example, an upgrade from TKE 8.*x* to TKE 9.0 requires the 4767 TKE crypto adapter to be replaced with the 4768 TKE local crypto adapter.
- You want to configure a new TKE workstation local crypto adapter with the same user-defined roles and user-defined profiles found on an existing TKE local crypto adapter.

You might prefer to manually configure the new TKE local crypto adapter, but there are three methods for creating files with user-defined role and user-defined profile definitions that can be copied and later used to load the roles and profiles onto a new TKE local crypto adapter. The different methods for creating role and profile definition files that can be used to load the roles and profiles onto a TKE local crypto adapter are:

- “Method 1: Creating TKESavedRoles.dat and TKESavedProfiles.dat files from CNM” on page 58
- “Method 2: Creating TKESavedRoles.dat and TKESavedProfiles.dat files from the TKE Workstation Setup wizard” on page 58
- “Method 3: Creating individual user-defined role and user-defined profile definition files” on page 59

Method 1: Creating TKESavedRoles.dat and TKESavedProfiles.dat files from CNM

Beginning in TKE 8.0, the Crypto Node Management utility provides a feature that allows you to collect all the user-defined role and user-defined profile definitions in one operation. If any user-defined roles are found, the definitions are placed in the TKESavedRoles.dat file. If any user-defined profiles are found, the definitions are placed in the TKESavedProfiles.dat file. The following steps can be used to create these files:

1. From the Trusted Key Entry Console, select **Cryptographic Node Management Utility**.
2. Select **Access Control > Save User Roles and Profiles**.

Method 2: Creating TKESavedRoles.dat and TKESavedProfiles.dat files from the TKE Workstation Setup wizard

Beginning in TKE 7.3, the TKESavedRoles.dat and TKESavedProfiles.dat files can be created by a step inside the TKE Workstation Setup wizard. In TKE 7.3, only the tasks in the TKE Workstation setup wizard can use these files. The following steps can be used to create these files:

1. On the source TKE workstation, close all windows except the pre-logon screen. The pre-logon screen has the title Welcome to the Trusted Key Entry Console.
2. Select **Privileged Mode access**.
3. Enter *admin* for the user ID.
4. Enter the password. The default password for the admin user ID is password.
5. From the Trusted Key Entry Console, select **Trusted Key Entry**.
6. Open the **TKE Workstation Setup** wizard.

7. Click **Next** as many times as necessary to skip to the Save User Roles and Profiles task.
8. Select **Yes**.
9. Click **Next** to perform the save.
   - If a file exists, you are asked whether it can be overwritten.
   - You are told if there are no user-defined roles and profiles on your system.
10. Click **Finish** to exit the wizard.

Method 3: Creating individual user-defined role and user-defined profile definition files

In all releases of the TKE, you can use a feature in the Cryptographic Node Management (CNM) utility to create individual role and profile definition files for each of your user-defined roles and profiles on the TKE's local crypto adapter. The files contain all the information that is required to load the roles and profiles onto a TKE's local crypto adapter. You can use the following steps to create individual role and profile definition files. **Note**: Use this method only if you are not on TKE 7.3 or later.

Procedure

1. On the source TKE workstation, from the Trusted Key Entry Console, select **Trusted Key Entry.**
2. Open the **Cryptographic Node Management** utility.
3. Sign on to the TKE crypto adapter if you are prompted to do so.
4. If you do not have customer-defined roles for which you need to create files, skip to step "7" on page 59.
5. **Select Access Control > Roles**.
   For each user-defined role:
   a) Highlight the user-defined role.
   b) Click **Edit**.
   c) Click **Save**.
   d) Enter a file name.
      File naming suggestion: Use *role name*.rol.
   e) Click **Save**.
      A message window opens confirming that the role has been saved.
   f) Click **OK** to close the message window.
   g) Click **Done** to end the edit session.
6. After the last user-defined role is saved, click **Done.**
7. If you do not have user-defined profiles, skip to step "10" on page 60
8. For each user-defined profile:
   a) Select **Access Controls > Profiles**.
   b) Highlight the user-defined profile.
   c) Click **Edit**.
   d) For passphrase profiles, enter a password.
      The password does not have to match the password that the profile has on the crypto adapter.
   e) Click **Save**.
   f) Enter a file name.
      File naming suggestion: Use *profile name*.pro.
   g) Click **Save**.
      A message window opens confirming that the profile has been saved.

h) Click **OK** to close the message window.

i) Click **Done** to end the edit session.

9. After the last user-defined profile is saved, click **Done**.
10. Select **File > Exit** to exit the utility.

Upgrading an existing TKE workstation to TKE 9.2

Notes:

- A TKE can only be upgraded to TKE 9.2 if the TKE feature is assigned to z14 or later.
- Only TRENTON workstations can be upgraded to TKE 9.2.
- If your TKE is currently at TKE 8.1 or older and you can upgrade it to TKE 9.2, you must purchase a 4768 crypto card with your upgrade.
- TKE 9.2 firmware is only available on USB media or through a network install.

When you upgrade an existing workstation to TKE 9.2, the TKE licensed internal code (LIC) is updated and a new TKE local crypto adapter is installed in the workstation. Both of these actions are completed by an IBM Customer Engineer (CE). At the end of the process, when the CE runs the TKE Workstation Setup wizard, you need to make the necessary customer-based decisions. The following steps are an overview of the entire upgrade process:

1. You need to create the **TKESavedRoles.dat** and **TKESavedProfiles.dat** files that are used to load your roles and profiles onto the new 4768 TKE local crypto adapter that the TKE workstation receives. For instructions on how to create these files, see “Preparing for a new TKE local crypto adapter” on page 58. These files are included in the data that is collected during the save upgrade data.
2. Before the CE starts the firmware upgrade, the CE collects customer data on the workstation by using the **Save Upgrade Data** utility. The data is placed on a USB flash memory drive.
3. The CE powers down the TKE workstation and replaces the 4767 crypto adapter with the 4768 crypto adapter.

   Notes:

   - When the 4767 crypto adapter is replaced with the 4768 crypto adapter, the TKE workstation's feature code also changes.

     Table 23. TKE feature code changes

Starting TKE workstation feature code	New TKE workstation feature code
0097	0080
0098	0081

   - Code is not placed on the new 4768 crypto adapter until the TKE Workstation Setup wizard is run.
4. The CE installs the new TKE firmware on the TKE workstation by using the Install/Recovery procedure.
5. The CE reapplies the customer data onto the TKE workstation by using the frame roll installation procedure. The USB flash memory drive with the **saved upgrade data** is used during this procedure. This step also restores the network settings.
6. The CE runs the TKE Workstation Setup wizard to complete the workstation setup process. The wizard includes a step for updating the code on the new TKE workstation’s local crypto adapter.
7. During a TKE workstation upgrade, you need to make the following customer configuration decisions. If you are not present when the CE runs the TKE Workstation Setup wizard, you can run the TKE Workstation Setup wizard on your own. The following are a list of wizard steps that require your attention:

   Initialize TKE crypto adapter
   The new 4768 TKE local crypto adapter must be initialized. You need to decide whether the TKE local crypto adapter is to be initialized for use with passphrase or smart card profiles.

Note that initializing the TKE local adapter zeroizes the adapter. Initialize the TKE local crypto adapter only one time or when you want to return to a known starting point.

Hints:

- If your user-defined TKE local adapter profiles use the system-supplied roles of TKEUSER or TKEADM, you want to initialize your adapter for use with Passphrase profiles.
- If your user-defined TKE local adapter profiles use the system-supplied roles of SCTKEUSR or SCTKADM, you want to initialize your adapter for use with smart card profiles.

Enable smart card readers
If you use smart cards, select **Yes**.

Customize displayed hash size
If you are subject to any regulations or policies that require you to limit the length of your displayed key verification patterns, you can select a reduced display length.

Load user roles and profiles
In the TKE 9.2 upgrade, the TKE workstation received a new TKE local crypto adapter. Your user-defined roles and profiles need to be loaded onto this new adapter. If you created and saved the **TKESavedRoles.dat** and **TKESavedProfiles.dat** files, as mentioned in step 1, the wizard finds the files and reloads your roles and profiles.

Note: You must set the passphrase for any passphrase profile you load onto the new TKE crypto adapter.

Add new access control points to your user roles
If you have any user-defined roles, you might need to add new access control points to the roles.

Check TKE crypto adapter group profiles
In the past, it was recommended that members of a TKE local crypto adapter group profile be assigned the role of DEFAULT. TKE now contains the system-supplied role of TKEGRPMB (TKE group member role). The TKEGRPMB role contains only the required ACPs. Checking TKE crypto adapter group profiles determines whether you have any TKE local adapter group profile members with the role of DEFAULT. If you do, the wizard offers you the option to change the member's role to TKEGRPMB.

Save user roles and profiles
If you changed any group member profiles, you might want to save your updated user-defined roles and profiles.

Convert crypto module groups to domain groups
If you have any crypto module groups from a pre-TKE 8.0 system, you can use this utility to created new domain groups based on the existing group definition.

Note: You can do this process only when you are willing and able to open the hosts included in the group. You might want to do the conversion later.

Enroll TKE crypto adapter in a zone
If your TKE was enrolled in a zone before the upgrade, you need to enroll your new 4768 TKE local crypto adapter in your zone. The CA smart card with the zone is required for this operation.

Add migration zone
If you use the Configuration Migration Tasks application, the list of known MCAs was cleared when the new 4768 crypto module was initialized. You need to add your MCAs to your MCA zone list. The MCA smart card or cards are required for this operation.

Add key part holder certificates
The upgrade operation saved and restored customer data. The list of known key part holders (KPHs) is restored. You do not need to add your KPH certificates again.

Change enhanced password encryption policy
The TKE always uses the best available method for protecting the host password during a sign-on operation. When ICSF is at FMID HCR77B0 or later, enhanced password protection is used. You can select a policy that only allows a host sign-on attempt if enhanced password protection is used. IBM recommends that you move to the minimum ICSF level of FMID HCR77B0 and that you

select the TKE policy that only allows a sign-on to systems that support enhanced password protection.

Your TKE 9.2 is ready for use when all preceding steps are completed.

Moving data from a TKE Version 5.*x*, 6.0, 7.*x*, 8.0, or 9.*x* to a new workstation at TKE 9.2

In this case, you have a new TKE 9.2 workstation (the target TKE) that is up and running. You also have an existing TKE (the source TKE) which you have been using for some amount of time. The goal is to copy your client data from the source TKE workstation to the target TKE workstation. This task might be done because the target TKE replaces the source TKE or the target TKE is a backup for the source TKE.

The process to move client data is broken down into these steps:

- "Identifying data to be copied from the source TKE to the target TKE" on page 62.
- "Copying customer data from the source TKE to USB memory in a form that the target TKE can read" on page 66.
- "On the Target TKE, copying data from USB memory onto the TKE's hard drive" on page 67.
- "Loading TKE local adapter roles and profiles" on page 69.

Identifying data to be copied from the source TKE to the target TKE

Six directories are visible to customers on the TKE workstation. These directories might contain customer data, system-supplied data, or both. These directories and their contents, in addition to an indication if the data can be copied from a source TKE to a target TKE (if the target TKE is to be a copy or a replacement for the source TKE), are:

- TKE Data Directory.
- CNM Data Directory.
- Configuration Data Directory.
- SCUP Data Directory.
- Migration Backup Data Directory.
- CCA Audit Log Data Directory.

TKE Data Directory

Table 24. TKE Data Directory

Files	File contents	Copy from source TKE to target TKE
host.dat	The list of host definitions.	Yes.
group.dat	The list of Crypto Module Group definitions.	Yes.
domaingroup.data	The list of Domain Group definitions.	Yes.
TKESavedProfiles.dat	The information necessary to reload user-defined profiles onto the TKE local crypto adapter. **Note:** This file can be generated only on TKE 8.0 or later.	Yes.

Table 24. TKE Data Directory (continued)		
Files	**File contents**	**Copy from source TKE to target TKE**
TKESavedRoles.dat	The information necessary to reload user-defined roles onto the TKE local crypto adapter. **Note:** This file can be generated only on TKE 8.0 or later.	Yes.
kphcard.dat	The list of known Key Part Holders that are used in various features of the Configuration Migration Tasks application.	Yes.
zone.dat	The list of known Migration Certificate Authorities that are used in various features of the Configuration Migration Tasks application.	No. The MCA must be explicitly added to the list of known MCAs on the target TKE.
customer-named key part file	Each file contains one key part.	Yes. However, do not move obsolete part.
customer-named authority signature key file	Each file contains one Authority Signature Key.	Yes. However, it is recommended that you store Signature Keys on smart cards and not in files.
customer-named miscellaneous file	Files might contain client generated screen captures, trace information, or other items.	Maybe. Copy if you want to archive or retain the data for any reason. However, do not move obsolete data.

CNM Data Directory

Table 25. CNM Data Directory (system-supplied files)		
Files	**File contents**	**Copy from source TKE to target TKE**
adapterinit_*xx*.cni adapteSCrinit_*xx*.cni Where *xx* is the TKE release used. For example, 71.	Cryptographic Node Initialization files.	No.
default_*xx*.rol tempdefault_*xx*.rol keyman1_*xx*.rol keyman2_*xx*.rol sctkeadm_*xx*.rol sctkeusr_*xx*.rol tkeadm_*xx*.rol tkeuser_*xx*.rol Where *xx* is the TKE release used. For example, 71.	Role definition files.	No.

Table 25. CNM Data Directory (system-supplied files) (continued)		
Files	**File contents**	**Copy from source TKE to target TKE**
keyman1.pro keyman2.pro tkeadm.pro tkeuser.rol	Profile definition files.	No.
aesstore.dat aesstore.dat.NDX fesstore.dat desstore.dat.NDX pkastore.dat kastore.dat.ND	Local Key Store files.	No.
Fcv_4tk*xx*.crt Where *xx* is the TKE release used. For example, 80.	Function Control Vector files.	No.

Table 26. CNM Data Directory (Customer-named files)		
Files	**File contents**	**Copy from source TKE to target TKE**
customer-named cni file File name likely ends with .cni.	Cryptographic Node Initialization files. **Note:** Old method for configuring local crypto module. This method is obsolete and discouraged.	No. Obsolete data.
customer-named role definition file File name likely ends with .rol.	Role definition files.	Maybe. Only move if **TKESaveRoles.dat** support is not available.
customer-named profile definition file File name likely ends with .pro.	Profile definition files.	Maybe. Only move if **TKESaveProfiles.dat** support is not available.

Configuration Data Directory

Table 27. Configuration Data Directory		
Files	**File contents**	**Copy from source TKE to target TKE**
customer-named full collect file	Collect files from the Configuration Migration Tasks application.	Yes. However, do not move obsolete files.
customer-named public info collect file	Collect files from the Migrate Host Crypto Module Public Configuration Data application.	Yes. However, do not move obsolete files.

SCUP Data Directory

This directory is empty.

Migration Backup Data Directory

This directory is empty.

CCA Audit Log Data Directory

The CCA Audit Log Data Directory is new with TKE 9.0 and only available when you sign on to the TKE workstation in Privileged Mode Access with the AUDITOR ID.

Table 28. CCA Audit Log Data Directory

Files	File contents	Copy from source TKE to target TKE
customer-named audit log file	Archive files of domain-specific audit logs from a host crypto module domain. Available with CEX6C and later.	Maybe. Move the files if you want to archive the files on the target TKE.

Table 29 on page 65 contains a summary of the data that can be copied from the source TKE to the target TKE.

Table 29. Summary of data to be copied from the source TKE

Source directory	File name	Copy from source TKE to target TKE
TKE Data Directory	host.dat	Yes.
	group.dat	Yes.
	domaingroup.data	Yes.
	TKESavedProfiles.dat	Yes.
	TKESavedRoles.dat	Yes.
	kphcard.dat	Yes.
	customer-named key part files	Yes, if current.
	customer-named authority signature key files	Yes, if current.
	customer-named miscellaneous files	Yes, if current.
CNM Data Directory	*customer-named role definition files*	Yes, if TKESavedRoles.dat is not available.
	customer-named profile definition files	Yes, if TKESavedProfiles.dat is not available.
Configuration Data Directory	*customer-named full information collect files*	Yes, if current.
	customer-named public information collect files	Yes, if current.

Table 29. Summary of data to be copied from the source TKE (continued)		
Source directory	**File name**	**Copy from source TKE to target TKE**
CCA Audit Log Data Directory	*customer-named domain-specific audit log archive files*	Yes, if retaining or backing up data.

Copying customer data from the source TKE to USB memory in a form that the target TKE can read

When you know what data needs to be copied and moved to the target TKE, select a method for copying the data to removable media. The options are:

- "Format USB memory for TKEDATA" on page 66.
- "Method 1: Copying data to USB memory by using the Save/Restore Customizable Console Data application" on page 66.
- "Method 2: Manually copy data to USB memory by using the TKE File Management Utility" on page 67.

Format USB memory for TKEDATA

All the methods for copying and moving data require the USB memory to be formatted for TKEDATA. Use the following procedure to format the removable USB memory:

1. From the Trusted Key Entry Console select **Service Management**.
2. Open the **Format Media** application.
3. Select the **Trusted Key Entry Data** radio button.
4. Click **Format**.
5. Select your USB flash memory device.
6. Click **OK** to start the format process.
7. Click **Format**. Do not change the file system format.
8. Click **Yes** to allow the media to be overwritten.
9. Click **OK** to close the completion message.

Method 1: Copying data to USB memory by using the Save/Restore Customizable Console Data application

This method is only available on TKE 8.1 and later. In this case, all the customer data is saved by using the Save/Restore Customizable Console Data application of the TKE. Use the following procedure to run the application:

Note: All the files in the listed directories are copied, including system-supplied files. There are no issues with moving the system-supplied files.

1. On the source TKE workstation, close all windows except the pre-logon screen. The pre-logon screen has the title Welcome to the Trusted Key Entry Console.
2. Select **Privileged Mode Access**.
3. Enter *admin* for the user ID.
4. Enter the password. The default password for the admin user ID is *password*.
5. From the Trusted Key Entry Console, select **Service Management**.
6. Open the **Save/Restore Customizable Console Data** application.
7. Select the following:
   a. The **TKE Data** check box.

b. The **USB flash memory driver** radio button.

c. (Optional) The **User Profile Data** check box if you want to copy the password information for Privileged Access Mode IDs of ADMIN, SERVICE, and AUDITOR.

8. Click **Save**.
9. Select your USB flash memory device.
10. Click **OK** to start the save process.
11. Click **Yes** to save.
12. Click **OK** to close the completion message.
13. Click **Cancel** to close the application.

Method 2: Manually copy data to USB memory by using the TKE File Management Utility

With this method, you explicitly decide which files you copy to USB memory. Use the following procedure to run the TKE file Management Utility:

1. From the Trusted Key Entry Console, select **Trusted Key Entry**.
2. Open the **TKE file Management Utility**.
3. On the right side of the **TKE file Management Utility** panel, select the **USB Flash Memory Drive** radio button.

   Note: If the copy is done on TKE 9.0 or later, you can preserve the TKE directory structure on the USB drive. You select the appropriate subdirectory on the USB flash memory drive.
4. On the left side of the **TKE file Management Utility** panel, select:

   a. The **local hard drive** radio button.

   b. The **TKE Data Directory**.

   c. Highlight the files to be copied.
5. Press the **Copy** button that points to the USB Flash Memory side.
6. Repeat steps 4 and 5 for any of the following directories if they exist and contain data that you want to copy onto the target TKE:

   a. CNM Data Directory.

   b. Configuration Data Directory.

   c. CCA Audit Log Data Directory.
7. Select **File > Exit** to close the utility.

On the Target TKE, copying data from USB memory onto the TKE's hard drive

When your customer data is on USB flash memory, copy the data onto the target TKE. The method that is used to copy the data on the target TKE depends on how the data was placed on the USB flash memory drive.

- "Method 1: Using the Save/Restore Customizable Console Data application to put your customer data onto the TKE" on page 67.
- "Method 2: Manually copy data from USB memory by using the TKE File Management Utility" on page 68

Method 1: Using the Save/Restore Customizable Console Data application to put your customer data onto the TKE

This method is only available on TKE 8.1 and later. In this case, your USB flash memory drive contains the file that is created during the save operation of the Save/Restore Customizable Console Data application. Use the following procedure to run the restore operation on the target TKE:

Notes:

- If a file was saved and exists on the target TKE, the file on the target TKE is overwritten during the restore operation.
- No files are removed from the target TKE by this operation.

1. On the source TKE workstation, close all windows except the pre-logon screen. The pre-logon screen has the title Welcome to the Trusted Key Entry Console.
2. Select **Privileged Mode Access**.
3. Enter *admin* for the user ID.
4. Enter the password. The default password for the admin user ID is *password*.
5. From the Trusted Key Entry Console, select **Service Management**.
6. Open the **Save/Restore Customizable Console Data** application.
7. Select the following:
   a. The **TKE Data** check box.
   b. The **USB flash memory driver** radio button.
   c. (Optional) The **User Profile Data** check box if you have this data and want to restore it.
8. Click **Restore**.
9. Select your USB flash memory device.
10. Click **OK** to start the restore process.
11. Click **Yes** to restore.
12. Click **OK** to close the completion message.
13. Click **Cancel** to close the application.

Important: This method restores the zone.dat file. If zone.data was copied onto the target TKE, you must open the **Configuration Migration Tasks** application, remove all the known migration zones from the list, and explicitly add your migration zones to the list.

Method 2: Manually copy data from USB memory by using the TKE File Management Utility

With this method, you explicitly copy the files onto the target TKE. Use the following procedure to run the TKE file Management Utility:

1. From the Trusted Key Entry Console, select **Trusted Key Entry**.
2. Open the **TKE file Management Utility**.
3. On the left side of the **TKE file Management Utility** panel, select:
   a. The **local hard drive** radio button.
   b. The **TKE Data Directory**.
4. On the right side of the **TKE file Management Utility** panel, select:
   a. The **USB Flash Memory Drive** radio button.

      Note: On TKE 9.0 or later, you need to select the subdirectory that contains your data.
   b. Highlight the files to be copied to the target directory.
5. Press the **Copy** button that points to the local hard drive.
6. Repeat steps 3, 4, and 5 for any of the files that belong in any of the following directories:
   a. CNM Data Directory.
   b. Configuration Data Directory.
   c. CCA Audit Log Data Directory.
7. Select **File > Exit** to close the utility.

Loading TKE local adapter roles and profiles

If you chose to save the TKE local crypto adapter user-defined role and user-defined profile definitions, it is time to load the roles and profiles onto the TKE local crypto adapter.

- "Method 1: Loading the roles and profiles from TKESavedRoles.dat and TKESavedProfiles.dat from CNM" on page 69
- "Method 2: Loading the individual user-defined roles and user-defined profiles for unique definition files" on page 69.

Method 1: Loading the roles and profiles from TKESavedRoles.dat and TKESavedProfiles.dat from CNM

Note: You can also use the TKESavedRoles.dat and TKESavedProfiles.dat files to reload the roles and profiles for the TKE Workstation Setup application.

This method is only available on TKE 8.0 or later. In this case, all the role and profile definitions are in files that a single Cryptographic Node Management Utility feature can use. The following procedure loads the roles and profiles for you:

1. From the Trusted Key Entry Console, select **Trusted Key Entry**.
2. Open the **Cryptographic Node Management Utility**.
3. Sign on as required.
4. Select **Access Control > Load User Roles and Profiles**.

   Note: For any passphrase profiles, you must enter a new passphrase. If a profile exists, you must decide whether it is over written.
5. You are asked if you want to delete or keep the TKESaveProfiles.dat and TKESavedRoles.dat files. Select **NO** to keep the files or **YES** to delete the files.
6. Select **File > Exit** to close the utility.

Method 2: Loading the individual user-defined roles and user-defined profiles for unique definition files

Using the Cryptographic Node Management (CNM) utility, you can load the roles and profiles from your individual role and profile definition files. The following procedure can be used to load roles and profiles from your role and profile definition files.

Procedure

1. On the source TKE workstation, from the Trusted Key Entry Console, select **Trusted Key Entry.**
2. Open the **Cryptographic Node Management** utility.
3. Sign on to the TKE crypto adapter if you are prompted to do so.
4. If you do not have customer-defined role definition files, skip to step "7" on page 69.
5. **Select Access Control > Roles**.

   For each user-defined role definition file:

   a) Click **Open**.

   b) Highlight the user-defined role definition file.

   c) Click **Open**.

   d) Click **Load**.

   e) Click **OK** to close the message window.
6. After the last user-defined role is saved, click **Done.**
7. If you do not have user-defined profiles for which you need to create files, skip to step "10" on page 70

8. Select **Access Controls > Profiles**. For each user-defined profile:
   a) Select **Open**.
   b) Highlight the user-defined profile definition file.
   c) Click **Open**.
   d) Click **Load**.
   e) Click **OK** to close the message window.
9. After the last user-defined profile is saved, click **Done**.
10. Select **File > Exit** to exit the utility.

Recovery installation

In general you should not need to install TKE code on your workstation. If you are directed to do so, follow these instructions.

Before you begin

You need to have the TKE installation DVD and a USB flash memory drive.

About this task

There are four parts to this task:

1. Save the customer data that is on the TKE workstation to the USB flash memory drive.
2. Perform the TKE workstation code update.
3. Reapply the saved customer data to the TKE workstation using a Frame Roll installation.
4. Run the TKE Workstation Setup wizard to complete the workstation setup tasks.

Procedure

Save the customer data on the TKE workstation to a USB flash memory drive.

1. Follow the instructions in “Copying customer data from the source TKE to USB memory in a form that the target TKE can read” on page 66.
2. You can install the USB flash memory with the save upgrade data onto your TKE workstation at this time or wait until step “9.a” on page 71.

Perform the TKE workstation code update.

3. Insert the USB install media on the TKE workstation.
4. Restart the TKE workstation:
   a) Select **Service Management**.
   b) Select **Shutdown or Restart**.
   c) Select **Restart Console**.
   d) Click **OK**.
   e) Click **Yes** on the **Confirm Shutdown or Restart** window.

   It can take over 7 minutes for the restart operation to complete.
5. On the **Trusted Key Entry: Upgrade / Install Recovery / Frame role** window, enter option **2** (Install Recovery) and click **Enter**.
6. Select option **1** and click **Enter** to start the Install Recovery process.

   It can take over 15 minutes for the TKE code installation to complete. You might receive the message `if the RC is zero, press ENTER to continue`. If so, click **Enter**.

   Note: Click **Enter** when you receive the green message, "The operation has completed with RC=0." and then click **Enter** on the "Part 1 successful" screen.

   After the reboot starts, you can remove the USB install media.

Apply the user data to the TKE workstation using a Frame Roll installation.

7. On the **Trusted Key Entry: Upgrade / Install Recovery / Frame Roll** window, enter option 3 (Frame Roll) and click **Enter**.
8. Select option 1 and click **Enter** to start the Frame Roll process.

   When the Frame Roll installation is complete, the DVD drive opens and a message window opens with `OPERATION SUCCESSFUL` at the top.
9. Follow the steps listed in the message window.
   a) Insert the USB flash memory drive that contains the Save Upgrade data, if it is not already installed in the workstation.
   b) Remove the TKE installation DVD from the DVD drive. You can manually close the door to the DVD drive, or let it close automatically in the next step.
   c) Click **Enter** to restart the TKE workstation.

   It can take over 10 minutes for the workstation to restart. When restart processing completes, the installation is complete and the message "TKE: Trusted Key Entry Console Workplace (Version 7.2)" displays.

Run the TKE Workstation Setup wizard to complete the workstation setup tasks.

10. Close all windows except the pre-logon window.

    The pre-logon window has the title **Welcome to the Trusted Key Entry Console**.
11. Select **Privileged Mode Access**.
12. Enter `admin` for the user ID.
13. Enter the password.

    The default password for the admin user id is `password`.
14. From the **Trusted Key Entry Console**, select **Trusted Key Entry**.
15. Open the TKE Workstation Setup Wizard
16. Click **Finish** when you are finished.

Results

Your recovery installation is complete. You have saved the customer data on the TKE workstation, updated the TKE workstation code, reapplied the customer data to the workstation, and completed the workstation setup.

Chapter 4. TKE setup and customization

To use the Trusted Key Entry key management system, several complex tasks must be completed.

Table 30. TKE management system task checklist

Task	Responsible	Where	Completed
1. Configure the host crypto modules	Client Operations or System Programmer	Support Element	
2. Load host crypto module configuration data, ensure LIC code has been loaded	Client Operations or System Programmer	Support Element	
3. If operating in LPAR mode, configure the processor	Client Operations or System Programmer	Support Element	
4. Permit each host crypto module for TKE commands	Client Operations or System Programmer	Support Element	
5. Update TCP/IP profiles for TKE	Client Network or Communications Server personnel and ICSF Administrator	Host z/OS System	
6. Customize TKE Host Program started procs (delivered with ICSF)	Client Network or Communications Server personnel and ICSF Administrator	Host z/OS System	
7. Ensure RACF administration is complete.	Client Security Administrator	Host z/OS System	
8. Start ICSF	Client Operations or System Programmer	Host z/OS System Console	
9. Customize the TKE workstation crypto adapter	TKE Administrator	TKE workstation	
10. TKE Application Customization	TKE Administrator	TKE workstation	

For more information on tasks 1 and 2, see *Z Service Guide for TKE Workstations*.

For more information on tasks 3 and 4, see:

- *Z Service Guide for TKE Workstations*.
- *PR/SM Planning Guide*.
- "TKE enablement" on page 11.
- Appendix B, "LPAR considerations," on page 321.

TKE TCP/IP setup

TKE uses TCP/IP for communication between the TKE workstation and the z/OS operating system. You should already have TCP/IP installed and configured.

1. If you do not have a domain name server running, update the Hosts file with your IP address. TKE refers to the host by IP address, not by the host name. If a domain name server (DNS) is running, then this update is unnecessary as all hosts will be identified to the DNS.

© Copyright IBM Corp. 2000, 2021

```
HOST   : 9.117.59.140 :
```

Figure 7. Entry example

2. Update your TCPIP profile to reserve a port for the TKE application.

```
PORT
50003 TCP CSFTTCP           ;ICSF TKE Server
```

Figure 8. Example of reserving a port

The example allows use of the port by the server named CSFTTCP. The port number must not start in column 1. TCP is the port type. CSFTTCP is the name of the started procedure. The 50003 is added to the port section and can be changed by the installation. The port number here has to be specified on the workstation when connecting to the host.

Any job with jobname CSFTTCP can connect to this port.

TKE host transaction program setup

The TKE Host Transaction Program (TKE HTP) is the host-based part of Trusted Key Entry. It forms the interface between the TKE workstation and the host crypto modules.

The TKE HTP (server) needs to be started before a TKE workstation (client) can communicate with the host crypto modules. The TKE HTP consists of a started procedure (CSFTTCP) which passes some start-up parameters to a REXX clist (CSFTHTP3). The clist then calls a module (CSFTTKE) that does RACF authorization checking to make sure that no unauthorized clients get to the TKE HTP server.

In order to run the new TKE Host Transaction program, the CSFTTKE module must be added to the authorized command list in IKJTSOxx on the system where the TKE HTP server will be started.

Perform these steps to install the server:

1. Update the authorized commands list in the TSO/E commands and programs member, IKJTSOxx, in the SYS1.PARMLIB data set.

```
AUTHCMD NAMES(                  /* AUTHORIZED COMMANDS */          +
       COMMAND1                 /*                     */          +
       COMMAND2                 /*                     */          +
       COMMAND3                 /*                     */          +
           .                                                       +
           .                                                       +
           .                                                       +
       CSFTTKE                  /* AUTHORIZE TKE       */          +
           .                                                       +
           .                                                       +
           .                                                       +
```

Figure 9. Format of AUTHCMD

2. Set up system security

   You will associate a RACF profile or group with the TKE Host Transaction Program. The userid or group associated with the TKE host transaction program must be authorized to all the APIs in the CSFSERV class it will use.

```
PERMIT CSFCRC  CLASS(CSFSERV) ID(userid or group) ACCESS(READ)
PERMIT CSFKIM  CLASS(CSFSERV) ID(userid or group) ACCESS(READ)
PERMIT CSFKRC  CLASS(CSFSERV) ID(userid or group) ACCESS(READ)
PERMIT CSFKRD  CLASS(CSFSERV) ID(userid or group) ACCESS(READ)
PERMIT CSFKRR  CLASS(CSFSERV) ID(userid or group) ACCESS(READ)
PERMIT CSFKRW  CLASS(CSFSERV) ID(userid or group) ACCESS(READ)
PERMIT CSFKYT  CLASS(CSFSERV) ID(userid or group) ACCESS(READ)
PERMIT CSFKYT2 CLASS(CSFSERV) ID(userid or group) ACCESS(READ)
PERMIT CSFPCI  CLASS(CSFSERV) ID(userid or group) ACCESS(READ)
PERMIT CSFPKRC CLASS(CSFSERV) ID(userid or group) ACCESS(READ)
PERMIT CSFPKRW CLASS(CSFSERV) ID(userid or group) ACCESS(READ)
PERMIT CSFPKI CLASS(CSFSERV) ID(userid or group) ACCESS(READ)
SETROPTS RACLIST(CSFSERV) REFRESH
```

To protect module CSFTTKE from unauthorized users, you must protect it using RACF. For more information, refer to *z/OS Security Server RACF Security Administrator's Guide* and *z/OS Security Server RACF System Programmer's Guide*.

See *z/OS Security Server RACF Command Language Reference* for the correct command syntax. You might need to work with your security administrator, because these RACF commands are not available to the general user.

This example permits the user ID or group assigned to the CSFTTCP started task to the CSFTTKE profile in the FACILITY class:

```
SETR CLASSACT(FACILITY)
SETR RACLIST(FACILITY)
RDEFINE FACILITY CSFTTKE UACC(NONE)
PERMIT CSFTTKE CLASS(FACILITY) ID(userid or group) ACCESS(READ)
SETROPTS RACLIST(FACILITY) REFRESH
```

Figure 10. Assign a user ID to CSFTTKE in FACILITY class

The module (CSFTTKE) must also be protected, using the APPL class to control which users can use the application when they enter the system.

This example assigns a user ID or group to the CSFTTKE profile in the APPL class:

```
SETR CLASSACT(APPL)
SETR RACLIST(APPL)
RDEFINE APPL CSFTTKE UACC(NONE)
PERMIT CSFTTKE CLASS(APPL) ID(userid or group) ACCESS(READ)
SETROPTS RACLIST(APPL) REFRESH
```

Figure 11. Assign a User ID to CSFTTKE in APPL Class

Note: The user IDs or groups of user IDs must be permitted to use the TKE workstation.

If you do not have a generic user ID associated to all started procedures, you can associate a user ID to the CSFTTCP proc by issuing a RACF RDEFINE command. For more information, see *z/OS Security Server RACF Security Administrator's Guide*.

Note: The RACF user ID associated with the CSFTTCP proc must have a valid OMVS segment.

This example assigns a user ID or group to the started task CSFTTCP:

```
SETR CLASSACT(STARTED)
SETR RACLIST(STARTED)
RDEFINE STARTED CSFTTCP.CSFTTCP STDATA(USER(userid))
SETROPTS RACLIST(STARTED) REFRESH
```

Figure 12. Assign a user ID to a started task

3. The TKE Host Transaction program must be started before you can logon to the host from TKE. A sample startup procedure is shipped in SYS1.SAMPLIB(CSFTTCP) and included here. Copy this procedure to your proclib data set and customize it for your installation.

```
//CSFTTCP  PROC LEVEL=CSF,MEMBER=CSFTHTP3,
//            CPARM='PORT;50003;SET DISPLAY LEVEL;TRACE ALL'
//CLIST    EXEC PGM= IKJEFT01,
//            PARM='EX ''&LEVEL..SCSFCLI0(&MEMBER)'' ''&CPARM'' EXEC'
//STEPLIB   DD DSN=EZA.SEZALINK,DISP=SHR
//SYSABEND  DD SYSOUT=*
//SYSPRINT  DD SYSOUT=*
//SYSEXEC   DD DSN=&LEVEL..SCSFCLI0,DISP=SHR
//SYSPROC   DD DSN=&LEVEL..SCSFCLI0,DISP=SHR
//SYSTSPRT  DD SYSOUT=*
//SYSTSIN   DD DUMMY
//TKEPARMS  DD DSN=&LEVEL..SAMPLIB(CSFTPRM),DISP=SHR
//*
//* customize the DSN to be the TCP/IP data set on your system
//*
//*SYSTCPD   DD DSN=TCPIP.SEZAINST(TCPDATA),DISP=SHR
//         PEND CSFTTCP
//* --------------------------------------------------------------------
```

Figure 13. Sample startup procedure

TKE startup parameters

Startup parameters may be passed to the TKE Host Transaction Program in a JCL parm field (CPARM) or in a data set referenced in the TKEPARMS DD statement. Parameters specified on the CPARM field override the parameters in the TKEPARMS data set. A sample TKEPARMS data set is shipped in SYS1.SAMPLIB(CSFTPRM).

These parameters are allowed:

- SET THE TKE DATA SETS;CM data set name

  The CM data set will contain the crypto module descriptions, domain descriptions, and authority information for a host. If the data set name does not exist, TKE will automatically create it on the host the first time you send updates to it. If you do not specify a CM data set name, TKE uses a default data set name of 'smfid.TKECM'.

  Note: A fully qualified data set name may not be specified on the CPARM field. Use the TKEPARMS to set the fully qualified TKECM data set name.

  Here are some examples:

  – Example 1: SET THE TKE DATA SETS;TKECM

    TKE will use data set name 'generic_id.TKECM'. The generic_id is the user ID assigned to the STARTED class for this proc.

  – Example 2: SET THE TKE DATA SETS;'TKEV3.TKECM'

    TKE will use data set name 'TKEV3.TKECM'.

- SET DISPLAY LEVEL;trace level

  This parameter sets the amount of trace information that is written to the job log of the started proc. The valid options are:

  – TRANSACTION TRACE - Logs HTP input and output transaction data

  – TRACE ALL - logs all HTP activities, including all TCP/IP verb return codes and information, input and output transaction data, and ICSF input and output data

  – TRACE NON-ZERO - Logs TCP/IP verbs with non-zero return codes only (this is the default if display level is not specified)

- PORT;port number

  This parameter defines the TCP/IP application port number that the started proc will use. This port number should be reserved in your TCP/IP profile for CSFTTCP to prevent other applications from using this port. This port number must be specified at the TKE workstation when defining a host (see “TKE TCP/IP setup” on page 73).

If a port number is not specified, a default port of 50003 will be used. However, if port 50003 is not reserved in your TCP/IP profile, another application may use it and the TKE HTP will fail.

For example: PORT;1000

SYSTCPD is optional but, depending on your TCP/IP installation, may be needed.

You may choose between implicit and explicit allocation.

- Implicit - The name of the configuration data set is constructed at run time, based on rules implemented in the components of TCP/IP. Once a data set name is constructed, TCP/IP uses the dynamic allocation services of z/OS to allocate the configuration data set.
- Explicit - TCP/IP searches for a specific DD name allocation for some configuration data sets. If you allocated a DD name with a DD statement in the JCL used to start a TCP/IP component, TCP/IP will read its configuration data from that allocation. It will not construct a configuration data set name for dynamic allocation.

4. Start the TKE server from the z/OS system console:

```
S CSFTTCP
```

Figure 14. Start the TKE server

Note: If you encounter problems during the start of CSFTTCP, the documented Errortype and Reason Codes are located within the REXX clist CSFTHTP3.

Cancel the TKE server

To cancel the TKE server:

```
S CSFTCTCP
```

Or

```
STOP CSFTTCP
```

Figure 15. Cancel the TKE server

A sample procedure CSFTCTCP is shipped in SYS1.SAMPLIB(CSFTCTCP). You must copy this procedure to your proclib data set and customize it with the port number reserved for the TKE HTP server. If a port number is not specified, it defaults to 50003.

Note: Depending on your system setup, you might have to define the CSFTCTCP task to the RACF STARTED class:

```
REDEFINE STARTED CSFTCTCP.CSFTCTCP STDATA(USER(userid))
SETROPTS RACLIST(STARTED) REFRESH
```

TKE workstation setup and customization

This topic describes several tasks that are necessary preparation for operating your TKE workstation.

The IBM CE installs the TKE cryptographic adapter into your TKE workstation and then powers it up.

Note: When using a KVM switching unit, the TKE windows might appear to be distorted. The TKE should be initialized while it is connected directly to the LCD monitor. After initial boot up on the LCD monitor, the TKE can be connected to the KVM switching unit.

Important: For reliable TKE operation, the customer must ensure an installation area ambient temperature in the range of 10 degrees Celsius to 40 degrees Celsius, plus or minus 5 degrees Celsius.

For TKE storage, the customer must ensure an installation area ambient temperature in the range of 1 degree Celsius to 60 degrees Celsius, plus or minus 5 degrees Celsius. In addition, the ambient relative humidity must not exceed 80 percent.

Most of the workstation setup and customization tasks require you to be signed on to TKE in privileged mode with the ADMIN user name. When TKE is initially started, you are not signed on to TKE in privileged mode. The following steps are used to sign on to TKE in privileged mode.

- Close the **Trusted Key Entry Console**.
- From the **Welcome to the Trusted Key Entry Console** screen select **Privileged Mode Access**.
- From the **Trusted Key Entry Console Logon** screen enter the user name ADMIN and the password PASSWORD.
- Click Logon.

You can determine whether you are signed on to the TKE in privileged mode by looking at the upper-right corner of the TKE console. When you are signed on in privileged mode, the ID is listed in the area.



Figure 16. Login with ADMIN user name

The TKE Workstation Setup wizard

Beginning in TKE 7.3, the TKE workstation includes the TKE Workstation Setup wizard. This wizard takes you through the process of performing the final configuration of your TKE workstation. The wizard tests for critical settings and ensures that the TKE workstation is set up correctly. After the workstation is set up, you can run the wizard at any time to check the TKE workstation or to make changes to it.

Guideline: Use the TKE Workstation Setup wizard to finish your workstation configuration.

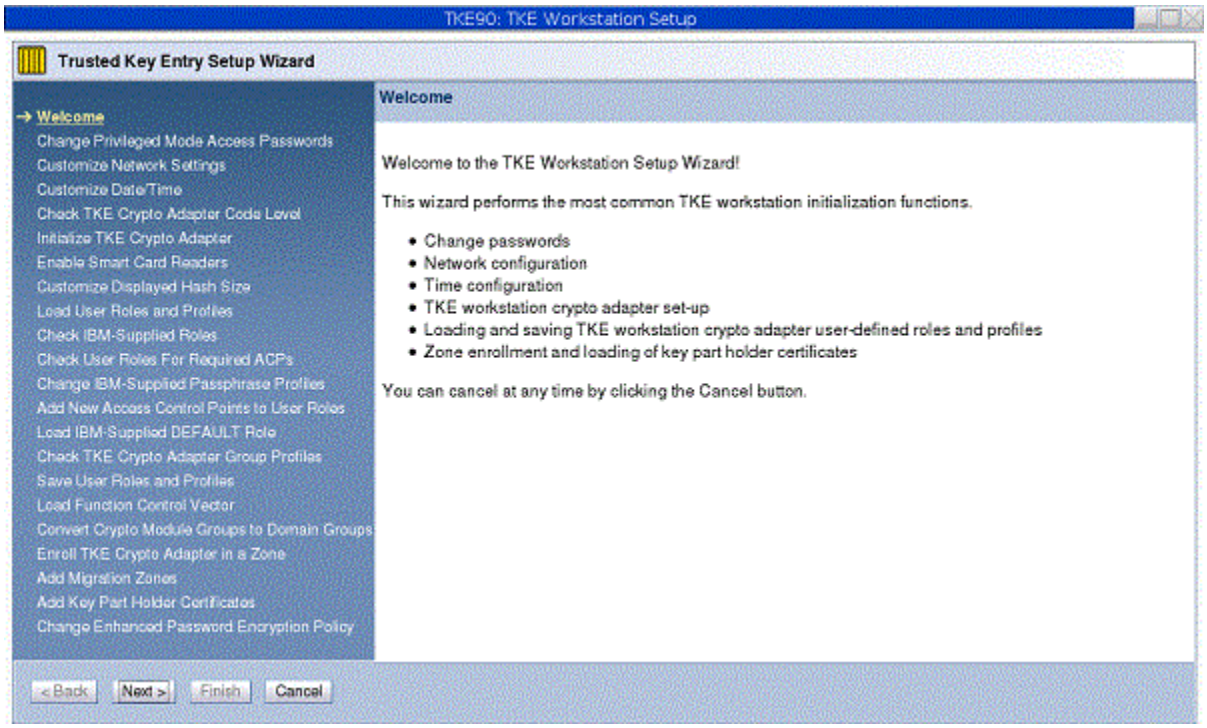


*Figure 17. The TKE Workstation Setup wizard **Welcome** window.*

Overview of the TKE Workstation Setup wizard

The TKE Workstation Setup wizard takes you through a series of workstation setup tasks. Perform the tasks in the order in which they are presented. Some conditions are required for the TKE workstation to work correctly. The wizard tests for these conditions and takes you through the process of making the necessary changes.

The wizard tasks fall into five categories:

- Basic Workstation Tasks

  These tasks start workstation configuration utilities. The wizard does not attempt to make any recommendations for these tasks. It is up to you to decide whether you want to perform these tasks. The following tasks are in this category:

  – Customize network settings. (For more information about this task, see "Customize network settings" on page 81, which describes how to perform this task if you do not use the Workstation Setup wizard.)

  – Customize date and time. (For more information about this task, see "Customize console date and time" on page 83, which describes how to perform this task if you do not use the Workstation Setup wizard.)

- Critical tasks

  These tasks check for conditions that are required for the TKE workstation to work correctly. If the wizard determines that the TKE workstation is not set up correctly, it issues a message that states the situation and suggests an action. When you click **Next**, the wizard performs the action. The following tasks are in this category:

  – Check the TKE crypto adapter code level

  – Load the function control vector

- Important tasks

  These tasks check for conditions that might limit the functionality of the TKE workstation. If the wizard task determines that the TKE workstation is not set up correctly, it issues a message that states the situation and suggests an action. When you click **Next**, the wizard performs the action. The following tasks are in this category:

  – Initialize the TKE crypto adapter.

  – Load user roles and profiles. For more information about this task, see "Wizard tasks to load and save customer-defined roles and profiles" on page 80.

  – Check system-supplied roles.

  – Check TKE crypto adapter group profiles.

  – Change enhanced password encryption policy.

  – Check user roles for required ACPs.

  – Add new access control points to user roles.

  – Convert crypto module groups, if present, to domain groups.

- Secure workstation tasks

  These tasks change default settings for system-supplied items. The wizard can test for the need to reload the DEFAULT role. You decide whether you want to perform the change password tasks. The following tasks are in this category:

  – Change privileged mode access passwords.

  – Change system-supplied profile passwords.

  – Load the system-supplied DEFAULT role.

- Customer preference tasks

These tasks configure optional features of the TKE workstation. You decide whether you want to perform these tasks. The following tasks are in this category:

- Enable smart card readers.
- Customize displayed hash size.
- Save user roles and profiles. For more information about this task, see "Wizard tasks to load and save customer-defined roles and profiles" on page 80.
- Enroll the TKE crypto adapter in a zone.
- Add migration zones.
- Add key part holder certificates.

Wizard tasks to load and save customer-defined roles and profiles

There are two wizard tasks that deal with customer-defined roles and profiles;

- Save user roles and profiles
- Load user roles and profiles

These two tasks work together to simplify the process of backing up, migrating, and loading customer-defined roles and profiles onto a TKE workstation local crypto adapter.

The save user roles and profiles wizard task performs the following tasks:

- It determines whether there are any customer-defined roles or profiles on the TKE workstation's local crypto adapter.
- If it finds customer-defined roles or profiles, it creates files that contain information that allows the load user roles and profiles wizard task to load the roles and profiles.

Notes:

- Role and profile information is kept in different files.
- The files are saved in the TKE Data Directory.
- The files can be left on the TKE workstation for recovery purposes, or moved to another TKE workstation for migration purposes.
- The save and load user roles and profiles tasks can also be run from the Access Control menu in the Cryptographic Node Management utility (CNM).

The load user roles and profiles wizard task performs the following tasks:

- It determines whether either of the files that are created by the save user roles and profiles wizard task is on the system.
- Depending on which files are found, all the roles, or profiles, or both, are loaded onto the TKE workstation's local adapter.

Note: When a passphrase profile is loaded, you must assign a new password to the profile. This password does not have to match the password that the profile had at the time the profile was saved.

Restriction: The load user roles and profiles wizard task requires data from the save user roles and profiles wizard task. Therefore, you can use the load task only when the roles and profiles come from a system with a minimum release level of TKE 7.3.

Running the TKE Workstation Setup wizard

The TKE Workstation Setup wizard is supported starting with TKE 7.3. To run the TKE Workstation Setup wizard, follow these steps:

1. Close all windows except the pre-logon screen. The pre-logon screen has the title **Welcome to the Trusted Key Entry Console**.
2. Select **Privileged Mode Access**.
3. Enter `admin` for the user ID.

4. Enter the password for the admin user ID. The default password for the admin user ID is `password`.
5. From the **Trusted Key Entry Console**, select **Trusted Key Entry**.
6. Open the **TKE Workstation Setup** wizard.
7. Take all appropriate actions in response to the prompts from the wizard.
8. Click **Finish** when you are done.

Configuring TCP/IP

The TKE Administrator must configure the TKE workstation for TCP/IP. You must be logged on with the ADMIN user name for this task. TCP/IP is configured through the Customize Network Settings task.

Customize network settings

In the left frame of the Trusted Key Entry Console, click on Service Management. In the right frame of the Trusted Key Entry Console, click on Customize Network Settings.

The Customize Network Settings window opens. Its Identification tab is displayed.

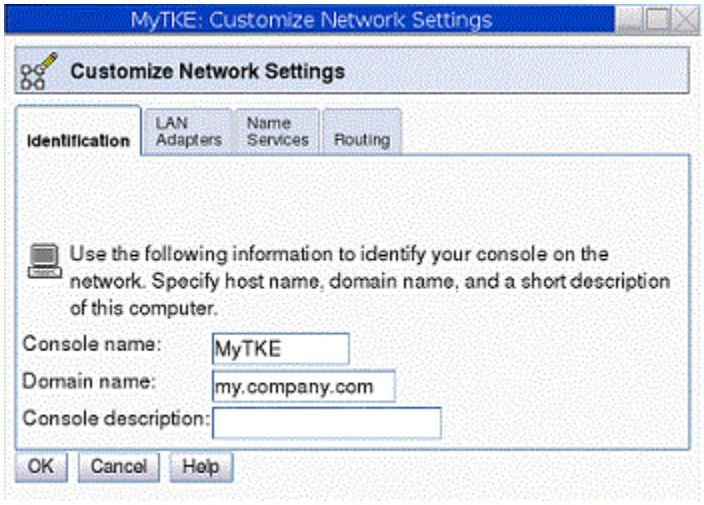


Figure 18. Customize Network Settings - Identification Tab

By default, the Console name is TKE. It is displayed in the title bar of all the window displays. Enter the domain name for your network and a brief description for the workstation. If you do not have any further updates to make, click OK. To continue with updates to your network settings, click on the LAN Adapters Tab.

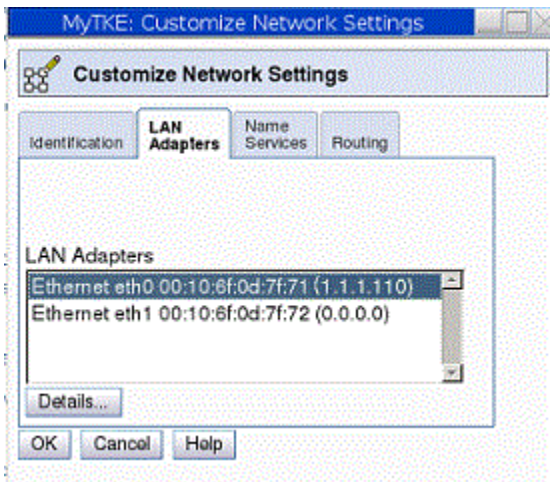


Figure 19. Customize Network Settings LAN Adapters Tab

With the Ethernet LAN adapter highlighted, click on Details.

The LAN Adapter Details window opens.

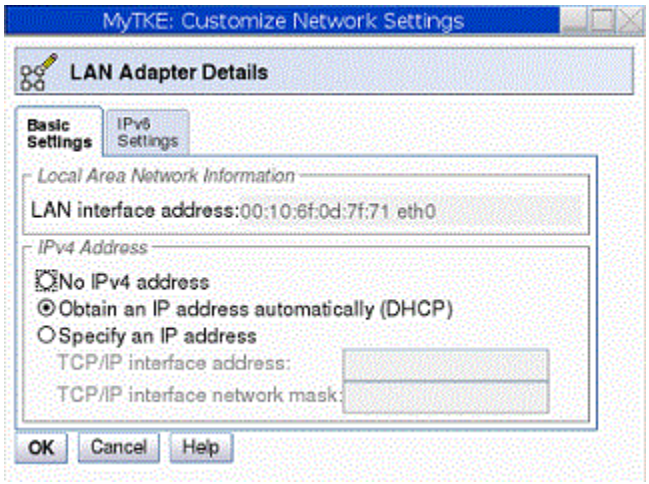


Figure 20. Local Area Network

Specify Local Area Network Information and DHCP Client/IP address information for your network. Press the **OK** push button. If you do not have any further updates to make, click the **OK** push button on the Customize Network Settings Window. To continue with updates to your network settings, click on the Name Services tab.

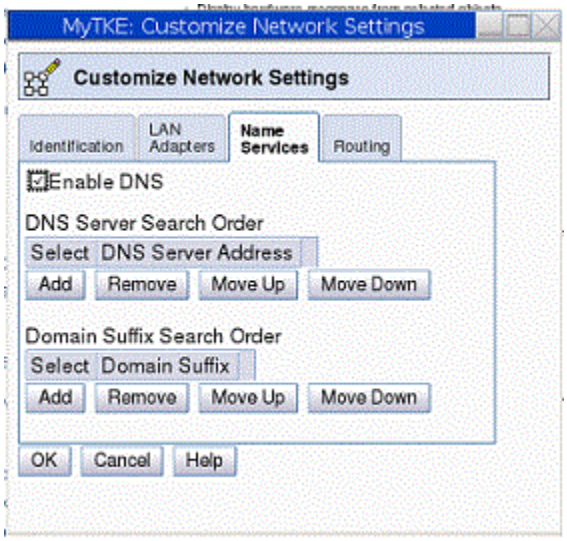


Figure 21. Customize Network Settings - Name Services Tab

Select whether DNS is enabled or disabled. Configure the DNS Server Search Order and the Domain Suffix Search Order for your network. If you do not have any further updates to make, click OK. If Routing information is required for your network, click on the Routing tab and configure as appropriate. When complete, click OK to save all updates to your network settings.

Problems associated with networking can be diagnosed with the Network Diagnostic Information task. To open this task select Service Management, Network Diagnostic Information.

If you are having problems connecting to a host system, test the TCP/IP connection by pinging the address. Enter the host address in the TCP/IP Address to Ping field and click on Ping.

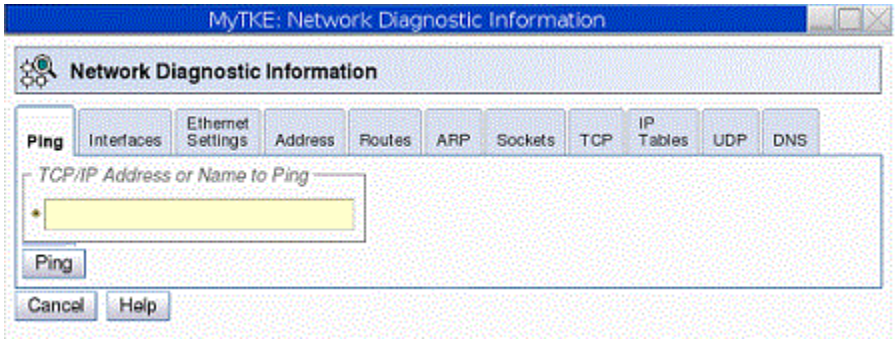


Figure 22. Network Diagnostic Information Task

Customize console date and time

To set the system clock on your workstation, open the Customize Console Date/Time task under Service Management. You must be logged on with the ADMIN user name for this task.

Setting the assigned time for your system manually

If you have selected **None** as your time source, specify the new time using the same format as shown in the Time field. For example,

```
09:35:00 AM
```

Setting the assigned date for your system

Specify the new date using the same format as shown in the Date field. For example,

```
September 10, 2005
```

If you have chosen the **None** time source, choose a city from the list that has the same time zone as the one you need. Click **OK** when finished.

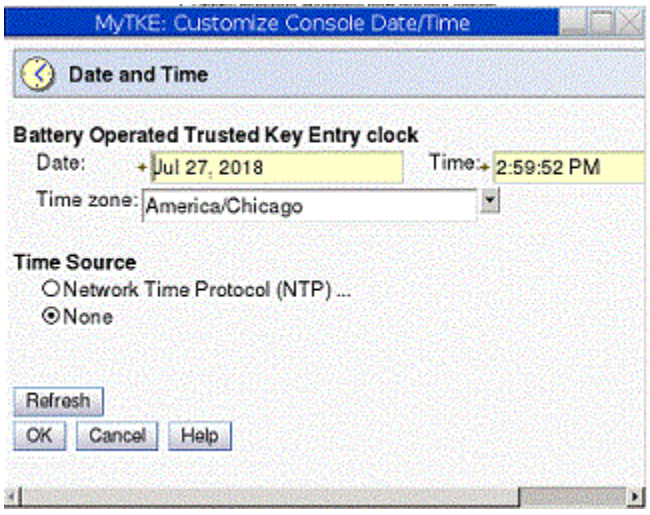


Figure 23. Customize Console Date and Time Window

Setting the assigned time for your system - NTP

If you have chosen the **Network Time Protocol (NTP)** time source option, a list of your available NTP servers will be displayed.

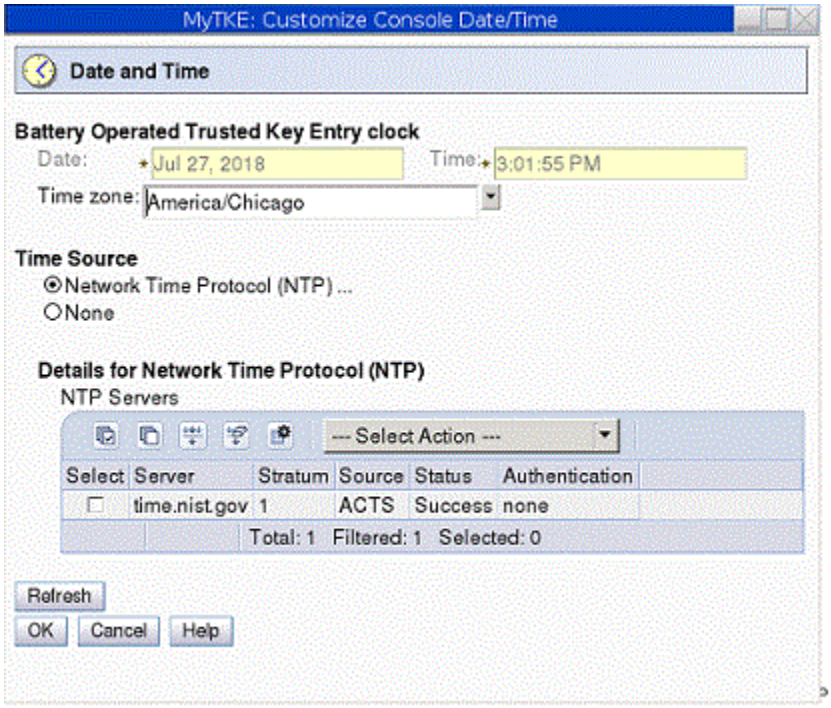


Figure 24. Configure NTP settings

To add an NTP server, choose **Select Action** from the drop down menu and then select **Add Server** option.

The Add Network Time Server dialog opens.

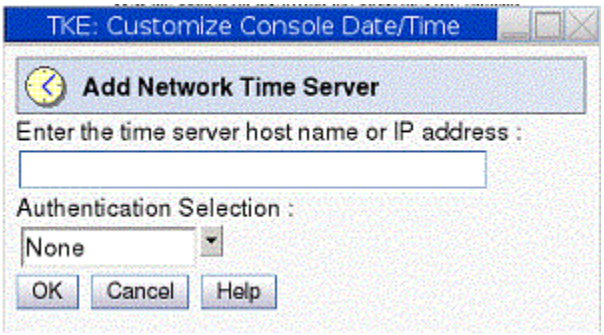


Figure 25. Add Network Time Server

Enter the NTP server host name or IP address, choose an appropriate Authentication Selection, and click **OK**.

Initializing the TKE workstation crypto adapter

The TKE workstation crypto adapter only needs to be initialized when:

- This is a first time setup for a TKE workstation.
- You want to zeroize the TKE workstation crypto adapter and start over.

The TKE workstation crypto adapter needs to be initialized before it can be used for cryptographic functions. You must be logged on with the ADMIN user name for this task.

You need to decide whether to use passphrase or smart card authentication. For simplicity, we recommend that you do not use a mix of authentication methods.

Initialize the TKE workstation crypto adapter using TKE's Crypto Adapter Initialization and Cryptographic Node Management Utility.

- If you are initializing using passphrase, see "Initializing the TKE workstation crypto adapter for use with passphrase profiles" on page 85.
- If you are initializing using smart cards, see "Initializing the TKE workstation crypto adapter for use with smart card profiles" on page 85.

Initializing the TKE workstation crypto adapter for use with passphrase profiles

Guideline: The TKE Workstation Setup wizard has a task that takes you through initializing the crypto adapter. If you want to initialize the adapter, use the wizard to do the initialization. For more information, see "The TKE Workstation Setup wizard" on page 78.

To initialize the TKE workstation crypto adapter for use with passphrase profiles:

1. Open the Trusted Key Entry window pane of the Trusted Key Entry Console.
2. From the Applications list, open the TKE Crypto Adapter Initialization application.

   The initialization script will be run inside of a script window. There are several messages you must reply to as the script runs:

   - A warning indicates that the action will delete any existing data on the card, and you are asked if you want to continue. Select **Y** if you want to continue.
   - A message asks if you want to initialize the adapter for use with passphrase or smart card profiles. Select **P** for passphrase profiles.
3. After the script has completed, you can review status messages that show what initialization actions were performed. After you have reviewed the data, press the **ENTER** key to close the script window.

The TKE workstation crypto adapter is initialized with the roles and profiles required for the passphrase environment. The times on the TKE workstation and the crypto adapter are synchronized. The crypto adapter master keys are set to random values, and DES, PKA, and AES key storages are initialized.

Initializing the TKE workstation crypto adapter for use with smart card profiles

To initialize the TKE workstation crypto adapter for use with smart card profiles:

1. Open the Trusted Key Entry window pane of the Trusted Key Entry Console.
2. From the Applications list, open the TKE Crypto Adapter Initialization application.

   The initialization script will be run inside of a script window. There are several messages you must reply to as the script runs:

   - A warning indicates that the action will delete any existing data on the card, and you are asked if you want to continue. Select **Y** if you want to continue.
   - A message asks if you want to initialize the TKE's adapter for use with passphrase or smart card profiles. Select **S** for smart card profiles.
3. After the script has completed, you can review status messages that show what initialization actions were performed. After you have reviewed the data, press the **ENTER** key to close the script window.

The TKE workstation crypto adapter is initialized with the roles required for the smart card environment. The times on the TKE workstation and the crypto adapter are synchronized. The crypto adapter master keys are set to random values, and DES, PKA, and AES key storages are initialized.

TKE workstation crypto adapter post-initialization tasks

After the TKE workstation adapter is initialized, you may need or want to do the following tasks:

- Verify that Function Control Vector (FCV) has been loaded onto the TKE workstation crypto adapter. The adapter is shipped with the FCV installed. The initialization script does not remove the FCV from the adapter. However, if the FCV was cleared by an administrator or was not properly installed, the TKE will

not function properly. Taking the time to verify the FCV is present is highly recommended and taking corrective action if it is not installed is mandatory.

- Change the passwords for the system-supplied passphrase profiles that were created on the adapter. We strongly recommend you perform this task.
- Load previously created user defined Roles and Profiles from role and profile definition files.
- Create new user defined Roles and Profiles.
- Load known master keys rather than use the random keys that were generated.
- Redefine the DEFAULT role if the TKE workstation crypto adapter was initialized for use with smart card profiles. We strongly recommend you perform this task.
- Add new ACPs to existing roles using the Add Access Control Points utility.
- Enroll the TKE workstation crypto adapter in a zone.
- Add migration zones.
- Configure 3270 emulators.

Verifying that the function control vector (FCV) has been loaded

Guideline: The TKE Workstation Setup wizard has a task for testing and loading the FCV. Use the wizard to test and update your workstation. For more information, see "The TKE Workstation Setup wizard" on page 78.

The TKE workstation crypto adapter function control vector governs what cryptographic services can be used on the adapter. If the FCV is not loaded, you will not have access to any cryptographic function. You can use the following steps to verify that the FCV is loaded:

1. Open the Trusted Key Entry window pane of the Trusted Key Entry Console.
2. From the Applications list, open the Cryptographic Node Management (CNM) Utility.
3. The CNM utility will prompt for a profile. Select TKEADM or equivalent profile.
4. From the main CCA Node Management Utility screen, select the **Crypto Node –> Status** pull-down.
5. From the CCA Node Management Utility – CCA Application Status screen, press the **Export Control** push button.

   The FCV is properly set when:

   - The maximum modulus size is 4096.
   - All values except CDMF are available.

   If the maximum modulus size is 0 and all other values are "not available", you must reload the FCV.
6. Press the **Cancel** push button to return to the main CCA Node Management Utility screen.
7. Exit and logoff the CNM utility.

Reloading the function control vector

This task is only necessary if you determined the FCV is not currently loaded on the TKE workstation crypto adapter.

To reload the Function Control Vector:

1. Open the Trusted Key Entry window pane of the Trusted Key Entry Console.
2. From the Applications list, open the Cryptographic Node Management (CNM) Utility.
3. The CNM utility will prompt for a profile. Select TKEADM or equivalent profile.
4. From the main CCA Node Management Utility screen, select **Crypto Node –> Authorization –> Load** off the pull-down menu.
5. Find the file named fcv_4tke80.crt and highlight it.
6. Press the **open** push button.

7. When prompted, press **yes** to confirm you want to load the FCV.
8. An "authorizations have been loaded" message window displays. Press **OK** to close this window.

   Note: If you are unable to load the FCV, contact your service representative.
9. Exit and logoff the CNM utility.

Changing the passwords for system-supplied passphrase profiles created on the TKE workstation crypto adapter

Guideline: The TKE Workstation Setup wizard has a task that tests to see if there are any system-supplied passphrase profiles on the TKE workstation's local adapter. If there are, you can use the task to change their passwords. If you decide you are going to change system-supplied profile passwords, use the wizard to change them. For more information, see "The TKE Workstation Setup wizard" on page 78.

When the TKE workstation crypto adapter was initialized for use with passphrase profiles, system-supplied profiles were created with passphrases that match their profile names. The profiles are:

- TKEADM
- TKEUSER
- KEYMAN1
- KEYMAN2

You should change the passwords for all of these profiles. The following steps can be used to change the profile passwords:

1. Open the Trusted Key Entry window pane of the Trusted Key Entry Console.
2. From the Applications list, open the Cryptographic Node Management (CNM) Utility.
3. The CNM utility will prompt for a profile. Select TKEADM or equivalent profile.
4. From the main CCA Node Management Utility screen, select **Access Control –> Profiles** off the pull-down menu.
5. Highlight the profile to be changed and press the **edit** push button.
6. Enter the **passphrase** and **confirm passphrase** values.
7. Press the **change passphrase** push button to make the change.
8. Press **OK** on the "passphrase changed" message.
9. Repeat the process for all the profiles you want to change.
10. When finished, press **done** to return to the main CCA Node Management Utility screen.
11. Exit and logoff the CNM utility.

Loading previously created user-defined roles and profiles from role and profile definition files

Guideline: The TKE Workstation Setup wizard has a task that simplifies the process of loading roles and profiles onto a TKE workstation's local adapter. There are limitations. For more information, "Wizard tasks to load and save customer-defined roles and profiles" on page 80.

If you have user-defined role and profile definition files and you want to install the roles and profiles on the TKE workstation crypto adapter, see the following topics for installation instructions:

- To load roles on the adapter, see "Opening a role definition file" on page 267 and "Making changes to a role or role definition file" on page 268.
- To load profile on the adapter, see "Opening a profile definition file" on page 257 and "Making changes to a profile or profile definition file" on page 258.

For more information about role and profile definition files, see "TKE workstation crypto adapter roles and profiles" on page 16.

Creating new user-defined roles and profiles

If you want to create new user defined roles and profiles (including group profiles), see “Managing roles” on page 264 and “Managing profiles” on page 254. For more information about role and profile definition files, see “TKE workstation crypto adapter roles and profiles” on page 16.

Loading a known master key instead of using the randomly generated key

Note: The TKE Workstation Setup wizard does not have a task for this activity.

When the TKE workstation crypto adapter is initialized, new random master key values are loaded. If you want to, you can load a new master key value from clear key parts or a smart card. If you want to load a known master key, see the following sections of this document for installation instructions:

- To load clear key parts, see “Parts — Loading a new master key from clear key parts” on page 273.
- To load smart card key parts, see “Smart card parts — loading master key parts from a smart card” on page 276.

After you load a new master key, you must set the master key and reencipher DES, PKA, or AES key storage. For more information, see “Reenciphering key storage” on page 279.

Note: If you initialized the TKE workstation crypto adapter for use with passphrase profiles, you must log on to the adapter using the profile of:

- KEYMAN1 or equivalent to clear the new master key register and load the first master key part role.
- KEYMAN2 or equivalent to combine master key parts, set the master key, and reencipher key storage.

Redefining the DEFAULT role when the TKE workstation crypto adapter has been initialized for use with smart card profiles

Guideline: The TKE Workstation Setup wizard has a task for testing and loading the DEFAULT role. Use the wizard to test and update your workstation. For more information, see “The TKE Workstation Setup wizard” on page 78.

The DEFAULT role that is created when a TKE workstation crypto adapter is initialized for use with smart card profiles is designed to provide enough authority to perform the initial administration of the adapter. Be aware, however, that the DEFAULT role is a powerful role. After the initial administration is done, you should replace the DEFAULT role with the less powerful DEFAULT role that is created when a TKE workstation crypto adapter is initialized for use with passphrase profiles. To reload the DEFAULT role, follow instructions in “Opening a role definition file” on page 267 and “Making changes to a role or role definition file” on page 268 using the default_81.rol file.

Adding new ACPs to existing roles using the Add Access Control Points utility

Guideline: The TKE Workstation Setup wizard has two tasks that are related to this activity. One task tests and updates system-supplied roles. The other task starts the Add Access Control Points utility for customer-defined roles. Use the wizard to test and update your workstation. For more information, see “The TKE Workstation Setup wizard” on page 78.

Sometimes between TKE releases, new Access Control Points (ACPs) are made available to the roles on the TKE workstation crypto adapter. New ACPs are never automatically added to existing roles during the migration process. For this reason, it might be necessary to add ACPs to existing roles after you upgrade to a new TKE release. Beginning in TKE 7.1, TKE included the Migrate Roles utility to simplify the process of adding new ACPs to existing roles on the TKE workstation crypto adapter. In TKE 9.2, the Migrate Roles utility was renamed the Add Access Control Points utility.

Note: In TKE 7.1,15 individual ACPs were added to control access to TKE applications and some functions within TKE applications. If you migrated roles from an earlier version of TKE to TKE 7.1 or later, review the information in “TKE 7.1 role migration considerations” on page 90.

The Add Access Control Points utility is a graphical user interface that allows you to quickly add new ACPs to existing roles. The utility lists the new ACPs that were added in each release. Using a tree structure

interface, you can quickly select the ACPs you want to add to your roles. After you make your selection, you send the command to make the updates.

Notes:

1. After you initialize your TKE workstation crypto adapter, the system-supplied roles have the correct Access Control Points for the TKE's release level.
2. In TKE 7.1, many ACPs were added to control access to TKE applications. See "TKE 7.1 role migration considerations" on page 90.
3. User-defined roles are normally based off of one of the system-supplied roles. It is highly recommended you view the new ACPs for the base system-supplied roles to help you determine what ACPs you might want to add to your user-defined roles.
4. The ACPs for all of the system-supplied roles are listed in "System-supplied role access control points (ACPs)" on page 23. The tables show what ACPs are new in any given release.

To start the Add Access Control Points utility, you must be signed onto the TKE with the Privileged Mode Access ID of ADMIN.

1. In the left frame of the Trusted Key Entry Console, click **Trusted Key Entry**.
2. In the right frame of the Trusted Key Entry Console, under the Applications list, click **Add Access Control Points Utility**.

   The Add Access Control Points utility starts.

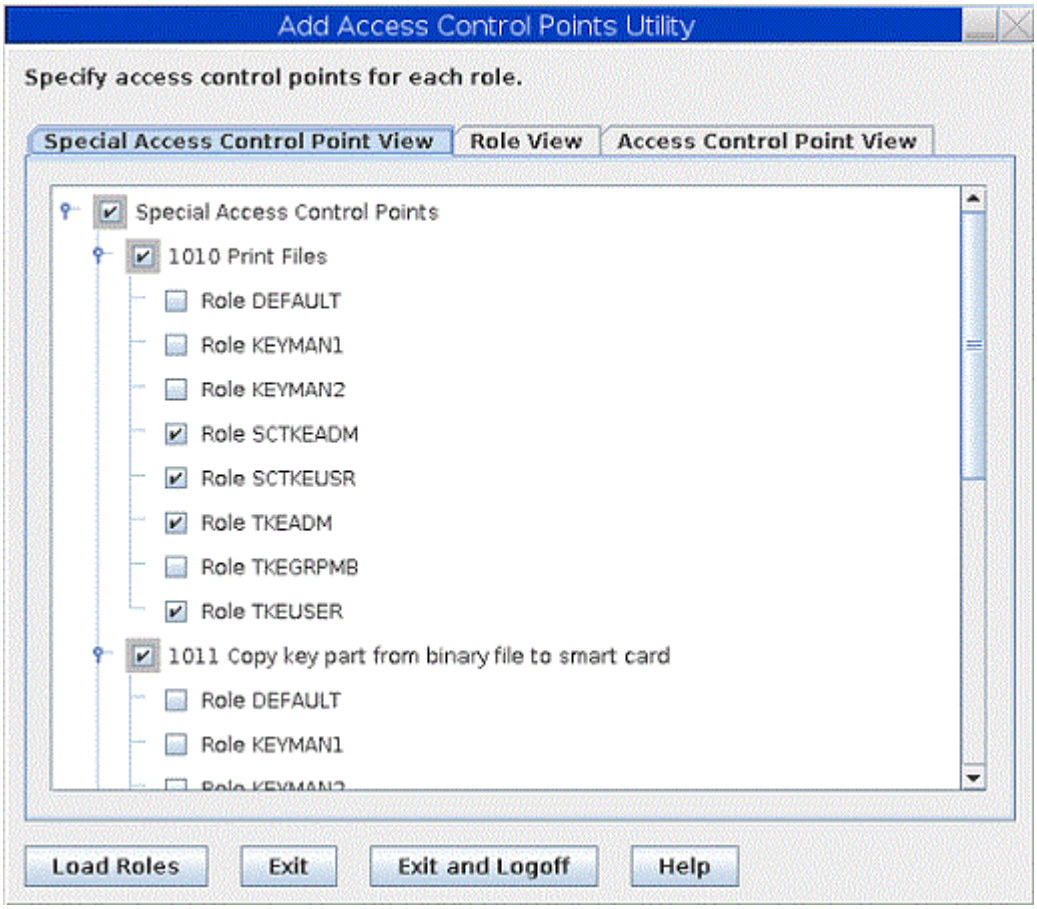


Figure 26. Add Access Control Points utility

The Add Access Control Points utility window has two tabs that provide three different views of the ACPs that can be added.

- In the **Special Access Control Points View**, you can add the print files, copy key part from binary file to smart card, or coordinated change master key and KDS to your roles. These ACPs are special because the are not added to any IBM supplied role and must be manually added to your roles.

- In the **Role View**, each individual Role has every new ACP listed under it. Check boxes under each role are provided to activate or deactivate individual ACPs for that role.
- In the **Access Control Point View**, each individual ACP has every role listed under it. Check boxes under each ACP are provided to activate or deactivate the ACP for individual roles.

To add new ACPs to existing roles:

1. Click on the **Role View** or **Access Control Point View** tab depending on your desired view of the new ACPs.
2. Use the check boxes provided to select which ACPs you want to add to which roles.
3. Press the **Load Roles** push button to add the selected ACPs to the selected roles.

   When the load operation completes, a message box displays a "Role loaded successfully" message. Press the **Close** push button on this message box. The process is complete.

TKE 7.1 role migration considerations

Beginning in TKE 7.1, fifteen individual ACPs were added to control access to TKE applications and some functions within TKE applications. The new TKE 7.1 ACPs were logically put into three groups. The following list shows the ACP groups and their ACP values. The items are listed in the order they appear in the Role View of the Add Access Control Points utility.

Application Logon ACPs

- 1000: Open Begin Zone Remote Enroll Process
- 1001: Open Complete Zone Remote Enroll Process
- 1002: Open Cryptographic Node Management Utility
- 1003: Open Migrate Host Crypto Module Public Configuration Data
- 1004: Open Configuration Migration Tasks
- 1005: Open Smart Card Utility Program
- 1006: Open Trusted Key Entry
- 100D: Open Edit TKE Files
- 100E: Open TKE File Management Utility

Crypto Module Group ACPs

- 100A: Create Crypto Module Group
- 100B: Change Crypto Module Group
- 100C: Delete Crypto Module Group

Domain Group ACPs

- 1007: Create Domain Group
- 1008: Change Domain Group
- 1009: Delete Domain Group

New ACPs are never automatically added to existing roles on a TKE workstation crypto adapter. You must take explicit actions to add the new ACPs to existing roles when:

- The role was created on a TKE workstation before the workstation was upgraded to TKE 7.1 or later.
- The role was created on TKE 7.1 or later from a role definition file that was created on a pre-TKE 7.1 system.

TKE 7.1 role migration considerations for system-supplied roles

If your system-supplied roles were created before your system was upgraded to TKE 7.1 or later, you need to add ACPs to your system-supplied roles. To do this, you must determine which system-supplied roles you have on your TKE workstation. If you initialized your TKE workstation for use with smart card profiles, you need to update the following roles:

- SCTKEUSR
- SCTKEADM

If you initialized your TKE workstation for use with passphrase profiles, you need to update the following roles:

- TKEUSER
- TKEADM
- KEYMAN1
- KEYMAN2

When you have determined which roles you need to update, go into the Crypto Node Management utility and reload the system-supplied roles from the system-supplied role definition files for this release. For instructions on loading system-supplied roles from system-supplied role definition files, see "Managing roles" on page 264.

TKE 7.1 role migration considerations for customer-defined roles

If your customer-defined roles were created before your system was upgraded to TKE 7.1 or later, or your roles were created from role definition files that were created on a TKE that was pre-TKE 7.1, you need to add ACPs to your customer-defined roles. To do this, you must determine which ACPs you want to add to your customer-defined roles. When you have made your choices, use the Add Access Control Points utility (described in "Adding new ACPs to existing roles using the Add Access Control Points utility" on page 88) to manually add the ACPs to each of the customer-defined roles.

The TKE has two pairs of general purpose roles; TKEUSER/SCTKEUSR and TKEADM/SCTKEADM. The TKEUSER and SCTKEUSR roles are designed for users responsible for managing host crypto modules. The TKEADM or SCTKEADM roles are designed for users responsible for managing the TKE workstation. Customer-defined roles should be modeled off of one of these two pairs of roles. The following lists show which new ACPs were added to these general purpose roles. You can use this information to help you decide which ACPs you need to add to your customer-defined roles.

In the TKEUSER and SCTKEUSR roles, the following ACPs were added:

- Application Logon ACPs
  - 1003: Open Migrate Host Crypto Module Public Configuration Data
  - 1004: Open Configuration Migration Tasks
  - 1005: Open Smart Card Utility Program
  - 1006: Open Trusted Key Entry
  - 100D: Open Edit TKE Files
  - 100E: Open TKE File Management Utility
- Crypto Module Group ACPs
  - 100A: Create Crypto Module Group
  - 100B: Change Crypto Module Group
  - 100C: Delete Crypto Module Group
- Domain Group ACPs
  - 1007: Create Domain Group
  - 1008: Change Domain Group
  - 1009: Delete Domain Group

In the TKEADM and SCTKEADM role:s, the following ACPs were added:

- Application Logon ACPs
  - 1000: Open Begin Zone Remote Enroll Process
  - 1001: Complete Zone Remote Enroll Process

- 1002: Open Cryptographic Node Management Utility
- 1005: Open Smart Card Utility Program
- 100D: Open Edit TKE Files
- 100E: Open TKE File Management Utility

TKE 7.3 role migration considerations for customer-defined roles

In TKE 7.3, an ACP was added to control the ability to manage a host entry. The new ACP is:

- 100F: Manage Host List

You must have this ACP to be able to create, delete, or change a host entry. The ACP was added to the system-supplied roles TKEUSER and SCTKEUSR. If you have any customer-defined roles that are modeled after these roles, you might want to add this ACP to them.

TKE 8.0 role migration considerations for customer-defined roles

In TKE 8.0, an ACP was added for shipping print support. The new ACP is:

- 1010: Print Files

You must have this ACP to be able to print a file on the TKE workstation. The ACP has not been added to any system-supplied roles for security reasons.

TKE 8.1 role migration considerations for customer-defined roles

Two ACPs were added in TKE 8.1 to control access to new functions in TKE 8.1:

- 1011: Copy binary file key part to smart card.
- 1012: Coordinated change master key and KDS.

The first function allows you to copy a key part stored in a binary file to a smart card. The second function allows you to invoke from the TKE workstation an ICSF function that coordinates the setting of one or more master keys with the updating of key storage on a host system.

These ACPs have not been added to any system-supplied roles. To use the new functions, you must add the new ACPs to the TKE roles you plan to use when performing the new functions.

TKE 9.0 role migration considerations for customer-defined roles

One ACP was added in TKE 9.0 to control access to new functions in TKE 9.0. This ACP should be added to the role TKEUSER, SCTKEUSR, or any role that is equivalent to these IBM-supplied roles:

0023
Compute CMACZERO Verification Pattern for DES.

TKE 9.2 role migration considerations for customer-defined roles

One ACP was added in TKE 9.2 to control access to new functions in TKE 9.2. This ACP should be added to the role TKEUSER, SCTKEUSR, or any role that is equivalent to these IBM-supplied roles:

0022
Compute CMACZERO Verification Pattern for AES.

Customize the TKE application

Note: The TKE Workstation Setup wizard does not have a task for this activity.

1. Open the TKE application by clicking on Trusted Key Entry and then clicking on Trusted Key Entry 9.0.
2. Logon to the TKE workstation crypto adapter. See Workstation Logon: Passphrase or Smart Card on “Crypto adapter logon: passphrase or smart card” on page 97 for details.
3. Click on Preferences on the task bar.
4. Enable/Disable the Preferences as appropriate. See “TKE customization” on page 134 for details.

Configure 3270 emulators

Note: The TKE Workstation Setup wizard does not have a task for this activity.

A z/OS session is required on the host for several tasks executed on TKE to complete. If you do not have access to the z/OS system outside of the TKE Workstation, create access to the z/OS system on the TKE by configuring a 3270 emulator session.

To configure a 3270 emulator session, click Service Management and then click **Configure 3270 Emulators**.

The Configure 3270 Emulators window is displayed.

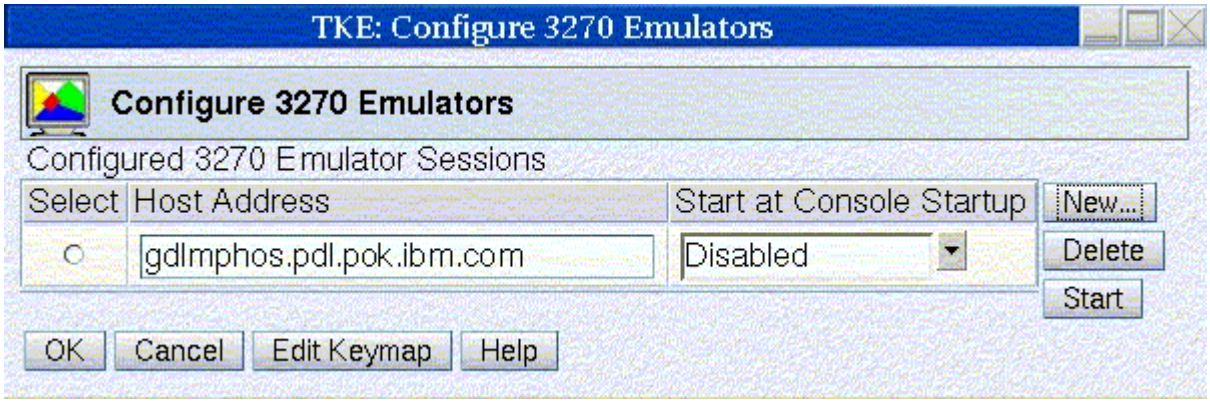


Figure 27. Configure 3270 Emulators

1. Click **New** to add a 3270 session.
2. The Add 3270 Emulator Session window is displayed.
3. Enter the Host Address you would like to connect to.
4. Select Enabled or Disabled from the Start at Console Startup drop down menu.

   Enabled
   When the console starts this session also starts.

   Disabled
   When the console starts this session does not start.



Figure 28. Add 3270 Emulator Session

5. To save the emulator session definition click **OK**.
6. On the Configure 3270 Emulators window click **OK** to save the session. Click **Cancel** to end without saving the session.



Figure 29. Start or Delete a 3270 Emulator Session

7. To start or delete a host address select the host address from the list and click **Start** or **Delete**.

If you click **Edit Keymap**, you can edit the keymap in the 3270 emulator session. You can customize the keyboard functions while in a 3270 session.

Using an TLS (SSL) 3270 emulation session

To use an TLS (SSL) 3270 emulation session, you must perform the following tasks:

1. Configure the TKE workstation to use TLS for 3270 emulation. For instructions, see "Configuring the TKE workstation to use TLS (SSL) for 3270 emulation" on page 94
2. Add a 3270 emulation session. See "Adding a 3270 emulator session" on page 95.

Configuring the TKE workstation to use TLS (SSL) for 3270 emulation

You must import the certificate for the session. Use the following procedure:

1. Sign on to the TKE workstation in Privileged Mode Access with the ADMIN profile.
2. From the Trusted Key Entry Console, click **Service Management**.
3. Under **Configuration**, open the "Certificate Management " application.
4. Click **Import > From Remote Server**.



Figure 30. Manage trusted signing certificates

The following window opens:

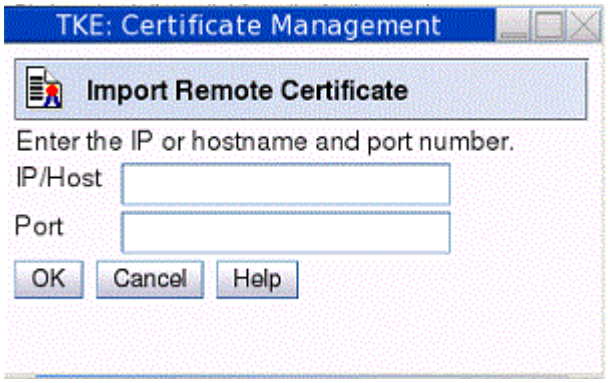


Figure 31. Import remote certificate

5. Enter the information about the certificate's location and click **OK**. For example, specify the host's TLS IP address and port to get the host certificate that is presented during the TLS handshake. A confirmation window opens:

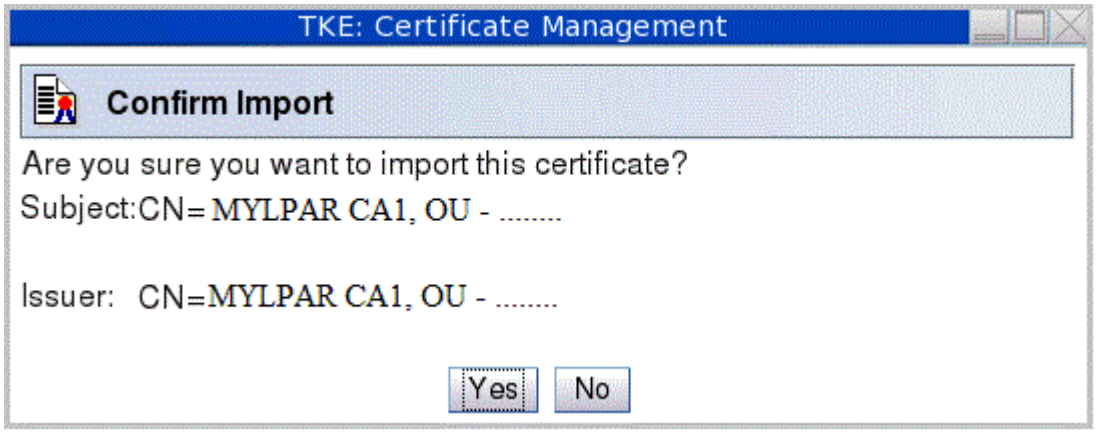


Figure 32. Confirm import

6. Click **Yes** to import the certificate. The imported certificate is now in the list of certificates.

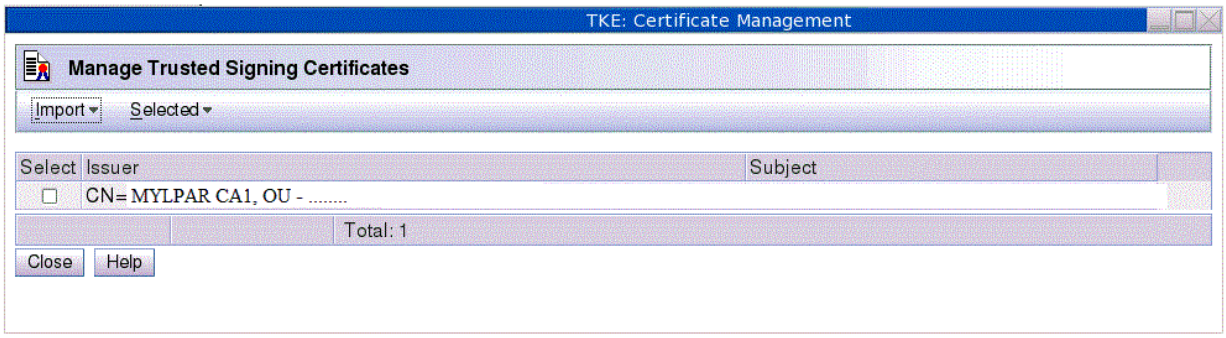


Figure 33. Manage trusted signing certificates

7. Close the Certificate Management utility.
8. Close your Privileged Mode Access session.

Adding a 3270 emulator session

1. From the Trusted Key Entry Console, click **Service Management**.
2. Under **Configuration**, click **Configure 3270 Emulators**. The following window opens:

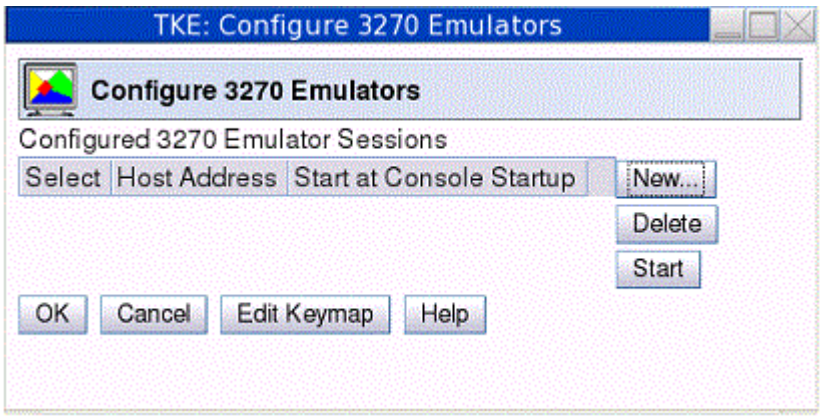


Figure 34. Configure 3270 emulators

3. Click New. A window opens in which you can enter the host address and initial state of the emulator session.
4. Specify the host address in the form L:*IP address or DNS name*:*port nmber* and click **OK**. For example:

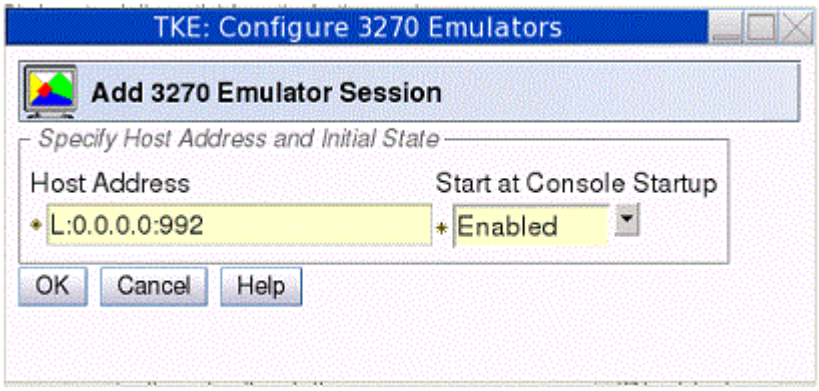


Figure 35. Add 3270 emulator session

5. The emulator session is now listed as a configured 3270 emulator session. To initiate a new emulator session, select it from the list of configured sessions and click **Start**. In the following example, the emulator session is started every time that the TKE console is started.

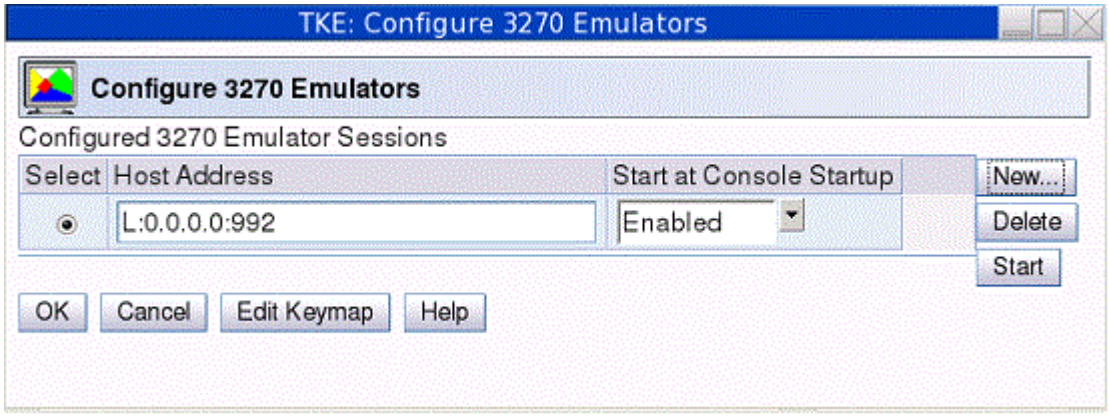


Figure 36. Configure 3270 emulators: Start at console startup

Chapter 5. TKE up and running

The Trusted Key Entry console displays the applications and utilities available on the TKE workstation. When you open a TKE application or utility, you must sign on with a profile that is on the TKE workstation crypto adapter. The individual or group profile you choose must have enough authority to do the functions performed by the application or utility.

Crypto adapter logon: passphrase or smart card

When you start any TKE application, you are presented a list of profiles that are allowed to start the application. Depending on how you initialized the TKE workstation crypto adapter and set up the TKE workstation crypto adapter profiles, you may have passphrase, smart card, or group profiles presented when you open an application. If you open a TKE application and the list of available profiles is empty, this may mean that you need to initialize your TKE workstation crypto adapter, or create and load profiles. For instructions on how to do this, refer to “Initializing the TKE workstation crypto adapter” on page 84.

Passphrase and passphrase group logon

From the Framework tree on the left panel of the main TKE console screen, click on **Trusted key Entry**, then click on **Trusted Key Entry 9.0**.

Depending on how you have initialized your environment, the Crypto Adapter Logon window will be displayed with Profile IDs that represent single and/or group passphrase logon.



Figure 37. Crypto Adapter logon window with passphrase profiles

Steps for logging on are:

1. Select the Profile ID that you would like to use to log on to the TKE workstation crypto adapter.
2. Select **OK**

If you selected a single passphrase profile ID

1. The Passphrase Logon window will be displayed.

© Copyright IBM Corp. 2000, 2021

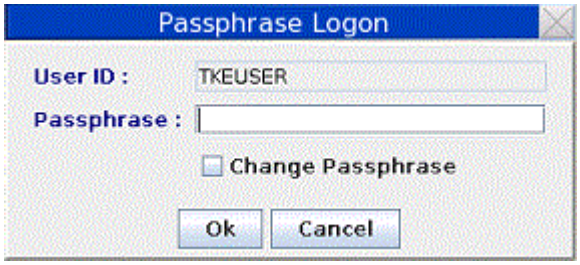


Figure 38. Enter passphrase for logon

2. Enter the passphrase for this profile ID and select **OK**.

   Note: The passphrase is case sensitive.

3. Optionally, the passphrase for the crypto adapter profile ID can be changed by the user by selecting the Change Passphrase check box before pressing OK to initiate the logon. If the Change Passphrase box was checked, then the Change Logon Passphrase dialog will be displayed after the user profile has been logged on, but before the selected TKE application is started.



Figure 39. Change logon passphrase

To change the passphrase, enter the current passphrase, the new passphrase and the verify new passphrase, then select **OK**.

If you selected a group passphrase profile ID

1. The Crypto Adapter Group Logon window will be displayed. This window displays the number of members required for logon and the profile IDs available for logon.

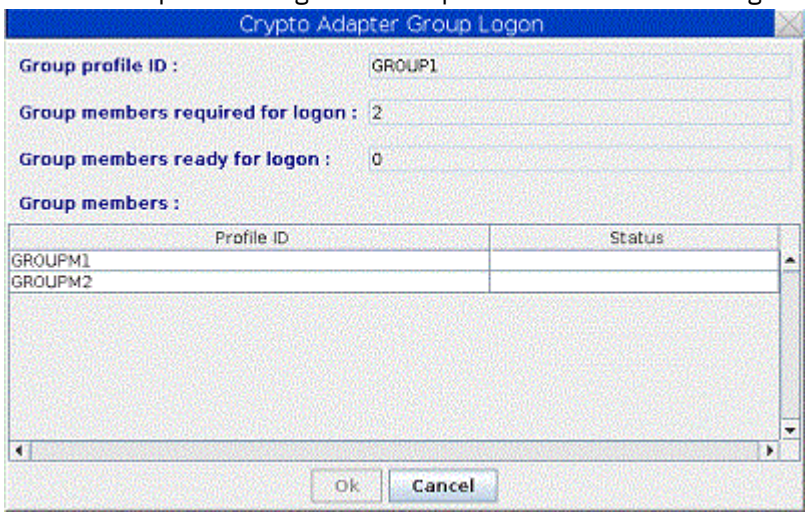


Figure 40. Crypto Adapter group logon window with passphrase profiles

2. Select the member profile ID that you would like to use to log on to the TKE workstation crypto adapter.
3. Select **OK**

The Passphrase Logon window is displayed.

4. Enter the passphrase for this profile ID and select **OK**.

   Note: The passphrase is case sensitive.



Figure 41. Enter passphrase for logon

5. Information in the Crypto Adapter Group Logon window is updated to reflect that the selected profile ID is now ready for logon.



Figure 42. Crypto Adapter Group logon window with passphrase profile ready

6. Repeat steps 2-4 until the number of group members required for logon is met

   Note: If the group logon should fail, the *Group members ready for logon* is reset to zero and group logon must start over.

Once the single or group passphrase logon is successful, the TKE application will be opened for use.

You may use the predefined user profile, TKEUSER, for single passphrase logon or another user profile with an equivalent role. If you choose to use passphrase group logon, the TKE Administrator must create a passphrase group profile and add the single user passphrase profiles to the group profile. The passphrase group profile should be mapped to the TKEUSER role or an equivalent role. The single user profiles that will be added to the group profile should be mapped to the DEFAULT role. This is done to limit the services permitted to the single users outside of the group. For details on creating single and group passphrase profiles see Chapter 11, “Cryptographic Node Management utility (CNM),” on page 251.

Smart card and smart card group logon

Depending on how you have initialized your environment, the Crypto Adapter Logon window will be displayed with profile IDs that represent single and/or group smart card logon.

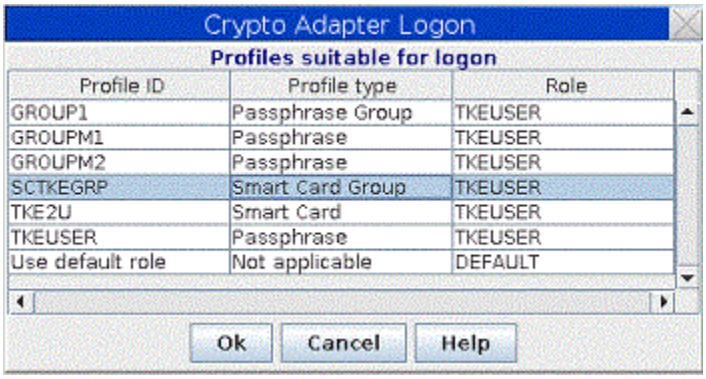


Figure 43. Crypto Adapter Logon Window with smart card profiles

Steps for logging on are:

1. Select the profile ID that you would like to use to log on to the TKE workstation crypto adapter.
2. Select **OK**.

If you selected a single smart card profile ID

1. The Smart Card Logon window will be displayed.
2. Insert the smart card that contains the crypto adapter logon key for the selected profile ID and select **OK**. Both TKE smart cards and EP11 smart cards can contain a TKE workstation crypto adapter logon key.

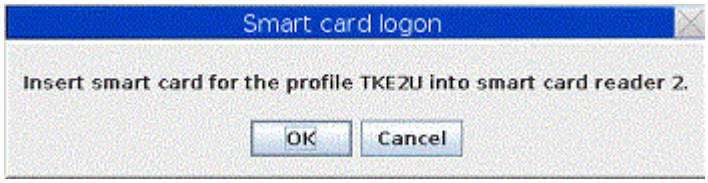


Figure 44. Insert the smart card

3. A message box displays, instructing you to "Enter your PIN in the Smart Card Reader". Enter the PIN for the smart card.

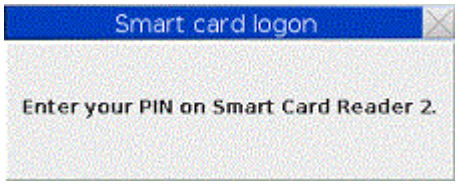


Figure 45. Enter smart card PIN

If you selected a group smart card profile ID

1. The Crypto Adapter Group Logon window will be displayed. This window displays the number of members required for logon and the profile IDs available for logon.

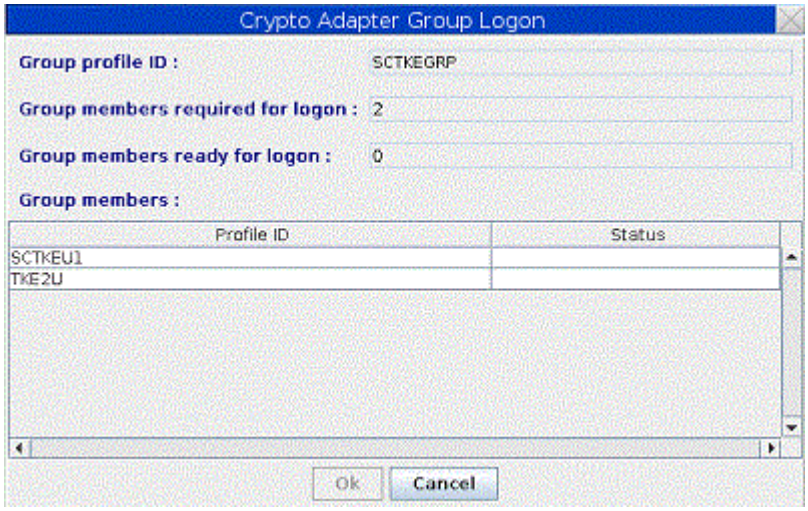


Figure 46. Crypto Adapter Group logon window with smart card profiles

2. Select the member profile ID that you would like to use to log on to the TKE workstation crypto adapter.
3. Select **OK**

   The Smart card logon window is displayed.
4. Insert the smart card that contains the crypto adapter logon key for the selected profile ID and select **OK**. Both TKE smart cards and EP11 smart cards can contain a TKE workstation crypto adapter logon key.

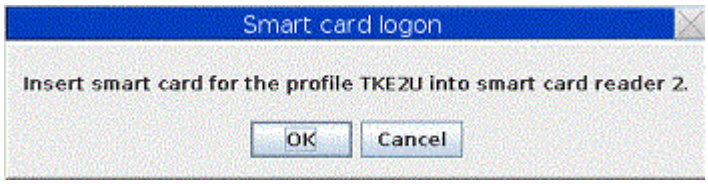


Figure 47. Insert the smart card

5. Information in the Crypto Adapter Group Logon window is updated to reflect that the selected profile ID is now ready for logon.

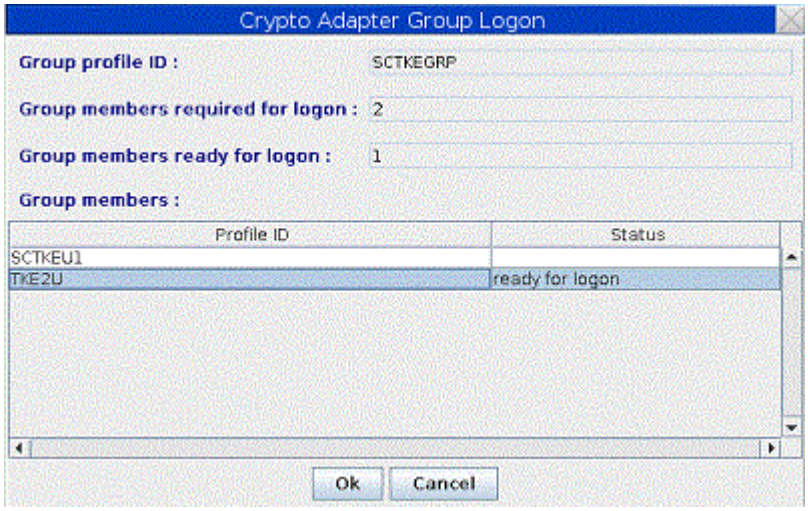


Figure 48. Crypto Adapter Group logon window with smart card profile ready

6. Repeat steps 2-4 until the number of group members required for logon is met

   Note: If the group logon should fail, the *Group members ready for logon* is reset to zero and group logon must start over.

Once the single or group smart card logon is successful, the TKE application will be opened for use.

You may use a group smart card profile assigned to the predefined role SCTKEUSR, or another user profile assigned to an equivalent role. If you choose to use single smart card logon, the TKE Administrator must create a single smart card user profile and map it to the SCTKEUSR role or an equivalent role. If a smart card group profile is used, the TKE Administrator must define single smart card user profiles to be added to the group. The single user profiles that will be added to the group profile should be mapped to the DEFAULT role. This is done to limit the services permitted to the single users outside of the group. For details on creating single and group smart card profiles see Chapter 11, “Cryptographic Node Management utility (CNM),” on page 251.

With either passphrase or smart card logon, if you cancel the logon, the TKE application is not opened.

Automated crypto module recognition

For each host, the TKE workstation maintains a list of the installed crypto modules. The list contains all the information required to protect communication between the workstation and the host crypto modules.

Whenever the user of the workstation connects to a host, TKE queries the host to determine the installed cryptographic hardware. The resulting list is compared to the contents of the crypto module file.

The user is notified if any of the following events occur:

- A new crypto module has been installed.
- A crypto module has been removed.
- A crypto module has been replaced.
- A new OA signature key has been generated for the crypto module. A new OA signature key is generated when the CCA CLU utility is used to zeroize and un-own segments 2 and 3, then load factory segments 2 and 3.
- A crypto module has been moved from one slot to another.

Authenticating host crypto modules

The TKE workstation uses the Crypto Module ID (CMID) and the public crypto module OA signature key to verify messages returned from a host crypto module.

To verify the CMID, you need to log on to your host TSO/E user ID. From the ICSF main panel, choose option 1, Coprocessor Management. This panel will list all the crypto modules available to this host. Verify the coprocessor index and serial number with the information on the 'Authenticate crypto module' window on TKE.

Beginning in TKE 9.2, you can configure your host definitions to automatically accept modules after they are authenticated. For new host definitions, auto-accept is the default setting. You can add the auto-accept option to an existing host definition using the change host feature of TKE.

On the Authenticate crypto module window:

- Press ***Yes*** if the coprocessor index and serial number on the host match the index and CMID on the window. The CMID value is saved on the TKE workstation for further communication with the host crypto module. The crypto module is marked as **Authenticated**.
- Press ***No*** if they do not match. The crypto module is marked as **Rejected by user**. You will not be able to work with the host crypto module but you are able to authenticate the module again. You select the crypto module and the CMID/type window is displayed for you to accept or reject the values.

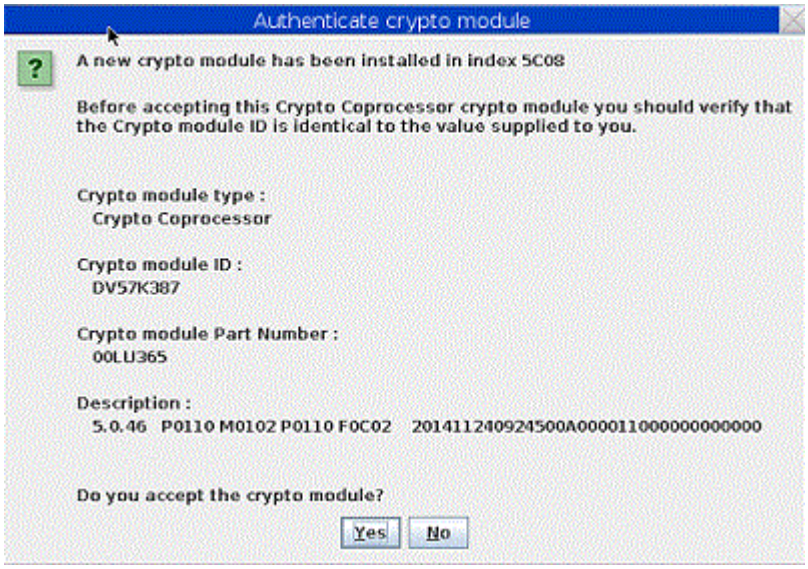


Figure 49. Authenticate Crypto Module

The crypto module type for all currently supported host crypto modules is "Crypto Coprocessor". Prior versions of TKE could manage other crypto module types that are no longer supported.

It is not necessary to authenticate the public crypto module OA signature key. The OA signature key is authenticated by a chain of certificates. The public key of the IBM Class Root certificate is hardcoded into the TKE workstation. The user is informed of the result of the verification process.

The IBM Customer Engineer (CE) may need to reload code in the host crypto module on the host for maintenance. If the code is reloaded, it may become necessary to reauthenticate the host crypto module during the first communication with it after the code reload. The reauthentication is necessary because the OA signature key has been regenerated.

Initial authorities

Commands from the TKE workstation to a host crypto module are signed. In order to configure a CCA host crypto module, an initial authority with a signature key must exist on the crypto module. This initial authority uses the Default Signature Key.

When a CCA host crypto module is initialized in the factory or by performing certain operations using the CCA CLU Utility, an authority with index 0 and the default signature key is created on the crypto module.

Backing up files

During normal TKE operations, users can create and modify files to:

- Store key parts, signature keys, and TKE roles and profiles.
- Define host connections and domain groups.
- Save host crypto module configuration data that will be applied to other host crypto modules.
- Implement key storage used by the TKE workstation.
- Save printable information for later reference.

Several directories on the TKE hard drive are used for these files.

Backing up these files on a regular basis is good practice. For information on file backups, see “Backup critical console data” on page 351. To schedule a one-time backup or repeating backups, see “Customize scheduled operations” on page 353.

Individual files can also be copied to USB flash memory. For more information, see “TKE File Management utility” on page 340.

Some files of interest in the TKE Data Directory are:

- host.dat -- holds host TCP/IP addresses and port numbers for the TKE Host Transaction program.
- domaingroup.dat -- holds domain group definitions.
- zone.dat -- holds information on configuration migration zones known to the TKE workstation.
- kphcard.dat-- holds information on key part holders used during configuration migration.

Some files of interest in the CNM Data Directory are:

- desstore.dat and desstore.dat.NDX -- implement DES key storage on the TKE workstation.
- aesstore.dat and aesstore.dat.NDX -- implement AES key storage on the TKE workstation.
- pkastore.dat and pkastore.dat.NDX -- implement PKA Key storage on the TKE workstation.

DES and AES key storage on the TKE workstation can hold EXPORTER keys used to transfer RSA keys to a host system. PKA key storage on the TKE workstation can hold a single RSA key for signing commands.

Host file to back up

The TKE Host Transaction program running on a z/OS host system uses a host data set to save crypto module descriptions, domain descriptions, and authority information, such as name, address, phone, and so on. This information is not critical for managing host crypto modules using TKE, but improves usability.

The default data set name is *smfid*.TKECM, where *smfid* is the System Management Facility identifier for the TKE Host Transaction program. The data set name can also be passed as the SET THE TKE DATA SETS startup parameter to the TKE Host Transaction program. See “TKE host transaction program setup” on page 74 for more information.

Chapter 6. Main window

The purpose of the TKE application is to allow administrators to manage host cryptographic modules, either individually or through groups. From the main window, you also create host definitions and group definitions.

Note: Many screen captures show smart card options. If Enable Smart Card Readers is not checked, you will not see the smart card options.

Beginning in TKE 7.1, when you initialize a TKE workstation crypto adapter for use with smart card profiles, the Enable Smart Card Readers option is automatically selected.

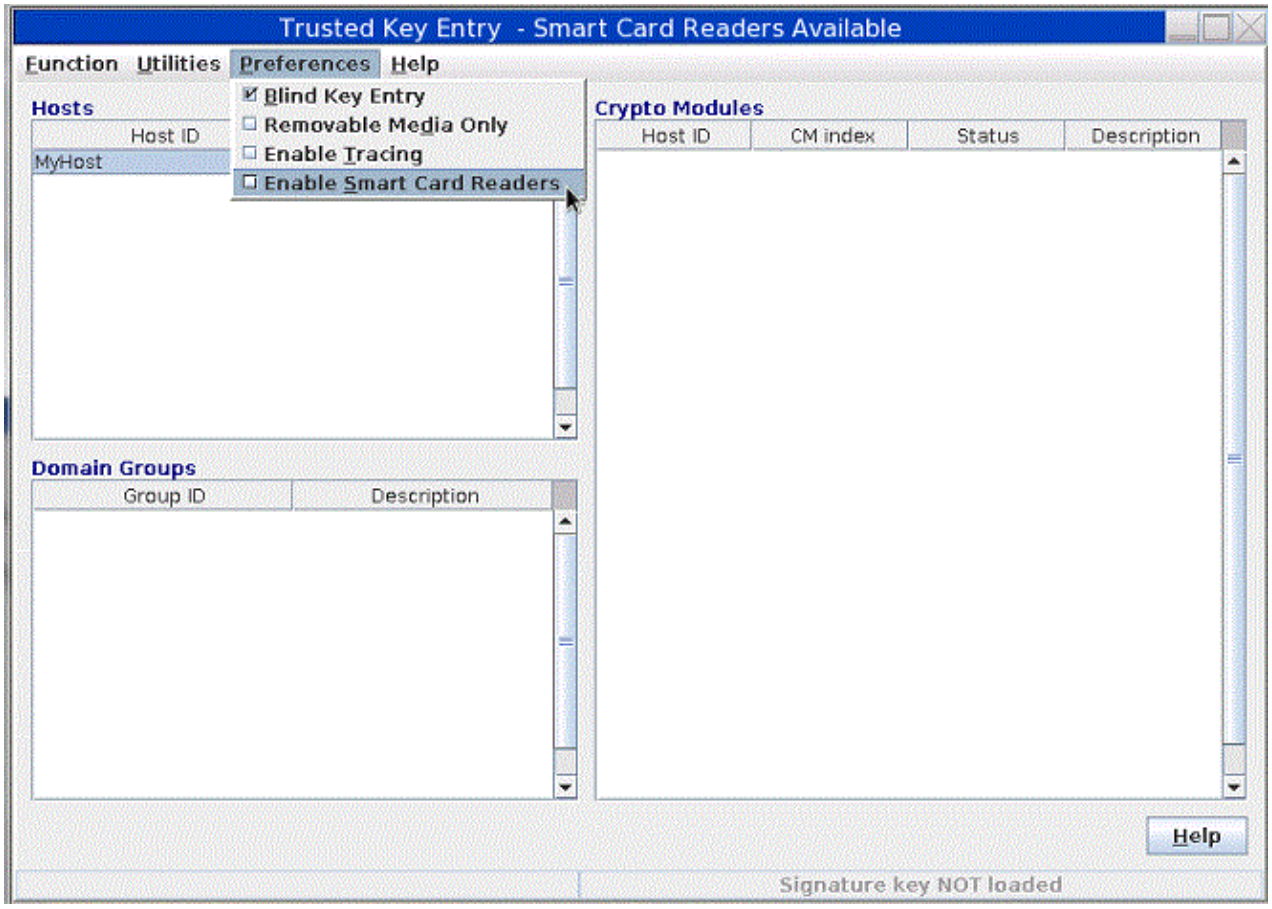


Figure 50. TKE Preferences

You can update the TKE application preferences by using the Preferences pull-down menu. To display the pop-up menu, click Preferences in the toolbar. Click individual items to enable or disable them. A check mark indicates that the preference is enabled. For details on each of the preferences, see "TKE customization" on page 134.

Note: When the Enable Smart Card Readers preference is enabled or disabled, the updated setting does not take effect until you restart the TKE application.

The main window has three containers that are labeled Hosts, Domain Groups, and Crypto Modules. All containers are blank until you create a host.

When you have created one or more hosts, decide whether you are working with single crypto modules or with domain groups. To work with domain groups, right-click in the Domain Groups container to display a menu. the pop-up menu contains options to create, change, delete, open, view, and close domain groups and an option to check group overlap.

© Copyright IBM Corp. 2000, 2021

To open a crypto module notebook for a single crypto module, open a host. (Right-click on it and select the Open Host option from the pop-up menu, or double-click it with the left mouse button.) After you log on to the host, TKE queries it and displays a list of the attached host crypto modules in the Crypto Modules window. To open a crypto module notebook, right-click on one of the host crypto modules and select Open Crypto Module from the pop-up menu, or double-click it with the left mouse button.

To open a crypto module notebook for a domain group, right-click the group and select the Open Group option from the pop-up menu, or double-click it with the left mouse button. You are prompted to log on to all host systems with crypto modules that are part of the group. A list of the crypto modules that are part of the group is displayed in the Crypto Modules container. Right-click in this list and select Open Domain Group from the pop-up menu, or double-click it with the left mouse button.

Note: Support for crypto module groups is removed beginning with TKE 8.0. If any crypto module groups are defined on your TKE workstation, a fourth container is displayed in the main window, labeled Crypto Module Groups. Right-clicking in this container causes a menu to be displayed, but the only options are to delete the group or convert the group to a domain group. For more information, see "Crypto module groups" on page 122.

Note the message in the lower right that the signature key is not loaded. See "Load signature key" on page 122.

Working with hosts

The Hosts container of the TKE Main Window lists the host IDs currently defined to the TKE workstation. You can create, change, delete, open, or close host definitions from this container. When you select your host (by double-clicking or selecting open), the host logon window opens if you are not yet logged on. When you are logged on, the crypto modules available for that specific host are displayed in the crypto module container. In addition, the specify auto-accept for all hosts option will turn on auto-accept for every host definition you currently have.

Beginning in TKE 7.3, your TKE workstation profile's role must have the Manage Host List ACP to be able to create, change, or delete a host list entry.

Creating a new host

The TKE workstation keeps a host definition for every host it can connect to. Clicking the right mouse button in the Hosts container causes a pop-up menu to be displayed, allowing you to choose the **Create Host** menu item.

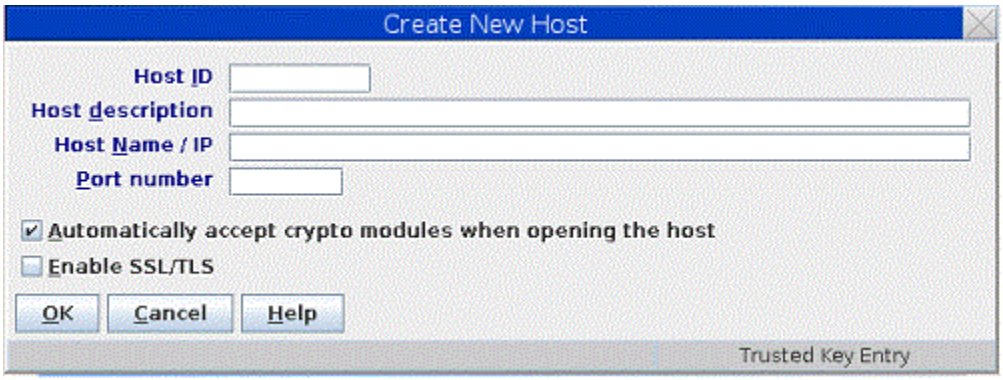


Figure 51. Create Host

The host definition contains the following information:

Host ID
Mandatory free format text used for referencing the host within TKE.

Host description
Free-format text for your own use.

Host Name / IP
Address in decimal-dot notation of the host where the TKE Host Transaction Program server is running. The field can contain a host name or a TCP/IP address in either TCP/IP V4 or TCP/IP V6 format.

Port number
Application port number reserved in your host TCP/IP profile for the TKE Host Transaction Program server. See Chapter 4, “TKE setup and customization,” on page 73.

Automatically accept Crypto Modules when opening the host check box
When selected, modules are automatically added to the list of modules you can manage from the host after the module is successfully authenticated.

Enable SSL/TLS check box
When selected, the host and port specified in this host definition must be configured for SSL/TLS communications. Also, the TKE administrator must have used the Certificate Management tool (found under Service Management - Configuration) to import the server certificate being used by the specified host name and port number.

It is not necessary to define each logical partition to TKE. One partition will have its control domain contain its own domain as well as any other domain where you want to load keys. This domain must be unique and must have access to all host crypto modules that it is to control.

For additional details on LPAR setup, refer to Appendix B, “LPAR considerations,” on page 321.

Changing host entries

Right-click on the host definition in the hosts container that you want to change. A menu is displayed. Select the **Change Host** menu item.

You can change the host description, IP address and port number. However, you cannot change the host ID. If you want to change the host ID, you must delete the host definition. You then create a new host ID.

Deleting host entries

To delete a host definition, right-click on the host you want to delete from the hosts container. A menu is displayed. Select the **Delete Host** menu item. A confirmation message is displayed. Select **Yes** to confirm the delete request. Select **No** to cancel the delete. Multiple hosts can be deleted at the same time by using ctrl+left-click or shift+left-click to highlight more than one host entry. When more than one host entry is selected, right-clicking on one of the selected host entries allows the **Delete Host** option to apply to all of the selected entries.

Logging on to a host

To log on, left-double-click on the host entry or right-click on the host entry and select **Open Host** from the pop-up menu. If you are working with a domain group, left-double-click on the domain group or right-click on the domain group and select **Open Group** from the pop-up menu. When you open a domain group in the TKE main window, you must log on to all hosts that are to be accessed within that group.

Note: Before attempting to use a user ID that has been configured to use Multi-Factor Authentication (MFA), see Appendix I, “Multi-Factor Authentication (MFA) and the TKE,” on page 393.

The Logon window is displayed for the host logon.

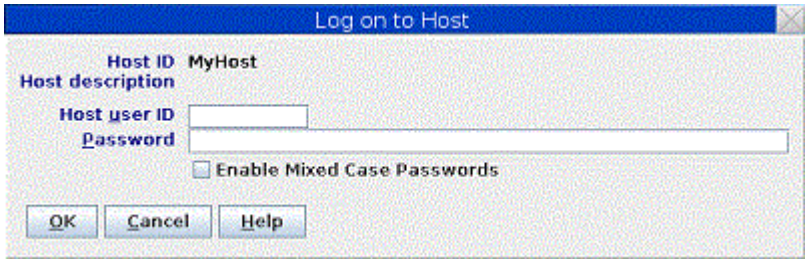


Figure 52. Host Logon window

Enter your RACF-defined TSO/E host user ID and password. Your RACF-defined TSO/E host user ID is the user ID of the TKE administrator.

If z/OS V1R7 or higher is installed, mixed case passwords are supported by RACF. If the Enable Mixed Case Passwords check box is enabled on the Log on to Host window, passwords are used as entered and are not automatically folded to uppercase. You must enter your password as it was defined in the RACF database. If your system does not support mixed case passwords and you check the Enable Mixed Case Passwords check box, you must enter your password in uppercase or you get "The password is incorrect" error.

Note: If your TSO/E password has expired, the message `The password has expired. Change password from TSO` is displayed. Change your password and perform the logon again.

Closing a host

To close a host, in the hosts container right-click the host that you want to close. Then, click **Close host**.

Close a host when you are done working with the crypto modules in the host. The next time that you open the host, a logon is required.

Specify auto-accept for all hosts

When selected, this option turns on auto-accept on every host definition your currently have.

Understanding crypto modules and domain groups

The term *host crypto module* refers to an IBM cryptographic coprocessor plugged into an IBM host system. Host crypto modules support up to 85 domains, where each domain may be assigned to a different logical partition on the host system. Domains include one or more master key registers. These support key storage for the logical partition.

When you open a host, TKE queries the host system to determine what host crypto modules are attached and available. These are displayed in the Crypto Modules container of the TKE Main Window. You can open a crypto module notebook for individual host crypto modules. This allows you to display information related to the crypto module and to issue commands to it. Some commands are *module scoped* and some are *domain scoped*.

- A *module scoped* command applies to the entire crypto module. For example, creating, changing, and deleting roles and authorities are module scoped commands because there is only one set of roles and authorities for the entire crypto module. Similarly, the commands to enable and disable the crypto module are module scoped commands.
- A *domain scoped* command applies to a single domain on the crypto module. For example, commands to load and clear master keys, change the domain controls, and zeroize the domain, are domain scoped commands.

To make the administration of crypto modules easier, you can create domain groups. A domain group allows you to use a single crypto module notebook to administer a set of domains or a set of crypto modules as a single unit. For example, you can use a domain group to load the same master key value in a set of domains (the member domains of the group).

To create a domain group, right-click in the Domain Groups container in the TKE Main Window. This displays a pop-up menu. Select the **Create CCA Group** option to create a domain group containing CCA host crypto modules. Select the **Create EP11 Group** option to create a domain group containing EP11 host crypto modules. You can create domain groups containing either CCA host crypto modules or EP11 host crypto modules, but you cannot create a domain group that includes both types of host crypto modules.

When you create a domain group, you select the domains to be included in the group. You can include domains from multiple host crypto modules from multiple hosts. You also specify a master domain. When you open a crypto module notebook for a domain group, the domain-level information displayed is information for the master domain. The module-level information displayed is for the crypto module containing the master domain.

For information on how to copy and paste domains into individual modules or all the modules in a host, see "Copy and paste domains using a create or change domain group screen" on page 109.

When you issue a domain-scoped command using a crypto module notebook for a domain group, the command is normally sent to every domain in the group. When you issue a module-scoped command using a crypto module notebook for a domain group, the command is sent to every crypto module having at least one domain included in the group.

A special case is commands to load or clear operational key registers in CCA domain groups. When you create or change a CCA domain group, you specify whether commands on operational key registers should be sent to just the master domain or to all domains in the group.

Copy and paste domains using a create or change domain group screen

Starting in TKE 9.2 with the latest maintenance installed, you can highlight a module in a create or change domain group screen, right click for options, and copy the selected domains of the module in the group. You can then paste the domain selections into individual modules or all the modules in a host to add domains to your group.

Notes:

- Master domain information is not included in the copied data.
- The paste operation replaces any domain selection you currently have.
- A paste will not change the master domain unless the paste removes the master domain from the group.
- The paste option is only available after a copy operation has been done.

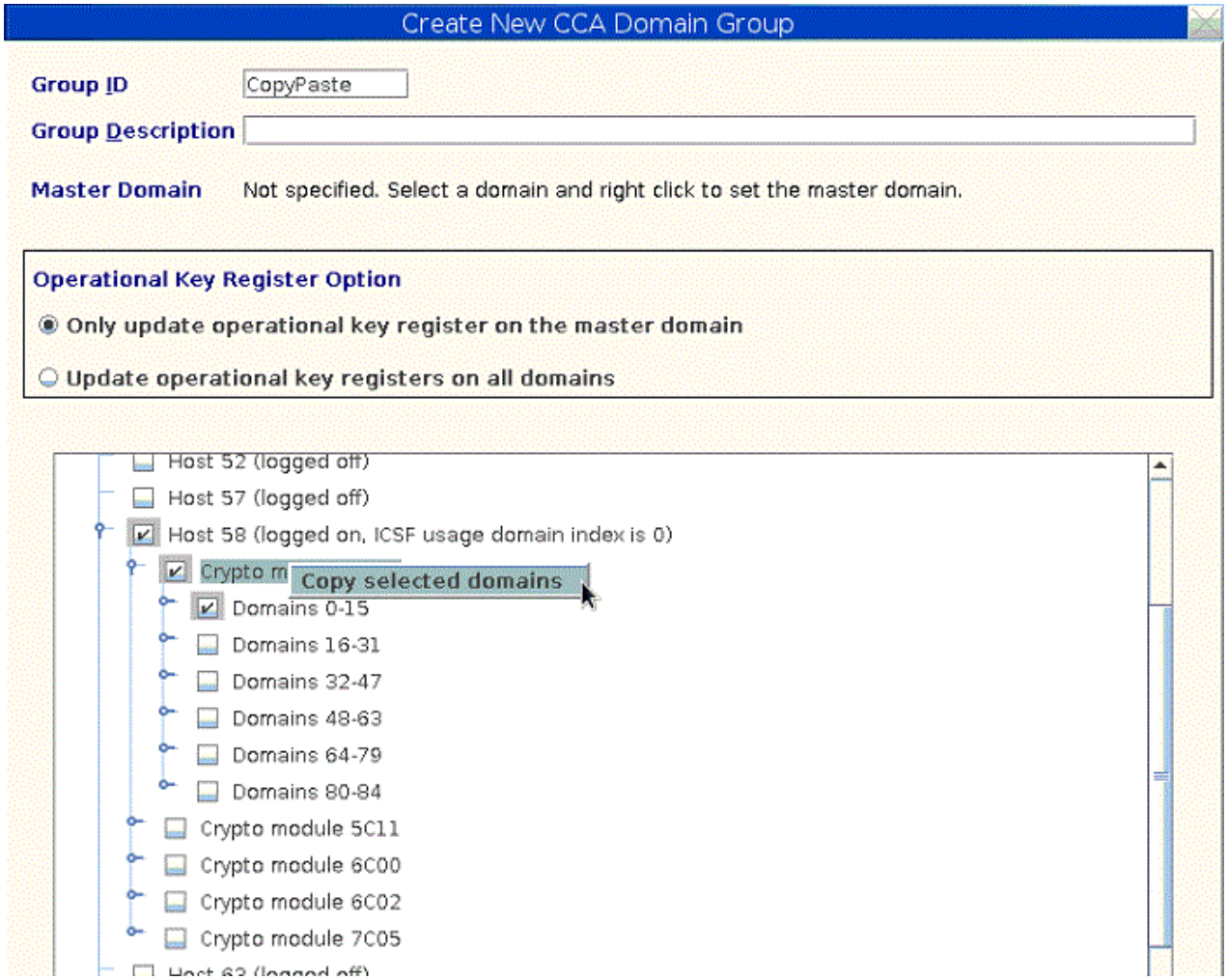


Figure 53. Example of a copy

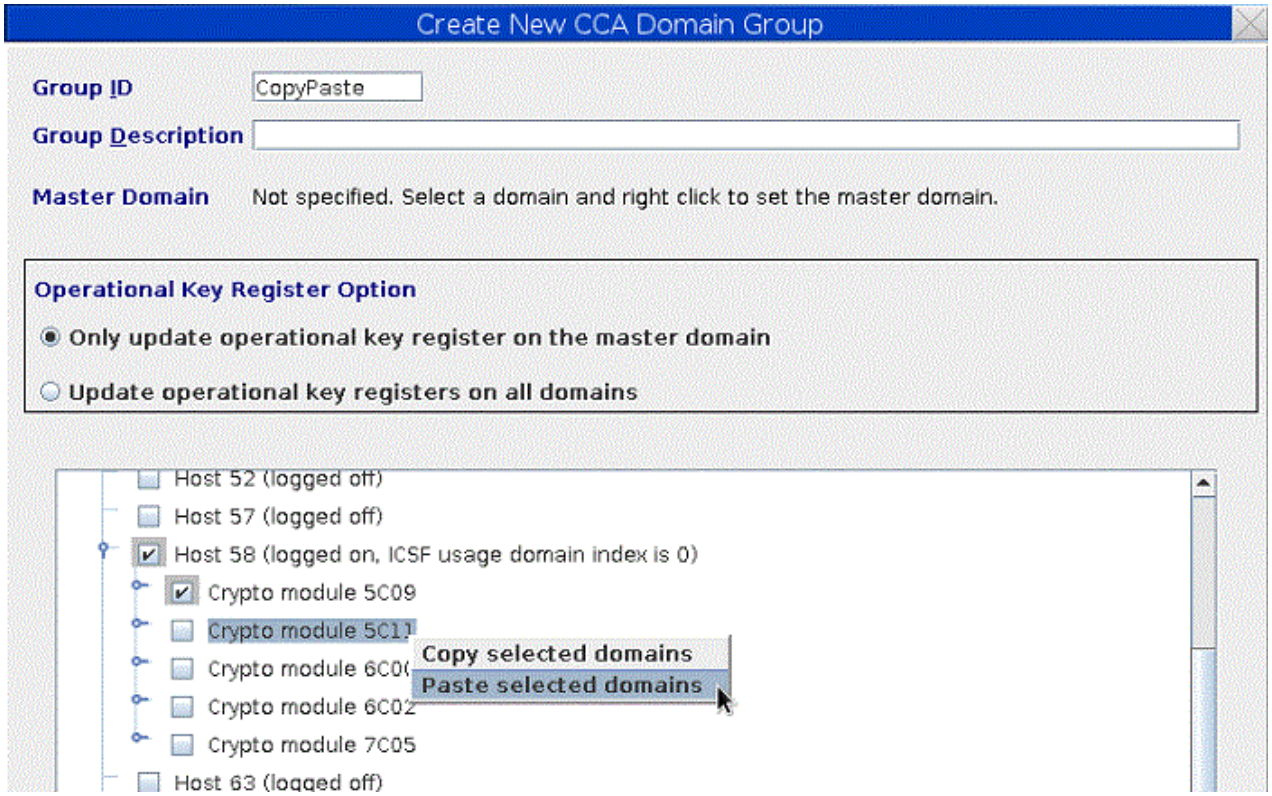


Figure 54. Example of a paste into an individual module

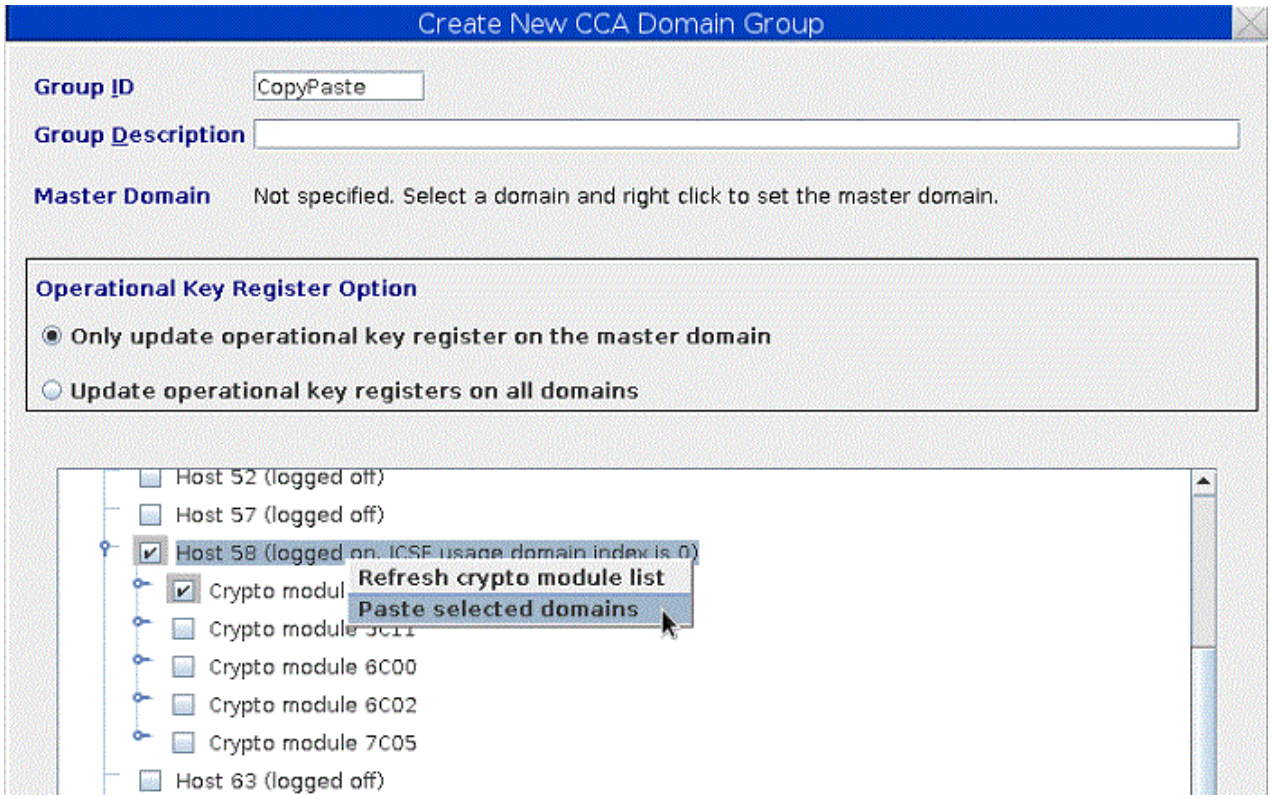


Figure 55. Example of a paste into all the modules in a host

Working with crypto modules

The crypto module container of the TKE Main Window displays the crypto modules that are available for use with the host or group you have selected. The container lists the host ID that the crypto module belongs to, the crypto module index, the status of the crypto module and the description of the crypto module. You are not able to change any of these fields from this container.

Figure 56 on page 112 illustrates the main window after logging on to a host. Note that in this screen capture, the signature key has not been loaded. To load a signature key, refer to "Load signature key" on page 122.

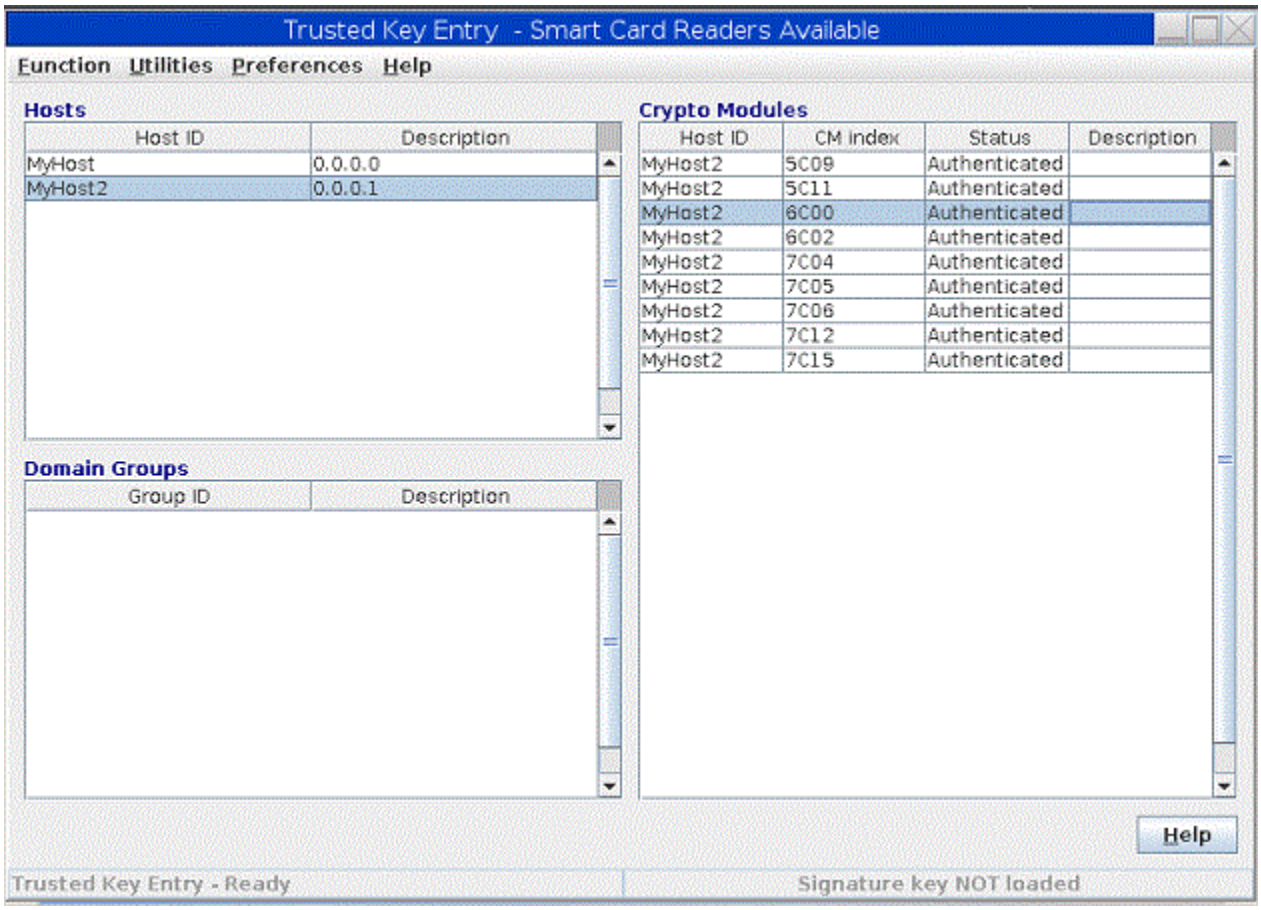


Figure 56. Main window

As discussed in "Automated crypto module recognition" on page 102, the Crypto Module container is filled in automatically once you have logged onto the host or hosts.

If you have selected a host to work with, you will be able to choose the crypto module you would like to open by highlighting it.

If you have chosen a group, when you highlight a crypto module all of the crypto modules will be highlighted.

To open a crypto module notebook, you can either left-double-click on a crypto module or right-click on a crypto module and select **Open Crypto Module** from the pop-up menu.

Working with domain groups

You manage domain groups in the TKE main window. You can add, change, delete or view domain group definitions from this container. You can also check group overlap.

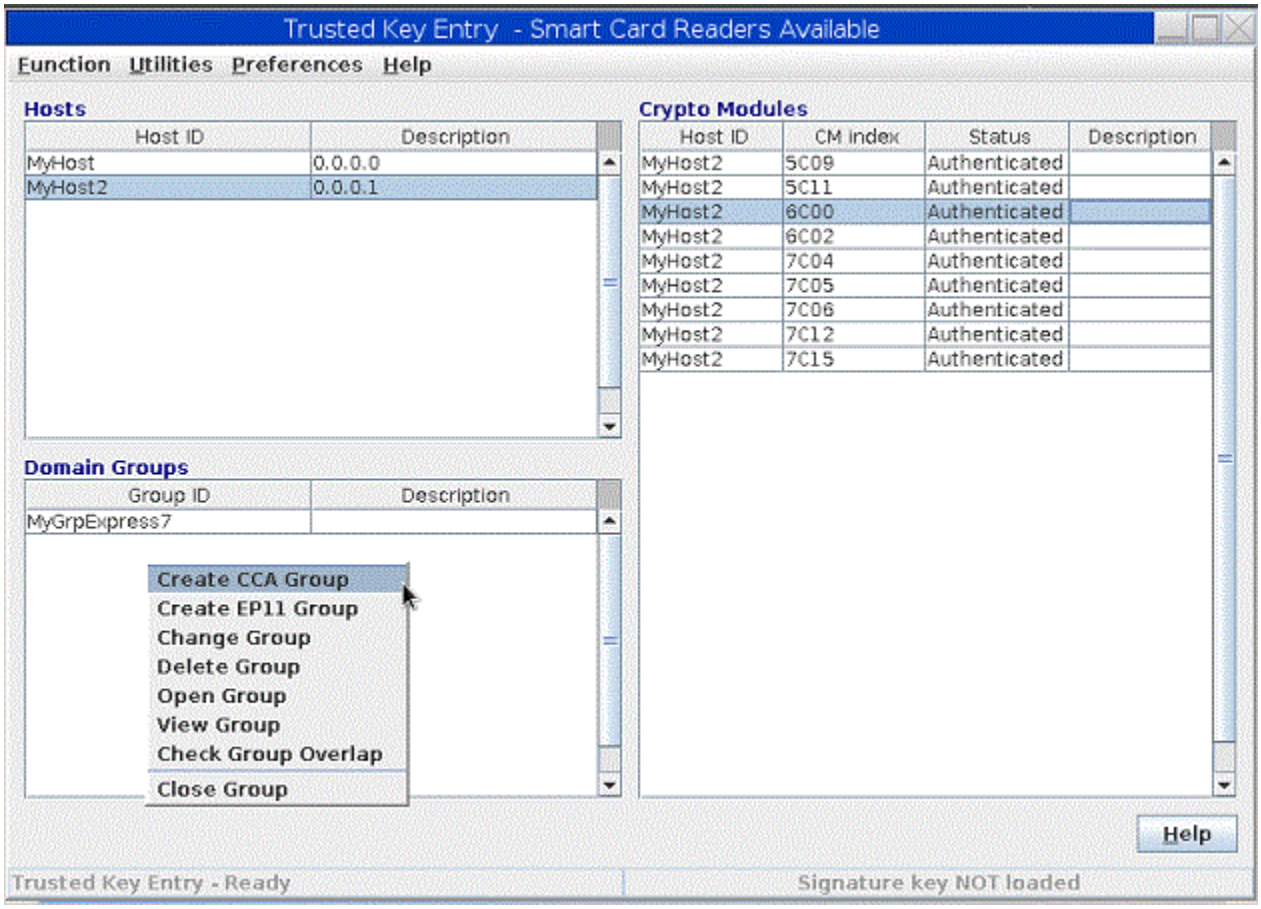


Figure 57. Main window - working with domain groups

The domain group concept allows you to perform operations on a set of crypto module domains as you would on a single crypto module domain. A domain group can include crypto modules from many hosts.

A domain group can contain domains on one or more crypto modules configured with CCA firmware or else can contain domains on one or more crypto modules configured with EP11 firmware. A domain group cannot contain a mixture of CCA-configured and EP11-configured domains.

In general, you work with the domain group as if it is a single domain. For example, you will see only one New Master Key register. The values displayed for a domain group are the values of the master domain. You select the master domain when you create the domain group. Also, note that the master crypto module of a domain group is the crypto module that contains the master domain.

For most operations, it is important that the crypto modules and domains within a domain group are in the same state. For example, the crypto modules have identical roles and domains have the same master keys. You maintain this by always working on members of the domain group using the domain group interface, and not operating on the crypto modules individually.

When TKE performs a domain group operation that is not successful, two new groups are created. One domain group contains the successfully updated crypto module domains and one domain group contains the crypto module domains where the update failed. This allows you to operate on the crypto module domains of the failed group until the update is successful. You may then delete the two new domain groups as you wish.

When you work with a domain group, either left-double-click on one of the domain groups defined in the Domain Groups container or right-click on one of the domain groups defined in the Domain Groups container and select **Open Group** from the pop-up menu. You are prompted to log on to the hosts associated with the crypto module members of the domain group.

When you open the crypto modules of a domain group, a crypto module notebook is displayed.

When loading operational key parts using a CCA domain group, with TKE 8.1 and later, you have the option to load them to either the master domain only or to all domains in the group. The desired behavior is selected when the domain group is created or changed.

Creating a domain group

You can create a domain group containing domains on one or more crypto modules configured with CCA firmware, or else containing domains on one or more crypto modules configured with EP11 firmware. A domain group cannot contain a mixture of CCA crypto module domains and EP11 crypto module domains.

To create a new domain group:

1. Right-click the mouse button in the Domain Groups container.

   A pop-up menu displays.

2. To create a domain group containing domains from CCA crypto modules, select the **Create New CCA Domain Group** menu item. To create a domain group containing domains from EP11 crypto modules, select the **Create New EP11 Domain Group** menu item.

   The “Create New Group” window opens.

   Note: For CCA domain groups, the supported crypto module types are CEX2C, CEX3C, CEX4C, CEX5C, CEX6C, and CEX7C. For EP11 domain groups, the supported crypto module types are CEX4P, CEX5P, CEX6P, and CEX7P.

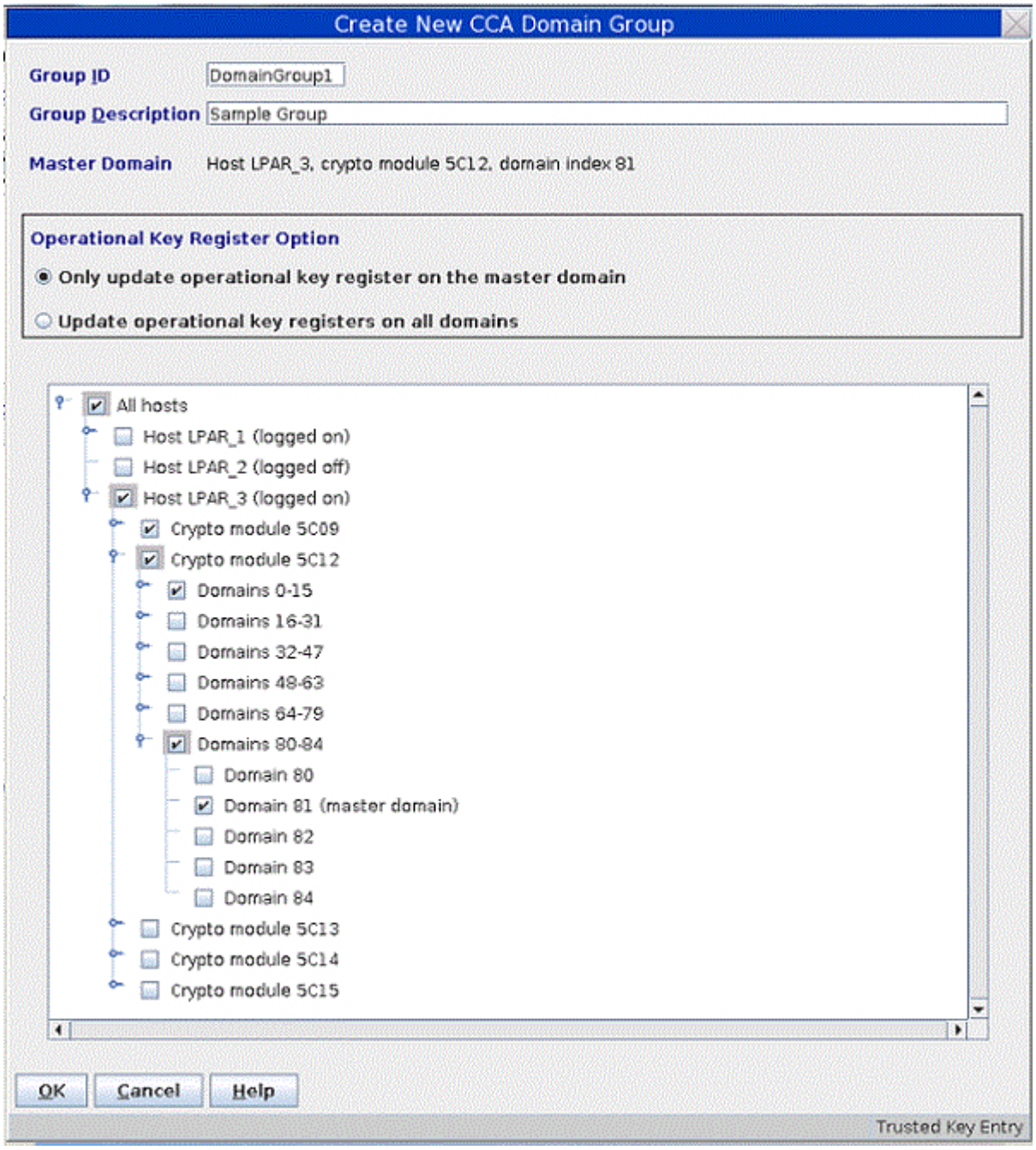


Figure 58. Create New CCA Domain Group

3. Enter your information in the following fields:
   a. **Group ID** - Name of the domain group (mandatory)
   b. **Description** - Optional free text description
   c. **Operational Key Register Option** - Beginning with TKE 8.1, you can choose to only update the operational key register on the master domain (selected by default) or you can choose to update operational key registers on all domains in the group.
   d. Select the crypto module domains to be in the domain group. In the Host tree structure, select the domains from each host you want to include in the domain group by selecting the check box associated with the domain. You will be prompted to log on to the selected host or hosts if you are not currently logged on.

      Note: Only domains defined as control domains on the crypto module will be available for inclusion in the domain group.

e. Select the crypto module domain to be the Master Domain by right-clicking on the domain and selecting **Make this the Master Domain**. The Master Domain information field of the **Create New Group** window changes to represent the Master Domain information.

f. When finished, press **OK**.

Notes:

1. Crypto modules at different CCA levels may support different features. For example, ECC (APKA) master keys were introduced with the CEX3C crypto module and restricted PIN support was introduced with the CEX4C crypto module. Domain groups can be created using crypto modules at different CCA levels. The notebook for the domain group will reflect the features supported on the crypto module containing the master domain.
2. If the crypto module containing the master domain has capabilities that other crypto modules in the group do not have, what happens during a group operation depends on the specific command executed. Commands to clear and load the AES and ECC (APKA) master keys are ignored on crypto modules that do not support those master key types. All other commands, such as commands to manage decimalization tables and restricted PINs, are attempted on all domains in the group and will fail on crypto modules that do not support those operations.

Changing a domain group

To change a domain group, right-click on the desired domain group in the Domain Groups container in the TKE main window and select the **Change Group** option.

The **Change Group** window is displayed.

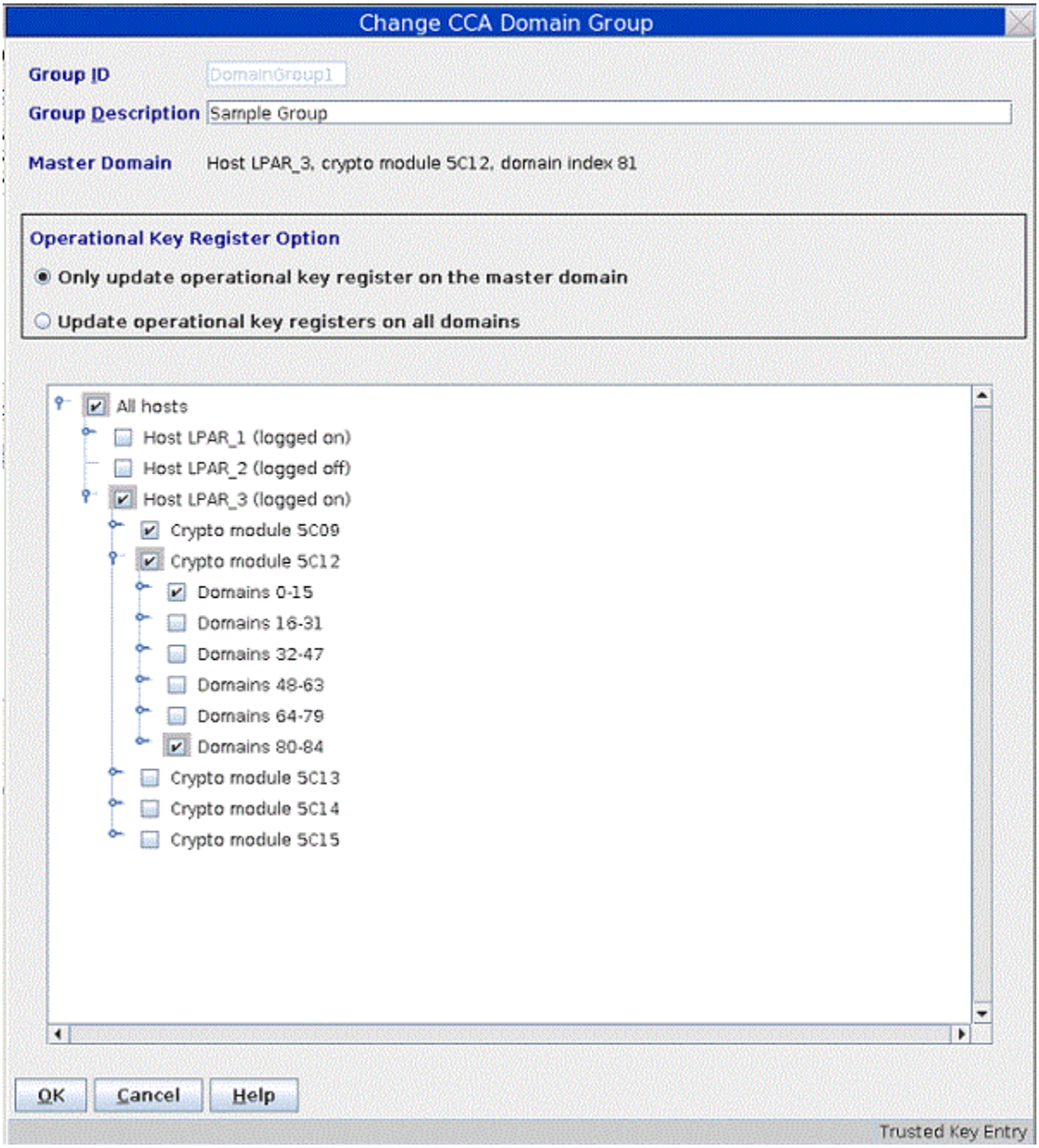


Figure 59. Change CCA Domain Group

To change the description, edit the **Group Description** field.

To change the Operational Key Register Option, select the other radio button.

To modify which crypto module domains are in the domain group, check the boxes corresponding to the domains to be included in the domain group. At least one domain must be checked.

To refresh the list of crypto modules associated with a host, do the following:

1. Highlight the host with the left mouse button.
2. Click the right mouse button to display a pop-up selection menu.
3. Select **Refresh crypto module list**.

To select which domain is the master domain, do the following:

1. Highlight a checked domain with the left mouse button.

2. Click the right mouse button to display a pop-up selection menu.
3. Select **Make this the master domain** menu item from the pop-up menu.

One domain must be selected as the master domain.

When finished, press **OK**.

Viewing a domain group

To view a domain group, either right-click on the desired domain group in the Domain Groups container in the TKE main window and select the **View Group** action or open a domain group in the crypto module container and press the **View Group** button on the Domain tab.

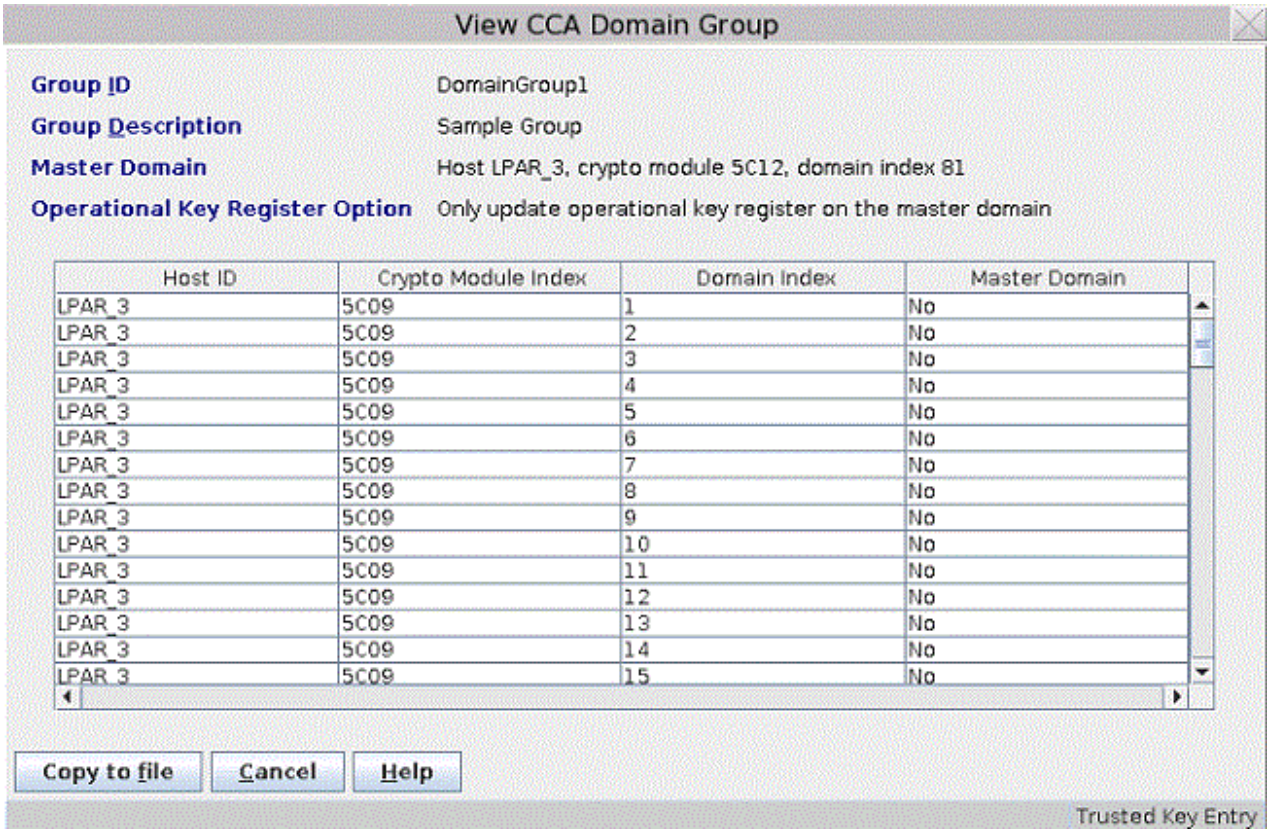


Figure 60. View CCA Domain Group

The **View Group** window is opened. The following information is displayed:

- **Group ID** – The group identifier
- **Group Description** – Optional free text description
- **Master Domain** – The master domain for this domain group. All displayed values for this group are retrieved from this domain.
- **Operational Key Register Option** - Indicates if domains in the group can have operational key register updates.
- **Domain table window** – A window containing a table that lists the crypto module domains in the domain group. There are four columns in the table: Host ID, Crypto Module Index, Domain Index and Master Domain.

You can copy the domain group information to a file by selecting **Copy to file** and specifying the file name and location to be saved. Otherwise, when finished, press **Cancel**.

Checking domain group overlap

To check if domain groups defined on the TKE workstation contain crypto module domains that are found in more than one domain group, click with the right mouse button in the “Domain Groups” container in the TKE main window and select the **Check Group Overlap** action. The **Domain Group Overlap** window is opened.

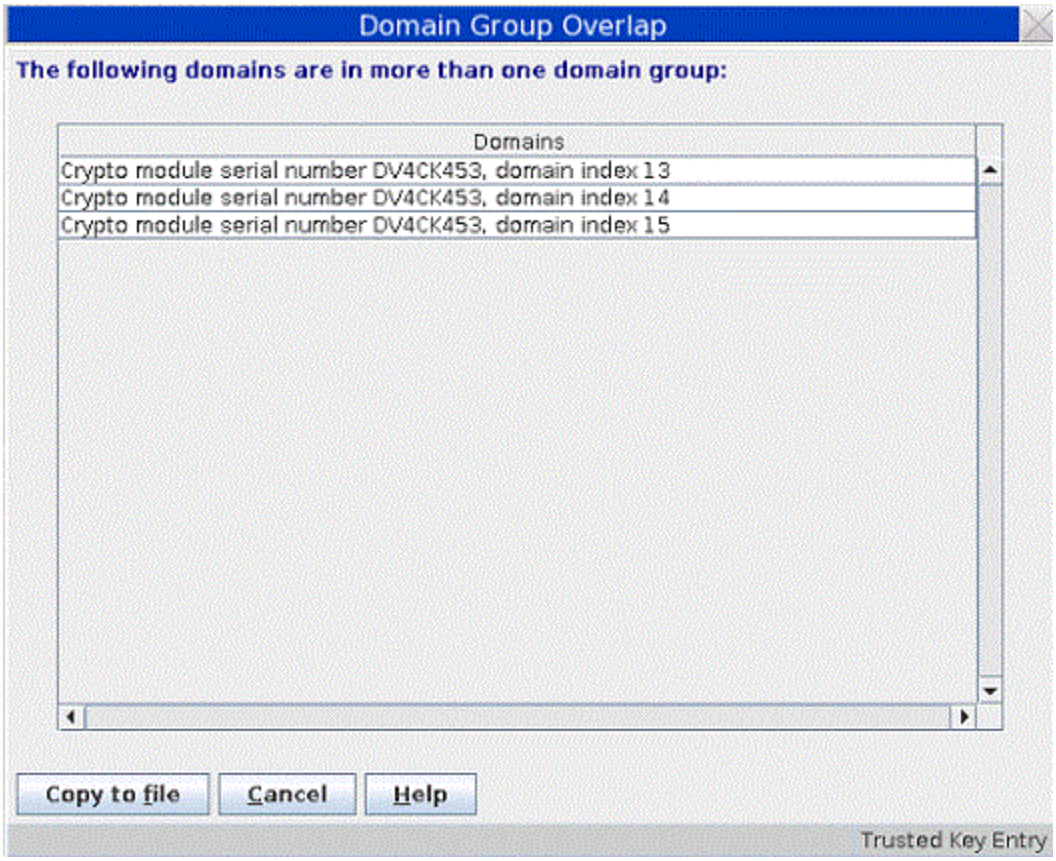


Figure 61. Check Domain Group Overlap

This window displays a list of domains that are specified in more than one domain group defined on the TKE workstation. Double clicking with the left mouse button on one of the domains displays an **Overlap Details** window that lists the names of the domain groups that contain the selected domain.

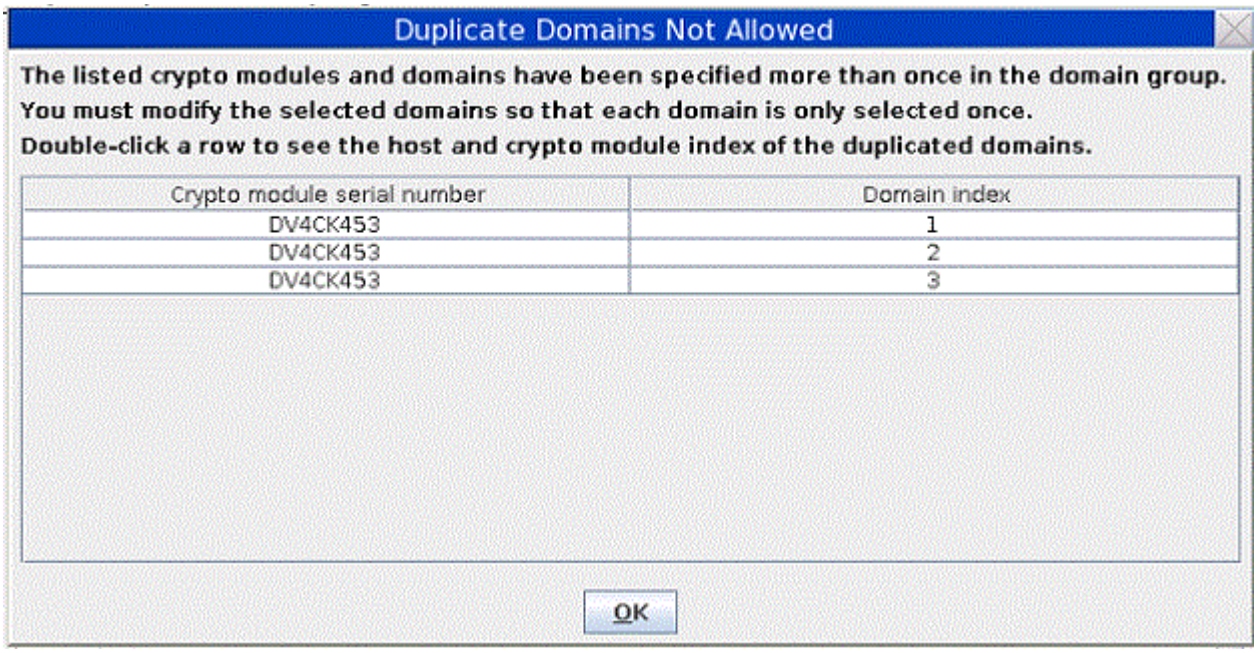


Figure 62. Duplicate Domains Not Allowed

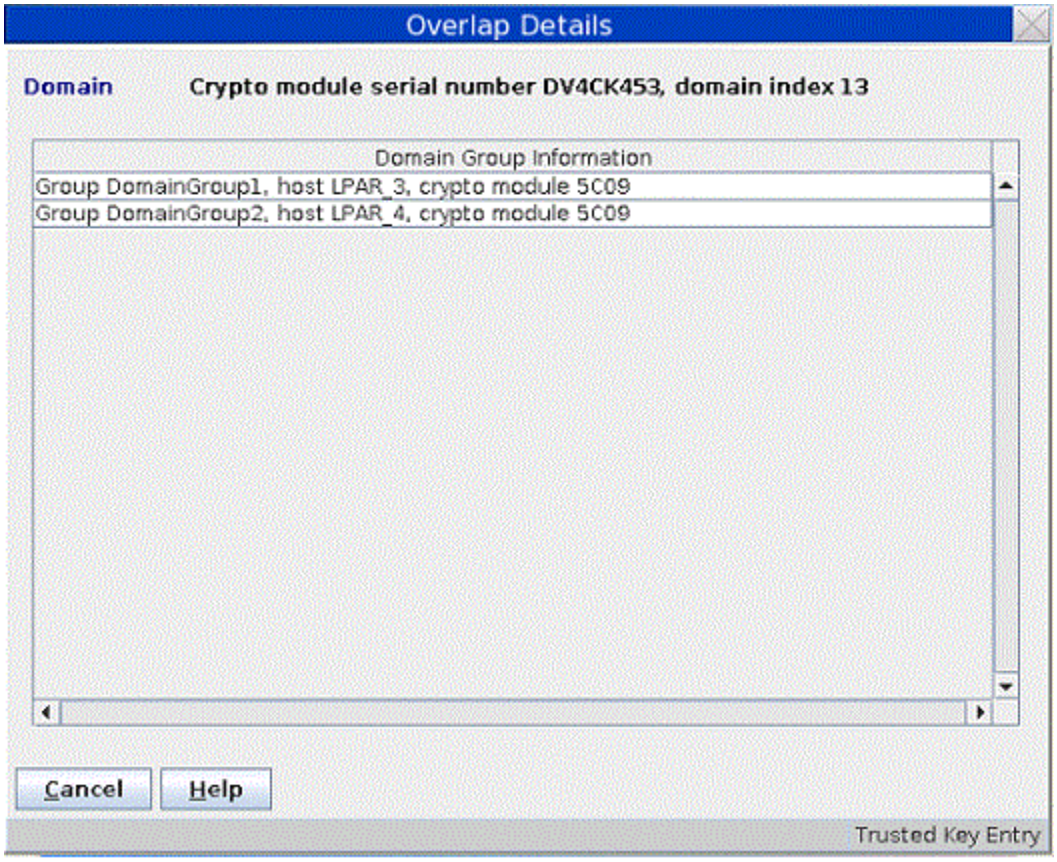


Figure 63. Domain Group Overlap Details

You can copy the domain group overlap information to a file by selecting **Copy to file** and specifying the file name and location to be saved. Otherwise, when finished, press **Cancel**.

Comparing groups

In order for operations on a domain group to be successful, all member domains need to be configured the same. For example, the status of a master key register needs to be the same in each domain of a domain group in order for an operation on that master key register to have the same result in each member domain.

The Group Compare function reads the state of the domains and crypto modules in a domain group and checks for differences. To run the group compare function, open the domain group, click on the **Function** menu at the top of the domain group notebook, and select **Compare Group** and select any one the three types of **Compare Group** functions.

TKE reads and compares the state of all domains and crypto modules in the group. If differences are found, a Group Compare window is displayed showing the differences. Differences can also be saved in a file.

Notes:

- Beginning in TKE 9.1, you can also run the Compare Group (Same Domain Index) function. This compare highlights differences between domains with the same index. For example, domain 0 and domain 1 can have different settings. However, the compare highlights only the differences between the domains with the same index, not differences between domain 0 and domain 1.
- With the latest TKE 9.2 maintenance installed, you can also run the Compare Group (Module-wide only) function. This compares only the module-wide settings of every module in the group.

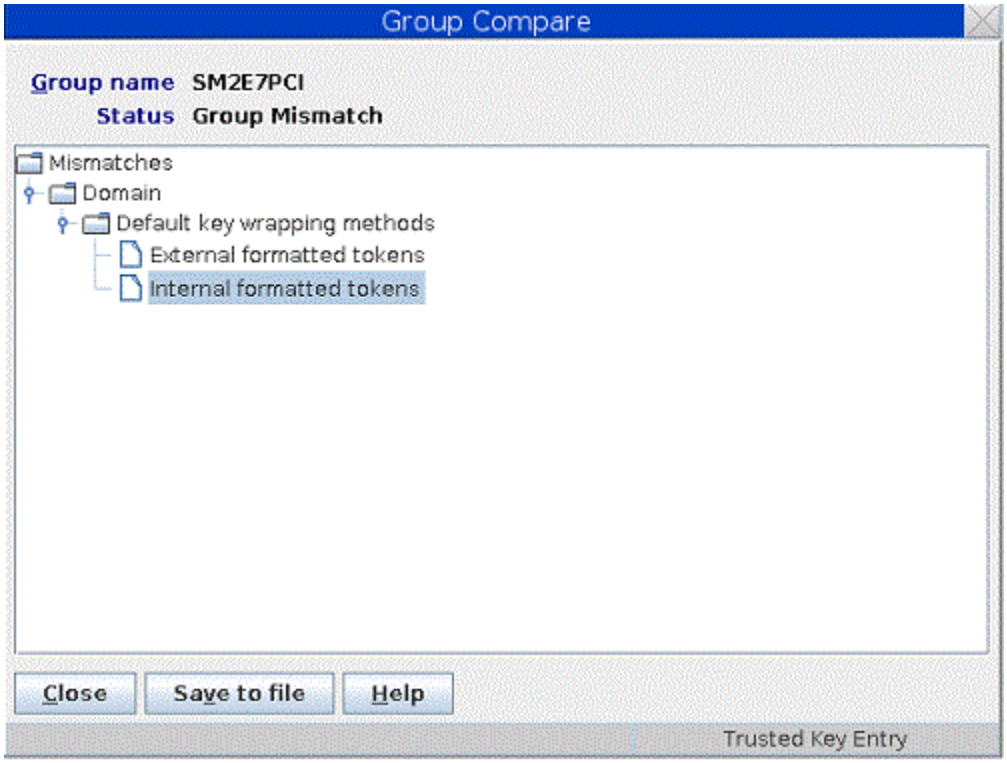


Figure 64. Compare Group

The Group Compare window displays the following results:

- **Group Name** – Name of the group that has been compared
- **Status** – Overall result of the compare operation
- **Mismatches** – A list of properties that do not match.

  If you select a property, a list of all crypto modules in the group with the actual values for that property is displayed.

TKE functions supporting domain groups

The values displayed in a domain group notebook are those read from the master domain, or from the crypto module that contains the master domain. In general, updates made in a domain group notebook are made in all member domains or member crypto modules of the group. For CCA domain groups, the operation 'View operational key part register' is only performed on the master domain.

Nearly all operations that can be performed in a crypto module notebook can also be performed in a domain group notebook. The only exception is for CCA domain groups. When creating or changing a role, users are not allowed to directly manage the domain access ACPs.

Crypto module groups

The Trusted Key Entry workstation no longer supports crypto module groups. To manage a group of crypto modules, a domain group can be created instead.

To assist users in converting from crypto module groups to domain groups, TKE provides a utility to create domain groups from crypto module groups. The utility is invoked as part of the TKE Workstation Setup wizard. From the utility, users select a crypto module group to be converted. The utility displays a proposed domain group for the crypto module group, and users may either accept this definition or make changes before creating the domain group.

Crypto module groups can also be converted to domain groups from the main TKE application. If at least one crypto module group is defined on the TKE workstation, the main TKE application displays a Crypto Module Groups container. From this container, you can select a crypto module group and either delete it or convert it to a domain group.

If no crypto module groups are defined on the TKE workstation, a Crypto Module Groups container is not displayed in the main TKE application.

Function menu

These selections are available from the **Function** menu in the TKE main window:

- **Load signature key**
- **Unload signature key**
- **Display signature key information**
- **Define transport key policy**
- **Exit**
- **Exit and logoff**

Load signature key

This function is used to load the authority signature key. Authority signature keys are used when managing CCA host crypto modules. The authority signature key is active for all operations until explicitly changed by clicking on this option again to load a different authority signature key, or until the signature key is unloaded.

A message is displayed in the lower-right corner of the TKE main window, indicating what signature key is active. If no signature key has been loaded, the message `SIGNATURE KEY NOT LOADED` is displayed. If a signature key has been loaded, the message `SIGNATURE KEY LOADED` is displayed, along with the index and name associated with the active signature key.

The CEX2C supports only 1024-bit RSA authority signature keys. CEX3C and CEX4C host crypto modules support 1024-bit, 2048-bit and 4096-bit RSA authority signature keys. CEX5C and later host crypto modules support 1024-bit, 2048-bit, and 4096-bit RSA authority signature keys, and BP-320 EC and 521-bit EC authority signature keys. Note: CEX7C will only support the carrying forward of a 1024-bit RSA authority signature key, not the generation of one.

To create an authority signature key, see “Generating authority signature keys” on page 147.

A **Select Source** window opens. Select the source of the authority signature key, and click **Continue**.

Notes:

- In order to see a smart card as one of the authority signature key sources, you must have previously selected **Enable Smart Card Readers** through the TKE main window **Preferences** menu.
- Starting in TKE 7.2, the TKE supports 2, 3 or 4 smart card readers.

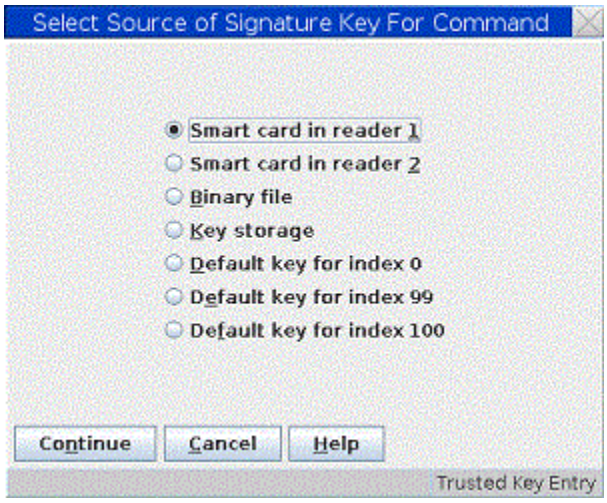


Figure 65. Select Authority Signature Key Source

- If you select **Key storage** or any **Default key** as the authority signature key source, the **Specify authority index** window opens. Enter the authority index to be used and click **Continue**.

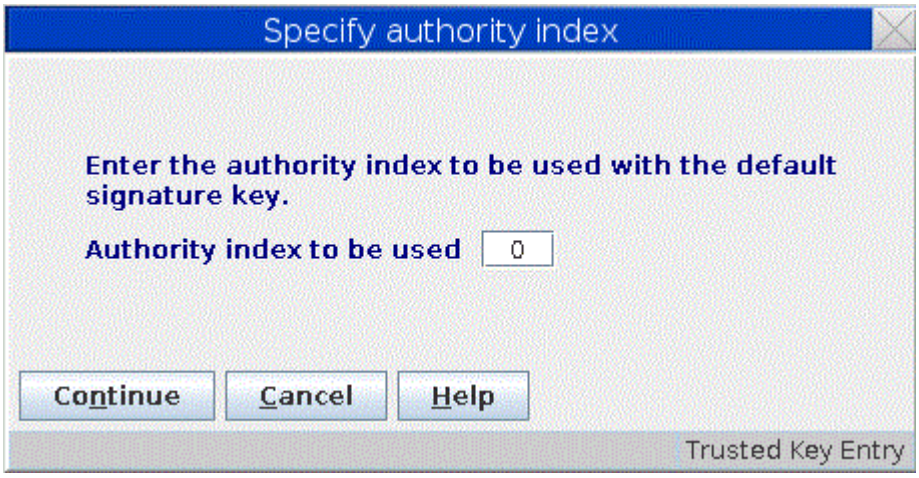


Figure 66. Specify Authority Index

- If you select **Binary file** as the authority signature key source, the **Load Signature Key** window opens. The authority signature key must have been previously generated and saved to a binary file. Either select a file from the **Files** list or enter a file name. Additionally, you must enter a password.

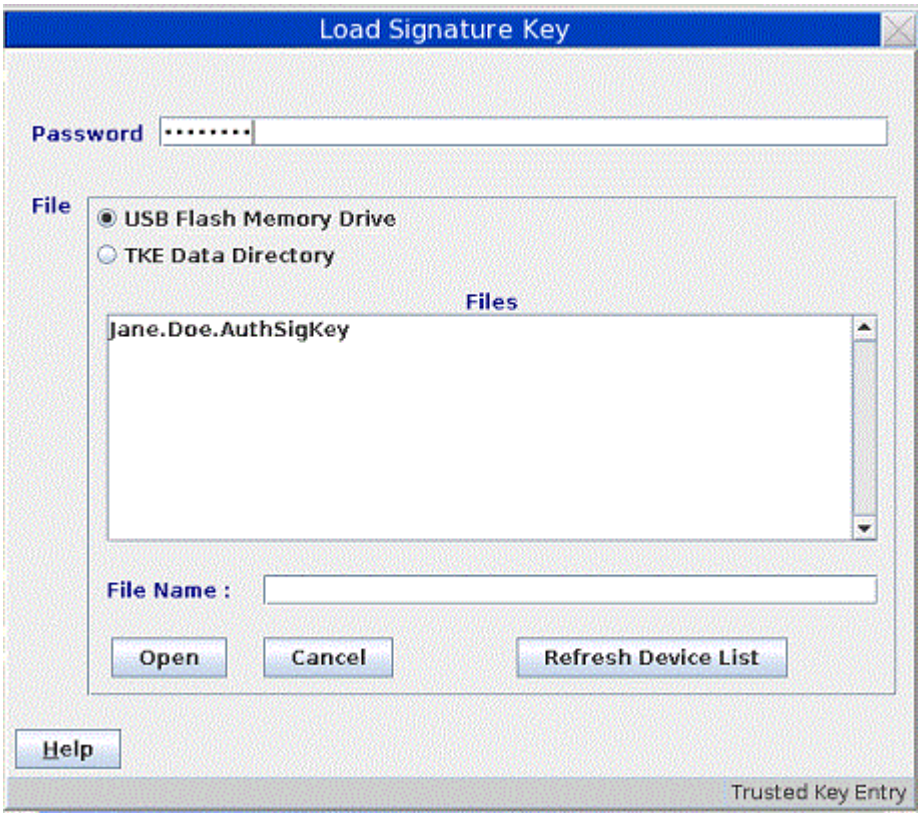


Figure 67. Load Signature Key

You are then prompted to specify the authority index.

- If you select **Smart card in reader 1** or **Smart card in reader 2**, you are prompted to insert your TKE smart card into the smart card reader. You are then prompted to enter the PIN on the TKE smart card reader's PIN pad.

You will then be prompted to specify the authority index.

Unload signature key

This function unloads the authority signature key. Use this function when you are finished using the key and want to ensure that the key is not used until it is loaded again.

Display signature key information

Selecting **Display signature key information** displays a panel showing the current signature index, key type, and the key identifier for the current authority signature key.

Define transport key policy

For CCA host crypto modules, master keys and operational keys are protected by encryption during transfer between the TKE workstation crypto adapter and host crypto modules. The transport encryption keys (key-encrypting keys) are established by means of a Diffie-Hellman key agreement mechanism. The Select Transport Key Policy Window lets you select the policy for the transport key.

For EP11 host crypto modules, master keys are also protected by encryption during transfer between the TKE workstation and host crypto modules, but a different mechanism is used. The policy selected by the Select Transport Key Policy Window does not apply to EP11 host crypto modules.

For CCA host crypto modules, TKE supports two Diffie-Hellman key agreement protocols: Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH). DH is used when TKE sends key material to a CCA host

crypto module with a CCA level earlier than 4.2. ECDH is used when the host crypto module has a CCA level of 4.2 or greater.

From the TKE main window, selecting **Function –> Define Transport Key Policy...** displays the Select Transport Key Policy window. This window lets you choose the transport key policy to follow.

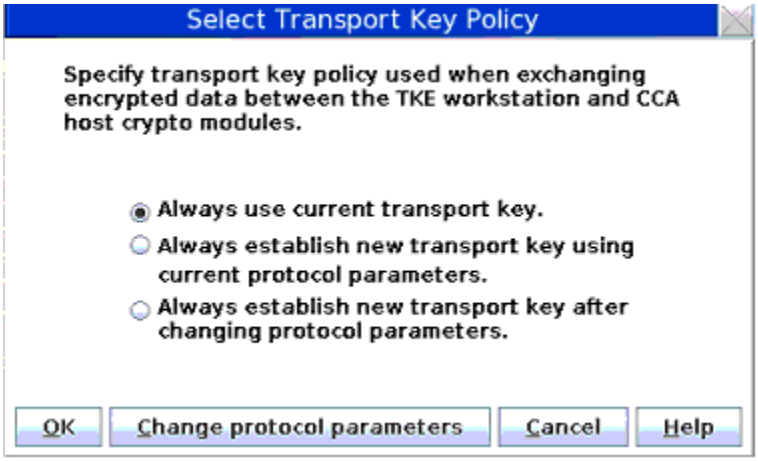


Figure 68. Select Transport Key Policy

Using the Select Transport Key Policy window, you can select one of the following:

- **Always use current transport key.**

  This is the default selection. TKE uses the current transport key or establishes a new transport key if one is not available. This avoids other key agreement protocol actions.
- **Always establish new transport key using current protocol parameters.**

  If TKE is communicating with a host crypto module using DH, it reuses the current Diffie-Hellman modulus and generator values to generate a new transport key for each key transfer. If they are not the correct key length or do not exist, TKE will automatically generate the correct Diffie-Hellman values. This selection avoids the time-consuming generation of the Diffie-Hellman values.

  If TKE is communicating with a host crypto module using ECDH, it uses the current ECDH domain parameters to generate a new transport key for each key transfer.
- **Always establish new transport key after changing protocol parameters.**

  If TKE is communicating with a host crypto module using DH, it will generate a new pair of Diffie-Hellman modulus and generator values and a transport key for each key transfer.

  If TKE is communicating with a host crypto module using ECDH, it uses new ECDH domain parameters to generate a new transport key for each key transfer. If a new transport key is established using this option, the curve type and size used to generate a new transport key are toggled to either NIST P521 or Brainpool 512 depending on the previous curve type and size used.

Select the required option by pressing the radio button and then press **OK**.

If you have selected to reuse the current values of Diffie-Hellman modulus and generator, you can force TKE to generate new Diffie-Hellman values by clicking **Change protocol parameters**. For ECDH, **Change protocol parameters** forces the TKE to use different ECDH parameters and causes TKE to establish a new transport key when needed using the new ECDH parameters.

Exit

Selecting **Exit** closes the TKE application window but does not log the current user off the TKE workstation crypto adapter. The TKE application can be restarted without logging in to the TKE workstation crypto adapter.

Exit and logoff

Selecting **Exit and logoff** closes the TKE application window and logs the current user off the TKE workstation crypto adapter. A user login is required to restart the TKE application.

Utilities menu

These selections are available from the **Utilities** pull-down menu in the TKE main window:

- **Copy binary file key part...**
- **Copy smart card contents...**
- **Create CCA key parts...**
- **Duplicate TKE or EP11 smart card...**
- **Generate EP11 master key parts...**
- **Manage smart card contents...**
- **Manage Workstation AES keys...**
- **Manage Workstation DES keys...**
- **Manage Workstation PKA keys...**

These utilities are used for managing the keys in TKE workstation DES, PKA, and AES key storage, managing smart card contents, and copying smart card contents.

The following utilities require the use of smart card readers and are grayed out if **Enable Smart Card Readers** is not selected in the **Preferences** menu:

- **Copy binary file key part...**
- **Copy smart card contents...**
- **Duplicate TKE or EP11 smart card...**
- **Generate EP11 master key parts...**
- **Manage smart card contents...**

Manage workstation DES keys

TKE workstation DES key storage is used to hold DES IMP-PKA keys that encrypt RSA keys for transfer to host systems. DES IMP-PKA keys can be loaded into TKE workstation DES key storage using an option on the Domain Keys page in the crypto module notebook. When DES IMP-PKA keys are loaded into TKE key storage, the key type is changed from IMP-PKA to EXPORTER.

This option lets you view and delete keys in TKE workstation DES key storage.

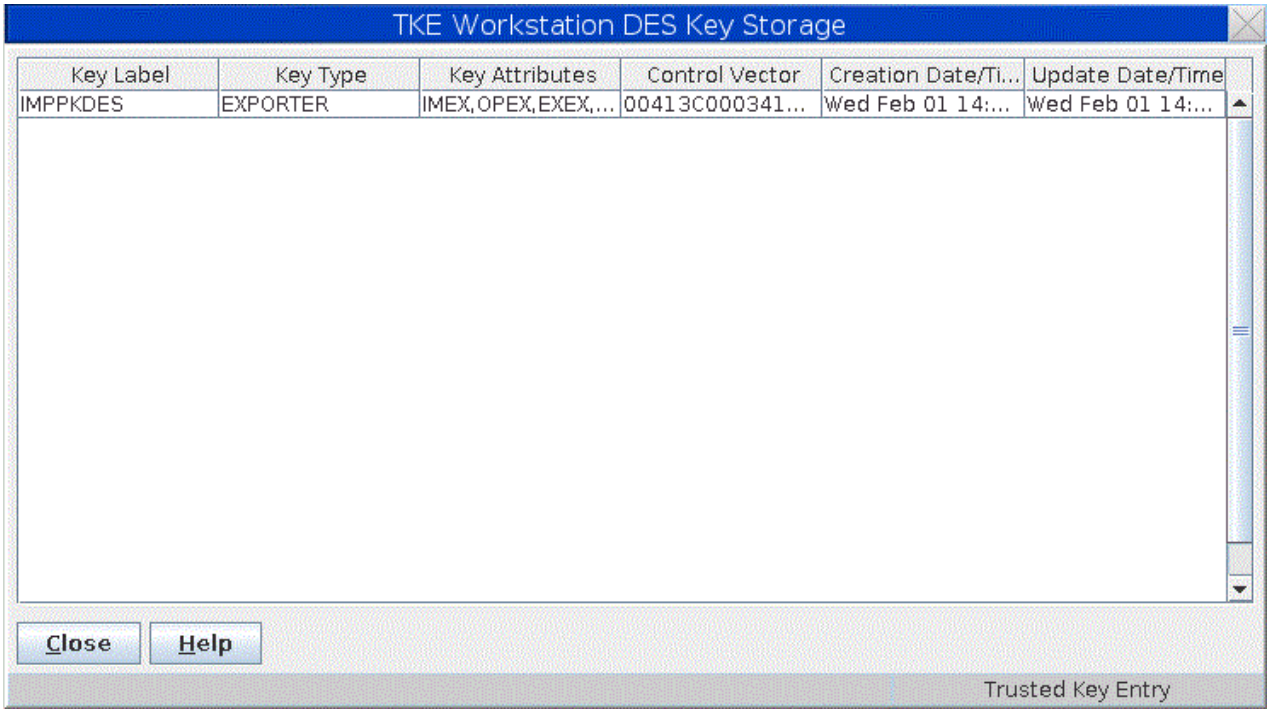


Figure 69. TKE Workstation DES Key Storage Window

The TKE Workstation DES Key Storage window displays the following information:

- Key label
- Key type

  DES IMP-PKA keys written to key storage have the key type *EXPORTER*. Keys with key type *NO_KEY* are empty and can be deleted. There might be other key types if the TKE workstation crypto adapter is used for purposes other than TKE.
- Key Attributes

  Following is a list of some of the key words used by the TKE workstation crypto adapter card for defining the control vector.

  – KEY-PART - The initial key part has been loaded but the last key part has not been loaded.

  – NO-XPORT - The key cannot be exported. IMP-PKAs used to protect generated RSA keys have this attribute.

  – XPORT-OK - The key is exportable. IMP-PKAs used to protect entered RSA keys have this attribute.
- Control vector - The CCA control vector.
- Created date and time
- Updated date and time

Deleting an entry

When you right-click on an entry, a menu is displayed. The only selection is **Delete Key**. This allows you to permanently delete a key from key storage.

Manage workstation PKA keys

TKE uses the TKE workstation PKA key storage for holding one authority signature key. This can be a 1024-bit, 2048-bit, or 4096-bit RSA signature key.

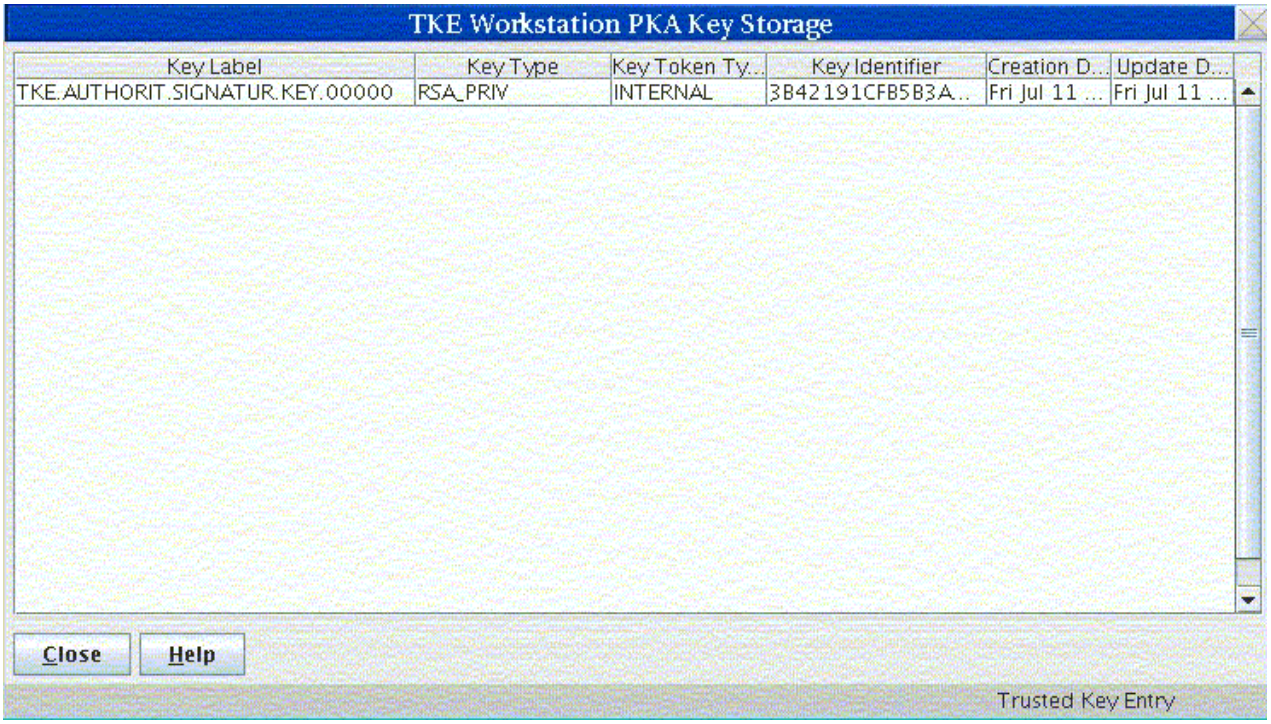


Figure 70. TKE Workstation PKA Key Storage Window

The TKE Workstation PKA Key Storage window displays the following information:

- Key label
- Key type

  The type of key is one of the following:

  – RSA-PRIV - A token holding the private and public key part of a PKA key pair. This is the key type for an authority signature key.
  – RSA-PUB - A token holding the public part of a PKA key pair.
  – RSA-OPT - A token holding the private and public part of a PKA key part in optimized form.
- Key Token Type

  The type of token is one of the following:

  – Internal - The key token is internal and the key value is enciphered under the TKE workstation crypto adapter master key.
  – External - The key token is external and the key value is either enciphered by a key-encrypting key or unenciphered.
  – NO_KEY - The key token is empty.
- Key Identifier - Identifies the RSA key in PKA key storage. The key identifier is the SHA-256 hash of the DER-encoded public modulus and public exponent of the RSA key pair.
- Created date and time
- Updated date and time

Deleting an entry

When you right-click on an entry, a menu is displayed. The only selection is **Delete Key**. This allows you to permanently delete a key from key storage.

Manage workstation AES keys

TKE workstation AES key storage is used to hold AES IMPORTER keys that encrypt RSA keys for transfer to host systems. AES IMPORTER keys can be loaded into TKE workstation AES key storage using an option on the Domain Keys page in the crypto module notebook. When AES IMPORTER keys are loaded into TKE key storage, the key type is changed from IMPORTER to EXPORTER.

This option lets you view and delete keys in TKE workstation AES key storage.

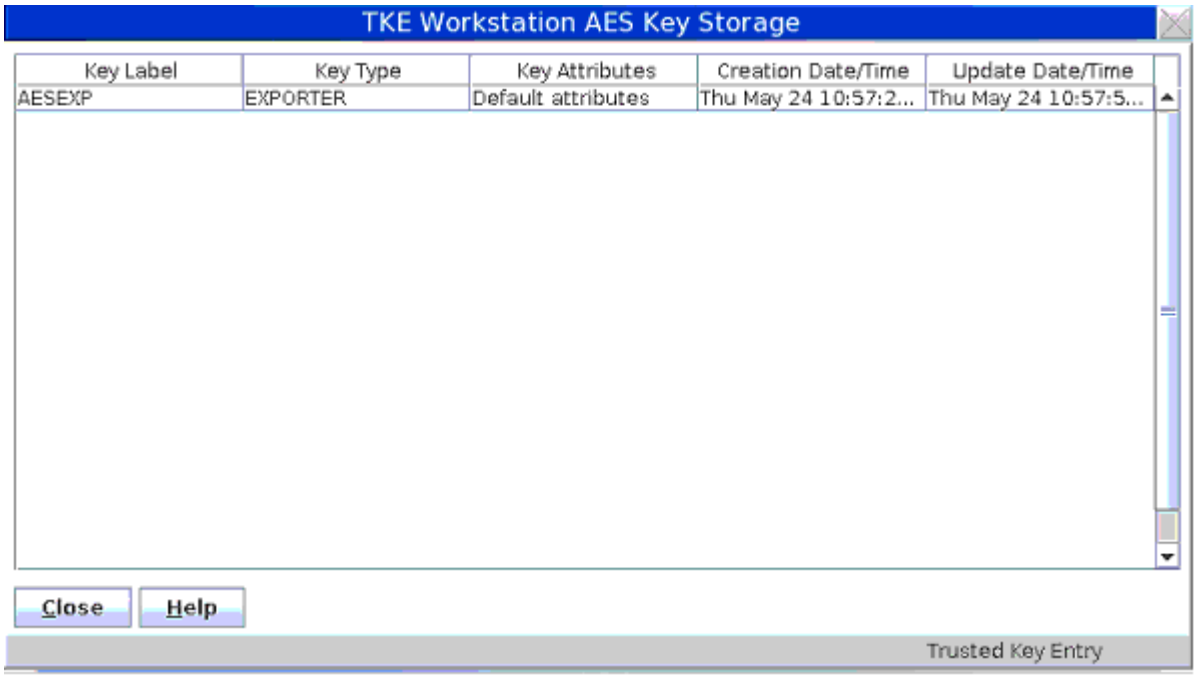


Figure 71. TKE Workstation AES Key Storage window

The TKE Workstation AES Key Storage window displays the following information:

- Key label
- Key type

  AES IMPORTER keys written to key storage have the key type EXPORTER. Keys with key type NO_KEY are empty and can be deleted.
- Key attributes

  Indicates whether the AES EXPORTER key has default or custom attributes. You can display the specific key attributes by right-clicking on an entry to display a menu. Select **Display key attributes** to view the attributes of the selected key.
- Created date and time
- Updated date and time

Deleting an entry

When you right-click on an entry, a menu is displayed. Select **Delete Key** to permanently delete a key from key storage.

Manage smart card contents

This function allows you to view a list of the keys and key parts stored on the smart card, delete keys and key parts from the smart card, and, for TKE smart cards, display information about AES EXPORTER, IMPORTER, and CIPHER operational keys stored on the smart card. This function can be used with both TKE smart cards and EP11 smart cards.

1. At the prompt, insert your smart card into smart card reader 2.
2. The utility reads the smart card contents. This may take some time. The card ID is displayed followed by the card description. Verify that this is the smart card you want to work with.

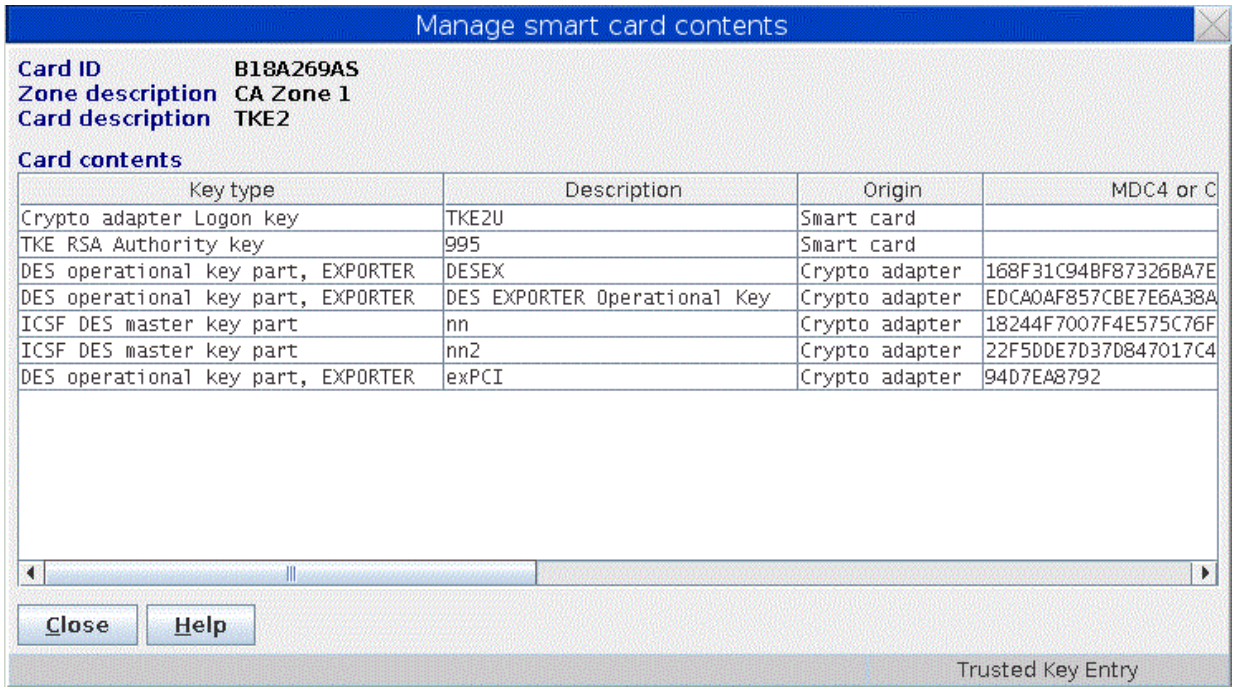


Figure 72. Smart card contents (for TKE smart cards)

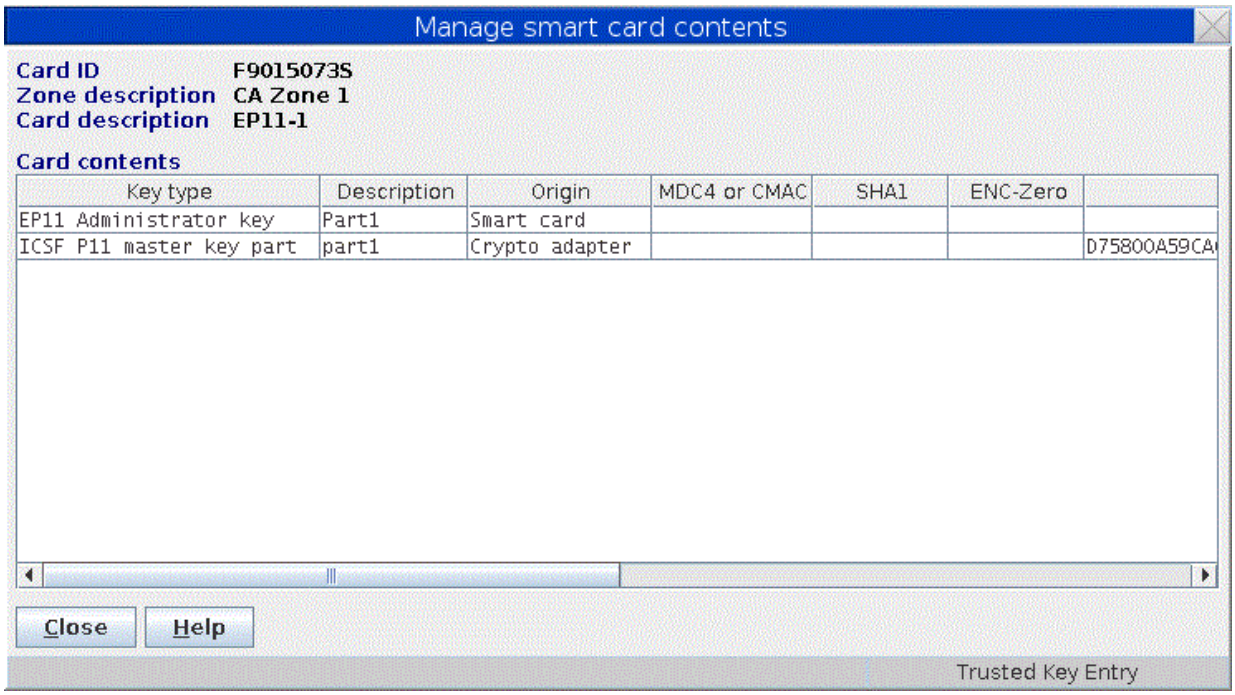


Figure 73. Smart card contents (for EP11 smart cards)

The Manage smart card contents window displays the following information for a smart card:

Card ID
Identification string for the smart card

Zone description
Description of the zone in which the smart card is enrolled

Card description
Description of the smart card; entered when the smart card was personalized

Card contents
Key type, Description, Origin, MDC4 or CMAC, SHA1, ENC-Zero, AES-VP or HMAC-VP, Control Vector or Key Attributes (for operational keys only), and Length.

3. To delete multiple keys at once, highlight all the keys you want to delete. By holding down the control button, you can select specific entries on the list with your mouse. By holding down the shift button, you can select a specific range of entries on the list with your mouse.
4. Right-click on either the single entry you would like to delete or one of the highlighted entries when deleting more than one entry at a time. Then, select **Delete** from the menu.
5. Right click and select **Delete**.
6. Confirm the delete.
7. Enter the 6-digit PIN.

   Note: TKE smart cards created before TKE 7.0 use 4-digit PINs.
8. You will get a message that the command was executed successfully.
9. You can display the key attributes associated with a CIPHER, EXPORTER, or IMPORTER AES operational key part stored on the smart card. Right-click on the desired key part to display a pop-up menu. Select the **Display key attributes** option to display the key attributes.

Copy smart card contents

This function allows you to copy keys and key parts from one TKE smart card to another TKE smart card, or from one EP11 smart card to another EP11 smart card. You can copy these types of keys:

- Crypto adapter logon key
- TKE authority signature key
- EP11 administrator signature key
- ICSF operational key parts
- ICSF master key parts
- Crypto adapter master key parts

Notes:

1. The two smart cards must be enrolled in the same zone; otherwise, the copy fails. To display the zone of a smart card, exit from the TKE application and use either the Cryptographic Node Management Utility or the Smart Card Utility Program found in the Trusted Key Entry category's Applications list on the TKE Workstation Console. See Chapter 11, “Cryptographic Node Management utility (CNM),” on page 251 or Chapter 12, “Smart Card Utility Program (SCUP),” on page 291.
2. To copy ECC (APKA) master key parts from a source TKE smart card to a target TKE smart card, the applet version of the target TKE smart card must be 0.6 or greater.
3. To copy an ECC authority signature key from a source TKE smart card to a target TKE smart card, the version of the target TKE smart card must be 0.10 or greater.

To copy a smart card:

1. Select **Copy smart card contents** from the **Utilities** menu.

   A message box prompts you to “Insert source TKE or EP11 smart card in smart card reader 1”.
2. Insert the source smart card in smart card reader 1 and press **OK**.

   A message box prompts you to insert the target smart card in smart card reader 2. The target smart card must be the same type (TKE or EP11) as the source card.
3. Insert the target smart card in smart card reader 2 and press **OK**.

The utility reads the smart card contents, which may take some time. The card ID is displayed, followed by the card description. Verify that these are the smart cards that you want to work with.

The Copy smart card contents window lists the following information for a smart card:

Card ID
Identification string for the smart card.

Zone description
Description of the zone in which the smart card is enrolled.

Card description
Description of the smart card, which was entered when the smart card was personalized.

Card contents
Key type, Description, Origin, MDC4 or CMAC, SHA1, ENC-Zero, AES-VP or HMAC-VP, Control Vector or Key Attributes (for operational keys only), and Length.

4. To copy multiple keys at the same time, highlight all the keys that you want to copy. By holding down the control button on the keyboard, you can select specific entries on the list with your mouse. By holding down the shift button on the keyboard, you can select a specific range of entries on the list with your mouse. Left-click on the **Copy** button or right-click on one of the highlighted entries and select **Copy** from the menu. To copy a single key, right-click on the wanted key, and select **Copy** from the menu.

   Note: Smart card copy does not overwrite the target smart card. If there is not enough room on the target smart card, you get an error message. You can either delete some of the keys on the target smart card (see "Manage smart card contents" on page 129) or use a different smart card.

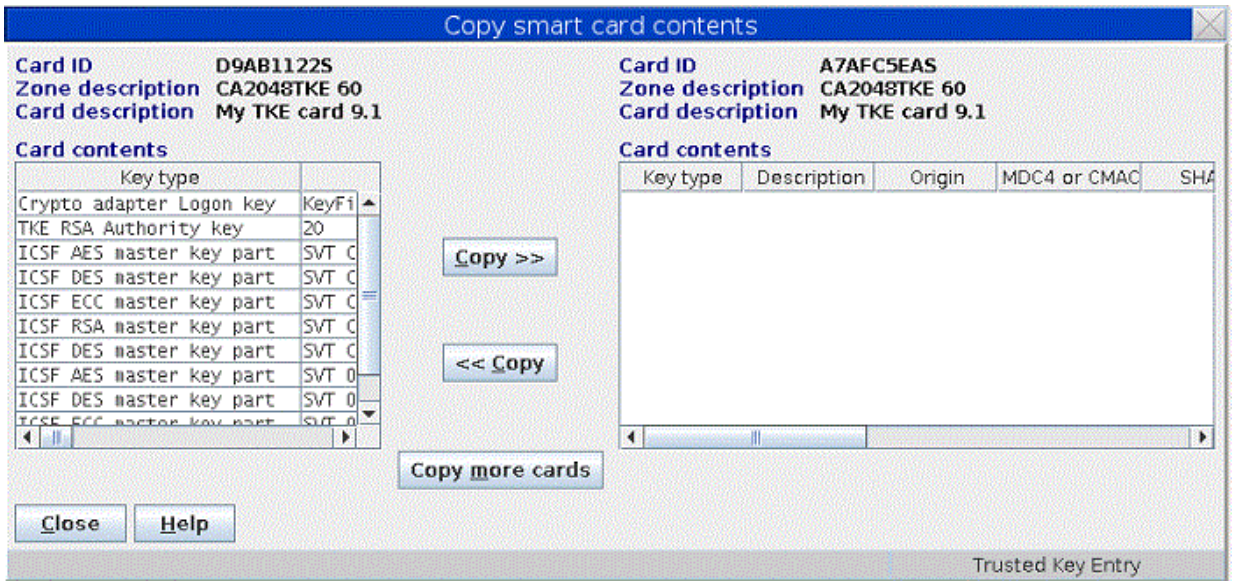


Figure 74. Select keys to copy

5. At the prompts, enter the PINs for the smart cards on the smart card reader PIN pads. The keys are then copied to the target smart card. The target smart card contents panel is refreshed.

Note: You can display the key attributes that are associated with an AES non-DATA operational key part that is stored on either the source or target TKE smart card. Right-click on the wanted key part to display a pop-up menu. Select the **Display key attributes** option to display the key attributes.

Copy key part from binary file to smart card

The Copy binary file key part utility allows a TKE application user, with the proper role, to copy a key part from one or more binary files to a smart card for secure storage. The user is then given the opportunity to delete the binary files after the copies are complete.

A user is allowed to use this feature if their TKE local adapter profile has a role that includes the Copy binary file key part to smart card Access Control Point (ACP 1011). If the role does not have this ACP, the feature is greyed out and cannot be selected.

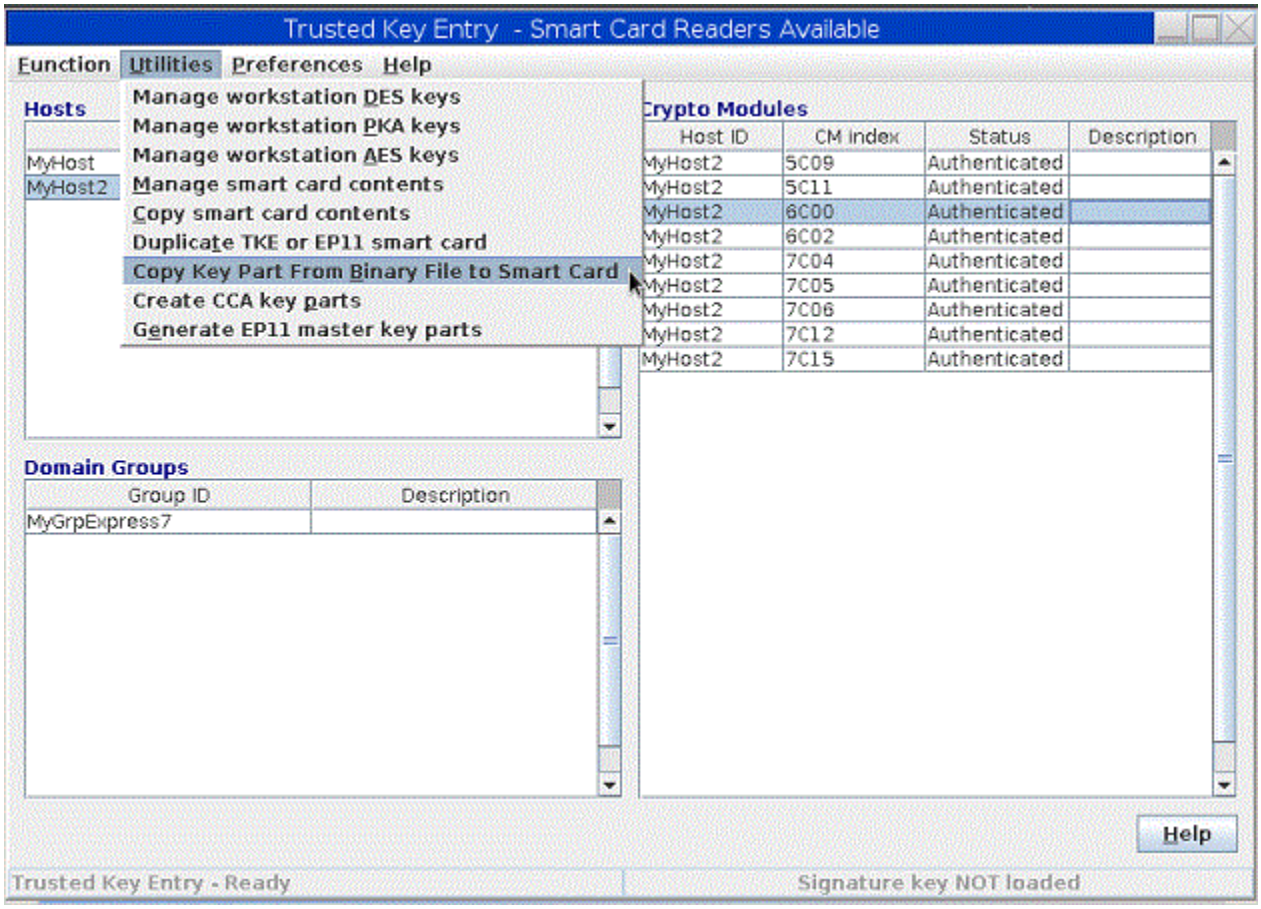


Figure 75. Copy binary file key part utility

Create CCA key parts

The Create CCA key parts utility allows for the creation of CCA key parts outside of a host crypto module. This utility has similar behavior to key part creation inside of a host, but without the ability to load the key parts onto the host.

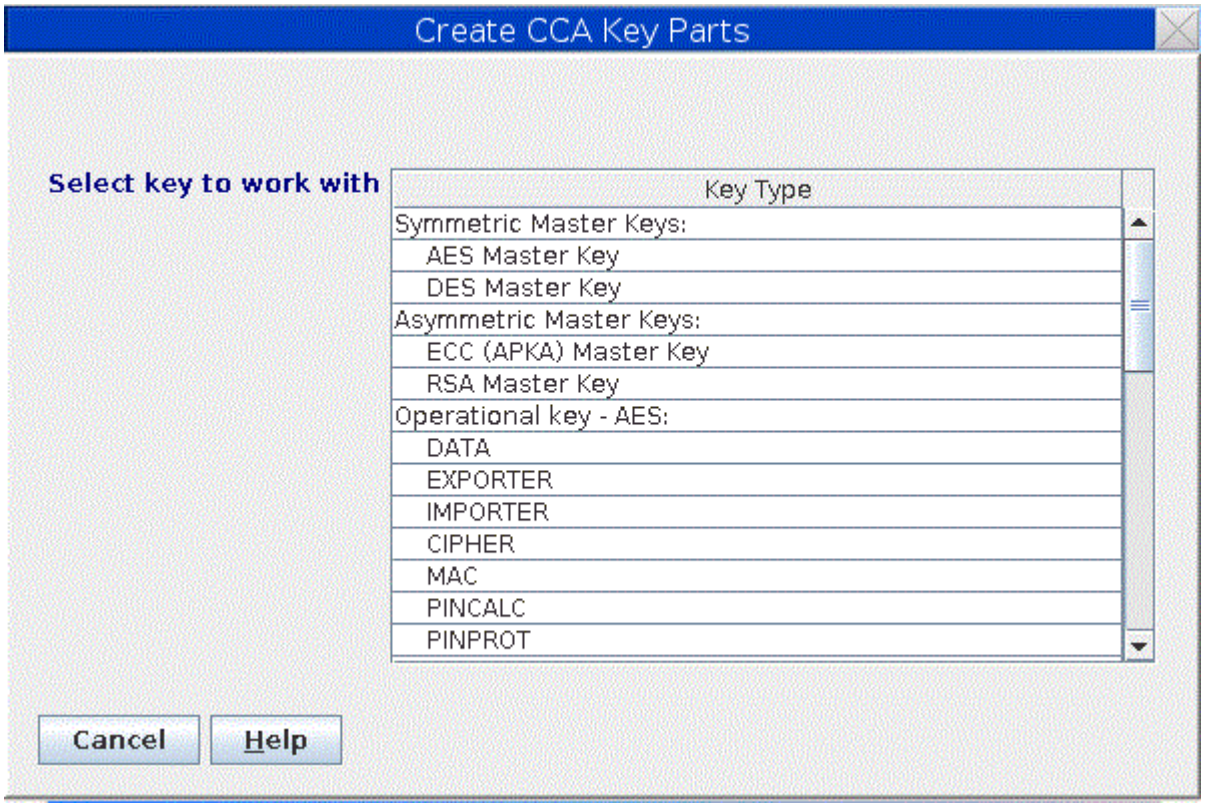


Figure 76. Create CCA key parts

Duplicate TKE and EP11 smart card

The Duplicate TKE or EP11 Smart Card feature allows you to delete existing content from a target smart card and then copy data from a source smart card to the target smart card. Once the duplicate feature has determined you can copy the contents of a source smart card to a target smart card, there are two types of duplicate functions that you can do:

Duplicate an entire smart card
: The target smart card becomes a complete copy of the source smart card. All the current content of the target smart card is deleted and then all the content of the source smart card is copied to the target smart card.

Only duplicate master and operational key parts
: Any signature keys that are on the target smart card stay on the target smart card. Only the current master and operational key parts on the target smart card are deleted and then all of the master and operational key parts from the source smart cards are copied to the target smart cards.

Note: You can only use the duplicate feature if the target smart card is at the same or newer applet version as the source smart card and the primary zone of the source smart card matches the primary or alternate zone of the target smart card.

Generate EP11 master key parts

The Generate EP11 master key parts utility allows for the creation of EP11 key parts outside of a host crypto module. You must have smart cards that are enabled and EP11 smart cards that are already initialized to use this utility. This utility has similar behavior to key part creation inside of a host, but without the ability to load the key parts onto the host.

TKE customization

After installation of the TKE workstation, the following parameters can be customized by using the TKE Preferences menu.

Blind Key Entry
Controls whether key values entered at the TKE keyboard are displayed or hidden. With hidden entry, a * character is displayed for each entered hexadecimal character.

Ensure the menu item is checked if you want hidden entry; otherwise uncheck the menu item.

Removable Media Only
Limits file read and write operations to removable media only.

When unchecked, the TKE data directory on the TKE local hard drive can also be used for file read and write operations.

Enable Tracing
Activates the trace facility in TKE. The output can be used to help debug problems with TKE. Do not check this menu item unless a service representative instructs you to do so.

When checked, TKE produces a trace file named `trace.txt` in the TKE Data Directory. Every time TKE is restarted, the `trace.txt` file is overwritten and a new file is created.

Enable Smart Card Readers
Enables the smart card option for TKE.

If the menu item is unchecked, TKE will remove or gray out menu options that require the use of smart cards.

Note: When the TKE workstation crypto adapter is initialized for smart card use, this option is automatically selected.

Chapter 7. Using the Crypto Module Notebook to administer CCA crypto modules

The Crypto Module Notebook is the central point for displaying and changing all information that is related to a crypto module. It is used for single crypto modules as well as for domain groups. The contents of some of the pages will vary depending on whether you selected a single crypto module or a domain group.

The TKE Main Window lists the crypto modules available on each host machine to which the TKE Workstation is connected and also lists any crypto module groups and domain groups you have created. Double-clicking on a single crypto module or domain group in the TKE Main Window opens the Crypto Module Notebook, which enables you to work with the selected crypto module or domain group. There are two versions of the Crypto Module Notebook — one for CCA crypto modules (CEX2C, CEX3C, CEX4C, CEX5C, CEX6C, and CEX7C) and one for EP11 crypto modules (CEX4P, CEX5P, CEX6P, and CEX7P).

This topic describes how to use the Crypto Module Notebook for CCA crypto modules. For information on how to use the Crypto Module Notebook for EP11 crypto modules, refer to Chapter 8, “Using the Crypto Module Notebook to administer EP11 crypto modules,” on page 209.

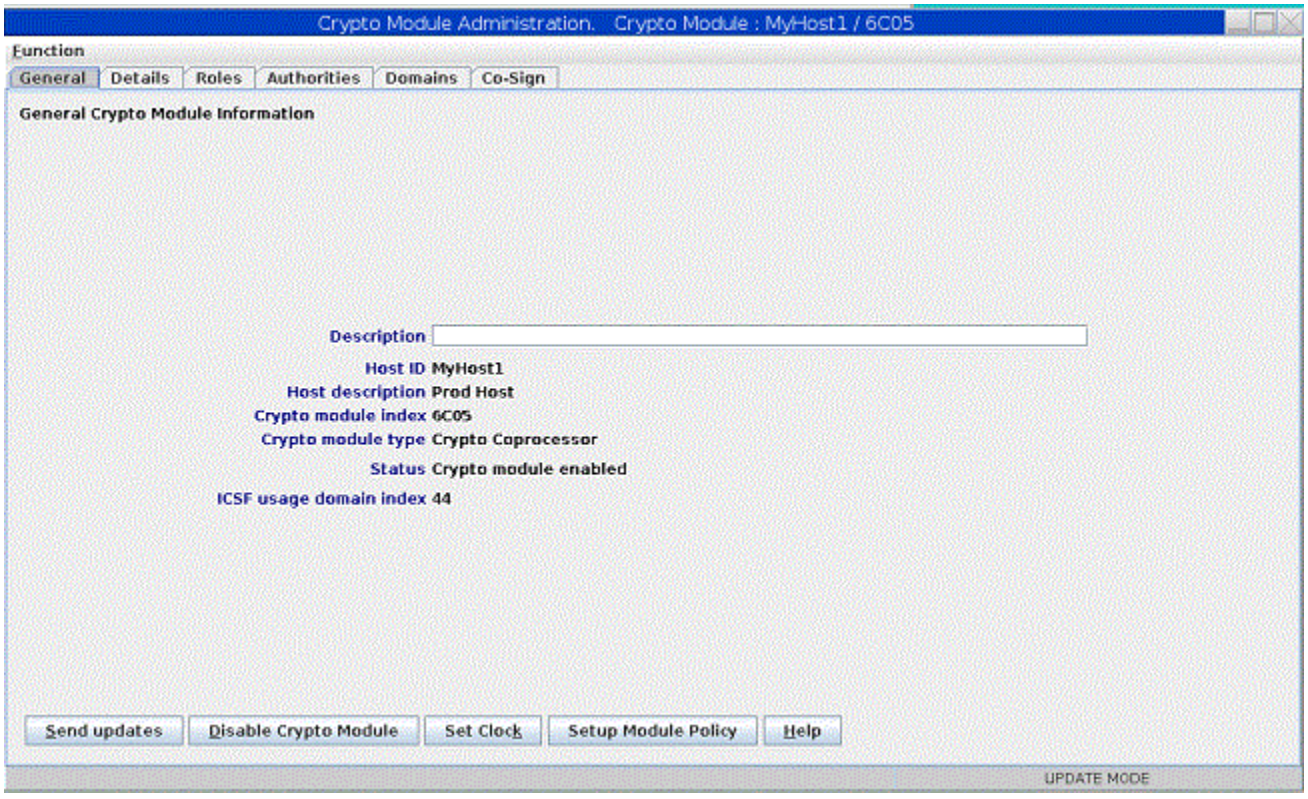


Figure 77. Crypto Module Notebook for CCA - General Page

Notebook mode

The notebook is opened in one of four possible modes:

- **UPDATE MODE**
- **READ-ONLY MODE**
- **PENDING COMMAND MODE**
- **LOCKED READ-ONLY MODE** - group notebooks only

The mode is displayed in the lower-right corner on all of the Crypto Module Notebook pages.

© Copyright IBM Corp. 2000, 2021

In **UPDATE MODE**, you are able to display crypto module information and to perform updates to the crypto module.

In **READ-ONLY MODE**, you are able to display crypto module information but not update it.

In **PENDING COMMAND MODE**, a command is waiting to be co-signed. A multi-signature command issued by an authority, but not yet executed, is called a pending command. You must perform the co-sign. You cannot issue other commands in this mode. For information about co-signing a pending command, refer to "Crypto Module Notebook Co-Sign tab" on page 196.

In **LOCKED READ-ONLY MODE**, you are able to display crypto module information for the master module and to compare the reduced group of crypto modules. You are not allowed to do updates. TKE was not able to access one or more crypto modules of the group or domain group.

Crypto Module Notebook function menu

The selections under the **Function** pull-down menu are:

- **Refresh Notebook** - The content of the notebook is refreshed by reading information from the host. Be aware that performing a refresh may change the mode of the notebook.
- **Load Signature Key** - For more information, see "Load signature key" on page 122.
- **Unload Signature key** - For more information, see "Unload signature key" on page 124.
- **Release Crypto Module** - A window displays the user ID that currently has this crypto module open. This selection releases the crypto module from the update lock. This selection is only active if the notebook is in read-only mode.

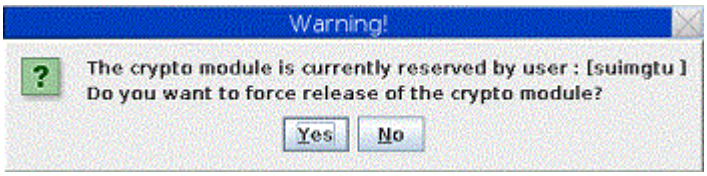


Figure 78. Window to Release Crypto Module

You can confirm release of the crypto module by pressing **Yes**.

Attention: Releasing a crypto module can damage an on-going operation initiated by another authority. Use this option only if you are certain that the crypto module must be released.

- **Display Crypto Module Settings** - This produces a summary report of how the crypto module is configured, which can include what roles and authorities are defined, the master key register status and hash values for each domain, the domain control settings for each domain, and other information. You are asked to select what information to collect and display.

  The information is displayed on a new panel with tabs for each of the selected categories. A **Save** button allows you to save the information in a file, and a **Print** button allows you to print the information.

  In a domain group notebook, the displayed information is for the crypto module containing the master domain.
- **Display Domain Mode States** - This produces a summary report of the states of all the domains on a crypto module or in a domain group. The summary shows the mode of each domain, and for domains that are not in normal mode, the number of audit log entries that have not been downloaded to the file.
- **Compare Group** - This selection is only displayed if working with a domain group. For more information, see "Comparing groups" on page 121.
- **Compare Group (Same Domain Index)** - This selection is only displayed if working with a domain group. For more information, see "Comparing groups" on page 121.
- **Compare Group (Module-wide Only)** - This selection is only displayed if working with a domain group. For more information, see "Comparing groups" on page 121.
- **Close** - This selection closes the Crypto Module Notebook.

Tabular pages

For the host cryptographic modules, the tabular pages available are:

- **General:** see "Crypto Module Notebook General tab" on page 139.
- **Details:** see "Crypto Module Notebook Details tab" on page 141.
- **Roles:** see "Crypto Module Notebook Roles tab" on page 142.
- **Authorities:** see "Crypto Module Notebook Authorities tab" on page 146.
- **Domains:** see "Crypto Module Notebook Domains tab" on page 155.
- **Co-sign:** see "Crypto Module Notebook Co-Sign tab" on page 196.

The notebook opens to the **General** tab.

Crypto Module Notebook General tab

The contents of the Crypto Module Notebook General tab are:

- Description

  An optional free text description that is displayed in the crypto module container at the main window. This description is saved in the crypto module data set specified in the TKE host transaction program started procedure on the host. To change the description, edit the field contents and press **Send updates**.
- Host ID
- Host Description
- Crypto Module Index

  Identifies the crypto module type and installed location on the host system. The last two characters can range from 00 to 63. For more information, see "Host crypto module index values" on page 196.

  Together with the crypto module type, the index uniquely identifies the crypto module within a host. The index value is 00 through 63.
- Crypto Module Type
- Status

  A crypto module is either enabled or disabled. When a crypto module is enabled, it is available for processing. You can change the status of the module by pressing the **Enable Crypto Module / Disable Crypto Module** push button. **Enable Crypto Module** is a dual-signature command and another authority may need to co-sign. **Disable Crypto Module** is a single signature command.

  Disabling a crypto module disables all the cryptographic functions for a single crypto module, a group of crypto modules, or a domain group. This disables the crypto module for the entire system, not just the LPAR that issued the disable.
- ICSF usage domain index

  The usage domain on the crypto module where the TKE host transaction program is running. The usage domain is also indicated by an asterisk on one of the numbered domain tabs when these are displayed in the notebook.

  This field appears only when ICSF FMID HCR77B1 with APAR OA49067, or later, is running in the usage domain.

If you press the **Disable Crypto Module** button, a series of windows opens. You are asked if you are sure that you want to disable the module, and are then notified if the command runs successfully. If the authority signature key has not been loaded, you are asked, through a series of windows, to load an authority signature key. Once the module is disabled, the **Enable Crypto Module**/**Disable Crypto Module** button changes from **Disable Crypto Module** to **Enable Crypto Module**.

If you press the **Set Clock** button, a window displays and you are allowed to configure the time on the crypto module. You must have the authority in your role to perform this update.

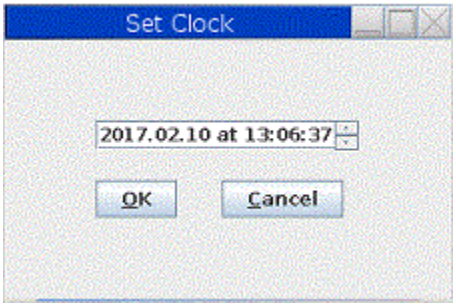


Figure 79. Set clock

If you press the **Setup Module Policy** button, you launch a wizard that helps you create a set of host crypto module roles and authorities that your administrators will use when managing module-wide and normal-mode domain specific settings that comply with these rules. The wizard contains online documentation that describes the policies that it implements for you.

Intrusion latch

Under normal operation, a cryptographic card's intrusion latch is tripped when the card is removed. This causes all installation data, master keys, retained keys, roles and authorities to be zeroized in the card when it is reinstalled. Any new roles and authorities are deleted and the defaults are re-created. The setting for TKE Enablement is also returned to the default value of *Denied* when the intrusion latch is tripped.

A situation may arise where a cryptographic card needs to be removed. For example, you may need to remove a card for service. If you do have to remove a card, and you do not want the installation data to be cleared, perform the following procedure to disable the card. This procedure will require you to switch between the TKE application, the ICSF Coprocessor Management panel, and the Support Element.

1. Open an Emulator Session on the TKE workstation and log on to your TSO/E user ID on the Host System where the card will be removed.
2. From the ICSF Primary Option Menu, select Option 1 for Coprocessor Management.
3. Leave the Coprocessor Management panel displayed during the rest of this procedure. You will be required to press ENTER on the Coprocessor Management panel at different times. **DO NOT EXIT this panel.**
4. Open the TKE Host where the card will be removed. Open the crypto module notebook and click on the **Disable Crypto Module** push button.
5. After the crypto module has been disabled within TKE, press ENTER on the ICSF Coprocessor Management panel. The status should change to DISABLED.

   Note: You do not need to deactivate a disabled card before configuring it OFFLINE.
6. **Configure Off** the card from the Support Element. The Support Element is a dedicated workstation used for monitoring and operating Z hardware. A user authorized to perform actions on the Support Element must complete this step.
7. After the card has been taken Offline, press ENTER on the Coprocessor Management panel. The status should change to OFFLINE.
8. Remove the card. Perform whatever operation needs to be done. Replace the card.
9. **Configure On** the card from the Support Element. The Support Element is a dedicated workstation used for monitoring and operating Z hardware. A user authorized to perform actions on the Support Element must complete this step.
10. When the initialization process is complete, press ENTER on the Coprocessor Management panel. The status should change to DISABLED.

11. From the TKE Workstation Crypto Module General page, click on the **Enable Crypto Module** push button.
12. After the card has been enabled from TKE, press ENTER on the Coprocessor Management panel. The Status should return to its original state. If the Status was ACTIVE in step 2, when the card is enabled it should return to ACTIVE.

All installation data, master keys, retained keys, roles, and authorities should still be available. The data was not cleared with the card removal because it was disabled first using the TKE workstation.

Crypto Module Notebook Details tab

The Details tab contains five pages, two for crypto modules and three for crypto module and diagnostic information. These five pages are accessible through tabs found on the right side of the Details tab screen. To view these pages, click on the corresponding tabs. The pages and their contents are:

- **Crypto Module:** Shows basic information needed to recognize a host crypto module. Different information is displayed, depending on the crypto module type. The following fields may be displayed on this page:
  - **Crypto Module ID** - Unique identifier burned into the crypto module during the manufacturing process.
  - **Public Modulus** - For crypto modules with an RSA OA signature key, the modulus of the key. TKE uses the public key to verify signed replies from the host crypto module.
  - **Modulus Length** - For crypto modules with an RSA OA signature key, the length of the modulus, in bits.
  - **ECC Public Key** - For crypto modules with an ECC OA signature key, the ECC public key.
  - **Key Identifier** - The SHA-256 hash over the public part of the OA signature key. For RSA keys, the hash is over the DER-encoded modulus and public exponent. For ECC keys, the hash is over the ECC public key.
  - **Signature Sequence Number** - Each signed reply from the crypto module contains a unique sequence number; the current value is displayed.
  - **Hash pattern of transport key** - For CEX2C crypto modules, the MDC-4 hash value of the current Diffie-Hellman generated triple-DES transport key for the crypto module. For later crypto modules, the first 16 bytes of the SHA-256 hash value of the current Diffie-Hellman generated AES transport key.
- **Crypto Services (Function Control Vector Values)**
  - Base CCA services availability
  - CDMF availability
  - 56-bit DES availability
  - Triple DES availability
  - 128-bit AES availability
  - 192-bit AES availability
  - 256-bit AES availability
  - SET services
  - Maximum length of RSA keys used to encipher DES keys
  - Maximum elliptic curve field size in bits for key management
- **Other CM Info** - The following crypto module information is displayed:
  - CCA Version
  - CCA Build Date
  - DES Hardware Level
  - RSA Hardware Level

  - Power-On Self Test Version (0,1,2)
  - Operating System Name
  - Operating System Version
  - Part Number
  - Engineering Change Level
  - Miniboot Version (0,1)
  - Adapter ID
  - Processor Speed
  - Flash Memory Size
  - Dynamic RAM Memory Size
  - Battery-Backed Memory Size
- **Diagnostic Info** - The following diagnostic information is displayed:
  - Intrusion Latch
  - Battery State
  - Error Log Status
  - Command Information
- **Dual Validation** - This tab validates that the host crypto co-processor code load has not been tampered with. This is done by retrieving the data in two different ways and comparing the results. If the two results are identical, then there are no signs of tampering.

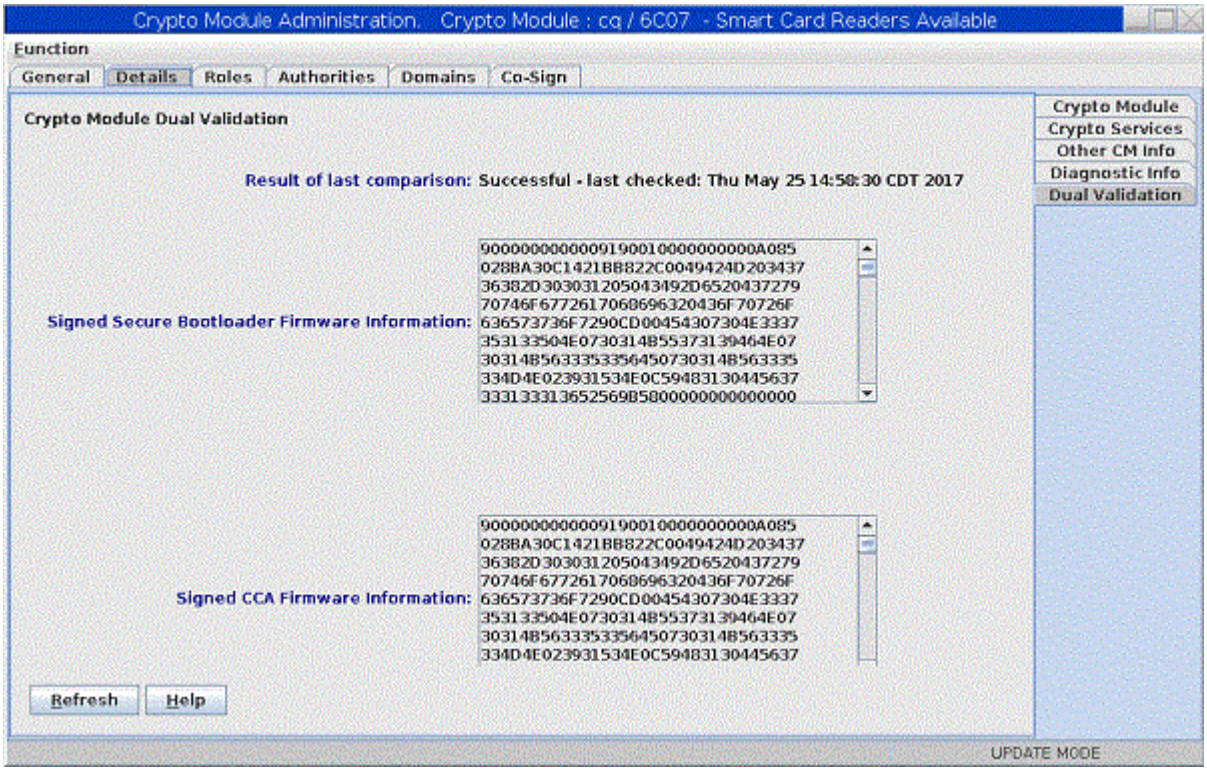


Figure 80. Dual Validation

The settings in the Crypto Module Details tab are loaded during crypto module initialization.

Crypto Module Notebook Roles tab

CCA crypto modules use role-based authority. Each authority has an associated role. This role indicates what operations the authority is permitted to execute and what domains on the crypto module the authority is permitted to change.

With role-based authority, a set of roles can be defined that correspond to different classes of coprocessor users. For example, one class of users might be permitted to access only test domains, while another class of users might be permitted to access production domains. One class of users might be permitted to perform only key operations, while another class of users might be permitted only to change domain controls.

For key operations, further granularity is possible, with separate controls for loading first, middle, and final key parts, and for setting, completing, and clearing keys. Permission to execute these operations can be assigned to different roles, implying that multiple users are needed to manage keys. Or, one role can indicate permission to execute them all.

You can create, change, and delete roles from the **Roles** tab.

INITADM is a pre-defined role available on coprocessors that are shipped with the system, or after segments 2 and 3 of the coprocessor are zeroized and unowned (ownership surrendered) and then reloaded. It is assigned to authority 00. It allows you to create an initial set of roles and authorities on the crypto module. After you create these initial roles and authorities, you can choose to delete authority 00 or to assign a different role to it.

Dual-signature commands

To complete some commands, two authority signatures are required. For these commands there are two entries in the Role Access Control Points tree, one indicating issue authority and one indicating co-sign authority. If a role contains both permissions, both signatures are collected automatically when an authority with that role is used to execute the command. If an authority with a role containing only issue authority is used to execute the command, the command is held in a pending command buffer until a signature is collected from a second authority whose role contains the co-sign permission.

When working with a single crypto module, use the **Co-Sign** tab in the notebook to collect the second signature for the command. When working with a domain group, a window opens asking you to co-sign the command.

Domain access

When you work with a role by using a crypto module notebook, the Role Access Control Points tree contains a Domain Access category that allows you to specify what domains the role gives permission to change.

When you work with a role by using a domain group notebook, the Role Access Control Points tree does not include a Domain Access category. Instead, three Domain Access options are displayed:

- **Set all Domain Access control points**
- **Set Domain Access control points from group definition**
- **Clear all Domain Access control points**

Selecting the first option causes the role to allow access to all domains on the crypto module, whether or not the domain is a member of the domain group.

Selecting the second option causes the role to allow access only to those domains on the crypto module that are members of the domain group. If the domain group includes domains on more than one crypto module, the Domain Access values can be different on different crypto modules. For example, if the domain group includes domains 0, 1, and 2 on crypto module A and domains 3, 4, and 5 on crypto module B, the role on crypto module A has only domains 0, 1, and 2 set in the Domain Access category, and the role on crypto module B has only domains 3, 4, and 5 set.

Selecting the third option causes the role to remove all domain access to all domains on the crypto module, whether or not the domain is a member of the domain group. Select this option when the role does not have any access control points that require access to domains. A role does not need any domain access if it includes only access control points from these categories:

- Crypto Module Enable
- Access Control

- Configuration Migration

Creating or changing a role

When you right-click in the Roles tab container, a menu opens and you can select **Create Role**, **Change Role**, **Delete Role**, **View Role**, or **Guided Create Roles**.

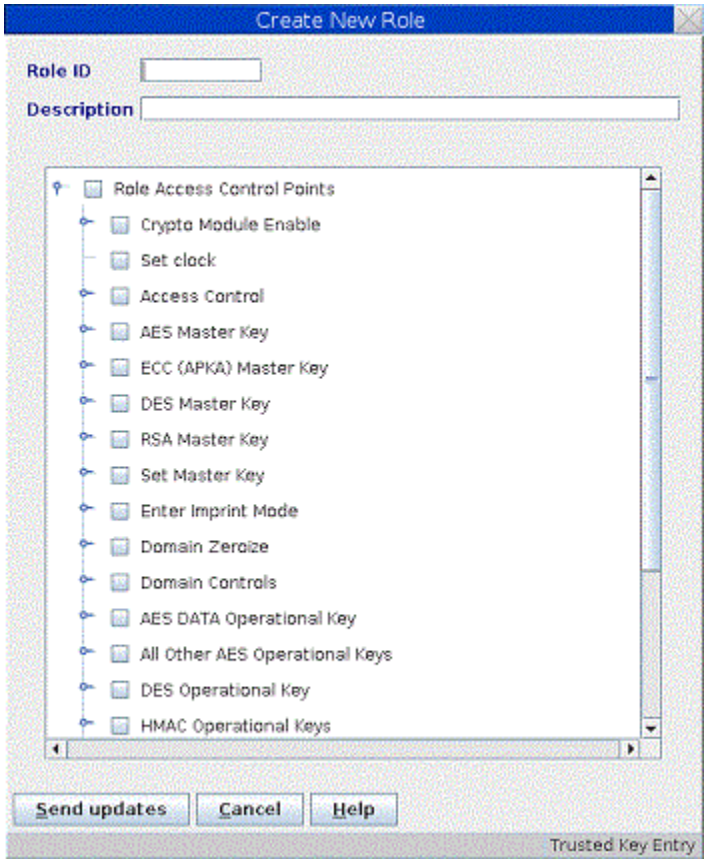


Figure 81. Create New Role page

If you select **Create Role** or **Change Role** from the menu, a window opens displaying the following fields and elements:

- **Role ID**: Enter the Role ID. If you are creating a new role, you must enter a name for that role. If you are changing a role, you cannot change this field.
- **Description** : Optional free text description.
- Tree structure and check boxes: This pane shows the operations and domains that can be allowed or restricted by the role. Figure 81 on page 144 shows the list of categories. Each category can be expanded to show a list of operations or domains. A check mark indicates that the operation or access to the domain is permitted. The absence of a check mark indicates that the operation or access to the domain is not permitted.

  The Access Control category controls whether an authority can create, change, and delete roles and authorities.

  Dual-signature commands have entries for issue and co-sign authority.

Some categories in the Role Access Control Points tree are not shown if the crypto module does not support the operations in that category. For example, the ECC (APKA) Master Key category is not displayed for crypto modules that do not support ECC (APKA) master keys.

After you complete the fields on the panel and select the operations and domains to be permitted for the role, click **Send Updates** to create or change the role.

Deleting a role

To delete a single role, right-click on the wanted role to display a menu. Select **Delete Role** from the menu. To delete multiple roles at the same time, highlight all the roles that you want to delete. By holding down the control button on the keyboard, you can select specific entries on the list with your mouse. By holding down the shift button on the keyboard, you can select a specific range of entries on the list with your mouse. Right-click on one of the highlighted entries and select **Delete Role** from the menu. You are prompted to confirm that you want to delete the previously selected number of roles.

You are not allowed to delete a role if it is assigned to one or more authorities. You are only allowed to delete unused roles.

View a role

To view a single role, highlight the role and right-click for options. Select **View Role**. You can examine the settings of the role, but you cannot change them.

Using Guided Create Roles

To use the **Guided Create Roles** process, right-click to display the menu. Select **Guided Create Roles**.

Note: Informational dialogs will appear during the process to help describe each step as it occurs.

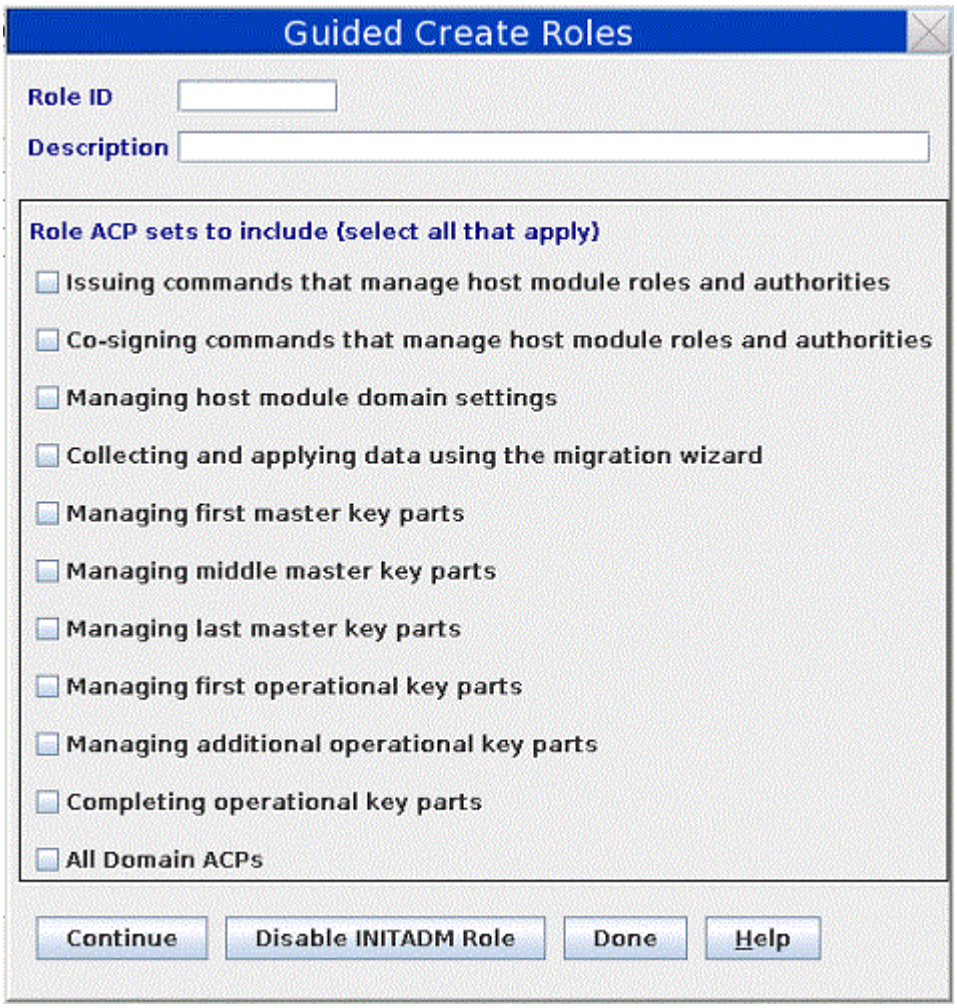


Figure 82. Guided Create Roles page

The **Guided Create Roles** window contains the following elements:

Role ID
You have the option to fill in the name of the new role you are creating on the **Guided Create Roles** window.

Description
You have the option to fill in the description of the new role you are creating on the **Guided Create Roles** window.

Role ACP sets to include
A set of check boxes that describe commonly used sets of ACP choices for role creation. Multiple check boxes can be selected. When more than one check box is selected, the ACPs from all selected sets will be set ON when the **Create New Role** panel is brought up later in the **Guided Create Roles** process. The following check boxes are provided:

- Issuing commands that manage host module roles and authorities.
- Co-signing commands that manage host module roles and authorities.
- Managing host module domain settings.
- Collecting and applying data using the migration wizard.
- Managing first master key parts.
- Managing middle master key parts.
- Managing last master key parts.
- Managing first operational key parts.
- Managing additional operational key parts.
- Completing operational key parts.
- All domain ACPs.

The domain selections will not appear when processing a domain group.

Once you have selected all of the ACP sets that you wish to include in the role, press the Continue button to proceed with role creation.

The **Create New Role** panel is displayed with the ACP choices that were chosen on the **Guided Create Roles** panel.

Setup Module Policy

This option launches a wizard that helps you create a set of host crypto module roles and authorities that your administrators will use when managing module-wide and normal-mode domain specific settings that comply with these rules. The wizard contains online documentation that describes the policies that it implements for you.

Crypto Module Notebook Authorities tab

An authority is a person who is able to issue signed commands to the crypto module. For each of the currently defined authorities, this container lists the name, index, and other authority information.

When you right-click in the Authorities container, you can:

Create Authority
Upload the public part of the authority signature key and the authority information for the selected crypto module or group of crypto modules.

Change Authority
Display and edit the authority-related information for the selected crypto module or group of crypto modules.

Delete Authority
Delete the authority-related information for the selected crypto module or group of crypto modules.

View Authority
View the authority-related information for the selected crypto module or group of crypto modules.

Generate Signature Key
Generate a signature key for an authority and save it on a selected medium together with authority-related information (name, telephone number, and so on).

Guided Create Authorities
Generate signature keys and carry them forward into the creation of authorities in a guided process.

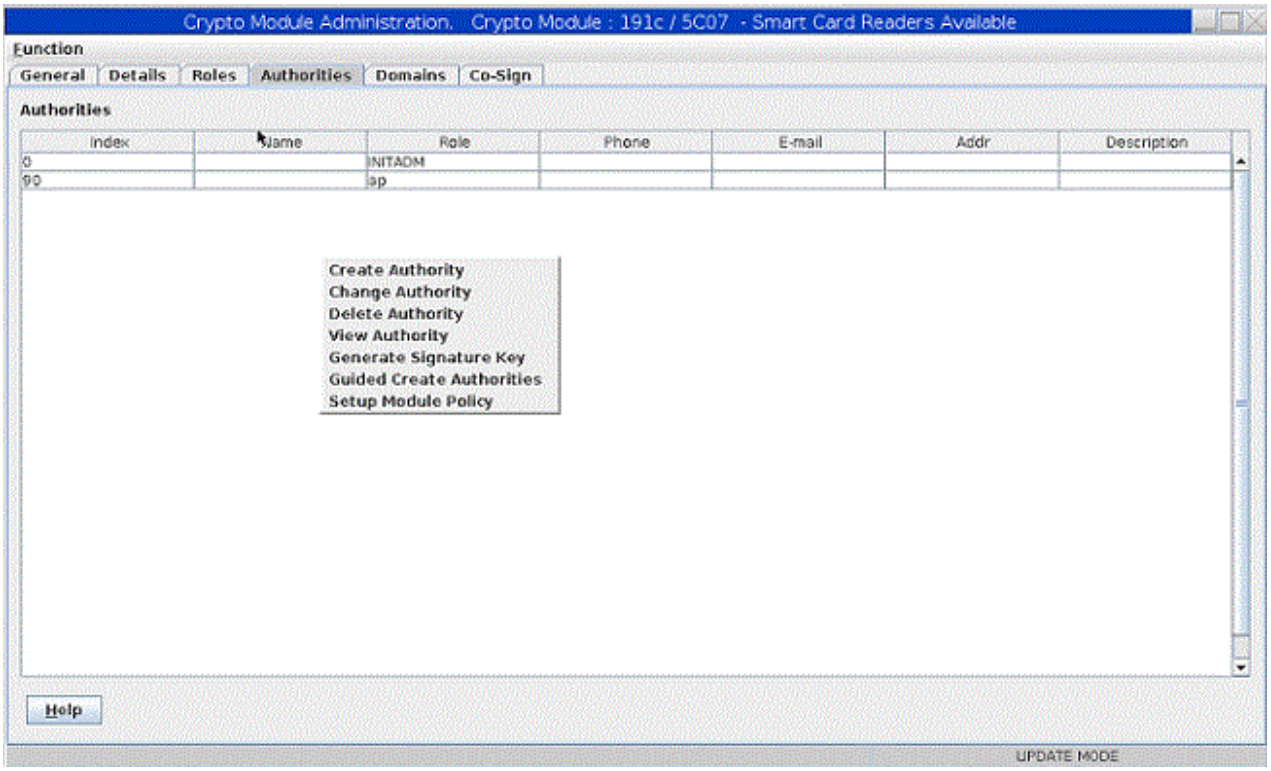


Figure 83. Authorities Page

Generating authority signature keys

You generate and save an authority signature key by right-clicking in the Authorities container and selecting the *Generate Signature Key* action.

The Generate Signature Key window is displayed.

Follow this procedure:

1. Enter **Authority index**. This is a mandatory field with the index of the authority. Valid range is 00 through 99. The authority index is saved with the key and is called the Default Authority index. The Default Authority index for a saved authority signature key can be overridden when the authority signature key is loaded.
2. Enter information about the authority by using one of the following two common practices:
   - Enter **Name**, **Phone**, **E-mail**, **Address**, and **Description** to identify the authority to a person. These are optional free text fields. The information that you enter here is saved with the key. It is filled in automatically when the key is selected for creating a new authority. Press **Continue**.



Figure 84. Completed generate signature key window

- Enter a **Name** that identifies the purpose of the authority. This is the second most common practice because associating a card to a person can become hard to maintain, so using the name field as a card identifier might be a better solution for you.

3. Enter **Name**, **Phone**, **E-mail**, **Address**, and **Description** to identify the authority. These are optional free text fields. The information that you enter here is saved with the key. It will be filled in automatically when the key is selected for creating a new authority. Press **Continue**.
4. A **Select Target** dialog box is displayed that allows you to select the target destination for the generated key. Authority signature keys can be saved to a **binary file** or **key storage**, or generated and saved on a **TKE smart card**. Make your selection and press **Continue**.
5. Select the length of the authority signature key you want to generate. The length choices vary depending on the signature key target. If the signature key target is a smart card, you can generate 1024-bit or 2048-bit RSA or BP-320 ECC authority signature keys. BP-320 ECC authority signature keys can only be generated to a TKE smart card with applet version 0.10 or greater. If the signature key target is a binary file or key storage, you can generate 1024-bit, 2048-bit, or 4096-bit RSA authority signature keys.
6. If the authority signature key is to be saved to a **binary file**, a password and file name are required to encrypt and save the key file. After you save the authority signature key and information to a binary file or key storage, you are prompted to save the key again. It is not recommended that you save it again.

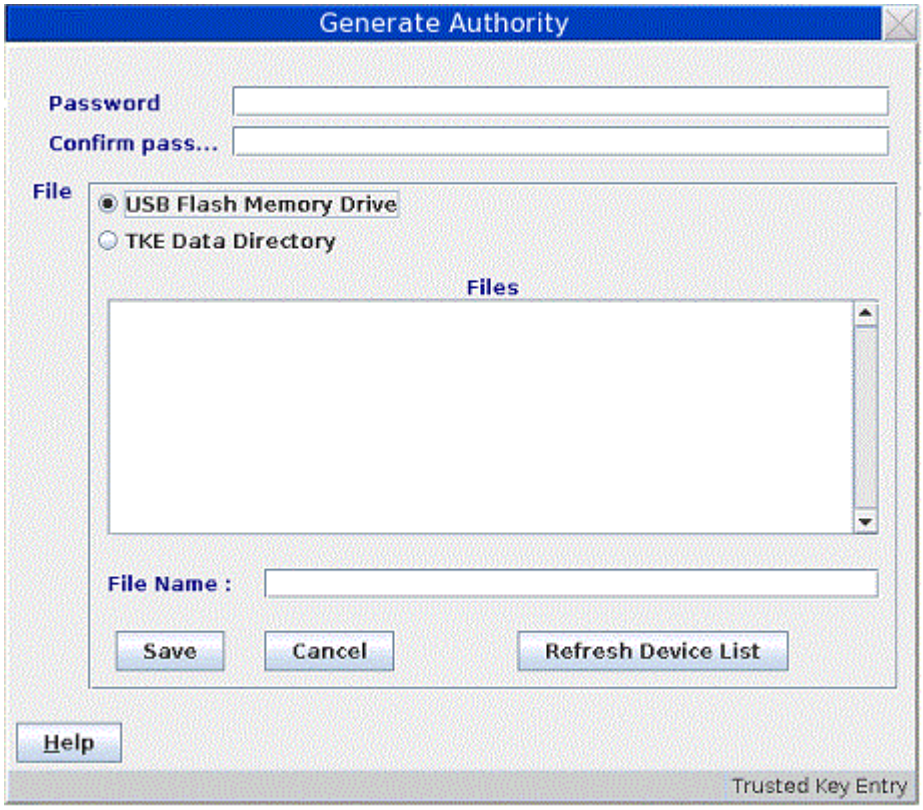


Figure 85. Save authority signature key

Attention : Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages might be generated on the TKE workstation.

7. If the key is to be generated and saved on a **TKE smart card**, a message box displays, prompting you to "Insert TKE smart card in smart card reader 2."
   a. Insert the TKE smart card into smart card reader 2. Press **OK**.
   b. When the authority signature key is generated and saved to a TKE smart card, it is protected by the PIN of the TKE smart card. A message box prompts you to “Enter a 6-digit PIN on smart card reader 2 PIN pad”. Enter the PIN as prompted.

      Note: If the TKE smart card was created on a version of the TKE Workstation before version 7.0, the PIN of the TKE smart card is 4 digits instead of 6 digits.

      The authority signature key is generated on the TKE smart card and a successful message is displayed.



Figure 86. Generate signature key

When generating and saving an authority signature key on a TKE smart card, you are not given the option to save it again. You should use the **Copy smart card contents** utility to save the signature key again. See "Copy smart card contents" on page 131.

Each TKE smart card can hold only one authority signature key.

8. If the keys are to be saved in **Key Storage**, only one authority signature key can be stored in PKA key storage.



Figure 87. Key saved status message

Create authority

This selection allows you to create an authority at the host and select its authority signature key. Before you can create a new authority, you need to generate an authority signature key (see "Generating authority signature keys" on page 147).

To create an authority, click with the right mouse button in the container on the Authorities page. A pop-up menu displays. From this menu, select the **Create Authority** menu item.

The Select Source window opens, enabling you to specify the authority signature key source. Make your selection and press the **Continue** push button.

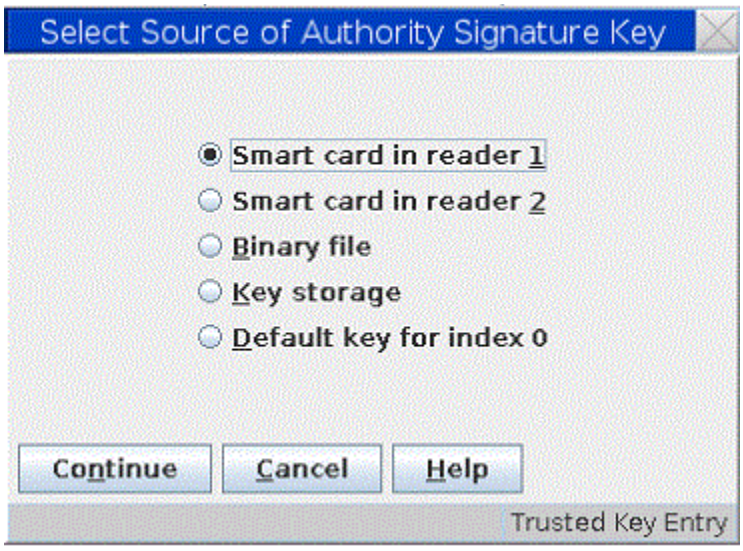


Figure 88. Select source of authority signature key

- If you select **Key storage**, the key and accompanying information from key storage appears in the Create New Authority window.

- If you select **Smart card in reader 1** or **Smart card in reader 2**, you are prompted to insert the TKE smart card into the appropriate reader. Insert the smart card into the reader, and press **OK**.

  Notes:

  – Starting in TKE 7.2, you can have 2, 3, or 4 smart card readers. The number of attached smart card readers is detected when the main TKE application starts and controls the options that are displayed on the panel. If no attached smart card readers are detected, no smart card reader options are displayed.

  – BP-320 ECC authority signature keys may be used only on a CEX5C host crypto module.

  A message box prompts you to enter the TKE smart card PIN. Enter the PIN as prompted.

  After the PIN has been verified, the Create New Authority window opens.

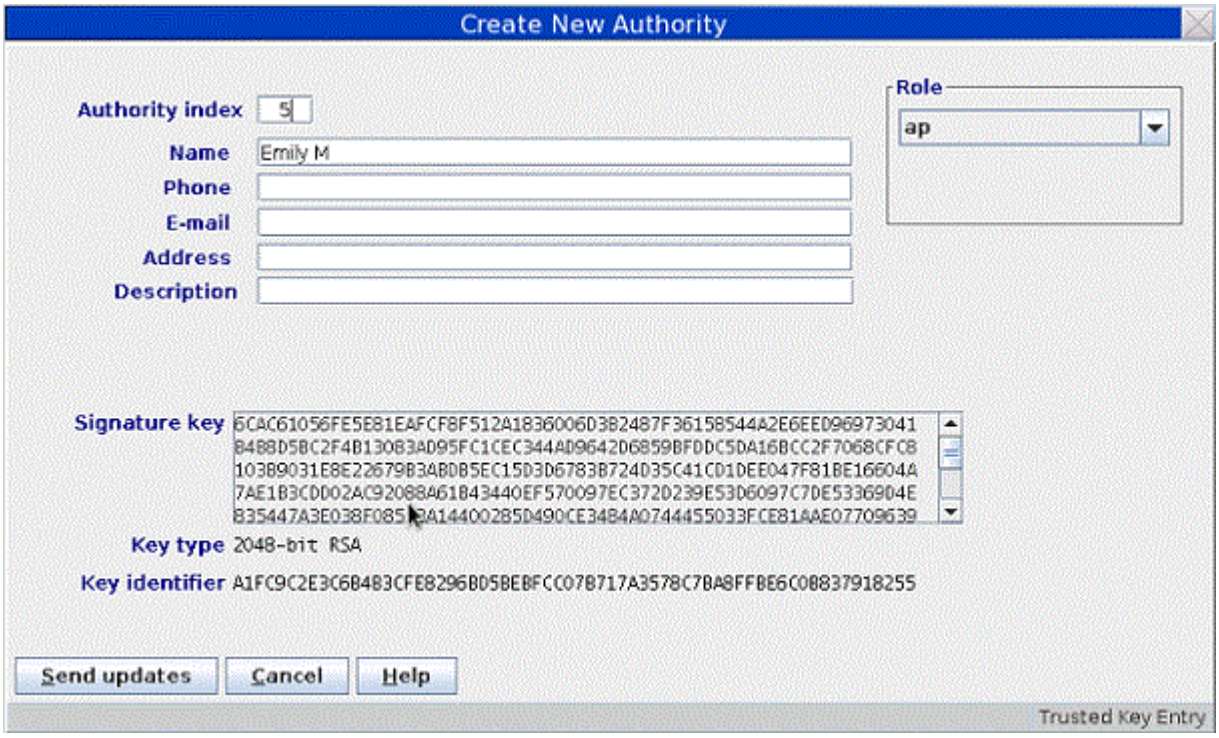


Figure 89. Create new authority

- If you select **Binary file**, the Load Signature Key window is displayed. You are prompted for the signature key file to load and password before the Create New Authority window appears.

  Attention : Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages might be generated on the TKE workstation.

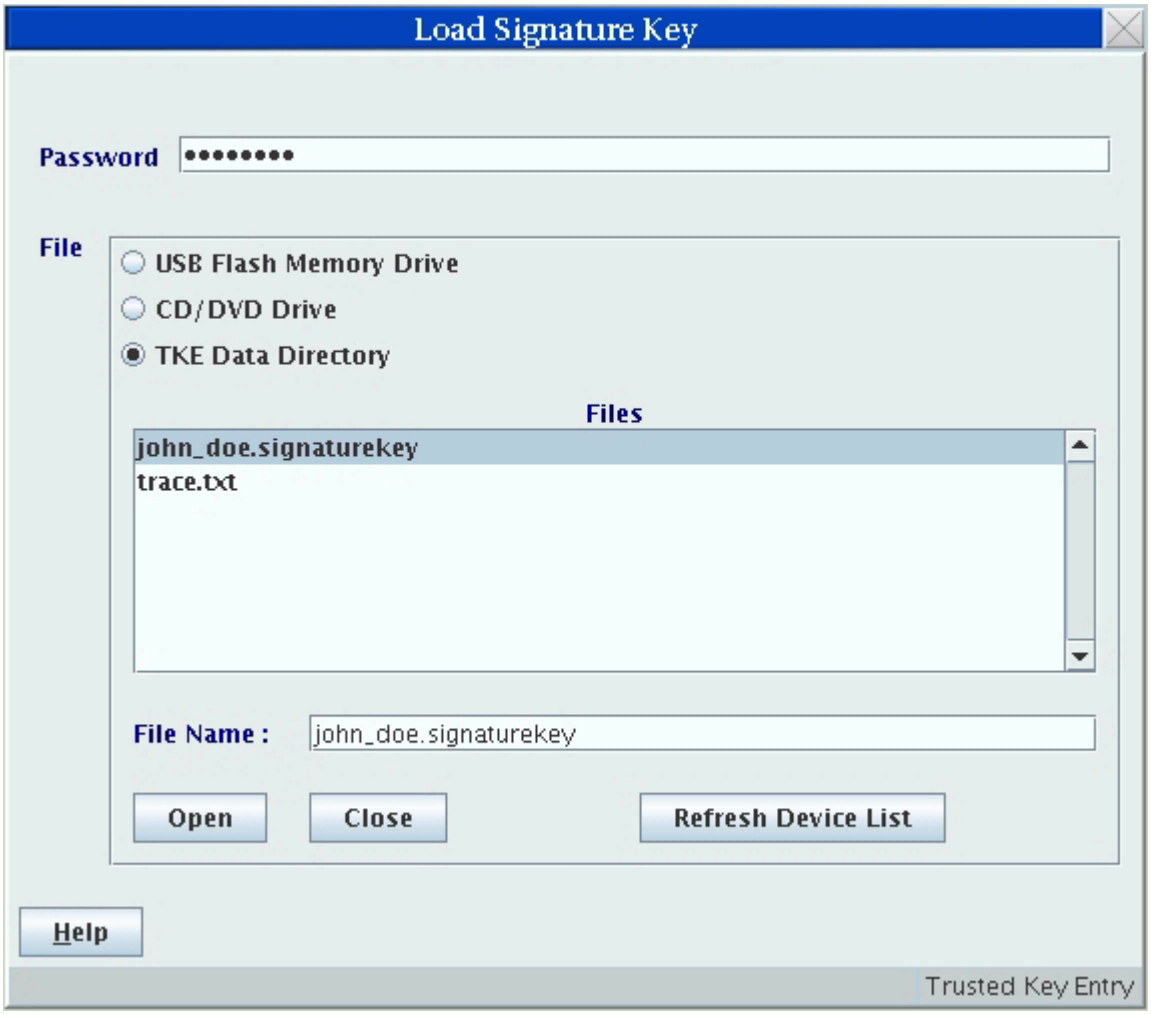


Figure 90. Load Signature Key from binary file

- If you select any **Default key** for options from the Select Source dialog, the word "Default" is automatically placed in the **Name** field of the **Create New Authority** window.

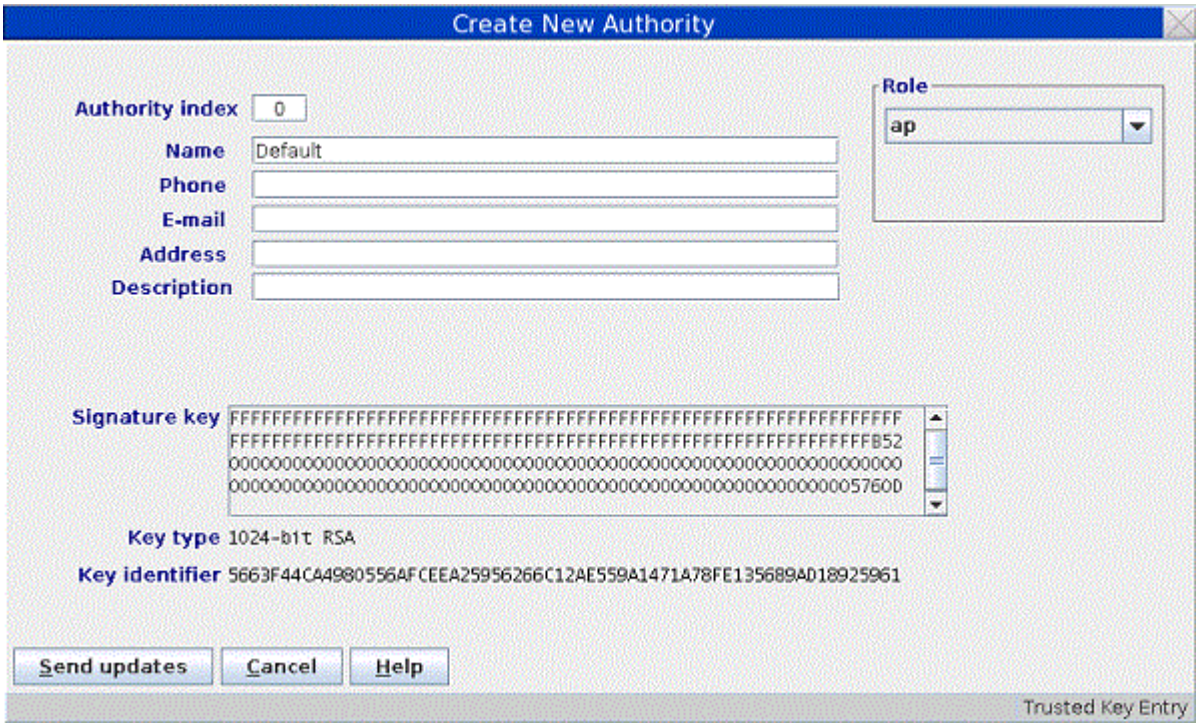


Figure 91. Create New Authority with Role Container

The Create New Authority window is opened with the following authority information that is read from the signature key source:

Authority index
This is a mandatory field with the index of the authority. Valid range for module-wide authorities is 00 through 99.

If the authority signature key is going to be used on several crypto modules, it simplifies matters to use the same authority index for all crypto modules.

Name
Name of the authority. Optional free text entry field.

Phone
Telephone number of the authority. Optional free text entry field.

E-mail
E-mail address for the authority. Optional free text entry field.

Address
Address of the authority. Optional free text entry field.

Description
Description of the authority. Optional free text entry field.

Signature key
Public modulus of the authority signature key.

Key Length
Length of the authority signature key.

Key Identifier
Identifier for the authority signature key that is associated with the authority. The key identifier is the SHA-256 hash of the DER-encoded public modulus and public exponent of the authority signature key.

You can edit all of the entry fields.

In the **Role** container, there is a drop-down list. Select one of the previously defined roles. The authority is mapped to the access rights of that role. This is available only when creating or changing a crypto module authority.

Press **Send updates**. This is a dual signature command. If you do not have both sign and co-sign authority, another authority is required to co-sign.

The authority information (name, telephone, e-mail, and address) is saved in the crypto module data set specified in the TKE host transaction program started procedure on the host.

Change authority

This selection opens the Change Authority window, allowing you to change authority information, change the role, and replace the authority signature key.

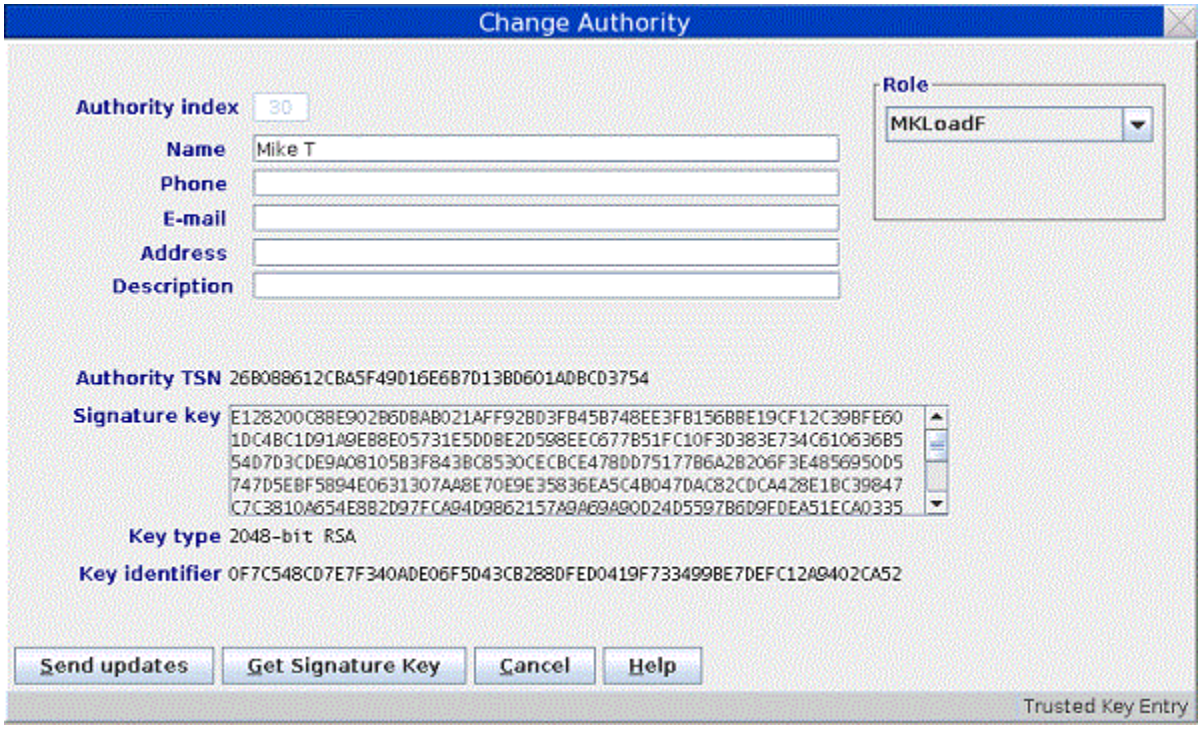


Figure 92. Change Authority

When an authority is selected, you will be able to update the Name, Phone, E-mail, Address and Description fields. You can change the Role definition by clicking on the pull-down menu and selecting a different role. You can change the authority signature key by clicking on **Get Signature Key**.

Get Signature Key opens a Select Source window and a Load Signature Key window. The contents of the selected key file replace the contents of the Change Authority window except for the index.

Send updates uploads the information displayed at the window to the crypto module. The authority information (name, phone, e-mail and address) is updated in the crypto module dataset specified in the TKE host transaction program started procedure on the host.

Delete authority

The supported crypto modules operate with a variable number of TKE authorities (TKEAUTxx profiles). TKE allows a user to delete an authority from a crypto module. TKE performs a consistency check of the resulting TKE roles and profiles to ensure that access to the crypto module is not lost when the profile is deleted.

Using Guided Create Authorities

To use the **Guided Create Authorities** process, right-click to display the menu. Select **Guided Create Authorities**.

Note: Informational dialogs will appear during the process to help describe each step as it occurs.



Figure 93. Guided Create Authorities page

The **Guided Create Authorities** window contains the following elements:

Authority Index
You have the option to fill in the number of a new authority index on the **Guided Create Authorities** window.

Actions to Perform
You can select which actions you wish to perform as part of the **Guided Create Authorities** process. You can select either Generate Signature Key, or Create Authority, or both Generate Signature Key and Create Authority. It is important to note that you must have generated at least one signature key before you can create an authority because the Create Authority process requires a signature key as input.

Once you have chosen whether to specify an authority index or not and selected Generate Signature Key or Create Authority or both Generate Signature Key and Create Authority check boxes, press the Continue button to proceed with the **Guided Create Authorities** process. If it was previously selected, the Generate Signature Key panel will be displayed with the authority index filled in from the **Guided Create Authorities** panel. Once the Generate Signature Key process is completed, the **Guided Create Authorities** process will continue. If Create Authority was previously selected, the Create New Authority panel will be displayed with the authority index used in the Generate Signature Key process already filled in.

Setup Module Policy

This option launches a wizard that helps you create a set of host crypto module roles and authorities that your administrators will use when managing module-wide and normal-mode domain specific settings that comply with these rules. The wizard contains online documentation that describes the policies that it implements for you.

Crypto Module Notebook Domains tab

The Domains tab allows you to work with the domains on the host crypto module. Master keys and operational keys can be loading using the Domains tab and domain control values can be changed.

When the Domains tab is selected, numbered tabs are displayed on the right for each domain that is configured as a control domain on the host system. Up to 85 domain tabs may be displayed, depending on the host system type and the crypto module type that are accessed. When ICSF FMID HCR77B1 with APAR OA49067, or later, runs in the logical partition that services requests from the TKE workstation, the configured usage domain will be indicated by an asterisk on one of these tabs.

In the crypto module notebook for a domain group, numbered tabs for individual domains are omitted and the displayed information is for the master domain. The tab label at the top for a domain group is Domain instead of Domains.

Domain scoped commands issued using a domain group are normally broadcast to all domains in the group. Commands to load and clear operational key registers may optionally be issued to only the master domain. The desired behavior is selected when a CCA domain group is created or changed.

Domain General page

The **Domain General** page opens when you select a domain. By clicking tabs at the bottom of the page, you can work with the domain keys, domain control points, domain decimalization tables, domain restricted PINs, and domain certificates. From the **Domain General** page, you can update the domain description, zeroize the domain, change the default key wrapping methods, and change the mode of the domain.

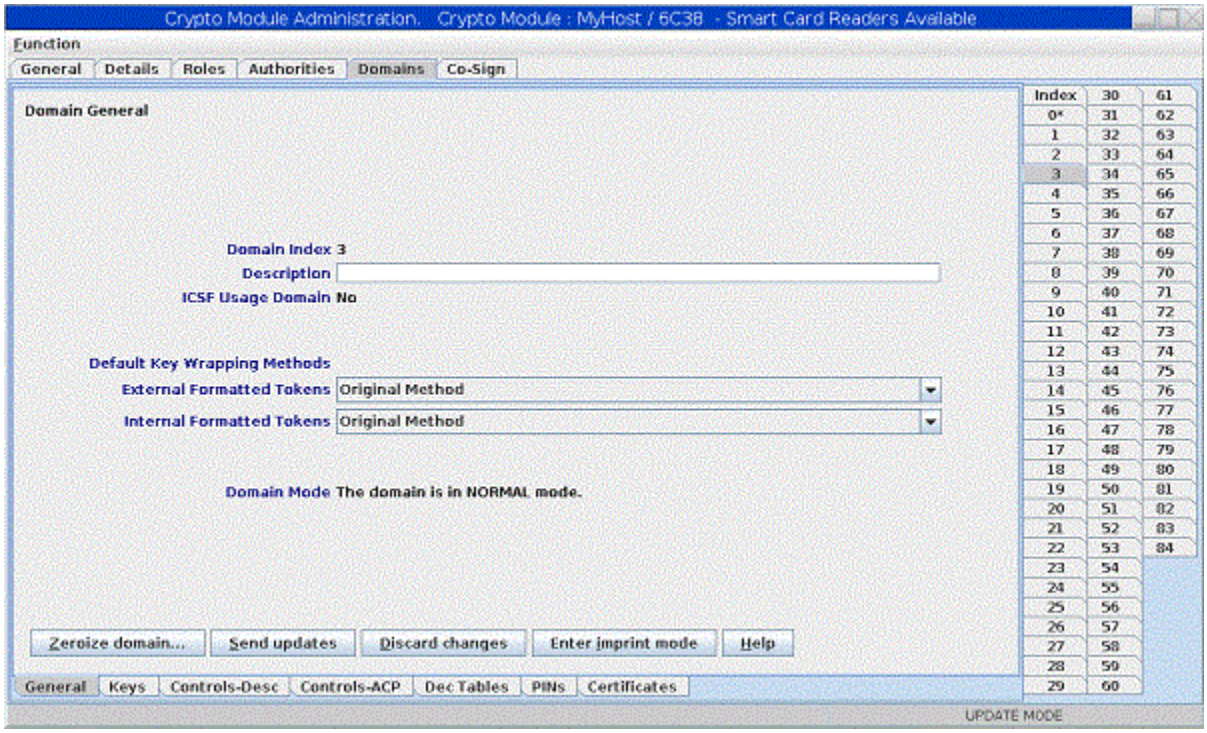


*Figure 94. **Domain General** page - Normal mode*

To change the description, edit the entry field and click **Send updates**. The description is saved in the crypto module data set specified in the TKE host transaction program started procedure on the host.

To change the default key wrapping methods that are used for the domain, select the methods for external and internal formatted tokens and click **Send updates**.

If you click **Discard changes**, any changes that you made on the panel to the domain description or the default key wrapping methods are discarded, and the current values are refetched from the crypto module.

Zeroize domain

Zeroizing a domain erases its configuration data and clears all cryptographic keys and registers for the current domain.

Selecting **Zeroize domain...** results in the display of an action (warning) message. By accepting the message, the domain is zeroized. That is, all registers and keys that are related to this domain are set to zero or set to not valid.

If you are reassigning a domain for another use, it is a good security practice to zeroize that domain before proceeding.

When a domain is zeroized, the domain's controls are reset to their initial state.

Note: Unlike the Global Zeroize issued from the Support Element, Zeroize Domain does not affect the enablement of TKE Commands on the supported crypto modules. Refer to "TKE enablement" on page 11.

Changing domain modes

Beginning with the CEX6C crypto module, a domain can exist in various modes or distinct operational states. The current domain mode is displayed on the Domain General panel.

The Domain General panel includes a button that allows you to change from one mode to another. For a domain in normal mode, an **Enter imprint mode** button is displayed. For a domain in one of the other modes, a **Change mode** button is displayed. Clicking the button causes a secondary panel to be displayed with a set of mode transition options.

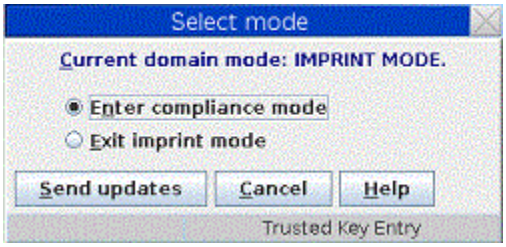


Figure 95. Select mode panel for IMPRINT mode

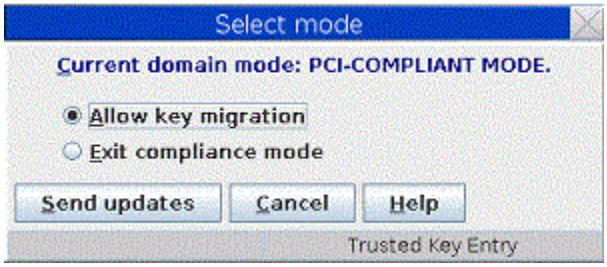


Figure 96. Select mode panel for PCI-COMPLIANT mode

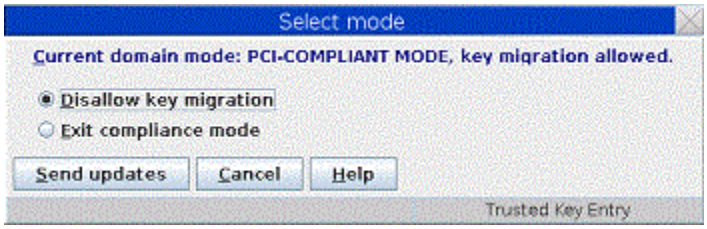


Figure 97. Select mode panel for PCI-COMPLIANT mode, key migration allowed

For a domain in imprint mode or PCI-compliant mode, extra tabs are displayed at the bottom of the crypto module notebook panel that allow you to work with the domain roles, domain authorities, and domain audit log.

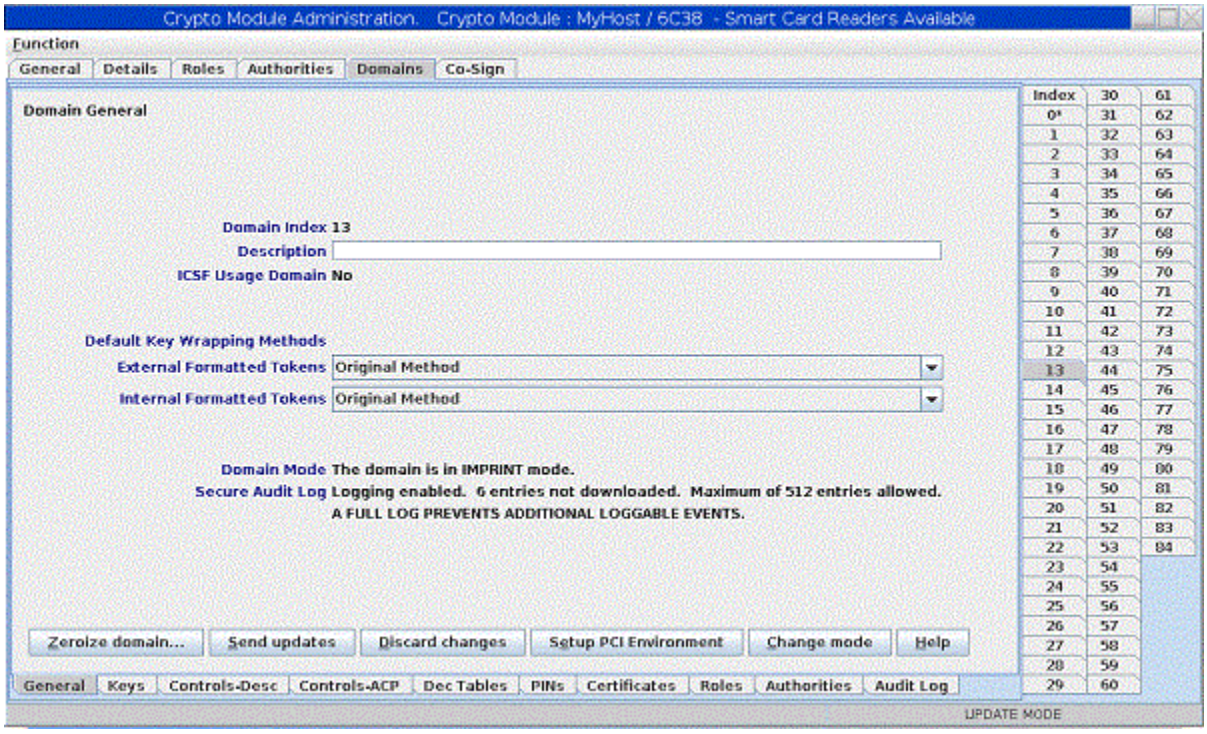


Figure 98. Domain in IMPRINT mode

For more information, see “Domain modes” on page 9.

Domain Keys page

This page displays the status and hash patterns of the master key registers. It allows you to generate key parts; load, clear, and set master key registers; and load, view, and clear operational key registers. It also allows you to enter key parts on a smart card using secure key entry.

The upper part of the window displays the status and hash patterns of the master key registers. The master key registers shown depend on the crypto module type.

Note: ICSF uses the term 'ECC master key register' and CCA uses the term 'APKA master key register' to refer to the same entity. On TKE, this is labeled 'ECC (APKA) master key register'.

If you are using smart cards, the TKE workstation crypto adapter must be enrolled in the same zone as the smart cards you are using. Otherwise, you cannot generate key parts and save them on the smart card or load key parts from the smart card to a master key register or operational key register.

You can view the zone for smart cards using the Smart Card Utility Program. Insert the smart card in a reader and select **File** and then **Display smart card information**. You can view the zone for the TKE workstation crypto adapter and enroll the TKE workstation crypto adapter in a zone using the Smart Card Utility Program using options under the **Crypto Adapter** pull-down menu.

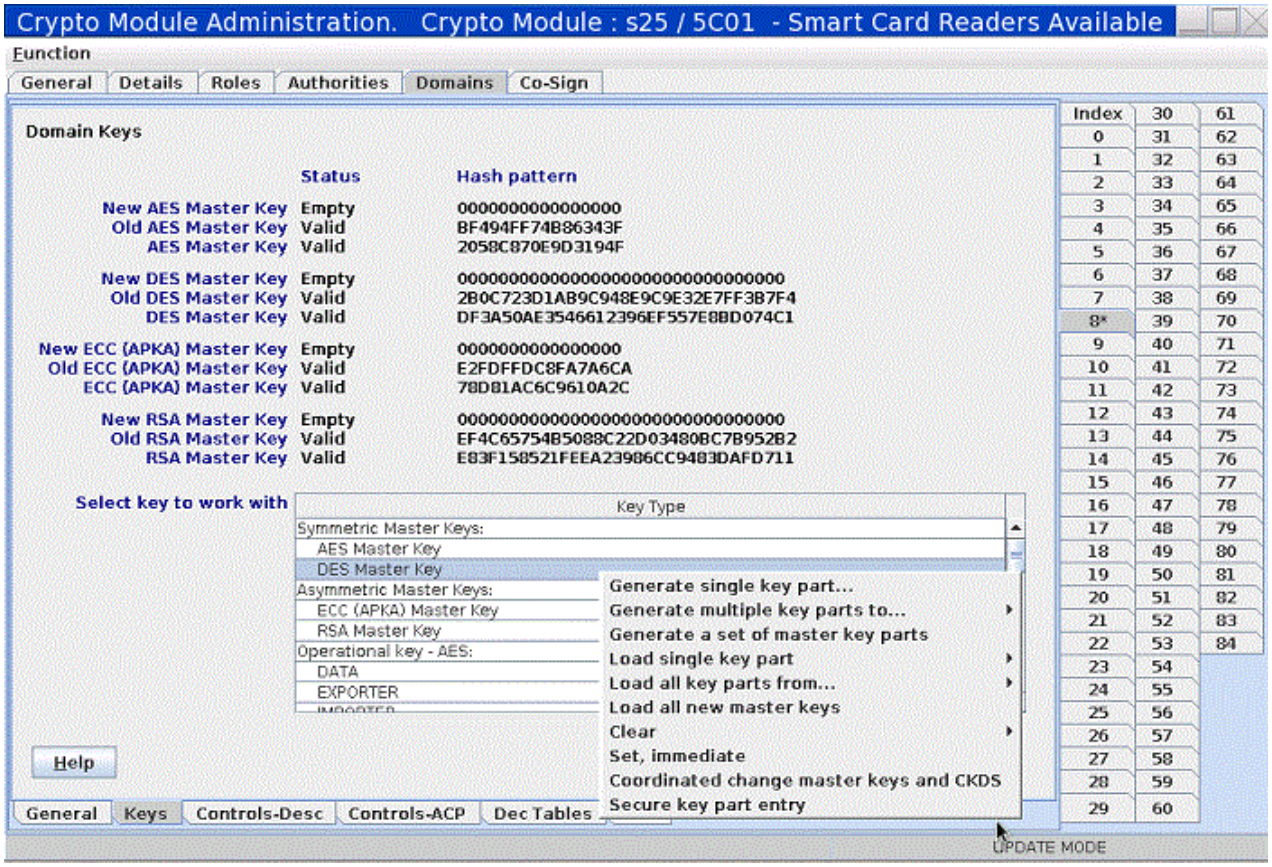


*Figure 99. **Domain Keys** page*

The lower part of the **Domain Keys** page allows you to work with different key types. Right-click on a key type in the Key Type container to display a pop-up menu. Table 31 on page 159 describes what menu options are available for the different key types.

Table 31. Key types and actions for the supported crypto modules

Key type	Pop-up	Sub-pop-up	Action description
AES master key **ECC (APKA) master key** **DES master key** **RSA master key**	Generate single key part		Generate one master key part and store it on a TKE smart card or save it to a binary or print file.
	Generate multiple key parts to ...	Smart card Binary file Print file	Run a wizard-like feature to generate a user specified number of master key parts and store them on TKE smart cards or save them to binary or print files. **Note:** You can use the same smart card or switch smart cards between key part generations.
	Generate a set of master key parts		Run a wizard-like feature to generate a set of master key parts (AES, DES, RSA or ECC (APKA)).

Table 31. Key types and actions for the supported crypto modules (continued)

Key type	Pop-up	Sub-pop-up	Action description
	Load single key part	First Intermediate Last	Load one key part into the appropriate "new" master key register. **Notes:** 1. To load a first part, the "new" master register status must be "empty". 2. To load an intermediate or last part, the "new" master register status must be "part full" (partially full).
	Load all key parts from	Smart card Binary file Print file	Run a wizard-like feature to load an entire "new" master key register. At the beginning of the process, you specify the total number of key parts and have the option of clearing the "new" master key register. **Note:** No new security controls are introduced by this feature. ALL authority and dual control requirements you put in place remain in effect. It takes the same number of people to load an entire key using this procedure as it does loading an entire key one part at a time.
	Load all new master keys		Run a wizard-like feature to load one or more new master key registers -- first, middle (optional), and last key parts. At the beginning of the process, you have the option of clearing one or more master key registers. Note: No new security controls are introduced by this feature. ALL authority and dual control requirements you put in place remain in effect. It takes the same number of people to load an entire key using this procedure as it does loading an entire key one part at a time.
	Clear	New Master Key Register Old Master Key Register	Clear the new or old master key register. The status of the register will be "empty" when the operation is complete.

Table 31. Key types and actions for the supported crypto modules (continued)

Key type	Pop-up	Sub-pop-up	Action description
	Set (Option only shown on RSA master key)		Sets the RSA master key. **Notes:** 1. Beginning with ICSF FMID HCR7790, ICSF blocks the use of the Set RSA Master Key command from TKE if any online host crypto modules are found with the September 2011 LIC or later (CEX3C or later). The set must be done from ICSF. 2. The current RSA master key is transferred to the old RSA master key register. 3. The new RSA master key register is transferred to the current RSA master key register. 4. The new RSA master key register is reset to zeros.
	Set, immediate		Sets the master key. Transfers the value in the current master key register to the old master key register, transfers the value in the new master key register to the current master key register, and clears the new master key register. Under normal circumstances, set master keys using ICSF procedures or services that coordinate setting the master key with initializing or re-enciphering key storage. This option sets the master key but does not change the associated key storage. If used inappropriately, this command causes the keys in key storage to become unusable when accessed by ICSF in the domain. Use this option only when key storage does not need to be initialized or re-enciphered when the master key is set. For example, this command can be used to reload previous master key values if a host crypto module has been inadvertently zeroized.
	Secure key part entry		Enter known key part value to a TKE smart card; see Appendix A, “Secure key part entry,” on page 311.

Table 31. Key types and actions for the supported crypto modules (continued)			
Key type	**Pop-up**	**Sub-pop-up**	**Action description**
AES master key **DES master key**	Coordinated change master keys and CKDS		Run a wizard-like feature to re-encipher the current ICSF cryptographic key data set (CKDS) under the new AES or DES master keys or both, set the AES or DES master keys or both, and make the re-enciphered CKDS the active in-store CKDS used by ICSF. **Note:** This option is displayed only when the following conditions are met: • The current domain is the usage domain. • The "Coordinated change master key and KDS" operation is permitted in the role for the user currently logged on the TKE crypto adapter. • The host usage domain is running ICSF FMID HCR77B1 with APAR OA49067, or later.
ECC (APKA) master key **RSA master key**	Coordinated change master key and PKDS		Run a wizard-like feature to re-encipher the current ICSF public key data set (PKDS) under the new ECC (APKA) or RSA master keys or both, set the ECC (APKA) or RSA master keys or both, and make the re-enciphered PKDS the active in-store PKDS used by ICSF. **Note:** This option is displayed only when the following conditions are met: • The current domain is the usage domain. • The "Coordinated change master key and KDS" operation is permitted in the role for the user currently logged on the TKE crypto adapter. • The host usage domain is running ICSF FMID HCR77B1 with APAR OA49067, or later.
DES, AES, or HMAC operational keys	Generate single key part		Generate one key part and store it on a TKE smart card or save it to a binary or print file.
	Generate multiple key parts to ...	Smart card Binary file Print file	Run a wizard-like feature to generate a user specified number of key parts and store them on TKE smart cards or save them to binary or print files. **Note:** You can use the same smart card or switch smart cards between key part generations.

Table 31. Key types and actions for the supported crypto modules (continued)

Key type	Pop-up	Sub-pop-up	Action description
	Load single key part	First First (minimum of 2 parts) First (minimum of 3 parts) Add part Complete	Load one key part into a key part register. **Note:** 1. When the first key part is loaded, you must enter a unique key label for the register. 2. The **First** option can be selected only for DES operational keys and AES DATA operational keys. 3. The **First (minimum of 2 parts)** and **First (minimum of 3 parts)** options can be selected only for AES operational keys (other than DATA) and HMAC operational keys. 4. After selecting **First** or **First (minimum of 2 parts)**, you must load at least one additional key part before completing the register. 5. After selecting **First (minimum of 3 parts)**, you must load at least two additional key parts before completing the register.
	Load to Key Storage	First Intermediate Last	Load a key part to the TKE workstation's DES or AES key storage. **Note:** These options can be selected only for DES IMP-PKA operational keys and AES IMPORTER operational keys.
	Load all key parts from	Smart card Binary file Print file	Run a wizard-like feature to load an entire operational key register. At the beginning of the process, you specify the total number of key parts and have the option of clearing the "new" master key register. **Note:** No new security controls are introduced by this feature. ALL authority and dual control requirements you put in place remain in effect. It takes the same number of people to load an entire key using this procedure as it does loading an entire key one part at a time.
	View		View key part register information
	Clear		Clear (reset) the operational key part register.
	Secure key part entry		Enter known key part value to a TKE smart card; see Appendix A, “Secure key part entry,” on page 311.
RSA keys	Generate single key part		Generate an RSA key and encrypt it under a DES IMP-PKA key or AES IMPORTER key.
	Encipher		Encipher an unencrypted RSA key under an IMP-PKA key.
	Load to PKDS		Load an RSA key to the PKDS active in the logical partition where the Host Transaction Program is started.

Table 31. Key types and actions for the supported crypto modules (continued)			
Key type	**Pop-up**	**Sub-pop-up**	**Action description**
	Load to dataset		Load an RSA key to the host data set

Master keys - AES, ECC (APKA), DES, or RSA

Generate single key part

This generates and saves a random master key part.

When you select this option, you are prompted to enter the following information:

- The target for the master key part. This can be a smart card reader, a binary file, or a print file.
- The length of the key part. This is requested only for DES master key parts on CCA 4.3 or later. The allowed choices are 16 bytes and 24 bytes.
- If the target is a binary file or print file, the file name and location are requested. The target file can be in the TKE Data Directory or on USB memory.
- If the target is a binary file or print file, after the key part is generated and saved, you are asked if you want to save the key part elsewhere.
- If the target is a smart card reader, you are prompted to insert the smart card and enter the PIN. You are prompted to supply a key part description.

Attention : Removing a USB flash memory drive from a USB port while an operation accessing the drive is in progress can cause hardware messages on the TKE workstation. Wait for the operation to complete before removing the USB flash memory drive.

Generate multiple key parts

If you are going to create more than one key part at a time, use the “generate multiple key part to” feature. When this feature is started, you are asked to provide the total number of key parts you want to create. The minimum number of key parts that can be specified is 2.

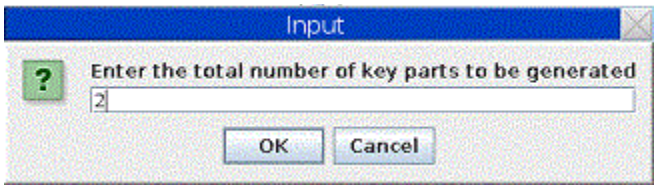


Figure 100. Enter number of keys to be generated

The feature will walk you through the process of creating the requested number of key parts.

Generate a set of master key parts

To create a set of master key parts of different types, use the 'generate a set of master key parts' feature. The feature helps you through the process of generating the set of master key parts.

Load single key part

This loads a key part into the new master key register. Cascaded options on the pop-up menu select whether the First, Intermediate, or Last key part is to be loaded.

The new master key register must be Empty in order to load a First key part. It must be Partially full in order to load an Intermediate or Last key part. You must load a First and a Last key part, and you can load any number of Intermediate key parts (zero or more).

After selecting the pop-up menu option, you are asked to select the source of the key part.

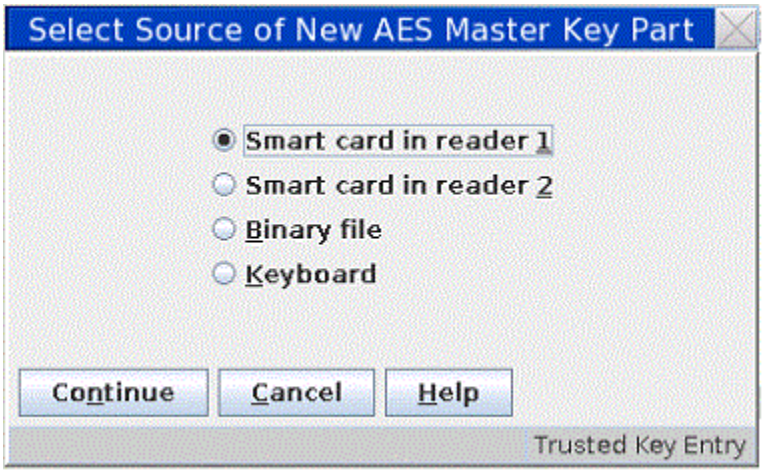


Figure 101. Select source of new AES Master Key part

Load from TKE smart card

You are prompted to insert the smart card in the reader. The smart card contents are read, and you are prompted to select a key part. Only key parts for the selected master key type are displayed.

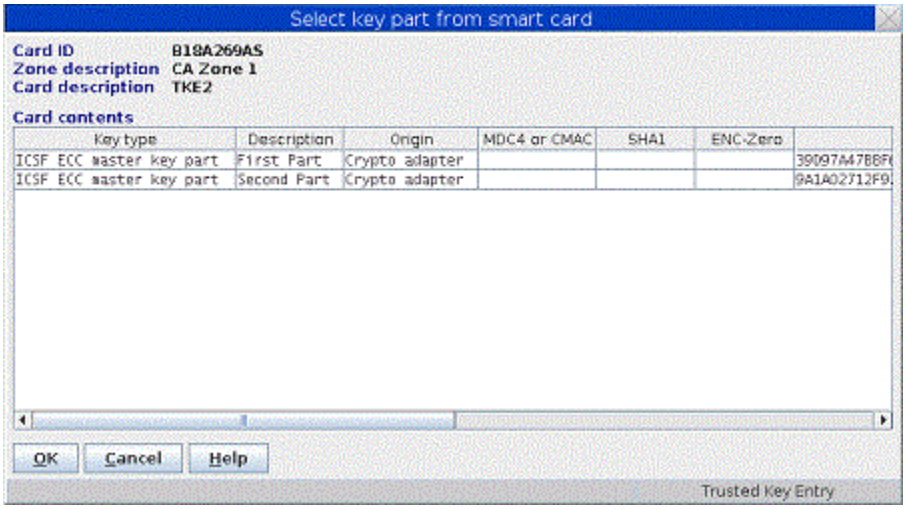


Figure 102. Select key part from TKE smart card

If no matching key parts are found, a warning message is displayed and the load operation terminates.



Figure 103. Warning message

Left-click on a key part to select it, then click on the OK button. You are asked to enter the PIN for the smart card if it has not been entered already. When the PIN is entered, the key part is read and one or more hash patterns or verification patterns are displayed. For DES master keys, the ENC-ZERO and MDC-4 or CMAC hash patterns are displayed. For RSA master keys, the MDC-4 hash pattern is displayed. For AES and ECC (APKA) master keys, the AES-VP or HMAC-VP is displayed.

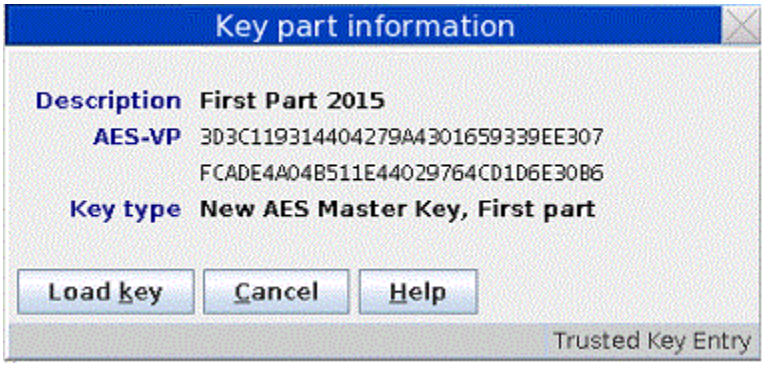


Figure 104. Key part information panel

Click on the Load key button to load the key part.

Load from keyboard

You can load a key part whose value you type in from the keyboard. The **Blind Key Entry** option on the **Preferences** pull-down menu on the main TKE panel controls the appearance and behavior of the panel used to enter the key part using the keyboard.

When the **Blind Key Entry** option is selected, only asterisks are displayed in the Enter Key Value panel as characters are entered using the keyboard. Optional reenter fields are displayed on the right side of the panel. If these are filled in, the values entered must match the values entered on the left side of the panel in order for the key part to be accepted.

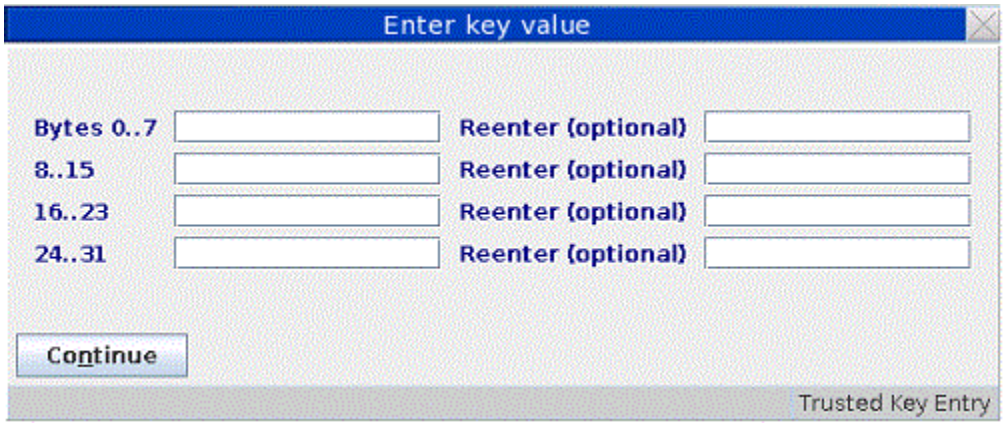


Figure 105. Enter Key Value - Blind Key Entry

When the **Blind Key Entry** option is not selected, the characters entered using the keyboard are displayed on the **Enter Key Value** panel and there are no reenter fields.

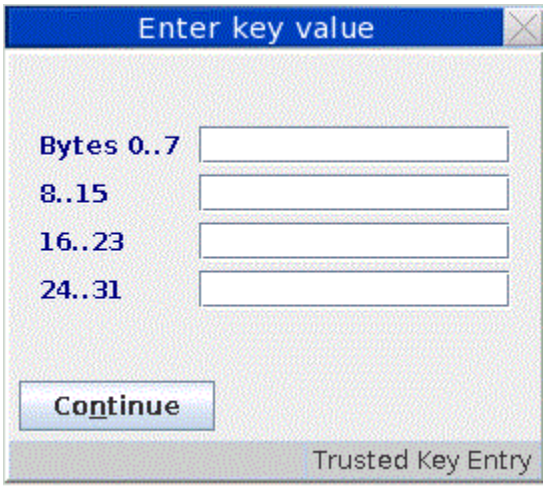


Figure 106. Enter Key Value

When you have entered the key part, click on the **Continue** button. A **Key Part Information** panel is displayed showing one or more hash patterns or verification patterns for the key part. Click on the **Load key** button to load the key part.

Before the key part is actually loaded, you are asked if you would like to save the key part. You can save the key part in one or more binary files or print files.

Load from binary file

You can load a key part saved in a binary file. The binary file can be in the TKE Data Directory or on USB memory. When you select this option, the **Specify Key File** window is opened.

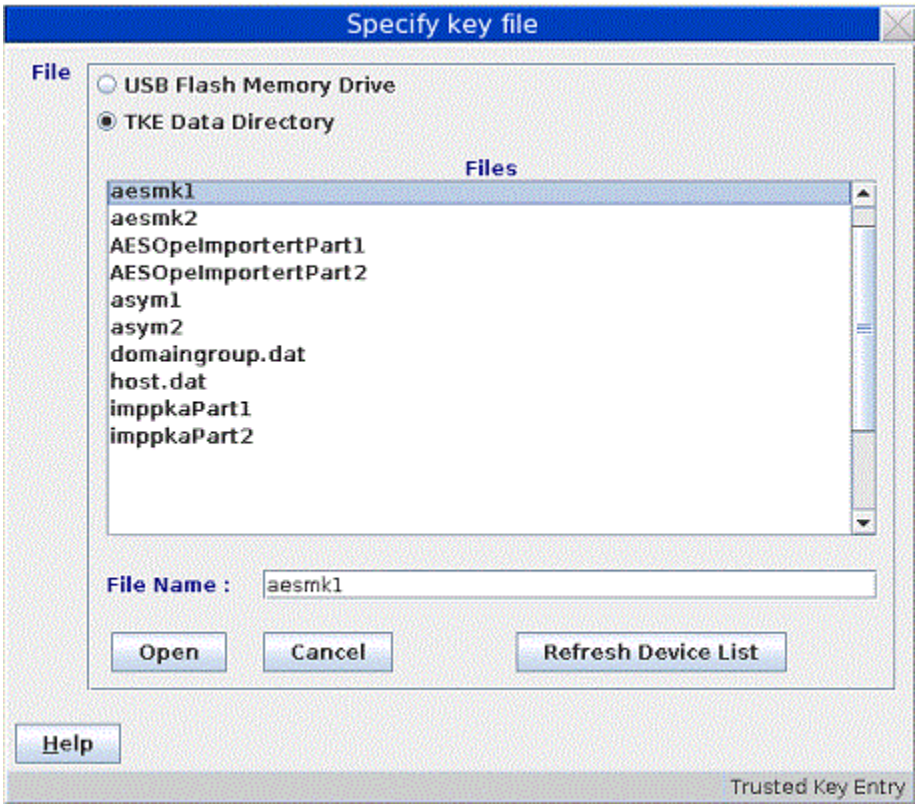


Figure 107. Specify Key File

Select the file location by clicking on a radio button at the top. The Files container lists the files for this location. A radio button for USB flash memory is displayed only when a USB flash memory drive is plugged into a USB port on the TKE workstation.

Left-click on one of the listed files to select the file containing the key part, then click on the **Open** button. A **Key Part Information** panel is displayed showing one or more hash patterns or verification patterns for the key part. Click on the **Load key** button to load the key part.

Attention : Removing a USB flash memory drive from a USB port while an operation accessing the drive is in progress can cause hardware messages on the TKE workstation. Wait for the operation to complete before removing the USB flash memory drive.

Note on DES master key length

Starting with CCA 4.3, a DES master key can be either 16-bytes or 24-bytes long. For earlier CCA versions, the DES master key length is always 16 bytes.

To load 24-byte DES master keys, you must use TKE 7.2 or later and run ICSF FMID HCR77A0 or later on the host system.

The DES master key length is selected through a domain control setting. The 'DES master key - 24-byte key' domain control under 'ISPF Services' controls the length of the first DES master key part that can be loaded into the new DES master key register. When the domain control is enabled, only a 24-byte key part can be loaded. When the domain control is disabled, only a 16-byte key part can be loaded.

The domain control setting only affects loading the first DES master key part. If a first DES master key part is loaded and the domain control setting is changed, the length of additional key parts must match the length of the first key part, regardless of the domain control setting.

Note on weak keys

Two other domain controls were introduced with CCA 4.3 and ICSF FMID HCR77A0: 'Warn when weak wrap - Master keys' and 'Prohibit weak wrapping - Master keys', both under 'Coprocessor Configuration'.

The first causes a warning to be signaled when loading a last 24-byte DES or RSA master key part, if the final key is considered weak. The final key is considered weak if two or more 8-byte pieces of the key are identical. For example, if A, B, and C represent the 8-byte pieces of the master key, an A-B-C key would be considered 'strong', but an A-B-A key would be considered 'weak'.

The second domain control causes an error to be reported instead of a warning for the same scenario.

Load all key parts from

This option allows you to fully load a new master key register without having to open and choose from the pop-up menu for each part. Cascaded options on the pop-up menu allow you to choose the source type (smart cards, binary files, or the keyboard).

You are asked to enter the number of key parts. You can optionally clear the new master key register. Then you are led through the process of loading each of the key parts from the selected source type.

When loading key parts from smart cards, you can use different smart cards for each key part, if desired.

For each operation that requires an authority signature, if no authority signature key is loaded or if the current authority is not allowed to perform the operation, you are prompted to load an appropriate authority signature key.

Load all new master keys

This option allows you to load all of the new master key registers (DES, AES, RSA and ECC(APKA)) using a single selection from the pop-up menu.

You are first asked to select the new master key registers to be cleared. Select the registers and click on the **Continue** button to proceed. If no registers need to be cleared, leave all check boxes unchecked and click on **Continue**.

If you do not have the latest TKE 9.2 maintenance installed:

You are asked to select the registers where first master key parts are to be loaded. Select the registers and click on the **Continue** button. You are asked to select the source of the key parts (smart card or binary file). For each of the registers you selected, you are guided through the process of loading a key part.

You are then asked whether you want to load middle master key parts. If yes, click on the **Yes** button. You are asked to select the master key registers where middle key parts will be loaded. You are asked to select the source of the key parts, and are then guided through the process of loading the middle key parts.

Similar actions take place for additional middle key parts and for the final key parts.

Beginning in TKE 9.2 with the latest maintenance level installed:

You are asked how many key parts each master key will have. The value must be at least 2. You are then asked to select which types of master keys you want to load key part 1 into. You are taken through the load process for all the types of keys you selected. The process is repeated for as many parts as you said you have. You no longer have a question asking you if you have middle key parts.

Clear

This option allows you to clear either the new master key register or the old master key register for the selected master key type.

Set

This option is available only for RSA master keys. PKA Callable Services must be disabled on ICSF before you use this option.

This option transfers the value in the current RSA master key register to the old RSA master key register, transfers the value in the new RSA master key register to the current RSA master key register, and clears the new RSA master key register.

Note: Beginning with ICSF FMID HCR7790, ICSF blocks the use of the Set RSA Master Key command from TKE if any online host crypto modules are found with the September 2011 LIC or later (CEX3C or later). ICSF signals an error in this case. You can use the Set RSA Master Key command with earlier versions of ICSF, or if all online host crypto modules are at earlier CCA levels.

Set, immediate

This option is available for all master key types (AES, ECC (APKA), DES, and RSA). It transfers the value in the current master key register to the old master key register, transfers the value in the new master key register to the current master key register, and clears the new master key register.

Under normal circumstances, set master keys by using ICSF procedures or services that coordinate setting the master key with initializing or re-enciphering key storage. This option sets the master key but does not change the associated key storage. If used inappropriately, this option causes the keys in key storage to become unusable when accessed by ICSF in the domain.

Use this option only when key storage does not need to be initialized or re-enciphered when the master key is set. For example, this command can be used to reload previous master key values if a host crypto module was inadvertently zeroized.

Coordinated change master keys and CKDS (AES and DES master keys only)

Beginning with TKE 8.1 and ICSF FMID HCR77B1 with the PTF for APAR OA49067, you can perform an operation from the TKE workstation that will set the host crypto module master key or keys and re-encipher your ICSF cryptographic key data set (CKDS) using the updated master key or keys. This function uses the same ICSF support as the 'coordinated CKDS change master key' option that appears on the CKDS Management panel in ISPF.

This option will appear on the pull-down menu only if the TKE workstation is connected to a host that is running ICSF FMID HCR77B1 with the PTF for APAR OA49067. The option will be disabled unless the active TKE crypto adapter role has the X'1012' 'Coordinated change master key and KDS' ACP defined.

This function does the following:

- Takes the ICSF CKDS that is enciphered under the current DES or AES master keys or both and re-enciphers it under the new DES or AES master keys or both. The re-enciphered content is placed in a new data set and becomes the active in-store CKDS copy used by ICSF.
- Sets the DES or AES master keys or both. This involves moving the contents of the current master key register or registers to the old master key register or registers, moving the contents of the new master key register or registers to the current master key register or registers, and then clearing the new master key register or registers.
- Optionally renames the current CKDS to a supplied archive data set name and then renames the new re-enciphered data set to the current CKDS name. If this option is not chosen, the CKDSN parameter in the ICSF installation options data set will need to be updated to the name of the new re-enciphered data set in order for that data set to be used the next time ICSF is started.
- Optionally makes a back-up copy of the re-enciphered new data set.

The master key registers involved with this operation are determined by how the CKDS was originally initialized – using the DES master key only, using the AES master key only, or both the DES and AES master keys.

The new master key registers that are used must be in a 'full' state and current master key registers must be in a 'valid' state before the coordinated change operation is performed. The new master key register checking includes all CCA crypto modules being used by the host ICSF, not just this crypto module. The verification patterns of the master key registers (new and current) are also checked for consistency for all CCA crypto modules being used by the host ICSF.

If the host ICSF is in a sysplex environment, the coordinated change operation will be performed sysplex-wide. In the sysplex environment, the current and new master key registers must be set properly on all systems in the sysplex.

If the new CKDS or back-up CKDS are not allocated, you will have an opportunity to allocate those data sets automatically. The TKE host transaction program job will attempt to allocate those data sets based on the attributes of the current CKDS using the TSO ALLOCATE command with the LIKE operand specified. The TKE host transaction program job user will need to have the proper authority in order for the data set allocation to succeed.

More information about the coordinated change master keys and CKDS function can be found in 'Coordinated KDS Administration (CSFCRC and CSFCRC6)' in *z/OS Cryptographic Services ICSF Application Programmer's Guide* and 'Performing a coordinated change master key' section in *z/OS Cryptographic Services ICSF Administrator's Guide*.

Coordinated change master keys and PKDS (ECC (APKA) and RSA master keys only)

This function is the same as the 'Coordinated change master keys and CKDS' function, but uses the ECC (APKA) or RSA master keys or both and public key data set (PKDS).

Operational keys

Host crypto modules contain a set of operational key part registers that allow you to accumulate the values of operational keys before loading a host Cryptographic Key Data Set (CKDS). On the CEX2C, CEX3C, and CEX4C coprocessors, there are 100 operational key part registers that are shared by all domains. On the CEX5C, CEX6C, and CEX7C coprocessors, there are 512 operational key part registers.

Operational key part registers in the Complete state can be loaded into a CKDS using ICSF panels (see “Loading operational keys to the CKDS” on page 245) or using the Key Generator Utility Program (KGUP) (see *z/OS Cryptographic Services ICSF Administrator's Guide*).

An operational key part register is freed when its contents are loaded into a CKDS, when it is explicitly cleared, or when the owning domain is zeroized.

You can use the TKE workstation to generate operational key parts, load operational key parts into an operational key part register on a host crypto module, load operational key parts into TKE key storage (this is required for transferring RSA keys from the TKE workstation to a host system), view operational key part registers, and clear operational key part registers. You can also enter operational key parts on a smart card using secure key entry.

There are three types of operational keys: DES, AES, and HMAC.

Most DES operational keys have a fixed length of 16 bytes. A control vector associated with DES operational keys determines how the key can be used. For more information on control vectors, see Appendix C in *z/OS Cryptographic Services ICSF Application Programmer's Guide*. AES operational keys (other than AES DATA) and HMAC operational keys have a set of key attributes instead of a control vector. Key attributes are divided into key usage attributes and key management attributes. For more information on key attributes, see Appendix B in *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

Note: Beginning in TKE 9.2 with the latest maintenance installed, the UDATAM and UDATAMV key types have been removed from the DES operational key list. Existing UDATAM parts can be used any place that a DATAM key part can be used. Existing UDATAMV key parts can be used any place that a DATAMV key part can be used. When viewing any existing DATAM, DATAMV, UDATAM, and UDATAMV key part on a smart card, the Control Vector (CV) that is shown is the CV that will be used when the part is used in a load operation.

Generate single key part

This generates and saves a random operational key part. Operational key parts can be saved in a binary file, a print file, or on a smart card.

When you select this option, a secondary panel is displayed that allows you to select the key part length and the control vector or key attributes, and specify a description for the key part. A default description is filled in for you. For most DES operational key types, the key length and control vector are fixed. For these operational key types, the length and control vector are displayed, but you cannot change them. For creating key parts that are PCI-compliant, make sure that you select the **PCI-Compliant** check box that modifies the control vector for you. The DES EXPORTER operational key is an example of an operational key with a fixed length and fixed control vector value.

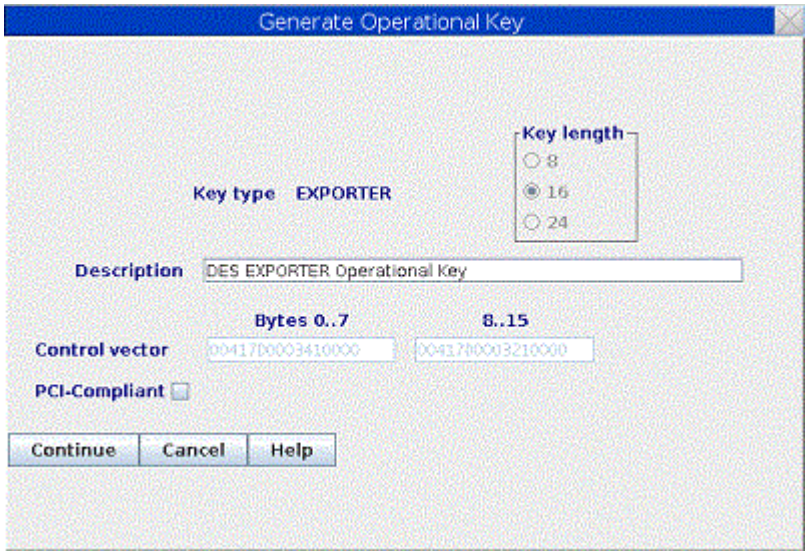


Figure 108. Generate Operational Key - predefined EXPORTER key type

The DES MAC and DES MACVER operational key types have fixed control vector values, but you can specify a length of 8 bytes or 16 bytes.

The DES DATA operational key type has a fixed control vector value of all zeros, but you can specify a length of 8, 16, or 24 bytes.

For the DES USER DEFINED operational key type, you can specify a length of 8, 16, or 24 bytes, and you can specify the control vector value.

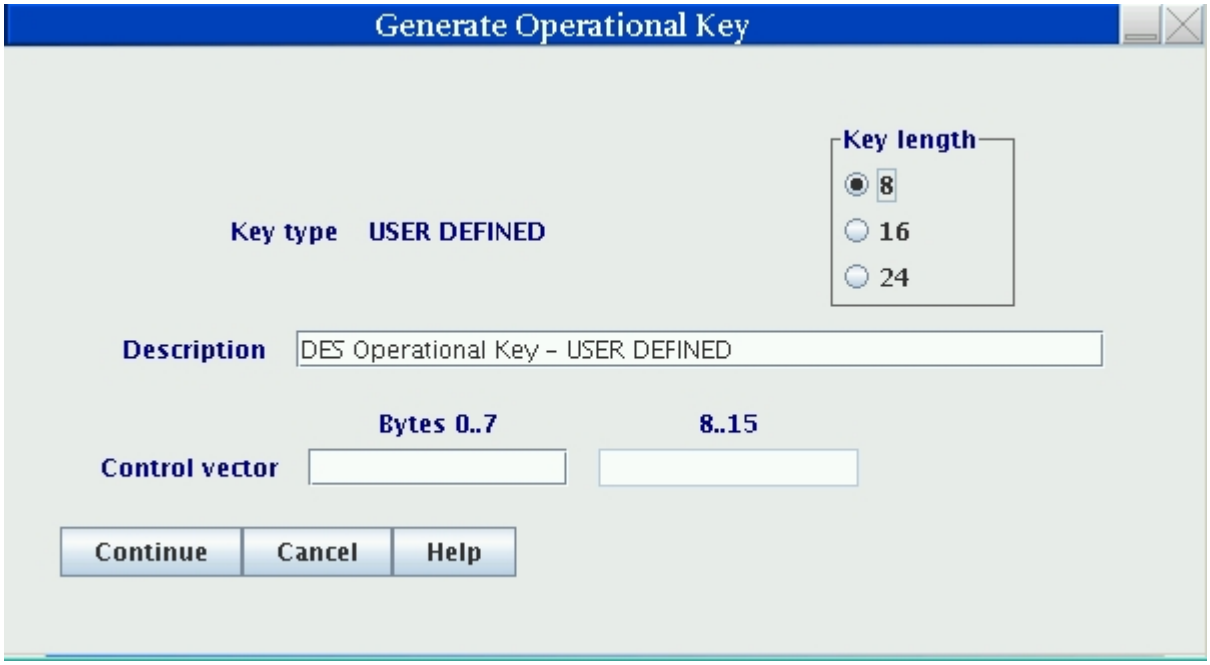


Figure 109. Generate Operational Key - USER DEFINED

For the AES DATA operational key type, you can specify a length of 16, 24, or 32 bytes, and a fixed control vector of all zeros is used.

All other AES operational key types and HMAC operational keys have associated key attributes instead of a control vector. The set of key attributes for the key depends on the key type. You can select a length of 16, 24, or 32 bytes for these operational key types. Default attributes are defined for each of these operational key types, but you can change them.

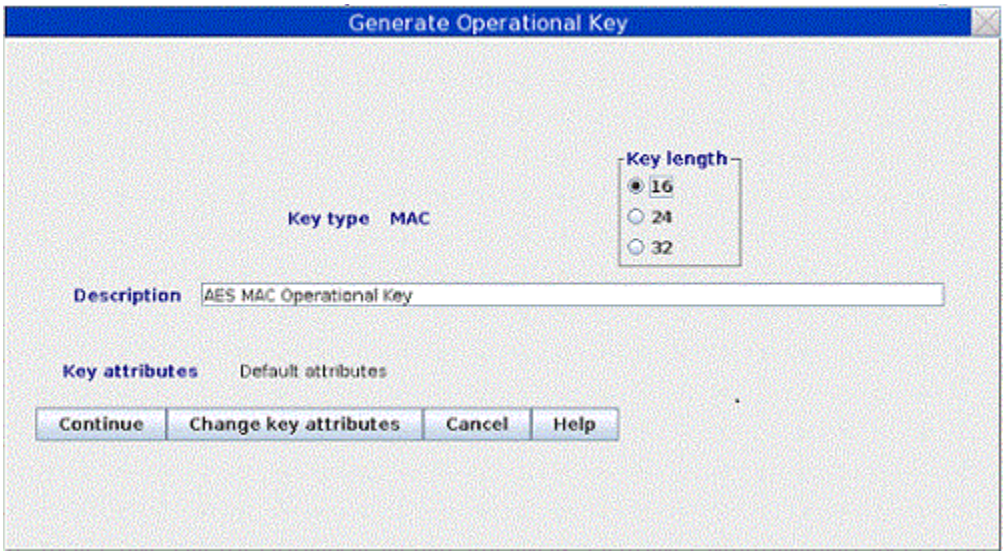


Figure 110. Generate Operational Key panel - AES MAC operational key

Click on the **Change key attributes** button to display a secondary panel that shows the key attributes.

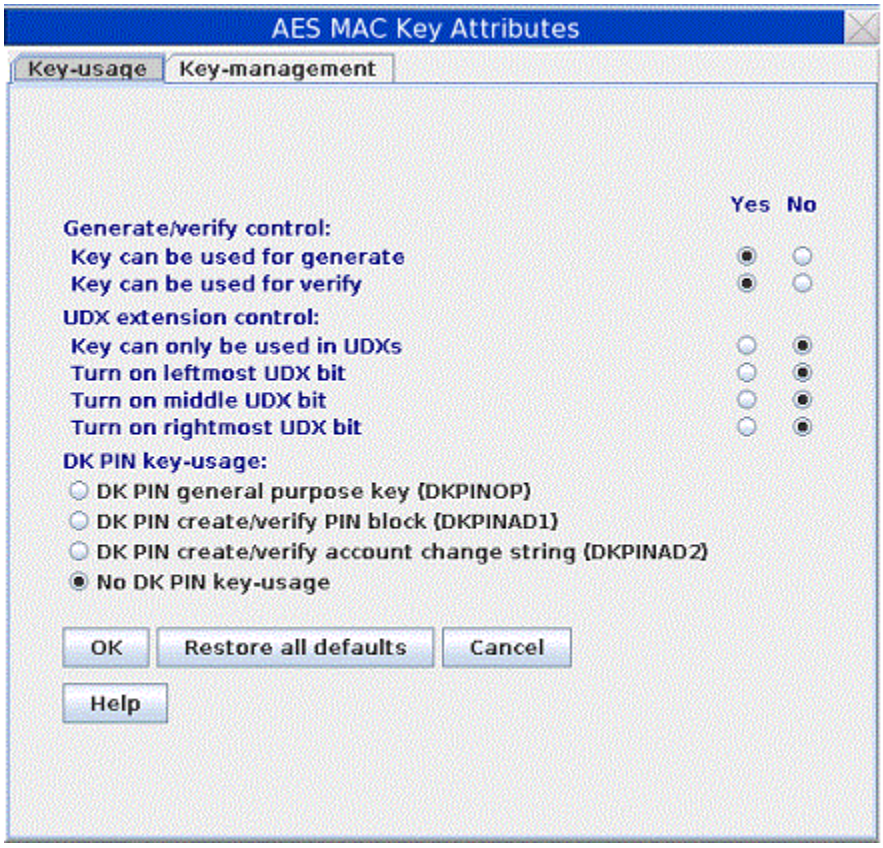


Figure 111. AES MAC Key Attributes panel

Click on radio buttons to change the attributes. If you want to restore the default attributes, click on the **Restore all defaults** button.

After you have specified the key length, description, and control vector or attributes, click on the **Continue** button. You are asked to select the target of the operational key part. When the target is a binary file or print file, a panel is displayed allowing you to specify the target file name and location. You can save to a file in the TKE Data Directory or on a USB flash memory drive. After the operational key part is saved, you are asked if you want to save the key part in another file or location.

Attention : Removing a USB flash memory drive from a USB port while an operation that is accessing the drive is in progress can cause hardware messages on the TKE workstation. Wait for the operation to complete before removing the USB flash memory drive.

When the target is a smart card, you are prompted to insert a smart card in the reader and enter the PIN. You are given the opportunity to change the description before the key part is saved on the smart card.

Generate multiple key parts

This option allows you to generate multiple key parts without having to select from the pop-up menu for each one. Cascaded menu options select whether the key part is saved in a binary file, print file, or on a smart card.

You are asked to enter the number of operational key parts to be generated. For each operational key part to be generated, you are led through the process of specifying the length, description, and control vector or attributes as described above, and selecting the target file or inserting the target smart card in a reader and entering the PIN.

Load single key part

This option allows you to load a single operational key part to an operational key part register, or to change the state of one or more operational key part registers to 'Complete'.

For DES operational keys and the AES DATA operational key, cascaded options on the pop-up menu allow you to select First, Add part, and Complete. For these keys, you must load at least two key parts before completing the register.

For AES operational keys other than DATA and HMAC operational keys, cascaded menu options let you select First (minimum of 2 parts), First (minimum of 3 parts), Add part, and Complete. For these keys, you must load at least two key parts when you used the First (minimum of 2 parts) option to load the first key part, and you must load at least three key parts when you used the First (minimum of 3 parts) option.

When loading a first operational key part, you enter a new key label to identify the operational key part register. An error is reported if you use an existing key label. The key label must conform to valid key label names in the CKDS. Key labels can be up to 64 characters long. The first character must be an alphabetic or national character (#, %, or @). The remaining characters can be alphanumeric, national, or a period (.). When the key part is processed, the label is converted to uppercase.

When adding a key part or completing an operational key part register, you are given a list of key labels to choose from. When adding a key part, only key labels for operational key part registers containing a key of a matching type, with attributes that are compatible with the operational key part being loaded, are shown. When completing an operational key part register, only key labels for operational key part registers containing a key of the correct type, where the required minimum number of key parts have been loaded, are shown.

In some cases, an exact match on the key part type or key part attributes is not required when loading key parts. A warning is displayed for these cases, or you are asked in advance whether using an alternate type or alternate attributes should be allowed.

Load first DES operational key part

When **Load single key part --> First** is selected for a DES operational key, you are asked to select the source of the key part. The source can be a binary file, a smart card, or the keyboard. When the source is a binary file, a secondary panel is displayed asking you to select the location of the file and the file name. Files in the TKE Data Directory or on a USB flash memory drive can be selected.

After the source file is selected, a Key Part Information panel is displayed. If the key part is non-PCI-compliant, it shows the ENC-ZERO and MDC-4 hashes for the operational key part and the control vector. If the key part is PCI-compliant, it shows the ENC-ZERO and CMAC hashes for the operational key part and the control vector. To load the first operational key part, type a valid key label in the text box and click the **Load key** button.

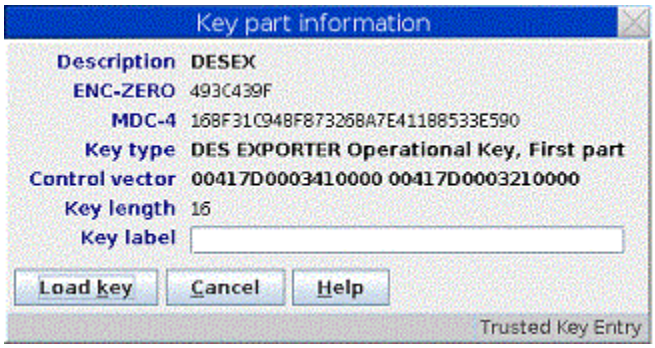


Figure 112. Key part information - first DES key part

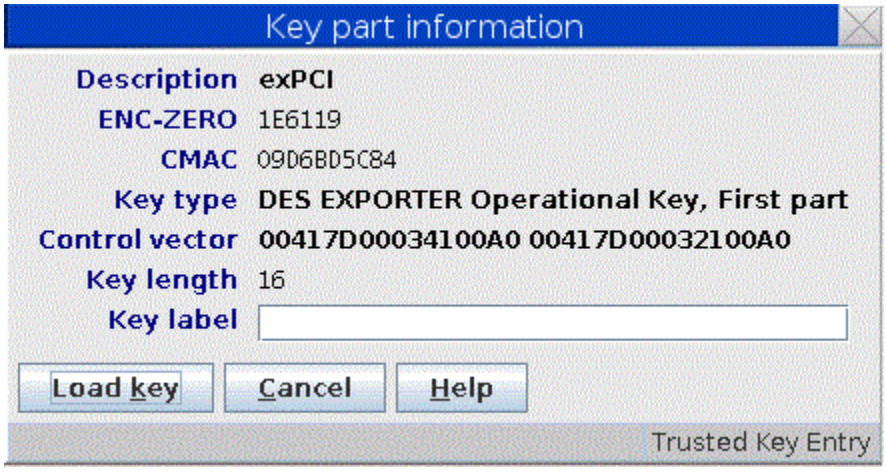


Figure 113. Key part information - first DES key part PCI-compliant

After the key is loaded into the operational key part register, a Key Part Register Information panel is displayed showing the SHA1 hash and control vector for the operational key part register.

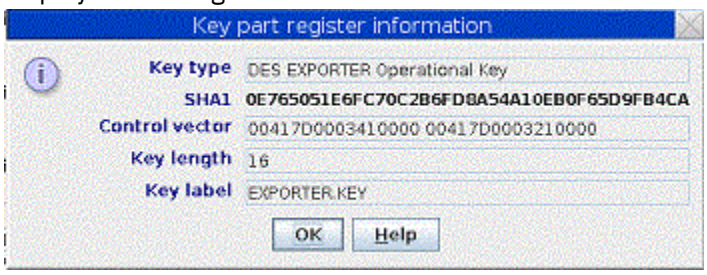


Figure 114. DES key part register information

When the source is a smart card, you are prompted to insert a smart card in the reader. The smart card contents are read and a list of key parts whose type matches the key type selected on the Domain Keys page is displayed. If you select one and click on the **OK** button, you are asked to enter the PIN. After entering the PIN, a Key Part Information panel is displayed and the process continues as for a binary file.

When the source is the keyboard, an Enter Key Value panel is displayed. For most DES operational key types, you will not be able to change the key length or control vector value displayed on this panel. For the DES USER DEFINED operational key type, you will need to enter a valid control vector value. You can change the default description and enter the key value in the 'key value' text boxes.

The appearance and behavior of the Enter Key Value panel depends on how the **Blind Key Entry** option on the **Preferences** pull-down menu on the main TKE panel is set. When the **Blind Key Entry** option is selected, only asterisks are displayed in the Enter Key Value panel. Optional 'confirm key value' text boxes are displayed at the bottom of the panel. If used, the values entered must match the values in the 'key value' boxes in order for the key part to be accepted. When the **Blind Key Entry** option is not selected, the characters entered by using the keyboard are displayed in the 'key value' text boxes and there are no 'confirm key value' text boxes on the panel.

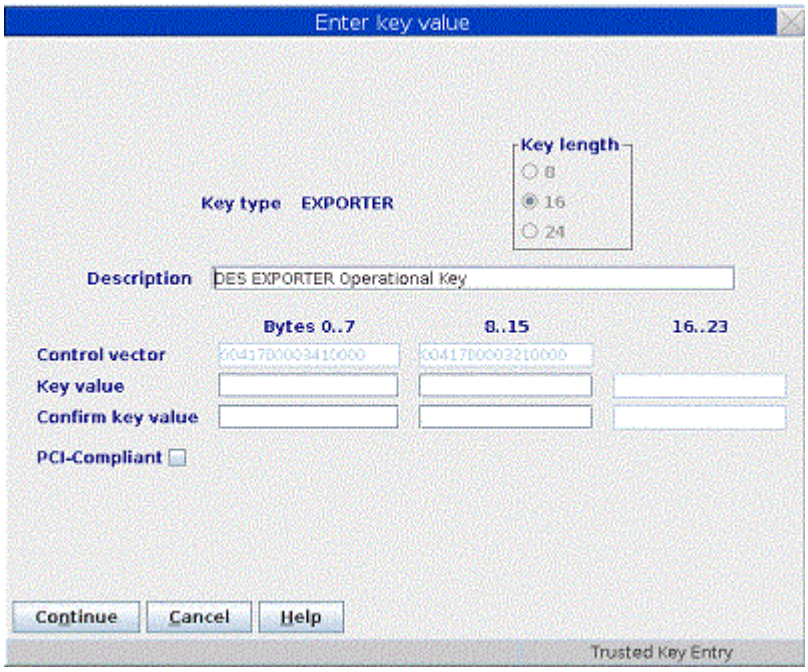


Figure 115. Enter key value - keyboard source for predefined EXPORTER key type

After entering a key value and clicking the **Continue** button, you are asked if you would like to save the key part before loading it. If you answer Yes, you are asked to choose between saving the key part in a binary file or in a print file. You are then asked to provide the file name and location. Files in the TKE Data Directory or on a USB flash memory drive can be used.

Attention : Removing a USB flash memory drive from a USB port while an operation accessing the drive is in progress can cause hardware messages on the TKE workstation. Wait for the operation to complete before removing the USB flash memory drive.

Finally, a Key Part Register Information panel showing the SHA1 hash and control vector of the operational key part register is displayed.

Note: Some DES operational key types can be substituted for other DES operational key types when loading an operational key part register. The following substitutions are allowed:

- A DES IMPORTER key part may be used to build a DES EXPORTER operational key.
- A DES EXPORTER key part may be used to build a DES IMPORTER operational key.
- A DES CIPHERXI key part may be used to build a DES CIPHERXO operational key.
- A DES CIPHERXO key part may be used to build a DES CIPHERXI operational key.
- A DES DATAM key part may be used to build a DES DATAMV operational key.
- A DES MAC key part may be used to build a DES MACVER operational key.
- A DES UDATAM key part may be used to build a DES UDATAMV operational key.

When loading an operational key part register, you are either asked in advance whether these substitutions should be allowed, or a warning message is displayed after you have selected a key part whose type is different from the type selected on the Domain Keys page.

Add DES operational key part

When **Load single key part --> Add part** is selected for a DES operational key, the process is similar to that for loading the first key part. You are asked to select the source of the key part. After the key part is read or entered, a Key Part Information panel is displayed. Instead of a text box for the Key Label, a drop down menu is displayed showing key labels for operational key part registers containing a matching key type in an appropriate state for adding the key part. Select one of these and click the **Load key** button.



Figure 116. DES Key part information - add part

If there are no operational key part registers for the domain containing a matching key type in an appropriate state for adding the key part, a warning message is displayed and the load operation terminates.

After the key part is added to the register, a Key Part Register Information panel is displayed showing the SHA1 hash and control vector of the updated operational key part register.

Entering an additional key part for a DES USER DEFINED operational key from the keyboard is a special case. After selecting the keyboard as the source, a panel is displayed showing all control vectors found for operational key part registers for the domain that are in a state where key parts can be added. This includes DES operational keys of all types, not just the DES USER DEFINED type. After selecting a control vector, the Enter Key Value panel is displayed and you are allowed to enter the additional key part. The drop down menu on the Key Part Information panel showing key labels will include key labels only for operational key part registers where the control vector matches the control vector you selected.

Complete DES operational key part

When the **Load single key part --> Complete** option is selected, a Complete Operational Key Part panel is displayed. This contains a list of key labels for operational key part registers holding an operational key whose type matches the type selected on the Domain Keys page and where enough key parts have been loaded to allow the register to be completed. If no appropriate operational key part registers are found, a warning message is displayed and the complete operation terminates.

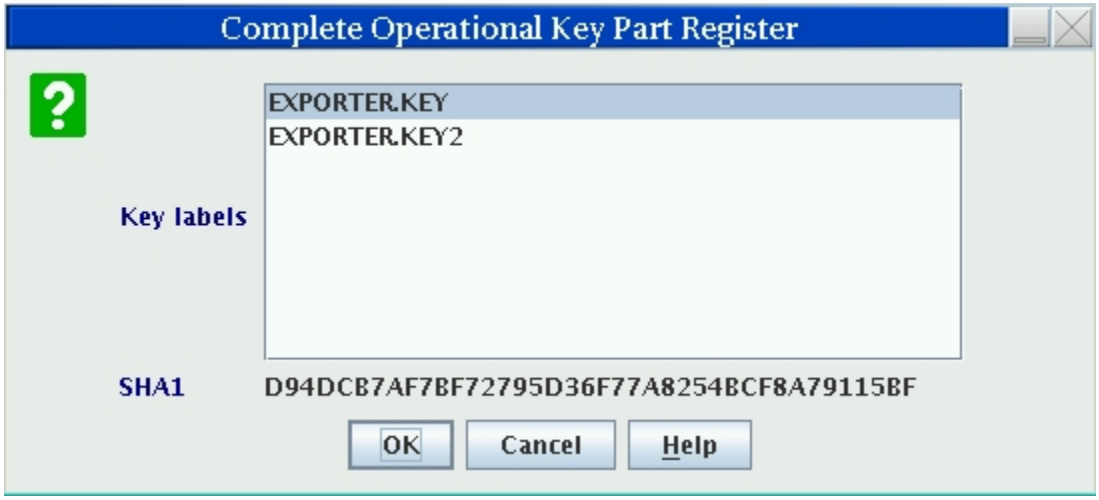


Figure 117. Complete DES Operational Key Part Register - predefined EXPORTER key type

Left-clicking on a key label causes the SHA1 hash for that key label to be displayed.

Select one or more key labels and click on the **OK** button to complete the selected operational key registers.

To select more than one key label, left-click to select the first key label. Hold down the **Ctrl** key on the keyboard and left-click to select additional key labels. To select a range of key labels, left-click to select the first key label, then hold down the **Shift** key and left-click to select the last key label. To select all key labels on the panel, hold down the **Ctrl** key and then press the **A** key.

When more than one key label is selected, a dash (-) is displayed for the SHA1 hash.

For each operational key part register that is completed, a Key Part Register Information panel is displayed. This shows the ENC-ZERO hash and control vector for the completed operational key part register.

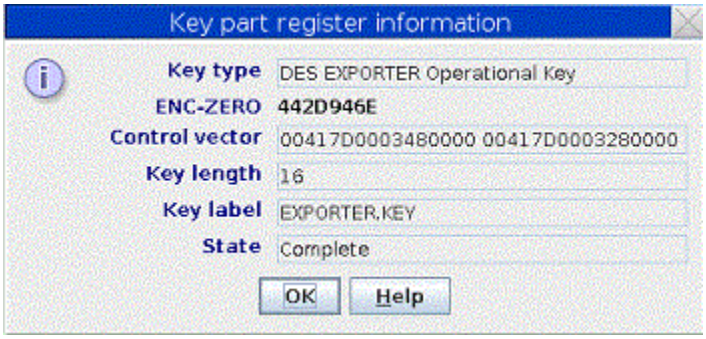


Figure 118. DES Key part register information - predefined EXPORTER key type in Complete state

AES operational keys and HMAC operational keys

Processing for AES operational keys and HMAC operational keys is similar to processing for DES operational keys, with a few differences.

The AES DATA operational key has a control vector of all zeros. On the Key Part Information panel and Key Part Register Information panel, an AES-VP is shown instead of the ENC-ZERO, MDC-4, and SHA1 hashes.

When loading a first AES or HMAC operational key part from a binary file, usually if the key type in the file does not match the key type selected on the Domain Keys page, an error message is displayed and the load processing terminates. An exception is that AES IMPORTER and AES EXPORTER key parts can be substituted for each other.

AES operational keys (other than AES DATA) and HMAC operational keys have key attributes instead of a control vector. The key attributes for an operational key part or operational key part register depend on the operational key type. The Key Part Information panel does not show a control vector for AES and HMAC operational keys, but instead indicates whether the key part has the default attributes or custom attributes. The Key Part Information panel has either a **Display key attributes** button or a **Change key attributes** button, which can be used to display or change some attributes.

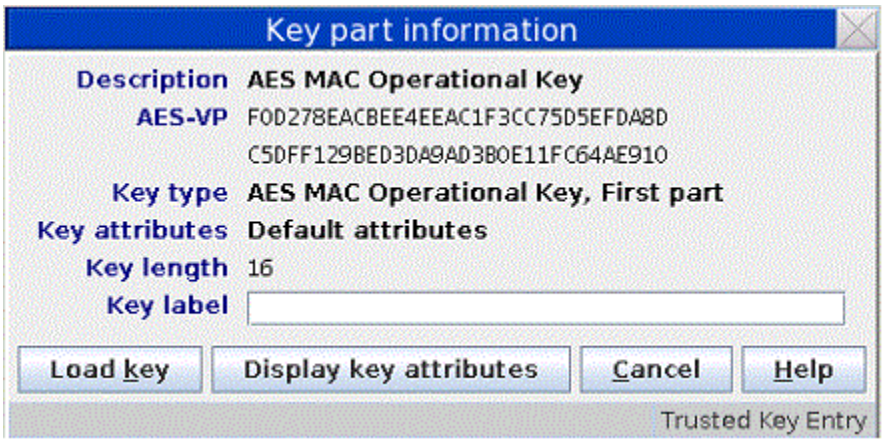


Figure 119. Key Part Information panel for an AES operational key other than DATA

Similarly, the Key Part Register Information panel does not show a control vector. Instead, it indicates whether the operational key part register contains a key with the default attributes or custom attributes. It has a **Display key attributes** button that allows you to view the attributes for the key part in the key part register.

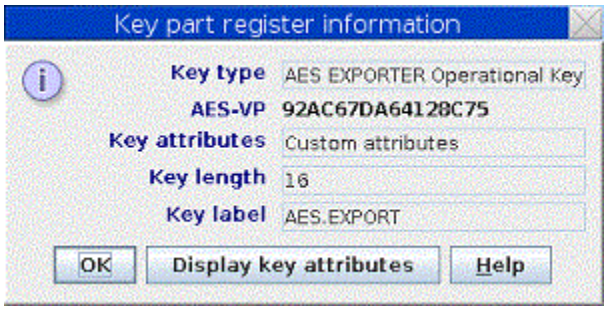


Figure 120. Key Part Register Information panel for an AES operational key other than DATA

On both panels, for AES operational keys, an AES-VP is shown, and for HMAC operational keys, an HMAC-VP is shown.

When generating an AES or HMAC operational key part, a set of attributes is selected and saved with the key part. For some key types, some of the saved attributes can be changed when loading a first operational key part into an operational key register:

- When loading a first AES CIPHER operational key part, you can change the encrypt control and data translate control attributes.
- When loading a first AES MAC operational key part, you can change the generate/verify control attributes.
- When loading a first AES PINPROT operational key part, you can change the encrypt control attributes.
- When loading a first AES PINPRW operational key part, you can change the generate/verify control attributes.
- When loading a first HMAC operational key part, you can change the generate/verify control attributes.

For these key types, the Key Part Information panel has a **Change key attributes** button that allows you to change the indicated attributes before the key part is loaded. Other attributes are grayed out, and you are not allowed to change them.

Similarly, when loading an additional key part, you are asked whether these attributes in the selected key part should be ignored. If you answer No, the Key Part Information panel will show only key labels where the attributes match exactly. If you answer Yes, the Key Part Information panel will include key labels with mismatches on these attributes. After the additional key part is loaded, the operational key part register will continue to have the attribute settings that were loaded with the first key part.

Load all key parts

This option allows you to fully load an operational key part register without having to open and choose from the pop-up menu for each part. Cascaded options on the pop-up menu allow you to choose the source type (smart cards, binary files, or the keyboard).

You are asked to enter the number of key parts. You can optionally clear the operational key part register. You are then led through the process of loading each of the key parts from the selected source type.

When loading key parts from smart cards, you can use different smart cards for each key part, if desired.

View

This option allows you to view the operational key part registers that exist in the domain for a particular key type. It displays a list of key labels for the key type, and you are allowed to select one or more of these key labels. After you click on the **OK** button, a Key Part Information Panel is displayed for each of the selected key labels showing additional information.

For DES operational keys, the SHA1 hash is displayed. For AES operational keys, the AES-VP is shown. For HMAC operational keys, the HMAC-VP is shown.



Figure 121. View Operational Key Part Register panel - AES CIPHER operational key

Left-click on a key label to select it. To select more than one key label, left-click to select the first key label and then hold down the **Ctrl** key on the keyboard and left-click to select additional key labels. To select a range of key labels, left-click to select the first key label, then hold down the **Shift** key and left-click to select the last key label. To select all key labels on the panel, hold down the **Ctrl** key and then press the A key.

After you have selected one or more key labels and clicked on the **OK** button, a Key Part Register Information panel is shown for each of the selected key labels. This shows the key type, hash pattern or verification pattern, control vector or key attributes, key length, key label, and state of the register.



Figure 122. Key Part Register Information panel - AES CIPHER operational key

To view the full key attributes, click the **Display key attributes** button. This displays a secondary panel showing the key attributes. DES operational keys and AES DATA operational keys have a control vector rather than key attributes and therefore, do not have a button to display a key attributes panel.

The DES USER DEFINED operational key type is a special case. When you select the View option for this key type, the View Operational Key Part Register panel shows the key labels in the domain for all DES operational key types, not just those created as DES USER DEFINED types. This is because a DES USER DEFINED key can have any valid control vector value, including the fixed values assigned for other DES operational key types.

Clear

This option allows you to clear operational key part registers for the domain.

After you confirm your intention to clear one or more operational key part registers for the domain, a Clear Operational Key Part Register panel is displayed showing the existing key labels for operational key part registers in the domain for the selected key type. Select one or more of these and click on the **OK** button to remove the key label from the set of active operational key part registers for the domain.



Figure 123. Clear Operational Key Part Register panel -- AES CIPHER operational key

Left-click on a key label to select it. To select more than one key label, left-click to select the first key label and then hold down the **Ctrl** key on the keyboard and left-click to select additional key labels. To select a range of key labels, left-click to select the first key label, then hold down the **Shift** key and left-click to select the last key label. To select all key labels on the panel, hold down the **Ctrl** key and then press the **A** key.

After you select one or more key labels and click on the **OK** button, the key part registers are cleared.

The DES USER DEFINED operational key type is a special case. When you select the Clear option for this key type, a Clear Operational Key Part Register panel is displayed showing the existing key labels for all DES operational key types, not just those created as DES USER DEFINED types. This is because a DES USER DEFINED key can have any valid control vector value, including the fixed values assigned for other DES operational key types.

DES operational key: Load to Key Storage

This selection is only possible for operational IMP-PKA keys. The IMP-PKA key-encrypting keys are used to protect RSA keys during transport from the workstation to ICSF. After selecting **Load to Key Storage**, the user chooses one of the following key parts to load to the workstation key storage:

- **First**
- **Intermediate**
- **Last**

The contents of the container depend upon the user's selection.

If the user selected **First**, the container shows all keys in the workstation key storage usable as IMP-PKA key encrypting keys. The user can utilize these as skeletons for composing the new key label.

If the user selected **Intermediate** or **Last**, the container shows all keys in the workstation key storage that have been installed with the first key part. It also shows any optional intermediate key parts that have been installed. The user must select one of these as the key label.

A window opens for the user to specify the workstation key label and whether this IMP-PKA key will be used to protect an RSA key to be generated at the workstation or a clear RSA key to be enciphered at the workstation.

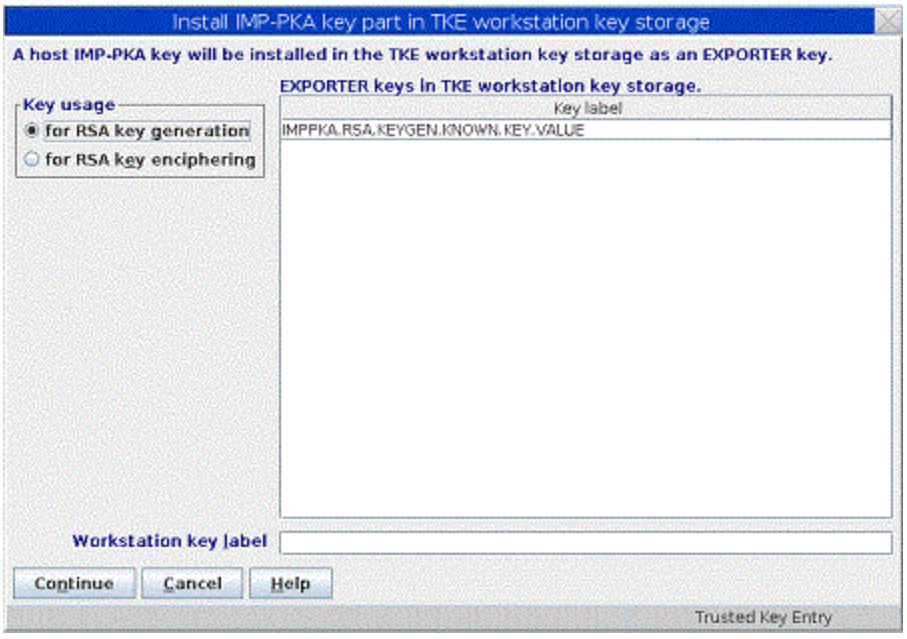


Figure 124. Install IMP-PKA Key Part in Key Storage

Note: For the RSA key to be loaded into the PKDS, the same IMP-PKA key value must be stored in the CKDS. See "Load single key part" on page 173.

AES operational key: Load to Key Storage

This selection is only possible for AES IMPORTER keys. An AES IMPORTER key can be used to protect RSA keys during transport from the workstation to ICSF as long as the 'Key can be used for IMPORT', 'Key can be used for GENERATE-PUB' and 'Key can wrap RSA keys' attributes are set to 'Yes' in the key's attributes. After selecting **Load to Key Storage**, the user chooses one of the following key parts to load to the workstation key storage:

- First...
- Intermediate...
- Last...

The contents of the container depend upon the user's selection.

If the user selected **First**, the container shows all keys in the workstation key storage usable as AES IMPORTER key encrypting keys. The user can utilize these as skeletons for composing the new key label.

If the user selected **Intermediate** or **Last**, the container shows all keys in the workstation key storage that have been installed with the first key part. It also shows any optional intermediate key parts that have been installed. The user must select one of these as the key label.

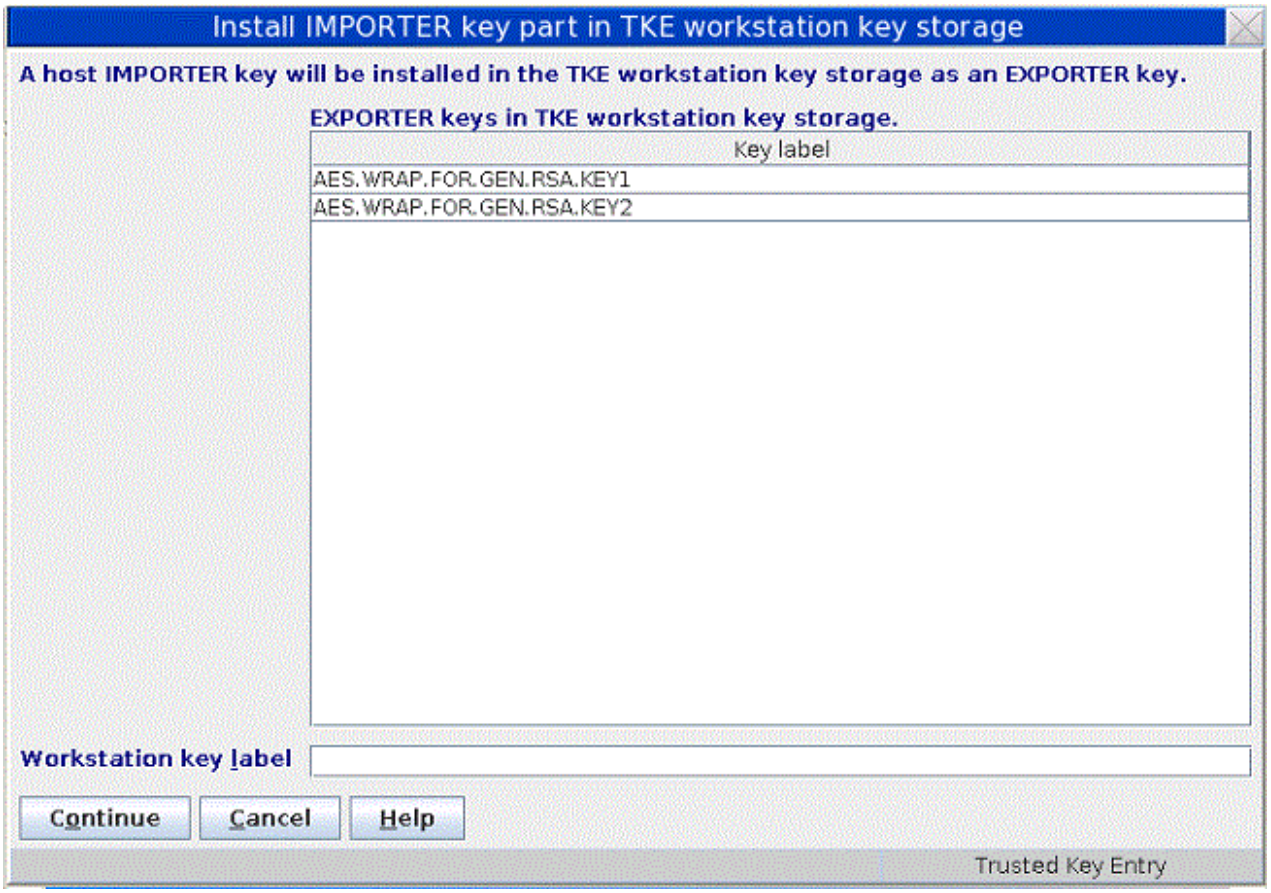


Figure 125. Install AES IMPORTER Key Part in Key Storage

Note: For the RSA key to be loaded into the PKDS, the AES IMPORTER key value must be stored in the CKDS. See "Load single key part" on page 173.

Secure key part entry

To save known key part values to a TKE smart card, use secure key part entry. Refer to Appendix A, "Secure key part entry," on page 311 for details on using this function.

RSA keys

Generate RSA Key

This selection initiates RSA key generation at the workstation. The generated RSA key is protected with a previously generated DES IMP-PKA or AES IMPORTER key, and the encrypted RSA key is saved in a file.

Notes:

- RSA keys can also be generated and saved in the host PKDS using ICSF panels and services (CSNDPKG for generate, and CSNDKRC or CSNDKRW to write to the host PKDS.) For more information, see *z/OS Cryptographic Services ICSF Application Programmer's Guide*.
- An RSA key with a length of 1024 or less can be wrapped with a DES IMP-PKA or AES IMPORTER key.
- An RSA key with a length greater than 1024 must be wrapped with an AES IMPORTER key.

From the Domain Keys page, right-click **RSA key** in the **Key Types** container and select **Generate**. The **Generate RSA Key** window opens.

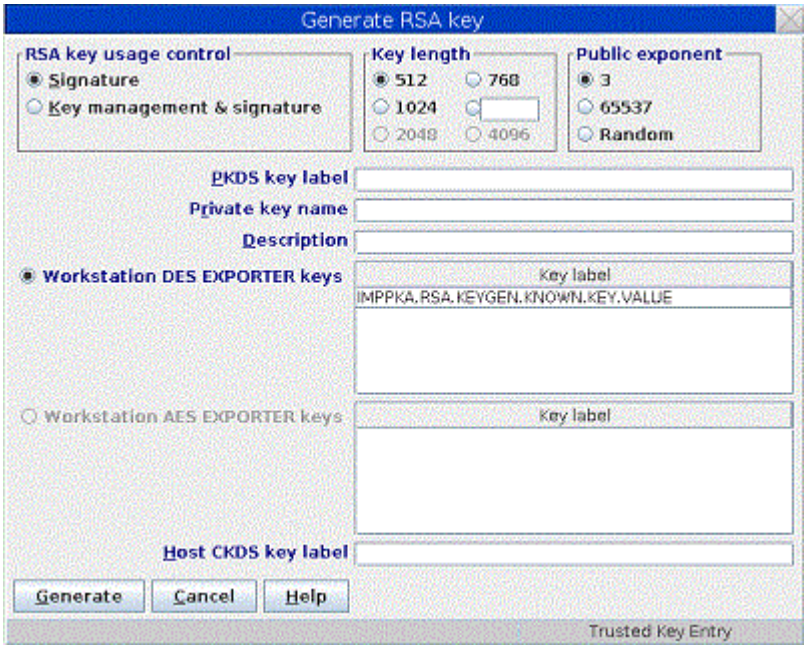


Figure 126. Generate RSA Key

In the **Generate RSA key** window, specify the following information:

RSA key usage control
Specifies whether or not the RSA key can be used for key management purposes (encryption of DES keys). All RSA keys can be used for signature generation and verification.

Key length
Length of the modulus of the RSA key in bits. For RSA keys protected by a DES EXPORTER key, any length between 512 and 1024 is allowed. For RSA keys protected by an AES EXPORTER key, any length between 512 and 1024, and lengths of 2048 and 4096 are allowed. When a length of 2048 or 4096 is selected, the AES EXPORTER key should be at least 24 bytes long. If not, a message is displayed.

Public exponent
Value of the public exponent of the RSA key.

PKDS key label
Label to be given the imported RSA key at the host. The information provided in this field can be changed when you load the RSA key to the host.

Private key name
Text string that is included in the RSA key token and cryptographically related to the key. The private key name can be used for access control for the key. The information you entered in the PKDS key label field is copied to this field and can be edited.

Description
Optional free text that is saved with the RSA key and displayed when you retrieve the key.

Workstation DES EXPORTER keys
This container displays the labels of the DES EXPORTER keys currently in TKE workstation DES key storage that can be used to protect RSA keys generated at the TKE workstation. When these keys were loaded into TKE DES key storage, key usage of "for RSA key generation" was specified. To select one of these keys, click **Workstation DES EXPORTER keys** and select a key label.

Workstation AES EXPORTER keys
This container displays the labels of the AES EXPORTER keys currently in TKE workstation AES key storage that can be used to protect RSA keys generated at the TKE workstation. Only keys with set attributes including "Key can be used for IMPORT", "Key can be used for GENERATE-PUB", and "Key can wrap RSA keys" are listed. To select one of these keys, click **Workstation AES EXPORTER keys** and select a key label.

Host CKDS key label
The CKDS key label at the host used to import the RSA key. The selected workstation DES EXPORTER or AES EXPORTER key label is copied to this field and can be edited. This information can be changed when you load the RSA key to the host.

When the key is generated, a window opens that prompts the user to specify the file location (USB flash memory drive or TKE Data Directory) and file name for saving the generated RSA key.

Attention : Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages might be generated on the TKE workstation.

Encipher RSA Key

This selection allows an RSA key to be read from a clear key file, encrypted with a previously generated IMP-PKA key encrypting key, and saved in a file. The format of the clear key file is described in Appendix D, “Clear RSA key format,” on page 329.

Having selected the Encipher action, the Encipher RSA Key window is displayed:

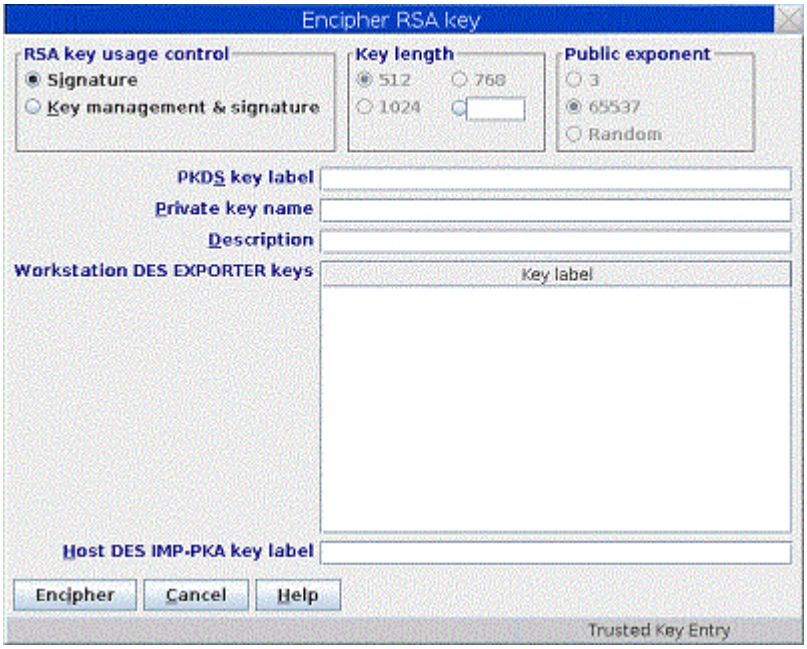


Figure 127. Encipher RSA Key

In the Encipher RSA key window, specify the following information:

- **RSA key usage control** — Specifies whether the RSA key can be used for key management purposes (encryption of DES keys). All RSA keys can be used for signature generation and verification.
- **PKDS key label** — Label to be given the imported RSA key at the host. The information provided in this field can be changed when you load the RSA key to the host.
- **Private key name** — Text string that is included in the RSA key token and cryptographically related to the key. The private key name can be used for access control for the key. The information you entered in the PKDS key label field is copied to this field and can be edited.
- **Description** — Optional free text that is saved with the RSA key and displayed when you retrieve the key.
- **Workstation DES EXPORTER keys** — This container displays the labels of the DES EXPORTER keys currently in TKE workstation DES key storage that can be used to protect RSA keys entered from a clear key file. When these keys were loaded into TKE DES key storage, key usage of "for RSA key enciphering" was specified. AES EXPORTER keys in TKE workstation AES key storage cannot be used to encipher an RSA key. Select a key label by clicking it.

- **Host DES IMP_PKA key label** — The CKDS key label at the host used to import the RSA key. The selected workstation DES EXPORTER key label is copied to this field and can be edited. This information can be changed when you load the RSA key to the host.

When the key is enciphered, a file chooser window is displayed for the user to specify the file location (USB flash memory drive or TKE Data Directory) and file name for saving the encrypted RSA key.

Attention : Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages might be generated on the TKE workstation.

Load RSA Key to PKDS

This selection allows the user to load an RSA key to the host and install it in the PKDS. Using this function, it is only possible to load the RSA key to the PKDS in the TKE Host logical partition (LPAR). For loading RSA keys to TKE target LPARs, see “Load RSA key to host dataset ” on page 187.

Having selected **Load to PKDS**, a dialog box is displayed for selecting the input file holding the encrypted RSA key. When completed, the **Load RSA key to PKDS** window is displayed.

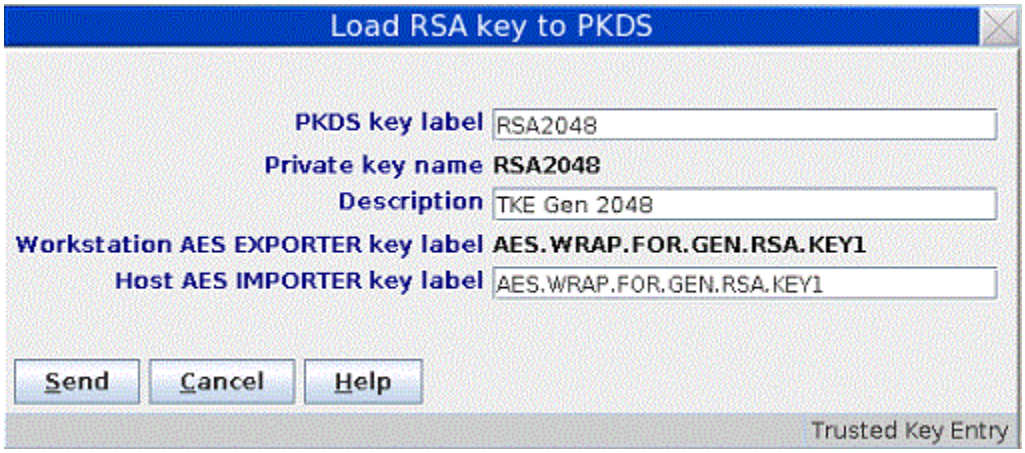


Figure 128. Load RSA Key to PKDS

In the **Load RSA key to PKDS** window, specify the following information:

- **PKDS key label** — Label to be given the imported RSA key at the host. Change this field as needed.
- **Private key name** — Text string that is included in the RSA key token and cryptographically related to the key. The private key name can be used for access control for the key. The information you entered in the PKDS key label field is copied to this field and can be edited.
- **Description** — Optional free text that was saved with the RSA key.
- **Workstation DES EXPORTER key label** — Label of the workstation DES IMP-PKA key that protects the RSA key. Displayed when the key-encrypting key is a DES IMP-PKA key.
- **Workstation AES EXPORTER key label** — Label of the workstation AES IMPORTER key that protects the RSA key. Displayed when the key-encrypting key is an AES IMPORTER key.
- **Host DES IMP-PKA key label** — Label of the DES IMP-PKA key stored in the host CKDS that will be used to import the RSA key. Displayed when the key-encrypting key is a DES IMP-PKA key. Change this field as needed.
- **Host AES IMPORTER key label** — Label of the AES IMPORTER key stored in the host CKDS that will be used to import the RSA key. Displayed when the key-encrypting key is an AES IMPORTER key. Change this field as needed.

Load RSA key to host dataset

This selection allows the user to load an RSA key to a host data set as an external key token. From this data set it is possible to install the key in the PKDS by means of TSO/E ICSF panels.

The host data set must be defined in advance. If a workstation DES EXPORTER key was used to protect the RSA key at the time the RSA key was generated or enciphered, the host data set must have the following attributes:

```
recfm fixed, lrecl=1500, partitioned
```

If a workstation AES EXPORTER key was used to protect the RSA key at the time the key was generated, the host data set must have the following attributes:

```
recfm fixed, lrecl=3000, partitioned
```

Using this installation method, it is possible to load RSA keys into any PKDS in any LPAR. For information about the TSO/E ICSF interface, "Installing RSA keys in the PKDS from a data set" on page 248.

The steps are the same as for loading an RSA key to PKDS (see "Load RSA Key to PKDS" on page 186), except that the user has to specify the full data set and member name. If you do not specify the data set and member name in quotes, the high level qualifier for the data set is the TSO/E logon of the administrator/host user ID.

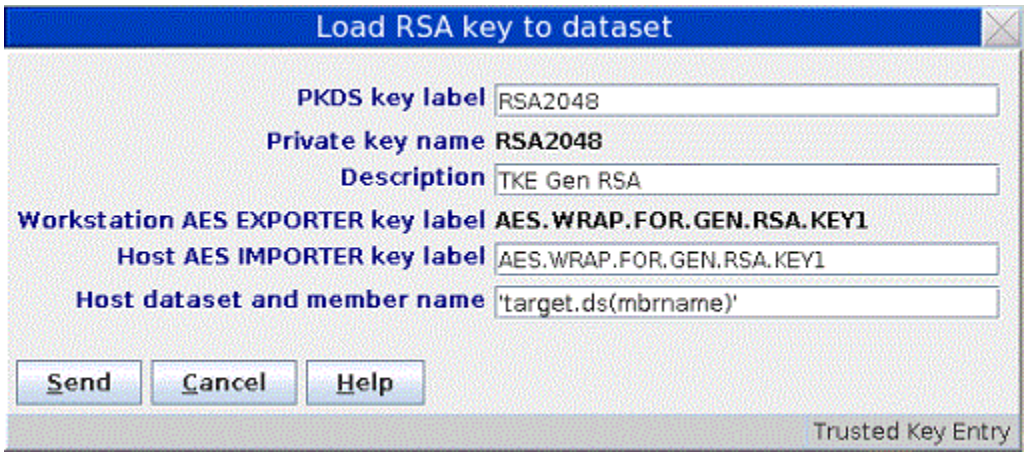


Figure 129. Load RSA Key to Dataset

Domain Controls pages

The Domain Controls pages display the cryptographic functions that are allowed for the domain and allows you to make changes to them. The 'Controls-Desc' page displays the domain controls sorted by description, and the 'Controls-ACP' page displays the domain controls sorted by ACP value.

- To change a setting, click on it. Changing a setting on one domain controls page changes the corresponding setting on the other domain controls page.
- To upload the controls settings to the crypto module, click **Send updates**.
- To leave the controls settings unaltered after you have made changes to the page, click **Discard changes**.
- To save the displayed domain control settings to a file, click **Save to file**.
- To load the domain control settings from a previously saved file, click **Load from file**. This option changes the displayed control settings. Click **Send updates** to upload the displayed settings to the crypto module.

The last two options cause a window to open that allows you to select the file to use.

Notebooks for a host crypto module at CCA 5.2 or later will also show an **ACP Tracking** button. See "Access Control Tracking" on page 189 for more information about the function of the **ACP Tracking** button.

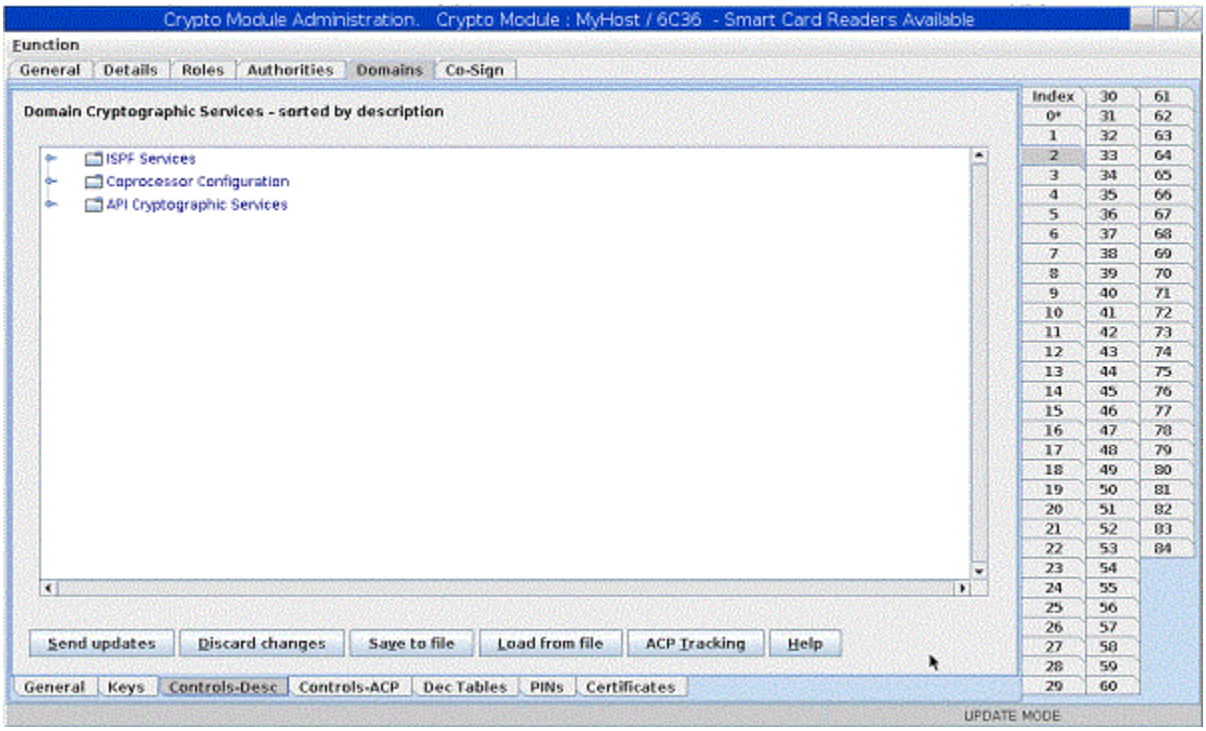


Figure 130. Domain Controls page

Note: When managing domain controls through a TKE workstation, some services displayed on the Domain Controls panel might not be available on the host crypto module. Enabling a service on this panel that is not supported by the host crypto module does not make this service available.

Working with Domain Controls settings

You can enable and disable access control points to ISPF Services, API Cryptographic Services and User Defined Extensions (UDX) from these pages.

There are expandable folders for the Domain Cryptographic services. Some services cannot be disabled because they are “required”. This is indicated on the panel. You can enable or disable services within the following folders:

- ISPF Services
- Coprocessor Configuration
- API Cryptographic Services
- UDXs (appears only if you have created UDXs on your system)

The access control points displayed on the Domain Controls pages depend on the level of ICSF used to communicate with the host crypto module. Later versions of ICSF may support additional access control points not supported on earlier versions.

Some access control points displayed on the Domain Controls pages may not be implemented on the host crypto module. You can change the value of these access control points, but they do not affect the operation of the host crypto module.

When moving to a later version of ICSF, you may need to manually set or reset the new access control points that are displayed.

ISPF Services

Under the ISPF Services folder, there are check boxes for the services that you can enable or disable. These services are for loading and setting the DES, AES, ECC (APKA), and RSA master keys on supported host crypto modules through the ICSF panel interface. These services are listed in Appendix E, 'CCA access control points and ICSF utilities', in *z/OS Cryptographic Services ICSF Administrator's Guide*.

Coprocessor Configuration

Under the Coprocessor Configuration folder are all of the controls that govern the key wrapping behavior of ICSF callable services. See the table, 'Access control points affecting multiple services or requiring special consideration', in *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

API Cryptographic Services

Under the API Cryptographic Services folder are all the ICSF services that can be enabled or disabled from the TKE workstation. See the table, 'Access control points – Callable Services', in *z/OS Cryptographic Services ICSF Application Programmer's Guide* for the correlation between the access control point and the ICSF callable service.

UDXs

The UDX folder appears only if there are User Defined Extensions on your system. The UDXs folder lists your extensions and allows you to enable or disable them.

Access Control Tracking

Beginning with CCA 5.2, CCA host crypto modules can keep track of the access control points that are checked as applications run. Tracking is done on a per domain basis. The tracking information can be used to tailor the domain controls that are enabled for the domain.

To enable tracking and to view the tracking data, click on the **ACP Tracking** button. This brings up a secondary panel with tracking information displayed in a tree format and buttons at the bottom of the panel to control tracking. A signature key must be loaded in order to obtain and display the tracking data.

Beginning with TKE 9.2 and CCA 7.0, additional information about the tracking data is displayed at the top of the panel. When tracking started and when tracking ended is shown, as well as the number of times tracking was suspended during that interval. If tracking is currently active, the text indicates 'Still tracking...'. If tracking has never been active for the domain or has not been active since the last time the tracking data was cleared, the text indicates 'Tracking data has not been collected for this domain'.

A check mark next to the tracking information indicates that an application running in the domain attempted to run a function that required the access control point to be enabled. A check mark indicates only that execution was attempted and not that the execution request was granted.

The Access Control Tracking panel has the following buttons:

Start
: Starts access control tracking for the domain. This button is displayed only when access control tracking is off.

Stop
: Stops access control tracking for the domain. This button is displayed only when access control tracking is on.

Refresh
: Obtains and then re-displays the tracking data. Clicking on the **Start**, **Stop**, and **Clear** buttons also refreshes the panel.

Clear
: Clears the access control tracking data for the domain.

Save
: Saves the access control tracking data for the domain to a file.

Print
: Prints the access control tracking data for the domain. This button is displayed only when print support is enabled.

Done
: Closes the Access Control Tracking panel.

Help
Displays the online help information for the Access Control Tracking panel.

The **ACP Tracking** button is displayed only for the CCA host crypto modules that support access control tracking.

Domain Decimalization Tables page

Decimalization tables map hexadecimal digits to decimal digits, and are used in certain host crypto module operations that process Personal Identification Numbers (PINs). By selecting **Use Only Valid Decimalization Table** in the domain controls for a domain, you can restrict the set of allowed decimalization tables for the domain. Only decimalization tables with a status of “Active” in the **Decimalization Tables** page are allowed to be used.

Decimalization tables can contain only decimal digits (0 through 9) and must be exactly 16 digits long. Every domain has slots for 100 decimalization tables. These tables can be managed only from a TKE workstation. You can load, activate, or delete tables from this page. The **Decimalization Tables** page is displayed only for host crypto modules that support decimalization tables.

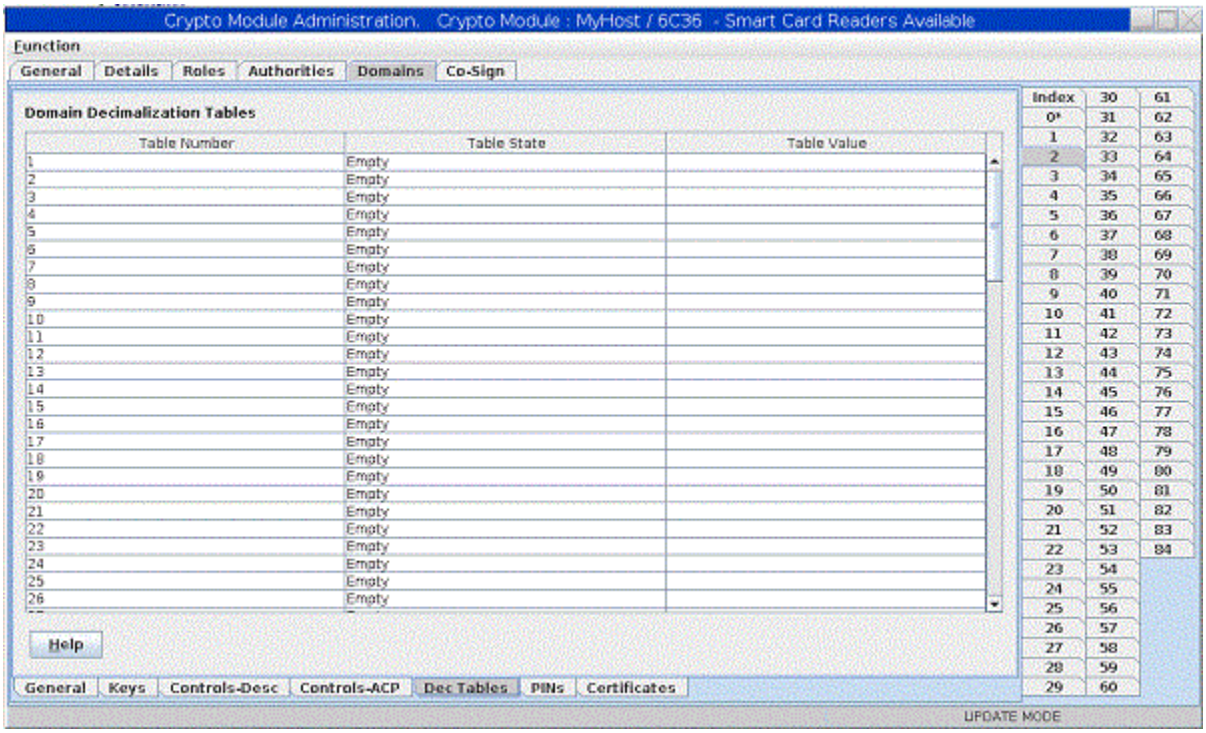


*Figure 131. **Decimalization tables** page*

To manage a table entry, right-click on an entry to display command options. The available options are:

- **Load**
- **Activate**
- **Activate All**
- **Delete**
- **Delete All**

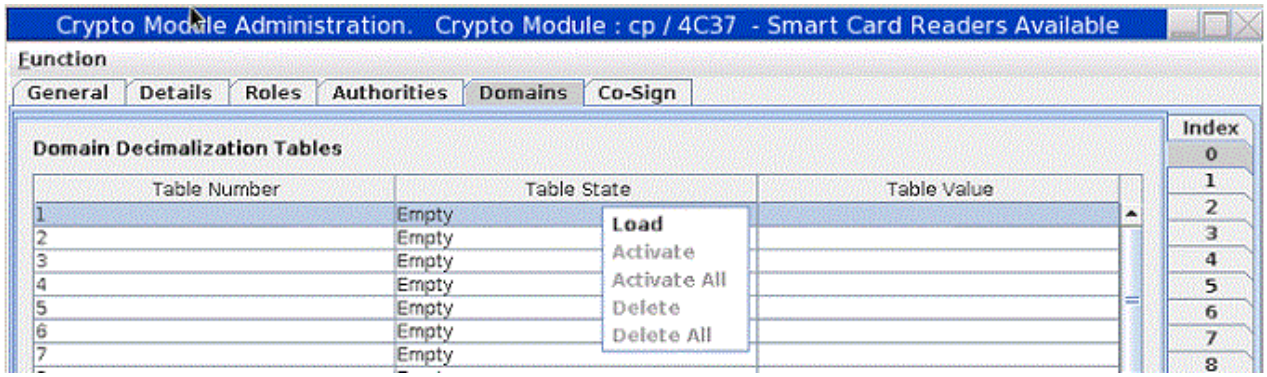


Figure 132. Table entry options

There are three access control points that control the ability to manage decimalization Tables. They are:

- Load Decimalization Tables
- Delete Decimalization Tables
- Activate Decimalization Tables

A table entry can be in any of the following states:

- Empty
- Active
- Loaded

Load table

Right-click on a table entry to display the table options. Select the load option. From the “Enter new decimalization table value” screen, enter a 16-digit decimalization table value. The table can contain only decimal digits (0 through 9). Press the **Continue** button to create the table entry.

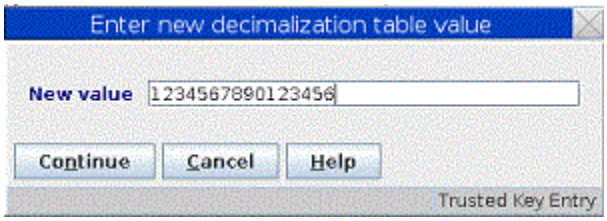


Figure 133. Enter new decimalization table value

Notes:

1. You must have the “load” ACP in order to load a table.
2. If the status of a table entry is “Active”, you must also have the “Delete” ACP to load a new table. You must be allowed to delete the current table.
3. If you load a table, and you also have the “activate” ACP, the new table is immediately activated.

Activate or Activate All

Right-click on a table entry to display the table options. Select the Activate or Activate All option. After the command completes successfully, press the **Close** button in the information message box.

Notes:

1. Only tables with a current state of “Loaded, Not Active” can be activated.
2. You must have the “activate” ACP to activate a table.

Delete or Delete All

Right-click on a table entry to display the table options. Select the Delete or Delete All option. After the command completes successfully, press the **Close** button in the information message box.

Note:

1. Only tables with a current state of “Loaded, Not Active” or “Active” can be deleted.
2. You must have the “delete” ACP to delete a table.

Domain Restricted PINs page

You can restrict the use of weak or trivial Personal Identification Numbers (PINs) in a domain by using the **Domain Restricted PINs** page. You can specify up to 20 PIN values to be disallowed. Disallowing a PIN value prevents users from changing a PIN to the disallowed value, and prevents CCA verbs from ever generating the disallowed PIN value. Disallowing a PIN value on the **Domain Restricted PINs** page does not affect the use of existing PINs, however, even if they have the disallowed value.

The PINs to be disallowed can be 4 - 12 digits long, and can contain only decimal digits (0 through 9). The **Domain Restricted PINs** page is displayed only for host crypto modules that support restricting weak or trivial PINs.

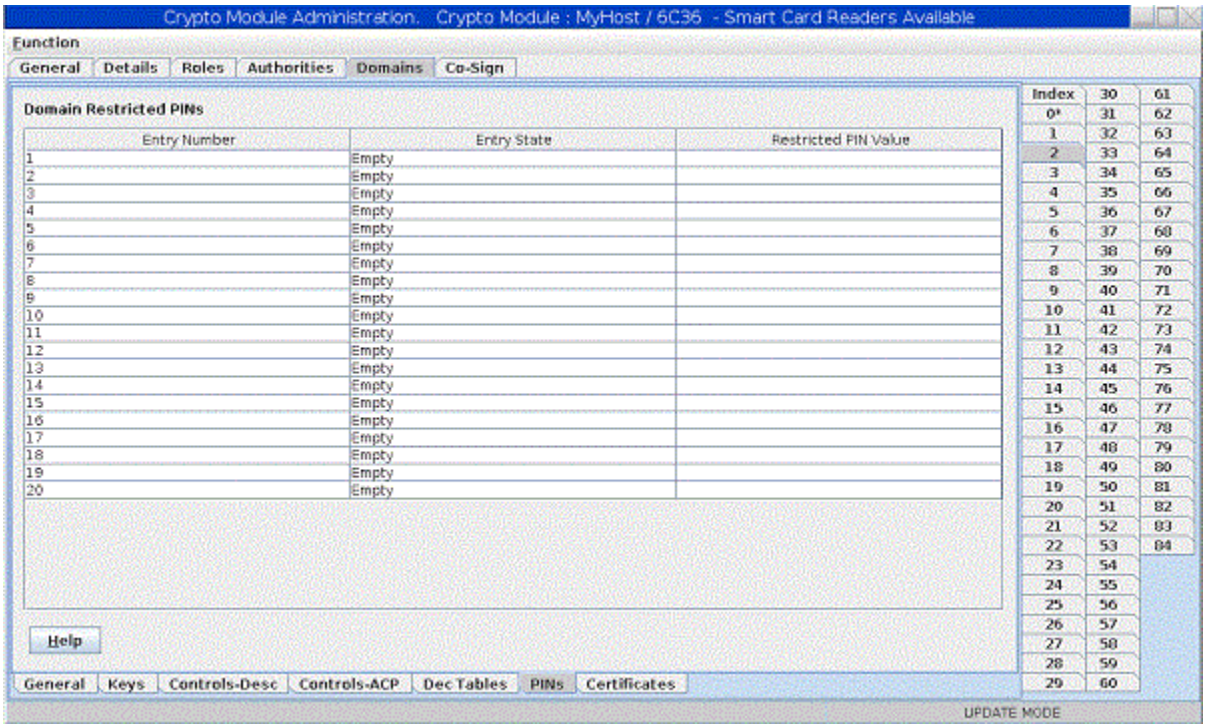


*Figure 134. **Domain Restricted PINs** page*

To manage an entry, right-click on the entry to display command options. The available options are:

- **Load**
- **Activate**
- **Activate All**
- **Delete**
- **Delete All**

Options that are not valid are disabled. An option might be invalid because of the state of the selected entry (you cannot delete an empty entry, for example), or because the role of the current authority does not allow the option.

There are three access control points in roles that control the ability to manage what PINs are restricted:

- Load Restricted PIN
- Activate Restricted PIN
- Delete Restricted PIN

When you select the **Load** option, a window opens in which you can enter the value of the PIN to be restricted. You can enter 4 - 12 decimal digits. If the role of the current authority has both the load and the activate ACPs selected, the entry goes to the “Active” state. If the role of the current authority has only the load but not the activate ACP selected, the entry goes to the “Loaded, Not Active” state. Separate ACPs for the load and activate options supports dual control of adding a PIN to the restricted PINs list, for users who require dual control.

You can load an entry that is already in the “Loaded, Not Active” or “Active” state, if the role of the current authority has the Delete Restricted PIN ACP. This ACP is required because reloading an entry effectively deletes the current entry.

The **Activate** option changes the state of the entry from “Loaded, Not Active” to “Active”.

The **Delete** option removes the PIN and changes the state of the entry to “Empty”.

The **Activate All** option activates all entries that are in the “Loaded, Not Active” state.

The **Delete All** option deletes all entries in the table.

Domain Certificates page

Beginning with the CEX6C crypto module, each domain can load and manage a set of parent X.509 certificates for validating operational X.509 certificates that are used by applications in the domain.

Certificates are identified by a certificate label. The Domain Certificates page displays the set of certificates that have been loaded for the domain. Right-clicking in the panel displays a pop-up menu that allows you to perform the following operations:

Load certificate
Loads a certificate from a file on the TKE workstation or from USB memory.

Activate certificate
A certificate must be activated before it can be used by applications. If the role associated with the current signature key and index has both load and activate authority, the certificate is activated automatically when it is loaded.

Delete certificate
Removes the certificate from the domain.

Display certificate
Displays information from the certificate, such as the issuer and period of validity.

Change certificate label
Allows you to choose a new label to associate with the certificate.

Replace certificate
Replaces an installed certificate. The replacement certificate must have the same public key as the original certificate. This can be used to replace an expired certificate without requiring dual control.

Validate certificate
Allows you to determine whether the input certificate is validated by one of the installed parent certificates in the domain. The certificate to be validated can be in a file on the TKE workstation or on USB memory.

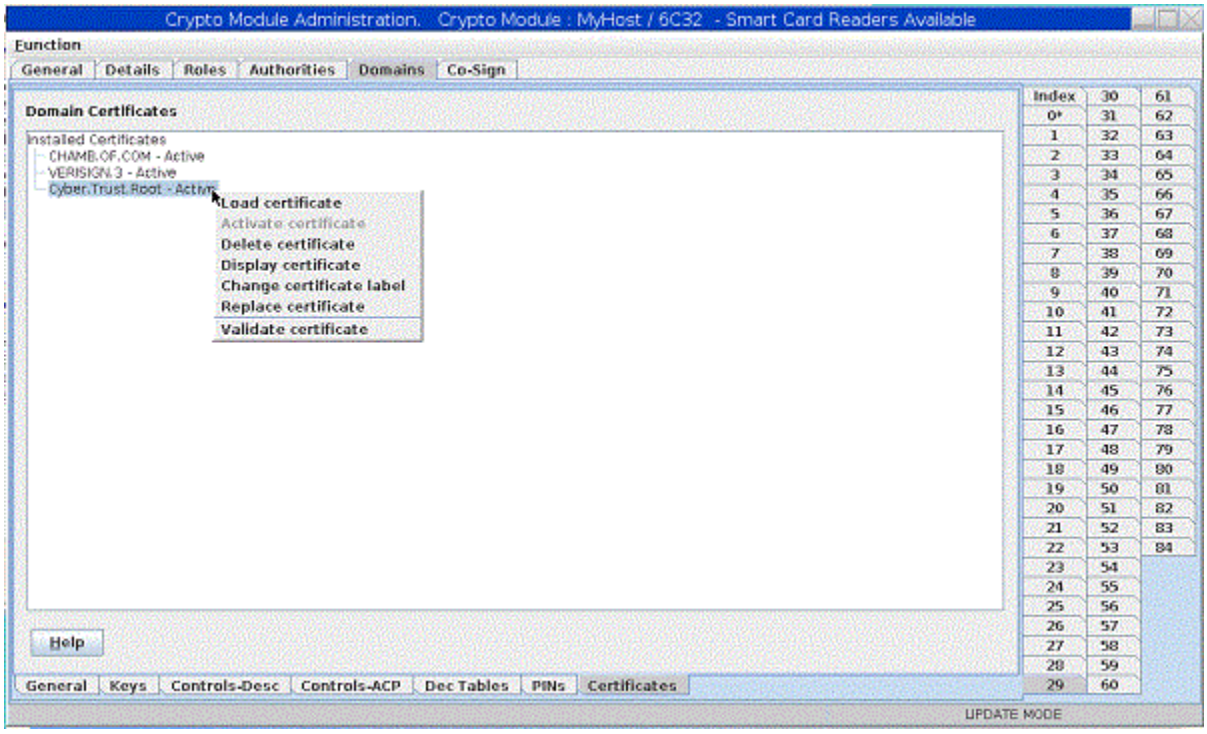


Figure 135. Domain certificates

Domain Roles page

Beginning with the CEX6C crypto module, domains can exist in various modes or distinct operational states. Domains in imprint mode or PCI-compliant mode are administered by using domain-specific roles and authorities.

When a domain changes from normal mode to imprint mode, extra tabs are displayed at the bottom of the crypto module notebook panel that allow you to work with the domain roles, domain authorities, and domain audit log.

When the **Domain Roles** tab is selected, the set of domain-specific roles that are installed in the domain is displayed. This panel looks the same as the panel for module-wide roles. Right-clicking in the panel displays a pop-up menu with options to create, change, delete, and view domain-specific roles for the domain.

When you create or change a domain-specific role, the set of access control points that the role is allowed to have is different than for the module-wide roles. To meet PCI requirements for dual control, domain-specific roles cannot have certain combinations of access control points that are enabled in the same role:

- A role cannot have both issue and cosign authority for a given operation.
- For domain decimalization tables, domain PINs, and domain certificates, a role cannot have both load and activate authority.
- A role cannot have both load new first key part and combine new middle key part authority for a given master key type.
- A role cannot have both load new first key part and combine new final key part authority for a given master key type.
- For DES, AES, AES KEK, and HMAC operational keys, a role cannot have both load first key part and load additional key part authority.

The INITADDM role is automatically created when a domain enters imprint mode and cannot be changed or deleted. It can be used only while the domain is in imprint mode.

Domain Authorities page

Domains in imprint mode and PCI-compliant mode are administered by using domain-specific roles and authorities.

The **Domain Authorities** tab displays the set of domain-specific authorities that are installed in the domain. The panel looks the same as the panel for module-wide authorities. Right-clicking in the panel displays a pop-up menu with options to create, change, delete, and view domain-specific authorities for the domain and to generate an authority signature key.

Domain-specific authorities must be assigned an authority index in the range 100 to 999. When a domain enters imprint mode, a domain-specific authority with index 100 is automatically created. It is assigned the INITADDM role and a default signature key. Users are allowed to change and delete the domain-specific authority with index 100. On the transition to PCI-compliant mode, if the domain-specific authority with index 100 still exists and uses the default signature key, it is deleted automatically.

Domain Audit Log page

For domains in imprint mode and PCI-compliant mode, a domain audit log is displayed to users and is active.

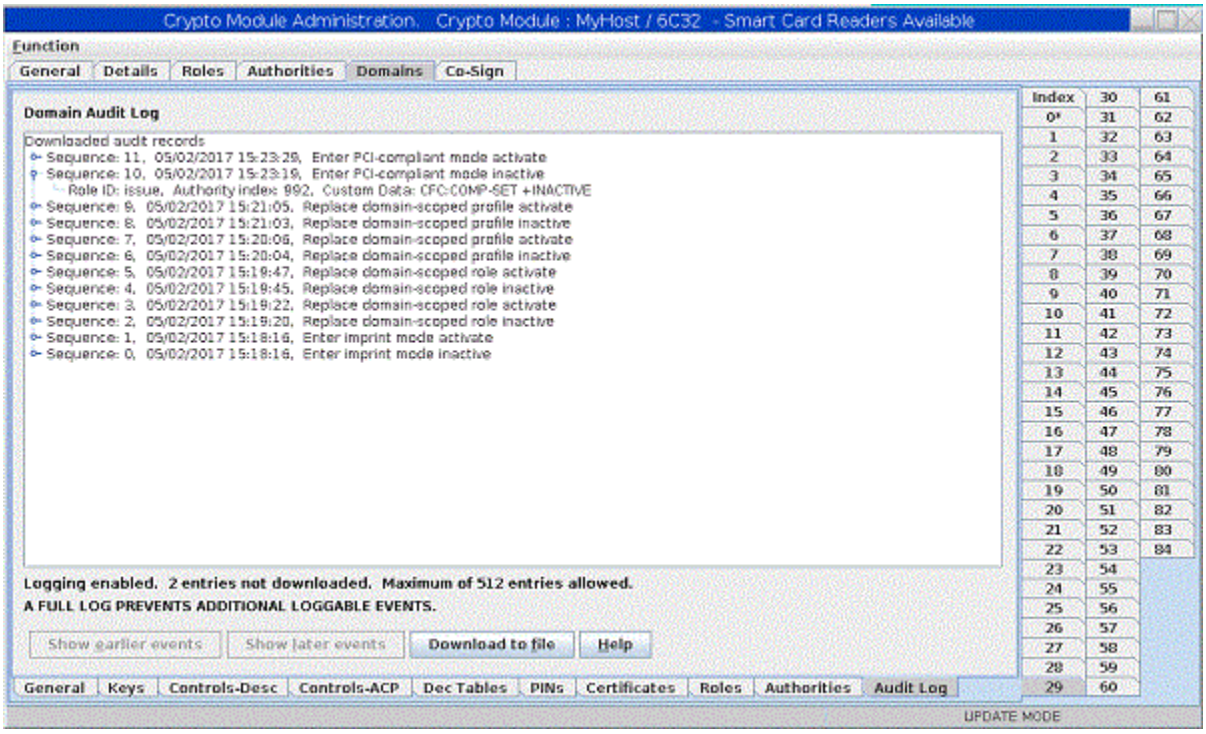


Figure 136. Domain audit log

The domain audit log has room for 512 entries. If the log fills, most TKE administrative operations in the domain are blocked until space is available in the log to create more audit log entries. The domain audit log can be read and cleared by clicking the **Download to file** button.

The **Domain Audit Log** page displays how many entries in the domain audit log are currently used. This information is also displayed on the **Domain General** page.

The audit log entries that are displayed on the **Domain Audit Log** page are those that have been downloaded to a file on the TKE workstation. Audit log entries still on the crypto module are not displayed.

To work with the audit log files on the TKE workstation by using the TKE File Management utility, you must sign on the TKE console by using the AUDITOR privileged mode ID.

Crypto Module Notebook Co-Sign tab

For co-signing a pending command in a host crypto module, open the notebook for that crypto module and select the **Co-Sign** tab. The **Co-Sign** tab panel displays the following information on the command to co-sign:

- **Pending command** – Name of the pending command
- **Pending command reference** – Unique hexadecimal number returned to the issuer of the command
- **Loading Authority** – Issuer of the command
- **Pending command details container** – Important parts of the pending command
- **Signature requirements container** – Current status for the fulfillment of the signature requirements

  For a host crypto module, exactly two signatures are required for a dual-signature command. The authority index and name of each authority allowed to sign the pending command are displayed.

Authorities who have already signed the command are indicated by a **Yes** in the column labeled ***Signed***.

Pressing the **Co-sign** push button initiates the signing of the pending command. It opens windows in which you can choose the source of the authority signature key and then choose the authority index associated with that key. The possible authority signature key sources are as follows:

- **Current key** - Uses the currently loaded signature key
- **Smart card** - Reads an authority signature key from a TKE smart card
- **Binary file** - Reads an authority signature key from a hard disk or diskette
- **Key storage** - Reads an authority signature key from PKA key storage
- **Default key** - Uses the default authority signature key hardcoded into TKE

Press **Delete** if you want to delete the pending command.

Host crypto module index values

After a host or domain group is opened, a list of cryptographic modules is displayed. Table 32 on page 196 shows the crypto module index value that is displayed based on the type of module and the mode it is running.

Notes:

- A host cryptographic coprocessor running IBM Common Cryptographic Architecture (CCA) code is running in CCA mode.
- A host cryptographic coprocessor running IBM Enterprise PKCS #11 (EP11) code is running in EP11 mode.

Table 32. Module index type displayed on the TKE

Host cryptographic coprocessor type and mode	Module index type displayed on the TKE	
	TKE 8.0 or later	Prior to TKE 8.0
Crypto Express7S running in EP11	7P*xx*	N/A
Crypto Express7S running in CAA mode	7C*xx*	N/A
Crypto Express6S running in EP11	6P*xx*	N/A
Crypto Express6S running in CAA mode	6C*xx*	N/A
Crypto Express5S running in EP11 mode	5P*xx*	N/A
Crypto Express5S running in CAA mode	5C*xx*	N/A
Crypto Express4S running in EP11 mode	4P*xx*	SP*xx*

Table 32. Module index type displayed on the TKE (continued)		
Host cryptographic coprocessor type and mode	**Module index type displayed on the TKE**	
	TKE 8.0 or later	**Prior to TKE 8.0**
Crypto Express4S running in CAA mode	4C*xx*	SC*xx*
Crypto Express3 running in CAA mode	3C*xx*	G*xx*
Crypto Express2 running in CAA mode	2C*xx*	E*xx*

Placing a domain in PCI-compliant mode

Beginning with Crypto Express6S running in Common Cryptographic Architecture (CCA) mode, host crypto module domains can be configured to run in PCI-compliant mode. Two of the PCI requirements make managing a PCI-compliant domain different from managing a normal mode domain:

- Administrative actions that are done in a PCI-compliant domain must be performed by domain-specific authorities.
- When managing a PCI-compliant domain, it must take at least two authorities to perform sensitive administrative actions. That is, management requires dual controls.

Note: TKE already provides the ability to manage settings with dual controls. Therefore, this might not be a change to your host crypto module security management policy.

For information about required dual controls, see "Required dual controls" on page 197. For information on how to configure a domain to be in PCI-compliant mode, see "Configuring a domain to be in PCI-compliant mode" on page 197.

Required dual controls

A key requirement of PCI standards is that one authority cannot have a role that allows them to do an entire sensitive configuration operation by themselves. There are two methods for enforcing dual controls:

Issue and co-sign
If the role of the authority can issue a sensitive command, the role cannot also have the corresponding co-sign authority for that command. Three examples of commands that use the issue and co-sign mechanism are:

- Create and change role.
- Create and change authority.
- Changing domain controls.

Multiple commands
If it takes two commands to complete a sensitive action, the role of the authority cannot include the authority to do all of the commands that are needed to complete the operation. An example of this situation is the load master key operation. When you load ANY key from the TKE, you must enter at least two key parts. The role of the authority that can load the first part cannot have the authority to load the corresponding intermediate or last key part.

Any attempt to create or change a domain-specific role, such that it violates any required dual control rules, fails.

Configuring a domain to be in PCI-compliant mode

There are four steps to move a domain from normal to PCI-compliant mode:

1. Create the smart cards that are needed to hold the domain-specific authority signature keys and key parts that are used when managing the PCI-compliant domain.

Note: In TKE 9.0, the Smart Card Utility Program (SCUP) includes the PCI-HSM smart card wizard, which takes you through the process of initializing and personalizing the smart cards that you need. The wizard even creates a TKE zone if you do not have one yet.

In TKE 9.1, the PCI-HSM smart card wizard features were folded into the TKE Smart Card Wizard. This wizard provides you with the option to initializing and personalizing the smart cards that you need. The wizard even creates a TKE zone if you do not have one yet.

You can load a domain-specific authority into as many domains as you like. Therefore, depending on your security policy, you might need only one set of smart cards for managing your PCI-compliant domains.

For more information, see "Step 1: Create the smart cards needed to manage a PCI-compliant domain" on page 198.

You can load a domain-specific authority into as many domains as you like. Therefore, depending on your security policy, you might need only one set of smart cards for managing your PCI-compliant domains.

For more information, see "Step 1: Create the smart cards needed to manage a PCI-compliant domain" on page 198.

2. Move the domain to imprint mode. This is a simple push of a button by an authorized administrator.

   For more information, see "Step 2: Place a domain in imprint mode" on page 202.

3. Create, at least, the minimum number of domain-specific authorities necessary to manage the PCI-compliant domain.

   Note: Once a domain is in imprint mode, the Setup PCI Environment wizard creates a set of domain-specific roles and domain-specific authorities for managing a PCI-compliant domain. In TKE 9.1, the Setup PCI Environment wizard only works with smart cards that have specific descriptions. The Setup PCI Environment wizard uses smart cards that were initialized in either the older PCI-HSM smart card wizard or the newer TKE Smart Card Wizard.

   For more information, see "Step 3: Create the domain-specific roles and authorities needed to manage a PCI-compliant domain" on page 203.

   Note: Once a domain is in imprint mode, there is a wizard that creates a set of domain-specific roles and domain-specific authorities for managing a PCI-compliant domain. The wizard does not depend on the PCI-HSM smart card wizard, but the two wizards are designed to work together.

   For more information, see "Step 3: Create the domain-specific roles and authorities needed to manage a PCI-compliant domain" on page 203.

4. Move the domain to PCI-compliant mode. This is a simple push of a button, but requires two authorities. The first authority is allowed to issue the command and the second authority must co-sign the command.

   Note: Once in PCI-compliant mode, managing domain settings is done by using the same procedures that you use in normal mode. However, dual administration is now required.

   For more information, see "Step 4: Place a domain in PCI-compliant mode" on page 206.

Step 1: Create the smart cards needed to manage a PCI-compliant domain

For TKE 9.0

The Smart Card Utility program has a feature that is called PCI-HSM smart card wizard. It is started from the **File > PCI-HSM smart card wizard** pull down menu.

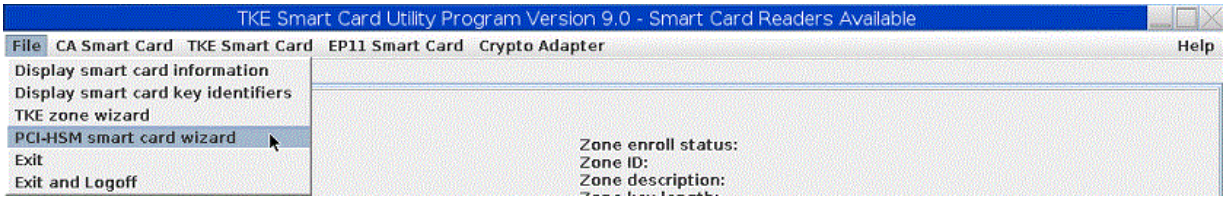


Figure 137. PCI-HSM smart card wizard

The wizard presents you with a welcome screen.

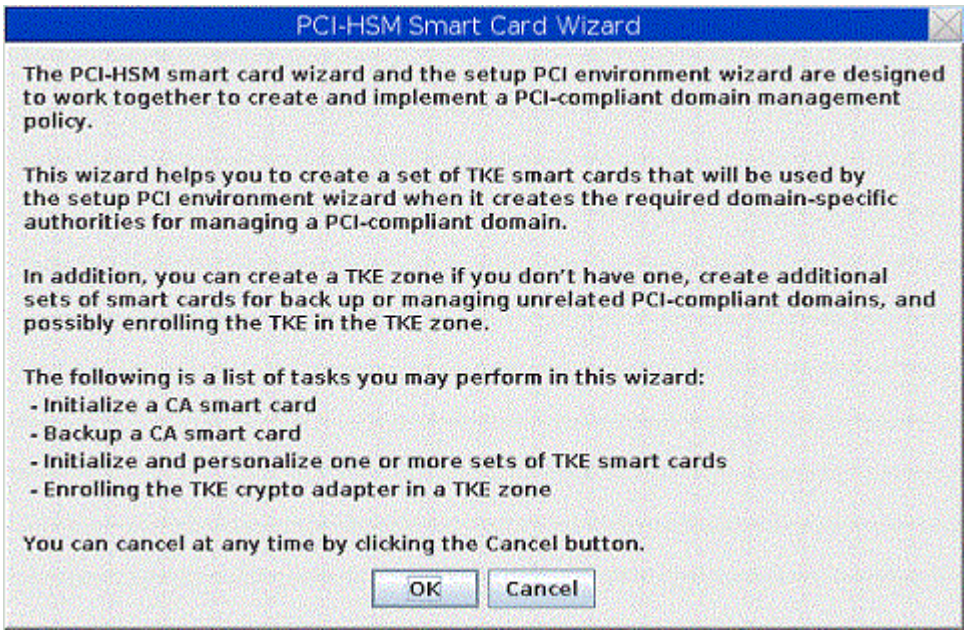


Figure 138. PCI-HSM smart card wizard - Welcome screen

Starting in TKE 9.1

The Smart Card Utility program has a feature that is called TKE Smart Card Wizard. It is started from the **File > TKE Smart Card Wizard** pull down menu.



Figure 139. TKE smart card wizard

The wizard presents you with a welcome screen.

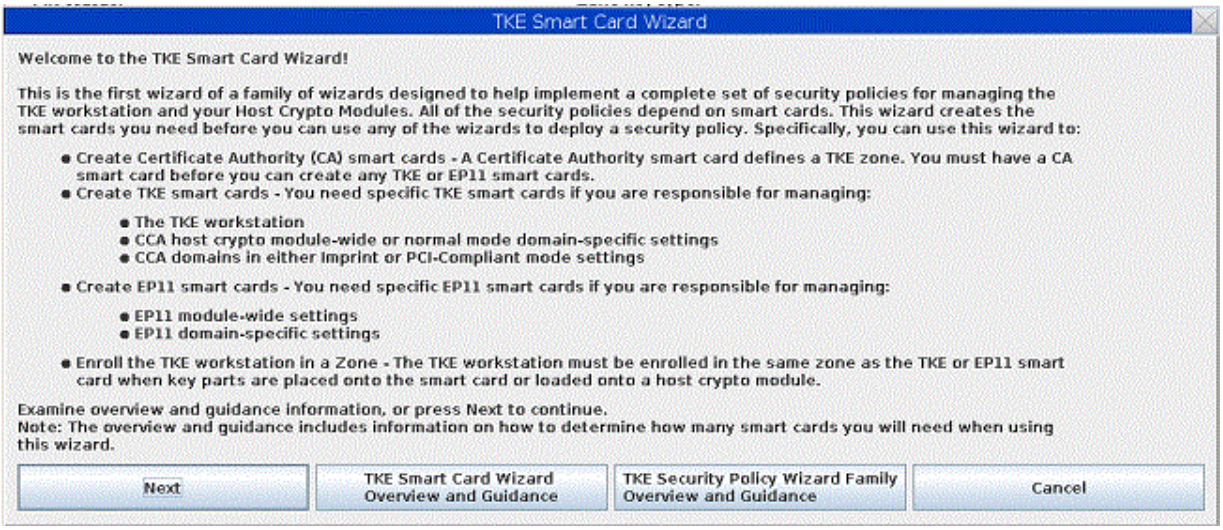


Figure 140. TKE smart card wizard - Welcome screen

After you press Next, select the smart cards you want to create. Select the 'TKE smart cards for managing CCA host crypto domains running in imprint and PCI-compliant mode' check box. Select the 'Certificate Authority (CA) smart cards' check box if you want to create a new zone.

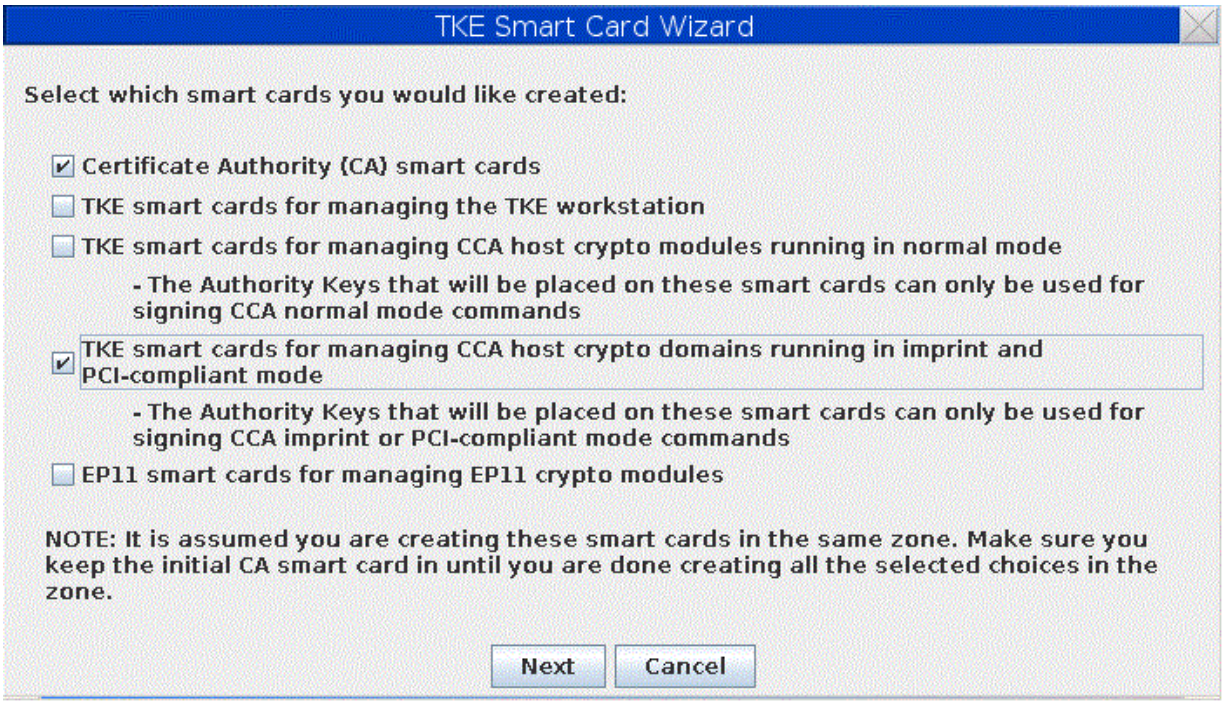


Figure 141. TKE smart card wizard - Creation screen

The wizard takes you through the process of creating the smart cards that are needed to implement a basic PCI-compliant domain management policy. In this policy, two authorities are used for managing the domain settings that are not related to key management and two or three authorities are used for doing master key management. The wizard takes you through the process of creating all the smart cards that are listed in Table 33 on page 201. If you already have a CA smart card with a minimum zone strength of RSA 2048, you can skip the create CA and create CA backup steps of the wizard.

Notes:

- If you log on to the TKE workstation with a profile that has the role of SCTKEADM or TKEADM or an equivalent authority, you can also use this wizard to enroll your TKE in your TKE zone that uses your new or existing CA smart card.

- None of the screens and prompts for the **PCI-HSM smart card wizard** or **TKE Smart Card Wizard**are included in this topic.

Table 33. Smart cards

Type of smart card	Purpose	Wizard-provided smart card description
CA smart card	A Certificate Authority (CA) smart card defines a TKE zone. The zone must have a minimum key strength of RSA 2048. The TKE smart cards are enrolled in the TKE zone. **Note:** If you already have a 2048 strength CA smart card, you can add the TKE smart cards to the existing TKE zone.	N/A (User provided description.)
CA smart card	A copy of the CA smart card.	N/A (Copied from the source.)
TKE smart card	To hold the signature key of the authority that can issue domain management commands.	**TKE 9.0** DAissue. **TKE 9.1 or later** DAIss (Domain Admin Issue).
TKE smart card	To hold the signature key of the authority that can co-sign domain management commands.	**TKE 9.0** DAcosign. **TKE 9.1 or later** DACos (Domain Admin Cosign).
TKE smart card	To hold the signature key of the authority that can load the first master key part of any type of master key. To hold master key parts.	**TKE 9.0** KEYfirst. **TKE 9.1 or later** KEYFst (Domain First Key Admin).
TKE smart card	To hold the signature key of the authority that can load an intermediate or last key part of any type of master key. To hold master key parts.	**TKE 9.0** KEYmdlst1. **TKE 9.1 or later** KEYMl1 (Domain Middle/ Last Key Admin 1).
TKE smart card	To hold the signature key of the authority that can load an intermediate or last key part of any type of master key. To hold master key parts.	**TKE 9.0** KEYmdlst2. **TKE 9.1 or later** KEYMl2 (Domain Middle/ Last Key Admin 2). (Only needed if your master key has three or more parts and you want the parts split between three authorities.)

Step 2: Place a domain in imprint mode

To move a normal mode domain to imprint mode, open a host and a module from the main TKE application. From the Crypto Module Administration window, open the **Domains > General** tab. Press the Enter imprint mode button.

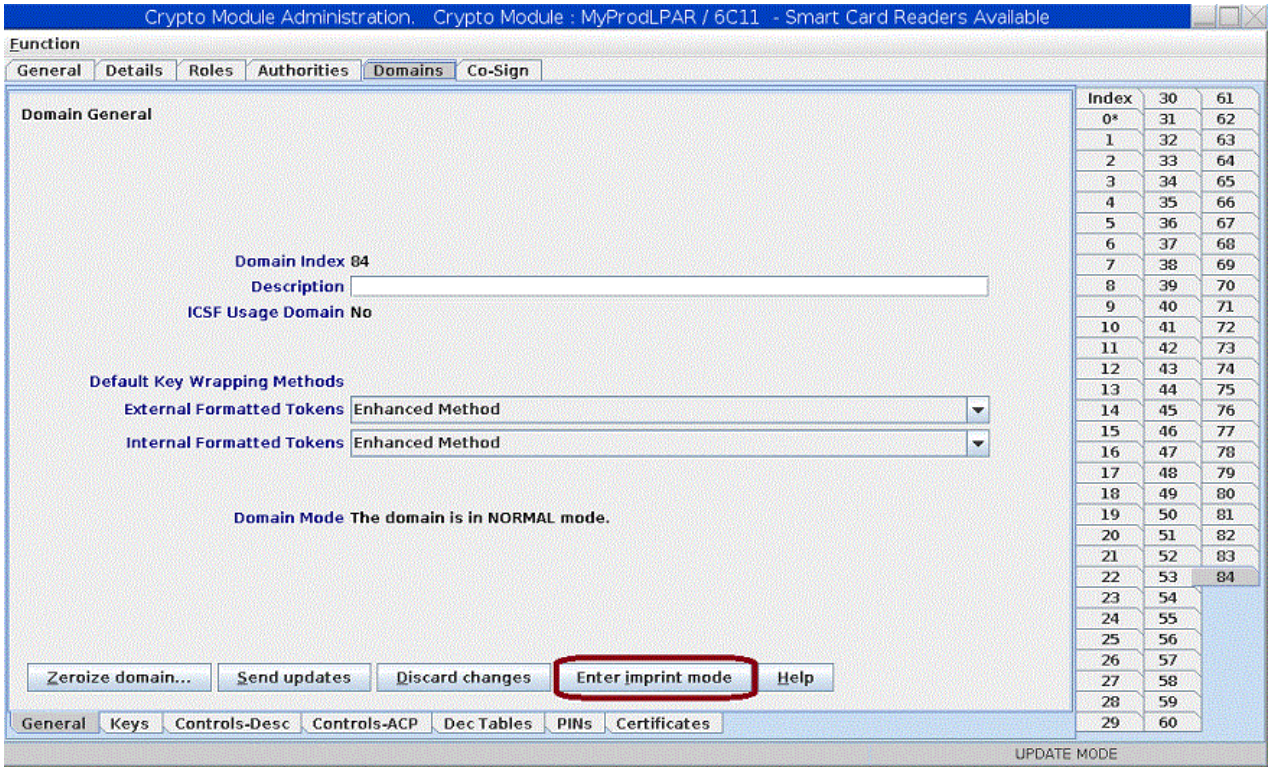


Figure 142. Enter imprint mode

For a new or zeroized module, you can use either the Default key for index 0 or the Default key for index 99 to enter imprint mode.

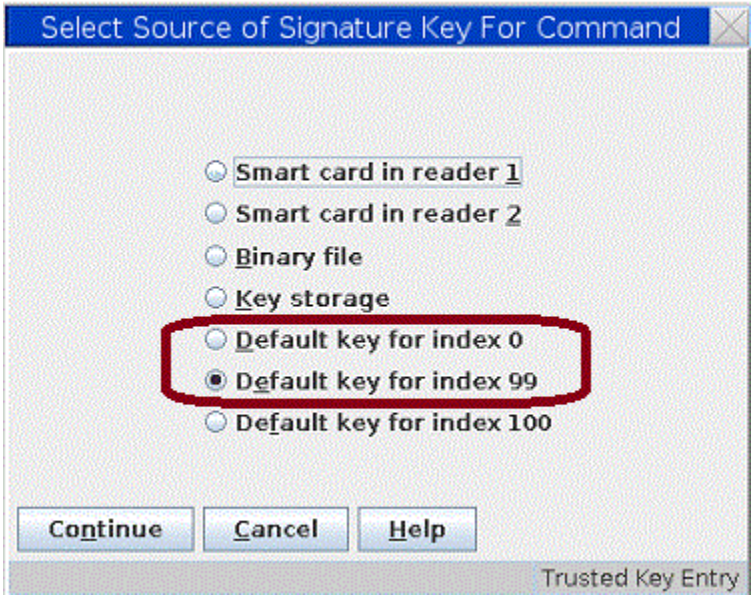


Figure 143. Select source for signature key for command

You might be prompted to set the clock of the crypto module because the module's clock must be set before you can enter imprint mode.

If you do not use a default key to enter imprint mode, the role of the current authority index must have the following Access Control Points (ACPs):

Enter Imprint Mode, Issue

Enter Imprint Mode, Co-sign
You can assign this ACP to a second authority and require them to explicitly co-sign the command.

Set Clock
Only needed if the clock has not been set yet.

Domain Access *xx*
Where *xx* is the domain that is being placed in imprint mode.

Step 3: Create the domain-specific roles and authorities needed to manage a PCI-compliant domain

When a domain is in imprint mode, all domain administration must be done by using domain-specific authorities. Authority index 100 is provided for doing the initial role and authority index creation. Dual controls can be used, but are not required until you enter PCI-compliant mode.

A wizard is provided to create the domain-specific roles and domain-specific authorities that are needed to implement the basic PCI security policy that is first described in "Step 1: Create the smart cards needed to manage a PCI-compliant domain" on page 198. The wizard also generates authority signature keys onto the smart cards if requested.

The wizard is started by pressing the **Setup PCI Environment** button.

Note: Not all of the screens and prompts for the **Setup PCI Environment** wizard are included in this topic. Only significant highlights are included.

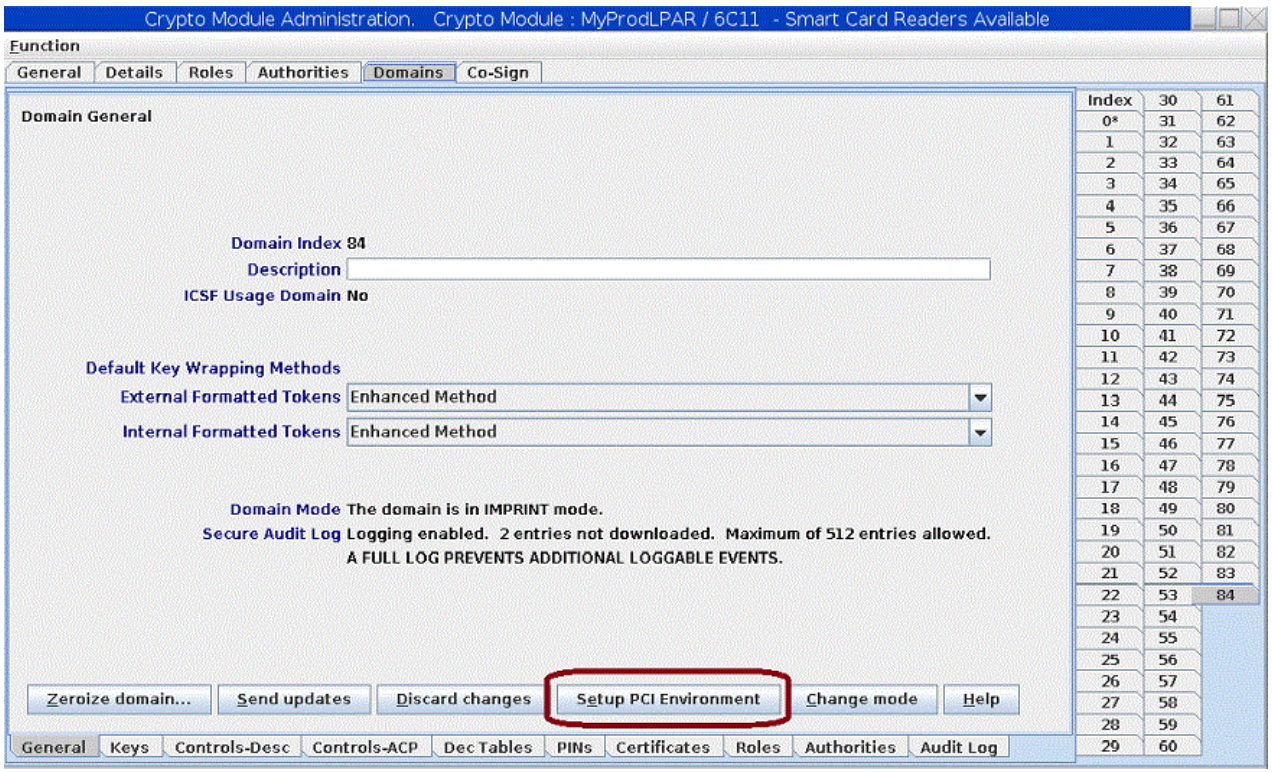


Figure 144. Setup PCI Environment

You see the wizard's welcome screen:

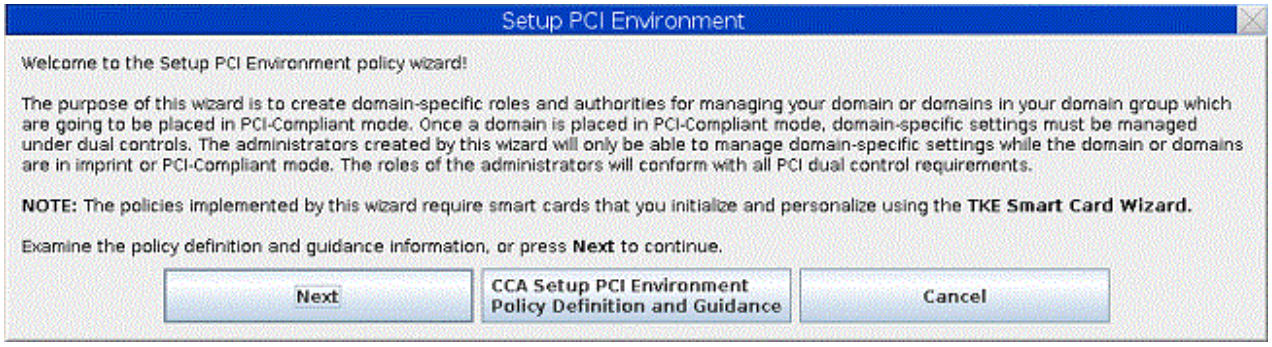


Figure 145. Setup PCI Environment - Welcome screen

After you press OK, the wizard tells you it is going to create the domain-specific roles that are described in the welcome screen.

The wizard creates the domain-specific roles that are listed in the welcome screen. After the wizard creates the set of domain-specific roles, you are provided a summary of the activity.

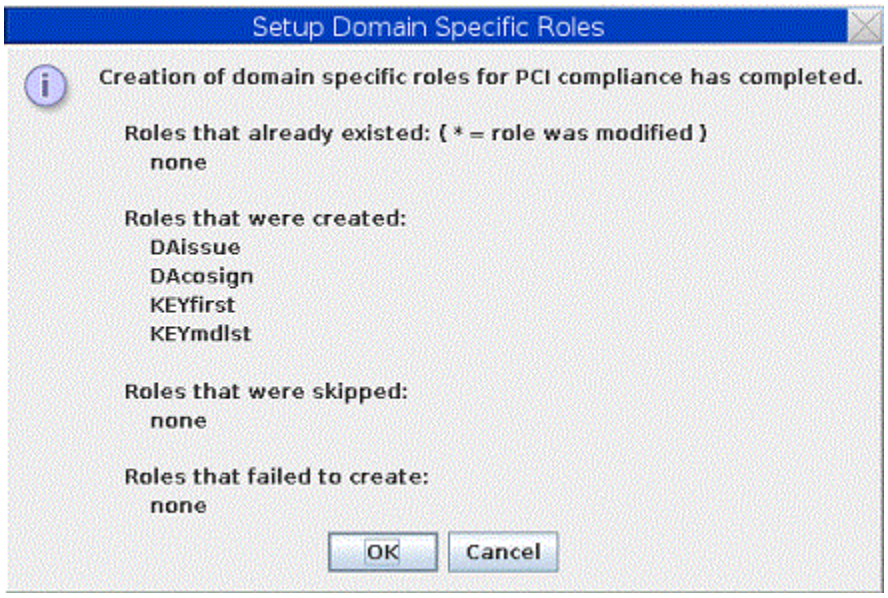


Figure 146. Setup domain-specific roles

The Setup PCI Environment wizard was redesigned in TKE 9.1. There is a new interface for creating the domain-specific authorities. With the new design, you are asked to insert any of the smart cards that are used by the administrators and key managers for when configuring the domain.

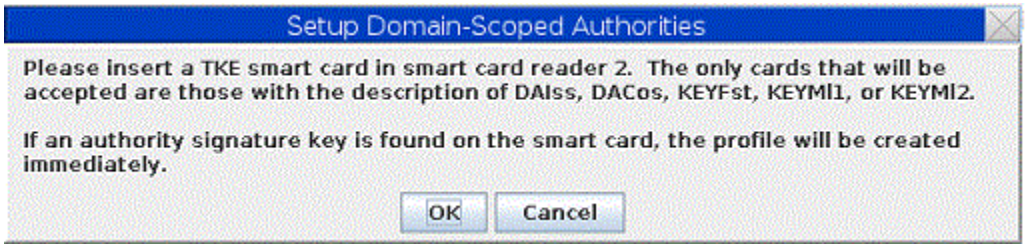


Figure 147. Setup PCI environment

When you insert the smart card, the wizard verifies that the smart card is one of the smart cards it is looking for. This is done by making sure the smart card description matches the one that would have been assigned by the Smart Card Utility Program (SCUP) PCI-HSM Smart Card wizard or TKE Smart Card Wizard.

If the smart card contains an Authority Signature Key, the wizard creates an Authority Index using the Authority Signature key. If it does not find a key, one is created for you. You are allowed to select the key strength if the wizard has more than one choice. In general, you should pick the strongest possible key strength.

After the index has been created, you are asked if you want to create another Authority Index. When you are done, press No.

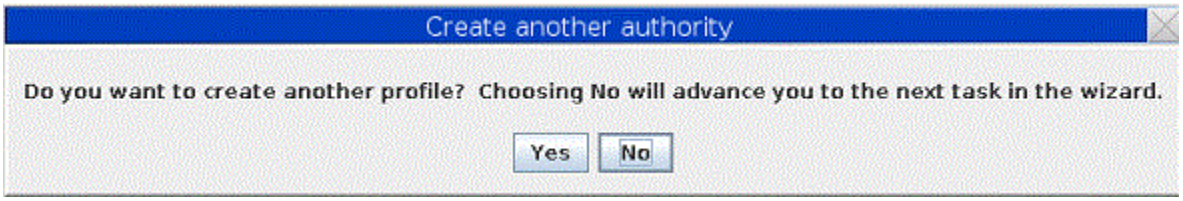


Figure 148. Setup domain specific authorities

After you press no, you are provided with a list of all the Authorities that were created during the wizard session. The list is provided in the order that the authorities were created.

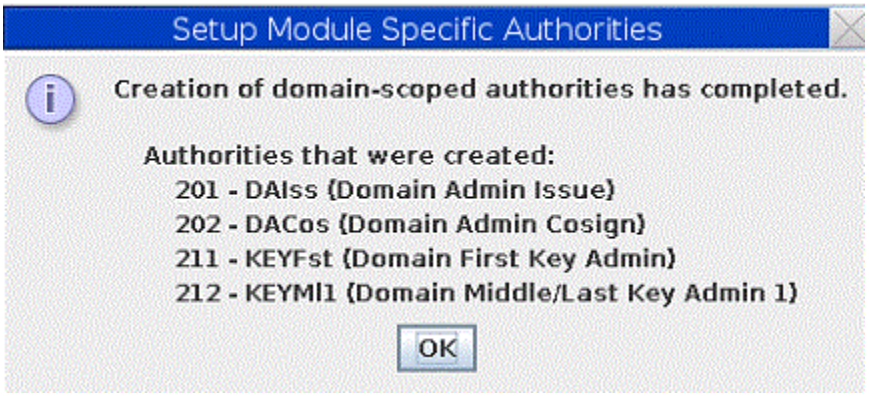


Figure 149. Setup domain specific authorities - Summary

The smart cards, domain-specific roles, and domain-specific authorities that are needed to manage your PCI-compliant domain have all been created. The domain management part of the security policy has been implemented by using the **PCI-HSM Smart Card Wizard** or **TKE Smart Card Wizard** and the **Setup PCI Environment Wizard**.

Table 34. Smart cards and purpose

Type of smart card (SC)	**Purpose**	**SC contains authority signature key for authority index**	**Role of the authority index**
TKE smart card	To hold the signature key of the authority that can issue domain management commands.	201	DAissue
TKE smart card	To hold the signature key of the authority that can co-sign domain management commands.	202	DAcosign
TKE smart card	To hold the signature key of the authority that can load the first master key part of any type of master key. To hold master key parts.	211	KEYfirst

Table 34. Smart cards and purpose (continued)			
Type of smart card (SC)	**Purpose**	**SC contains authority signature key for authority index**	**Role of the authority index**
TKE smart card	To hold the signature key of the authority that can load an intermediate or last key part of any type of master key. To hold master key parts.	212	KEYmdlst

Note: If the wizard generates the authority signature key, it will attempt to assign the listed index values. If they are not available, the wizard will select a different number. Also, if you manual create your authority signature keys, you can select any valid domain-specific index you want.

Backup the authority signature keys

Make a backup of your smart cards to protect against loss or damage to a smart card. Now that the smart cards contain authority signature keys, copy the authority signature keys to their backup smart card. For more information, see "Copy smart card contents" on page 131.

Step 4: Place a domain in PCI-compliant mode

To move an imprint mode domain to compliant mode:

1. Press the **Change mode** button.
2. Select the **Enter compliance mode** radio button.
3. Press the **Send updates** button.

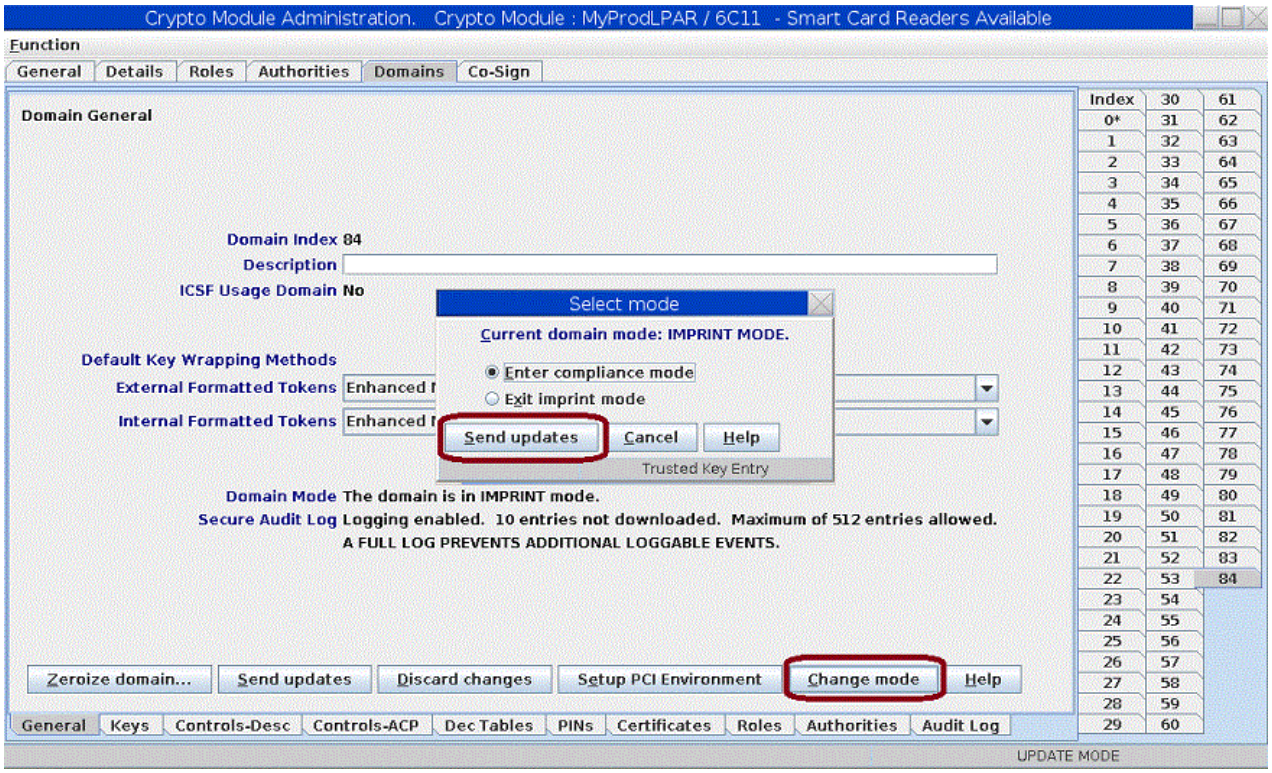


Figure 150. Move an imprint mode domain to compliant mode

After you press the **Send updates** button, you see the current authority error message, similar to:



Figure 151. Authority error message

Explanation of the error message

When you enter imprint mode for the first time, the only authority that can be used to create new domain-specific roles and authorities is the default domain-specific authority with index 100. The role for index 100 is not allowed to move the domain to PCI-compliant mode.

After you press the Retry button, you are asked for a new authority signature key. When you use the TKE wizards to create your smart cards and setup the PCI environment, you need to load the authority signature key for the authority with index 201. You can place the smart card with the signature key for index 201 into any available reader.

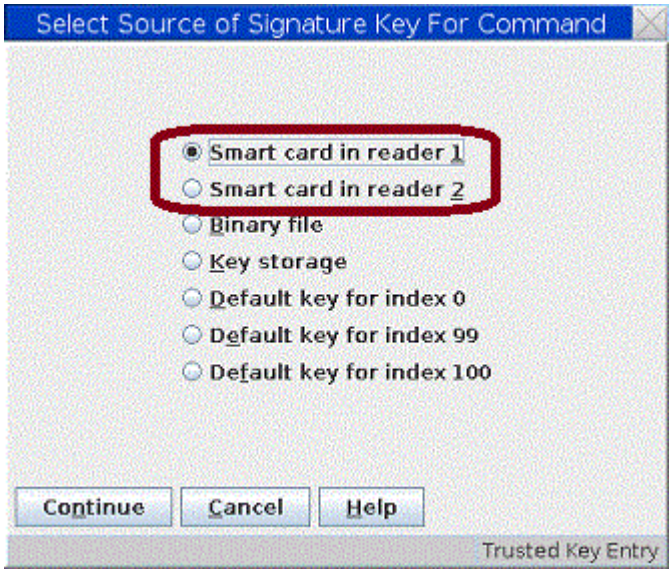


Figure 152. Select source

When the command is issued, it must be co-signed.

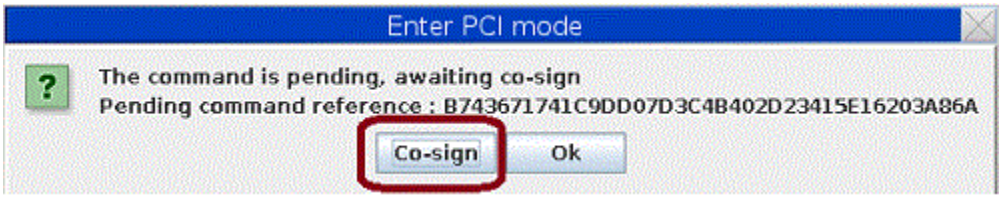


Figure 153. Enter PCI mode - Co-sign

After you press the Co-sign button, you are taken to the co-sign pending command screen. You can see who has already signed the command (the authority with index 201) and who can co-sign the command (the authority with index 202).

Note: The remaining part of the co-sign procedure is not shown in this topic.

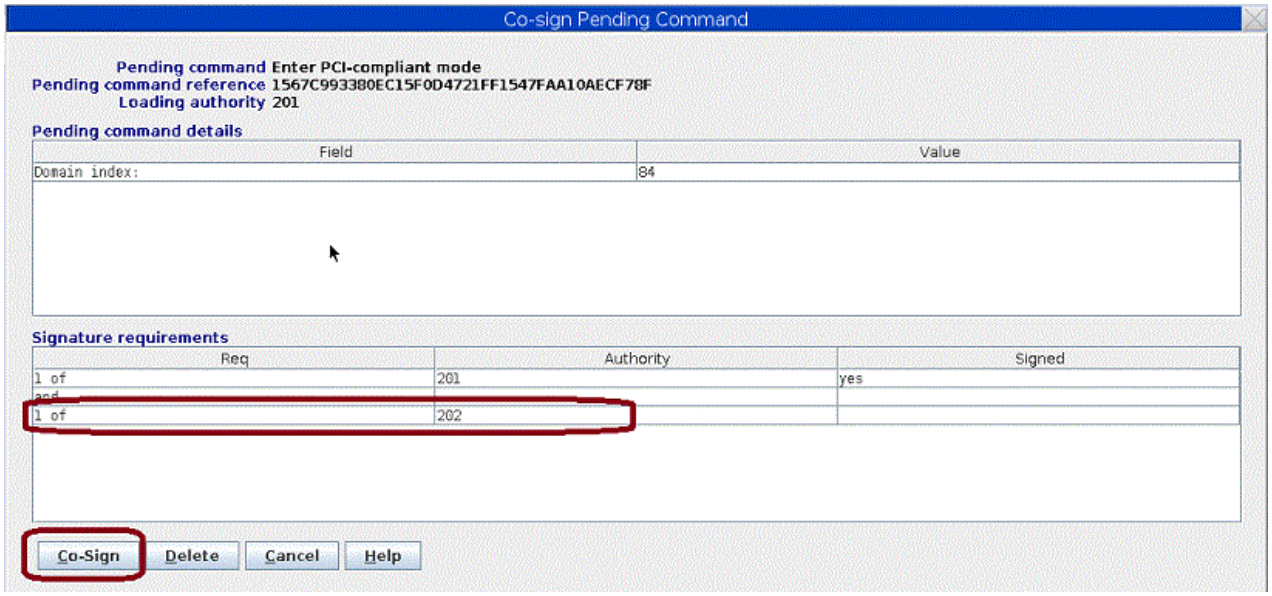


Figure 154. Co-sign pending

The domain is now in PCI-compliant mode. All domain management must be done by using the domain-specific authorities, which enforce dual controls. However, the processes for managing domain settings, like loading master keys or changing domain controls, has not changed.

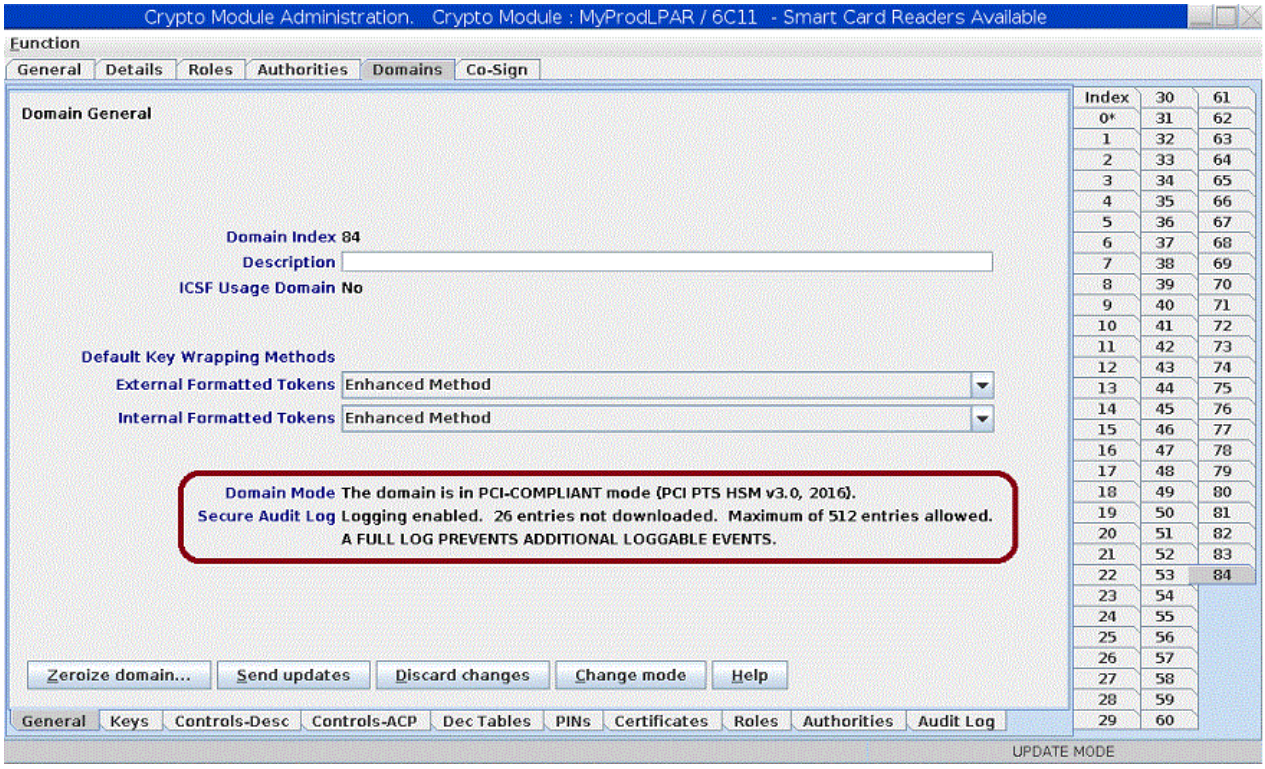


Figure 155. PCI-compliant mode

Chapter 8. Using the Crypto Module Notebook to administer EP11 crypto modules

The Crypto Module Notebook is the central point for displaying and changing all information that is related to a crypto module. It is used for single crypto modules and domain groups. The contents of some pages vary depending on whether you selected a single crypto module or a domain group.

The TKE Main Window lists the crypto modules available on each host machine to which the TKE Workstation is connected, and also lists any crypto module groups and domain groups you created. Double-click a crypto module or domain group in the TKE Main Window to open the Crypto Module Notebook and work with the selected crypto module or domain group. There are two versions of the Crypto Module Notebook — one for CCA crypto modules (CEX2C, CEX3C, CEX4C, CEX5C, CEX6C, and CEX7C) and one for EP11 crypto modules (CEX4P, CEX5P, CEX6P, and CEX7P).

This topic describes how to use the Crypto Module Notebook for EP11 crypto modules. For information about how to use the Crypto Module Notebook for CCA crypto modules, see Chapter 7, “Using the Crypto Module Notebook to administer CCA crypto modules,” on page 137.

In the main TKE window, when you open an EP11 host crypto module or a domain group made up of EP11 host crypto modules, the Crypto Module Notebook for EP11 crypto modules is displayed. The Crypto Module Notebook opens on the Module General tab.

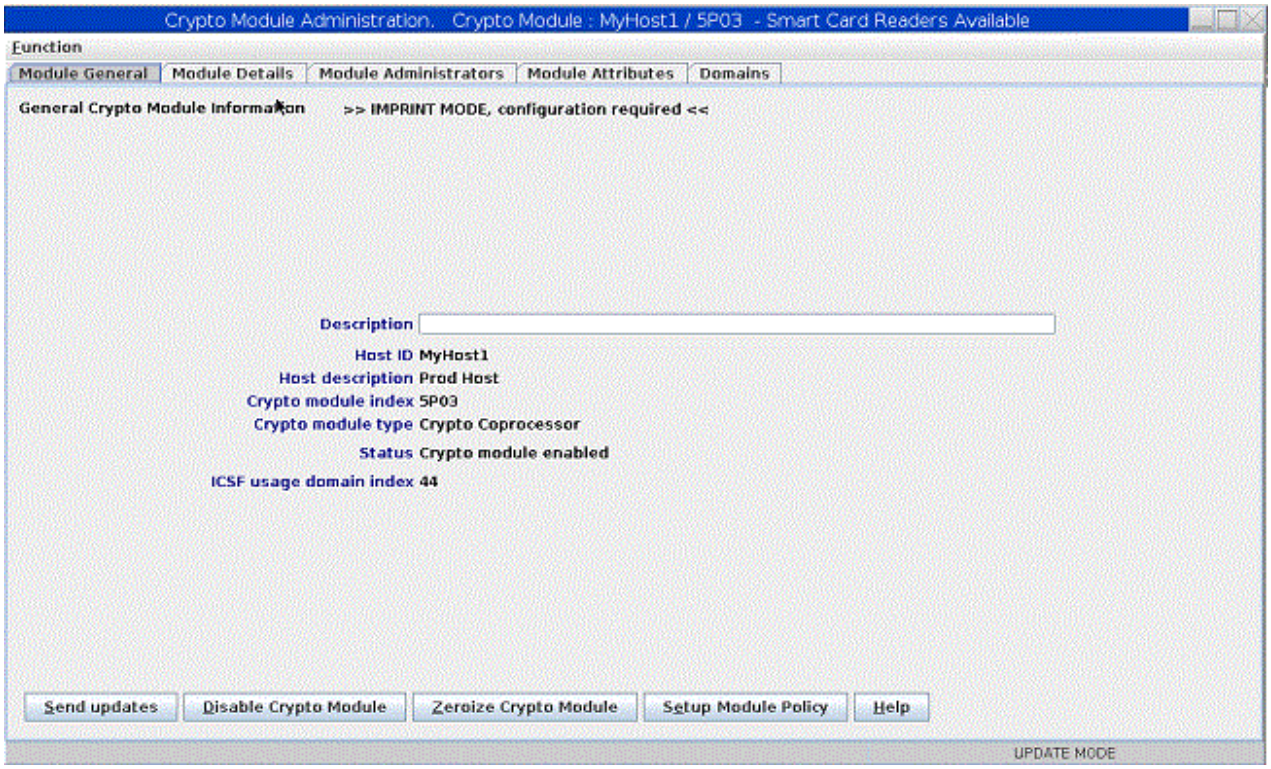


Figure 156. Crypto Module Notebook for EP11 - Module General page

The Crypto Module Notebook is the central point for displaying and changing all information that is related to a crypto module or a domain group. Most panels are the same when referencing a single host crypto module versus a domain group, but there are minor differences on some panels for the two cases.

Note: Master key parts for EP11 host crypto modules and administrator signature keys are held exclusively on smart cards. Smart card readers must be enabled to perform most administrative tasks. To enable smart card readers, check the Enable Smart Card Readers option on the Preferences pull-down

© Copyright IBM Corp. 2000, 2021

menu on the TKE main window. The main TKE application needs to be restarted for this option to take effect.

The **Setup Module Policy** button appears only when the module is in imprint mode. If you press this button, it launches the Setup Module Policy Wizard. The Setup Module Policy Wizard helps you create a set of EP11 administrators and adds them to the list of known module-wide administrators on your module or modules in your domain group. Once you have added the administrators to the list of known administrators, the Setup Module Policy Wizard takes your module or the modules in your domain group out of imprint mode. The Setup Module Policy Wizard does this by setting the Signature Threshold and Revocation Signature Threshold values to 2.

Note: EP11 administrator signature keys must be stored on smart cards. The Setup Module Policy Wizard uses smart cards that were created using the Smart Card Utility Program (SCUP) TKE Smart Card Wizard.

Notebook mode

The notebook is opened in one of three possible modes:

- **UPDATE MODE**
- **READ-ONLY MODE**
- **LOCKED READ-ONLY MODE** - domain group notebooks only

The mode is displayed in the lower-right corner on all crypto module notebook pages.

In **UPDATE MODE**, you are able to display crypto module information and to perform updates to the crypto module.

In **READ-ONLY MODE**, you are able to display crypto module information but not update it.

In **LOCKED READ-ONLY MODE**, you are able to display crypto module information for the master module and to compare the reduced group of crypto modules. You are not allowed to do updates. TKE was not able to access one or more crypto modules of the domain group. This mode applies to domain group notebooks only.

Imprint mode

Imprint mode is a temporary operational mode for EP11 crypto modules and domains and is intended for initial setup only. A crypto module and all domains are placed in imprint mode when:

- Segments 2 and 3 of an EP11 crypto module are loaded for the first time
- Ownership of segments 2 and 3 is surrendered and segments 2 and 3 are reloaded
- An EP11 crypto module is zeroized

A domain reenters imprint mode when it is zeroized.

In imprint mode, most commands are executed without requiring command signatures. Administrators can be added and removed, attributes can be changed, the crypto module can be enabled and disabled, and the domain or crypto module in imprint mode can be zeroized. But other commands are not allowed. Imprint mode is used for initial crypto module setup, before master keys can be loaded and control points can be reset to restrict domain functionality.

The concept of "imprint mode" exists at both the crypto module level and the domain level. You must exit imprint mode at the crypto module level before you are allowed to exit imprint mode in any domain on the crypto module.

When a crypto module or its domains are placed in imprint mode, the signature threshold and revocation signature threshold values are set to zero. The crypto module threshold values are shown on the Module Attributes tab. Domain threshold values are shown on the Domain Attributes tabs. To exit imprint mode, the signature threshold and revocation signature threshold must be changed to nonzero values. The command to change the signature threshold value to a nonzero value must be signed, with the number of required signatures equal to the new signature threshold value. If you try to set the signature threshold or

revocation signature threshold to a number larger than the number of administrators that are installed in the crypto module or domain, an error is signaled.

When a module or domain is in imprint mode, the **Setup Module Policy** or **Setup Domain Policy** wizards are available to you. These wizards provide a simple path for adding your administrators and taking your modules or domains out of imprint mode.

Crypto Module Notebook Function menu

The selections under the **Function** pull-down menu are:

- **Refresh Notebook**. This option refreshes the notebook by reading information from the host. Performing a refresh might change the mode of the notebook.
- **Manage Signature Keys**. Use this option to predefine the smart card readers that are checked for administrator signature keys when signatures are needed for administrative commands to the host crypto module. If no smart card readers are selected using this option, you are prompted to insert a smart card with an administrator signature key in smart card reader 1 for each required signature. The result can be frequent prompts to insert or replace a smart card in smart card reader 1.

  If this option predefines smart card readers as the source of signature keys, commands that require administrator signatures automatically use the smart cards in those readers to generate signatures whenever signatures are needed. If the smart card reader does not initially contain a smart card, you are prompted to insert a smart card and enter the PIN. After a valid smart card is inserted in the reader and the PIN is entered, the card can be used to generate additional signatures without further user action.

  All smart card readers are automatically selected as sources of administrator signature keys under this option when the TKE workstation crypto adapter is initialized for smart card use.
- **Release Crypto Module**. An update lock maintained by ICSF prevents attempts to update a host crypto module by more than one TKE workstation at a time. If communication between TKE and a host crypto module is abnormally terminated, the update lock might not be released. If the TKE attempts to reconnect to the host crypto module, it is not able to obtain the update lock and displays a warning indicating the user ID that currently owns the update lock. Selecting the **Release Crypto Module** option releases the update lock and reassigns it to the current user. Be aware, however, that releasing a crypto module can damage an on-going operation initiated by another user. Use this option only if you are certain that the crypto module must be released.

  A dialog prompts you to confirm that you want to release the crypto module.

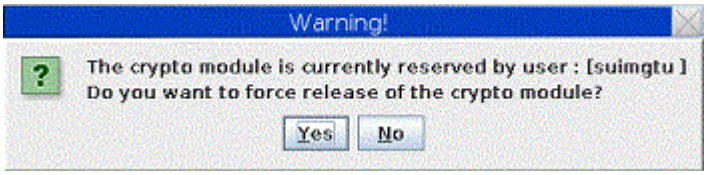


Figure 157. Window to release crypto module

  You can confirm release of the crypto module by clicking **Yes**.
- **Display Crypto Module Settings**. This produces a summary report of how the crypto module is configured, which can include what module and domain administrators are defined, the module and domain attributes, the master key register status and hash values for each domain, and the domain control points for each domain. You are asked to select what information to collect and display.

  The information is displayed on a new panel with tabs for each of the selected categories. A **Save** button allows you to save the information in a file, and a **Print** button allows you to print the information.

  In a domain group notebook, the displayed information is for the crypto module containing the master domain.

- **Download EP11 Audit Data**. This function copies the audit data from the EP11 module into the file of your choice. The file can be placed directly onto a USB flash memory drive that is formatted for Trusted Key Entry data or onto your TKE local hard drive.

  Note: Starting in TKE 9.1, the data is presented in human-readable form.

  In TKE 9.0, the data is unformatted. The format of the audit data can be found in *Enterprise PKCS#11 (EP11) Library structure* in the PCIeCC2 Enterprise PCKS #11 (EP11) section at CryptoCards (www.ibm.com/security/cryptocards). The event types that can generate an audit record are found in section 5.4.3 of this document. You can map these audit event names to the audit event values found in section 8.9.1 of this document.
- **Compare Group**. This option is displayed only when working with a domain group. It compares members of the group and identifies any differences between them. Group members should be configured the same (for example, all member domains should have the same set of installed administrators and the same signature threshold) in order for group operations to complete successfully on all group members.
- **Compare Group (Same Domain Index)**. This selection is only displayed if working with a domain group. This compare highlights differences between the domains with the same index. For example, domain 0 and domain 1 can have different settings. However, the compare only highlights the differences between the domains with the same index, not differences between domain 0 and domain 1.
- **Compare Group (Module-wide Only)**. This selection is only displayed if working with a domain group. This compare highlights differences between the modules included in the group. No domain data is collected or compared by this function.
- **Close**. This option closes the crypto module notebook.

Tabular pages

Tabular pages available in the crypto module notebook for EP11 are:

- **Module General**: see “Crypto Module Notebook Module General tab” on page 212.
- **Module Details**: see “Crypto Module Notebook Module Details tab” on page 214.
- **Module Administrators**: see “Crypto Module Notebook Module Administrators tab” on page 215.
- **Module Attributes**: see “Crypto Module Notebook Module Attributes tab” on page 217.
- **Domains**: see “Crypto Module Notebook Domains tab” on page 219.

The notebook opens to the Module General tab.

Crypto Module Notebook Module General tab

The contents of this page are:

Description
: This field is an optional free text description for the crypto module. For a domain group, this field is an optional description for the crypto module that contains the master domain for the group. You can change the description by typing the new description in the text box and clicking **Send updates**.

Host ID
: This field is the ID of the host that contains the crypto module, or, in the case of a domain group, that contains the crypto module with the master domain for the domain group.

Host Description
: This field is the description of the host that contains the crypto module, or, in the case of a domain group, that contains the crypto module with the master domain for the domain group.

Crypto Module Index
: This field is the index of the crypto module or of the crypto module with the master domain for the domain group. Together with the crypto module type, the index uniquely identifies a crypto module within a host. The index value is 00 through 63.

Crypto Module Type
For the crypto modules that TKE currently supports, this field is always set to *Crypto Coprocessor*.

Status
A crypto module is either enabled or disabled. When a crypto module is enabled, it is available for processing. You can change the status of the module by clicking **Enable Crypto Module** or **Disable Crypto Module**.

When the crypto module is enabled, **Disable Crypto Module** is displayed at the bottom of the page. When the crypto module is disabled, **Enable Crypto Module** is displayed.

If you click **Disable Crypto Module** in a domain group notebook, all crypto modules with at least one domain in the domain group are disabled. This action disables the crypto module for the entire system, not just the LPAR that issued the disable. You are asked to confirm this choice.

On CEX6C crypto modules and later, if you click **Set Clock**, an editable clock displays the date and UTC time that the crypto module on the host is set to. Changing this value and clicking **OK** sets the date and UTC time of the clock to the new value.

If you click **Zeroize Crypto Module** in a domain group, all crypto modules with at least one domain in the domain group are zeroized. You are asked to confirm this choice.

Zeroizing a crypto module has the following effects:

- The signature threshold and revocation signature threshold for the crypto module are set to zero, and the crypto module reenters imprint mode. See “Imprint mode” on page 210.
- The crypto module permissions, attribute controls, and operational mode bits are set to their default values.
- All crypto module administrators are removed.
- All domains on the crypto module are zeroized. Zeroizing a domain makes the following changes to the domain:
  - Sets the domain signature threshold and revocation signature threshold to zero, and causes the domain to re-enter imprint mode.
  - Sets the domain permissions, attribute controls, and operational mode bits to their default values.
  - Removes all domain administrators.
  - Clears the new and current master keys in the domain.
  - Re-enables all domain control points.

The **Setup Module Policy** button appears only when the module is in imprint mode. If you press this button, it launches the Setup Module Policy Wizard. The Setup Module Policy Wizard helps you create a set of EP11 administrators and adds them to the list of known module-wide administrators on your module or modules in your domain group. Once you have added the administrators to the list of known administrators, the Setup Module Policy Wizard takes your module or the modules in your domain group out of imprint mode. The Setup Module Policy Wizard does this by setting the Signature Threshold and Revocation Signature Threshold values to 2.

Note: EP11 administrator signature keys must be stored on smart cards. The Setup Module Policy Wizard uses smart cards that were created using the Smart Card Utility Program (SCUP) TKE Smart Card Wizard.

Intrusion latch

Under normal operation, the intrusion latch of a cryptographic card is tripped when the card is removed. This trip causes all master keys to be erased, all administrators to be removed, and all other configuration settings to revert to their default values. The card and all domains reenter imprint mode. See “Imprint mode” on page 210.

A situation might arise where a cryptographic card needs to be removed. For example, you might need to remove a card for service. If you must remove a card, and you do not want the installation data to be cleared, perform the following procedure to disable the card. This procedure requires you to switch between the TKE application, the ICSF Coprocessor Management panel, and the Support Element.

1. Open an emulator session on the TKE workstation and log on to your TSO/E user ID on the host system where the card will be removed.
2. From the ICSF Primary Option Menu, select Option 1 for Coprocessor Management.
3. Leave the Coprocessor Management panel displayed during the rest of this procedure. You will be required to press Enter on the Coprocessor Management panel at different times.

   Important: Do not exit this panel.
4. Open the TKE Host where the card will be removed. Open the crypto module notebook for the host crypto module. Click **Disable Crypto Module**.
5. After the crypto module is disabled within TKE, press the Enter key on the ICSF Coprocessor Management panel. The status should change to DISABLED.

   Note: You do not need to deactivate a disabled card before configuring it OFFLINE.
6. **Configure Off** the card from the Support Element. The Support Element is a dedicated workstation used for monitoring and operating Z hardware. A user authorized to perform actions on the Support Element must complete this step.
7. After the card is Offline, press the Enter key on the Coprocessor Management panel. The status should change to OFFLINE.
8. Remove the card. Perform whatever operation needs to be done. Replace the card.
9. **Configure On** the card from the Support Element. The Support Element is a dedicated workstation used for monitoring and operating Z hardware. A user authorized to perform actions on the Support Element must complete this step.
10. When the initialization process is complete, press the Enter key on the Coprocessor Management panel. The status should change to DISABLED.
11. From the TKE Workstation Crypto Module General page, click **Enable Crypto Module**.
12. After the card is enabled from TKE, press the Enter key on the Coprocessor Management panel. The Status should return to its original state. If the Status was ACTIVE in step 2, when the card is enabled it should return to ACTIVE.

All master keys, administrators, and other configuration data should still be available. The data was not cleared with the card removal because it was DISABLED first using the TKE workstation.

Crypto Module Notebook Module Details tab

The Module Details tab contains three pages, which can be selected by clicking the tabs on the right side of the window. The pages and their contents are:

- **Crypto Module** - Shows basic information needed to recognize a host crypto module. Different information is displayed, depending on the crypto module type. The following fields may be displayed on this page:
  - **Crypto Module ID** - Unique identifier burned into the crypto module during the manufacturing process.
  - **Public Modulus** - For crypto modules with an RSA OA signature key, the modulus of the key. TKE uses the public key to verify signed replies from the host crypto module.
  - **Modulus Length** - For crypto modules with an RSA OA signature key, the length of the modulus, in bits.
  - **ECC Public Key** - For crypto modules with an ECC OA signature key, the ECC public key.
  - **Key Identifier** - The SHA-256 hash over the public part of the OA signature key. For RSA keys, the hash is over the DER-encoded modulus and public exponent. For ECC keys, the hash is over the ECC public key.
- **Crypto Services (Function Control Vector Values)**
  - CDMF availability
  - 56-bit DES availability

  - Triple DES availability
  - 128-bit AES availability
  - 192-bit AES availability
  - 256-bit AES availability
  - SET services
  - Maximum modulus for key management
  - Maximum elliptic curve field size in bits for key management
- **Other CM Info**
  - API Ordinal Number
  - Firmware Identifier
  - API Version
  - CSP Version
  - Firmware Configuration ID
  - API Configuration ID
  - CSP Configuration ID

Crypto Module Notebook Module Administrators tab

An administrator controls a signature key that allows him or her to sign commands to a host crypto module. Administrator signature keys are stored on smart cards. The administrator has physical possession of the smart card and knows the smart card Personal Identification Number (PIN).

Up to eight administrators can be defined for each domain on a host crypto module, and eight additional administrators can be defined for the host crypto module as a whole. Domain-level administrators are allowed to sign commands to that domain. Crypto-module-level administrators can sign commands to any domain on the crypto module and to the crypto module as a whole.

The signature threshold and revocation signature threshold values on the **Module Attributes** tab determine how many administrators are required to sign commands to the crypto module. Some commands require only a single signature, regardless of how the signature threshold is set. The signature threshold and revocation signature threshold values on the **Domain Attributes** tab determine how many administrators are required to sign commands to that domain.

Administrators are allowed to sign any command. For EP11 crypto modules, there is no concept of "role" (in which the role associated with an administrator defines the set of commands the administrator is allowed to sign).

To work with the crypto-module-level administrators, click the **Module Administrators** tab on the main crypto module notebook page. To work with domain-level administrators, click the **Domains** tab on the main crypto module notebook page, select a domain, and then click the **Domain Administrators** tab for that domain. Right clicking in these pages displays a pop-up menu with options to add or remove an administrator, or generate an administrator signature key and store it on a smart card.

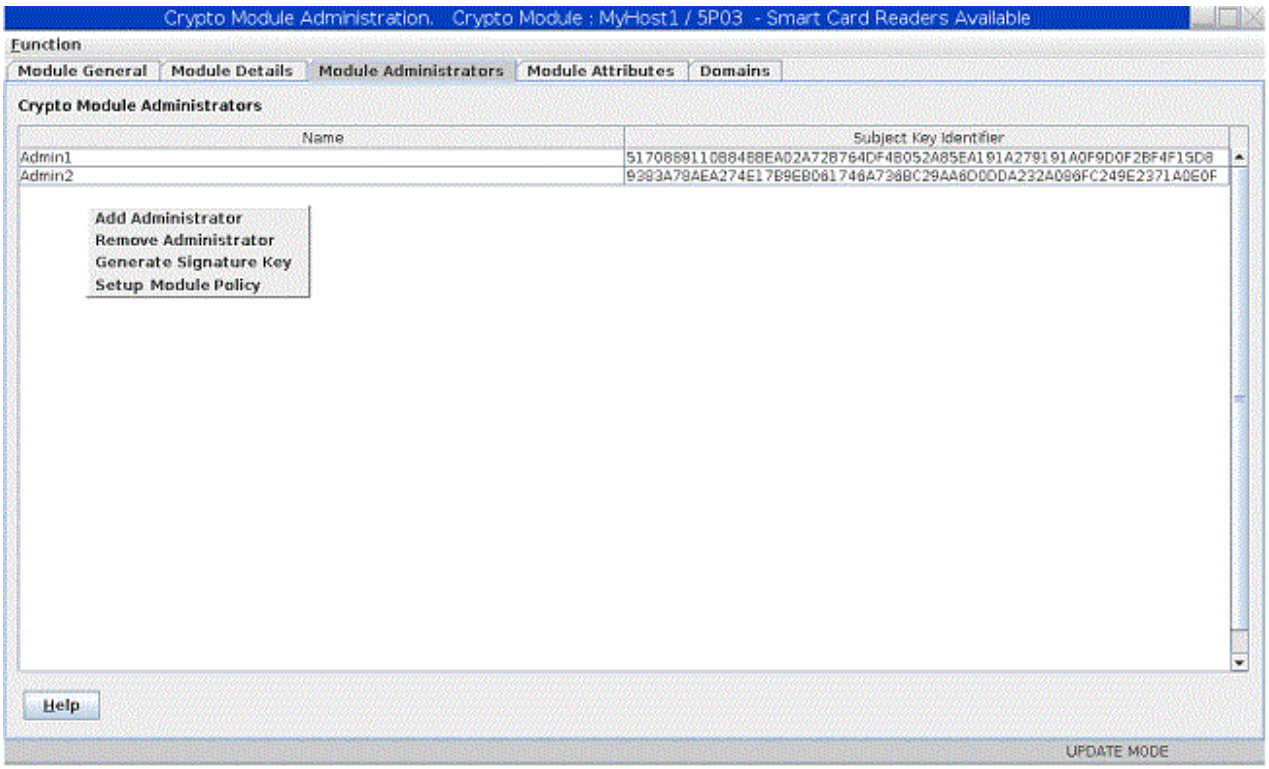


Figure 158. Module Administrators page

EP11 crypto modules identify administrators by using a 32-byte **Subject Key Identifier**, which is a hash of the signature key. The TKE workstation allows users to associate a name of up to 30 characters with each administrator. Users are encouraged to assign unique, meaningful names for each administrator signature key created. The administrator name and subject key identifier are displayed in the administrators list on the Module Administrators page. Both the name and the subject key identifier are written to audit records when commands are signed.

Generate signature key

To generate an administrator signature key and save it on a smart card, right click in the **Module Administrators** page to display the pop-up menu. From the pop-up menu, select the **Generate Signature Key** option.

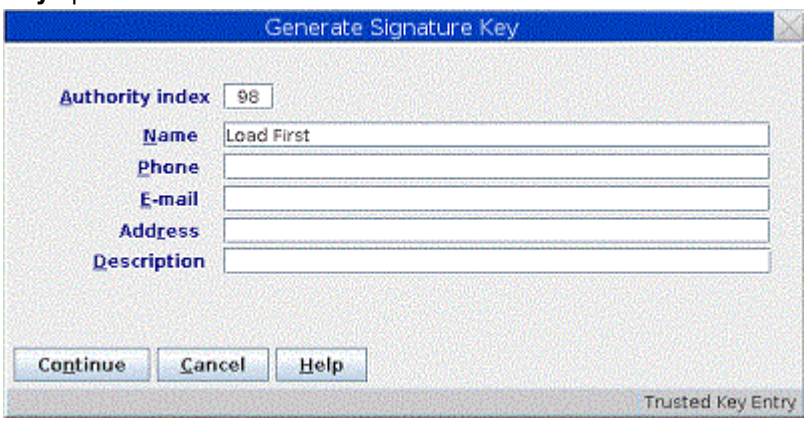


Figure 159. Generate Signature Key

You are asked to enter an administrator name. Users are encouraged to select unique, meaningful names for each signature key created. After entering the administrator name, you are prompted to insert a smart card in a reader and enter the PIN to complete the operation. The generated key is a 320-bit Brainpool ECC key.

Add administrator

To add an administrator, right click in the **Module Administrators** page to display the pop-up menu. From the pop-up menu, select the **Add Administrator** option.

You are asked to insert a smart card that contains an administrator signature key in a smart card reader and enter the PIN. The public key and administrator name are read from the smart card and used to define an administrator to the EP11 crypto module. Up to eight administrators can be defined.

Remove administrator

To remove an administrator, right-click on the administrator in the list of administrators to display a pop-up menu. Click **Remove Administrator** from the pop-up menu. You are not allowed to remove an administrator if removing the administrator would reduce the number of administrators below the signature threshold value or revocation signature threshold value.

Setup Module Policy

The **Setup Module Policy** option appears only when the module is in imprint mode. If you select this option, it launches the Setup Module Policy Wizard. The Setup Module Policy Wizard helps you create a set of EP11 administrators and adds them to the list of known module-wide administrators on your module or modules in your domain group. Once you have added the administrators to the list of known administrators, the Setup Module Policy Wizard takes your module or the modules in your domain group out of imprint mode. The Setup Module Policy Wizard does this by setting the Signature Threshold and Revocation Signature Threshold values to 2.

Note: EP11 administrator signature keys must be stored on smart cards. The Setup Module Policy Wizard uses smart cards that were created using the Smart Card Utility Program (SCUP) TKE Smart Card Wizard.

Crypto Module Notebook Module Attributes tab

Use the Module Attributes tab to display a set of attributes associated with the crypto module and change them.

To change the crypto module attributes, type new values in the **Signature Threshold** and **Revocation Signature Threshold** fields and select or clear check boxes in the attributes trees. Then click **Send updates**. If you change your mind you can click **Discard changes**. Your changes are discarded and the page is refreshed with attributes reread from the crypto module.

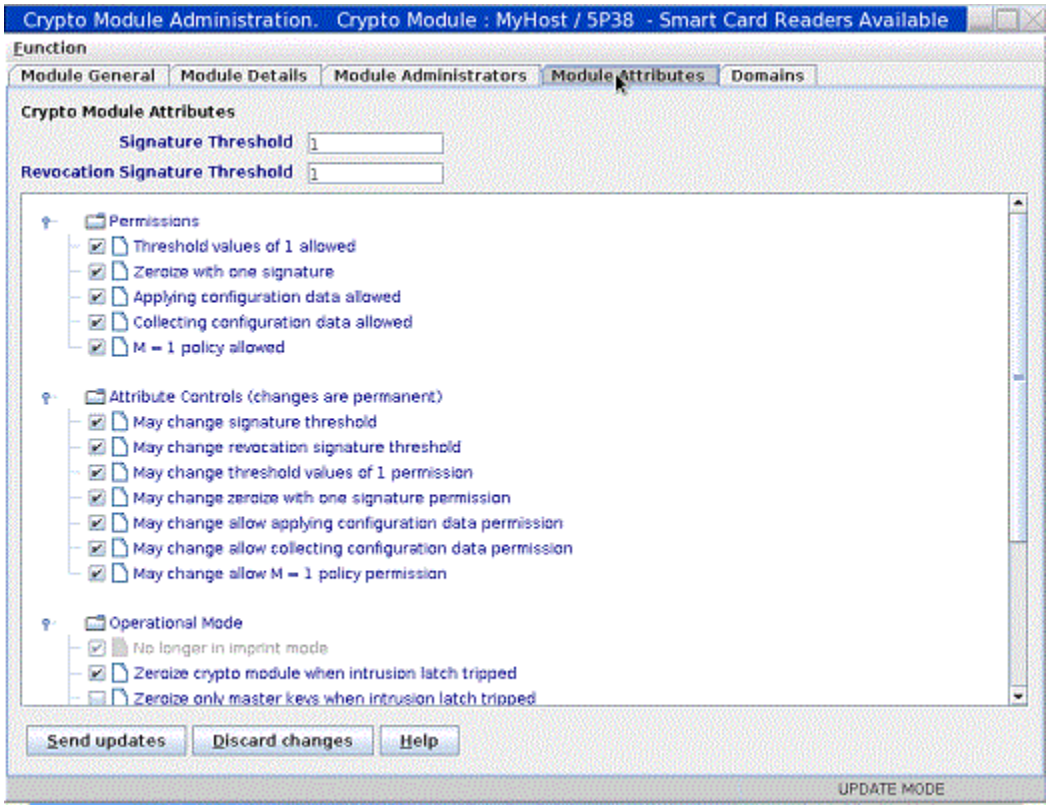


Figure 160. Module Attributes page

Using the Crypto Module Notebook Module Attributes Tab, you can set the following attributes:

- **Signature Threshold** and **Revocation Signature Threshold**.

  The signature threshold controls the number of signatures needed to execute most commands to the crypto module. Some commands require a single signature, regardless of how this attribute is set. Each domain on the crypto module has its own signature threshold attribute, which controls the number of signatures required for most commands sent to that domain. The maximum signature threshold value that can be set is 8.

  The revocation signature threshold controls the number of signatures required to remove a crypto module administrator. The maximum revocation signature threshold value that can be set is 8.

  When the crypto module is zeroized, the signature threshold and revocation signature threshold are set to 0 and the crypto module is put in imprint mode. In imprint mode commands to the crypto module do not require administrator signatures. Imprint mode is intended for initial crypto module setup, before the crypto module is used to manage master keys. To exit imprint mode, set the signature threshold and revocation signature threshold to nonzero values. You must exit imprint mode at the crypto module level before you can exit imprint mode in any domain on the crypto module.
- **Permissions**.
  - **Threshold values of 1 allowed** - When checked, the signature threshold and revocation signature threshold can be set to 1. If not checked, the signature threshold and revocation signature threshold must be set to values greater than 1.
  - **Zeroize with one signature** - When checked, zeroizing the crypto module requires just one signature, regardless of the signature threshold value. When not checked, the signature threshold value specifies the number of signatures required to zeroize the crypto module.
- **Attribute Controls**

  These check boxes restrict changes to other fields on the panel. After the crypto module is zeroized, these check boxes are all selected and any attribute on the panel can be changed. If you clear one of these check boxes and click **Send updates**, the corresponding attribute is frozen and you are not

allowed to change it. You can clear these fields, but you cannot select them again. The crypto module must be zeroized to select them again. You are asked to confirm your choice if you clear one of these fields and click **Send updates**. The attributes controls are:

- **May change signature threshold** This control allows the crypto module signature threshold value to be changed.
- **May change revocation signature threshold** This control allows the crypto module revocation signature threshold to be changed.
- **May change threshold values of 1 permission** This control allows the **Threshold values of 1 allowed** permission to be changed.
- **May change zeroize with one signature permission** This control allows the **Zeroize with one signature** permission to be changed.

- **Operational Mode**. The operational mode bits are:
  - **No longer in imprint mode**. This bit is read-only and indicates whether the crypto module is in imprint mode. Imprint mode is a temporary condition used for initial setup. Setting the signature threshold and revocation signature threshold to nonzero values exits imprint mode.
  - **Zeroize crypto module when intrusion latch tripped**. When checked this bit specifies that the entire crypto module is to be zeroized when the intrusion latch is set. Physically removing a crypto module from a host system sets the intrusion latch.
  - **Zeroize only master keys when intrusion latch tripped**. When checked, this bit specifies that only the master keys on the crypto module are to be zeroized when the intrusion latch is set. Physically removing a crypto module from a host system sets the intrusion latch. This bit is ignored when the **Zeroize crypto module when intrusion latch tripped** bit is set.
  - **Battery is low**. This bit is read-only and indicates the battery on the EP11 crypto module needs to be replaced.
  - **Crypto module is enabled**. This bit is read-only and indicates whether the crypto module is enabled or disabled. The crypto module can be enabled and disabled by clicking **Enable Crypto Module** and **Disable Crypto Module** on the Module General page.

    Clicking **Enable Crypto Module** and **Disable Crypto Module** on the Module General tab changes the state of the **Crypto module is enabled** bit, the **Zeroize crypto module when intrusion latch tripped** bit, and the **Zeroize only master keys when intrusion latch tripped** bit. When **Disable Crypto Module** is clicked on the Module General tab, all 3 bits are cleared. This allows the crypto module to be physically removed from the host system without losing configuration data. See "Intrusion latch" on page 213 for the procedure to follow when moving a host crypto module. When the crypto module is enabled by clicking **Enable Crypto Module**, this bit and the **Zeroize crypto module when intrusion latch tripped** bits are checked, but the **Zeroize only master keys when intrusion latch tripped** bit remains unchecked.
- **Standards Compliance Settings**. These bits indicate whether all domains on the crypto module are configured to conform to the indicated industry standard. Domains conform to a standard based on their control point settings. Each domain has its own Standards Compliance Settings attribute. If one or more domains does not conform to a standard, the crypto module as a whole is shown to not conform to the standard. The EP11 crypto module is always compliant with the FIPS 2009 standard, so that **Standards Compliance Settings** attribute is always set. These bits are read-only.

Crypto Module Notebook Domains tab

To manage the administrators, attributes, master keys, and control points for the domains on an EP11 crypto module, click the **Domains** tab in the crypto module notebook. Use the set of tabs on the right side of this page to select a domain to manage. Tabs are present only for those domains configured using the Support Element as control domains for the TKE workstation. Select a domain by clicking it. A set of tabs is displayed at the bottom of the page with functions to manage domain facilities: **Domain General**, **Domain Administrators**, **Domain Attributes**, **Domain Keys**, and **Domain Control Points**.

When ICSF FMID HCR77B1 with APAR OA49067, or later, runs in the logical partition that services requests from the TKE workstation, the configured usage domain will be indicated by an asterisk on one of the numbered domain tabs.

In a domain group notebook, the **Domains** tab is replaced by a **Domain** tab, and there is no list of control domains on the right side of the page. In a domain group notebook, the displayed attributes, administrators, keys, and control points are from the master domain of the group. Updates made in a domain group notebook are made to all member domains of the group, or to all crypto modules with at least one domain in the domain group.

Domain General page

The domain general page displays the domain index and domain description for the domain, and contains a **Zeroize domain** push button that allows the domain to be zeroized. For domain groups, the index and description of the master domain are displayed, and a **Zeroize domain group** push button replaces the **Zeroize domain** push button. Clicking **Zeroize domain group** causes all member domains to be zeroized.

You can change the domain description by typing a new description in the text box and clicking **Send updates**. If you change your mind after entering a new description, you can click **Discard changes**. Your changes are discarded and the existing domain description is refetched from ICSF. Updating the description in a domain group notebook causes the description of all member domains to be updated.

Zeroizing a domain has the following effects:

- The signature threshold and revocation signature threshold are set to zero, and the domain re-enters imprint mode. See “Imprint mode” on page 210.
- The domain permissions, attribute controls, and operational mode bits are set to their default values.
- All domain administrators are removed.
- The domain new master key and current master key are erased. Any data in the ICSF PKCS #11 token data set (TKDS) encrypted by the current master key becomes unrecoverable.
- All domain control points are set.

The **Setup Domain Policy** button appears only when the module is in imprint mode. If you press this button, it launches the Setup Domain Policy Wizard. The Setup Domain Policy Wizard helps you create a set of EP11 administrators and adds them to the list of known module-wide administrators on your domain or domains in your domain group. Once you have added the administrators to the list of known administrators, the Setup Domain Policy Wizard takes your domain or the domains in your domain group out of imprint mode. The Setup Domain Policy Wizard does this by setting the Signature Threshold and Revocation Signature Threshold values to 2.

Note: EP11 administrator signature keys must be stored on smart cards. The Setup Domain Policy Wizard uses smart cards that were created using the Smart Card Utility Program (SCUP) TKE Smart Card Wizard.

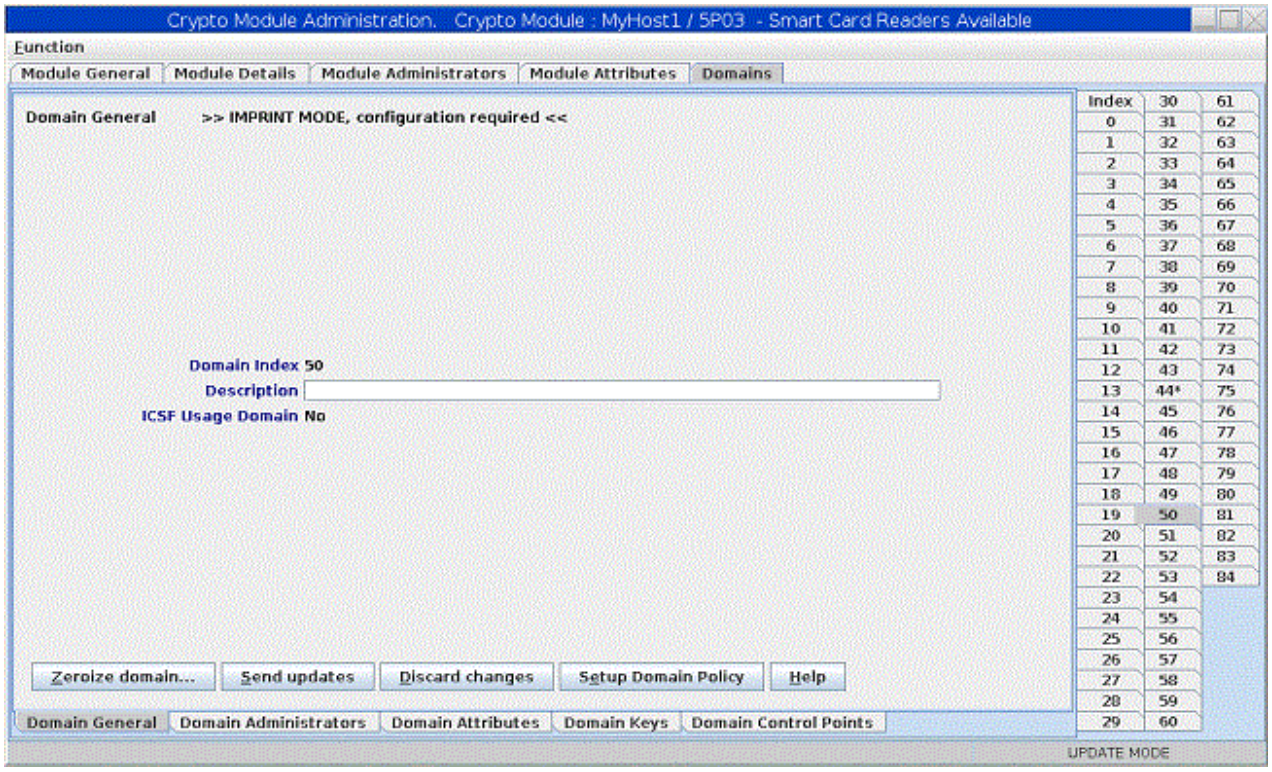


Figure 161. Domain General page

Domain Administrators page

The domain administrators page is identical to the module administrators page, but manages the domain administrators rather than the crypto module administrators. See “Crypto Module Notebook Module Administrators tab” on page 215 for a description of this page.

Domain Attributes page

Use the Domain Attributes tab to display a set of attributes associated with the domain and change them. The attributes displayed are:

- Signature Threshold
- Revocation Signature Threshold
- Permissions
- Attribute Controls
- Operational Mode
- Standards Compliance Settings

To change the domain attributes, type new signature thresholds in the text fields or select or clear check boxes in the attributes trees. Then click **Send updates**. If you change your mind, you can click **Discard changes**. Your changes are discarded and the page is refreshed with domain attributes reread from the crypto module.

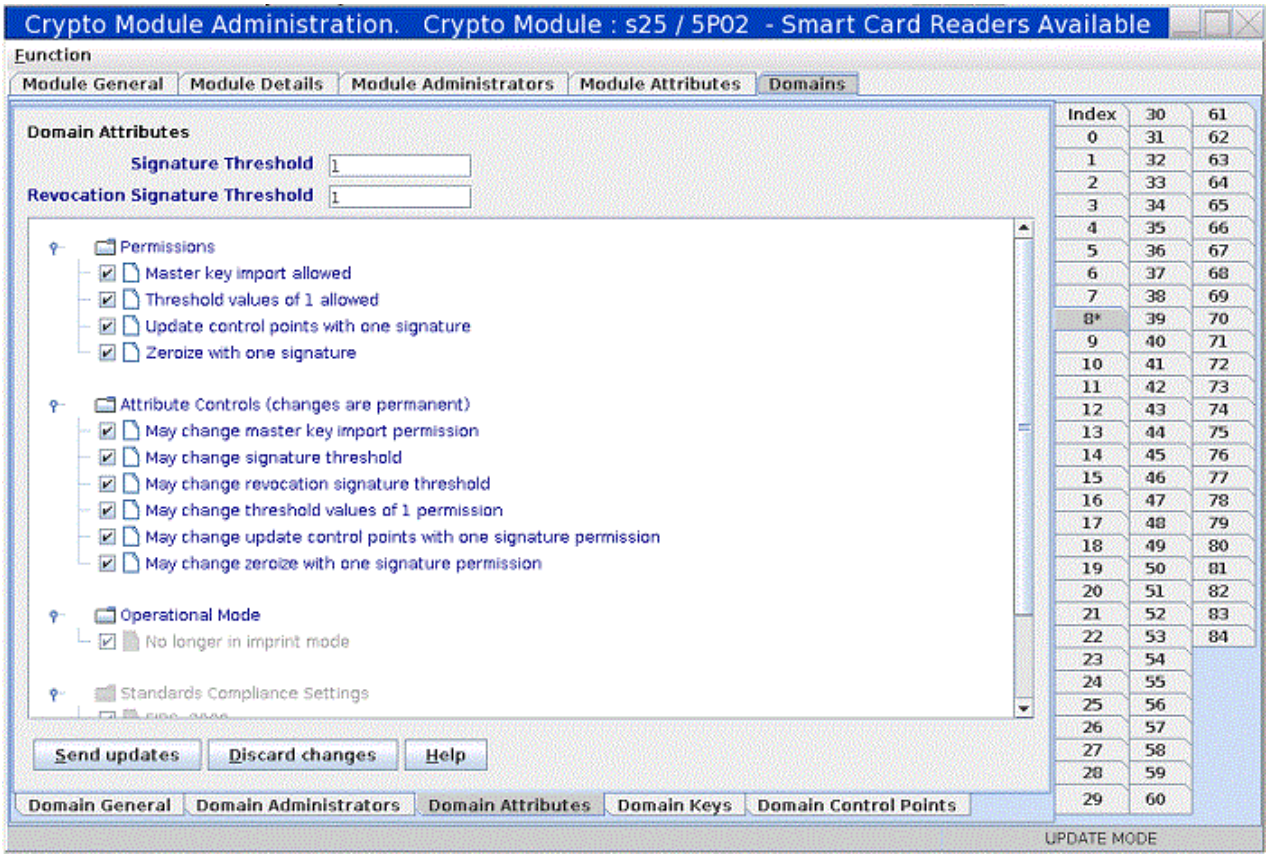


Figure 162. Domain Attributes page

Using the Domain Attributes tab, you can set the following attributes:

- **Signature Threshold** and **Revocation Signature Threshold**.

  The signature threshold controls the number of signatures needed to execute most commands to the domain. Some commands require a single signature, regardless of how this attribute is set. The maximum signature threshold value that can be set is 8.

  The revocation signature threshold controls the number of signatures required to remove a domain administrator. The maximum revocation signature threshold value that can be set is 8.

  When the domain is zeroized, the signature threshold and revocation signature threshold are set to 0 and the domain is put in imprint mode. In imprint mode you can add and remove administrators, zeroize the domain, and change attributes, but you are not allowed to load or clear the master keys or change the domain control points. Imprint mode is a temporary condition intended for initial setup. To exit imprint mode, set the signature threshold and revocation signature threshold to nonzero values. You must exit imprint mode at the crypto module level before you can exit imprint mode in the domain.
- **Permissions**. When a permissions bit is checked, the operation is allowed. When the permissions bit is unchecked, the operation is prohibited.
  - **Master key import allowed** - allows the new master key register in the domain to be loaded.
  - **Threshold values of 1 allowed** - When selected, the signature threshold and revocation signature threshold can be set to 1. If not selected, the signature threshold and revocation signature threshold must be set to values greater than 1.
  - **Update control points with one signature** - When selected, updating the control points requires a single signature. When not selected, the signature threshold specifies the number of signatures needed to update the control points.
  - **Zeroize with one signature**- When selected, zeroizing the domain requires just one signature, regardless of the signature threshold value. When not selected, the signature threshold value specifies the number of signatures required to zeroize the domain.

- **Attribute Controls**. Use these check boxes to restrict changes to other fields on the panel. After the domain is zeroized, these check boxes are all selected and any attribute on the panel can be changed. If you clear one of these check boxes and click **Send updates**, the corresponding attribute is frozen and you are not allowed to change it. You can clear these check boxes, but you cannot reselect them. The domain must be zeroized to select them again. You are asked to confirm your choice if you clear one of these check boxes and click **Send updates**.
  - **May change master key import permission** - controls whether the **Master key import allowed** permission can be changed.
  - **May change signature threshold** - controls whether the domain signature threshold value can be changed.
  - **May change revocation signature threshold** - controls whether the domain revocation signature threshold value may be changed.
  - **May change threshold values of 1 permission** - controls whether the **Threshold values of 1 allowed** permission can be changed.
  - **May change update control points with one signature permission** - controls whether the **Update control points with one signature permission** can be changed.
  - **May change zeroize with one signature permission** - controls whether the **Zeroize with one signature** permission can be changed.
- **Operational Mode**. The operational mode bits are:
  - **No longer in imprint mode**. This bit is read-only and indicates whether the domain is in imprint mode. Imprint mode is a temporary condition used for initial setup. Setting the signature threshold and revocation signature threshold to nonzero values exits imprint mode.
- **Standards Compliance Settings**. These bits indicate whether the domain is configured to conform to the indicated industry standard. Domains conform to a standard based on their control point settings. These bits are read-only.

Domain Keys page

The domain keys page displays the status and verification pattern of the new master key register and current master key register for the domain.

The current master key encrypts all data stored for the domain in the ICSF PKCS #11 token data set (TKDS). To change the current master key, first the new master key register must be loaded, using two or more key parts stored on smart cards.

Right clicking in the page causes a pop-up menu to be displayed. From this menu you can select the following operations:

- **Generate key part** - Generate a random master key part value and save it on a smart card.
- **Load new master key** - Load the new master key register on the host crypto module using two or more key parts previously saved on smart cards.
- **Commit new master key** - Commit the value in the new master key register. The value in the new master key register must be committed before ICSF can use it to re-encrypt data in the TKDS for the domain.
- **Set, immediate** - Sets the new master key, but without re-encrypting the data in the TKDS for the domain.

  Normally, use ICSF procedures or services that coordinate setting the master key with initializing or re-encrypting TKDS. This option sets the master key but does not change TKDS. If used inappropriately, this option causes the data in the TKDS to become unusable when accessed by ICSF in the domain.

  Use this option only when the TKDS does not need to be initialized or re-encrypted when the master key is set. For example, this option can be used to reload the previous master key value if a host crypto module has been inadvertently zeroized.
- **Clear new master key** - Clear the new master key register.

- **Clear current master key** - Clear the current master key register. Use this option with caution. Any data stored in the ICSF TKDS for the domain becomes unusable. You are asked to confirm this choice
- **Coordinated change master key and TKDS** - Run a wizard-like feature to re-encipher the current ICSF token key data set (TKDS) under the new P11 master key, set the P11 master key, and make the re-enciphered TKDS the active in-store TKDS used by ICSF.

  This option is enabled only if the 'Coordinated change master key and KDS' operation is permitted in the TKE crypto adapter role associated with the current TKE crypto adapter user.
- **Secure key part entry** - Use the PIN pad on the smart card reader to enter a known key part value and save it on a smart card.

After the new master key register is loaded and its value is committed, ICSF can re-encrypt data in the TKDS for the domain. After all data is re-encrypted, ICSF can finalize the new master key. Finalizing moves the value in the new master key register to the current master key register and changes the state of the new master key register to *Empty*.

The domain keys panel in a domain group notebook shows the status and verification patterns of the master key registers in the master domain. When load, commit, and clear options are executed in a domain group, commands are sent to each member domain of the domain group.

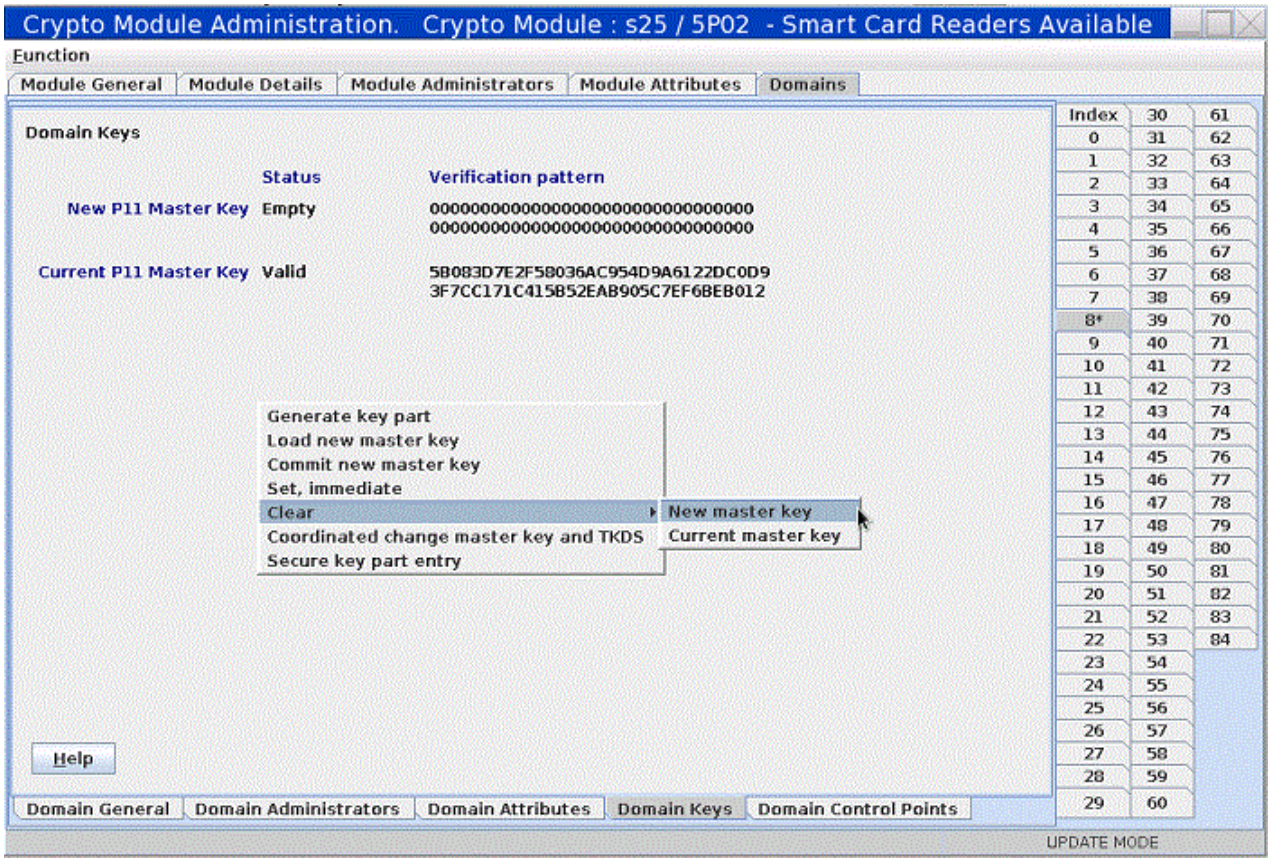


Figure 163. Domain Keys page

Generate key part

To generate one or more P11 master key parts and save them on smart cards, right click in the Domain Keys page to display the pop-up menu. From the pop-up menu, select the **Generate key part** option.

You are asked to enter the number of key parts you want to generate. For each key part, you are guided through the process of selecting a smart card reader to use, inserting a smart card in the reader, entering the PIN, and entering a description to associate with the key part. You can cancel at any time.

Load new master key

To load the new master key register for the domain, right click in the Domain Keys page to display the pop-up menu. From the pop-up menu, select the **Load new master key** option.

You are asked to enter the total number of key parts to be loaded. For each key part, you are guided through the process of selecting a smart card reader to use, inserting a smart card in the reader, entering the PIN, and selecting the key part on the smart card to be loaded. You can cancel at any time.

Key parts on the smart card are encrypted for transport to the host crypto module using Elliptic Curve Diffie-Hellman (ECDH). The first step in ECDH is to generate an IMPORTER key on the crypto module. Generating the key requires a signed command. Therefore, signatures are collected twice when you run the Load New Master Key option – once to generate an IMPORTER key and once to do the final load. Both commands require only a single signature, regardless of how the domain signature threshold is set.

Coordinated change master key and TKDS

This function is the same as the 'coordinated change master keys and CKDS' function in the CCA crypto module notebook, but uses the P11 master key and token key data set (TKDS).

Secure key part entry

To enter a known value for an P11 master key part onto a smart card, right click in the Domain Keys page to display the pop-up menu. From the pop-up menu, select the **Secure key part entry** option.

The same process is followed for secure key part entry of P11 master key parts as for secure key part entry of other key types. See Appendix A, “Secure key part entry,” on page 311 for details on this process.

Domain Control Points page

Use the **Domain control points** page to display the set of control points that are currently active for the domain and change them. When selected, a control point permits an operation in the domain. When not selected, the operation is not allowed.

To change control points, select or clear check boxes to select or deselect individual control points. Then click **Send updates** to send the changes to the host crypto module. If you change your mind, you can click **Discard changes**. Any changes you made are discarded and the page is refreshed with the current control points for the domain.

You can save the displayed control points to a file by clicking **Save to file**. You can load the control points from a previously saved file by clicking **Load from file**. In both cases, a window opens in which you can select the file to use. After loading the control points from a file, click **Send updates** to send the changes to the host crypto module.

Right click in an open area of the page to display a pop-up menu. From this menu you can reset collections of control points to ensure conformity with an operating standard such as FIPS or BSI. After selecting the wanted standard, click **Send updates** to send the updates to the host crypto module.

Use care when deselecting control points in the Control Point Management category. These control points can be used to prevent further updates to the control points for the domain. After these control points are turned off, further updates to the control points are not permitted. The domain must be zeroized before the control points can be changed again. You are asked to confirm your choice when turning off these control points.

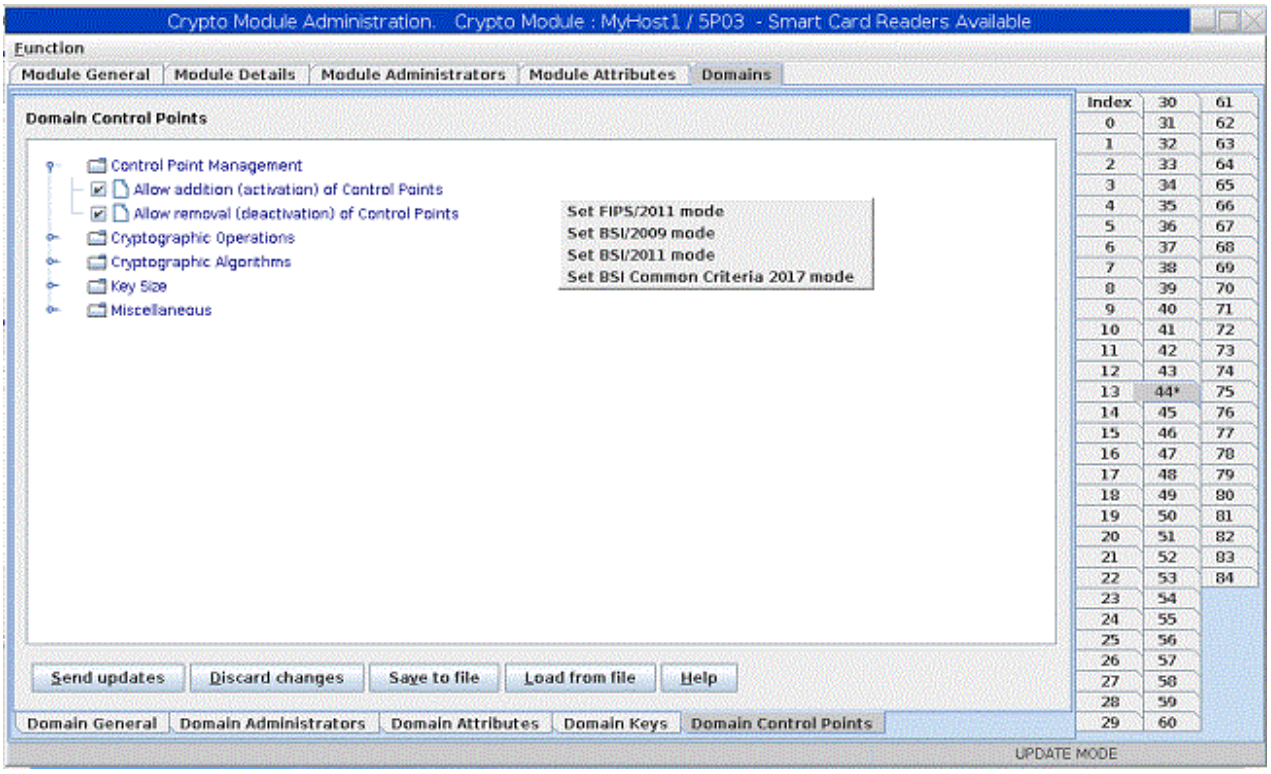


Figure 164. Domain Control Points page

Chapter 9. Auditing

TKE implements logging of security relevant operations that occur on the TKE workstation. TKE provides auditors with a trail of activities on the TKE workstation that are not currently tracked. Security actions that are performed on the TKE workstation are recorded in a security log and tied to a user identity. TKE security audit records are in addition to the System Management Facilities (SMF) records that are already cut on the host system that are triggered by requests from TKE.

To perform auditing tasks or configure auditing settings on the TKE workstation, you must log on with the AUDITOR user name. When logged on to the TKE Workstation as AUDITOR, you are able to:

- Use the TKE Audit Configuration Utility to turn TKE auditing on and off.
- Use Service Management functions to:
  - View the security log.
  - Archive the security logs.
- Use the TKE Audit Record Upload Configuration Utility to configure audit record upload to a Z host, where the audit records are saved in the z/OS SMF data set.
- Use the TKE Security Event Viewer to view the security event Logs.
- Set heartbeat interval.

ICSF also uses SMF record type 82 to record certain ICSF events. ICSF writes to subtype 16 whenever a TKE workstation either issues a command request to, or receives a reply response from, a CCA or EP11 crypto module. In addition to the subtype 16 records, you can use the TKE Audit Record Upload Configuration Utility to send Trusted Key Entry workstation security audit records to a Z host. These security audit records are stored in the SMF data set as a type 82 subtype 29 record.

TKE Audit Configuration utility

To configure auditing, log on with the AUDITOR user name, select **Trusted Key Entry** and then select the **Audit Configuration Utility**.

The TKE Audit Configuration Utility is displayed.

By default, all available auditing is enabled.

© Copyright IBM Corp. 2000, 2021

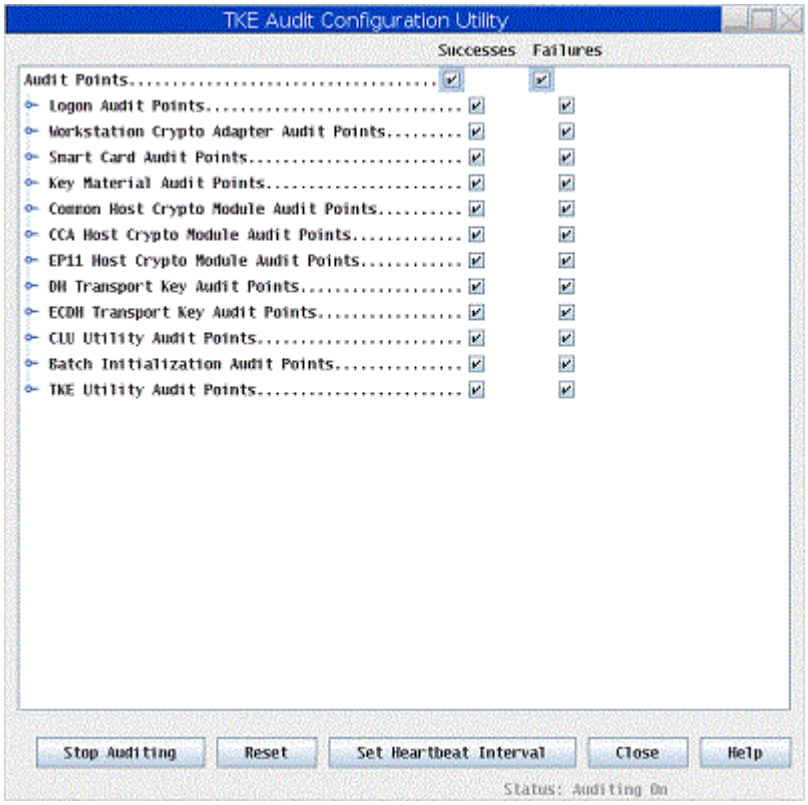


Figure 165. Default settings for auditing

You can customize the auditing utility to your wanted preference. To turn off auditing, click **Stop Auditing** to change the status to **Auditing Off**.

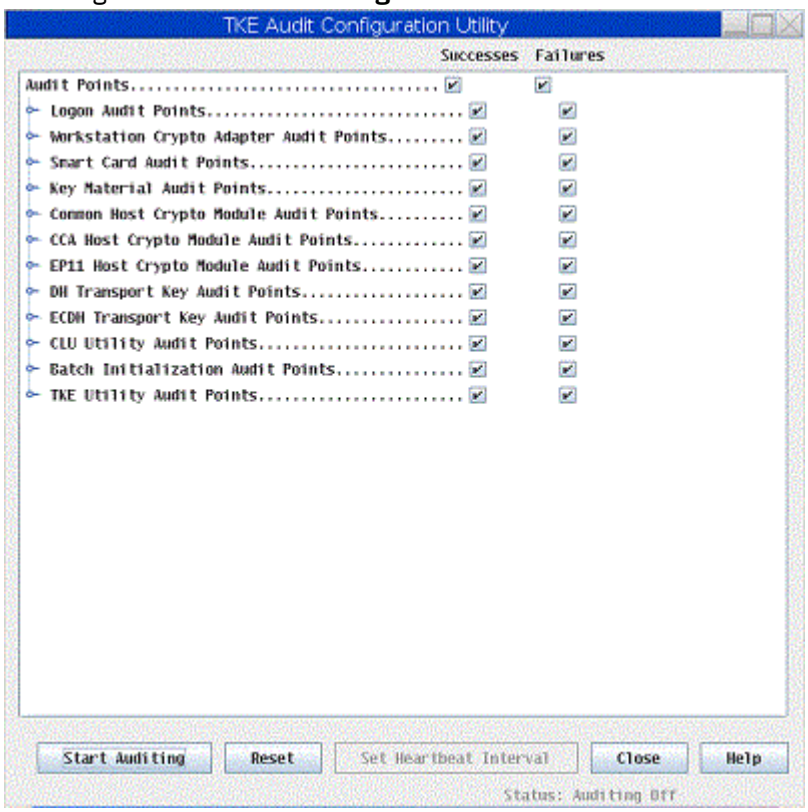


Figure 166. Auditing is off

If you want to enable and disable specific audit records (both successes and failures), you can expand each audit point to see the individual audit records associated with the group by clicking the symbol to the left of the audit point.

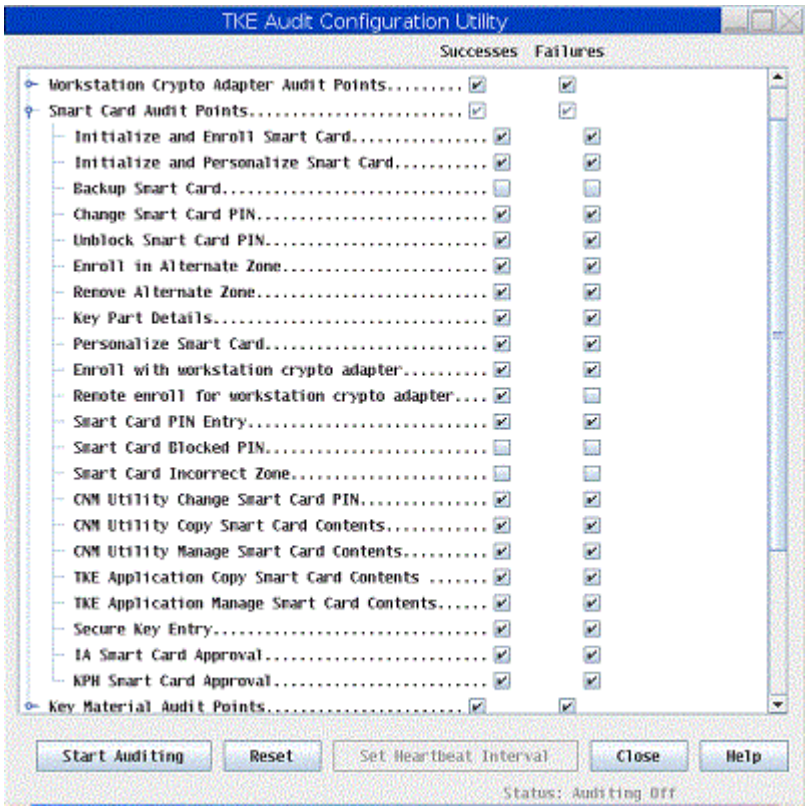


Figure 167. Example of expanded auditing points

When you expand an audit point, you can configure the individual audit records as wanted.

If you want to enable or disable all success or failure audit points, you can click the successes or failures check box on the line corresponding to the audit points group.

To reset the utility, click the **Reset** button. This button reestablishes the default state of auditing. The default state is **Auditing On** and all events are selected to write audit records. Also, the heartbeat interval is set to one day.

If you want to change the interval of the heartbeat record, click **Set Heartbeat Interval** and select an interval that best suits your requirements. If auditing is active, a heartbeat audit record is written if no other audit records have been written during the specified interval.

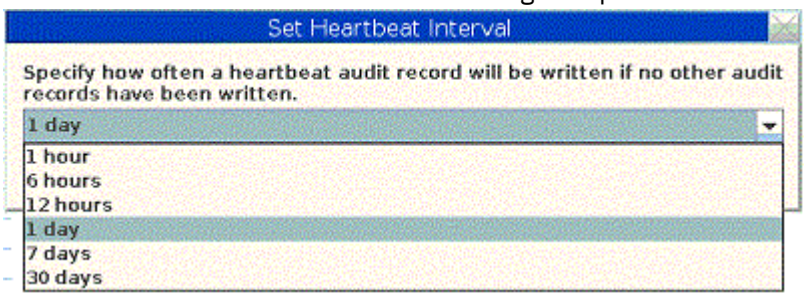


Figure 168. Set heartbeat interval

Service Management auditing functions

You can use Service Management functions to perform the following auditing tasks:

- View the security log

- Archive the security logs

View security logs

The security logs can be viewed on the TKE, but only when you are logged in with the AUDITOR user name. The security log has a maximum size of 30 MB.

When the security log reaches 75% full, a hardware message alerts the user on the TKE console. The View Security Logs task determines whether the message displays. By default, the message displays.

When the security log reaches 100% capacity, the oldest third of the audit records are deleted.

In order to avoid deleting records you can archive the security logs (see “Archive security logs” on page 235).

In order to view the security logs, log in as the AUDITOR user, select **Service Management** and select **View Security Logs**.

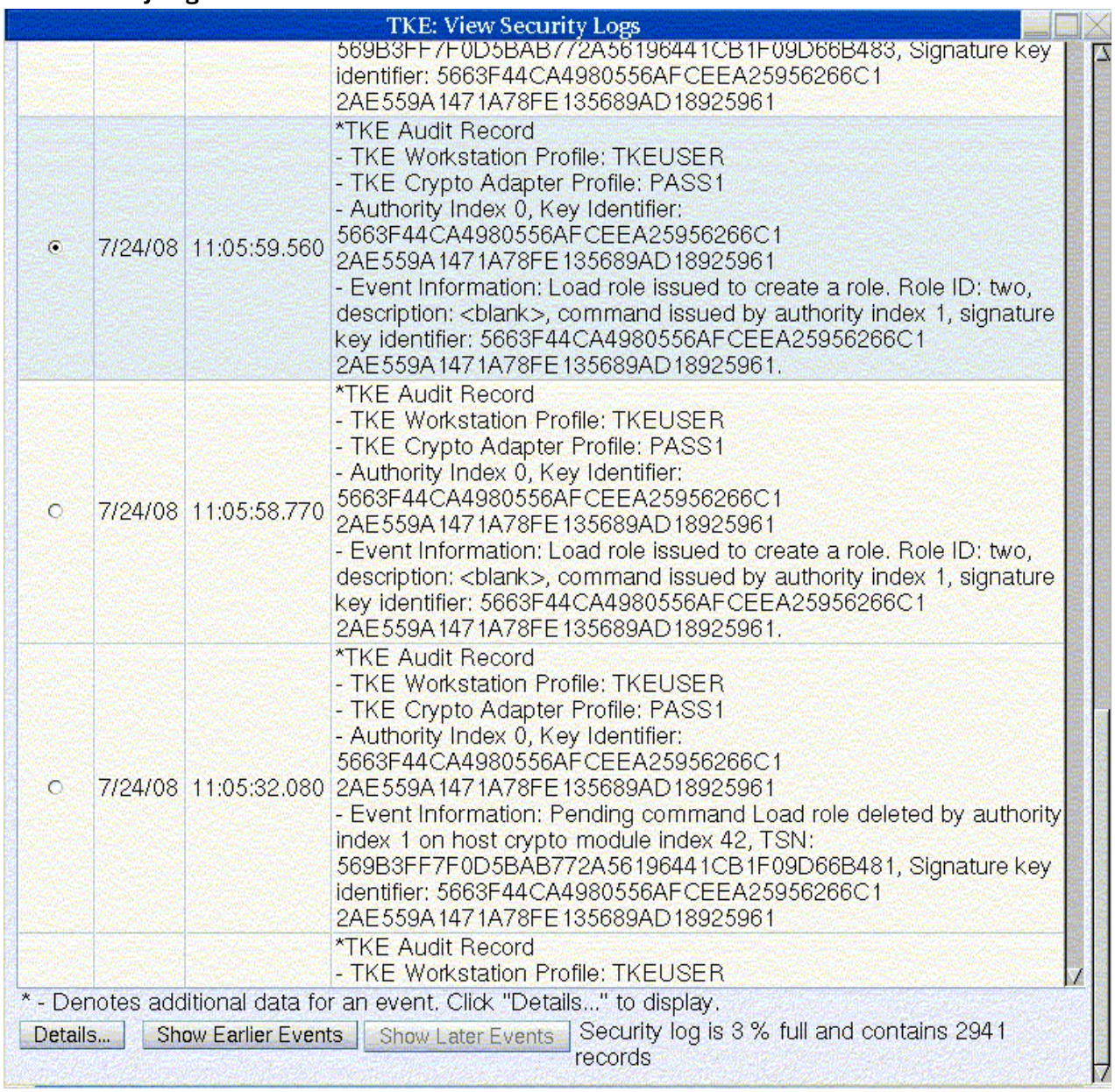


Figure 169. Viewing the security logs

This log displays 1000 records per page. The 1000 record pages can be navigated by clicking on **Show Earlier Events** and **Show Later Events**.

If the audit record contains an asterisk (*) next to the line saying 'TKE Audit Record', this means that there are further details available to view. You can view the details by selecting the radio button corresponding to the desired audit record and clicking **Details**.



Figure 170. Viewing additional details of the security logs

Audit and log management

Audit and log management copies the console events log, security log, and tasks performed log to a USB flash memory drive. Select **Service Management** and, from the service management window, select **Audit and Log Management**.

The Audit and Log Management dialog box is displayed.

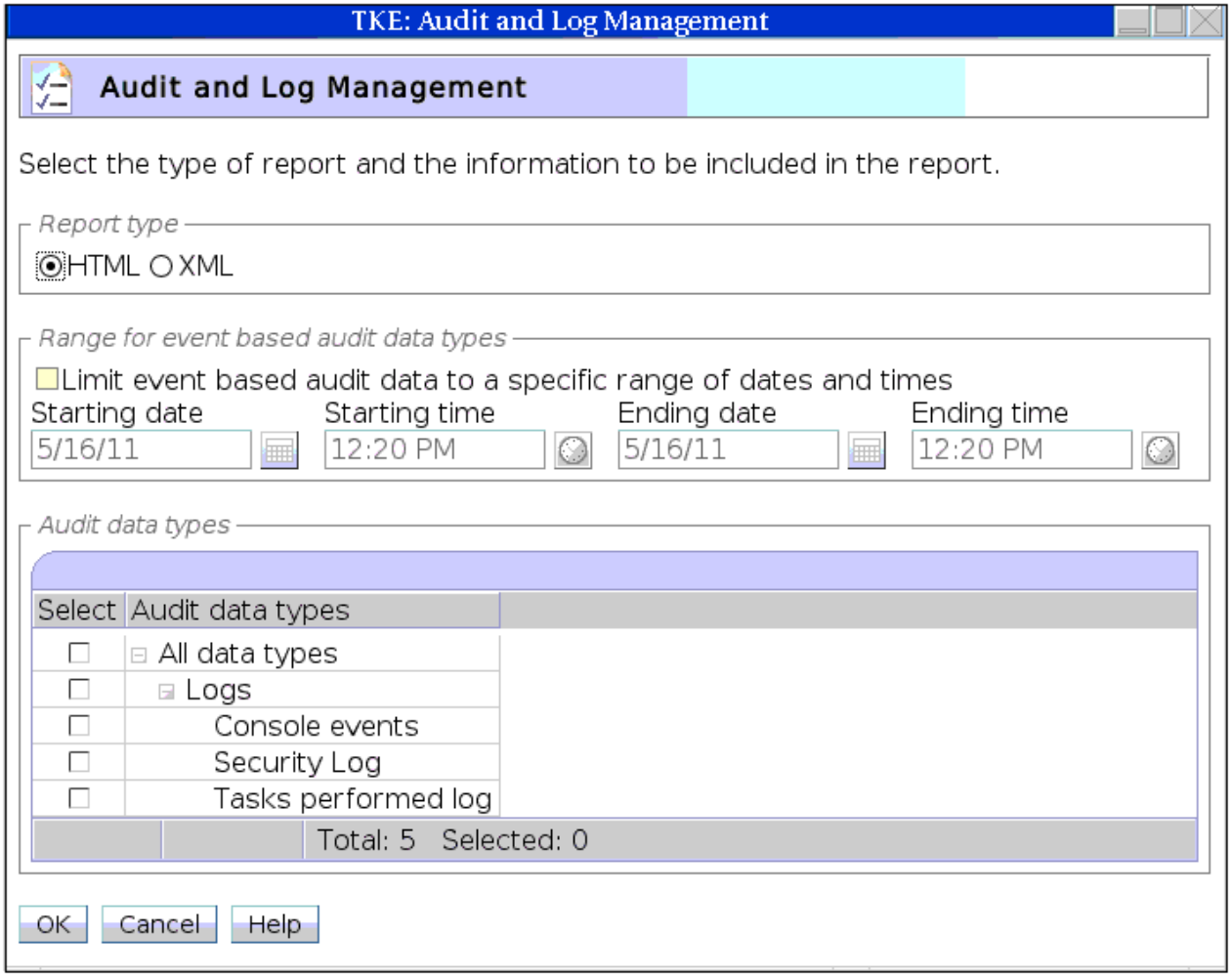


Figure 171. Audit and Log Management dialog

The log data can be formatted in either HTML or XML format.

The starting and ending date and time values may be specified to limit the amount of log data that will appear in the report.

The types of data (console events, security log, and tasks performed log) can also be specified to limit the amount of data that appears in the report. Note that the events related to the TKE utilities are logged in the security log.

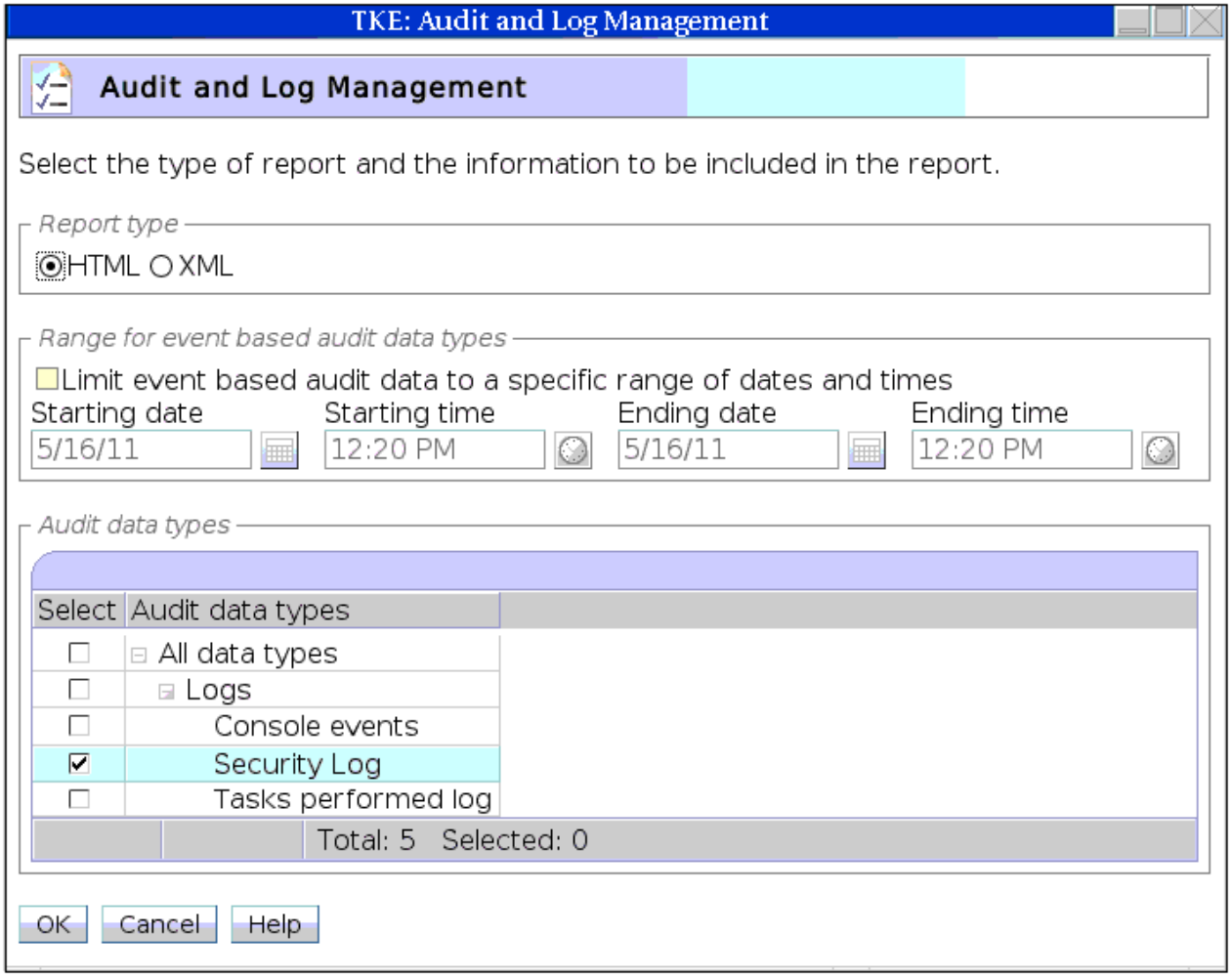


Figure 172. Audit and Log Management dialog (security log data selected)

After pressing OK, the log data is formatted in either HTML or XML format, and is displayed in a window.

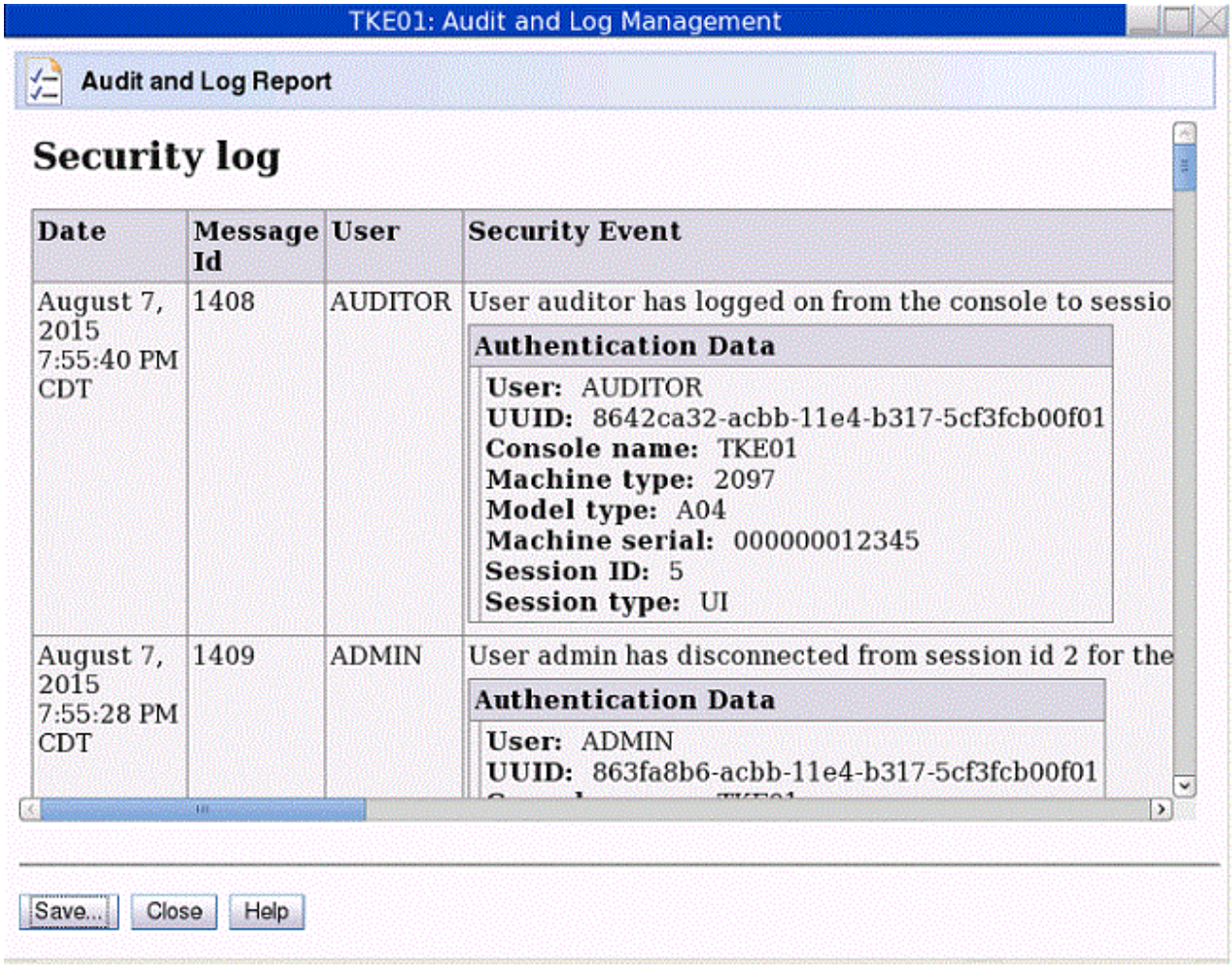


Figure 173. Security Log

This window contains the report produced from the log data. To save the report to a USB flash memory drive, click **Save**. The Export Data window opens.

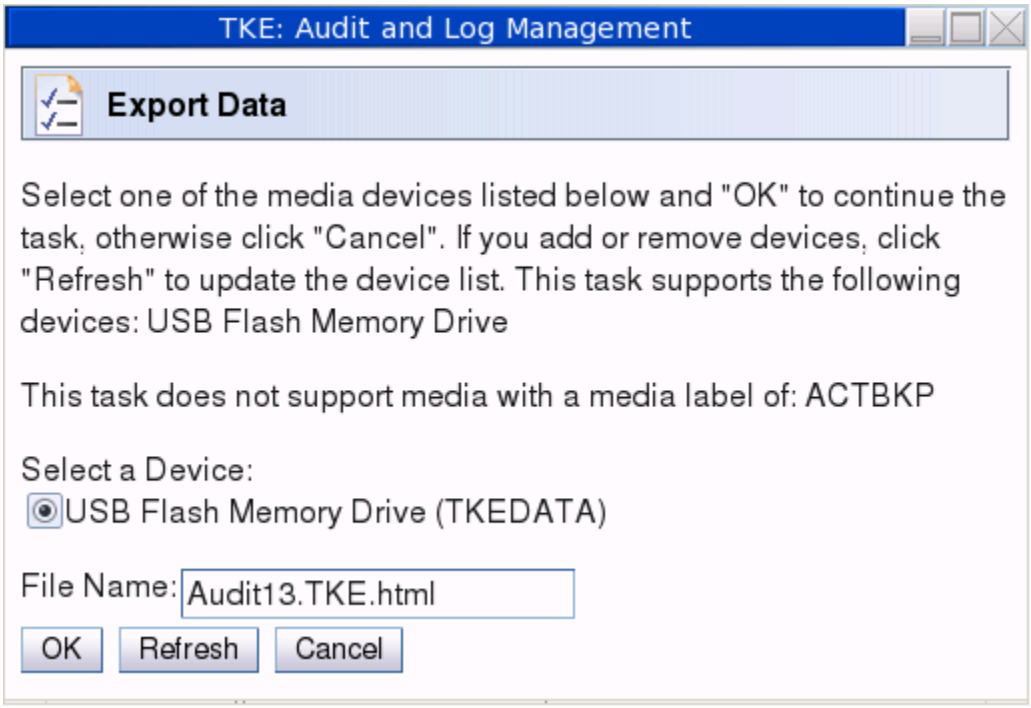


Figure 174. Export Data

Note: If a USB flash memory drive is not currently present, nothing is listed under **Select a Device**. To write to a USB flash memory, drive insert the drive, wait for the USB Device Status window to appear, and then click **Refresh**. When **OK** is clicked, the report is saved with the specified file name to the USB flash memory drive.

A pop-up window is displayed to indicate that the report was saved successfully.

Archive security logs

If you wish to archive the security logs you must be logged onto the TKE console with the AUDITOR user name. Archiving the security logs saves the security log's event data in another file on the USB flash memory drive, and then erases enough events from the security log to reduce its size to 20% of its maximum capacity.

In order to Archive the Security log, log in as the AUDITOR user and select **Service Management**. From the service management window select **Archive Security Logs**.

Note: You must have a USB flash memory drive that is formatted with no volume label or a volume label of ACTSECLG. Use the Format Media utility to format the flash memory drive (see “Format media” on page 358).



Figure 175. Archiving the security logs

With a valid USB flash memory drive inserted, click **Archive**.

While the security log is being archived, an "Archiving Security Log..." message box displays. After the archiving is completed, a message box displays indicating that the archive operation has completed.

TKE Security Events Viewer

Use the TKE Security Events Viewer to view TKE-specific security events within a specified date range.

TKE security events are displayed in a tree format, where each node is a TKE security event with a corresponding timestamp. Expand the security event to see the security event details and header information. Expand the security event details and header information to further view the detailed information. Collapse to hide the content.

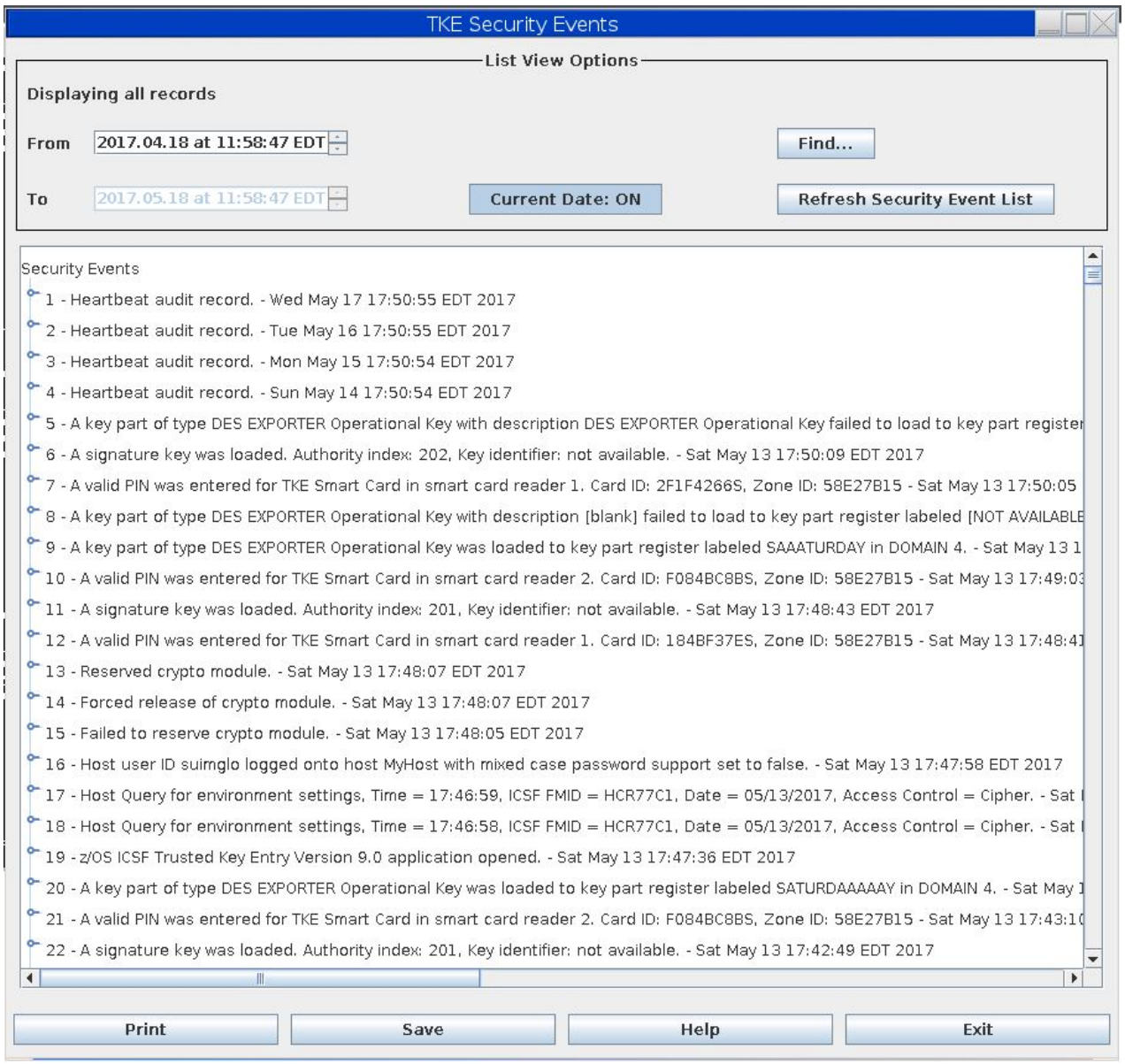


Figure 176. TKE Security Events

To view records within a different date range, change the dates in the From and To fields on the TKE Security Events panel and click the **Refresh Security Event List** button. The tree is refreshed with security events within the new date range.

Note: If the **Current Date** button is toggled to ON, the audit log retrieves records up until the current time. If the **Current Date** button is toggled to OFF, the audit log retrieves records up until the date in the To field.

To filter or find security events that contain a specific string of text, click the **Find...** button. In the text box that is displayed, enter the string of text that you want to search for in the Security Audit log and click the **Ok** button. The tree is refreshed to include only those security events that contain the text string entered that fall within the given To and From date range.

To print the currently displayed, fully expanded audit report, click the **Print** button.

To save the currently displayed, fully expanded audit report to a file, click the **Save** button.

To display the help text, click the **Help** button.

To close the TKE Security Events Viewer, click the **Exit** button.

TKE Audit Record Upload Configuration utility

ICSF uses SMF record type 82 to record certain ICSF events. ICSF writes to subtype 16 whenever a TKE workstation either issues a command request to, or receives a reply response from, a CCA or EP11 crypto module. In addition to the subtype 16 records, you can use the TKE Audit Record Upload Configuration Utility to send Trusted Key Entry workstation security audit records to a Z host, where they will be saved in the z/OS System Management Facilities (SMF) dataset. Each TKE security audit record is stored in the SMF dataset as a type 82 subtype 29 record.

Note: The audit upload process does not remove any data from the TKE Workstation. Copies of security audit records are sent to the host system and all data is retained by the TKE Workstation.

Starting the TKE Audit Record Upload Configuration utility

To use the TKE Audit Record Upload Configuration utility, you must first sign on to the Trusted Key Entry console in **Privileged Mode Access** with the AUDITOR user ID. To do this:

1. Close the Trusted Key Entry Console.
2. From the Welcome to the Trusted Key Entry Console screen select *Privileged Mode Access*.
3. From the Trusted Key Entry Console Logon screen, enter the user name AUDITOR and the password. (The default password is PASSWORD, but this can be changed by the user. See “Change password ” on page 353.)
4. Press the **Logon** push button.

To start the TKE Audit Record Upload Configuration utility, go to the Trusted Key Entry Console Workplace window and select *TKE Audit Record Upload Utility*.

The TKE Audit Record Upload Configuration Utility window is displayed.

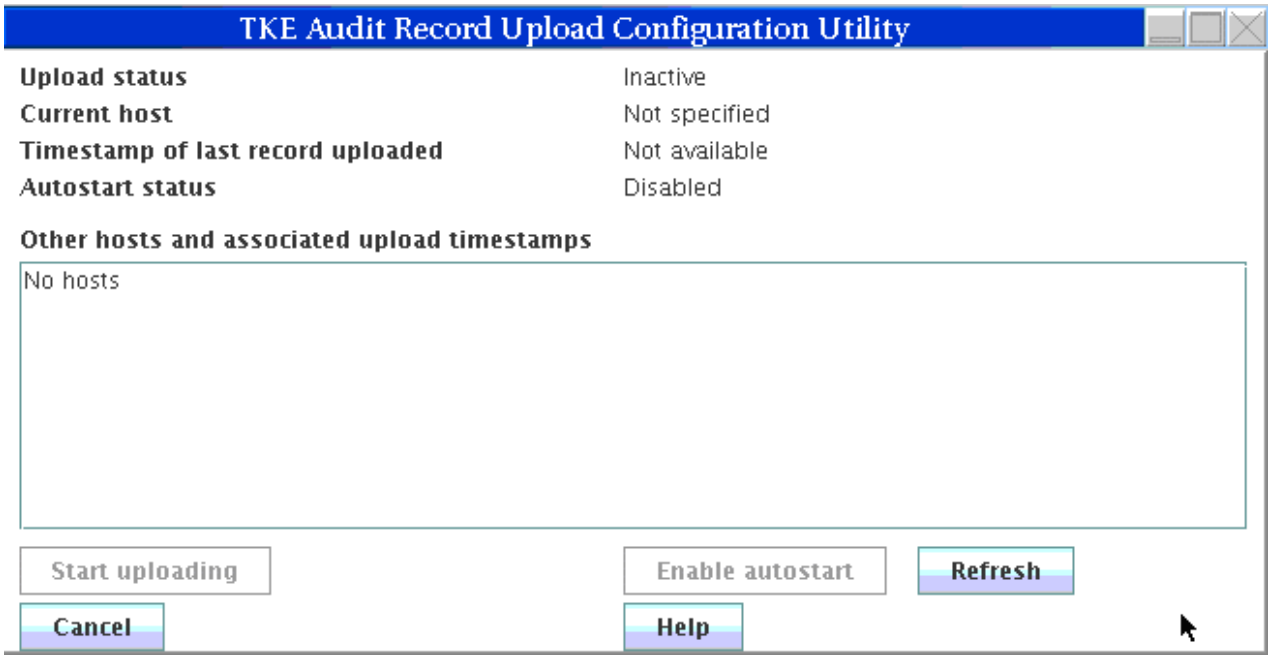


Figure 177. TKE Audit Record Upload Configuration utility

Using the TKE Audit Record Upload Configuration utility, you can:

- Specify the host machine to which the audit records will be sent. See “Configure TKE for audit data upload” on page 239 for more information.
- Upload audit records to the target host. See “Uploading audit records” on page 240 for more information.

- Enable automatic audit record upload. When enabled, audit records will be uploaded every time the workstation is rebooted. See “Enabling and disabling automatic audit record upload” on page 240 for more information.

Configure TKE for audit data upload

To upload audit data to a host system, you need to add the target host to the TKE Audit Record Upload utility's host list, and make the target host the current host:

1. Add the target host to the TKE Audit Record Upload utility's host list:
   a. In the TKE Audit Record Upload Configuration Utility window, right-click to display a pop-up menu, and select the **Add Host** menu item.

      The Specify Host Information dialog is displayed.

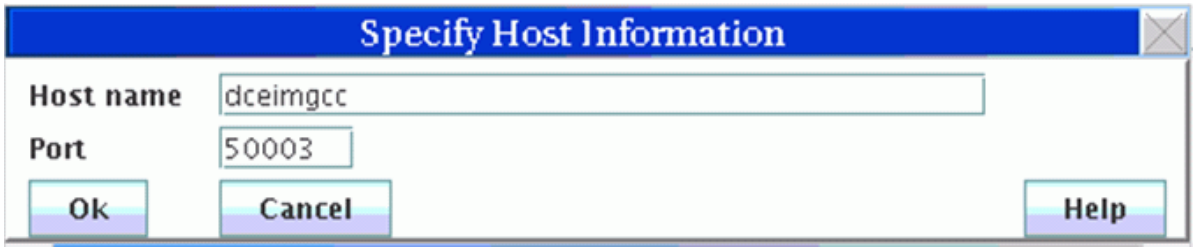


      Figure 178. Specify Host Information dialog

   b. In the Specify Host Information dialog's Host name field, enter the host name.
   c. In the Specify Host Information dialog's Port field, enter the port number that is assigned to the TKE Host Transaction Program.
   d. Click the **Ok** button.

      The Specify Host Information dialog closes and the host name is added to the TKE Audit Record Upload Configuration Utility's host list. The host name appears in the *Other hosts and associated timestamps* area of the window.

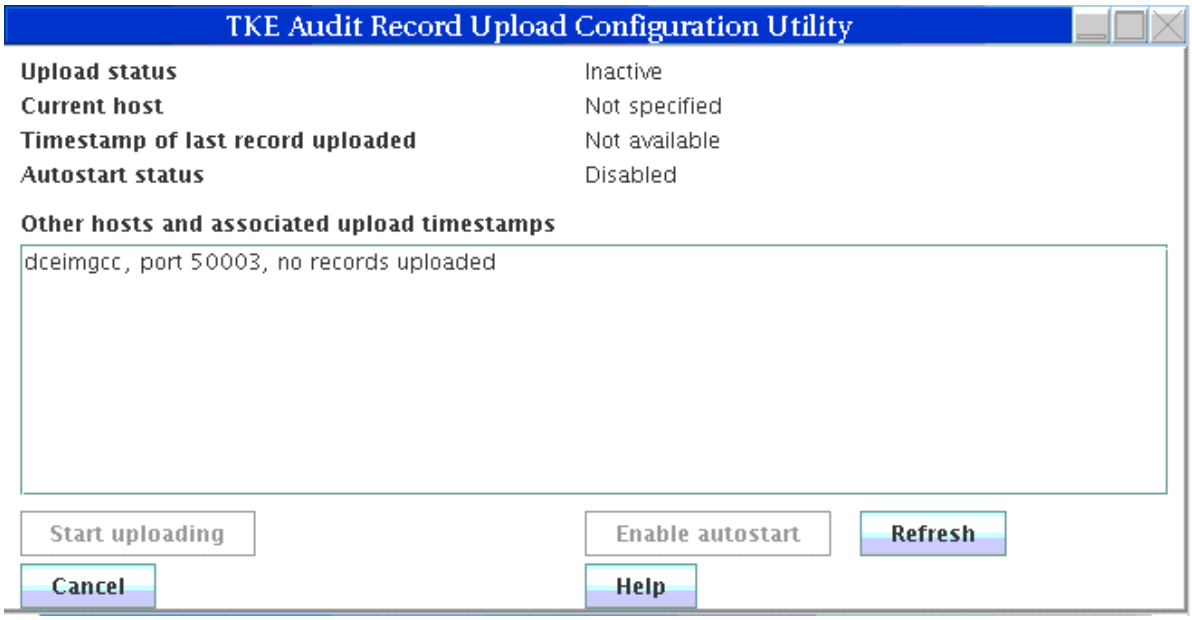


      Figure 179. Other hosts and associated timestamps

2. Make the target host the current host. To complete this step, you must have a user ID and password for the target host.

a. In the TKE Audit Record Upload utility window's *Other hosts and associated upload timestamps* area, right-click on the target host name to display a pop-up menu, and select the **Specify current host** menu item.

   The Specify Host Login Information dialog is displayed.



Figure 180. Specify Host Login Information

b. In the Specify Host Login Information dialog, enter the user ID and password, and click the **Ok** button.

   The target host is made the current host. The host name appears in the Current Host field of the TKE Audit Record Upload Configuration Utility.

After the target host has been identified in the TKE Audit Record Upload utility, you can:

- Upload audit records to the target host. For more information, see "Uploading audit records" on page 240.
- Enable automatic audit record upload. When enabled, audit records are uploaded every time that the workstation is rebooted. For more information, see "Enabling and disabling automatic audit record upload" on page 240.

Uploading audit records

Once you have used the TKE Audit Record Upload Configuration utility to specify the target host (as described in "Configure TKE for audit data upload" on page 239), you can upload audit records to the target host. If you have not already logged onto the host system during this session, the Specify Host Logon Information dialog will prompt you for a user ID and password before the audit records will be uploaded. To complete this task, you must have a user ID and password for the target host.

In the TKE Audit Record Upload Utility window, click the **Start uploading** push button.

Note: If you have not already logged onto the host system, the Specify Host Logon Information dialog will prompt you for a user ID and password.

The TKE Audit Record Upload Configuration utility will begin uploading the audit records to the target host. The TKE Audit Record Upload Configuration Utility window's Upload status field will indicate the status of the upload operation.

- Pressing the **Refresh** push button will refresh the TKE Audit Record Upload Utility window. In particular, the Timestamp of last record uploaded field will be updated.
- Pressing the **Stop uploading** push button will stop the audit record upload.

You can also enable automatic audit record upload. When enabled, audit records will be uploaded every time the workstation is rebooted. See "Enabling and disabling automatic audit record upload" on page 240 for more information.

Enabling and disabling automatic audit record upload

Once you have used the TKE Audit Record Upload Configuration utility to specify the target host (as described in "Configure TKE for audit data upload" on page 239), you can enable automatic audit record

upload. This is called autostart mode. In autostart mode, audit records will be uploaded every time the workstation is rebooted. If you have not already logged on to the host system during this session, the Specify Host Logon Information dialog will prompt you for a user ID and password before autostart mode will be enabled. To complete this task, you must have a user ID and password for the target host.

In the TKE Audit Record Upload Utility window, click the **Enable autostart** push button.

Note: If you have not already logged on to the host system, the Specify Host Logon Information dialog will prompt you for a user ID and password.

The TKE Audit Record Upload Configuration Utility will enable autostart mode, and will upload audit records every time the workstation is rebooted. The TKE Audit Record Upload Configuration Utility window's Autostart status field will indicate that autostart is enabled.

To disable automatic audit record upload, click the **Disable autostart** push button.

Chapter 10. Managing keys using TKE and ICSF

Master keys are used to protect all cryptographic keys that are active on your system.

Because master key protection is essential to the security of the other keys, ICSF stores the master keys within the secure hardware of the cryptographic feature. This nonvolatile key storage area is unaffected by system power outages because it has a battery backup. The values of the master keys never appear in the clear outside the cryptographic feature.

Requirements: ICSF is required to complete some operations that are initiated from TKE:

- For CCA host crypto modules, operations that require ICSF include setting the master keys, loading operational keys into the CKDS, and loading RSA keys from a host data set to the PKDS.
- For CCA host crypto modules, ICSF is also required for initializing or refreshing the CKDS, disabling and enabling PKA services, PKDS initialization, PKDS reencipher, and PKDS activate.
- For EP11 host crypto modules, operations that require ICSF include first-time setting of the P11 master key, any subsequent P11 master key change, initializing or updating the TKDS, and reenciphering the TKDS.

For more information about these ICSF procedures, see *z/OS Cryptographic Services ICSF Administrator's Guide*.



Attention: Be prepared to switch between your TKE workstation and your ICSF host session.

Note: Under normal circumstances, set master keys by using ICSF services that coordinate setting the master key with initializing or re-enciphering key storage. Failure to do this can cause the keys or tokens in key storage to become unusable when accessed by ICSF. There are some exceptions.

- ICSF before FMID HCR7790 allows the RSA master key to be set from TKE by using the **Set** option, but PKA Callable Services must be disabled first. If no online host crypto modules are at the September 2011 LIC level or later, ICSF at FMID HCR7790 or later also allows the RSA master key to be set from TKE by using the **Set** option.
- Beginning with TKE 7.3, the **Set, immediate** option allows any master key to be set from TKE. Use this option only when key storage does not need to be initialized or re-enciphered when the master key is set. For example, this option can be used to reload a previous master key value if a host crypto module has been inadvertently zeroized.

Changing master keys

For security reasons your installation should change the master keys periodically. In addition, if the master keys have been cleared, you might want to change the master keys after you reenter the cleared master keys.

For CCA host crypto modules, the DES and AES master keys protect the Cryptographic Key Data Set (CKDS). There are three main steps involved in changing the DES or AES master key:

1. Load the DES or AES master key parts into the new master key register.
2. Reencipher the CKDS under the new DES or AES master key.
3. Change the new DES or AES master key and activate the reenciphered CKDS.

In the first step, DES and AES master key parts can be loaded using TKE, or from ICSF panels. The second and third steps are performed using ICSF, or can be done using the Coordinated KDS Change Master Key utility (FMID HCR7790 or higher). For information about this utility, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

For CCA host crypto modules, the RSA and ECC (APKA) master keys protect the Public Key Data Set (PKDS). There are six main steps involved in changing the RSA or ECC (APKA) master key:

© Copyright IBM Corp. 2000, 2021

1. Disable PKA Services (required to load the RSA master key).
2. Enter the RSA or ECC (APKA) master key parts into the new master key register.
3. Reencipher the PKDS under the new RSA or ECC (APKA) master key.
4. Change the new master keys and activate the reenciphered PKDS.
5. Enable PKA Services.
6. Enable Dynamic PKDS Access.

RSA and ECC (APKA) master key parts can be loaded using TKE or from ICSF panels. The other steps are performed using ICSF, or can be done using the Coordinated KDS Change Master Key utility (FMID HCR77A0 or higher). For information about this utility, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

Notes:

1. On older versions of ICSF, the RSA master key is called the asymmetric master key.
2. ICSF uses the term 'ECC master key'. CCA calls it the 'APKA master key'. On TKE, it is referred to as the 'ECC (APKA) master key'.
3. Steps “1” on page 244, “5” on page 244, and “6” on page 244 are not required on z196/z114 and newer systems.

For EP11 host crypto modules, the P11 master keys protect the PKCS #11 token key data set (TKDS).

If multiple instances of ICSF share the same TKDS in a sysplex environment, the P11 master key must be set to the same value for each instance. All instances must be at FMID HCR77A0 or higher, even if they do not use secure PKCS #11 services. A TKE domain group can be used to manage the multiple domains of the ICSF instances so that all receive the same new P11 master key value.

There are three main steps involved in changing the P11 master key:

1. Load the P11 master key parts into the new master key register.
2. Create a VSAM data set to hold the reenciphered keys.
3. Do a coordinated TKDS master key change.

In the first step, P11 master key parts must be loaded using TKE. There is no ICSF option to load P11 master key parts. ICSF is required to perform the other steps.

For step-by-step ICSF procedures for changing master keys, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

Adding host crypto modules after ICSF initialization

You might want to add additional host crypto modules to your system. After the new crypto modules have been installed and configured by the appropriate hardware personnel, make them known to the TKE workstation by following the appropriate procedure.

1. Open the Host where the crypto module or modules were added. You will be prompted to authenticate the crypto module.
2. Open the new crypto module or modules.
3. Use the authority 0 default signature key to administer access control (create the same roles and authorities for the new crypto module to match the crypto modules currently on the host). Load the authority signature keys to match the other crypto modules.
4. Load a new signature key for an authority that can load master keys. If one authority does not have the ability to load all the master key parts for each master key, you may need to load additional authority signature keys.
5. Load the master keys.

Note: The keys should be the same keys that you loaded to the other crypto modules. If you are adding more than one crypto module, load the keys in all crypto modules before setting the master key.

6. Set the DES or AES master key on the crypto module from ICSF when everything is the same (roles, authorities, controls, master keys).
7. If desired, add the new crypto module to the group by doing a group change.

Loading operational keys to the CKDS

You can load operational key parts into operational key part registers on host crypto modules using the TKE workstation. To load the completed operational keys into a host CKDS, you need to use the ICSF Operational Key Load panel or the Key Generator Utility Program (KGUP). For KGUP details, refer to *z/OS Cryptographic Services ICSF Administrator's Guide*.

There are two access control points that control the use of the Operational Key Load Utility:

For fixed length DES and AES key tokens
X'0309' - Operational Key Load must be enabled.

For variable-length AES key tokens
X'029E' - Operational Key Load - Variable-Length Tokens must be enabled.

The names of the access controls depends on the release of ICSF where the utility is used:

For ICSF FMID HCR7780 and older releases
X'0309' - Key Part Import - RETRKPR

For ICSF FMID HCR7790

- X'029E' - Key Part Import2 - RETRKPR
- X'0309' - Key Part Import - RETRKPR

For ICSF FMID HCR77A0

- X'029E' - Key Part Import2 - RETRKPR
- X'0309' - Operational Key Load

For ICSF FMID HCR77A1 and later releases

- X'029E' - Operational Key Load - Variable-Length Tokens
- X'0309' - Operational Key Load

If an access control is disabled, the following panel message appears, 'ACCESS CONTROL FOR KEY PART IMPORT - RETRKPR FAILED'. The message is meant to indicate that the access control required for your key is not enabled.

Before a key can be loaded into the CKDS from a key part register, it must be in the complete state. If the key part register is not in the complete state, the error message `KEY NOT COMPLETE` will result.

To load operational keys into the CKDS, start at the ICSF main menu and follow these instructions:

1. Select option 1, `COPROCESSOR MGMT`, on the primary menu panel

```
HCR77C1 ------------ Integrated Cryptographic Service Facility ---------

System Name:                                  Crypto Domain:
Enter the number of the desired option.

   1  COPROCESSOR MGMT    -  Management of Cryptographic Coprocessors
   2  KDS MANAGEMENT      -  Master key set or change, KDS processing
   3  OPSTAT              -  Installation options
   4  ADMINCNTL           -  Administrative Control Functions
   5  UTILITY             -  ICSF Utilities
   6  PPINIT              -  Pass Phrase Master Key/KDS Initialization
   7  TKE                 -  TKE PKA Direct Key Load
   8  KGUP                -  Key Generator Utility processes
   9  UDX MGMT            -  Management of User Defined Extensions

      Licensed Materials - Property of IBM
      5650-ZOS (C) Copyright IBM Corp. 1989, 2017.
      US Government Users Restricted Rights - Use, duplication or
      disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

 Press ENTER to go to the selected option.
 Press END   to exit to the previous menu.
```

Figure 181. ICSF primary menu panel

2. The Coprocessor Management panel appears. Put a 'K' by the coprocessor that contains the key part register to load.

```
CSFCMP00 ---------------- ICSF Coprocessor Management -------------

Select the coprocessors to be processed and press ENTER.
Action characters are: A, D, E, K, R, S, and V. See the help panel for details.

               Serial
 CoProcessor   Number    Status               AES   DES   ECC   RSA    P11
 -----------  ---------  ------               ---   ---   ---   ----   ___
 __ 4P00      16BA6173   Active                                         A
 __ 4C01      16BBP109   Master key incorrect  U     U     U     U
 __ 4A02      N/A        Active
 __ 4P03      16BBP103   Active                                         A
 __ 3C04      99001650   Active                A     A     A     A
 __ 3C05      99001652   Active                A     A     A     A
 __ 3A06      N/A        Active
 __ 3C07      99002519   Master key incorrect  U     U     U     U
 __ 3C08      91008972   Active                A     A     A     A
 __ 3C09      90008301   Active                A     A     A     A
 __ 4C14      16C35329   Active                A     A     A     A
 __ 4P15      16C2H305   Active                                         A
```

Figure 182. Coprocessor Management panel

3. The Operational Key Load panel appears. The coprocessor previously selected and the active CKDS are displayed at the top of the panel.

```
CSFCMP50 ---------------- ICSF - Operational Key Load ------------------------
COMMAND ===>

Coprocessor selected for new key:  7C41
CKDS Name:  CSF.CKDS

Enter the key label.

Key label
===>

Control Vector    ===> YES  YES or NO (DES IMPORTER and EXPORTER only)
Enhanced Wrapping ===> NO   YES or NO (DES keys only)
```

Figure 183. Operational Key Load panel

a. In the Key Label field, enter the CKDS entry label for the key. The label must match the key label specified on the key part information window on TKE when the First key part was loaded to the key part register. Otherwise, a KEY NOT FOUND message is displayed. See "Load single key part" on page 173.

b. In the Control Vector field, enter YES or NO. This field only applies if the key being loaded is a standard CV IMPORTER or EXPORTER key. If it is and you specify NO, ICSF will mark the key as a NOCV KEK. Select NO for keys that will be exchanged with a system that does not use control vectors. The default is YES.

c. In the Enhanced Wrapping field, enter YES or NO. This field applies to DES keys only. If you specify YES, the key is wrapped with the enhanced wrapped method. If you specify NO, the key is wrapped based on the default wrapping parameter DEFAULTWRAP in the installation options data set. DES keys that are required to be enhanced wrapped will always be wrapped with the enhanced method and this option has no effect. When the coprocessor does not support enhanced wrapping for DES keys, this option is ignored and has no effect.

If ICSF FMID HCR77D1 APAR OA60318 is installed, the panel will have a new option for enhanced wrapping.

```
CSFCMP50 ---------------- ICSF - Operational Key Load -------------------------
COMMAND ===>

Coprocessor selected for new key:  7C41
CKDS Name:  CSF.CKDS

Enter the key label.

Key label
===>

Control Vector    ===> YES  YES or NO (DES IMPORTER and EXPORTER only)
Enhanced Wrapping ===> NO   ENH, ENH3, or NO (DES keys only)
```

In the Enhanced Wrapping field, specify NO, ENH, or ENH3.

- If you specify ENH3, the key will be wrapped with the WRAPENH3 method if it is available on your system or the enhanced wrapping method if the WRAPENH3 method is not available on your system.
- If you specify ENH, key will be wrapped with the enhanced wrapping method.
- If you specify NO, the key will be wrapped based on the setting of the DEFAULTWRAP parameter in the installation options data set. When the coprocessor does not support enhanced wrapping for DES keys, this option has no effect. DES keys that are required to be enhanced wrapped will always be wrapped with the enhanced method and this option has no effect.

If a record already exists in the CKDS with a label that matches the key label specified, the Operational Key Load panel appears alerting you that CKDS RECORD EXISTS. If you want to replace the existing key with the new key you are trying to load, press ENTER.

```
CSFCMP51 -------------- ICSF - DES Operational Key Load --- CKDS RECORD EXISTS
COMMAND ===>

A record with the following specifications has been found in the CKDS:

Key label: DES.IMPPKA.0305
Key type : IMP-PKA
```

Figure 184. Operational Key Load panel

When a DES operational key is successfully loaded, the ENC-ZERO value and control vector are displayed for the user. When an AES operational key is successfully loaded, the AES-VP is displayed.

```
CSFCMP50------------------ ICSF - Operational Key Load ------ KEY LOAD COMPLETE
COMMAND ===>

Coprocessor selected for new key:  7C41
CKDS Name:  CSF.CKDS

Enter the key label.

Key label
===> DES.IMPPKA.0305

Control Vector    ===> YES  YES or NO (DES IMPORTER and EXPORTER only)
Enhanced Wrapping ===> YES  YES or NO (DES keys only)

ENC-ZERO VP:         77C92984

Control vector:      0042050003410000
0042050003210000
```

Figure 185. Operational Key Load Panel - ENC-ZERO and CV values displayed

```
CSFCMP50------------------ ICSF - Operational Key Load ------ KEY LOAD COMPLETE
COMMAND ===>

Coprocessor selected for new key:  7C41
CKDS Name:  CSF.CKDS

Enter the key label.

Key label
===> AES.IMPORTER.0305

Control Vector    ===> YES  YES or NO (DES IMPORTER and EXPORTER only)
Enhanced Wrapping ===> NO   YES or NO (DES keys only)

AES-VP:              8B0CEDFD74D1CC3E
```

Figure 186. Operational Key Load Panel - AES -VP displayed

Installing RSA keys in the PKDS from a data set

If you used TKE to load an RSA key into a host data set member, you load it from the data set to the PKDS by this method.

1. Select option 7, TKE, on the primary menu panel

```
HCR77B1 ------------- Integrated Cryptographic Service Facility ---------

System Name:                                    Crypto Domain:
Enter the number of the desired option.

   1  COPROCESSOR MGMT    -  Management of Cryptographic Coprocessors
   2  KDS MANAGEMENT      -  Master key set or change, KDS processing
   3  OPSTAT              -  Installation options
   4  ADMINCNTL           -  Administrative Control Functions
   5  UTILITY             -  ICSF Utilities
   6  PPINIT              -  Pass Phrase Master Key/KDS Initialization
   7  TKE                 -  TKE PKA Direct Key Load
   8  KGUP                -  Key Generator Utility processes
   9  UDX MGMT            -  Management of User Defined Extensions

      Licensed Materials - Property of IBM
      5650-ZOS (C) Copyright IBM Corp. 1989, 2015.
      US Government Users Restricted Rights - Use, duplication or
      disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

 Press ENTER to go to the selected option.
 Press END   to exit to the previous menu.
```

Figure 187. Selecting the TKE option on the ICSF primary menu panel

2. On the ICSF PKA Direct Key Load panel, enter the name of the pre-allocated partitioned data set and the member name of the RSA key to be loaded into the PKDS.

```
-------------------------- ICSF - PKA Direct Key Load -------------------------
COMMAND ===>

 Enter the data set name and the key specifications.

 Key Data Set
  Name   ===> 'SUIMGCD.PRIVATE.RSAKEYS.AES(R0525A)'
```

Figure 188. PKA Direct Key Load

If the RSA key is loaded successfully into the PKDS, a **LOAD COMPLETED** message is displayed in the upper right corner. If an error occurs during the load process, an applicable error message is displayed in the upper right corner with detailed error information displayed in the middle of the display for selected errors. You may also press the PF1 key for more information.

Chapter 11. Cryptographic Node Management utility (CNM)

The Cryptographic Node Management (CNM) utility is a Java application that provides a graphical user interface to initialize and manage the TKE workstation crypto adapter. It is part of the IBM Cryptographic Coprocessor CCA Support Program.

This topic describes the functions of CNM that are used for initializing and managing the TKE workstation crypto adapter.

Note: Smart Card and Smart Card Group options within the CNM panels will only be available if CNM is enabled to support Smart Cards. See “Initializing the TKE workstation crypto adapter for use with smart card profiles” on page 85.

To start CNM, click with the left mouse button on the "Trusted Key Entry" link in the left panel of the main Trusted Key Entry Console page. Then, under the "Applications" section displayed in the right panel, click with the left mouse button on "Cryptographic Node Management Utility".

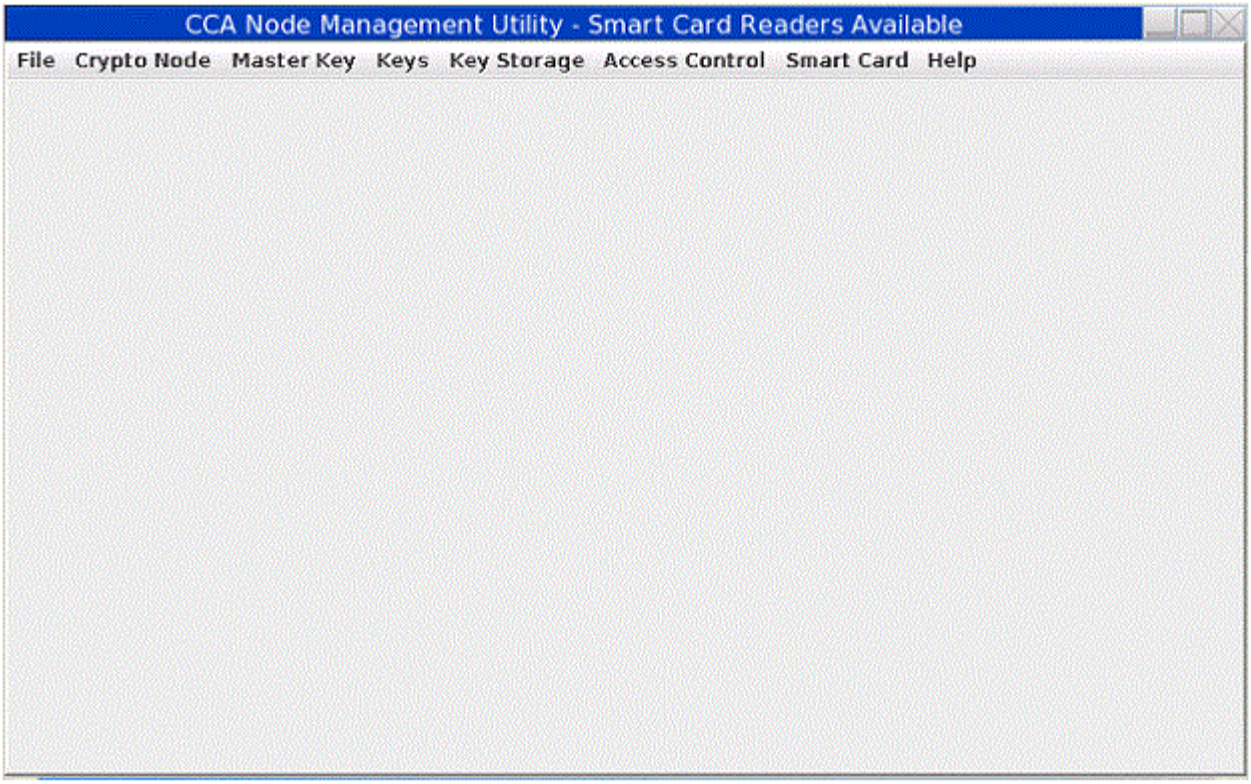


Figure 189. CNM main window

Crypto adapter logon

To run the Cryptographic Node Management utility (CNM), you must log on to the TKE workstation crypto adapter. If you start CNM and are not already logged on to the TKE workstation crypto adapter, you will be prompted to select a user profile and log on (as described in “Crypto adapter logon: passphrase or smart card” on page 97).

Only profiles authorized to run CNM will be displayed. If, when you start CNM, you are logged on to the TKE workstation crypto adapter with a profile that is not authorized to run CNM, a warning will be displayed and you will be asked if you want to log off and log on with a different user profile.

© Copyright IBM Corp. 2000, 2021

File menu

From the **File** pull-down, you can choose the following actions:

CNI editor
The CNI editor is a utility within the CNM utility that is used to create CNI scripts to automate some of the functions of CNM.

Enable smart card readers
This option enables smart card readers for CNM and for other TKE applications.

Note: When the TKE workstation crypto adapter is initialized for smart card use, this option is automatically selected.

Exit
Exit the CNM application.

Exit and logoff
Exit the CNM application and log off from the TKE workstation crypto adapter.

Select **Yes** to confirm logoff. A successful message is displayed.

Crypto Node menu

TKE crypto adapter clock-calendar

The TKE workstation crypto adapter uses its clock-calendar to record time and date and to prevent replay attacks in passphrase logon.

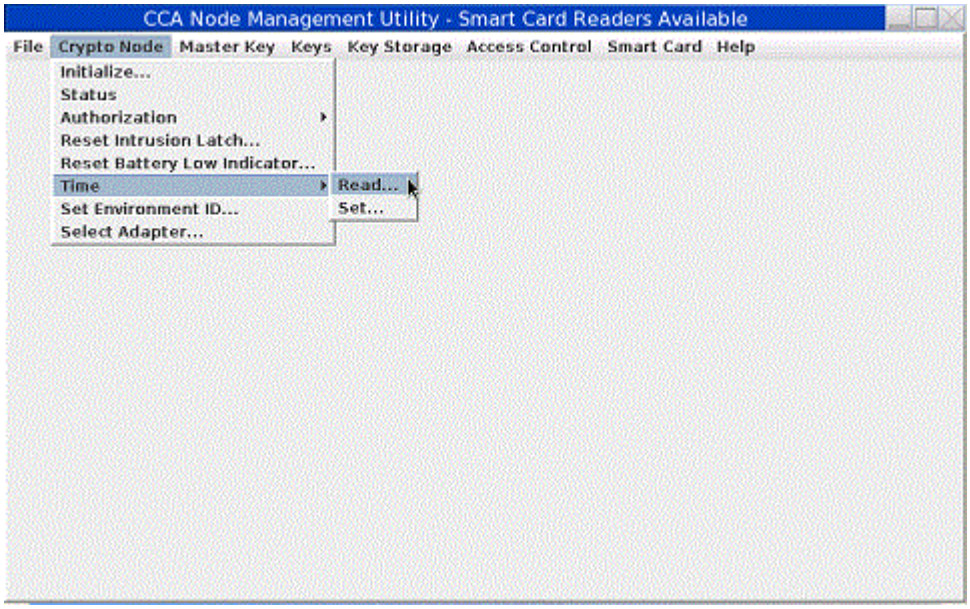


Figure 190. CNM main window — Crypto Node Time sub-menu

Read clock-calendar

To read the TKE workstation crypto adapter clock-calendar:

1. From the **Crypto Node** pull-down menu, select **Time**. A sub-menu is displayed.
2. From the sub-menu, select **Read**; the current date and time is displayed. The time is displayed in Greenwich Mean Time (GMT).

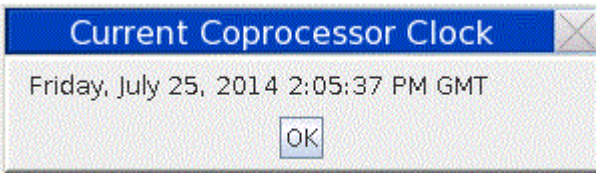


Figure 191. Current Coprocessor Clock

3. Finish the task by selecting **OK**.

Synchronize clock-calendar

To synchronize the TKE workstation crypto adapter clock-calendar with the TKE workstation clock:

Note: You must be logged on to the TKE workstation crypto adapter using TKEADM or an equivalent profile.

1. From the **Crypto Node** pull-down menu, select **Time**. A sub-menu is displayed.
2. From the sub-menu, select **Set**; a confirmation dialog is displayed.

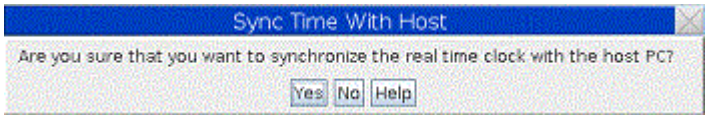


Figure 192. Sync time with host window

3. Respond **Yes** in the confirmation dialog to synchronize the clock-calendar with the host.
4. Finish the task by selecting **OK**.

Access Control menu

The Access Control pull down menu provides a set of features for managing roles and profiles on the crypto card that is on the TKE workstation. The crypto card on the TKE workstations is referred to as the “TKE local crypto adapter”. The roles and profiles on the TKE local crypto adapter control who can access the TKE workstation and what applications they can use once they have logged onto the TKE workstation. Each of the Access Control features are described in this section.

Recommendation: Beginning with TKE 8.1, creating role and profile definition files is discouraged. The new recommended method for saving and loading user defined roles and profiles is:

1. Create your set of user defined roles and profiles onto your TKE local adapter. Do not use the save button to create the .rol and .prf files.
2. After your set of user defined roles and profiles have been created, use the **Save User Roles and Profiles** feature to save the definitions in the TKESavedRoles.dat and TKESavedProfiles.dat files.
3. At a later time, use the **Load User Roles and Profiles** feature to load the roles and profiles onto a TKE local crypto adapter from the TKESavedRoles.dat and TKESavedProfiles.dat files. This is only done as needed. Examples of when you would load the roles and profiles are:
   - You have a new crypto card on your TKE workstation and you want to load your user defined roles and profiles.
   - You have a new or back up TKE workstation and you put the TKESavedRoles.dat and TKESavedProfiles.dat files on the new or back up TKE workstation. Now, you want the same user defined roles and profiles on this TKE workstation.

Initialize

Recommendation: Use the crypto adapter initialization feature instead of the Initialize function.

The Initialize feature attempts to delete all the roles and profiles, except for the DEFAULT role, from the TKE local crypto adapter. To successfully complete the operation, you need to:

- Sign onto the TKE workstation with privileged mode access ADMIN.

- Open the Cryptographic Node Management (CNM) utility with the DEFAULT role.
- The DEFAULT role must have the ACPs listed in the tempdefault_*xx*.rol file, where *xx* matches the TKE release level.

Note: On a properly secured TKE workstation, the DEFAULT role will be secured and will not have enough authority to run this feature.

You should know that:

- If you logon to CNM with a profile like TKEADM or SCTKEADM, the Initialize function stops when it tries to delete the profile you have signed on with. Only some roles and profiles are deleted in this case.
- If you log on with privileged mode access ADMIN and the DEFAULT role, when the default role is secured, you will not have enough authority to run the feature.

Managing profiles

When you initialize the TKE workstation crypto adapter, a set of system-supplied profiles are loaded on the adapter. You can use the CCA Node Management Utility's Profile Management window to modify the system-supplied profiles on the adapter, or to define and load your own profiles on the adapter.

Each of the system-supplied profiles is created from a corresponding system-supplied profile definition file that is stored on the TKE workstation's hard drive. You can also define your own profile definition files. The profile definition files you create can be stored on the TKE workstation's hard drive or on removable media. A profile definition file describes the attributes of a profile, and are important for migration between versions of TKE and for recovery. We recommend that you:

- Create profile definition files for any new profiles you create. This will help during migration to a new TKE workstation or for recovery of the TKE workstation crypto adapter data. If you later modify the profile loaded on the TKE workstation crypto adapter, you should also modify the corresponding profile definition file.

  When creating profile definition files, we further recommend:

  – Using the naming convention *profile-name*.pro.
  – Using the system-supplied roles (such as TKEUSER, SCTKEADM) whenever possible.
- Do not edit the system-supplied profile definition files. By leaving the system-supplied profile definition files unedited, you preserve the ability to restore system-supplied profiles to their default settings, including the default passwords. If you edit the system-supplied profiles, we recommend you save the modified settings to a new profile definition file instead of editing the original profile definition file.

To open the CCA Node Management Utility's Profile Management window:

1. Go to the CCA Node Management Utility main window.
2. From the **Access Control** pull-down menu, select **Profiles**.

   The CCA Node Management Utility's Profile Management window is displayed. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter.

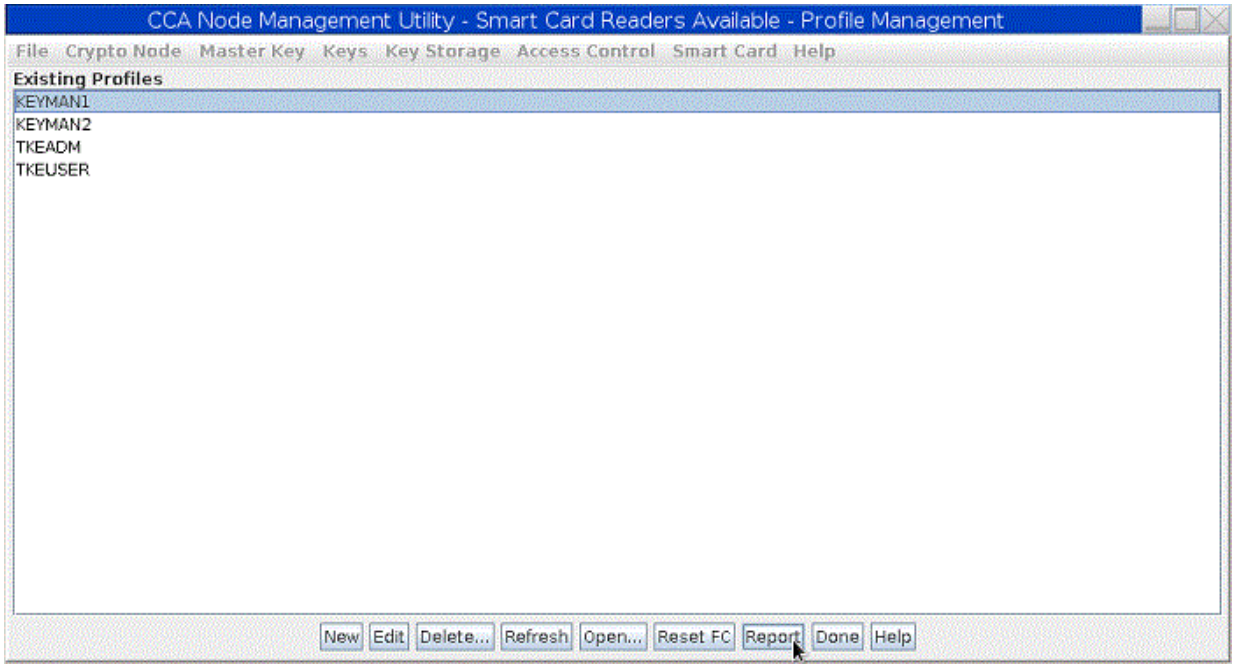


Figure 193. Profile Management window listing the profiles on the TKE's local crypto adapter

You can use the Profile Management window to manage the profiles on the TKE workstation crypto adapter and to manage any associated profile definition files. You can use:

- The **New** push button to create a new smart card, passphrase, or group profile.
- The **Edit** push button to edit a profile on the TKE workstation crypto adapter.
- The **Delete** push button to delete a profile by highlighting it and pressing the **Delete** button. To do this, you first select the profile in the window and then click the **Delete** button.
- The **Refresh** push button refresh the list in the window.
- The **Open** push button to open a profile definition file.
- The **Report** push button to create a report that lists all the individual and group profiles and their roles on your TKE workstation crypto adapter.
- The **Done** push button to close the window.

Clicking the **New**, **Edit**, or **Open** push buttons will all eventually open a window for modifying profile settings. The window will differ slightly depending on the type of profile – either a passphrase profile, a smart card profile, or a group profile. From this window, you will be able to load the settings as a profile on the TKE workstation crypto adapter (provided a profile of the same name is not already loaded on the adapter), or save the settings as a profile definition file on the TKE workstation's hard drive or on removable media.

To replace a profile that is already loaded on the TKE workstation crypto adapter, you will always want to use the **Edit** push button. Only by clicking the **Edit** push button will you be able to replace an already-loaded profile.

Creating a new profile or profile definition

Recommendation: Beginning with TKE 8.1, creating role and profile definition files is discouraged. The new recommended method for saving and loading user defined roles and profiles is:

1. Create your set of user defined roles and profiles onto your TKE local adapter. Do not use the save button to create the .rol and .prf files.
2. After your set of user defined roles and profiles have been created, use the **Save User Roles and Profiles** feature to save the definitions in the TKESavedRoles.dat and TKESavedProfiles.dat files.

3. At a later time, use the **Load User Roles and Profiles** feature to load the roles and profiles onto a TKE local crypto adapter from the TKESavedRoles.dat and TKESavedProfiles.dat files. This is only done as needed.

From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter.

To create a new profile or profile definition file, it does not matter if a profile name is highlighted in the CCA Node Management window, or if the list is empty. To create a new profile or profile definition file:

1. From the CCA Node Management Utility's Profile Management window, click on the **New** push button.

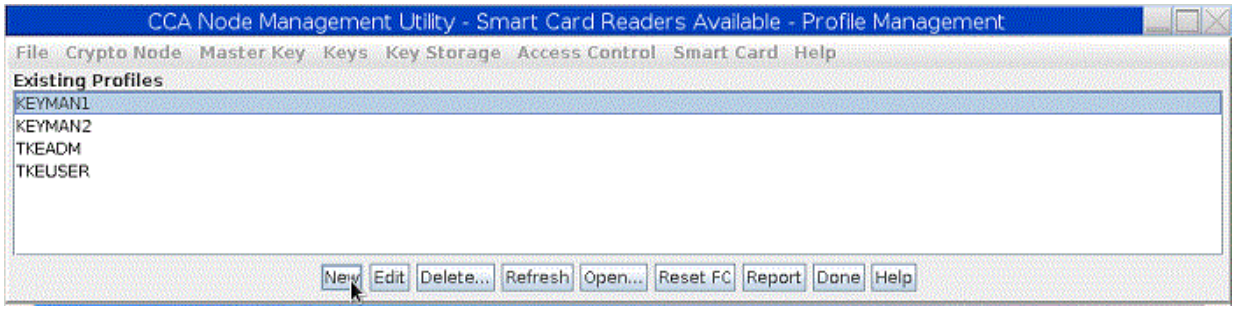


Figure 194. From the CCA Node Management Utility's Profile Management window, click on the New push button

A dialog window opens, prompting you for the type of profile you want to create.



Figure 195. Select profile type

2. In the dialog window, select the type of profile you want to create and click the **Continue** push button.

   A secondary window opens for modifying profile settings and then either loading those settings as a profile on the TKE workstation crypto adapter (provided a profile of the same name is not already loaded on the adapter) or saving those settings in a profile definition file. The window is populated with the default attributes and settings for a new passphrase profile, smart card profile, or group profile.

Editing a profile on the TKE workstation crypto adapter

From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter.

To edit a profile that is currently loaded on the TKE workstation crypto adapter:

1. In the list of profiles, click on the name of the profile you want to edit.

   The profile name is reverse highlighted (white on black) to show that it is selected.
2. Click on the **Edit** push button.

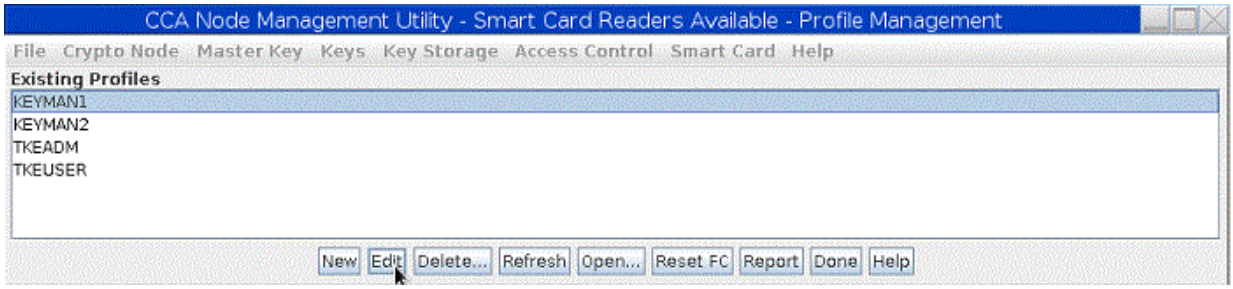


Figure 196. Select profile and click Edit

A secondary window opens for modifying profile settings and then either replacing profile on the TKE workstation crypto adapter or saving those settings in a profile definition file. This secondary window is populated with the attributes of the selected profile.

Opening a profile definition file

Profile definition files have all the attributes and settings necessary to create or update a profile on the TKE workstation crypto adapter. Unlike a profile, a profile definition file is not loaded onto the TKE workstation crypto adapter, but is instead stored on the TKE workstation's hard drive or on removable media. Keep in mind that:

- You can have a profile definition file for a profile that is not currently loaded on the TKE workstation crypto adapter.
- It is possible that the settings in a profile definition file do not currently match the settings of the actual profile on the TKE workstation crypto adapter.

From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter.

To open a profile definition file, it does not matter if a profile name is highlighted in the CCA Node Profile Management window, or if the list is empty. This is because you are not opening a profile on the TKE workstation crypto adapter. Instead, you are opening a file on the TKE workstation's hard drive or on removable media.

To open a profile definition file:

1. From the CCA Node Management Utility's Profile Management window, click on the **Open** push button.

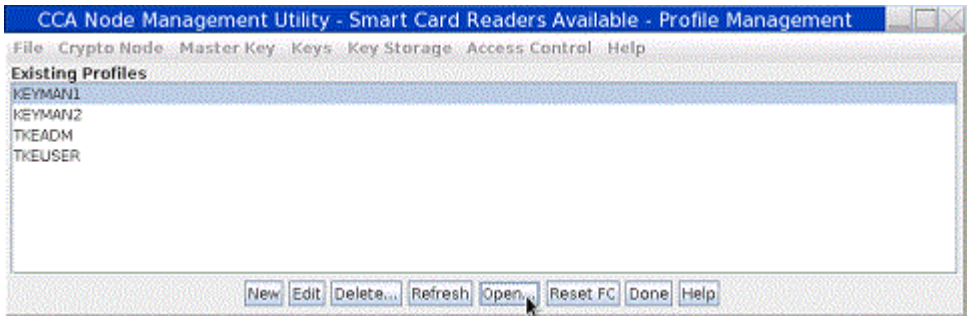


Figure 197. From the CCA Node Management Utility's Profile Management window, click on the Open push button

The **Specify file to open** dialog is displayed.

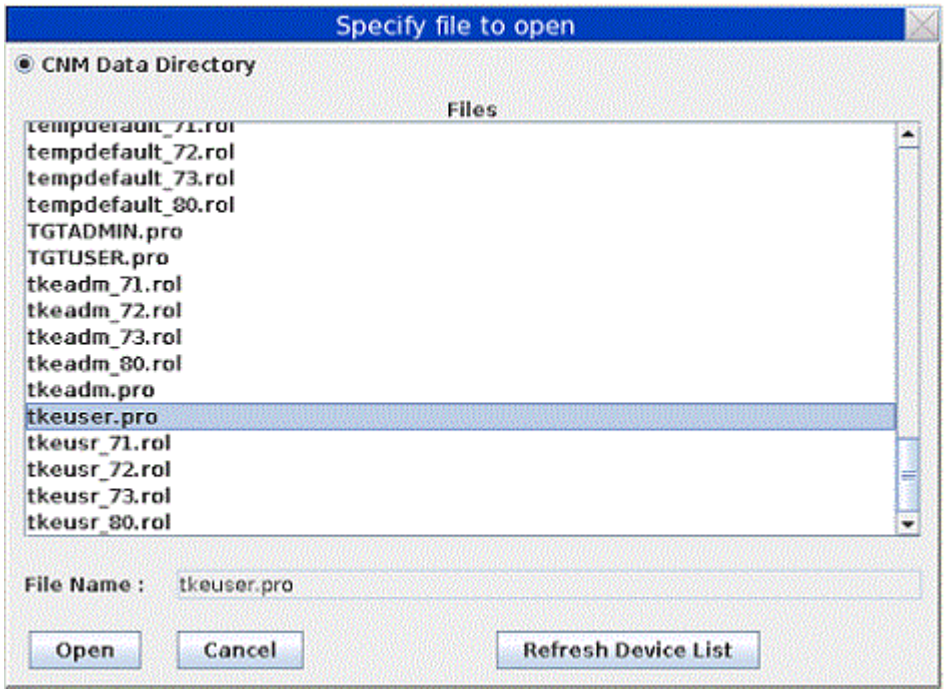


Figure 198. Specify file to open dialog

2. In the **Specify file to open** dialog:

   a. In the list of files, click on the name of the profile definition file you want to open. Profile definition files typically follow the naming convention *profile_name*.pro.

      The profile name is reverse highlighted (white on black) to show that it is selected.

   b. Click the **Open** push button.

      A secondary window opens for modifying profile settings and then either loading those settings as a profile on the TKE workstation crypto adapter (provided a profile of the same name is not already loaded on the adapter) or saving those settings in a profile definition file. This secondary window is populated with the attributes of the selected profile definition file.

Making changes to a profile or profile definition file

From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter. When you click the **New**, **Edit**, or **Open** push button on the initial window, a secondary window opens for modifying profile settings and then either loading those settings as a profile on the TKE workstation crypto adapter or saving those settings in a profile definition file.

- The **New** push button will first prompt you for the type of profile and then will open the window and populate it with default attributes for that profile type.
- The **Edit** push button will open the window and populate it with the attributes of the selected profile.
- The **Open** push button will open the window and populate it with the attributes of the selected profile definition file.

The window will differ slightly depending on the type of profile you are modifying – either a passphrase profile, a smart card profile, or a group profile.

Making changes to a passphrase profile or passphrase profile definition file

From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter. When you click the **New**,

Edit, or **Open** push button on the initial window, a secondary window opens for modifying profile settings and then either loading those settings as a profile on the TKE workstation crypto adapter or saving those settings in a profile definition file.

If the profile or profile definition file is for a passphrase profile, a window is displayed for making changes to a passphrase profile. In particular, fields are presented for entering the passphrase and passphrase expiration date.

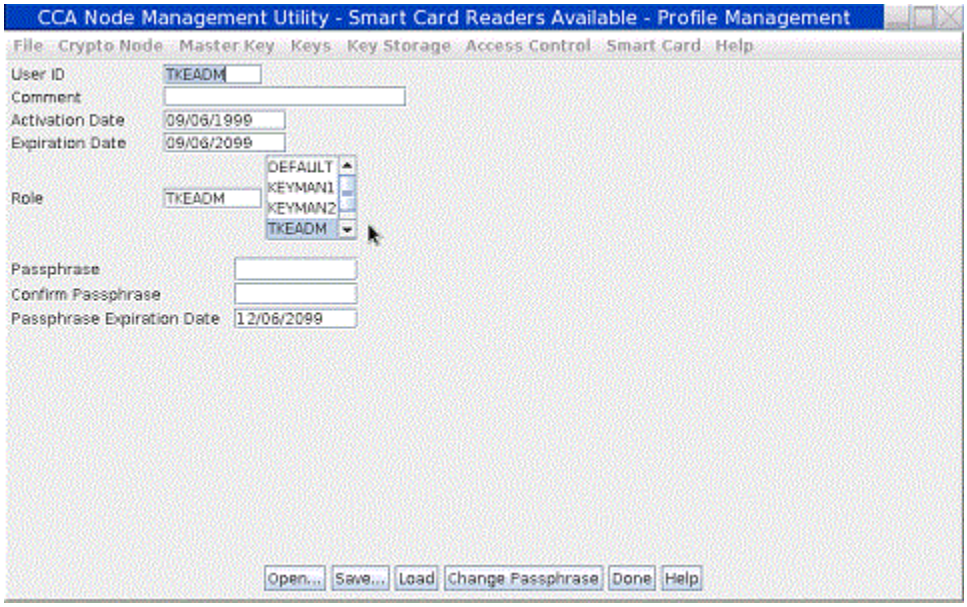


Figure 199. Profile Management window for passphrase profiles

To make changes to a passphrase profile or a passphrase profile definition file:

1. Edit the text entry fields and use the window's controls to modify the displayed attributes as desired.
   - The **User ID** field shows the name of the profile. It is a case-sensitive character string with a maximum length of 8 characters.
   - The **Comment** field shows an optional character string with a maximum length of 20 characters.
   - The **Activation Date** field determines the first date the user can log on. This field defaults to the current date.
   - The **Expiration Date** field determines the last date the user can log on. When a new profile is being created, the date will default to the current date. Remember to adjust this date.
   - The **Role** field shows the name of the role that defines the permissions granted to the profile. Select a role from the list.

     Note: Individual profiles that are intended to be used only as group members should be given a role that has very few or no permitted operations (such as the DEFAULT role). This is done to ensure the profile has very little authority outside the group.
   - The **Passphrase** field contains the case-sensitive character string that the user must enter to log on to the TKE workstation crypto adapter. The passphrase must:
     - Have a length between 8 and 64 characters.
     - Contain at least 2 letters and at least 2 numbers.
     - Must not contain the user ID.
   - The **Confirm Passphrase** field must contain the same case-sensitive character string as the **Passphrase** field.
   - The **Passphrase Expiration Date** contains the expiration date for the passphrase. When a new profile is created, the date defaults to three months after the current date. Remember to adjust this date.

2. Load the settings as a profile on the TKE workstation crypto adapter, save the settings in the profile definition file, or change just the passphrase for the profile.

   Note: If you want to save the settings as a profile definition file, and also either change the passphrase for the profile or load the profile on the TKE workstation crypto adapter, save the profile definition file first. When you change the passphrase for a profile or load a profile, the CCA Node Management Utility's Profile Management window closes. If you try to change the passphrase or load the profile first, the window will close before you have a chance to save the profile definition file.

   - To save a profile definition file:
     a. Click the **Save** push button.

        A standard save file dialog is displayed. We recommend you use the naming convention *profile_name*.pro.

     b. If you do not want to also change the passphrase or load the profile on the TKE workstation crypto adapter, you can click the **Done** push button. Clicking the **Done** push button closes the window.
   - To load the profile on the TKE workstation crypto adapter:
     a. Click the **Load** push button.

        The profile is loaded on the TKE workstation crypto adapter, and the window is closed.
   - To change the passphrase for the profile:
     a. Click the **Change Passphrase** push button. The passphrase profile on the TKE workstation crypto adapter is updated with the new passphrase and passphrase expiration date. No other changes will be make to the passphrase profile.

Notes:

1. You can click the **Done** push button to close this window at any time. Any changes you made that were not loaded or saved prior to pressing the **Done** push button will be lost.
2. You can click the **Open** push button at any time to select a new profile definition file to edit. Any changes you made that were not loaded or saved will be lost when the window is populated with the attributes of the new profile definition file.

Making changes to a smartcard profile or smartcard profile definition file

From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter. When you click the **New**, **Edit**, or **Open** push button on the initial window, a secondary window opens for modifying profile settings and then either loading those settings as a profile on the TKE workstation crypto adapter or saving those settings in a profile definition file.

If the profile or profile definition file is for a smartcard profile, a window is displayed for making changes to a smart card profile. In particular, the public modulus and key identifier for the TKE workstation crypto adapter logon key is displayed.

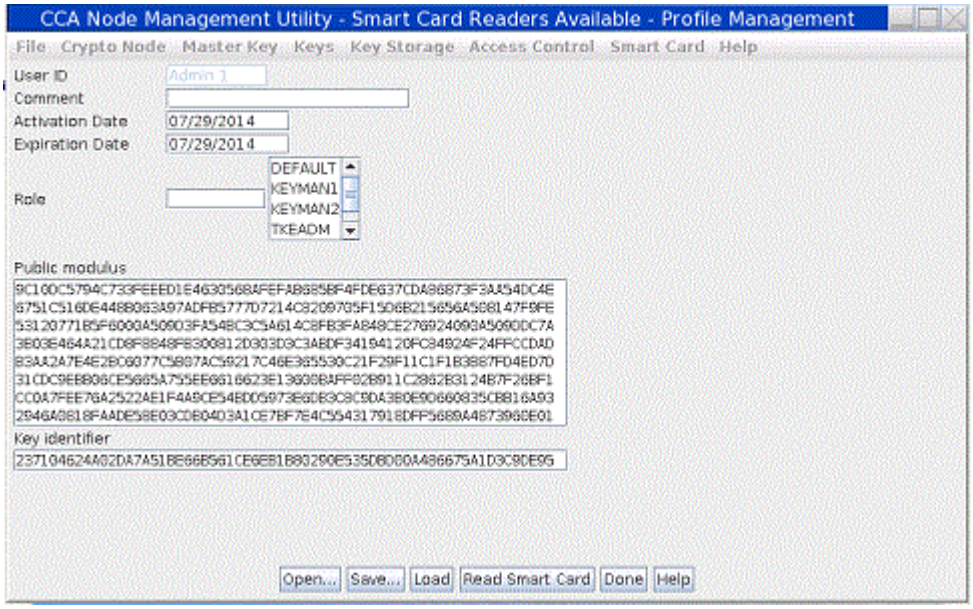


Figure 200. Profile Management window for smart card profiles

To make changes to a smartcard profile or a smartcard profile definition file:

1. Edit the text entry fields and use the window's controls to modify the displayed attributes as desired. Some of the fields are informational, and cannot be edited.
   - The **User ID** field shows the name of the profile. The name of the profile is obtained from the profile, the smart card, or a profile definition file. This value cannot my changed.
   - The **Comment** field shows an optional character string with a maximum length of 20 characters.
   - The **Activation Date** field determines the first date the user can log on. This field defaults to the current date.
   - The **Expiration Date** field determines the last date the user can log on. When a new profile is being created, the date will default to the current date. Remember to adjust this date.
   - The **Role** field shows the name of the role that defines the permissions granted to the profile. Select a role from the list.

     Note: Individual profiles that are intended to be used only as group members should be given a role that has very few or no permitted operations (such as the DEFAULT role). This is done to ensure the profile has very little authority outside the group.
   - The **Public Modulus** fields shows the public modulus of the TKE workstation crypto adapter logon key. This value is read from the profile, profile definition file, or smart card. This value cannot be changed.
   - The **Key Identifier** field shows a SHA-256 hash of the DER-encoded public modulus and public exponent of the TKE workstation crypto adapter logon key for this profile. This field cannot be changed.
2. Load the settings as a profile on the TKE workstation crypto adapter or save the settings in the profile definition file.

   Note: If you want to both save the settings as a profile definition file, and also load the profile on the TKE workstation crypto adapter, save the profile definition file first. When you load a profile, the CCA Node Management Utility's Profile Management window closes. If you try to save load the profile first, the window will close before you have a chance to save the profile definition file.
   - To save a profile definition file:
     a. Click the **Save** push button.

A standard save file dialog is displayed. We recommend you use the naming convention *profile_name*.pro.

b. If you do not want to also load the profile on the TKE workstation crypto adapter, you can click the **Done** push button. Clicking the **Done** push button closes the window.

- To load the profile on the TKE workstation crypto adapter:

a. Click either the **Load** or **Replace** push button. (If, from the initial Profile Management window, you selected the **New** push button to create a new profile, or the **Open** push button to open a profile definition file, this secondary window will contain a **Load** push button. If, from the initial Profile Management window, you selected the **Edit** push button to edit a profile already loaded on the TKE workstation crypto adapter, this secondary window will contain a **Replace** push button.)

The profile is loaded on the TKE workstation crypto adapter, and the window is closed.

If the profile is already loaded on the TKE workstation crypto adapter, and you click the **Load** push button, the load operation will fail. Go back to the initial Profile Management window and select the **Edit** push button to edit the profile. This window will then contain a **Replace** push button for replacing the already-loaded profile.

Notes:

1. You can click the **Done** push button to close this window at any time. Any changes you made that were not loaded or saved prior to pressing the **Done** push button will be lost.
2. You can click the **Open** push button at any time to select a new profile definition file to edit. Any changes you made that were not loaded or saved will be lost when the window is populated with the attributes of the new profile definition file.

Making changes to a group profile or group profile definition file

From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter. When you click the **New**, **Edit**, or **Open** push button on the initial window, a secondary window opens for modifying profile settings and then either loading those settings as a profile on the TKE workstation crypto adapter or saving those settings in a profile definition file.

If the profile or profile definition file is for a group profile, a window is displayed for making changes to a group profile. In particular, group member information is displayed.

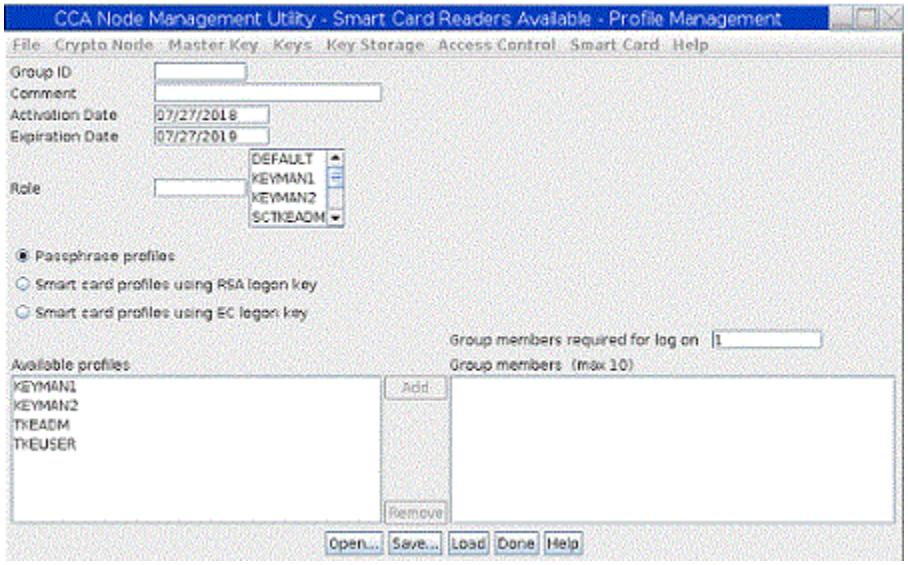


Figure 201. Profile Management window for group profiles

To make changes to a group profile or a group profile definition file:

1. Edit the text entry fields and use the window's controls to modify the displayed attributes as desired.
   - The **Group ID** field shows the name of the profile. It is a case-sensitive character string with a maximum length of 8 characters.
   - The **Comment** field shows an optional character string with a maximum length of 20 characters.
   - The **Activation Date** field determines the first date the user can log on. This field defaults to the current date.
   - The **Expiration Date** field determines the last date the user can log on. When a new profile is being created, the date will default to the current date. Remember to adjust this date.
   - The **Role** field shows the name of the role that defines the permissions granted to the profile. Select a role from the list.

     Note: The role of the group will override the roles of the individual users.
   - The **Passphrase profiles** and two **Smart card profiles** radio buttons determine the type or profiles that can be members of the group. All the profiles in a group must use the same authentication method. That is, all the profiles in the group must use passphrase logon, smart cards using RSA logon keys, or smart cards using EC logon keys.
   - The **Group members required for log on:** field shows the number of users that must sign on to complete the group sign on. The value must be between 1 and the number of profiles in the group. A group cannot contain more than 10 profiles.
   - The **Available profiles** area lists the profiles the selected type (passphrase profiles or smart card profiles) that are not currently members of the group, while the **Group members** area lists the profiles that are members of the group.
     - To add a profile to the group:
       a. In the list of **Available profiles**, click on the name of the profile you want to add to the group.

          The profile name is reverse highlighted (white on black) to show that it is selected.
       b. Click the **Add** push button.

          The profile name appears in the **Group members** list to show that it is now a member of the group.
     - To remove a profile from the group:
       a. In the list of **Group members**, click on the name of the profile you want to remove from the group.

          The profile name is reverse highlighted (white on black) to show that it is selected.
       b. Click the **Remove** push button.

          The profile name is removed from the **Group Members** list to show that it is no longer a member of the group.
2. Load the settings as a profile on the TKE workstation crypto adapter or save the settings in the profile definition file.

   Note: If you want to both save the settings as a profile definition file, and also load the profile on the TKE workstation crypto adapter, save the profile definition file first. When you load a profile, the CCA Node Management Utility's Profile Management window closes. If you try to save load the profile first, the window will close before you have a chance to save the profile definition file.
   - To save a profile definition file:
     a. Click the **Save** push button.

        A standard save file dialog is displayed. We recommend you use the naming convention *profile_name*.pro.
     b. If you do not want to also load the profile on the TKE workstation crypto adapter, you can click the **Done** push button. Clicking the **Done** push button closes the window.
   - To load the profile on the TKE workstation crypto adapter:

a. Click either the **Load** or **Replace** push button. (If, from the initial Profile Management window, you selected the **New** push button to create a new profile, or the **Open** push button to open a profile definition file, this secondary window will contain a **Load** push button. If, from the initial Profile Management window, you selected the **Edit** push button to edit a profile already loaded on the TKE workstation crypto adapter, this secondary window will contain a **Replace** push button.)

   The profile is loaded on the TKE workstation crypto adapter, and the window is closed.

   If the profile is already loaded on the TKE workstation crypto adapter, and you click the **Load** push button, the load operation will fail. Go back to the initial Profile Management window and select the **Edit** push button to edit the profile. This window will then contain a **Replace** push button for replacing the already-loaded profile.

Notes:

1. You can click the **Done** push button to close this window at any time. Any changes you made that were not loaded or saved prior to pressing the **Done** push button will be lost.
2. You can click the **Open** push button at any time to select a new profile definition file to edit. Any changes you made that were not loaded or saved will be lost when the window is populated with the attributes of the new profile definition file.

Managing roles

When you initialize the TKE workstation crypto adapter, a set of system-supplied roles are loaded on the adapter. You can use the CCA Node Management Utility's Role Management window to modify the system-supplied roles on the adapter, or to define and load your own roles on the adapter.

Each of the system-supplied roles is created from a corresponding system-supplied role definition file that is stored on the TKE workstation's hard drive. You can also define your own role definition files. The role definition files you create can be stored on the TKE workstations's hard drive or on removable media. A role definition file describes the attributes of a role, and are important for migration between versions of TKE and for recovery. We recommend that you:

- Create role definition files for any new roles you create. This will help during migration to a new TKE workstation or for recovery of the TKE workstation crypto adapter data. If you later modify the role loaded on the TKE workstation crypto adapter, you should also modify the corresponding role definition file.

  When creating role definition files, we recommend using the naming convention *role-name*.rol.
- Do not edit the system-supplied role definition files. By leaving the system-supplied role definition files unedited, you preserve the ability to restore system-supplied roles to their default settings, including the default passwords. If you edit the system-supplied roles, we recommend you save the modified settings to a new role definition file instead of editing the original role definition file.

To open the CCA Node Management Utility's Role Management window:

1. Go to the CCA Node Management Utility main window.
2. From the **Access Control** pull-down menu, select **Roles**.

The CCA Node Management Utility's Role Management window is displayed. Initially, this window lists the roles currently loaded on the TKE workstation crypto adapter.

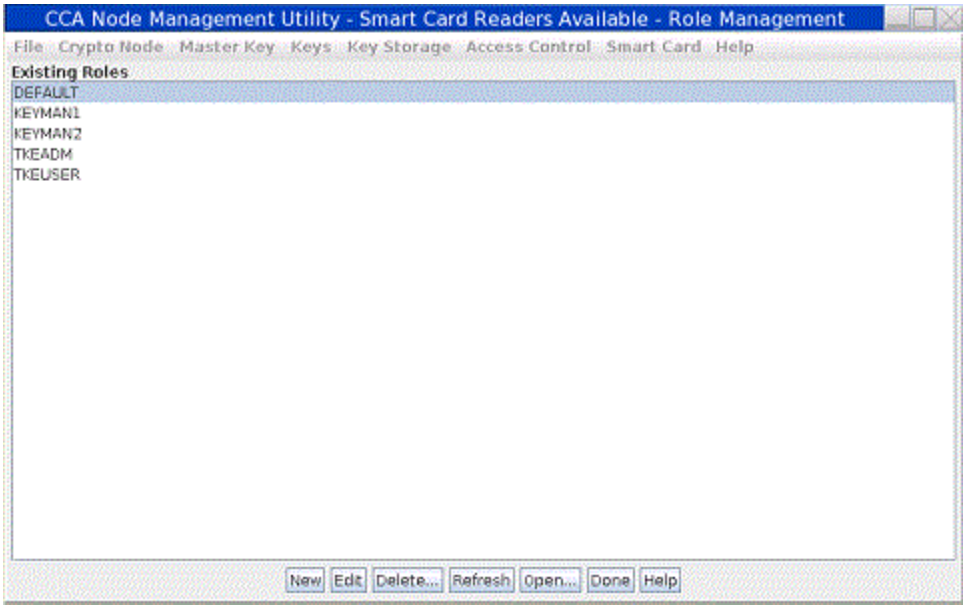


Figure 202. Role Management window listing the roles on the TKE workstation crypto adapter

You can use the Role Management window to manage the roles on the TKE workstation crypto adapter and to manage any associated role definition files. You can use:

- **New** to create a new role.
- **Edit** to edit a role on the TKE workstation crypto adapter.
- **Delete** to delete a role. To do this, you first select the role in the window and then click **Delete**.
- **Refresh** to refresh the list in the window.
- **Open** to open a role definition file.
- **Done** to close the window.

Clicking **New**, **Edit**, or **Open** all eventually open a window for modifying role settings and then either loading those settings as a role on the TKE workstation crypto adapter or saving those settings in a role definition file. It helps to think of **New**, **Edit**, and **Open** as different ways of populating that window with initial values for editing.

- Clicking **New** opens the window and populates it with default attributes for a new role.
- Clicking **Edit** opens the window and populates it with the attributes of the selected role.
- Clicking **Open** opens the window and populates it with the attributes of the selected role definition file.

From that point, however, you'll be able to modify any of the attributes (including the name) and load it as a role on the adapter or save it as a role definition file on the TKE workstation's hard drive or on removable media.

If you are creating a new role or role definition file, for example, you could open either an existing role or role definition file that has settings similar to the ones you want for the new role or role definition file. You would then only have to modify the name and any settings you want changed before loading it as a new role or saving it as a new role definition file.

Creating a new role or role definition

Recommendation: Beginning with TKE 8.1, creating role and profile definition files is discouraged. The new recommended method for saving and loading user defined roles and profiles is:

1. Create your set of user defined roles and profiles onto your TKE local adapter. Do not use the save button to create the .rol and .prf files.
2. After your set of user defined roles and profiles have been created, use the **Save User Roles and Profiles** feature to save the definitions in the TKESavedRoles.dat and TKESavedProfiles.dat files.

3. At a later time, use the **Load User Roles and Profiles** feature to load the roles and profiles onto a TKE local crypto adapter from the TKESavedRoles.dat and TKESavedProfiles.dat files. This is only done as needed.

From the CCA Node Management Utility main window, you can select **Access Control –> Roles** off the menu bar to display the CCA Node Management Utility's Role Management window. Initially, this window lists the roles currently loaded on the TKE workstation crypto adapter.

To create a new role or role definition file, it does not matter if a role name is highlighted in the CCA Node Role Management window, or if the list is empty. To create a new role or role definition file:

1. From the CCA Node Management Utility's Role Management window, click on the **New** push button.

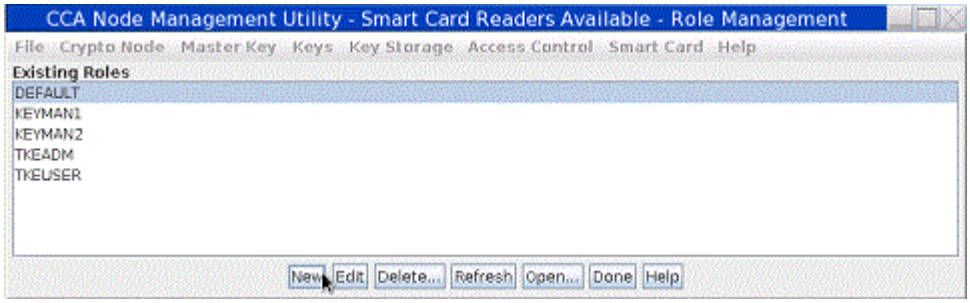


Figure 203. From the CCA Node Management Utility's Role Management window, click on the New push button

A secondary window opens for modifying role settings and then either loading those settings as a role on the TKE workstation crypto adapter or saving those settings in a role definition file. Because you selected the **New** push button, this secondary window is populated with the default attributes and settings for a new role.

Editing a role on the TKE workstation crypto adapter

From the CCA Node Management Utility main window, you can select **Access Control –> Roles** off the menu bar to display the CCA Node Management Utility's Role Management window. Initially, this window lists the roles currently loaded on the TKE workstation crypto adapter.

To edit a role that is currently loaded on the TKE workstation crypto adapter:

1. In the list of roles, click on the name of the role you want to edit.

   The role name is reverse highlighted (white on black) to show that it is selected.

2. Click on the **Edit** push button.

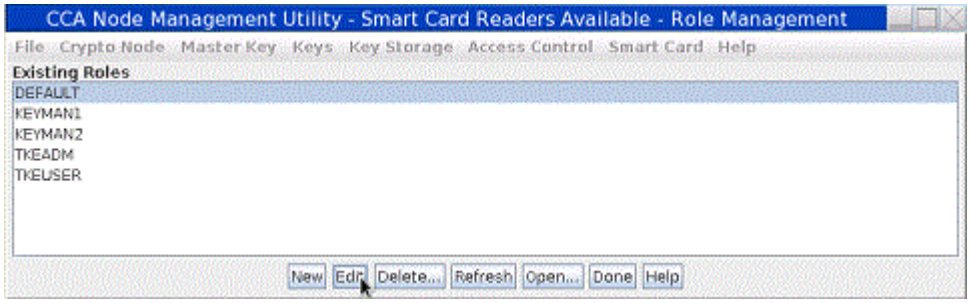


Figure 204. Select role and click Edit

A secondary window opens for modifying role settings and then either loading those settings as a role on the TKE workstation crypto adapter or saving those settings in a role definition file. This secondary window is populated with the attributes of the selected role.

Opening a role definition file

Role definition files have all the attributes and settings necessary to create or update a role on the TKE workstation crypto adapter. Unlike a role, a role definition file is not loaded onto the TKE workstation crypto adapter, but is instead stored on the TKE workstation's hard drive or on removable media. Keep in mind that:

- You can have a role definition file for a role that is not currently loaded on the TKE workstation crypto adapter.
- It is possible that the settings in a role definition file do not currently match the settings of the actual role on the TKE workstation crypto adapter.

From the CCA Node Management Utility main window, you can select **Access Control –> Roles** off the menu bar to display the CCA Node Management Utility's Role Management window. Initially, this window lists the roles currently loaded on the TKE workstation crypto adapter.

To open a role definition file, it does not matter if a role name is highlighted in the CCA Node Role Management window, or if the list is empty. This is because you are not opening a role on the TKE workstation crypto adapter. Instead, you are opening a file on the TKE workstation's hard drive or on removable media.

To open a role definition file:

1. From the CCA Node Management Utility's Role Management window, click on the **Open** push button.

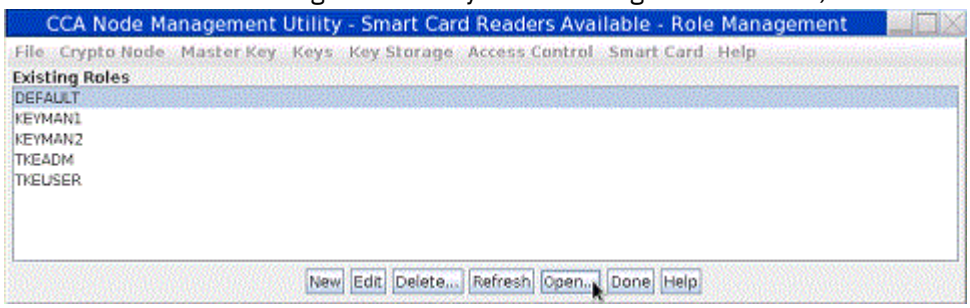


Figure 205. From the CCA Node Management Utility's Role Management window, click on the Open push button

The **Specify file to open** dialog is displayed.

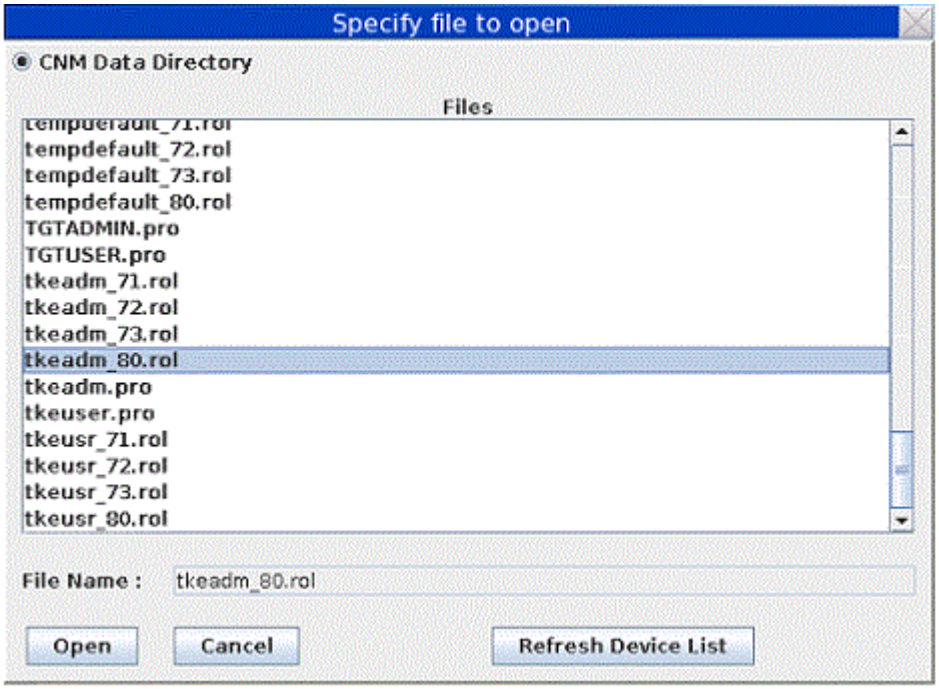


Figure 206. Specify file to open dialog

2. In the **Specify file to open** dialog:

   a. In the list of files, click on the name of the role definition file you want to open. Role definition files typically follow the naming convention *role_name*.rol.

      The role name is reverse highlighted (white on black) to show that it is selected.

   b. Click the **Open** push button.

      A secondary window opens for modifying role settings and then either loading those settings as a role on the TKE workstation crypto adapter or saving those settings in a role definition file. This secondary window is populated with the attributes of the selected role definition file.

Making changes to a role or role definition file

From the CCA Node Management Utility main window, you can select **Access Control –> Roles** off the menu bar to display the CCA Node Management Utility's Role Management window. Initially, this window lists the roles currently loaded on the TKE workstation crypto adapter. When you click the **New**, **Edit**, or **Open** push button on the initial window, a secondary window opens for modifying role settings and then either loading those settings as a role on the TKE workstation crypto adapter or saving those settings in a role definition file.

- The **New** push button will open the window and populate it with default attributes for a new role.
- The **Edit** push button will open the window and populate it with the attributes of the selected role.
- The **Open** push button will open the window and populate it with the attributes of the selected role definition file.

Regardless of how the window was opened and populated with attributes, you can use the window to modify any of the attributes. By changing the Role ID, in fact, you can create a new role or role definition file. Once you have modified the attributes as desired, you can load the role on the TKE workstation crytpo adapter, or save the settings as a role definition file on the TKE workstations's hard drive or on removable media. When making changes to a role you have created, in fact, you will likely want to also create or modify an associated role definition file for migration or recovery purposes.

Note: Do not edit the system-supplied role definition files. By leaving the system-supplied role definition files unedited, you preserve the ability to restore system-supplied profiles to their default settings,

including the default passwords. If you edit the system-supplied roles, we recommend you save the modified settings to a new role definition file instead of editing the original role definition file.

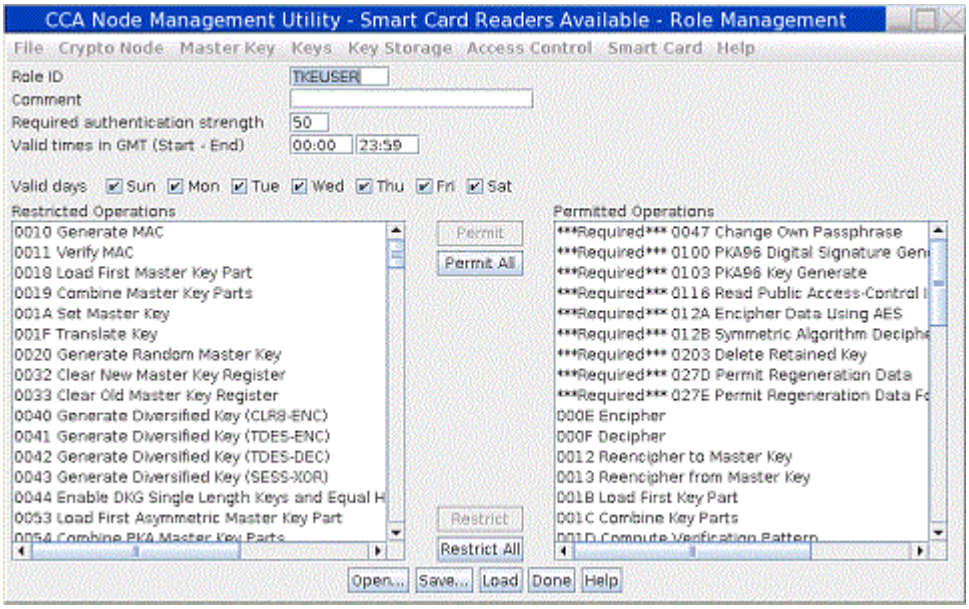


Figure 207. Role Management window modifying role attributes

To make changes to a role or role definition file:

1. Edit the text entry fields and use the window's controls to modify the displayed attributes as desired.
   - The **Role ID** field shows the name of the role. It is a case-sensitive character string with a maximum length of 8 characters.
   - The **Required authentication strength** field shows the level of authentication required to log on to user profiles with this role. Passphrase profiles created on the TKE have passphrases which have strength of 50. For a new role, this field defaults to 0.
   - **Valid times in GMT (Start – End)** fields show the range of hours during the valid days that the user is allowed to log on. For a new role, these fields default to the entire day.
   - The **Valid days** check boxes identify the days of the week that the user is allowed to log on. By default, none of the days are selected for a new role.
   - The **Restricted operations** area list of functions the role is not allowed to use, while the **Permitted operations** area lists the functions the role is allowed to use.
     - To permit the role to use a particular function:
       a. In the list of **Restricted Operations**, click on the name of the function.

          The function name is reverse highlighted (white on black) to show that it is selected.

       b. Click the **Permit** push button.

          The function name appears in the **Permitted Operations** list to show the role can use that function.
     - To restrict the role from using a particular function:
       a. In the list of **Permitted Operations**, click on the name of the function.

          The function name is reverse highlighted (white on black) to show that it is selected.

       b. Click the **Restrict** push button.

          The function name appears in the **Restricted Operations** list to show the role is not allowed to use that function.
     - To permit the role to use all functions, click on the **Permit All** push button.

– To restrict the role from using any function, click on the **Restict All** push button.

2. Load the settings as a role on the TKE workstation crypto adapter or save the settings in a role definition file.

   Note: If you want to both save the settings as a role definition file, and also load the role on the TKE workstation crypto adapter, save the role definition file first. When you load a role, the CCA Node Management Utility's Role Management window closes. If you try to save load the role first, the window will close before you have a chance to save the role definition file.

   - To save a role definition file:

     a. Click the **Save** push button.

        A standard save file dialog is displayed. We recommend you use the naming convention *role_name*.rol.

     b. If you do not want to also load the role on the TKE workstation crypto adapter, you can click the **Done** push button. Clicking the **Done** push button closes the window.

   - To load the role on the TKE workstation crypto adapter:

     a. Click the **Load** push button.

        The role is loaded on the TKE workstation crypto adapter, and the window is closed.

Notes:

1. You can click the **Done** push button to close this window at any time. Any changes you made that were not loaded or saved prior to pressing the **Done** push button will be lost.
2. You can click the **Open** push button at any time to select a new role definition file to edit. Any changes you made that were not loaded or saved will be lost when the window is populated with the attributes of the new role definition file.

Save user roles and profiles

The 'Save user roles and profiles' function saves all your user defined roles and profiles that are on the TKE local crypto adapter using a single operation. When you select this feature, the TKE workstation determines if you have created any user-defined roles and profiles onto the TKE local crypto adapter. If you have any user defined roles, they are saved in the file **TKESavedRoles.dat.** If you have any user defined profiles, they are saved in the file **TKESavedProfiles.dat.** These files are used with the corresponding Load User Roles and Profiles feature of the CNM utility.

Note: The passphrase of a passphrase profile is not saved.

The save and load user roles and profile features work together. This is the quickest and easiest way to back up your user defined roles and profiles. The user defined roles and profiles can be restored on the same TKE workstation local crypto adapter at any time. In addition, the **TKESavedRoles.dat** and **TKESavedProfiles.dat** files can be moved to other TKE workstations. Once the files are on the other TKE workstation, the Load User Roles and Profiles option can be used to apply the user defined roles and profiles to the new or back up TKE’s local crypto adapter.

Load user roles and profiles

The 'Load user roles and profiles' function looks for the files **TKESavedRoles.dat** and **TKESavedRoles.dat** on the TKE workstation. If it finds the file **TKESavedRoles.dat**, it loads the user defined roles onto the TKE local crypto adapter. If it finds the file **TKESavedProfiles.dat**, it loads the user defined profiles onto the TKE local crypto adapter. If a role or profile already exists, it is replaced.

Note: The passphrase of a passphrase profile is not saved. Therefore, when a passphrase profile is restored, you must enter a new passphrase for the profile.

The save and load user roles and profile features work together. This is the quickest and easiest way to back up your user defined roles and profiles. The user defined roles and profiles can be restored on the same TKE workstation local crypto adapter at any time. In addition, the **TKESavedRoles.dat** and

TKESavedProfiles.dat files can be moved to other TKE workstations. Once the files are on the other TKE workstation, the Load User Roles and Profiles option can be used to apply the user defined roles and profiles to the new or back up TKE's local crypto adapter.

Check TKE crypto adapter group profiles

When you initialize the TKE local crypto adapter using the TKE's Crypto Adapter Initialization application, the role TKEGRPMB is created. The TKEGRPMB role has access only to the required ACPs and does not provide access to any TKE capabilities. The TKEGRPMB role should be assigned to members of group profiles, which prevents each group member from having access to anything outside the group.

The 'Check TKE crypto adapter group profiles' function examines the role of every individual profile that is a member of a TKE local crypto adapter group profile. If the individual does not have the role TKEGRPMB, a change profile command is issued to change the role of the profile to TKEGRPMB. If the individual profile that is being changed is a passphrase profile, you have to set a new passphrase for the profile.

Load TKEGRPMB role

The 'Load TKEGRPMB role' function verifies that the TKEGRPMB role is on the TKE Local crypto adapter and that it does not have access that it should not have. If the TKE workstation determines that someone has added access to the TKEGRPMB role or that the TKEGRPMB role does not exist, a command is issued to create or change the TKEGRPMB role. If the role exists with the correct ACPs, a message lets you know that the TKEGRPMB role is correct.

TKE Workstation Logon Profile Wizard

The TKE Workstation Logon Profile Wizard is one of six TKE security policy wizards that work together to implement a comprehensive set of security policies for managing access to the TKE workstation and managing host crypto modules and their domains. The TKE Workstation Logon Profile Wizard implements a security policy for accessing your TKE workstation.

The TKE Workstation Logon Profile Wizard allows you to do three things:

1. Create individual smart card TKE local crypto adapter profiles, which you need to logon to the TKE local crypto adapter so that you can manage the TKE workstation.
2. Create individual smart card TKE local crypto adapter profiles, which you need to logon to the TKE local crypto adapter so that you can manage Host Crypto Modules.
3. Place individual smart card TKE local crypto adapter profiles into TKE local crypto adapter group profiles.

Every time the Logon Profile Wizard is run, it attempts to remove excess authority from the system-supplied DEFAULT role if the proper profiles and roles were created and installed on the crypto adapter. If it cannot remove the excess authority, it warns the user to provide instructions on how to proceed further.

Note: The TKE Workstation Logon Profile Wizard uses smart cards that you created using the TKE Smart Card Wizard, found in the Smart Card Utility Program.

Master Key menu

The Master Key pull-down menu has menu items for the following key stores you can manage:

- DES/PKA Master Key
- AES Master Key

These menu items have additional items for the following tasks you can perform:

- Auto set...
- Create Random Master Key... (Only available for DES/PKA master key)
- Clear New ...
- Parts

- Smart Card Parts (TKE must be enabled for use with smart cards)
- Set...
- Verify

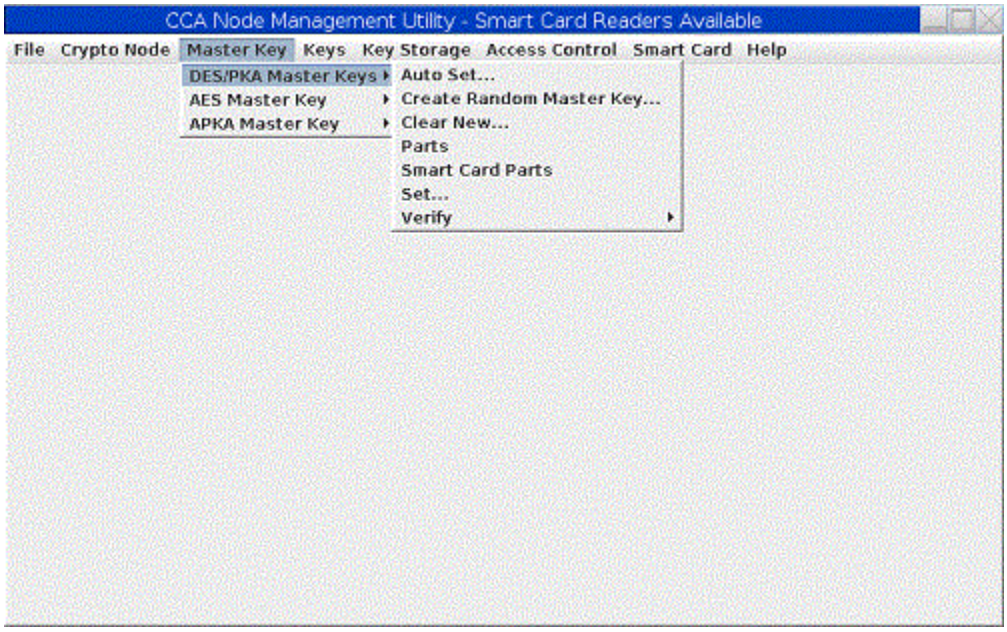


Figure 208. CNM main window — Master Key pull-down menu

The master keys are stored in the tamper-resistant TKE workstation crypto adapter.

The DES/PKA master keys are used to encipher other keys. Each master key is a 24 byte DES key (192 bits). However, because DES keys contain 1 parity bit per byte, it has an effective length of 168 bits of "real" key material. Random master keys are generated and set when the TKE workstation crypto adapter is initialized. If a master key of unknown value is lost, you cannot recover the keys enciphered under it. We recommend that you load a new master key by entering clear key parts or by loading key parts that are stored on smart cards.

The AES master key is used to encipher other keys.

Each master key on the TKE workstation crypto adapter has three registers:

- **Current Master Key Register.** The active master key is stored in the current master key register.
- **Old Master Key Register.** The previous master key is stored in the old master key register.
- **New Master Key Register.** The new master key register is an interim location used to combine master key parts to form a new master key

Auto Set and Create Random Master Key

The Auto Set and Create Random Master Key pull-down menu options use different methods to generate and set new master key values.

The Create Random Master Key option is only available for DES/PKA master keys pull-down.

Note: If a master key of unknown value is lost, you cannot recover the keys enciphered under it. We recommend that you load a new master key by entering clear key parts or by entering key parts generated to TKE smart cards.

Clear new

The Clear New pull-down menu option allows you to clear the new master key registers. If a new master key register has a value in it, you must clear it before you can do load a first key part. To clear the new master key register:

1. From the Master Key pull-down menu, select **Clear New...**

   A confirmation dialog displays, prompting you to verify that you want to clear the new master key register.

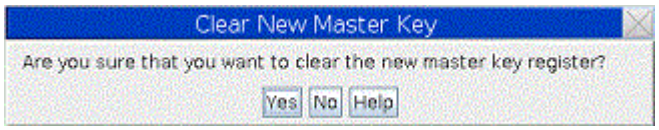


   Figure 209. Clear New Master Key Register — confirm clearing

2. If you are certain you want to clear the new master key register, click the confirmation dialog's **Yes** push button.

   An information box informs you that the new master key register is cleared. Select **OK** to finish.

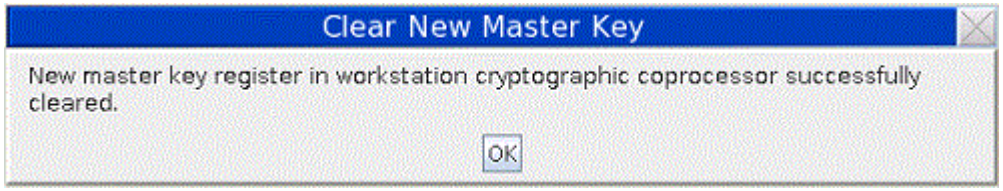


   Figure 210. Clear New Master Key Register — register cleared

Parts — Loading a new master key from clear key parts

To load new master key parts into the TKE workstation crypto adapter, load the first key part, any middle key parts, and the last key part into the new master key register, and then load the new master key. The first and last key parts are required. Middle key parts are optional; you can load multiple middle key parts.

1. From the **Master Key –> DES/PKA Master Key** or **Master Key –> AES Master Key** pull-down menu items, select the **Parts** menu option.

   The Load Master Key panel is displayed.

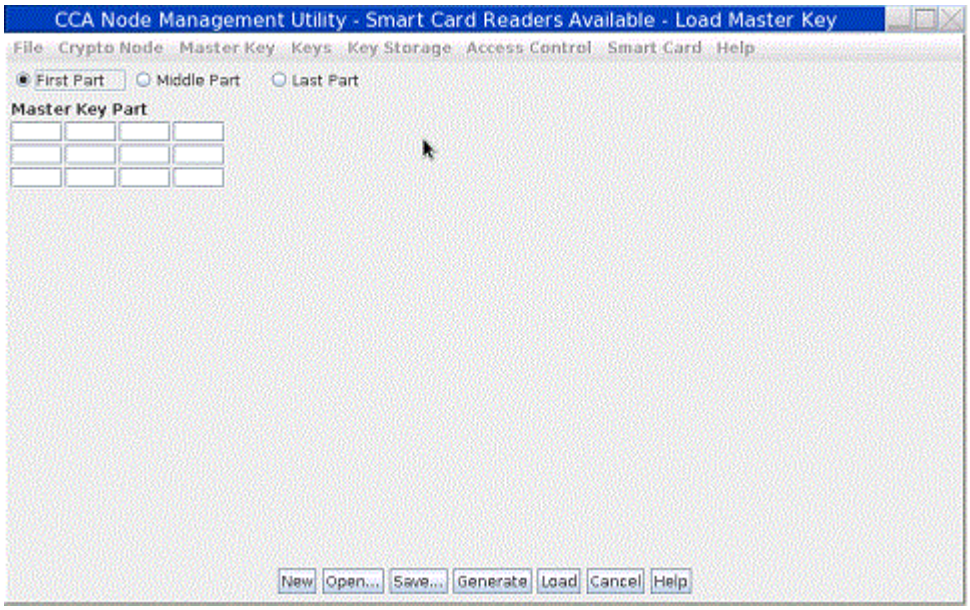


   Figure 211. Load Master Key from Clear Parts

2. Select the radio button corresponding to the key part you are loading (First Part, Middle Part or Last Part).
3. Enter the clear key part by doing one of the following:

   - Select **New** to clear data entered in error.

- Select **Open**... to retrieve key parts saved to disk.
- Select **Generate** to have the TKE workstation crypto adapter randomly generate a key part.
- Manually enter a key value into the "Master Key Part" fields. Each field accepts four hexadecimal digits.

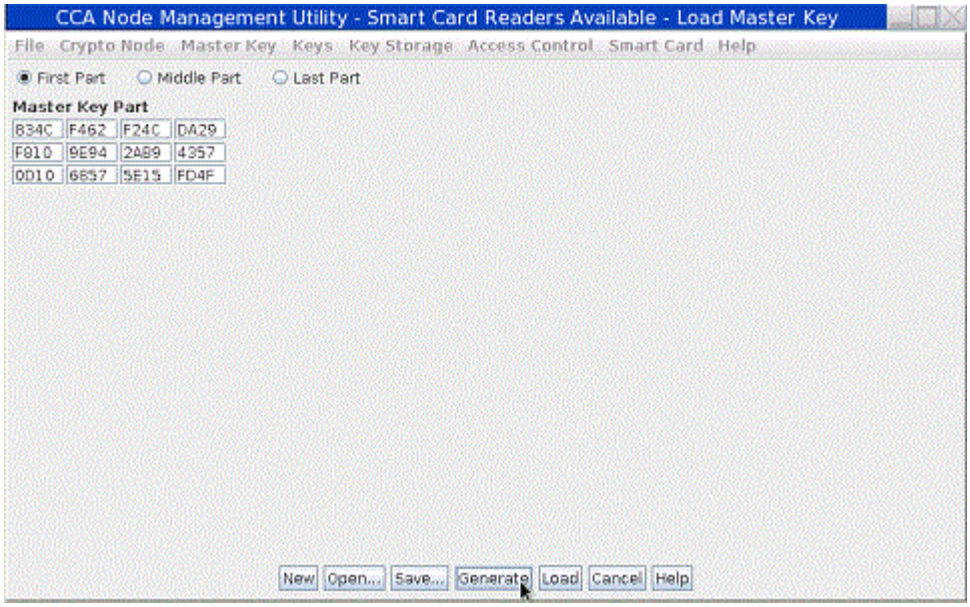


Figure 212. Load Master Key from Clear Parts — key part randomly generated

4. Select **Load** to load the key part into the new master key register, and select **Save** to save the key part to disk.

   Attention : Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages might be generated on the TKE workstation.

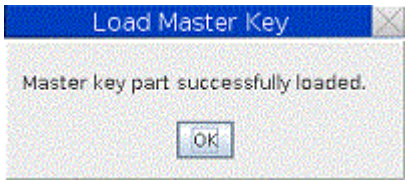


Figure 213. Load Master Key from Clear Parts — key part successfully loaded

   Note: Key parts saved to disk are not enciphered.

5. Repeat the preceding steps to load the remaining key parts into the new master key register.
6. From the **Master Key** pull-down menu, select **Set**... This will do the following:
   a. Transfer the key in the current master key register to the old master key register and delete the former old master key.
   b. Transfer the key in the new master key register to the current master key register.

After setting a new master key, reencipher the keys currently in key storage. (Refer to “Reenciphering key storage” on page 279.)

We recommend a dual control security policy. With a dual control security policy, the first and last key parts are loaded by different people.

Smart card parts — generating master key parts to a smart card

Steps for generating master key parts and saving them on a TKE or EP11 smart card are as follows:

1. From the **Master Key** pull-down menu, select **DES/PKA Master Keys** or **AES Master Key** and then select **Smart Card Parts**. You will be prompted to insert a TKE or EP11 smart card into smart card reader 2. A Smart Card Master Key Parts panel is displayed. Any TKE workstation crypto adapter master key parts stored on the smart card are listed in the container. The smart card description is displayed. Ensure this is the correct smart card you want to save the key part on.

   Note: Make sure that the TKE workstation crypto adapter and the smart card are in the same zone. To determine the zone for a smart card, use CNM, see "Display smart card details" on page 282 or SCUP "Display smart card information" on page 294. To determine the zone of the TKE workstation crypto adapter, use SCUP "View current zone for the crypto adapter" on page 310. To use SCUP, you must first exit from CNM.

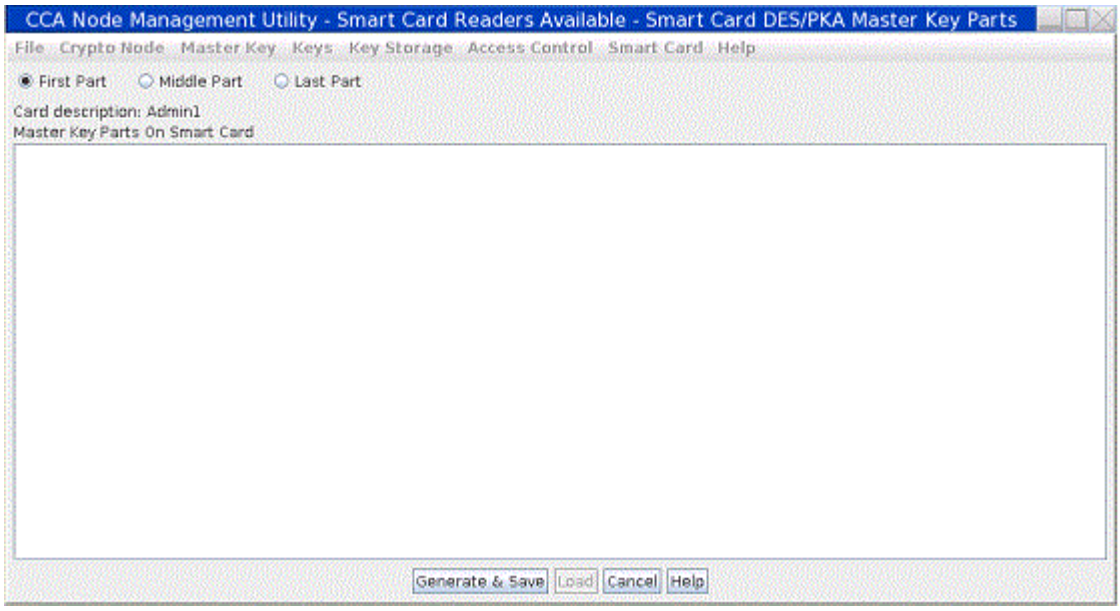


Figure 214. Smart Card Master Key Parts panel

2. Select the radio button for the key part you are generating (First Part, Middle Part, or Last Part).
3. Press the **Generate & Save** push button. You will be prompted for an optional description for the key part you are generating. A maximum of 32 characters may be specified.

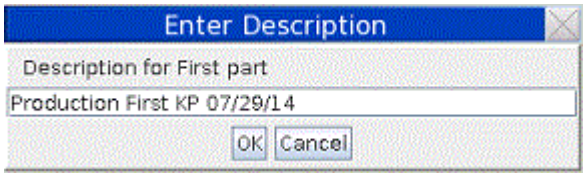


Figure 215. Smart Card Master Key Parts panel — key part description prompt

4. You will be prompted for the PIN of the smart card inserted in smart card reader 2.

A secure session is established between the TKE workstation crypto adapter and the smart card. The key part is generated to the smart card. The key part list is refreshed.

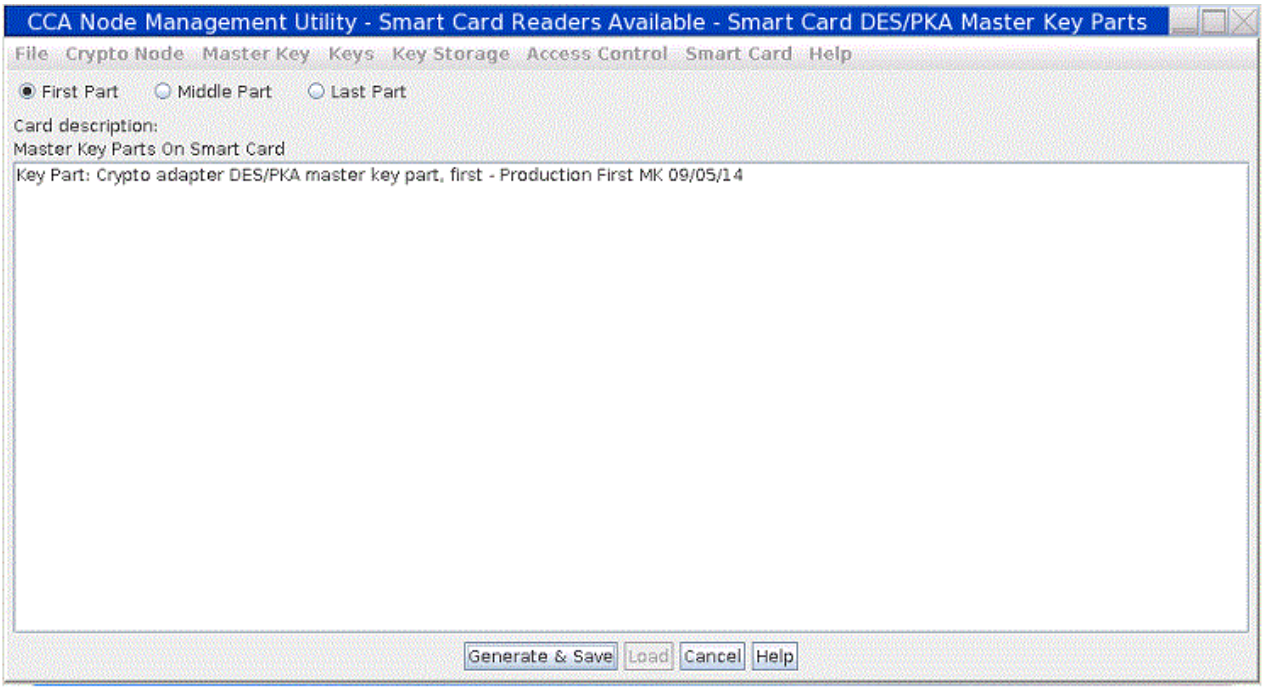


Figure 216. Smart Card Master Key Parts panel — key part generated

Note: The key parts in the list are prefixed as follows:

- Key Part: Crypto Adapter master key part, first - <optional description follows>
- Key Part: Crypto Adapter master key part, middle - <optional description follows>
- Key Part: Crypto Adapter master key part, last - <optional description follows>

A First and Last key part is required. Middle key parts are optional. We recommend a dual control security policy. With a dual control security policy, the first and last key parts are generated to different smart cards so that no one person has access to the complete key. At this point, we recommend that you insert a different smart card in smart card reader 2 to generate middle or last key parts. Repeat the preceding steps to generate any middle or last key parts.

Smart card parts — loading master key parts from a smart card

Steps for loading TKE workstation crypto adapter master key parts from a TKE or EP11 smart card are as follows:

1. From the **Master Key** pull-down menu, select **DES/PKA Master Keys** or **AES Master Key**, and then select **Smart Card Parts**. You are prompted to insert a TKE or EP11 smart card into smart card reader 2. A Smart Card Master Key Parts panel is displayed. Any TKE workstation crypto adapter master key parts stored on the smart card are listed in the container. The smart card description is displayed. Ensure that this is the correct smart card you want to work with.
2. Highlight the key part you want to load into the selected TKE workstation crypto adapter new master key register. Click **Load**. You are prompted for the PIN of the smart card inserted in smart card reader 2.

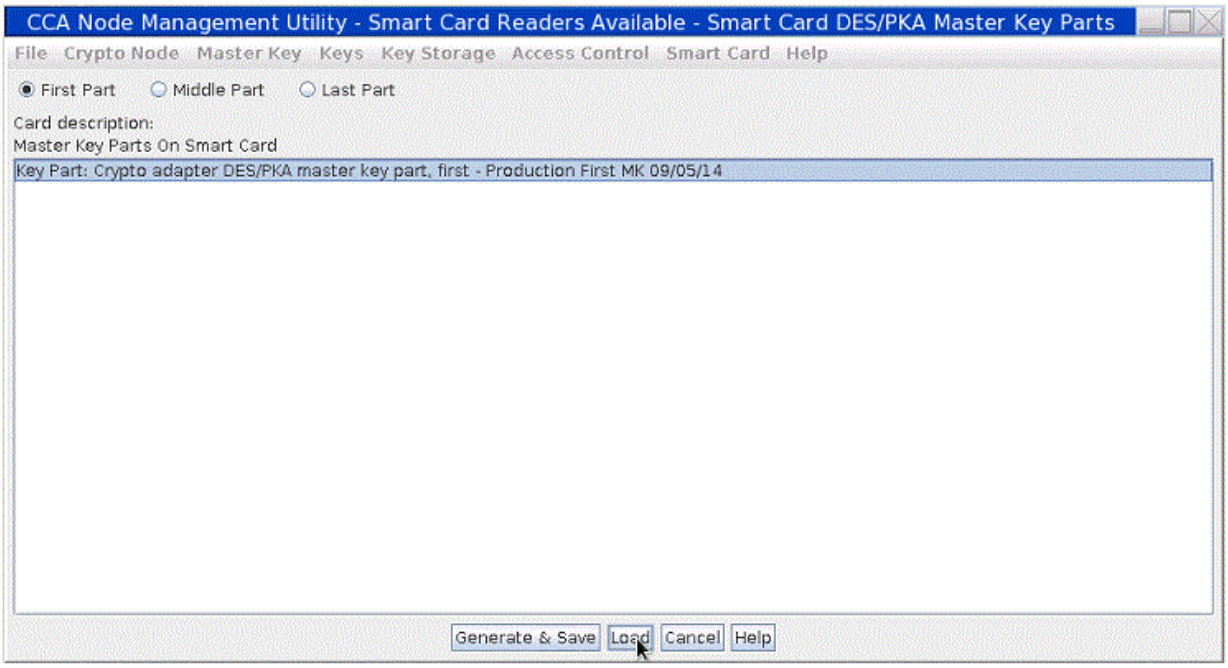


Figure 217. Master Key Part Smart Card panel — loading a Crypto Adapter key part from a smart card

3. A secure session is established between the TKE workstation crypto adapter and the smart card. A pop-up message displays, indicating that the key part was successfully loaded.

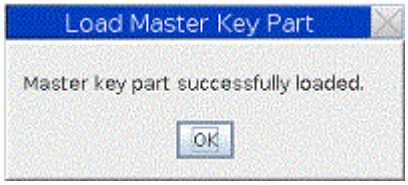


Figure 218. Master key part successfully loaded

4. Repeat steps "1" on page 276 through "3" on page 277 to load additional key parts into the TKE workstation crypto adapter new master key register. If the key parts are on different smart cards, remove the smart card from smart card reader 2 and insert the smart card that contains the next key part to load.

   Note: Key parts must be loaded in order. Specifically, a first key part must be loaded first (Key Part: Crypto Adapter master key part, first) and the last key part (Key Part: Crypto Adapter master key part, last) must be loaded last.

Set — setting the master key value

To set the master key value:

1. From the **Master Key** pull-down menu, select **DES/PKA Master Keys** or **AES Master Key**, and then select **Set...** This will do the following:
   - Transfer the key in the current master key register to the old master key register and delete the former old master key.
   - Transfer the key in the new master key register to the current master key register.
2. After setting a new master key, reencipher the keys currently in key storage. See "Reenciphering key storage" on page 279.

Verify — verifying the master key

A verification pattern (VP) is generated for each master key stored in the master-key registers (new, current and old). The VP can be used to verify that the correct key part was entered, for instance, when

you have many key parts stored to disk or smart cards. It can also be used to verify that the key part was entered correctly, particularly when key parts are entered manually. The VP is zero when the register is empty. After each key part is entered, the key part is combined with the existing key in the register and the VP is updated. The VP does not reveal information about the clear key value.

The VP can be saved to disk for future reference. For example, in the event the TKE workstation crypto adapter is initialized, the master key registers are cleared. When the master key is reloaded, you can compare the VP of the master key register to the VP saved to disk. If they are identical, it indicates that the correct master key parts were loaded. Then you can set the master key. If they are different, you can clear the new master key register and load the correct key parts.

To verify a master key, do the following:

1. From the **Master Key** pull-down menu, select **Verify**. A sub-menu is displayed.

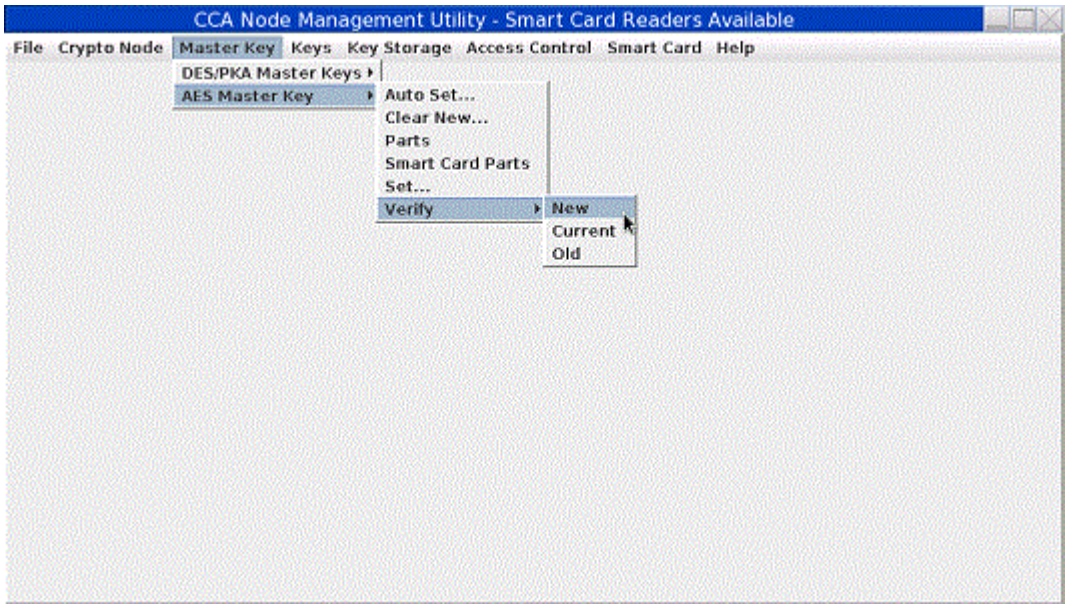


Figure 219. Master Key Verify sub-menu

2. From the submenu, select the master key register you wish to verify - **New**, **Current** or **Old**. Typically, you will choose **New**. You cannot change the current or old master key.
3. The VP is displayed in the Master Key Register Verification panel.

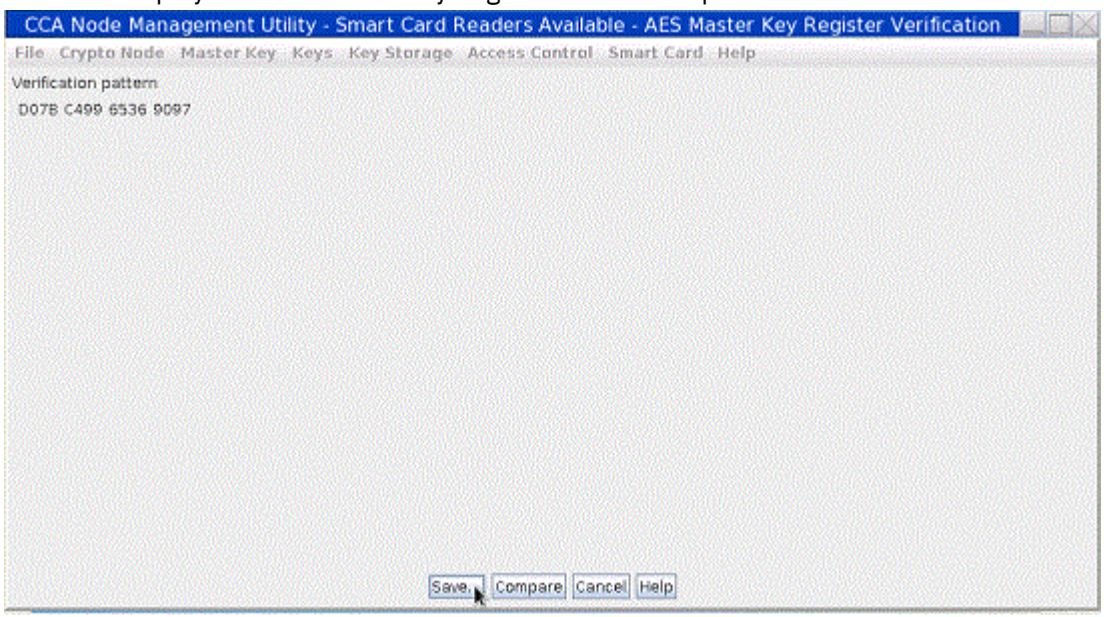


Figure 220. Master Key Register Verification panel - verification pattern is displayed

4. Select **Save** to save the VP to a file. A file chooser will be displayed for the user to specify both a file name, and where to save the file (USB flash memory drive or CNM Data Directory).

   Attention : Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages might be generated on the TKE workstation.

5. Select **Compare** to compare the VP to a VP previously saved to disk. A file chooser will be displayed for the user to specify the location and filename of the saved VP.

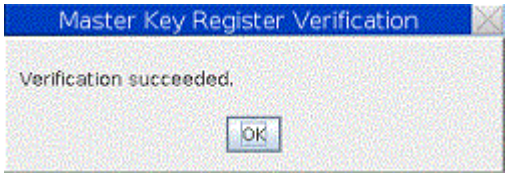


Figure 221. Master Key Register VP compare successful

Key Storage menu

The Key Storage pull-down menu of the CNM main window contains menu items to manage or initialize DES, PKA, or AES key storage.

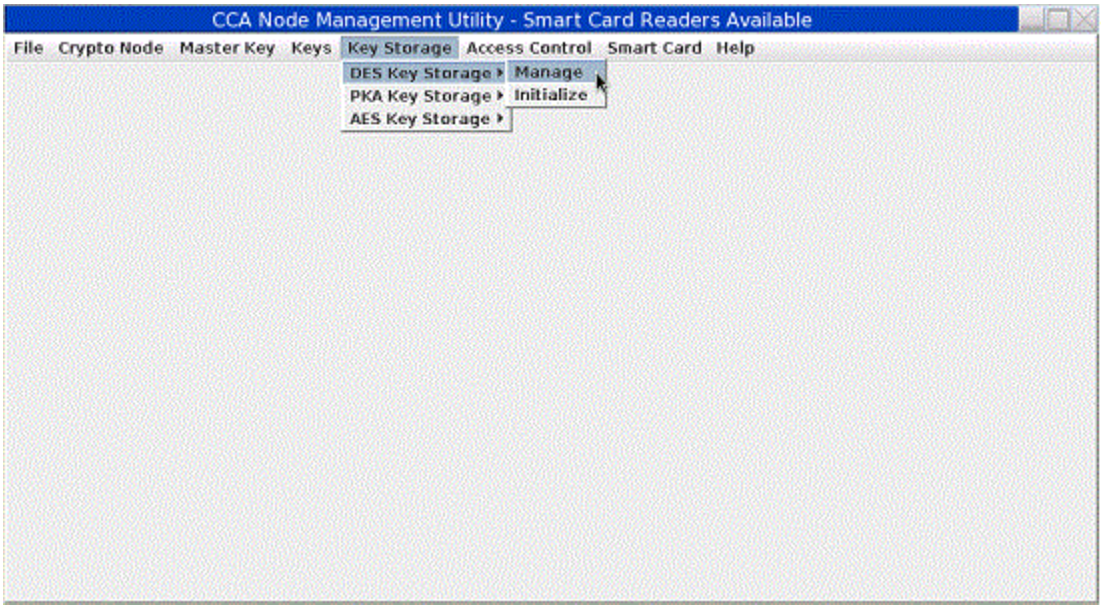


Figure 222. CNM main window — Key Storage pull-down menu

Reenciphering key storage

Key storage is a repository of keys that you access by key label. DES keys, PKA (RSA) keys, and AES keys are held in separate storage systems. The keys in key storage are enciphered under the current TKE workstation crypto adapter master key. When a new master key is set, thereby becoming the current master key, the keys must be reenciphered to the current master key.

To reencipher the keys in storage, do the following:

1. From the **Key Storage** pull-down menu, select **DES Key Storage**, **PKA Key Storage**, or **AES Key Storage**. A sub-menu is displayed.
2. From the sub-menu, select **Manage**. A Key Storage Management panel is displayed. The panel lists the labels of the keys in key storage.

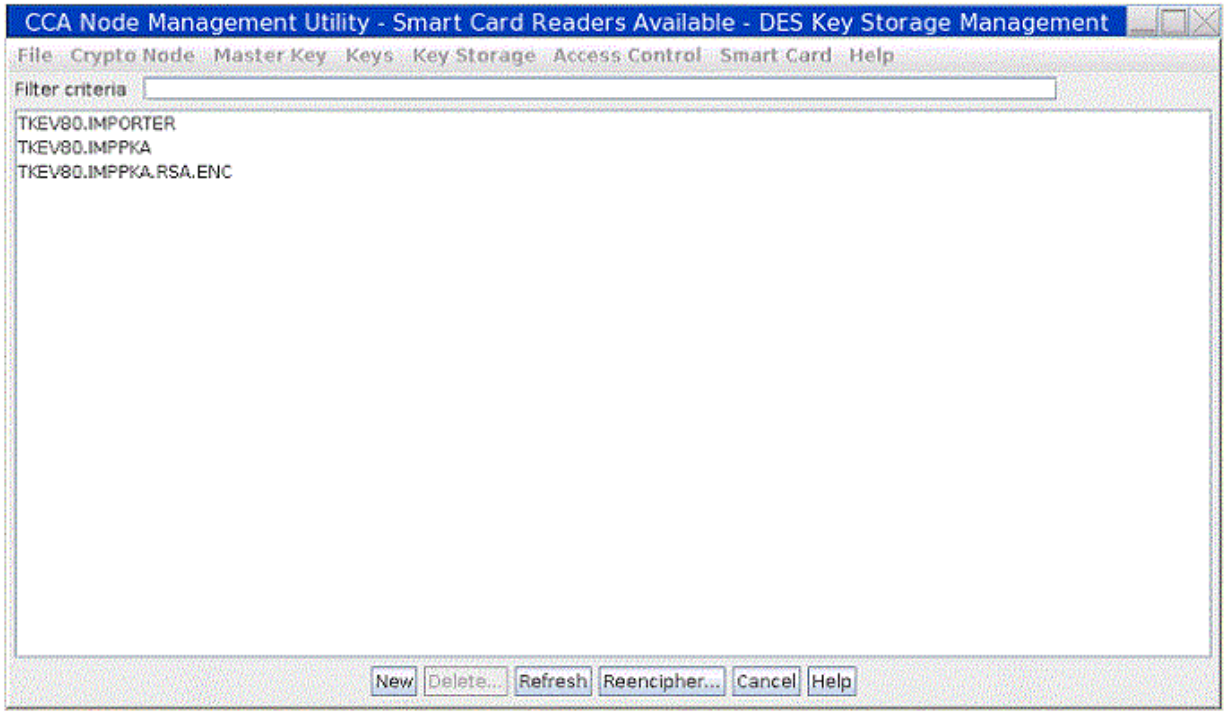


Figure 223. Key Storage Management Panel – key labels list

3. Select **Reencipher...**; the keys are reenciphered using the key in the current master key register.

Smart card menu

The Smart Card pull-down menu of the CNM main window contains the following menu items.

- Change PIN
- Generate Crypto Adapter Logon Key
- Display Smart Card Details
- Manage Smart Card contents
- Copy Smart Card

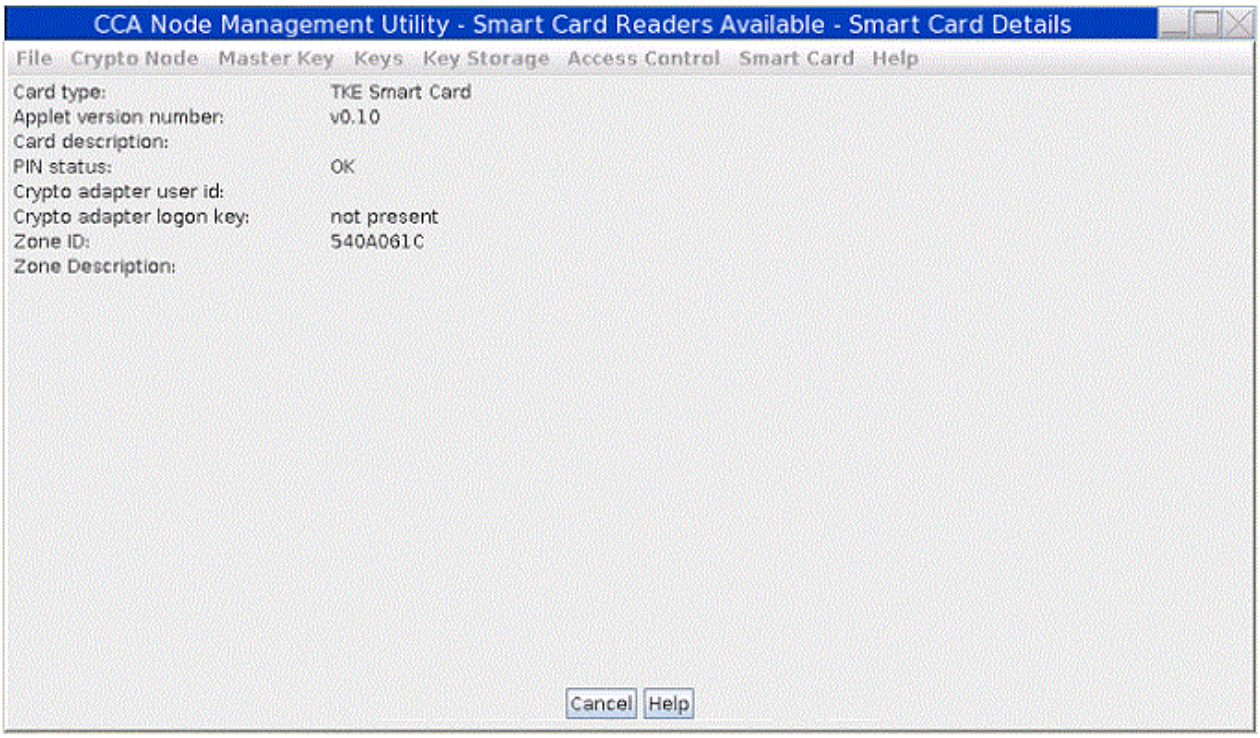


Figure 224. CNM main menu — Smart Card pull-down menu

Change PIN

TKE and EP11 smart cards are secured with a PIN. You can change your PIN using this function. You must know your current PIN. If your smart card is blocked due to too many incorrect PIN attempts, this function will fail.

To change the PIN, perform the following steps:

1. From the **Smart Card** pull-down menu, select **Change PIN**. An informational window will prompt you to insert your smart card into smart card reader 2. Insert your smart card and press **OK** to continue.

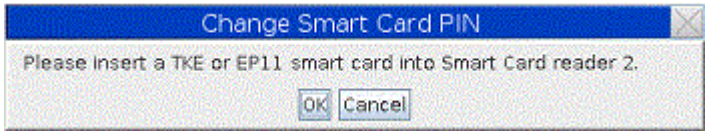


Figure 225. Change PIN — insert smart card prompt

2. You will be prompted for your current PIN. Enter your current PIN on the smart card reader 2 PIN pad.



Figure 226. Change PIN — enter current PIN prompt

3. You will be prompted for your new PIN. The new PIN must be entered twice and both PINs must match.



Figure 227. Change PIN — enter new PIN prompt

4. The PIN is successfully changed on the smart card.

Generate TKE crypto adapter logon key

A Crypto Adapter logon key allows a user to log on to the TKE workstation crypto adapter using a TKE or EP11 smart card to access functions not allowed in the default role. A Crypto Adapter logon key is an RSA public/private key pair generated within the smart card. The private key never leaves the smart card. The public key is read from the smart card and loaded to the TKE workstation crypto adapter when a user profile is defined.

To generate a Crypto Adapter logon key, do the following:

1. From the Smart Card pull-down menu, select Generate Crypto Adapter Logon Key. You will be prompted for a TKE or EP11 smart card. Insert the smart card into smart card reader 2.

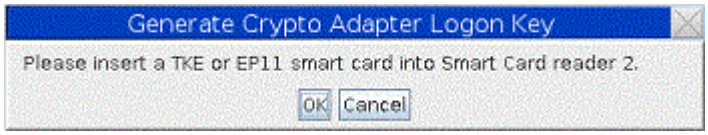


Figure 228. Generate Crypto Adapter Logon Key — insert smart card

2. You will be prompted for a PIN. Enter the PIN on the smart card reader 2 PIN pad.

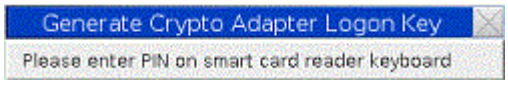


Figure 229. Generate Crypto Adapter Logon Key — PIN prompt

3. You will be prompted for a user ID for the smart card. This user ID will be read from the smart card when defining a smart card user profile.

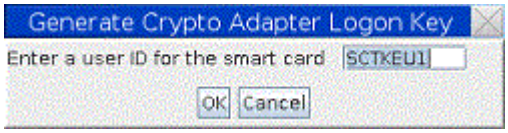


Figure 230. Generate Crypto Adapter Logon Key — User ID prompt

4. The Crypto Adapter logon key is generated.

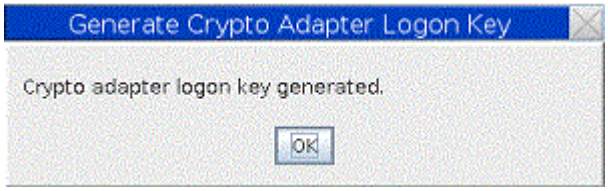


Figure 231. Generate Crypto Adapter Logon Key — key generated

Display smart card details

Use this function to display public information about a TKE or EP11 smart card.

1. From the **Smart Card** pull-down menu, select **Display Smart Card Details**. You will be prompted for a TKE or EP11 smart card. Insert the smart card into smart card reader 2.

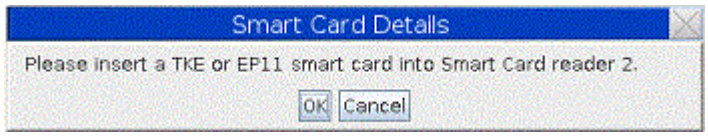


Figure 232. Display Smart Card Details — insert smart card prompt

The smart card is read and the public information is displayed.

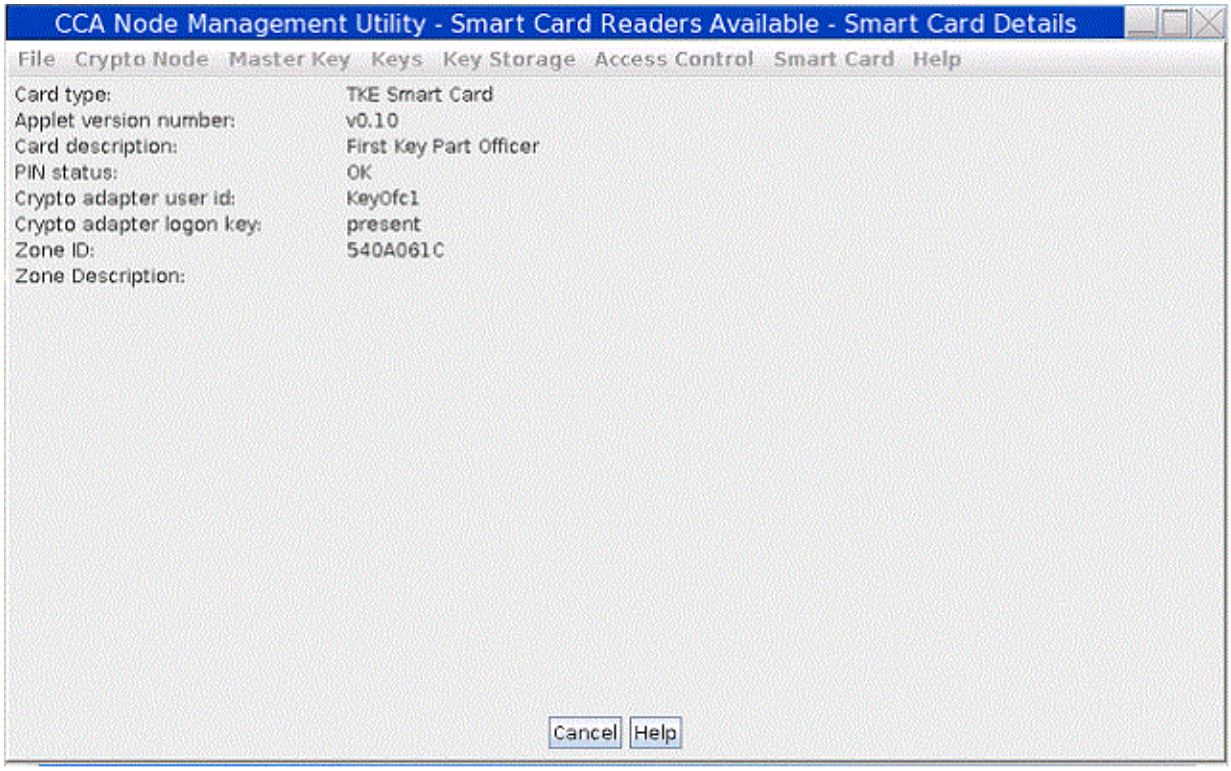


Figure 233. Display Smart Card Details — public information displayed

The following information is displayed for a TKE or EP11 smart card:

Card type
TKE smart card or EP11 smart card

Applet version number
Version number of applet loaded on smart card

Card description
Description of the smart card. The smart card description was entered when the smart card was personalized

PIN status
The PIN status can be OK/blocked/not set. The PIN is set when the smart card is personalized

Crypto Adapter User ID
User ID entered when a Crypto Adapter logon key is generated. The User ID may be blank if the smart card does not have a Crypto Adapter logon key

Crypto Adapter Logon Key
Status can be present/not present

Zone ID
Set when the smart card is initialized

Zone Description
Set when the smart card is initialized

Manage smart card contents

Use this function to delete keys or key parts from a TKE or EP11 smart card. A TKE or EP11 smart card can hold up to 50 key parts, a TKE authority signature key or EP11 administrator signature key, and a crypto adapter logon key. To display the smart card contents using the Manage Smart Card Contents function, do the following:

1. From the **Smart Card** pull-down menu, select **Manage Smart Card contents**. You will be prompted for a TKE or EP11 smart card. Insert the source smart card into smart card reader 2.

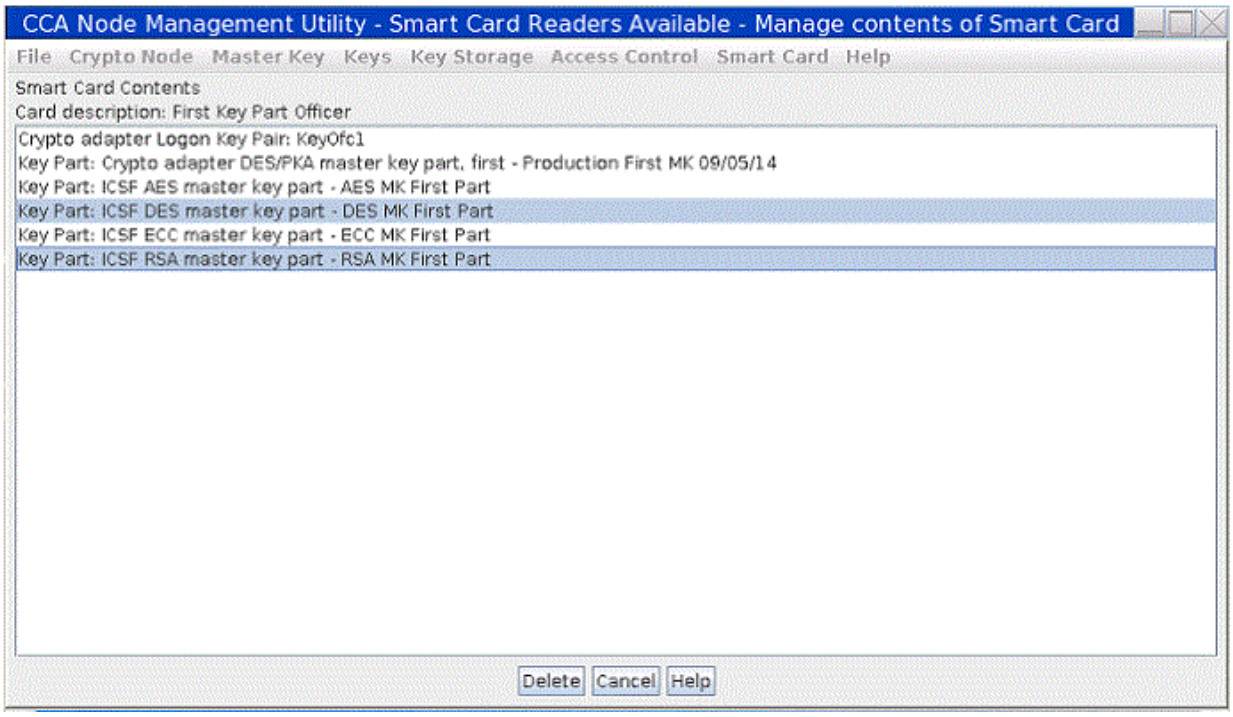


Figure 234. Manage Smart Card contents — contents of smart card are displayed

2. The smart card description is displayed. Ensure this is the correct smart card you want to work with. Highlight the keys and/or key parts you want to delete. Press the **Delete** push button.
3. You will be prompted for your PIN. Enter your PIN on the smart card reader 2 PIN pad.
4. You will be asked to confirm the deletion of the selected objects. Press **OK** to continue.

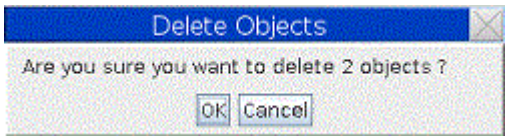


Figure 235. Manage Smart Card contents — confirm delete prompt

5. The objects are deleted and the list is refreshed.

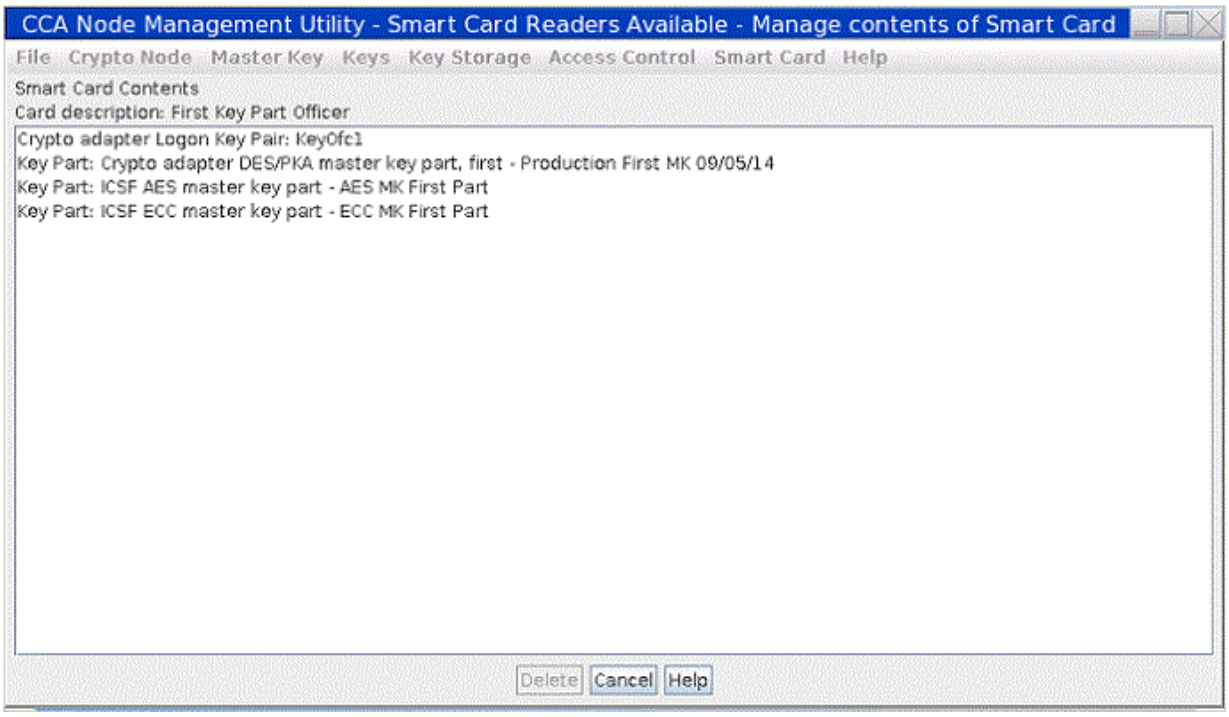


Figure 236. Manage Smart Card contents

Attention: If you delete a crypto adapter logon key, you will not be able to log on to the TKE workstation crypto adapter until you generate a new crypto adapter logon key and the administrator updates your crypto adapter user profile.

If you delete a TKE authority signature key, you will not be able to sign a TKE command until the administrator generates a new authority signature key and uploads it to the host.

Copy smart card

Use this function to copy a key or key part or parts from one TKE smart card to another TKE smart card, or from one EP11 smart card to another EP11 smart card. The two smart cards must belong to the same zone or share an alternative zone. Specifically, the two smart cards must have the same Zone ID or share an alternative Zone ID. Use **Display Smart Card Details** to verify the Zone ID of the smart cards.

Notes:

1. AES key parts cannot be copied to a TKE smart card that does not have the TKE applet version 0.4 or later. ECC (APKA) key parts cannot be copied to a TKE smart card that does not have the TKE applet version 0.6 or later.
2. ECC authority signature keys cannot be copied to a TKE smart card that does not have the TKE applet version 0.10 or later.
3. Smart card copy does not overwrite the target smart card. If there is not enough room on the target smart card, you get an error message. You can either delete some of the keys on the target smart card (see “Manage smart card contents” on page 283) or use a different smart card.
4. TKE Version 6.0 was the final release that supported DataKey smart cards. Copying a DataKey smart card is the only procedure that is still supported. You can only copy data from a DataKey smart card. You cannot copy to a DataKey smart card.

To copy smart card contents:

1. From the **Smart Card** pull-down menu, select **Copy Smart Card**. You are prompted to insert the first TKE or EP11 smart card into smart card reader 1. The contents of the smart card are displayed in the top container.

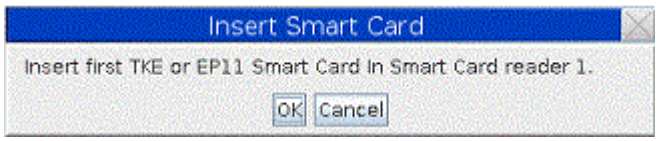
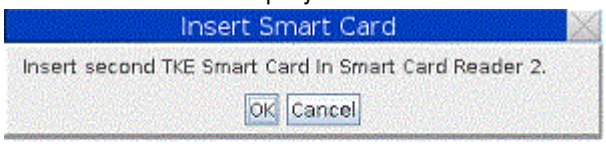


Figure 237. Copy Smart Card — insert first smart card

2. You are prompted for a second smart card. The second smart card must be the same type (TKE or EP11) as the first smart card. Insert the second smart card into smart card reader 2. The contents of the smart card are displayed in the bottom container.



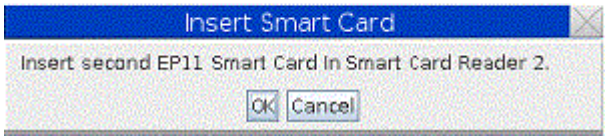




Figure 238. Copy Smart Card — asked for the TKE or EP11 smart card

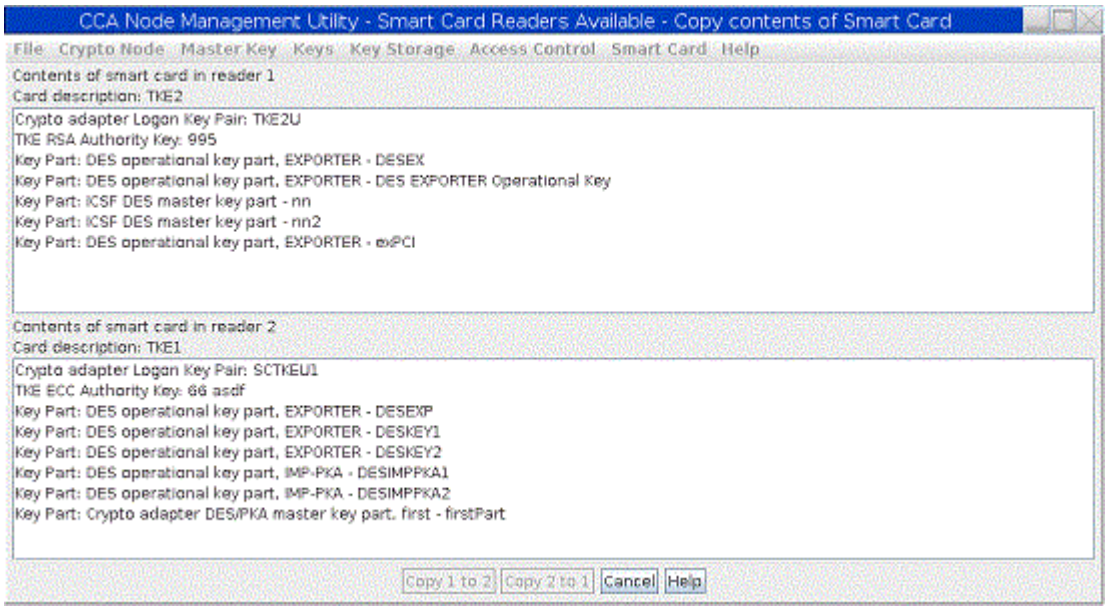


Figure 239. Copy Smart Card — smart card contents are displayed

3. Highlight the objects in the container you want to copy to the other container. Press the button that relates to the applicable direction to copy the parts. For example, Figure 240 on page 287 shows that the selected parts are the first container so the **Copy 1 to 2** button copies from container 1 to container 2.

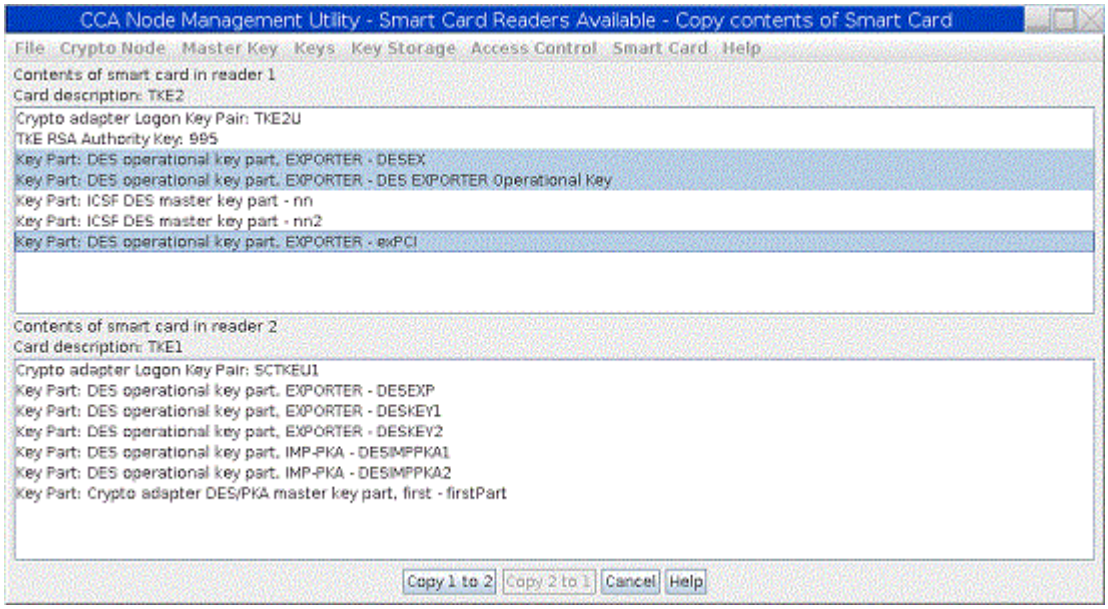


Figure 240. Copy Smart Card — highlight object to copy and direction

4. You are prompted for the PIN of the first smart card in smart card reader 1. Enter the PIN on the smart card reader 1 PIN pad.



Figure 241. Copy Smart Card — first smart card PIN prompt

5. You are prompted for the PIN of the second smart card in smart card reader 2. Enter the PIN on the smart card reader 2 PIN pad. A secure session is established between the two smart cards and the selected object or objects are copied. The contents of the target container is refreshed.



Figure 242. Copy Smart Card — second smart card PIN prompt



Figure 243. Establishing a secure session between the two smart cards



Figure 244. Objects are copied to the target smart card

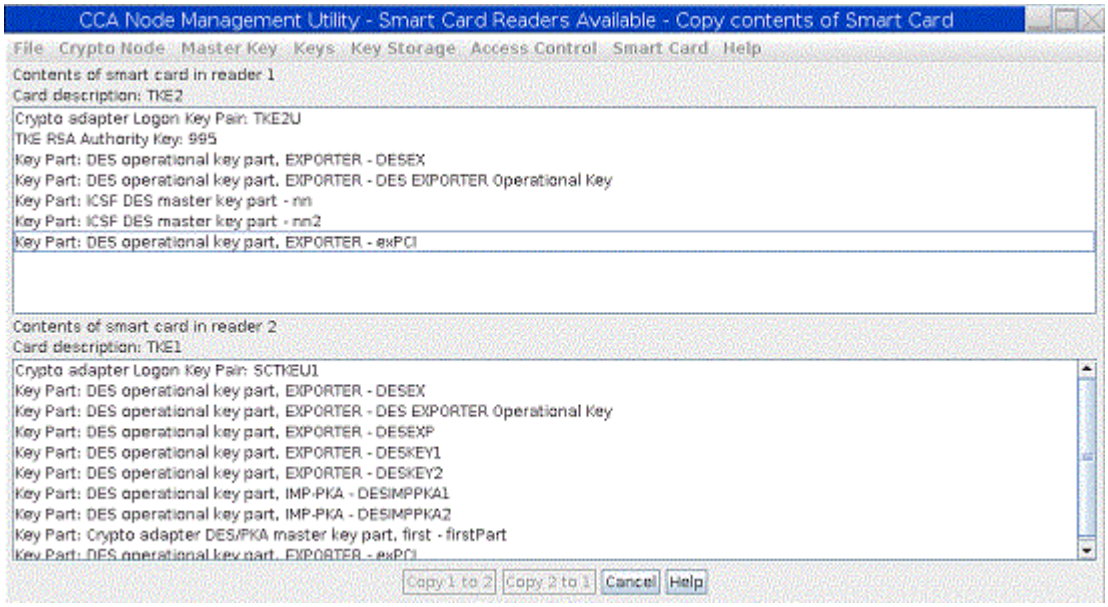


Figure 245. Copy Smart Card — objects are copied to the target container

TKE and EP11 smart cards can hold a maximum of 50 key parts, in addition to a crypto adapter logon key and a TKE authority signature key or an EP11 administrator signature key.

CNM common errors

Message: “Incorrect passphrase”
Return Code: 4
Reason Code: 2042
Explanation: Check that you typed in the passphrase correctly. The passphrase is case sensitive.

Message: “Access is denied for this function”
Return Code: 8
Reason Code: 90
Explanation: The role associated with your profile does not allow you to perform this function. Log off the crypto module and log on using a profile associated with a role that allows this function.

Message: “Your user profile has expired”
Return Code: 8
Reason Code: 92
Explanation: The TKE administrator must reset the expiration date on the user profile.

Message: “Your authentication data (for example, passphrase) has expired.”
Return Code: 8
Reason Code: 94
Explanation: The TKE administrator must change the passphrase and reset the passphrase expiration date on the user profile. Then, select **Replace** to load the profile into the workstation coprocessor.

Message: “The user profile does not exist”
Return Code: 8
Reason Code: 773
Explanation: Make sure you typed in the user ID correctly. The user ID is case sensitive.

Message: “The group logon failed because authentication of one or more group members failed.”
Return Code: 8
Reason Code: 2084
Explanation: One or more user profiles in the group failed authentication (for example, passphrase expired or profile expired) causing the group logon to fail. The group logon window will indicate which user failed and the reason for the logon failure. Correct the user profile or attempt group logon again and select a different member in the group members list for logon.

Message: “The profile is included in one or more groups”
Return Code: 8
Reason Code: 2085
Explanation: You attempted to delete a user profile that is currently a member of a group profile. You must remove the user profile from the group member list before deleting the profile.

Message: “The group role does not exist.”
Return Code: 8
Reason Code: 2086
Explanation: You attempted group logon using a group profile that is associated with a role that does not exist. The TKE administrator must define the role and load it to the TKE workstation crypto adapter before the group profile may be used.

Message: “Your group profile has not yet reached its activation date”
Return Code : 8
Reason Code: 2087
Explanation: The group profile has an activation date that is later than the current date. The TKE administrator must change the activation date before the group profile may be used or wait until the activation date arrives.

Message: “Your group profile has expired.”
Return Code: 8
Reason Code: 2088
Explanation: The group profile has surpassed its expiration date.
The TKE administrator must change the expiration date before the group profile may be used.

Chapter 12. Smart Card Utility Program (SCUP)

The TKE Smart Card Utility Program (SCUP) allows you to create and manage CA, TKE, and EP11 smart cards and to enroll the TKE workstation crypto adapter in a zone. TKE and EP11 smart cards can hold master and operational key parts for host crypto modules, an authority or administrator signature key used to sign host commands, and a logon key for the TKE workstation crypto adapter.

SCUP supports these general functions:

- “Display smart card information” on page 294
- “Display smart card key identifiers” on page 296
- “TKE zone wizard” on page 298
- “TKE Smart Card wizard” on page 298

For CA smart cards, SCUP supports these functions:

- “Initialize and personalize a CA smart card” on page 299
- “Create a backup CA smart card” on page 301
- “Change the CA smart card PINs” on page 302

For TKE and EP11 smart cards, SCUP supports these functions:

- “Initialize and enroll a smart card” on page 302
- “Personalize a smart card” on page 303
- “Unblock PIN on a smart card” on page 303
- “Change PIN of a smart card” on page 304
- “Enroll smart card in an alternate zone” on page 304
- “Remove alternate zone from smart card” on page 304

For the TKE workstation crypto adapter, SCUP supports these functions:

- “Enroll a TKE cryptographic adapter in a primary zone” on page 305
- “View current zone for the crypto adapter” on page 310
- “Remove current zone from the crypto adapter” on page 310

To create and manage the smart cards used for configuration migration (MCA, IA, and KPH smart cards), use the Configuration Migration Tasks utility.

General information

When entering PINs, the PIN prompt appears on both the TKE workstation screen as well as on the smart card reader. When certain tasks will take over one minute for SCUP to execute, information messages are returned. Be patient so that you do not have to restart the task.

Beginning in TKE 7.2, TKE supports 2, 3, or 4 smart card readers. The additional readers were added to reduce the amount of smart card swapping needed during the command signature phase for PKCS #11 (EP11) functions. However, the additional readers can be used in other operations too. Some screens in SCUP look different when more than 2 readers are present.

Note: On TKE workstation feature codes #0847 or older, there are only 6 USB ports. This is enough ports for the mouse, keyboard, and 4 smart card readers. However, this configuration does not leave any USB ports for removable media. If you want to have 4 smart card readers and have ports available for USB flash memory, we recommend the purchase of an unpowered 2 or 4 slot USB hub. Plug the smart card readers into the hub which will leave other USB ports available for USB flash memory drivers.

© Copyright IBM Corp. 2000, 2021

The utility is capable of overwriting your smart cards. You will be prompted to reply **OK** before the card is overwritten.

To start SCUP, click on **Trusted Key Entry** in the main workstation screen. This will display various workstation functions.

Note: You can use the Smart Card Utility Program if you are logged on at the console as ADMIN or TKEUSER. In addition, you must be logged onto the TKE workstation crypto adapter with a profile defined when you configured the TKE workstation from CNM. You are prompted to logon to the TKE workstation crypto adapter if you are not currently logged on.

Click on **Applications**. Under Applications, click on **Smart Card Utility Program**. The Smart Card Utility Program screen appears.

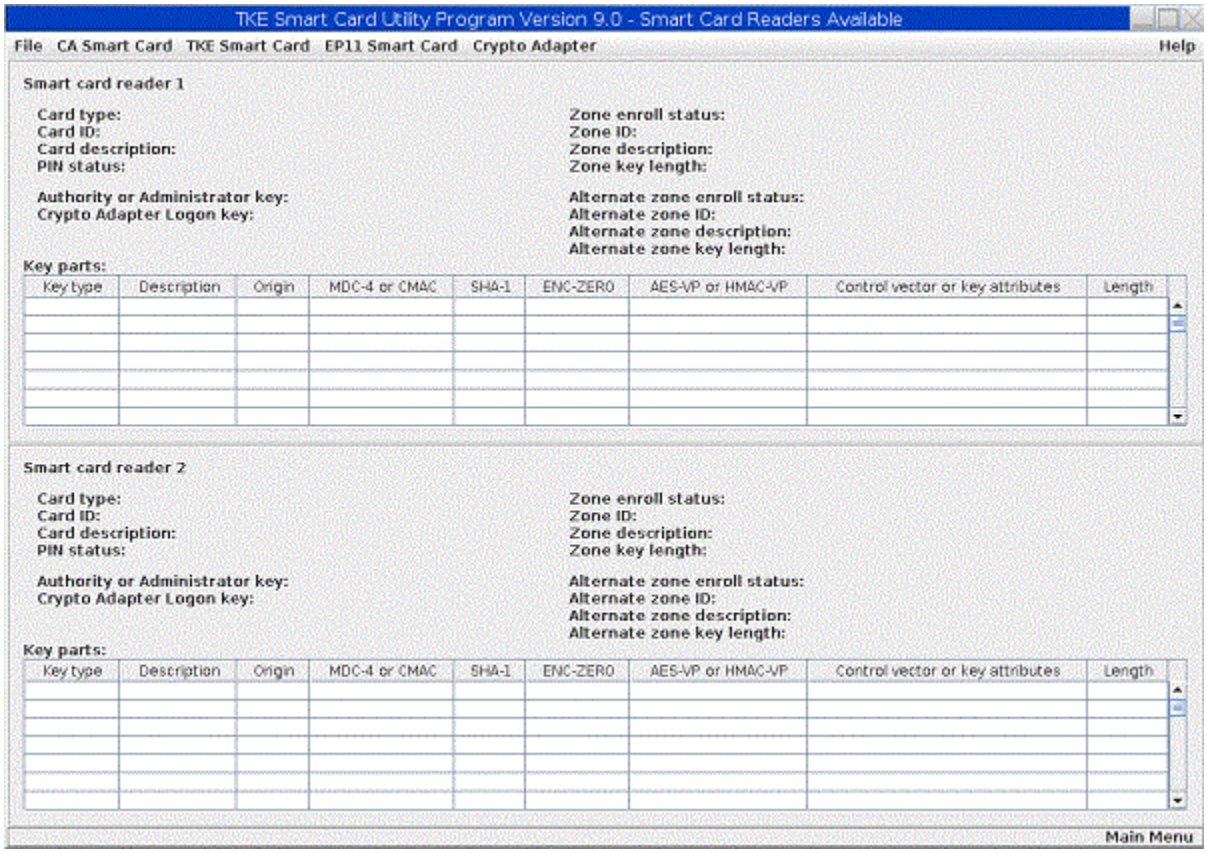


Figure 246. First screen of TKE Smart Card Utility Program (SCUP) with 2 readers

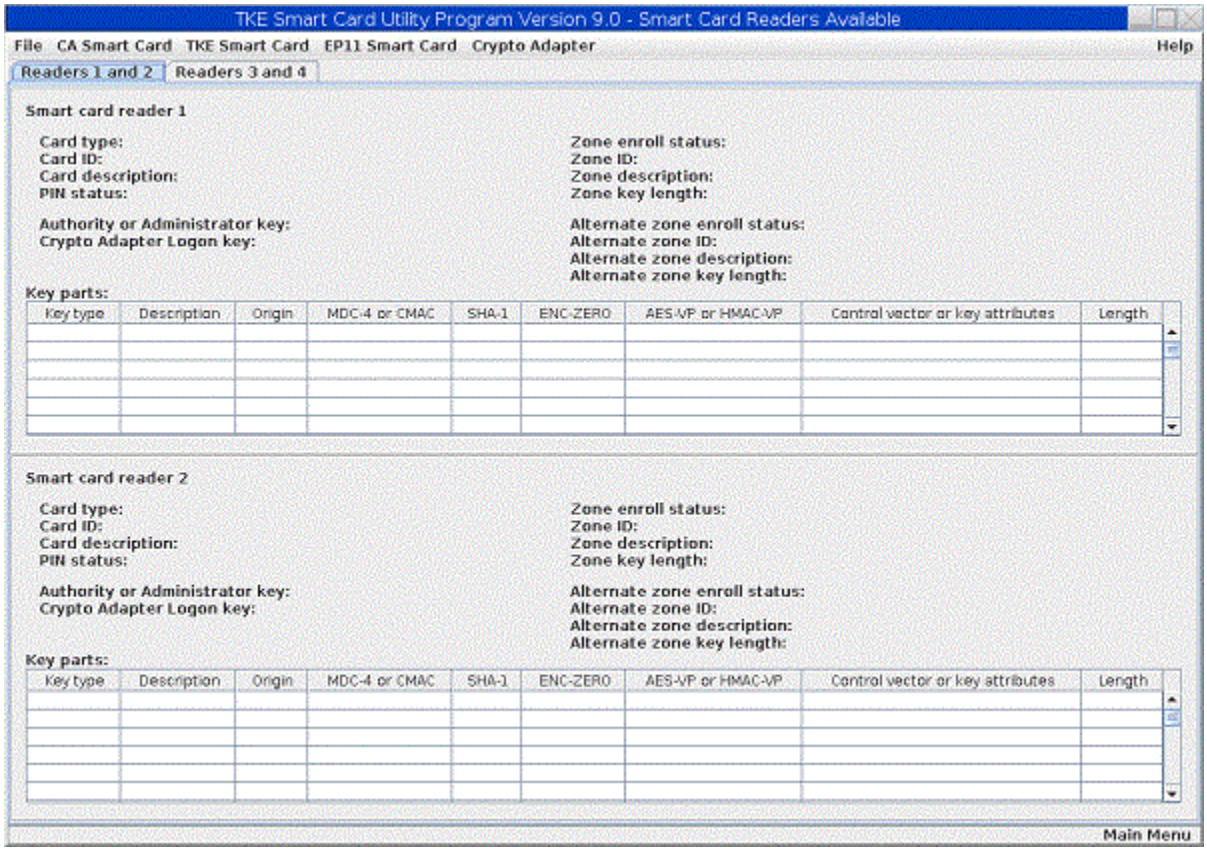


Figure 247. First screen of TKE Smart Card Utility Program (SCUP) with more than 2 readers

Starting point for all the TKE policy wizards

Starting with TKE 9.1, the TKE workstation provides six wizards that work together to implement a comprehensive set of security policies for managing access to the TKE workstation and managing host crypto modules and their domains. All of the policies require that something be stored on a smart card. Therefore, the first wizard, the **TKE Smart Card Wizard**, is found in the Smart Card Utility Program (SCUP). The **TKE Smart Card Wizard** creates all the smart cards that the other wizards need.

Gemalto smart card reader considerations

The following smart card reader considerations apply:

- You can carry your HID/OMNIKEY smart card readers from older TKEs forward to your TKE 9.0 system.
  - If you use HID/OMNIKEY smart card readers on your TKE 9.0 system, any initialized smart cards can be used on TKE 9.0. However, you are subject to any smart card part limitations that exist for the smart card part on TKE 8.1.
- Any smart card that is initialized and personalized on TKE 9.0 can be used in either the HID/OMNIKEY or Gemalto smart card reader.
- TKE 9.0 supports any combination of HID/OMNIKEY and Gemalto smart card readers at the same time.
- The Gemalto smart card reader requires you to press the green Enter button after you enter:
  - The PIN.
  - A character in the secure key entry process.

Important: Gemalto CT700 readers work only with smart cards that have applets that are loaded from TKE 8.1 or later. Therefore, you must carry Omnikey Cardman 3821 smart card readers forward to use smart cards with pre-TKE 8.1 applets on TKE 9.0. See Table 35 on page 294 for the actions that are required to move to smart cards that work in Gemalto smart card readers:

Table 35. Smart card migration actions	
Type of smart card	**Smart card migration actions**
TKE and EP11 smart cards	• Initialize and personalize the new smart cards on a TKE at TKE 8.1 or later. • Copy the contents from an old smart card to a new smart card. – If the copy is done on a TKE 9.0 system, the source smart card must be in an HID/ OMNIKEY smart card reader.
CA and MCA smart cards	• Initialize and personalize the new smart cards by using the CA and MCA backup procedure on a TKE at TKE 8.1 or later. – If the backup operation is done on a TKE 9.0 system, the source smart card must be in an HID/OMNIKEY smart card reader.
IA and KPH smart cards	• Initialize and personalize new smart cards on a TKE at TKE 8.1 or later. – There is no data to copy from one IA or KPH card to another. – For old KPH smart cards, if you have any exiting collect files that were created with KPH certificates from old KPH smart cards, you can use these files in an apply operation if the old KPH smart cards are put in an HID/OMNIKEY reader during the apply operation.

File menu functions

Display smart card information

After you have created a smart card, you are advised to check the results. If you are copying keys from one smart card to another, you might also want to verify that all of the keys were correctly copied to the other smart card.

1. Insert the smart cards to be displayed in the smart card readers. From the **File** menu, click **Display smart card information**.

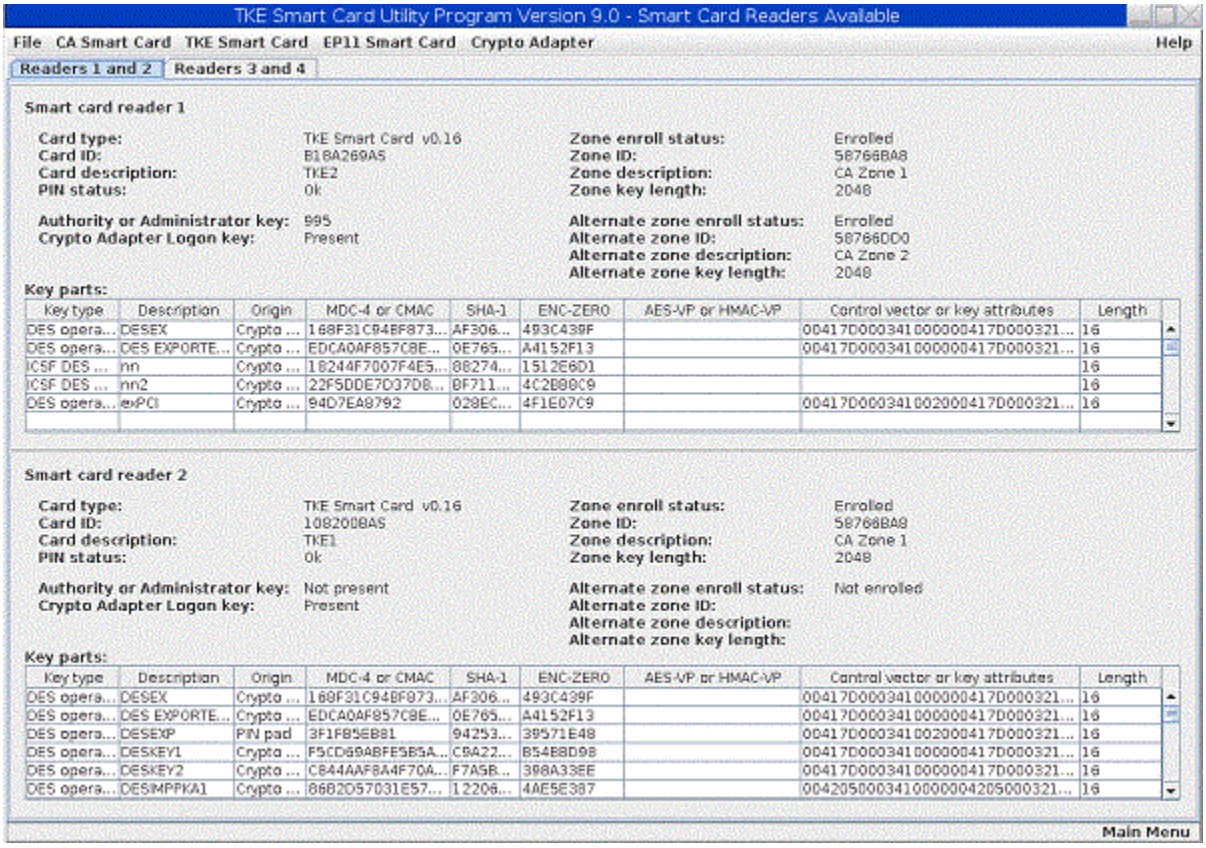


Figure 248. Display smart card information

The panel provides the following information about the smart card:

Card type
Identifies the type and applet version of the smart card in the reader. TKE supports CA, TKE, EP11, MCA, IA, and KPH smart cards.

Card ID
A 9-digit identifier that is generated when the smart card is initialized.

Card description
The description that you entered when creating the smart card. Can be 30 characters in length.

PIN status
Can be OK, Blocked, or Not set.

Authority or Administrator key
For TKE smart cards, displays the authority index and name. For EP11 smart cards, displays the administrator name.

Crypto Adapter Logon Key
For TKE and EP11 smart cards, the value is Present or Not Present.

Zone enroll status
Indicates whether the smart card is enrolled in a primary zone. It is either Enrolled or Not enrolled.

Zone ID
The zone ID from the CA or MCA smart card that is used to initialize and enroll the smart card. This is the zone ID of the primary zone.

Zone Description
The optional zone description from the CA or MCA smart card that is used to initialize and enroll the smart card. This is the zone description of the primary zone. Can be up to 12 characters in length.

Zone key length
The length in bits of the modulus of the public key that defines the primary zone.

Alternate zone enroll status
Indicates whether the smart card is enrolled in an alternate zone. The status is Enrolled or Not enrolled, or blank if the smart card does not support an alternate zone.

Alternate zone ID
The zone ID from the CA smart card that is used to establish an alternate zone. Blank if the smart card does not support an alternate zone or if the smart card is not enrolled in an alternate zone.

Alternate zone description
The optional zone description from the CA smart card that is used to establish an alternate zone. Blank if the smart card does not support an alternate zone or is not enrolled in an alternate zone.

Alternate zone key length
The length in bits of the modulus of the public key that defines the alternate zone. Blank if the smart card does not support an alternate zone or is not enrolled in an alternate zone.

Only TKE and EP11 smart cards store key parts, so fields in the **Key parts** table are filled in only for these smart card types.

Key type
Operational key parts, TKE crypto adapter master key parts, or ICSF master key parts.

Description
Description of key part (optional).

Origin
Crypto Adapter or PIN-PAD.

MDC-4
MDC-4 hash value of the key part.

SHA-1
SHA-1 hash value of the key part.

ENC-ZERO
ENC-ZERO hash value of the key part.

AES-VP
AES verification pattern of the key part.

Control vector or key attributes
For DES operational key parts and AES DATA operational key parts, contains the control vector. For AES non-DATA operational key parts, indicates whether the key part uses the default key attributes or custom key attributes. Blank for master key parts.

Length
8, 16, 24 or 32 bytes.

Display smart card key identifiers

This function displays the key identifiers and key lengths for the TKE Authority Key or EP11 Administrator Key, and the Crypto Adapter Logon Key, on a TKE or EP11 smart card. Some information from the Display smart card information panel is repeated to provide context.

1. Insert smart card or cards to be displayed in smart card reader 1 or 2. From the **File** menu, click **Display smart card key identifiers**.

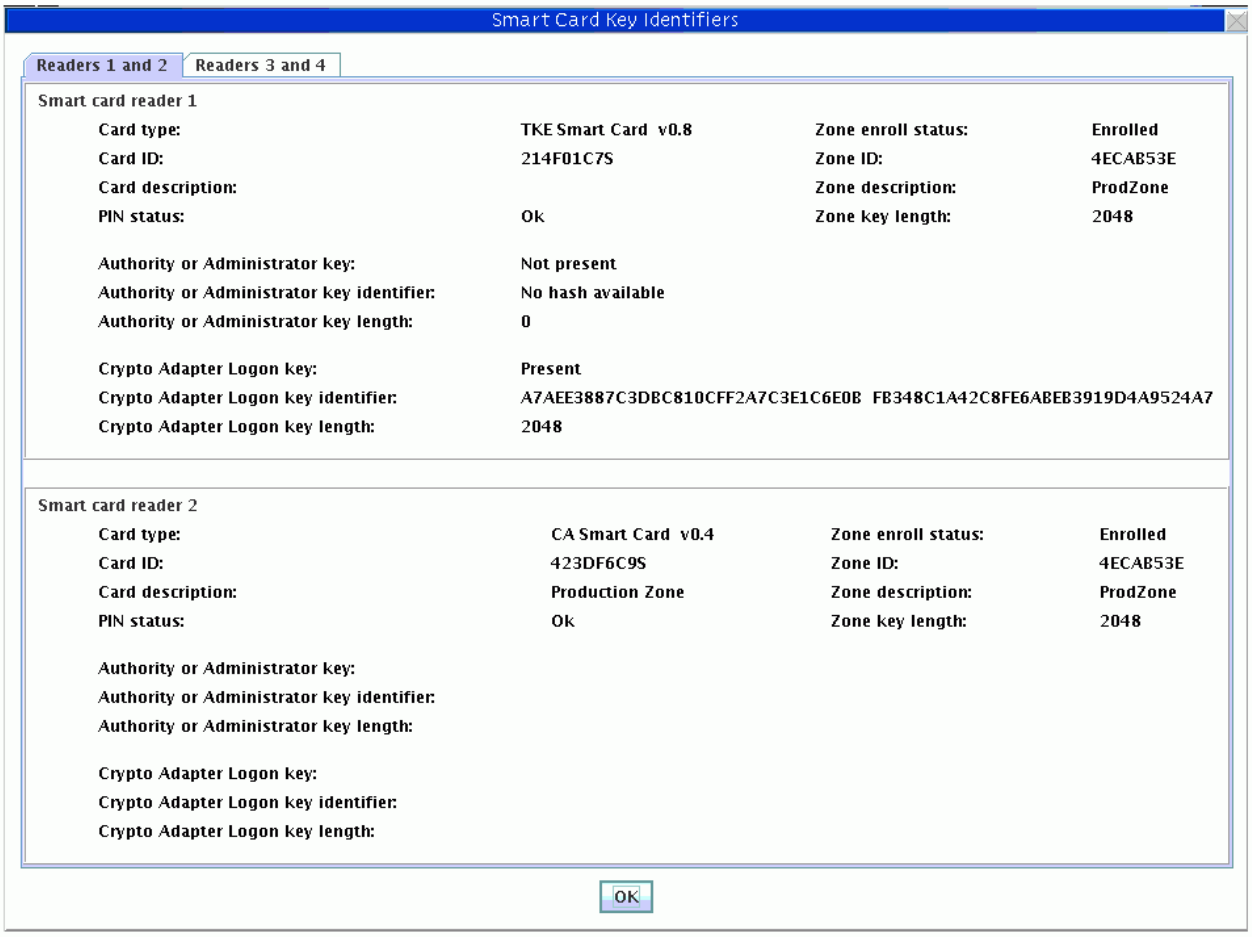


Figure 249. Display of smart card key identifiers

The panel provides this information about the smart card:

- **Card type**: Identifies the type and applet version of the smart card in the reader. TKE supports CA, TKE, EP11, MCA, IA, and KPH smart cards.
- **Card ID**: A 9-digit identifier generated when the smart card is initialized.
- **Card description**: This is the description you entered when creating the smart card. Can be 30 characters in length.
- **PIN status**: OK, Blocked or Not set
- **Authority or Administrator key**: For TKE smart cards, displays the authority index and name. For EP11 smart cards, displays the administrator name.
- **Authority or Administrator key identifier**: For TKE and EP11 smart cards, identifies the authority or administrator key. The key identifier is the SHA-256 hash of the public part of the signature key.
- **Authority or Administrator key length:** The type of the authority or administrator signature key, if present. The type (either RSA or ECC) is indicated along with either the key size in bits (RSA) or curve size in bits (ECC).
- **Crypto Adapter Logon Key**: For TKE and EP11 smart cards, the value can be Present or Not Present.
- **Crypto Adapter Logon Key Identifier**: For TKE and EP11 cards, identifies the crypto adapter logon key. The key identifier is the SHA-256 hash of the DER-encoded public modulus and public exponent of the RSA key pair.
- **Crypto Adapter Logon key length**: The length of the RSA key (in bits) on the smart card used to log on to the TKE workstation crypto adapter.
- **Zone enroll status**: The Zone enroll status is the status of the card. It is either Enrolled or Not enrolled.

- **Zone ID**: When a CA or MCA smart card is created, the system will generate an 8-digit zone number.
- **Zone Description**: This is the description you entered when creating the CA or MCA smart card. Can be 12 characters in length.
- **Zone key length**: The length of the zone certificate public modulus in bits.

TKE zone wizard

A TKE zone is defined by a Certificate Authority (CA) smart card. Members of the TKE zone include extra copies of the CA smart card, TKE smart cards initialized by using the CA smart card, and EP11 smart cards initialized by using the CA smart card. In addition, the TKE's local crypto adapter must be enrolled in the same zone as a TKE or EP11 smart card when you do any type of load key operation. The TKE zone wizard provides a feature that can be used to:

- Create a Certificate Authority (CA) smart card.
- Create any number of backup CA smart cards.
- Create any number of TKE smart cards.
- Create any number of EP11 smart cards.
- Enrolling the TKE workstation in the zone.

Note: You must be signed onto the TKE's local crypto adapter with a profile that has the role of SCTKEADM, TKEADM, or an equivalent authority to enroll the TKE workstation in the TKE zone.

To create a smart card:

1. Initialize the smart card. In this step, the applet is loaded on the smart card.
2. Personalize the smart card. In this step, the PIN or PINs are set and the card description is added.

After you start the TKE zone wizard, you can do all the tasks or just the ones you need. For example, if you want to add two TKE smart cards to an existing TKE zone, you can skip the create CA smart card and create backup CA smart card steps of the TKE zone wizard. The created TKE smart card step initializes and personalizes both cards in one process flow.

TKE Smart Card wizard

The TKE Smart Card Wizard is the first wizard in a family of wizards designed to implement a complete set of security policies for managing the TKE workstation and your host crypto modules. All of the security policies depend on smart cards. The TKE Smart Card Wizard creates the smart cards that you need before you can use any of the other wizards to deploy a security policy. Specifically, you can use this wizard to:

Create Certificate Authority (CA) smart cards
A Certificate Authority (CA) smart card defines a TKE zone. You must have a CA smart card before you can create any TKE or EP11 smart cards.

Create TKE smart cards
You need specific TKE smart cards if you are responsible for managing:

- The TKE workstation.
- CCA host crypto module-wide or normal mode domain-specific settings.
- CCA domains in either imprint or PCI-compliant mode settings.

Create EP11 smart cards
You need specific EP11 smart cards if you are responsible for managing:

- EP11 module-wide settings.
- EP11 domain-specific settings.

Enroll the TKE workstation in a zone
The TKE workstation must be enrolled in the same zone as the TKE or EP11 smart card when key parts are placed onto the smart card or loaded onto a host crypto module.

CA smart card menu functions

Initialize and personalize a CA smart card

A zone is created when a CA smart card is initialized and personalized.

Note: In general, CA smart cards that are created on a particular TKE release cannot be used on TKE workstations that are at prior release levels. There are exceptions. For more information, see "Smart card usage" on page 47.

To initialize a CA smart card, follow these steps:

1. From the *CA Smart Card* drop down menu, select *Initialize and personalize CA smart card* option.
2. When prompted, insert a smart card into smart card reader 1.

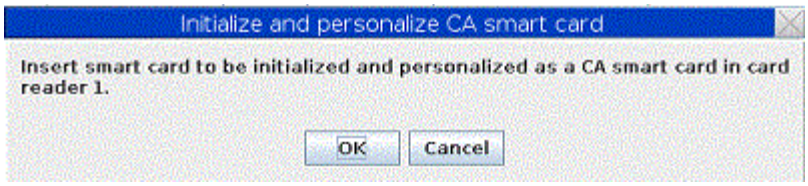


Figure 250. First step for initialization and personalization of the CA smart card

3. A dialog box displays, prompting you to select the zone key length. The zone key length can be either 1024 bit or 2048 bit.





Figure 251. Zone key length window

4. If the smart card is not empty, a message is displayed indicating that the smart card is not empty and all data will be overwritten. If this is acceptable, click **OK**.

Notes:

- The zone key length options you see are based on the type of smart card you have:
  - Only blue smart cards supports the 521-bit ECC key zone key length.
  - Blue CA smart cards never have a zone key length of 1024-bit RSA.
- If you create a CA with a zone key length of 521-bit ECC, all the smart cards enrolled in the zone have to be blue smart cards.

- 1024-bit RSA should not be used because it is considered too weak.

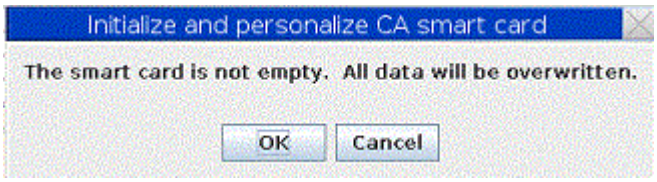


Figure 252. Message if card is not empty

5. The smart card will now be initialized.

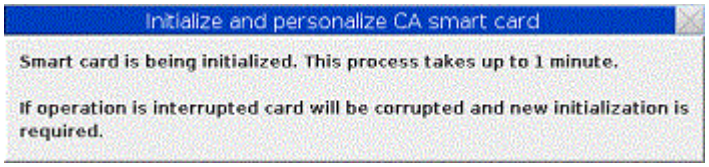


Figure 253. Initialization message for CA smart card

6. At the next prompt, enter a 6-digit PIN number twice. This is the first CA smart card PIN.

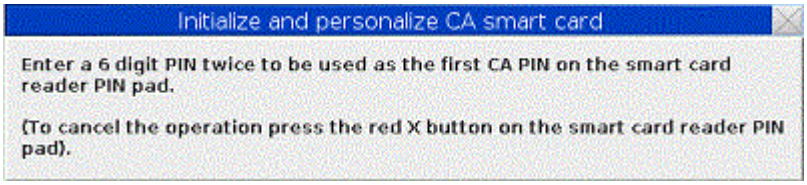


Figure 254. Enter first PIN for CA smart card

7. At the next prompt, enter a 6-digit PIN number twice. This is the second CA smart card PIN. For dual control, it is recommended that different administrators enter the first and second CA smart card PIN and the PINs should not be the same.

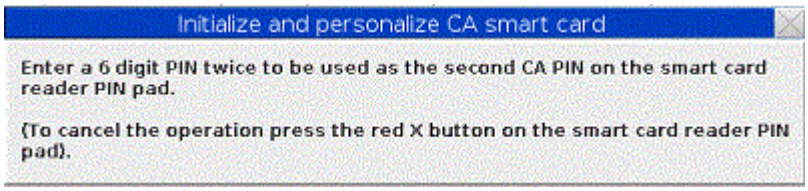


Figure 255. Enter second PIN twice for CA smart card

8. A dialog displays, prompting you to enter a zone description. A zone description helps you visually identify which zone you are using so ensure that each zone you make has a unique description.

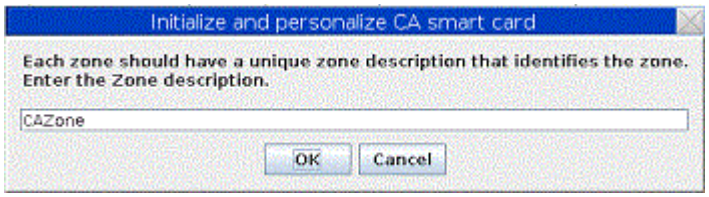


Figure 256. Enter zone description for CA smart card

9. A dialog displays, prompting you to enter a CA smart card description. A smart card description helps you visually identify a smart card so ensure that each smart card you make has a unique description. After the description is entered, the CA smart card is built.

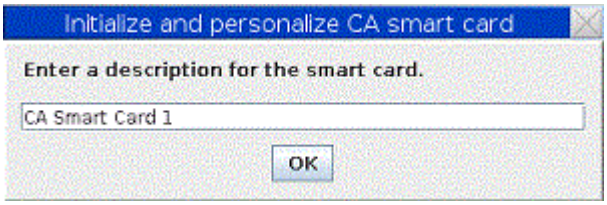


Figure 257. Enter card description for CA smart card

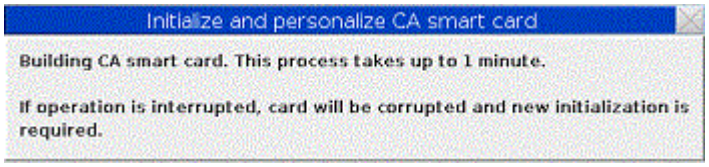


Figure 258. Building a CA smart card

10. You get a message that a CA smart card was successfully created.

Create a backup CA smart card

The CA smart card defines the zone. If the CA smart card is lost or blocked, the administrator is not able to initialize and enroll TKE smart cards, unblock TKE smart cards, or enroll TKE workstation crypto adapters in the zone. It is recommended that the CA smart card is backed up and stored in a secure place.

Note: Although Datakey smart cards are no longer supported in TKE 7.0 or later, you can still back up CA smart cards to IBM part number 45D3398, 74Y0551, or 00JA710 smart cards.

To back up a CA smart card, follow these steps:

1. From the *CA Smart Card* drop down menu, select the *Backup CA smart card* option.
2. When prompted, insert the CA smart card to be backed up into smart card reader 1.

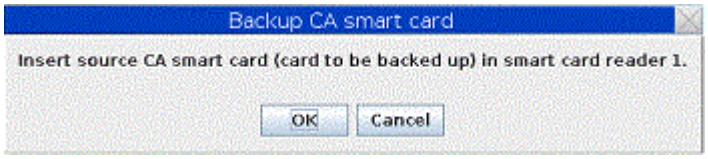


Figure 259. Begin creation of backup CA smart card

3. Enter the first CA smart card PIN.
4. Enter the second CA smart card PIN.
5. Insert the target CA smart card in smart card reader 2.
6. If the target smart card is not empty, you are asked to overwrite all of the data on the smart card.
7. The target smart card is initialized.

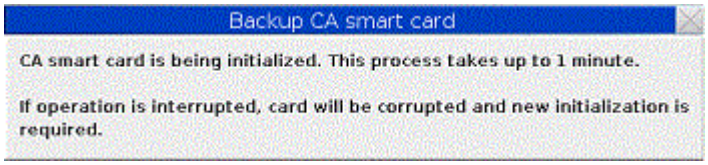


Figure 260. Initialization of backup CA smart card

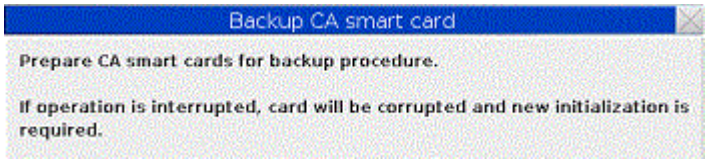


Figure 261. Continue creation of backup CA smart card

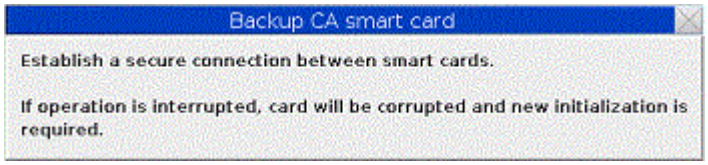


Figure 262. Establish secure connection for backup CA smart card

8. At the prompts, enter the first and second CA PINs of the original CA smart card on the smart card reader 2.

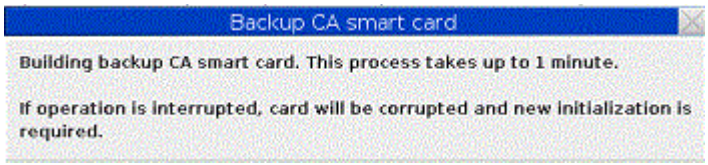


Figure 263. Building backup CA smart card

9. You get a message that a CA smart card was successfully copied.

Change the CA smart card PINs

To change the PIN of a CA smart card, follow these steps:

1. From the *CA Smart Card* drop down menu, select *Change PIN* option.
2. Insert the CA smart card in smart card reader 1.
3. A dialog displays, prompting you to select either first CA PIN or second CA PIN.

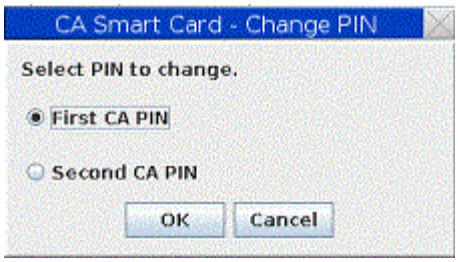


Figure 264. Select first CA PIN

4. Enter the current 6-digit PIN once.
5. Enter the new PIN twice — when prompted.
6. You will get a message that the PIN was successfully changed.

TKE smart card menu functions

The purpose of a TKE smart card is to hold key material for CCA host crypto modules (CEX2C, CEX3C, CEX4C, CEX5C, CEX6C, and CEX7C crypto modules). Before the TKE smart card can hold key material, however, it must be initialized and personalized. The TKE Smart Card menu contains options for initializing and personalizing a TKE smart card. Menu options are also available to unblock and change the smart card's PIN.

Initialize and enroll a smart card

In general, TKE smart cards created on a particular TKE release cannot be used on TKE workstations that are at prior release levels. There are exceptions. See “Smart card usage” on page 47 for more information.

To initialize a TKE smart card, follow these steps:

1. From the *TKE Smart Card* drop down menu, select *Initialize and enroll TKE smart card* option.
2. At the prompt, insert a CA smart card (into smart card reader 1) belonging to the zone you want to enroll the TKE smart card in.
3. Enter the first CA PIN on the PIN pad of smart card reader 1.
4. Enter the second CA PIN on the PIN pad of smart card reader 1.

   Note: If you have entered the two PINs for the CA card, have not restarted SCUP, and have not removed the CA card, the two PINs (of the CA smart card) may not require reentry when you are initializing TKE smart cards. This feature is only used when initializing TKE smart cards. All other functions that require the CA PINs will require reentry every time.
5. At the prompt, insert in smart card reader 2 a smart card to be initialized as a TKE smart card.

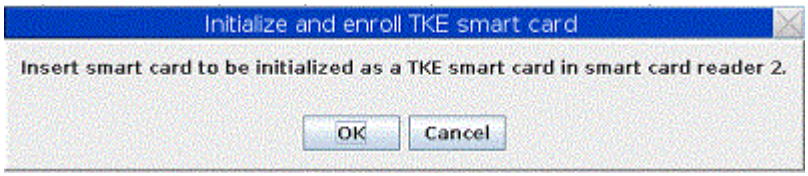


Figure 265. Initialize and enroll TKE smart card

6. If the card is not empty, you will be asked to overwrite all of the data on the smart card.
7. You will see screens indicating that the smart card is being initialized and then the TKE smart card is being built.

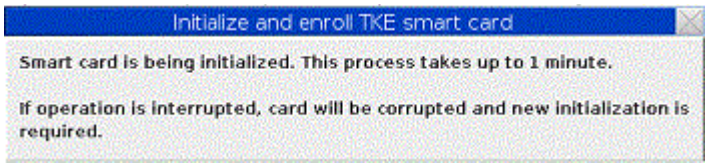


Figure 266. Initializing TKE smart card

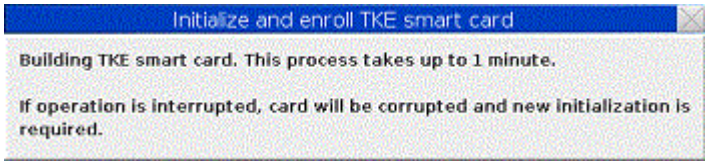


Figure 267. Building TKE smart card

8. When complete, you will get a message that the TKE smart card was successfully created. The TKE smart card must be personalized before it can be used for storing keys and key parts.

Personalize a smart card

To personalize a TKE smart card, follow these steps:

1. From the *TKE Smart Card* drop down menu, select the *Personalize TKE smart card* option.
2. You are prompted to insert an initialized TKE smart card in smart card reader 2.

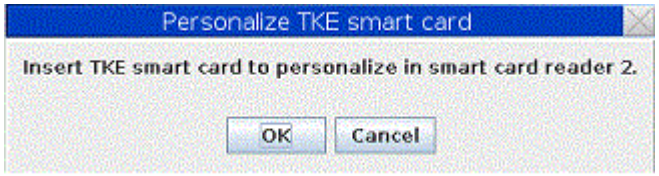


Figure 268. Personalizing TKE smart card

3. A window opens, prompting you to enter a 6-digit PIN twice on the PIN pad of smart card reader 2. Enter the 6-digit PIN when prompted.
4. At the prompt, enter a card description for the TKE smart card. A card description helps you visually tell one TKE smart card from other TKE smart cards so ensure that the card description is unique.
5. When complete, you get a message that the TKE smart card personalization was successful.

Unblock PIN on a smart card

If a TKE smart card PIN is entered incorrectly 3 times, the card becomes blocked and will be unusable until it is unblocked. When you unblock the PIN, the PIN does not change. You still need to enter the correct PIN and will have 3 more attempts to enter the PIN correctly.

To unblock the PIN on a TKE smart card, follow these steps:

1. From the *TKE Smart Card* drop down menu, select *Unblock TKE smart card* option.
2. Insert the CA smart card in smart card reader 1 when prompted.

3. Enter the first CA PIN on the PIN pad of smart card reader 1.
4. Enter the second CA PIN on the PIN pad of smart card reader 1.
5. At the prompt, insert the TKE smart card to be unblocked in smart card reader 2.
6. You will get a message that the TKE smart card was successfully unblocked.

Change PIN of a smart card

To change the PIN of a TKE smart card, follow these steps:

1. From the *TKE Smart Card* drop down menu, select *Change PIN* option.
2. Insert the TKE smart card in smart card reader 2.
3. Enter the current PIN once. For TKE Version 7.0 or later, this is a 6-digit PIN. For versions of TKE before 7.0, this is a 4-digit PIN.
4. At the prompt, enter the new PIN twice.
5. You get a message that the PIN was successfully changed.

Enroll smart card in an alternate zone

To enroll a TKE smart card in an alternate zone:

1. From the *TKE Smart Card* drop down menu, select *Enroll TKE smart card in alternate zone*.

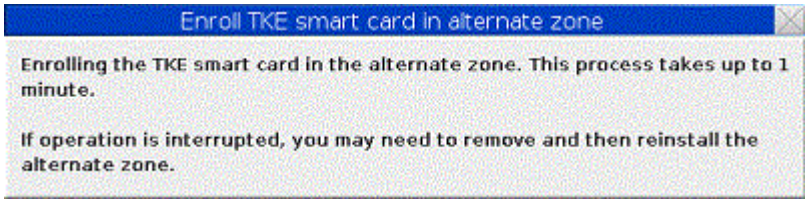


Figure 269. Enroll TKE smart card in alternate zone

2. Insert the CA smart card for the alternate zone in smart card reader 1.
3. Insert the TKE smart card to be enrolled in the alternate zone in smart card reader 2.
4. At the prompts, enter the CA smart card PINs on smart card reader 1.
5. At the prompt, enter the TKE smart card PIN on smart card reader 2.
6. You get a message that the TKE smart card was successfully enrolled in the alternate zone.

Alternate zone restrictions:

- A blue smart card may not have an alternate zone with a key length of 1024-bit RSA. Ff you need to move data onto a blue smart card, see “Moving data from a TKE smart card in a 1024-bit zone to a blue smart card” on page 53.
- Only blue smart cards can have an alternate zone with a key length of 521-bit ECC.

Remove alternate zone from smart card

To remove the alternate zone from a TKE smart card:

1. From the *TKE Smart Card* drop down menu, select *Remove alternate zone from TKE smart card*.
2. Insert the TKE smart card whose alternate zone is to be removed in smart card reader 2.
3. When prompted, enter the TKE smart card PIN on smart card reader 2.
4. You get a message that the alternate zone was successfully removed from the TKE smart card.

EP11 smart card menu functions

The purpose of an EP11 smart card is to hold key material for EP11 host crypto modules (CEX4P, CEX5P, CEX6P, and CEX7P crypto modules). This key material can include P11 master key parts, key parts for TKE

workstation crypto adapter master key registers, a TKE crypto adapter logon key, and an EP11 administrator signature key.

The **EP11 Smart Card** pull-down menu contains the same options as the **TKE Smart Card** pull-down menu, and the EP11 options operate the same as the TKE options.

Crypto adapter menu functions

Enroll a TKE cryptographic adapter in a primary zone

A TKE workstation with a crypto adapter can be enrolled locally or remotely.

Note: Enrolling of the TKE workstation crypto adapter must be done before loading key parts from TKE or EP11 smart cards.

You can check if the TKE workstation crypto adapter is enrolled in a zone from the Crypto Adapter drop down menu: select *View current zone* option. If it is not, a message window will indicate that the crypto adapter is not enrolled in a zone.

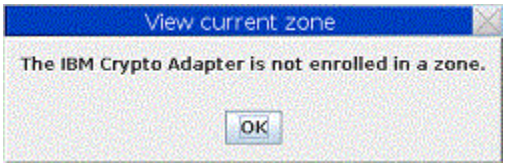


Figure 270. View current zone for a TKE cryptographic adapter

Local TKE workstations that have access to the CA Card may be enrolled locally. If you have offsite TKE workstations without access to the CA card, you may use the remote enroll application to enroll these workstations in the same zone.

If the enroll does not occur as part of the initialization, the current DEFAULT role will not have the necessary ACPs to perform the enroll. You can log on with a profile using SCTKEADM or equivalent authority, or you can reload the TEMPDEFAULT role (see “Managing roles” on page 264). If the TEMPDEFAULT role is used, then, once the enroll is complete, it is critical that the TEMPDEFAULT role be returned to the normal DEFAULT role. The TEMPDEFAULT role cannot be allowed to stay loaded as this role has ACPs for all functions.

Local crypto adapter enrollment

1. From the Crypto Adapter drop down menu, select Enroll Crypto Adapter option.
2. Select *local* when prompted for enrollment type.



Figure 271. Select local zone

3. At the prompt, insert the CA smart card in smart card reader 1.
4. At the prompt, enter the first CA PIN on the PIN pad of smart card reader 1.
5. At the prompt, enter the second CA PIN on the PIN pad of smart card reader 1.
6. You will get a message that the enrollment for the crypto adapter was successful.



Figure 272. Certifying request for local Crypto Adapter enrollment



Figure 273. Message for successful Crypto Adapter enrollment

7. View the zone information after the crypto adapter is enrolled by selecting *View current zone* from the Crypto Adapter drop down menu.

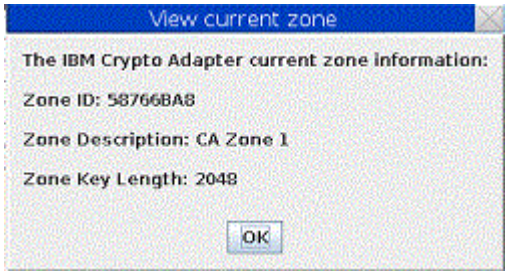


Figure 274. View current zone after Crypto Adapter enrollment

Remote crypto adapter enrollment

The "Begin Zone Remote Enroll Process" and the "Complete Zone Remote Enroll Process" applications work together. You can use them to enroll a TKE workstation in the same zone as another TKE workstation at a remote site when you do not have the CA smart card at the site where the TKE workstation to be enrolled is located. Use remote enrollment only under the following conditions:

- The TKE workstation that is to be enrolled in the zone is not at the same location as the TKE that is enrolled in the zone.
- The CA smart card is not available (and will never be available) at the site where the TKE workstation that must be enrolled is located.

Guideline: It is highly preferable that CA smart cards be available at both locations and that you use local zone enrollment in place of remote enrollment.

Note: Without a CA smart card, you cannot create any TKE or EP11 smart cards. Instead, you must create TKE and EP11 smart cards at the location with the CA smart card, and send them to the location without the CA smart card.

The following tasks are required to complete the remote zone enrollment on a TKE:

1. Task 1: If necessary, format a USB flash memory drive for Trusted Key Entry data. For more information, see “Formatting a USB flash memory drive for Trusted Key data (task 1)” on page 307.
2. Task 2: Create a remote zone enrollment request.

   From the TKE workstation that is to be enrolled, use the "Begin Zone Remote Enroll Process" application to create an enrollment request file. After the request file is created, it must be taken to the TKE that is enrolled in the zone. For more information, see “Creating a remote zone enrollment request (task 2)” on page 307.
3. Task 3: Process the remote zone enrollment request.

From the TKE workstation that is enrolled in the zone, use the "remote enrollment" function of the smart card utility program (SCUP) to process the request. This function produces an enrollment certificate file. After the certificate file is created, it must be taken back to the TKE that is to be enrolled in the zone. For more information, see “Processing the remote zone enrollment request (task 3)” on page 308

Requirement: The SCUP remote enroll operation requires a CA smart card.

4. Task 4: Complete the remote zone enrollment.

   From the TKE workstation that is to be enrolled, use the "Complete Zone Remote Enroll Process" application to finish the zone enrollment. For more information, see “Completing the remote zone enrollment (task 4)” on page 309.

Formatting a USB flash memory drive for Trusted Key data (task 1)

This task is the first task in the remote zone enrollment process. You can use a USB flash memory drive to move files between the TKE workstation that is going to be enrolled and the TKE workstation that is already enrolled in the zone. The USB flash memory drive must be formatted for Trusted Key Entry data.

About this task

If your USB flash memory drive is not formatted for Trusted Key Entry data, follow these instructions. Otherwise, skip to the next task, “Creating a remote zone enrollment request (task 2)” on page 307

Procedure

1. Install the USB flash memory drive in any open USB port and wait for the device to report in.
   It can take up to 30 seconds.
2. From the Trusted Key Entry console, click **Service Management**.
3. Open the **Format Media** application.
4. Click **Trusted Key Entry data**.
5. Click **Format**.
6. Click the choice for your USB flash memory device.
7. Click **OK**
   The format process starts.
8. Click **Format**. Do not change the file system format.
9. Click **Yes** to allow the media to be overwritten.
   A window with a completion message opens when the format process is complete.
10. Click **OK** to close the message window.

Results

The USB flash memory drive is formatted for Trusted Key Entry data. Continue to the next task, “Creating a remote zone enrollment request (task 2)” on page 307.

Creating a remote zone enrollment request (task 2)

This task is the second task in the remote zone enrollment process.

Before you begin

- You must have a USB flash memory drive that is formatted for Trusted Key Entry data. For more information, see “Formatting a USB flash memory drive for Trusted Key data (task 1)” on page 307.
- You must know the strength of the zone in which you are enrolling. It is either 1024 or 2048.

About this task

Perform this task on the TKE workstation that is to be enrolled in the remote zone.

Attention: After you complete this task, you must not reset the device key on this TKE workstation before you complete the zone enrollment. If you do, the remote zone enrollment fails and you must restart the remote zone enrollment process. Specifically, you must not take any of the following actions:

- Use the Cryptographic Node Management utility to initialize the TKE workstation's local crypto adapter.
- Use the TKE workstation's Crypto Adapter initialization application to initialize the TKE's local crypto adapter.
- Locally enroll the TKE in a zone.

If you take any of these actions, the error `exception during application install` is issued at the end of task 4.

Procedure

1. Install the USB flash memory drive that is formatted for Trusted Key Entry data.
2. From the Trusted Key Entry console, click **Trusted Key Entry**.
3. Open the "Begin Zone Remote Enroll Process" application.
4. If necessary, log on to the crypto adapter.
5. Click **Yes** when you see the message `Begin remote enroll`.
6. Respond to the message about the remote zone key length:
   - Click **Yes** if the strength of the zone is 1024.
   - Click **No** if the strength of the zone is 2048.
7. If you are prompted to confirm the 2048 zone strength, click **Yes**.
8. If you are prompted to confirm that the existing enrollment is to be replaced, click **Yes**.

   Note: This step removes the TKE workstation from its current zone. The TKE workstation is not enrolled in a zone until the entire remote crypto adapter enrollment process is complete. If you cancel the process after this point, you must restart and complete the remote crypto adapter enrollment process or perform a local "enroll crypto adapter" operation from the Smart Card Utility program.
9. When the "save the enrollment request file" window opens, respond:
   - Click **USB Flash Memory drive**
   - Enter a file name. For example, `MyEnrollmentRequestForTKExxxx`
   - Click **Save**.
10. When a window opens with a completion message, click **OK** to close the window.
11. When a window opens with a logoff message, click **OK**.

    Either logoff option is acceptable.
12. Remove the USB flash memory drive and send it to the remote location of the TKE that is enrolled in the zone.

Results

You created a remote zone enrollment request, saved the request to a USB flash memory drive, and sent the drive to the remote location. Continue to the next task, "Processing the remote zone enrollment request (task 3)" on page 308.

Processing the remote zone enrollment request (task 3)

This task is the third task in the remote zone enrollment process.

Before you begin

- You must have the CA smart card.

- You must have the USB flash memory drive that has the enrollment request file. This file was created in task 2 (“Creating a remote zone enrollment request (task 2)” on page 307.

About this task

Perform this task on the TKE workstation that is enrolled in the zone.

Procedure

1. Install the USB flash memory drive that has the enrollment request file on the TKE workstation.
2. From the Trusted Key Entry console, click **Trusted Key Entry**.
3. Open the Smart Card Utility Program (SCUP).
4. If necessary, log on to the crypto adapter.

   You must log on with a profile that has TKEADM, SCTKEADM, or equivalent authority.
5. Click **Crypto Adapter > Enroll Crypto Adapter**.
6. Click **Remote**.
7. Click **OK**.

   A window opens with a message that asks if the file is available.
8. Click **OK**.
9. Insert the CA smart card in reader 1 and press the **OK** button.
10. Enter the PINs when you are prompted.

    The **"open file that contains enrollment request"** window opens.
11. Open the enrollment request file.
    a) Select **USB Flash Memory drive**.
    b) Select the enrollment request file that was created in task 2.
    c) Click **Open**.

    A window with the message `do you want to enroll this adapter` opens.
12. Click **OK.**

    An enrollment certificate chain is created. A window with the message `enrollment has been granted` opens.
13. Save the enrollment certificate chain on the USB flash memory drive.
    a) Click **USB Flash Memory drive**.
    b) Enter a file name.
    For example, `EnrollmentCertForTKExxxx`.
    a) Click **Save**.
14. Click **OK** on the informational message.
15. Click **File > Exit and Logoff** to close the SCUP application.
16. Remove the USB flash memory drive and send it to the location of the TKE workstation that is to be enrolled in the zone.

Results

An enrollment certificate was created and saved to the USB flash memory drive. Continue to the next task, “Completing the remote zone enrollment (task 4)” on page 309.

Completing the remote zone enrollment (task 4)

This task is the fourth and last task in the remote zone enrollment process.

Before you begin

You must have the USB flash memory drive that contains the enrollment certificate file that was created in task 3 (“Processing the remote zone enrollment request (task 3)” on page 308).

About this task

Perform this task on the TKE workstation that is to be enrolled in the remote zone.

If you receive the error `exception during application install` during this task, you probably reset the device key before you completed the zone enrollment. You must restart the remote zone enrollment process. For more information, see "Creating a remote zone enrollment request (task 2)" on page 307.

Procedure

1. Install the USB flash memory drive that contains the enrollment certificate file on the TKE workstation.
2. From the Trusted Key Entry console, click **Trusted Key Entry**.
3. Open the application "Complete Zone Remote Enroll Process for a Crypto Adapter".
4. If necessary, log on to the crypto adapter.
5. Click **Yes** on the **"Complete remote enroll"** window.
6. If necessary, click **Yes** to allow the enrollment to replace an existing enrollment.
7. Open the enrollment request certificate.
   a) On the **"open the enrollment request certificate"** window, select **USB Flash Memory drive**.
   b) Select the enrollment certificate that you created in task 3.
   c) Click **Open**.

   A window opens with the message `Crypto adapter has been enrolled`.
8. Click **Yes**.

   A window opens with a logoff message.
9. Click **Yes**.

   Either logoff option is acceptable.

Results

The remote zone enrollment is complete.

View current zone for the crypto adapter

Use the View current zone function to determine the current zone of the TKE workstation crypto adapter. You may want to compare it to the zone of a TKE or EP11 smart card when working with key parts.

To view the current zone of the TKE workstation crypto adapter, follow these steps:

1. From the *Crypto Adapter* drop down menu, select *View current zone* option.

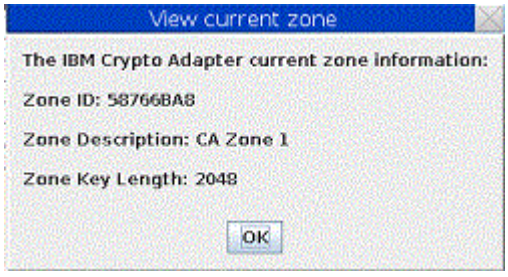


Figure 275. View current zone after crypto adapter enrollment

A window is returned with the Zone ID, Zone Key Length, and the Zone description (if you had previously entered a zone ID description).

Remove current zone from the crypto adapter

When you run this function, the TKE will no longer be enrolled in a zone.

Appendix A. Secure key part entry

This topic describes how you can enter a known key part value onto a TKE or EP11 smart card. A known key part will have been saved on paper or in a binary file.

Secure Key Part Entry allows migration of existing key parts to TKE or EP11 smart cards and provides an additional mechanism for key part entry. Using the PIN pad on the smart card reader, the key part can be stored on a smart card. You must enter the key part hexadecimal digits on the smart card reader key pad. See “Entering a key part on the smart card reader” on page 318.

By entering the key part on the PIN pad, the key part can be stored securely and any clear copies of the key part can be destroyed. Once stored on the smart card, the user should use the TKE to securely copy the key part to another smart card that is enrolled in the same zone for a backup. The user can then load the key part into key storage or onto the host.

Key parts for CCA host crypto modules (CEX2C, CEX3C, CEX4C, CEX5C, CEX6C, and CEX7C) are saved on TKE smart cards. Key parts for EP11 host crypto modules (CEX4P, CEX5P, CEX6P, and CEX7P) are saved on EP11 smart cards.

Steps for secure key part entry

The steps you need to follow for secure key part entry differ depending on whether you are entering the key parts on a TKE or an EP11 smart card.

Steps for secure key part entry for a TKE smart card

For CCA host crypto modules, secure key part entry begins from the Crypto Module Notebook Domains tab's Keys tab by right-clicking the desired key type for entry. Right-clicking the desired key type reveals a menu with an entry for secure key part.

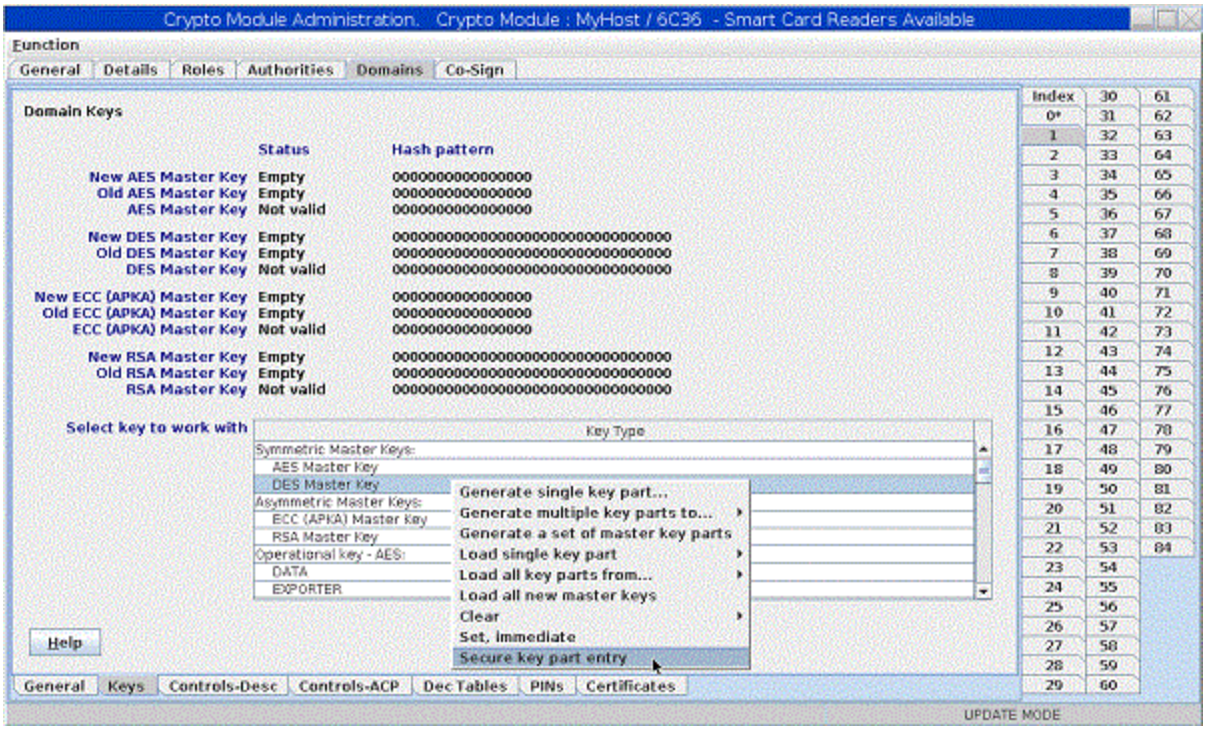


Figure 276. Choosing secure key part entry from the domains keys panel

This menu entry is available for all supported crypto module types.

© Copyright IBM Corp. 2000, 2021

1. Select **Secure key part entry**.

   For master keys on all host crypto modules, a panel for entering a key part description displays.



Figure 277. Enter description panel for secure key part entry

   For DES operational keys, the Secure Key Part Entry window opens.

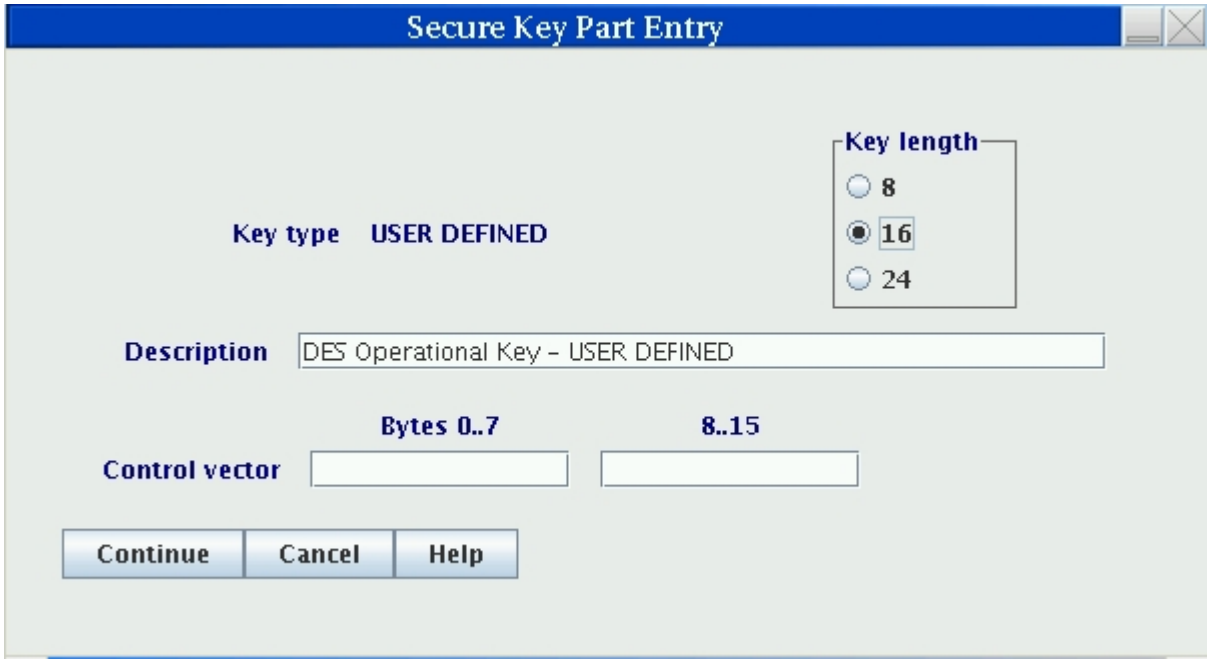


Figure 278. DES USER DEFINED operational key for secure key part entry

   For a DES USER DEFINED operational key, the user is allowed to update the description, the key length, and the control vector.

   For a predefined DES operational key or AES DATA operational key, only the description can be updated, unless the key type supports multiple key lengths. In that case, the key length field can also be updated. For a predefined DES operational key or AES DATA operational key, the control vector cannot be updated.

   For AES operational keys other than DATA, the following Secure Key Part Entry window opens.

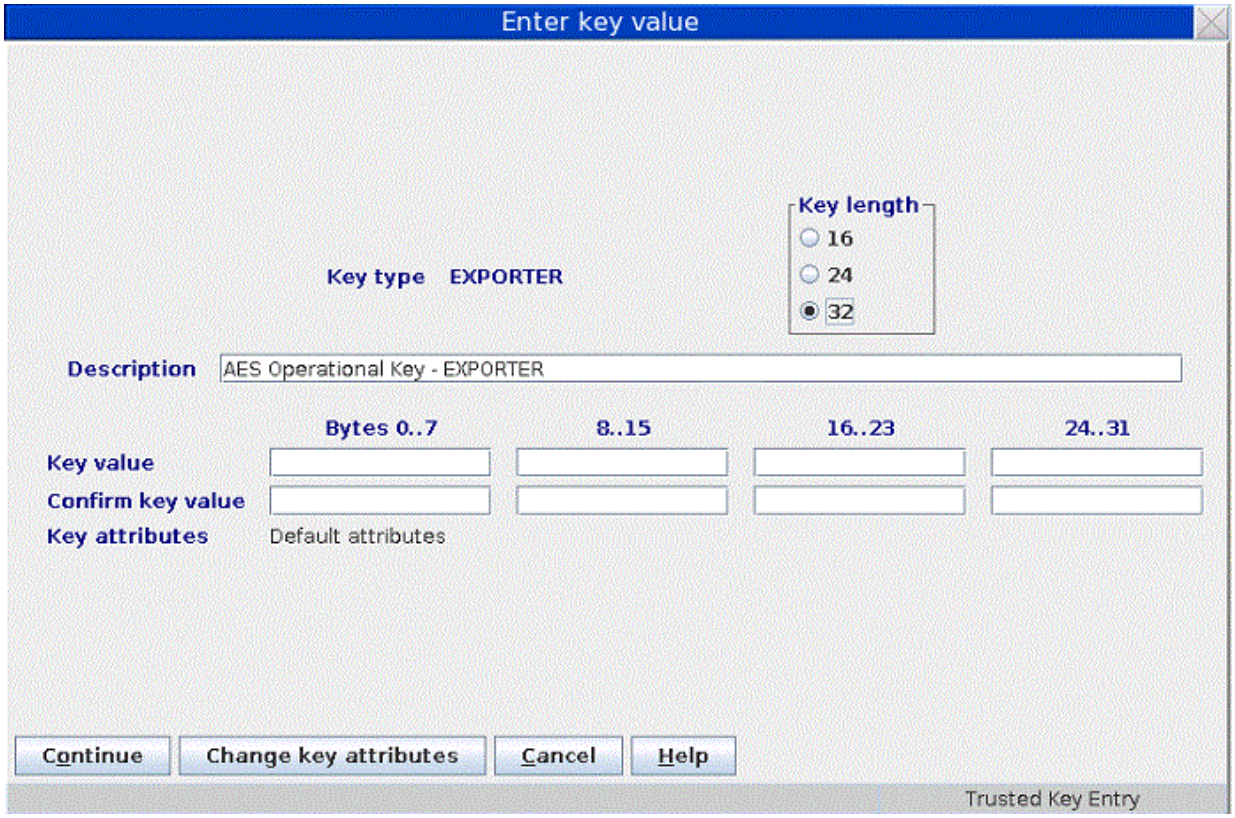


Figure 279. AES non-DATA operational key for secure key part entry

The key part description can be updated. Click **Change key attributes** to modify the key attributes.

2. After all the appropriate information has been entered for master and operational keys, the user is prompted to insert a TKE smart card into reader 2.



Figure 280. Secure key part entry — insert TKE smart card into reader

3. Enter the PIN on the smart card reader PIN pad when prompted.

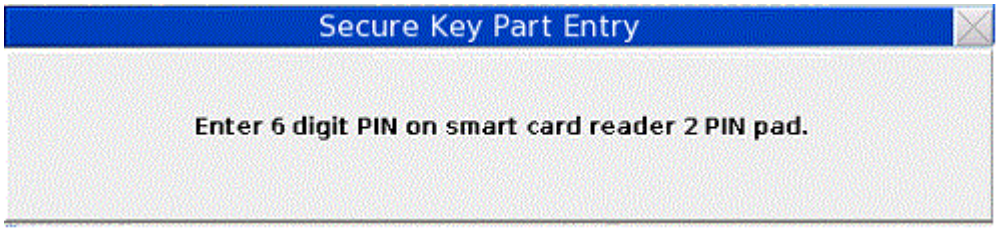


Figure 281. Secure key part entry — enter key part digits

A dialog displays information about the TKE smart card.

4. If the TKE smart card information is correct, press **Yes** to continue.

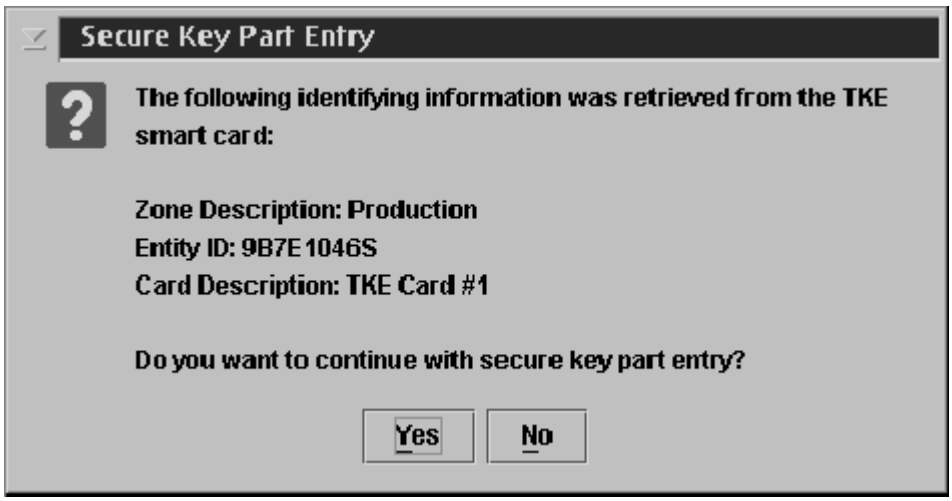


Figure 282. Secure key part entry card identification

The Secure Key Part Entry dialog displays.

5. Enter the known key part digits, which will have been saved on paper or in a binary file. See "Entering a key part on the smart card reader" on page 318.

   Note: Make sure that the TKE workstation crypto adapter and the TKE smart cards are in the same zone. To display the zone of a TKE smart card, exit TKE and use either the Cryptographic Node Management Utility or the Smart Card Utility Program under Trusted Key Entry Applications. See "Display smart card information" on page 294 or "Display smart card key identifiers" on page 296.

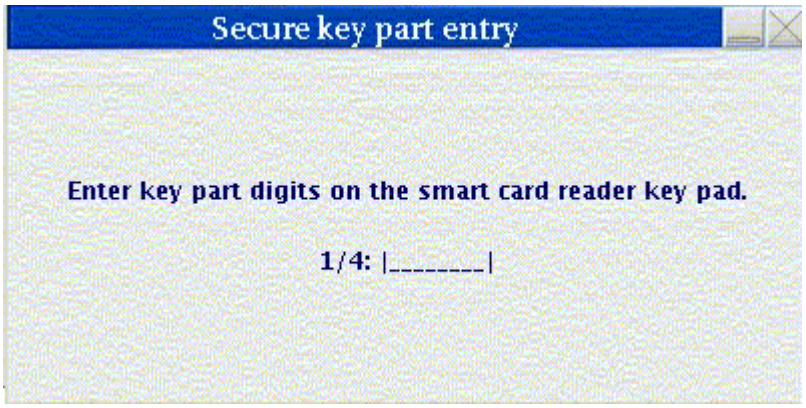


Figure 283. Secure key part entry — enter key part digits

The dialog shows the progress of each hexadecimal digit entered with an asterisk (*).

6. After the key part value has been successfully entered on the PIN pad, a window opens showing information about the key part just entered. Verify that you entered the information correctly.
   - For a DES key part, the ENC-ZERO, MDC-4, and SHA1 values are shown.
   - For an AES or ECC (APKA) key part, the AES-VP value is shown.
   - For a DES or AES DATA operational key, the control vector (CV) is also displayed.
   - For an AES non-DATA operational key, the window allows you to display key attributes.

   Click **OK** to continue.



Figure 284. Secure key part entry — DES key part information for a master key



Figure 285. Secure key part entry — AES key part information for a master key



Figure 286. Secure key part entry — DES key part information for operational key

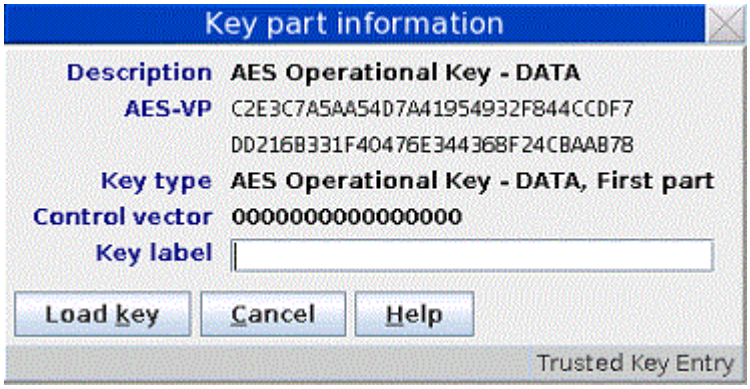


Figure 287. Secure key part entry — AES DATA operational key

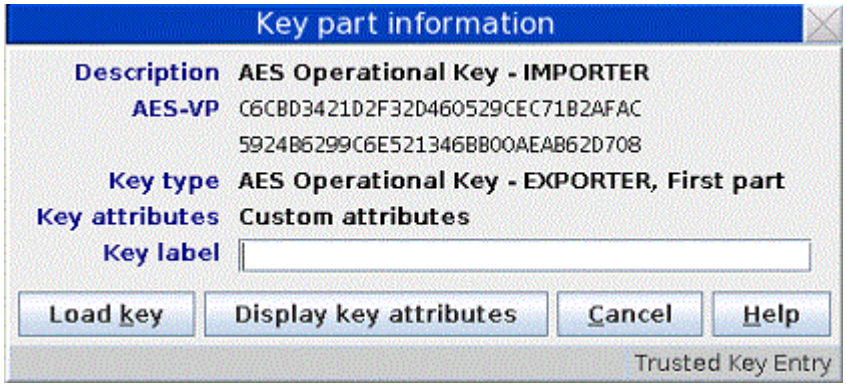


Figure 288. Secure key part entry — AES non-DATA key

7. A message is displayed if the command executed successfully.

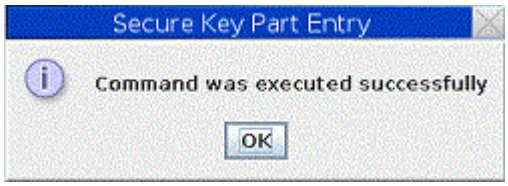


Figure 289. Secure key part entry — message for successful execution

Steps for secure key part entry for a EP11 smart card

For EP11 host crypto modules, secure key part entry begins from the **Keys** tab for a domain in the Crypto Module Notebook. Right-click in the domain keys window to display a menu, and click **Secure key part entry**.

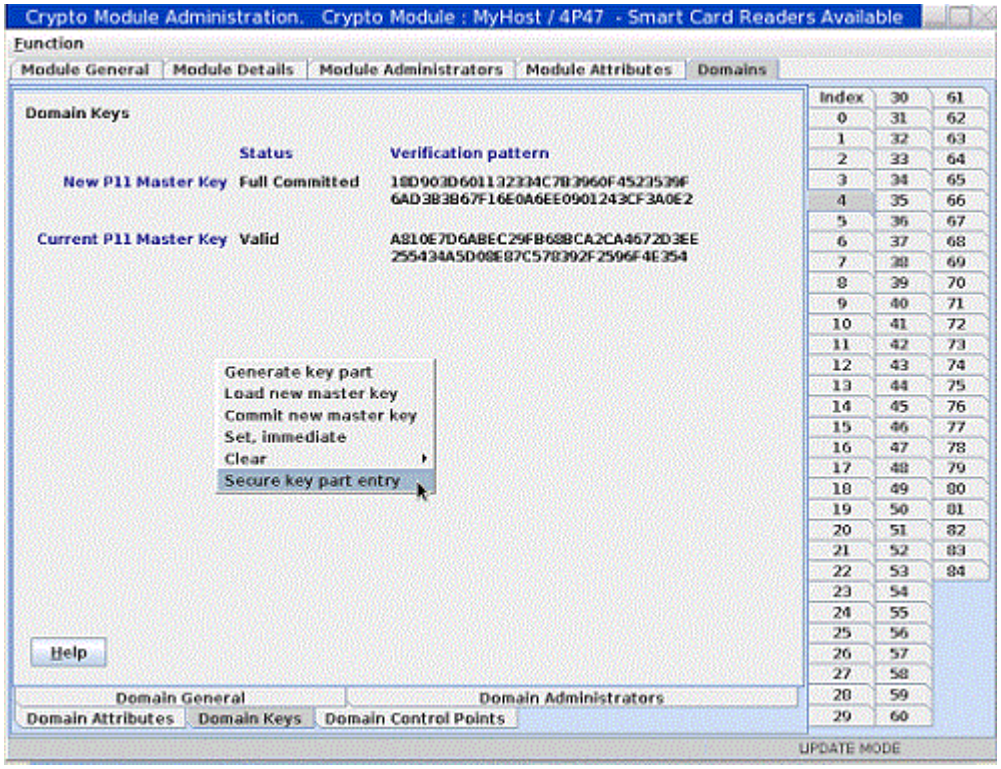


Figure 290. Choosing secure key part entry from the domain keys window

You are prompted to enter a description for the key part. After entering the description, you are prompted to select the smart card reader to use, to insert an EP11 smart card in the reader, and to enter the PIN. After the PIN is entered, a confirmation window opens showing the smart card's zone description, entity ID, and card description.



Figure 291. Secure key part entry card identification

Note: The smart card must be in the same zone as the TKE workstation crypto adapter in order for secure key part entry to be successful.

If you accept this smart card, you are prompted to enter the hexadecimal digits for the key part on the smart card reader PIN pad. To enter each hexadecimal digit, you must press two buttons on the PIN pad. For example, press "0" and "2" for the hexadecimal digit 2, or "1" and "4" for the hexadecimal digit E. After each hexadecimal digit is entered, an asterisk (*) is displayed on the panel to show how many hexadecimal digits have been entered.

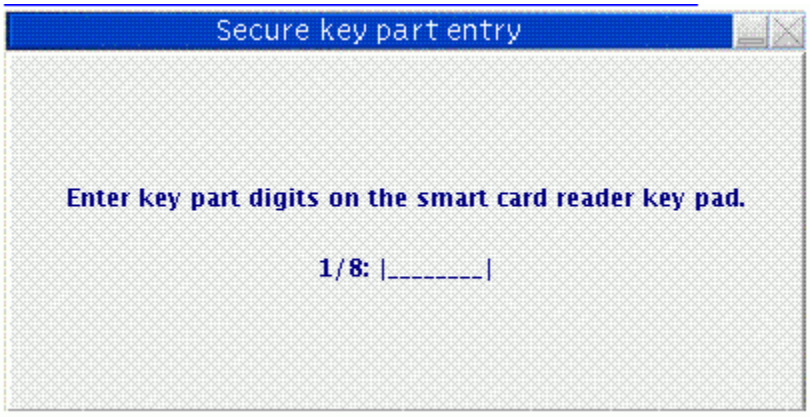


Figure 292. Secure key part entry -- enter key part digits

After all hexadecimal digits for the key part have been entered, a Smart Card key part information window opens showing the AES-VP for the key part that was entered.

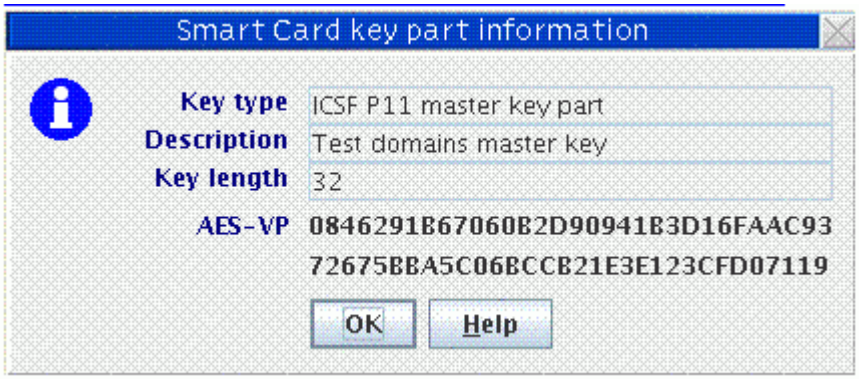


Figure 293. Secure key part entry -- key part information window

Entering a key part on the smart card reader

A key part is hexadecimal. The PIN pad on the smart card reader does not provide hexadecimal digits, so you must enter two digits that represent the decimal equivalent of a hexadecimal digit. The valid range of decimal digit input is 00–15. This range is equivalent to the hexadecimal digit input range of 0–F. A conversion table is provided (Table 36 on page 319).

Except for RSA keys, all other key types for all crypto module types can be entered securely on the smart card reader PIN pad. These key parts can then be used to load master or operational key registers on the host.

Secure key part entry on the smart card reader PIN pad works as follows:

- A key part is separated into blocks. The key length in bytes (2 hexadecimal characters per byte) is divided by 4 and gives you the number of blocks.
- A block on the smart card reader PIN pad consists of 8 hexadecimal digits.
- Once a hexadecimal digit has been entered, the value cannot be changed.
- After entering the two digit decimal equivalent, the smart card reader records a hexadecimal digit, updating the smart card reader display with an '*' in the section depicting the number of hexadecimal digits that have been recorded in the current block.
- After all the hexadecimal digits in a block have been entered, a running counter of the number of blocks completed on the screen is updated and the current block display is reset.
- Once a block is updated with a hexadecimal digit, the values cannot be changed.

- On the OmniKey reader, there is blank space for entering the two decimal digits. A single lock image is depicted on the right.
- The current decimal digit input can be changed. If an invalid two decimal digit input is entered, a change must occur. The Backspace key (yellow button labeled with a <-) on the smart card reader PIN pad can be used to undo entered decimal digits. The <- button lets the user change the first decimal of the hex digit. Example: if you entered 0_ you can use the <-button to reenter the 0. The abort key (red button labeled with an X) on the smart card reader PIN pad can be used to reset the current decimal digit. It can also be used to cancel the secure key entry process.

Example

Key part type: 8-byte DES data operational key
Key part hexadecimal digits: AB CD EF 12 34 56 78 90
Number of blocks: 2
Number of hexadecimal digits per block: 8
Initial Block Counter Value: 1/2
Two decimal digit conversion of key part hexadecimal digits:
1011 1213 1415 0102 0304 0506 0708 0900

Table 36. Decimal to Hexadecimal Conversion Table

Hexadecimal Digit	Decimal Digits Entered on PIN PAD
0	00
1	01
2	02
3	03
4	04
5	05
6	06
7	07
8	08
9	09
A	10
B	11
C	12
D	13
E	14
F	15

Appendix B. LPAR considerations

Host image profiles for logical partitions must be correctly configured in order to use the TKE workstation to manage keys and perform other operations. The host support element is used to set and change the configuration.

When customizing an image profile using the support element, four fields are specified:

- **Usage domain index** – The domain associated with the logical partition.
- **Control domain index** – The set of domains that can be managed from this logical partition. It must include the usage domain index value for this logical partition. A logical partition used as the TKE host includes the usage domain index values for all logical partitions the TKE workstation may manage.
- **Cryptographic Candidate List** – The set of cryptographic coprocessors that the logical partition may access.
- **Cryptographic Online List** – The set of cryptographic coprocessors that will be brought online when the logical partition is activated.

You must be running CSFTTCP on at least one LPAR on each machine. It is best to do all module administration for a single machine from a single LPAR. You can do this if you make all domains 'control domains' for the LPAR that is running CSFTTCP. You may want to run CSFTTCP on two LPARs on the same machine if you want TKE to have a second LPAR to use if needed. However, you should build your TKE domains groups such that you do all module administration using as few LPARs on each machine as possible.

If a command is sent to a domain that is not in a logical partition's control domain index, ICSF returns an error (return code 12, reason code 2015).

There is no specific field to identify a logical partition as a TKE host when you are customizing image profiles. You must decide which logical partition will be the TKE host and set up the control domain index and Cryptographic Candidate List appropriately. The control domain index for this partition must include the usage domain index values for all logical partitions that the TKE workstation will control, and the Cryptographic Candidate List for this partition must include all entries in the Cryptographic Candidate Lists for the logical partitions that the TKE workstation will control. The control domain index must also include the usage domain index value for the TKE host partition itself.

Multiple logical partitions can specify the same usage domain index, provided there are no common entries on their Cryptographic Candidate Lists. (Logical partitions may not share the same domain on the same cryptographic coprocessor, but can use the same domain index value on different cryptographic coprocessors.) In order to control these partitions, however, the TKE host partition must have a unique usage domain index, because its Cryptographic Candidate List must include all coprocessors of the logical partitions being controlled.

The example in Figure 294 on page 322 has 3 LPARs and 4 cryptographic coprocessors: 00, 01, 02, 03. There is no domain sharing. In this case, all the cryptographic coprocessors can be specified in the Candidate List for each LPAR.

© Copyright IBM Corp. 2000, 2021

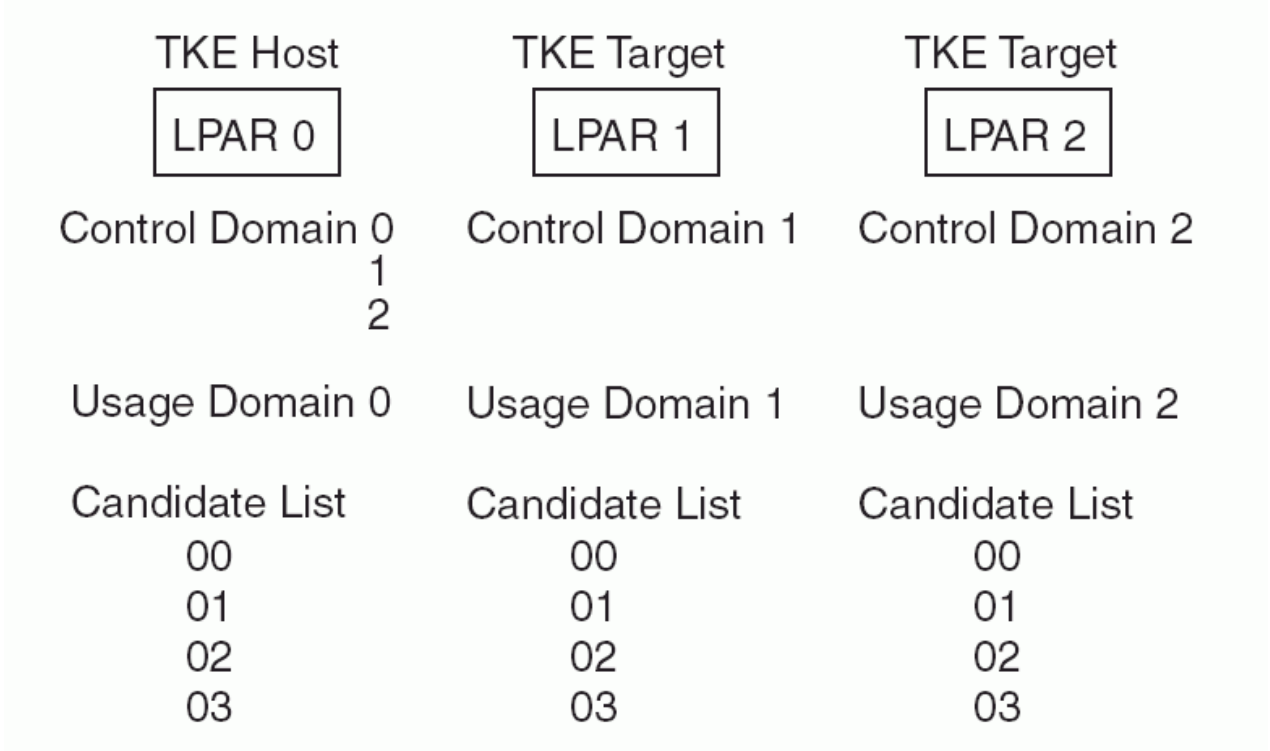


Figure 294. An example of TKE host and TKE target LPARs without domain sharing

The example in Figure 295 on page 322 has 4 LPARs, 2 sharing the same domain and 4 cryptographic coprocessors: 00, 01, 02, 03. In this case, LPAR 1 and LPAR 2 share the same domain, but the Candidate List does not share any of the same cryptographic coprocessors.

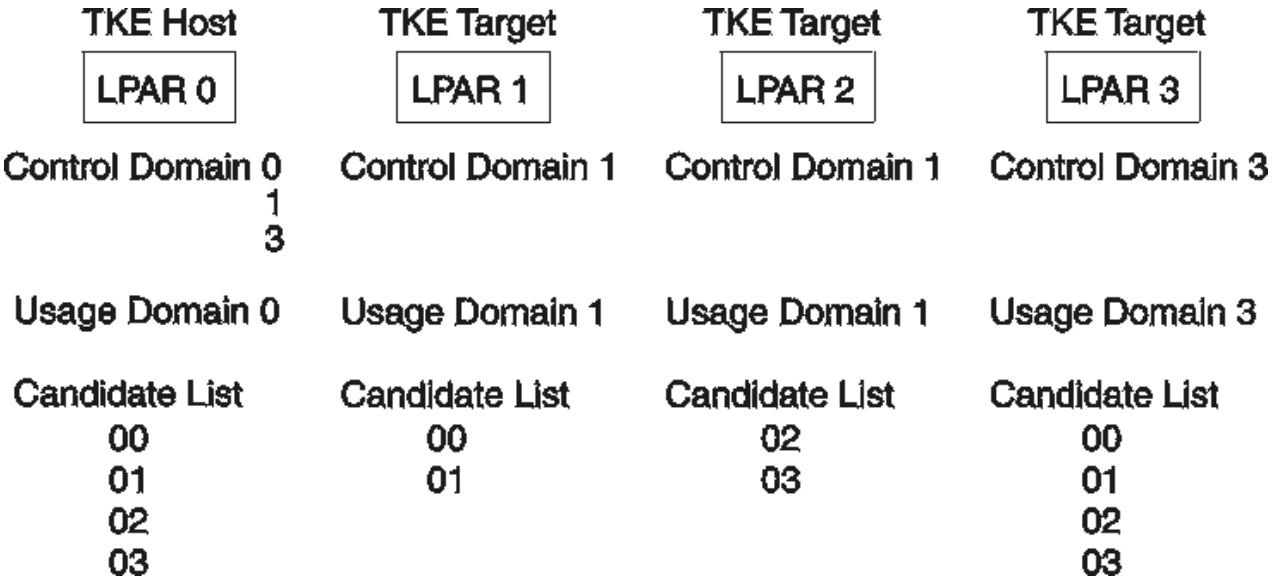


Figure 295. An example of TKE host and TKE target LPARs with domain sharing

If the same domain is specified by more than one LPAR and the Candidate List has any of the same cryptographic coprocessors, the first LPAR that is activated will IPL without error, but the other LPARs with the same domain will fail activation.

Appendix C. Trusted Key Entry - workstation crypto adapter initialization

Cryptographic Node Management Batch Initialization

The Cryptographic Node Management Batch Initialization task allows the user to execute user-created scripts.

User-defined scripts can be created using the CNI editor in the Cryptographic Node Management utility. Open the Cryptographic Node Management utility. Click **File** and select **CNI Editor**.

All scripts must be run from a USB flash memory drive or CNM data directory. User-created scripts can be used to further initialize the TKE workstation crypto adapter after passphrase or smart card initialization has been done. For details on initializing the TKE workstation crypto adapter for passphrase or smart card use, see "Initializing the TKE workstation crypto adapter for use with passphrase profiles" on page 85 and "Initializing the TKE workstation crypto adapter for use with smart card profiles" on page 85.

To execute a user-defined CNI script, click **Trusted Key Entry**, and then **Cryptographic Node Management Batch Initialization**. You must be logged onto the console as ADMIN to access this task. The **Select CNI file to Run** window opens. Select the location (USB flash memory drive or CNM data directory) and the file name of the CNI to execute. Click **Open**.

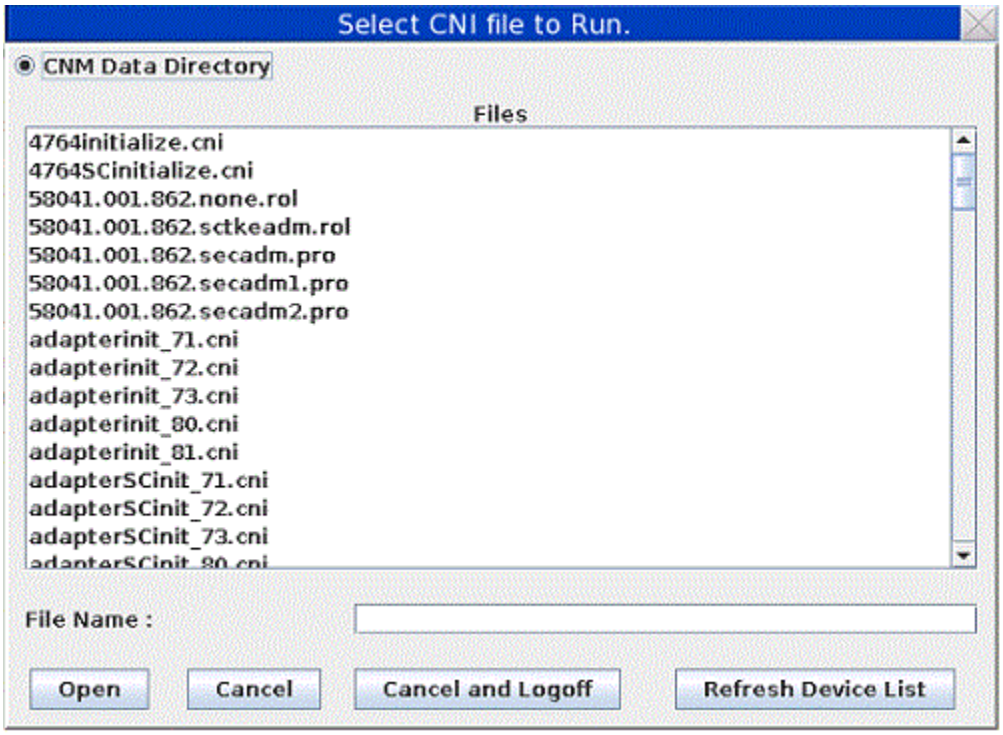


Figure 296. Cryptographic Node Management Batch Initialization task window

The output window shows the operations performed. Click **OK** to exit this task.

© Copyright IBM Corp. 2000, 2021

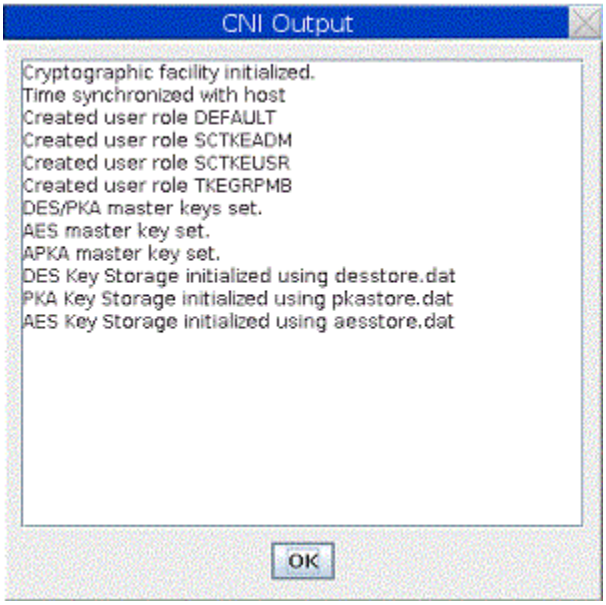


Figure 297. Cryptographic Node Management Batch Initialization task output window

CCA CLU (Code Load utility)

The CCA CLU task is used for loading and checking code on the TKE workstation crypto adapter.

CLU requires exclusive access to the TKE workstation crypto adapter. No other TKE applications can use the TKE crypto adapter while CLU is active, and no TKE crypto adapter user can be logged on. If TKE audit record upload is active at the time CLU is started, audit records are not uploaded to the host system until CLU is ended.

Note: CLU should be executed only when directed by support system. CLU functions can take several minutes to execute.

To invoke the CLU utility, click **Trusted Key Entry**, then select **CCA CLU**. You must be logged on as ADMIN to access this task.

Note: The CCA levels that are depicted in the screen captures might not be entirely accurate due to CCA fixes that might have been made to your system.

CLU processing

When CLU is invoked, the Non-Factory Mode is displayed. You can select any combination of CLU command check boxes.

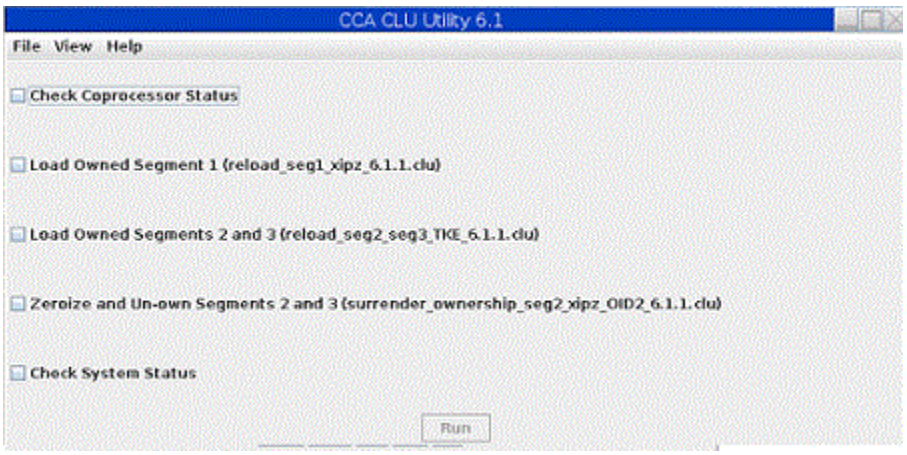


Figure 298. CLU command check boxes

When you click **RUN**, the commands execute in the order they appear on the application window.

If a command fails, the commands checked after the failing command do not execute and remain checked.

After clicking **Run**, view the Output Log or the Command History to check the output from the CLU commands. Both can be viewed by clicking **View** and then clicking **Output Log** or **Command History**.

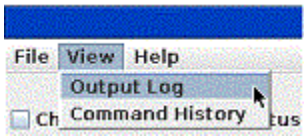


Figure 299. CLU View menu

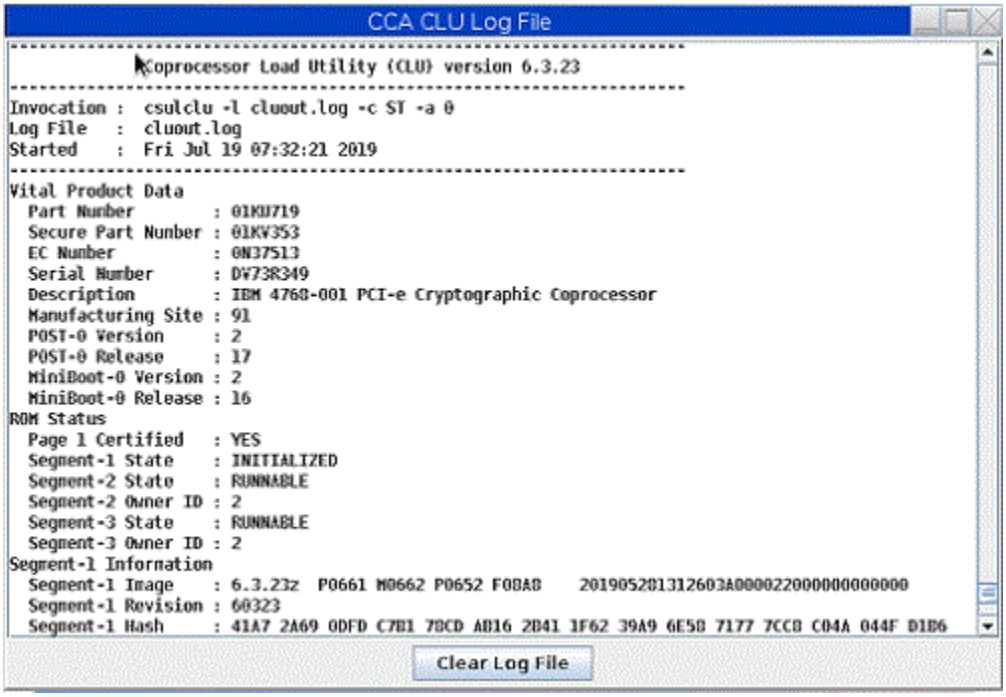


Figure 300. Output log file

The CLU output log file is available to the user in the CNM Data Directory.

Note: The version and segment image levels may have changed since the release of this documentation.

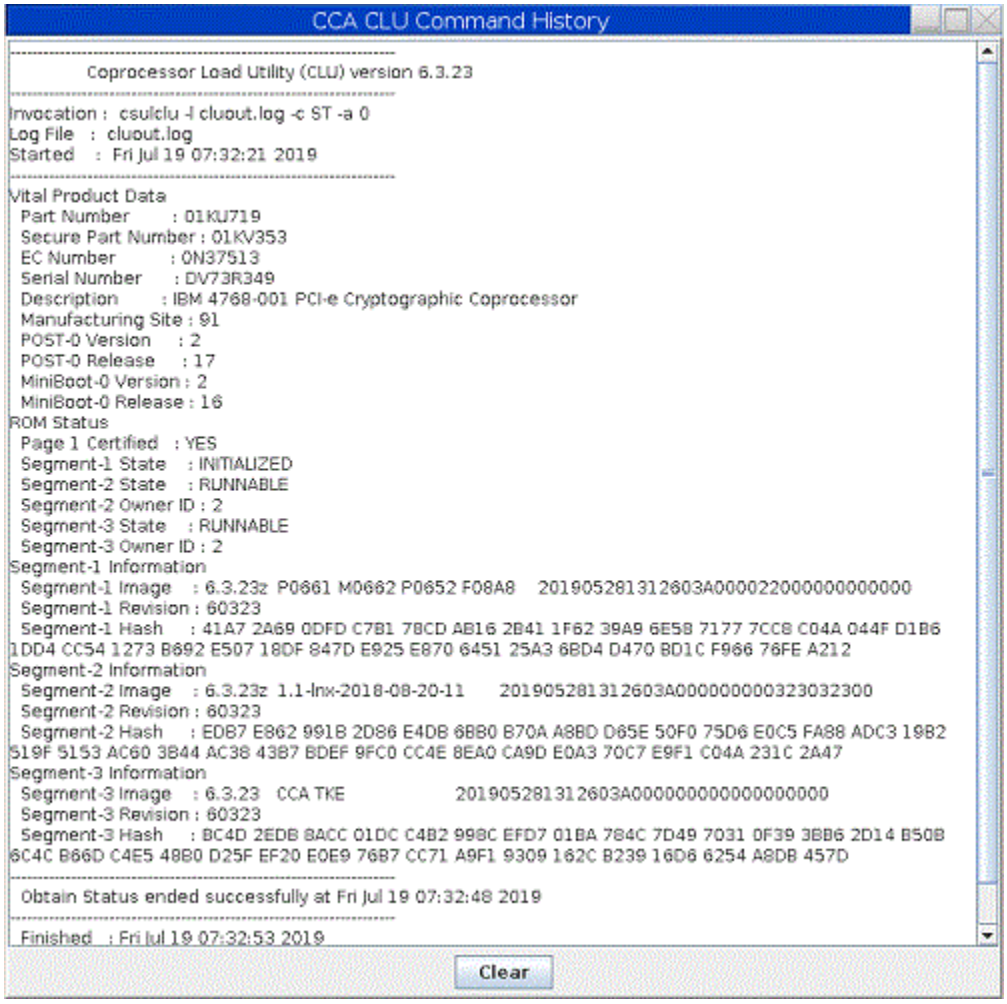


Figure 301. CLU command history

Note: The version and segment image levels may have changed since the release of this documentation.

The CLU command history window shows the CLU commands and output for the current CLU session. It can be erased by clicking on the Clear button and is erased automatically on exit from the CLU utility.

If all CLU commands complete without error, a message indicating that all CLU commands completed successfully is displayed.



Figure 302. Successful completion of CLU commands

Checking coprocessor status

Before loading code you should check the coprocessor status. To use the CLU utility check status command (ST), you must select the **Check Coprocessor Status** check box and then click **Run**.

View the results in the Output Log or Command History.

Loading coprocessor code

IBM 4768 crypto adapters are supported.

1. Change segment 1:
   a. If the segment 1 image name indicates ... Factory ..., set the application to Factory Mode (**File > Factory Mode**). The **Factory Mode** CLU window opens.

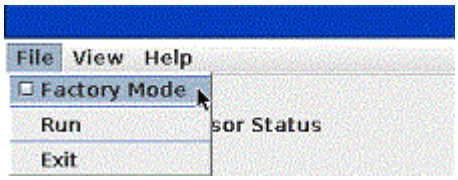


Figure 303. CLU File menu

   Reload segment 1 with the CCA segment 1 file by selecting **Load Factory Segment 1** and clicking **Run**.

   b. If the segment 1 image name does not indicate ... Factory ..., and the segment 1 revision level is less than 60003, reload segment 1 with the CCA segment 1.

   Note: This choice is only available when the application is not in Factory Mode (**File > Factory Mode**).

2. Change segments 2 and 3:
   a. If segment 2 ROM status indicates Unowned... Set the application to Factory Mode (**File > Factory Mode**). Select **Load Factory Segments 2 and 3 (establish_ownership_then_emergency_reload_seg2_seg3_TKE_6.0.*xx*.clu**) and click **Run**.
   b. If segment 2 and 3 ROM status both indicate owner 02... Select **Load Owned Segments 2 and 3 (reload_seg2_seg3_TKE_6.0.*xx*.clu**) and click **Run**.

   Note: This choice is only available when the application is not in Factory Mode (**File > Factory Mode**).

3. When you have successfully completed this process, a check of the coprocessor status or validate of the coprocessor code indicates that the segments contain:Segment 1 Image: 6.0.*xx* P*xx* Segment 2 Image: 6.0.*xx* 1*xx* Segment 3 Image: 6.0.*xx* CCA TKE where the *xx* values are dependent on the maintenance level of the TKE.

   View the results in the Output Log or Command History.

Validating coprocessor code

If you want to validate the code loaded on the crypto adapter use the CLU utility validate command (VA). Select the appropriate check box for your TKE workstation crypto adapter and click **Run**.

View the results in the Output Log or Command History.

Checking system status

If you want to check the system status of your TKE workstation crypto adapter, use the CLU utility check system status command (SS). Select the **Check System Status** check box and click **Run**.

View the results in the Output Log or Command History.

Resetting coprocessor

If you need to reset the TKE workstation crypto adapter use the CLU utility reset coprocessor command (RS). You must enter Factory mode by clicking **Factory Mode** under the **File** menu. Then select the **Reset Coprocessor** check box and click **Run**.

View the results in the Output Log or Command History.

Removing coprocessor CCA code and zeroizing CCA

To Zeroize the CCA node and remove the CCA Coprocessor Code from segments 2 and 3, select the **Zeroize and Unown Segments 2 and 3** check box and click **Run**. This should result in the segment 2 and 3 ROM Status indicated Unowned.

View the results in the Output Log or Command History.

Help menu

The CLU Utility has a help page. To view the help, click **Contents** from the **Help** menu.

Appendix D. Clear RSA key format

An RSA key can be imported from a file holding the unencrypted RSA key. The file must be an ASCII text file. CR/LF can be inserted at any place for enhanced readability of the file.

The contents of the file are:

Description	Length (characters)
Key modulus length in bits (hex value)	4
Length of Modulus field in bytes (hex value)	4
Length of Public exponent field in bytes (hex value)	4
Length of Private exponent field in bytes (hex value)	4
Modulus (hex value)	-
Public exponent (hex value)	-
Private exponent (hex value)	-

The format follows the key_value_structure format defined for the PKA Key token Build (CSNDPKB) callable service.

These are examples of two file contents for the same clear RSA key. The key length is 512 bits and the public exponent is 65537.

Example 1:

```
0200
0080
0003
0080
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
8000000000000001AE28DA4606D885EB7E0340D6BAAC51991C0CD0EAE835AF
D9CFF3CD7E7EA74141DADD24A6331BEDF41A6626522CCF15767D167D01A16F97
010001
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0252BDAD4252BDAD425A8C6045D41AFAF746BEBD5F085D574FCD9C07F0B38C2C
45017C2A1AB919ED2551350A76606BFA6AF2F1609A00A0A48DD719A55E9CA801
```

Example 2:

```
0200004000030040
8000000000000001AE28DA4606D885EB7E0340D6BAAC51991C0CD0EAE835AF
D9CFF3CD7E7EA74141DADD24A6331BEDF41A6626522CCF15767D167D01A16F97
010001
0252BDAD4252BDAD425A8C6045D41AFAF746BEBD5F085D574FCD9C07F0B38C2C
45017C2A1AB919ED2551350A76606BFA6AF2F1609A00A0A48DD719A55E9CA801
```

© Copyright IBM Corp. 2000, 2021

Appendix E. Trusted Key Entry applications and utilities

The TKE console supports a variety of tasks, applications, and utilities.

The set of tasks, applications, and utilities available depends on the console user name specified when the console is initially started. The default console user name is TKEUSER. Other console user names are AUDITOR, ADMIN, and SERVICE. See "Trusted Key Entry console" on page 11 for more information.

Table 37. Tasks, applications and utilities accessible by console user name

Navigation	Task	Privileged mode access ID - None	Privileged mode access ID - ADMIN	Privileged mode access ID - AUDITOR	Privileged mode access ID - SERVICE
Trusted Key Entry					
Applications	Begin Zone Remote Enroll Process for a Crypto Adapter	X	X		
	CCA CLU		X		
	Complete Zone Remote Enroll Process for a Crypto Adapter	X	X		
	Cryptographic Node Management Batch Initialization		X		
	Cryptographic Node Management Utility	X	X		
	Migrate Host Crypto Module Public Configuration Data	X	X		
	Configuration Migration Tasks	X	X		
	TKE Workstation Setup		X		
	Add ACPs to TKE Crypto Adapter Roles		X		X
	Smart Card Utility Program	X	X		
	TKE's Crypto Adapter Initialization		X		
	Trusted Key Entry	X	X		
Utilities	Edit TKE Files	X	X		
	TKE File Management Utility	X	X	X	X
	TKE Workstation Code Information	X	X		
	Configure Displayed Hash Size		X		
	Enhanced Password Encryption Policy		X		
	EP11 Transport Wrapping Key Policy		X		
	Configure Printers		X		
	TKE Audit Configuration Utility			X	

© Copyright IBM Corp. 2000, 2021

Table 37. Tasks, applications and utilities accessible by console user name (continued)

Navigation	Task	Privileged mode access ID - None	Privileged mode access ID - ADMIN	Privileged mode access ID - AUDITOR	Privileged mode access ID - SERVICE
	TKE Audit Record Upload Utility			X	
	TKE Security Event Viewer			X	
Service Management					
	Lock Console	X	X	X	X
	Shutdown or Restart	X	X	X	X
	Hardware Messages	X	X	X	X
	Network Diagnostic Information	X	X	X	X
	Users and Tasks	X	X	X	X
	View Console Information	X	X	X	X
	View Console Service History				X
	View Licenses	X	X	X	X
	Format Media	X	X	X	X
	Backup Critical Console Data		X		X
	Offload Virtual RETAIN Data to Removable Media				X
	Rebuild Vital Product Data				X
	Save Upgrade Data		X		X
	Save/Restore Customizable Console Data		X		X
	Transmit Console Service Data				X
	Manage Print Screen Files	X	X	X	X
Console Logs	View Console Events	X	X	X	X
	View Console Tasks Performed			X	X
	Audit and Log Management	X	X	X	X
	View Security Logs			X	
	Archive Security Logs			X	
Console Internal Code	Analyze Console Internal Code				X
	Authorize Internal Code Changes				X
	Change Console Internal Code				X
Configuration	Configure 3270 Emulators	X	X	X	X
	Configure Backup Settings		X		X
	Customize Console Date/Time		X		X

Table 37. Tasks, applications and utilities accessible by console user name (continued)					
Navigation	**Task**	**Privileged mode access ID - None**	**Privileged mode access ID - ADMIN**	**Privileged mode access ID - AUDITOR**	**Privileged mode access ID - SERVICE**
	Customize Network Settings		X		X
	Customize Scheduled Operations		X		X
	Reassign Trusted Key Entry Console				X
	Password Protect Console		X		X
	Change Password		X	X	X
	Certificate Management		X		X
	Manage SSH Keys		X		X

Using USB flash memory drives with TKE applications and utilities

Trusted Key Entry applications and utilities tasks recognize a USB flash memory drive and allow you to use the drive (if applicable for the task) only if the supported drive meets these requirements:

- It is plugged into a USB port on the TKE.
- It is 1 GB or larger in size.
- It has been formatted with the appropriate data label and format type for the application or utility. For a list of supported format types and labels and the applications that use them, see Table 38 on page 359.

Otherwise, Trusted Key Entry Applications and Utilities tasks do not recognize the drive and you are not able to use it.

Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages might be generated on the TKE workstation.

Begin Zone Remote Enroll Process

This task is for an IBM Crypto Adapter. It is for use on the remote TKE to begin the zone enrollment process.

See “Remote crypto adapter enrollment” on page 306.

CCA CLU

This task is for loading code onto the TKE workstation crypto adapter.

See “CCA CLU (Code Load utility)” on page 324.

Complete Zone Remote Enroll Process

This task is for an IBM Crypto Adapter. It is for use on the remote TKE to complete the zone enrollment process.

See “Remote crypto adapter enrollment” on page 306

Configure Displayed Hash Size

The Configure Displayed Hash Size utility allows you to set the maximum display length of hash values in TKE applications. The maximum display length can be set to 1 to 64 characters. Hash types that can be affected by this function are: MDC-4, SHA-1, SHA-256 and ENC-ZERO.

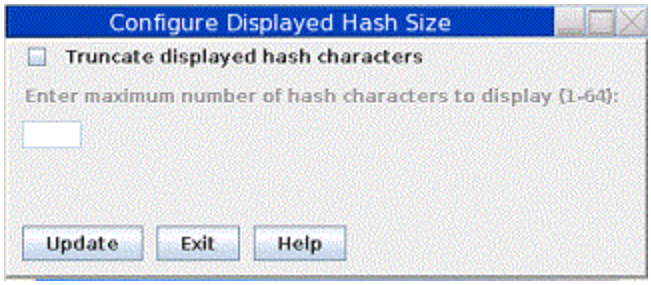


Figure 304. Configure Displayed Hash Size task window

To use the Configure Displayed Hash Size utility:

- Select the 'Truncate displayed hash characters' check box if you want to enable the truncation of displayed hash data. To disable the truncation of displayed hash data, unselect the 'Truncate displayed hash characters' check box.
- Enter the maximum number of hash characters to display (1-64) in the text field. This value must be an integer between 1 and 64.
- Click the Update button to save the changes entered on the panel.

Note: Hash data written to logs or files is only affected by the state of the Configure Displayed Hash Size settings at the time the data is output.

Enhanced Password Encryption Policy

The TKE workstation uses Enhanced Password Encryption whenever the host is running ICSF FMID HCR77B0 or higher. In this case, a user's password is encrypted with a secret AES (Advanced Encryption Standard) key at the time a user does an Open Host (sign-on). If the Enhanced Password Encryption Policy is selected, a user will only be allowed to sign-on to a host if the host has the Enhanced Password Encryption support (ICSF FMID HCR77B0 or higher). If the Enhanced Password Encryption Policy has not been selected, legacy techniques for protecting the host sign-on password will be allowed.

Note: It is highly recommended you migrate to ICSF FMID HCR77B0 or higher on all your hosts and activate this policy.

To manage the policy, you must be signed on in Privileged Mode Access with the ADMIN user ID. From the Trusted Key Entry console, open the Enhanced Password Encryption Policy utility.



Figure 305. Enhanced Password Encryption Policy window

To require Enhanced Password Encryption, select the check box and press **Update**. You will receive a confirmation message before the utility is closed.

EP11 Transport Wrapping Key Policy

The EP11 Transport Wrapping Key Policy utility allows the TKE administrator to set the Elliptic Curve (EC) strength used to derive the Transport Wrapping Key (TWK) to 521 bits.

To require a Transport Wrapping Key Policy of EC-521, select the check box and press Update. If the check box is not selected, EC-320 is used by default. If EC-521 is selected to derive the Transport Wrapping Key, the host crypto adapter must be at API version 7.04 or greater and all smart cards with EP11 master key parts should be initialized with applet version 7 or greater. A Transport Wrapping Key derived using EC-521 is a true 256-bit AES key.

To manage the policy, you must select Privileged Mode Access and sign on with the ADMIN user ID. From the Trusted Key Entry console, open the EP11 Transport Wrapping Key Policy utility.

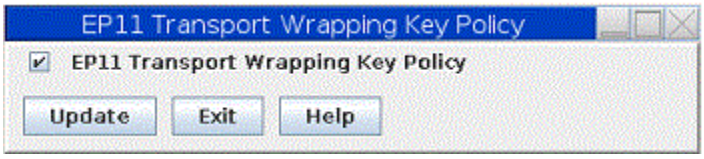


Figure 306. EP11 Transport Wrapping Key Policy window

To reset the policy to EC-320, deselect the check box and press Update. In both cases, you will receive a confirmation message about the strength of the policy before the utility is closed.

Configure Printers

To configure printers on the TKE workstation, you must:

1. Log on to the TKE workstation console through Privileged Access Mode as ADMIN.

   Note: You can only add printers if the device driver for the printer is included with the TKE. TKE includes the GUTENPRINT and HPLIP device driver packages. The TKE workstation does not allow you to load your own printer device drivers. Also, ensure that you have at least one profile with a role that has the "print files" ACP.
2. Open the **Configure Printers** application under Utilities.
3. Select the **Administration** tab.
4. Select **Add Printer**.
5. If you have printers plugged in, they show up in the **Local Printers** list. Otherwise, ensure that the printer you are trying to use is properly plugged in.
6. Change the name and description of the printer and press **Continue**. (Optional)
7. TKE finds the appropriate device driver. If not, select the appropriate device driver from the list and press **Add Printer**.
8. Enter the default options and press **Set Default Options**.

The printer is now defined. Information about each configured printer shows up in the **Printers** tab. The tab provides maintenance and administrative functions to use on the printer. To ensure that the printer is set up correctly, select **Maintenance** and choose **Print Test Page**.

Cryptographic Node Management batch initialization

This task is for using a batch interface to execute a user-created CNI file. A user-created CNI file can be used to initialize a TKE workstation crypto adapter differently than the TKE Crypto Adapter Initialization task. To create the user CNI, use the Cryptographic Node Management Utility, CNI Editor function.

See “Cryptographic Node Management Batch Initialization” on page 323

Cryptographic Node Management utility

This task is for managing the TKE workstation crypto adapter (create and manage Roles and Profiles, manage workstation master keys, et cetera).

See Chapter 11, “Cryptographic Node Management utility (CNM),” on page 251.

Edit TKE files

The Edit TKE Files task provides a way to edit and browse files on a USB flash memory drive or within the four allowed TKE-related data directories on the hard drive:

- TKE Data Directory
- Migration Backup Data Directory
- CNM Data Directory
- SCUP Data Directory

Files in the Configuration Data Directory cannot be accessed by the Edit TKE Files task and should be reviewed using the review functions in the configuration migration applications.

To open the Edit TKE Files task, click **Trusted Key Entry** and then click **Edit TKE Files**.

You must be logged on to the TKE workstation crypto adapter for this task. If you are not currently logged onto the adapter, a logon window is displayed. You will need to select a profile to log on to the adapter. If you are already logged onto the adapter, no logon window will be displayed (the current logon will be used).

In the Open Text Editor window, select a file from the displayed list or manually enter a file name. If you manually enter a file name that does not exist, a new file by that name will be created in the location specified.

If the crypto adapter profile currently being used is authorized to print files, the Print button is shown in the Open Text Editor window.

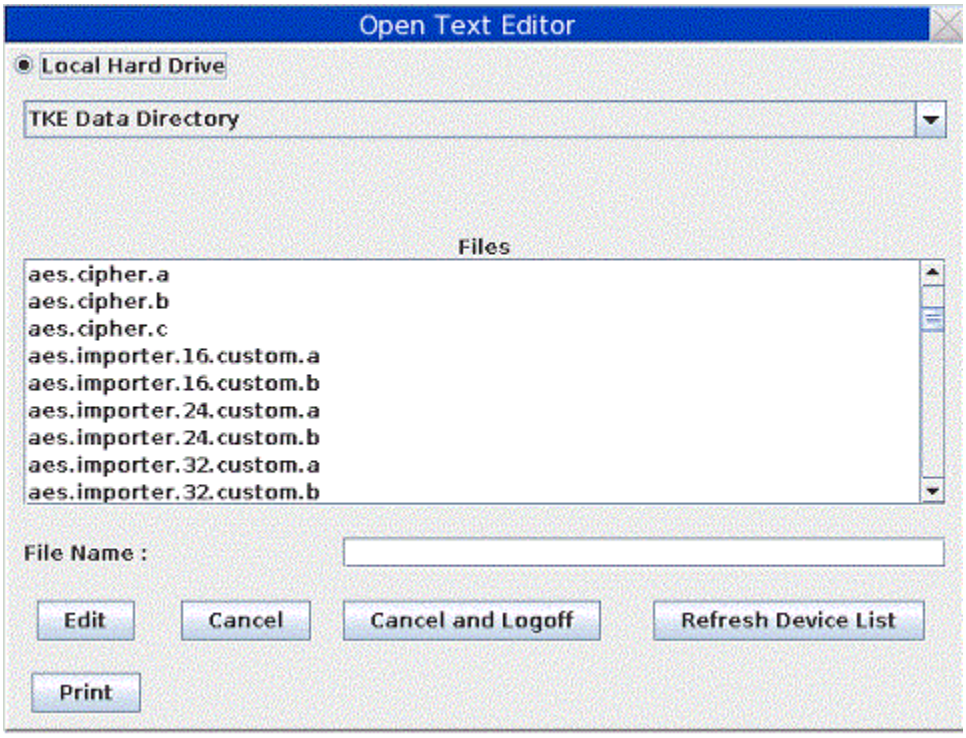


Figure 307. Edit TKE Files task window

You can edit the file within the edit text box and use File -> Save menu item to save the file.

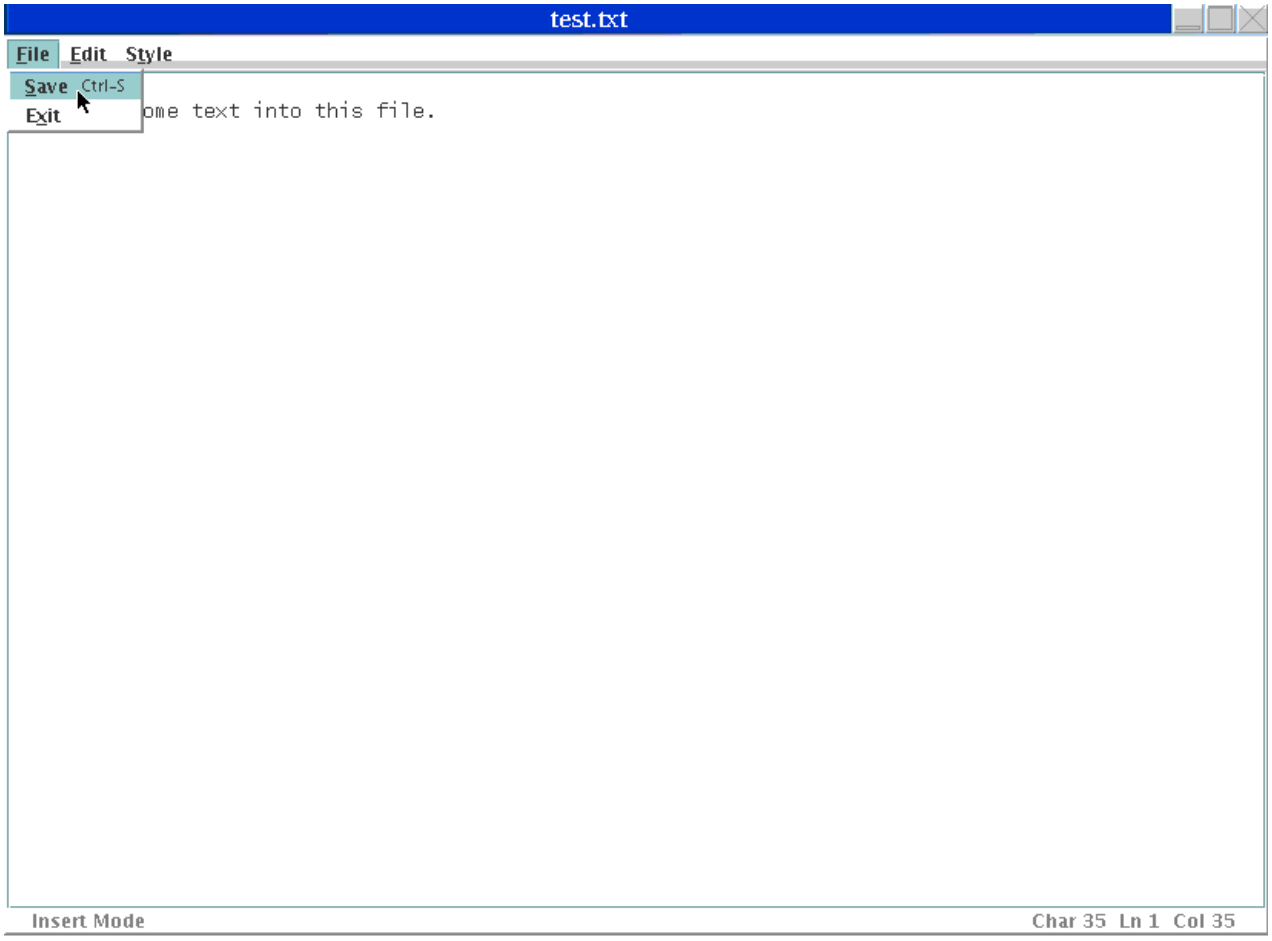


Figure 308. Editor - File menu items

Attention : Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages might be generated on the TKE workstation.

The editor provides options for Undo, Cut, Copy, Paste, along with Line Selection and Search/Replace.

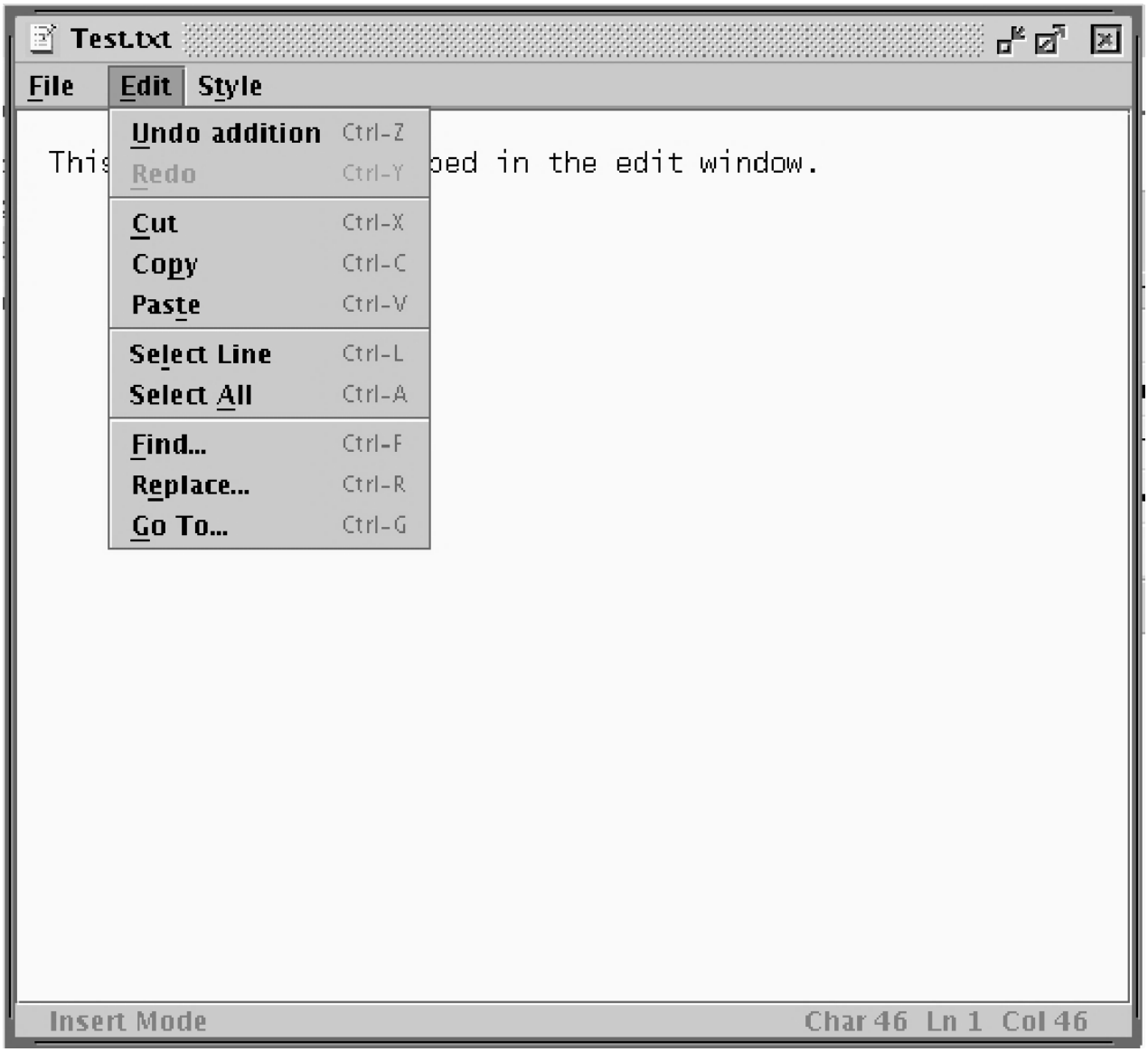


Figure 309. Editor - Edit menu items

In addition, there are options for Fonts, line wrap, and background.

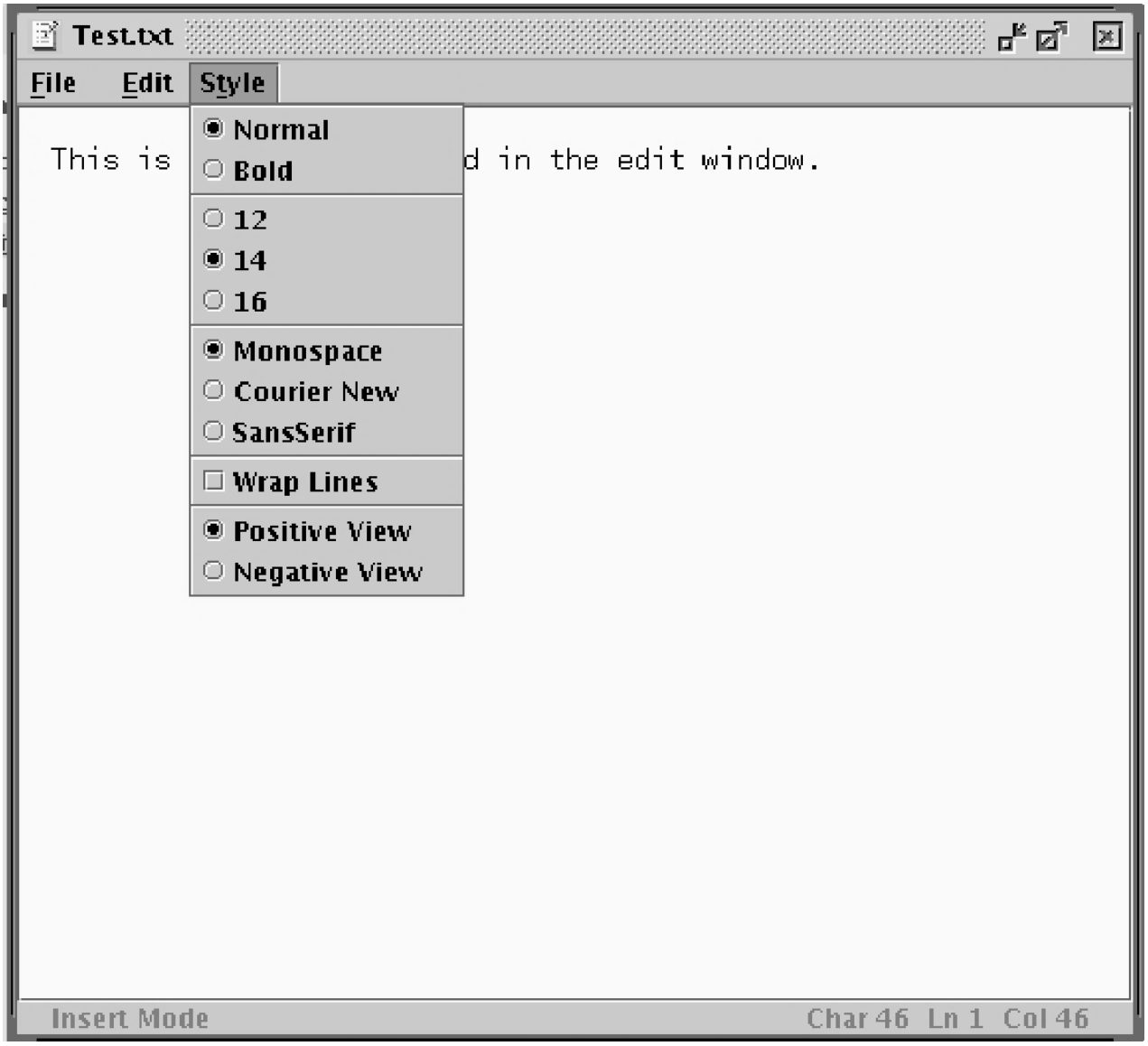


Figure 310. Editor - Style Menu Items

Add Access Control Points utility

This utility simplifies the process of adding new ACPs to existing roles on your TKE workstation crypto adapter. This is useful during migration, because new ACPs are not automatically added to existing roles during the migration process.

See "Adding new ACPs to existing roles using the Add Access Control Points utility" on page 88 for more information.

Smart Card Utility Program

This task is used for initializing smart cards, enrolling smart cards in a zone, and enrolling TKE workstations in a zone.

See Chapter 12, "Smart Card Utility Program (SCUP)," on page 291.

TKE Audit Configuration utility

This utility starts and stops auditing of security-relevant events on the TKE workstation, and controls what events will create audit records. You must log on with a console user name of AUDITOR to use this utility.

See "TKE Audit Configuration utility" on page 227 for more information

TKE Audit Record Upload Configuration utility

This utility enables you to send TKE workstation security audit records to a Z host where they will be saved in the z/OS System Management Facilities (SMF) data set. Each TKE security audit record is stored in the SMF dataset as a type 82 subtype 29 record. This allows you to place TKE security audit records from 1 or more TKE Workstations into a single SMF data set on a target host. From the host, a security officer can use SMF features to analyze and archive the TKE security audit data.

See "TKE Audit Record Upload Configuration utility" on page 238 for more information

TKE File Management utility

Attention: DVD-RAM is not supported on TKE 7.2 or later systems. If you have a DVD-RAM that is formatted for TKEDATA (TKEDATA DVD-RAM) and you want to use the files from the TKEDATA DVD-RAM on a TKE 7.2 or later system, see "DVD-RAM is not supported on a TKE 7.2 or later system" on page 55 for additional information.

The TKE File Management Utility task allows you to manage files on a USB flash memory drive, or within supported data directories on the local hard drive. It provides the ability to delete, rename, and copy files.

To invoke this task, click on **Trusted Key Entry** and then click on the **TKE File Management Utility**.

You must be logged on to the TKE workstation crypto adapter for this task. If you are not currently logged on to the adapter, a logon window is displayed. You will need to select a profile to log on to the adapter. If you are already logged onto the adapter, no logon window will be displayed (the current logon will be used).

When the TKE File Management Utility is opened the user is presented with the following task window.

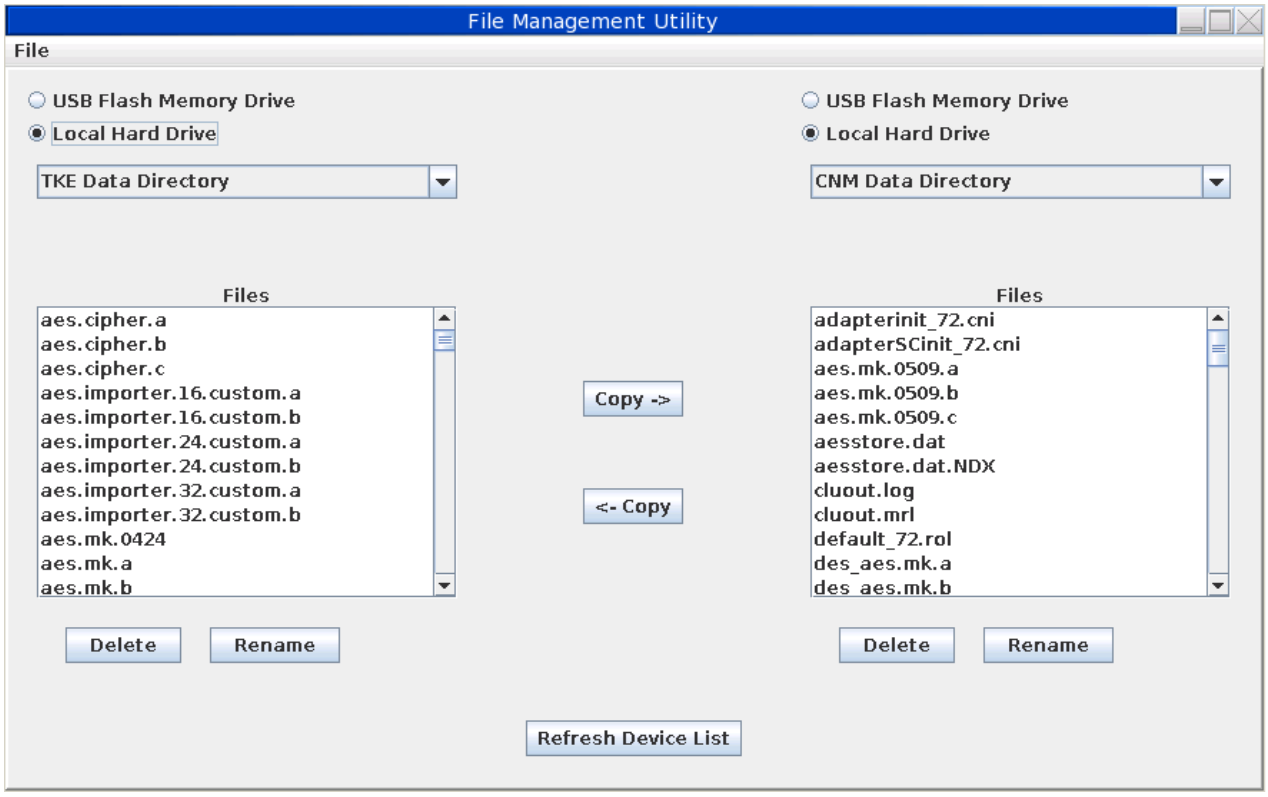


Figure 311. TKE File Management Utility task window

In the File Management Utility window, selecting the hard drive for either **Source** or **Target** will allow you to select from one of five data directories:

- TKE Data Directory
- Migration Backup Data Directory
- CNM Data Directory
- SCUP Data Directory
- Configuration Data Directory

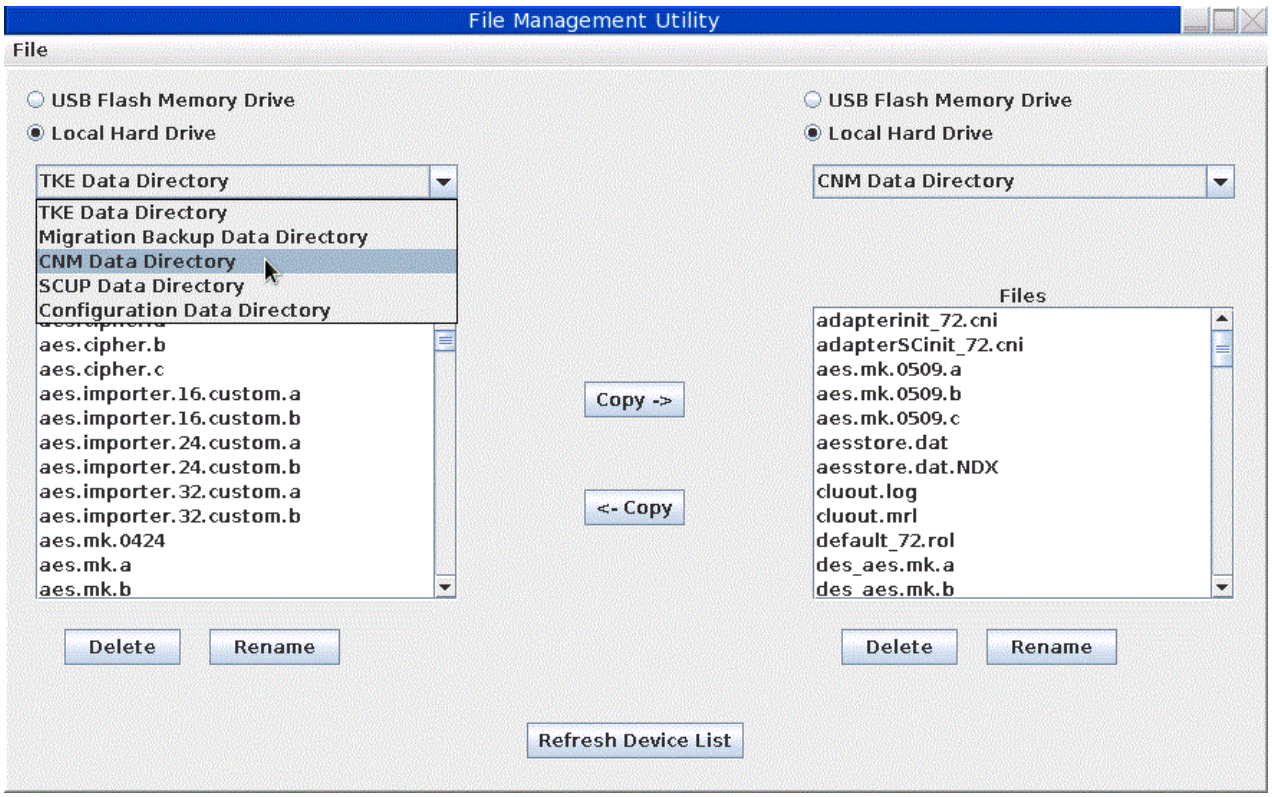


Figure 312. TKE File Management - directory options

From the displayed list you can select a single file, numerous files, blocks of files, or the entire display.

- For a single file, just click on the desired file.
- To select more than one file click on the first file, hold down the Ctrl key and click on each additional file.
- To select a block of files, click on the first file, hold down the Shift key and click on the last file. All files between the two selected files will be selected.
- To select all the files, hold down the Ctrl key and type an 'a'.

Clicking on **Delete** will display a confirmation window.

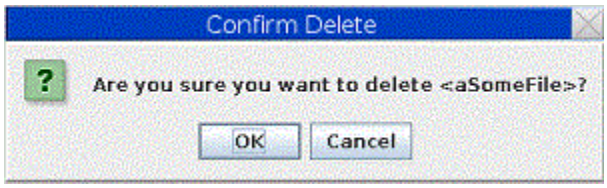


Figure 313. Delete confirmation window

Clicking on **Rename** will present a window for inputting a filename.

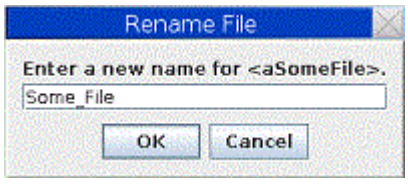


Figure 314. Window for inputting a filename

Attention : Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using

the drive. If you do remove a drive before the operation is complete, hardware messages might be generated on the TKE workstation.

TKE workstation code information

The TKE Workstation Code Information window shows information about the code used by the TKE applications. The information can be useful in problem determination. Updates to TKE application code are reflected in this window. This task does not give information about the code on the TKE workstation crypto adapter.

To invoke this task, click **Trusted Key Entry** and then click **TKE Workstation Code Information**.

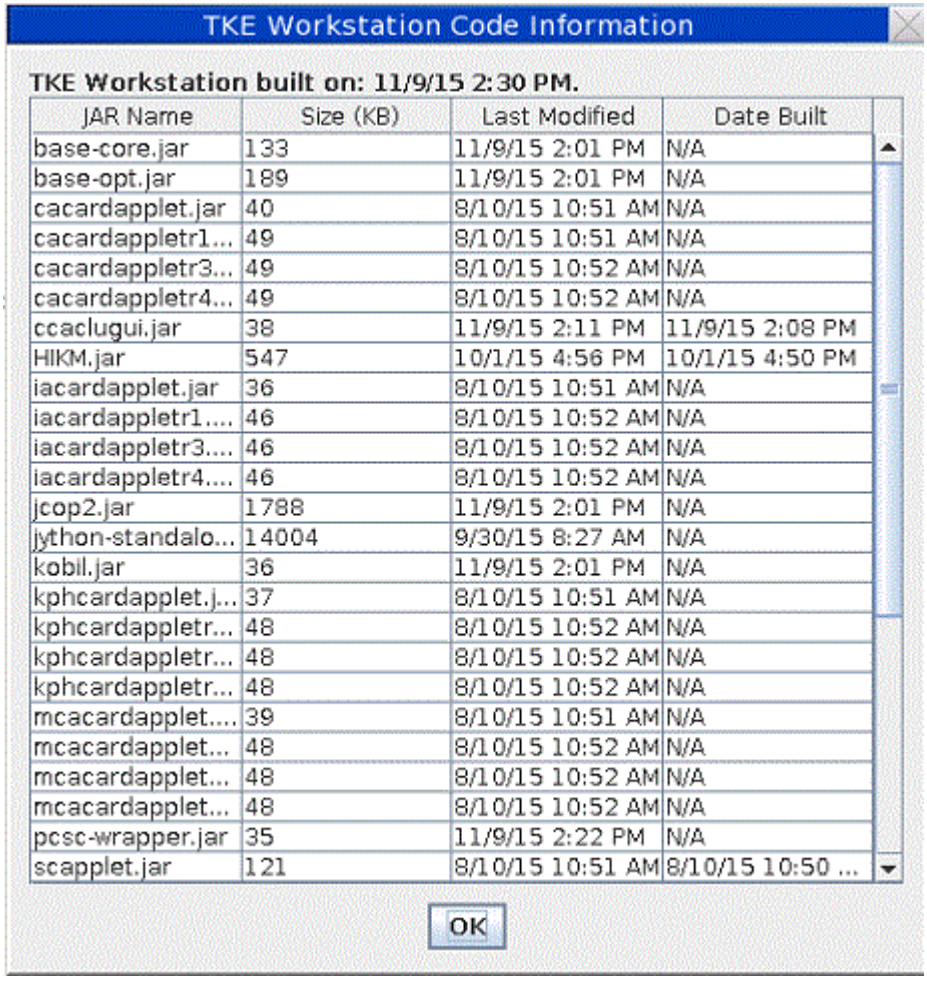


Figure 315. TKE Workstation Code Information window

Configuration migration

The TKE workstation provides tools to securely capture host crypto module configuration data to a file, and then apply this data to another host crypto module. Tools are provided for both CCA and EP11 host crypto modules. These tools simplify the task of installing new or replacement host crypto modules, and can be used for backup and disaster recovery.

For CCA crypto modules, three tools are provided:

- One tool migrates only public configuration data (roles, authorities, and domain control settings).
- A second tool migrates all configuration data, including secret data such as master key values. The protocol for migrating secret data is more complex than the protocol for migrating only public data and requires the participation of several smart card holders. This tool results in a complete replacement of the configuration on the target crypto modules.

- A third tool migrates only the configuration settings for a single source domain to one or more target domains. The existing module-level configuration settings on the target crypto modules (roles and authorities) and domain-level configuration settings for non-targeted domains are not changed. This tool can be used to transfer desired domain configuration settings to other domains on the same crypto module or on different crypto modules. This tool also relies on a protocol for handling secret data that requires the participation of several smart card holders.

For EP11 crypto modules, only the tool used to migrate all configuration data (including master keys) and the tool used to migrate only the configuration settings for a single source domain are supported.

To migrate only public configuration data on CCA crypto modules, click **Migrate Host Crypto Module Public Configuration Data** on the **Trusted Key Entry** menu. To use the other tools, click **Configuration Migration Tasks** on the **Trusted Key Entry** menu. The **Enroll source module in migration zone** and **Collect configuration data** buttons can be used to collect configuration data. The **Apply configuration data** button does a full replace of configuration data, and the **Domain-only apply** button replaces only domain-level configuration settings for the target domains. When doing a domain-only apply, the source configuration data file must contain data for just one domain

Migrate Host Crypto Module Public Configuration Data

Use this utility to save host crypto module configuration data (such as roles, authorities, and domain control settings) to a file on the TKE workstation, and to load a host crypto module with configuration data that was previously saved to a file. The utility simplifies the task of restoring the configuration when a host crypto module is replaced. This utility supports only CCA crypto modules and CCA domain groups.

The utility saves and loads only public configuration data. Private data, such as the value of master key registers, is not accessed.

The utility supports the following four tasks:

- Collecting configuration data from a host crypto module and saving it in a file.
- Applying previously saved configuration data to a host crypto module.
- Collecting configuration data from one host crypto module and applying it to a different host crypto module in one operation.
- Reviewing previously saved configuration information in a file.

The source and target can be either a single host crypto module or a domain group. When the source is a domain group, the crypto module containing the master domain of the group is located and used as the source crypto module. When the target is a domain group, all crypto modules with at least one domain in the domain group are updated with the configuration data read from a file.

To apply configuration data to a target host crypto module, you must use an authority that allows roles and authorities to be created on the target, such an authority with the predefined INITADM role. When the utility applies configuration data to a domain group, the current authority signature key is checked before each crypto module in the group is updated. If it does not have the required authority, you can load a different authority signature key.

The apply task creates and uses a temporary role and authority, which it removes when finished. In some cases, the temporary role cannot be removed. Because a temporary authority is used, 99 authorities are the most that can be migrated by the utility. If 100 authorities are defined in the source configuration, the authority at index 99 must be created on the target manually. A warning is displayed for these special cases.

Target crypto modules must support all cryptographic services of the source configuration. To ensure that this requirement is met, the utility checks that the CCA version on the target module is at a higher level than the source configuration. If it is not, migration is not allowed.

In the apply task, existing roles, authorities, and domain control settings on target crypto modules are removed and replaced with the configuration data from the file. Domains optionally can be zeroized before you apply configuration data. This action clears the master key registers. Only control domains can be zeroized. For more information about control domains, see Appendix B, “LPAR considerations,” on page 321.

Files that are used by the configuration migration utility are created in, and read from, the Configuration Data Directory. The TKE File Management utility can copy, rename, and delete files in this directory.

Note: The apply task reserves target host crypto modules for update. If a target host crypto module is already reserved for update by another application, the apply task fails with an error message. The other application must be closed before the apply task can be run. In abnormal situations, it might be necessary to take the following steps to force release of the target host crypto module:

1. Start the main TKE application.
2. Open a crypto module notebook for the reserved host crypto module.
3. Select **Release Crypto Module** from the **Function** menu of the crypto module notebook. This function forcibly releases the host crypto module from the application that was holding it and reserves it for the crypto module notebook.
4. Close the crypto module notebook to release the host crypto module.

Configuration migration tasks

This application provides access to utilities used to securely migrate configuration data, including secret data such as master key values, from one crypto module to another. This application can be used for both CCA crypto modules and EP11 crypto modules. When you select this application, the Configuration Migration Tasks panel is displayed.

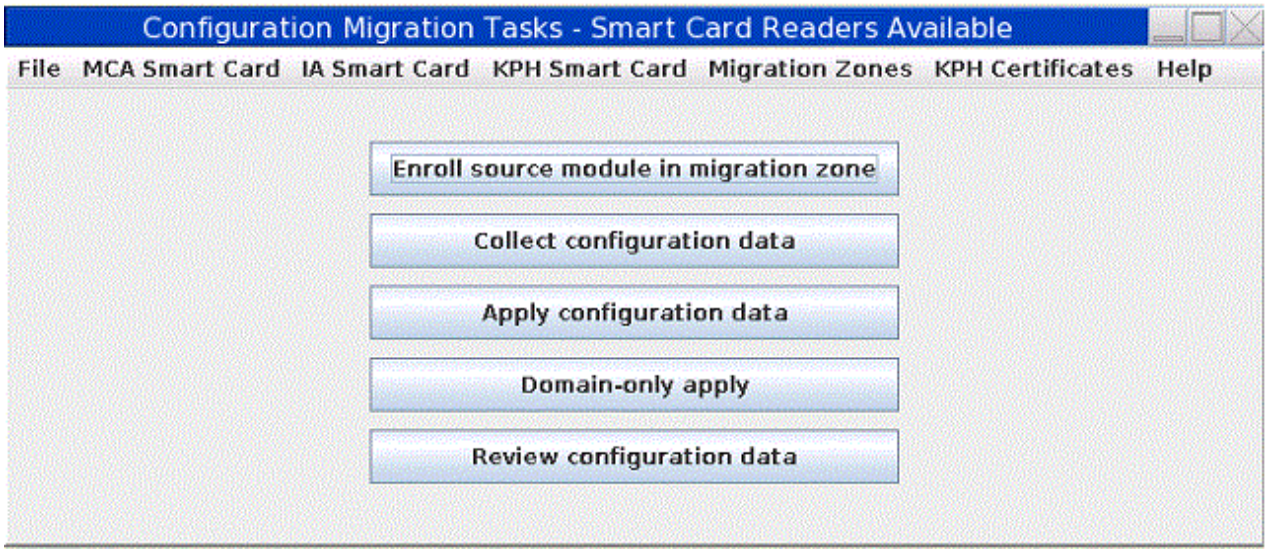


Figure 316. Configuration Migration Tasks panel

To use this application, you must create a set of smart cards that defines a migration zone. The smart cards are used as part of a secure protocol to protect secret configuration data while in transit from one crypto module to another. The protocol generates a 256-bit AES transport key for encrypting configuration data that is split into as many as 10 parts.

Three smart card types support configuration migration that includes master keys: Migration Certificate Authority (MCA) smart cards, Injection Authority (IA) smart cards, and Key Part Holder (KPH) smart cards.

The MCA smart card defines the migration zone. A migration zone is a set of smart cards that work together to accomplish a migration task. When the migration zone is created, two policies are set indicating the number of smart cards needed for the tasks. The "M-of-N" policy indicates the number of parts the transport key is split into (N), and the number of parts needed to reconstruct the transport key (M). The maximum value for N is 10, and M must be less than or equal to N. The "K" policy indicates the number of IA smart cards required to apply configuration data to a target host crypto module. The maximum value for K is 10.

The MCA smart card is used to create IA and KPH smart cards. These smart cards become part of that migration zone, and can be used only in that migration zone. An unlimited number of migration zones can

be created, but each migration zone has its own MCA smart card (and backup MCA smart cards) and set of IA and KPH smart cards.

The IA smart card authorizes application of configuration data to a target host crypto module or domain group.

The KPH smart card authorizes reconstruction of the transport key.

These smart cards can be created using the associated pull-down menus at the top of the Configuration Migration Tasks panel, or you can select the **Migration zone wizard** option on the **File** menu to start a wizard that guides you through the task.

For CCA crypto modules, before configuration data can be collected from a source host crypto module, the source host crypto module must be enrolled in the migration zone using the **Enroll source module in migration zone** task. EP11 crypto modules do not need to be enrolled in the migration zone.

During the **Collect configuration data** task, the source host crypto module generates a transport key and splits it into "N" parts. (The key splitting algorithm allows the key to be recovered with only "M" of the original "N" parts. It does not matter which "M" parts are provided.) Each key part is encrypted using the public key from one of the "N" KPH smart cards. The source host crypto module captures the configuration data and encrypts it using the transport key. The encrypted configuration data and "N" encrypted key parts are returned.

During the **Apply configuration data** task, the target crypto module generates and returns a target decryption public key. It also returns an Outbound Authentication (OA) signature over the target decryption public key and the target host crypto module OA certificate chain.

"K" IA smart cards approve the target crypto module and target decryption public key, with help from the OA proxy (see “OA proxy” on page 349).

"M" KPH smart cards approve reconstructing the transport key, with help from the OA proxy (see “OA proxy” on page 349). KPH smart cards receive the transport key part that was encrypted with their public key, decrypt it using their private key, re-encrypt it using the target decryption public key, and return the result.

The target crypto module receives the encrypted configuration data and the "M" rewrapped key parts. It decrypts the rewrapped key parts using its private key, reconstructs the transport key, and decrypts and applies the configuration data.

The target of the apply task can be either a single crypto module or a domain group. When the target is a domain group, the configuration data is applied to each crypto module with at least one domain in the group.

For the **Domain-only apply** task, processing is similar, but on the target crypto modules, only the configuration settings for the target domains are updated. Module-level configuration settings and domain-level configuration settings for non-target domains are not changed. When the target of the domain-only apply task is a single crypto module, you select the target domains to receive the new configuration. When the target is a domain group, each domain in the domain group receives the new configuration. To use the domain-only apply task, the source configuration data file must contain data for just one domain.

Signature collection

CCA and EP11 crypto modules have different command authentication architectures. CCA is role-based. Commands are signed by authorities whose roles allow the action. EP11 uses a signature threshold approach, where all administrators have equal authority to issue commands but must be installed on the target domain or crypto module. Each target domain and crypto module independently specifies the number of administrator signatures that are required to issue commands (the *signature threshold*).

Because of the different architectures, signature collection for configuration migration commands is different. For CCA, the role of the current authority is checked before each command is issued. You can load a different signature key if the authority is not authorized to issue the command.

For EP11, for each required signature you are prompted to insert a smart card with an administrator signature key in smart card reader 1. If that signature key does not match one of the installed administrators on the target crypto module or domain, you are prompted to insert a different smart card. This prompting continues until a valid signature key is found or until you cancel.

For EP11, you can bypass the prompting for each signature by predefining smart card readers as a source for signatures. After a smart card is inserted in the reader and the PIN is entered, signatures are collected automatically as needed, without further prompting. You can predefine signature key sources by using the **Manage EP11 Signature Keys** option on the **File** menu.

Window actions

File menu
This menu includes options to predefine smart card readers as the source of signatures for commands to EP11 crypto modules; to invoke a wizard for creating the MCA, IA, and KPH smart cards needed to define a migration zone; and to exit the Configuration Migration Tasks application.

MCA Smart Card menu
This menu includes options to display the contents of an MCA smart card, initialize and personalize an MCA smart card, back up an MCA smart card, or change the PIN on an MCA smart card.

IA Smart Card menu
This menu includes options to display the contents of an IA smart card, initialize and enroll an IA smart card in a migration zone, personalize an IA smart card (set the PIN and description), unblock an IA smart card, or change the PIN on an IA smart card.

KPH Smart Card menu
This menu includes options to display the contents of a KPH smart card, initialize and enroll a KPH smart card in a migration zone, personalize a KPH smart card (set the PIN and description), unblock a KPH smart card, or change the PIN on a KPH smart card.

Migration Zones menu
Use the **Work with migration zones** function on this menu to display the list of migration zones that are known to the TKE workstation, and add or delete entries.

To minimize the number of times an MCA smart card must be inserted in a card reader during migration tasks, the TKE workstation maintains a list of known migration zones. The list is updated automatically when a new MCA smart card is created. If you must add or remove migration zones from this list, you can use this function. To add a migration zone to the list, you must insert the MCA smart card for the zone in the smart card reader and enter the PINs.

KPH Certificates menu
Use the **Work with KPH certificates** function on this menu to display the list of KPH smart cards that are known to the TKE workstation, and add or delete entries.

To minimize the number of times KPH smart cards must be inserted in a card reader during migration tasks, the TKE workstation maintains a list of known KPH certificates. The list is updated automatically when a new KPH smart card is created. If you must add or remove a KPH certificate from this list, you can use this function. To add a KPH certificate to the list, you must insert the KPH smart card in the smart card reader.

Enroll source module in migration zone
This option starts a wizard that takes you through the steps to enroll a source host crypto module in a migration zone. The source crypto module must be enrolled in a migration zone before configuration data can be collected from it. This action is not needed for EP11 crypto modules.

You need to know what migration zone you will use before you run this wizard. If you must define a new migration zone, you can use the **MCA Smart Card** menu to create a new MCA smart card. If you define a new migration zone, you also must create IA and KPH smart cards to use in the zone.

To run this wizard, you must load a signature key that permits the Certificate Insert operation on the source crypto module. If the signature key has insufficient authority, you can load a different signature key.

Collect configuration data

This option starts a wizard that takes you through the steps to collect configuration data from a source host crypto module and save it in a file. Before you run this wizard on a CCA host crypto module, you must enroll the host crypto module in the migration zone.

You must know what migration zone and what KPH smart cards you will use before you run this wizard. Only KPH smart cards for the selected migration zone can be used.

In this wizard, you indicate the set of domains that you want to collect configuration data from. Configuration data for only those domains is saved in the configuration data file. During the apply task, configuration data for domains that are not saved in the configuration data file is set to the default value.

To run this wizard on a CCA crypto module, you must load a signature key that permits the Crypto Data Extract operation on the source host crypto module. If the signature key has insufficient authority, you can load a different signature key.

Starting with CCA 6.1, you are allowed to skip collecting configuration settings for optional, less commonly used features on CCA crypto modules. This reduces the amount of collected configuration data and the time it takes to collect and apply this data. Configuration settings not collected are set to their default values on the target crypto module. If you are uncertain about what optional features you use, collect all configuration settings (the default).

Starting with CCA 6.1 and TKE 9.1, you are allowed to collect configuration settings from domains in imprint mode and PCI-compliant mode. This includes the domain-specific roles and authorities for the domain. Prior to CCA 6.1 and TKE 9.1, you are allowed to collect configuration settings only from domains in normal mode. To collect configuration settings from domains in imprint mode and PCI-compliant mode, you must use smart cards with a P521 ECC zone.

Apply configuration data

This option starts a wizard that takes you through the steps to apply configuration data to a target host crypto module or target domain group.

The wizard prompts you to insert IA smart cards in the smart card reader and enter the PIN. The "K" policy for the migration zone specifies the required number of IA smart cards.

The wizard prompts you to insert KPH smart cards in the smart card reader and enter the PIN. "M" of the "M-of-N" policy for the migration zone is the required number of KPH smart cards.

To run this wizard on a CCA crypto module, you must load a signature key that permits the Target Prepare and Crypto Target Inject operations on the target host crypto module or target group. If the signature key has insufficient authority, you can load a different signature key. The default role and authority that is created when a host crypto module is initialized allow you to run these operations.

Starting with CCA 6.1, you are allowed to skip collecting configuration settings for optional, less commonly used features on CCA crypto modules. This reduces the amount of collected configuration data and the time it takes to collect and apply this data. Configuration settings not collected are set to their default values on the target crypto module. If uncertain about what optional features you use, collect all configuration settings (the default).

Starting with CCA 6.1 and TKE 9.1, you are allowed to collect configuration settings for domains in imprint mode and PCI-compliant mode. This includes the domain-specific roles and authorities for the domain. Prior to CCA 6.1 and TKE 9.1, you are allowed to collect configuration settings only from domains in normal mode. To collect configuration settings from domains in imprint mode and PCI-compliant mode, you must use smart cards with a P521 ECC zone.

Domain-only apply

This option starts a wizard that takes you through the steps to apply configuration data from a single source domain to one or more target domains. The wizard steps and protocol are similar to those for the **Apply configuration data** option.

When using this option, the source configuration data file must contain data for a single domain. When a single crypto module is selected as the target, you select the domains on that crypto module to receive the configuration data. When a domain group is selected as the target, each domain in the

domain group is updated with the source configuration. In both cases, module-level configuration settings and domain-level configuration settings for non-target domains are not changed.

Review Configuration Data
This option starts a wizard that displays the non-secret contents of a configuration data file that you select.

Different data is saved in the configuration data file for CCA and EP11 host crypto modules. For both crypto module types, the saved data includes the serial number and code level of the source crypto module, the date and time that the configuration data was collected, the migration zone and KPH certificates used, and what domains were collected. For CCA it includes a list of the roles and authorities collected, the domain controls for collected domains, and key register status and key hashes for collected domains. For EP11 it includes the crypto module administrators and attributes, and the domain administrators, attributes, control points, and key status and hash values for collected domains.

Instructions for migrating key material

If you want to migrate configuration data that includes master key values, follow these steps:

1. Decide what migration zone you are using. If you are not using an existing migration zone, create an MCA smart card that defines the new zone. You must define the M-of-N and K policies. "N" is the number of parts the transport key is split into and must be 1 - 10. "M" is the number of key parts that are required to reconstruct the transport key and must be between 1 and "N". "K" is the number of Injection Authorities that are required to approve applying configuration data on the target host crypto module and must be 1 - 10.

   Guideline: Create a backup whenever you create a new MCA smart card.
2. Use the **Migration Zones** menu to check that the migration zone you want to use is listed. If it is not listed, add it.
3. If you are using a new migration zone, create IA and KPH smart cards. You must create at least "K" IA smart cards and "N" KPH smart cards for the migration zone, but you can create more.
4. Decide what KPH smart cards you are using. Use the **KPH Certificates** menu to check that the KPH smart cards you want to use are listed. If they are not listed, add them.
5. Run the "Enroll source module in migration zone" wizard to enroll the source host crypto module in the migration zone. This step is not needed for EP11 crypto modules.
6. Run the "Collect configuration data" wizard to collect configuration data on the source host crypto module. The wizard prompts you to enter the media type and a file name for storing the encrypted configuration data.
7. Run the "Apply configuration data" wizard to apply configuration data on the target host crypto module. As the wizard runs, the IA and KPH smart card holders are prompted to insert their smart cards in a smart card reader and enter their PINs.

OA proxy

When migrating configuration data from one host crypto module to another, the Injection Authority (IA) and Key Part Holder (KPH) smart cards verify outputs from the source and target host crypto modules. These outputs are signed by the host crypto modules' private keys, as part of a process called Outbound Authentication. In addition to the OA signature, the source and target host crypto modules provide their OA certificate chain, which terminates in an IBM root certificate.

Some IBM host crypto modules use key sizes for their OA signatures and certificate chains that are larger than what is supported by currently available smart cards. To handle these host crypto modules, the TKE workstation crypto adapter acts as an OA proxy for the smart cards. The TKE workstation crypto adapter verifies the OA signature and certificate chain and signs the output data using a specially-generated OA proxy signing key.

Each migration zone on the workstation needs to create an OA proxy certificate for this OA proxy signing key. The OA proxy certificate is created automatically when Migration Certificate Authority (MCA) smart

cards are created, and when the migration zone is added or updated using the **Migration Zones** pull-down menu on the **Configuration Migration Tasks** panel.

If the TKE workstation crypto adapter is replaced or re-initialized, these OA proxy certificates are no longer valid. The migration zones listed under the **Migration Zones** pull-down menu will be removed automatically and must be re-registered using the MCA smart cards. Users who wish to change the OA proxy signing key can do so by manually deleting all migration zones found using the **Migration Zones** pull-down menu and then re-adding them.

Smart card applet level for configuration migration

To apply configuration data for the CEX5C, CEX5P, and later crypto modules, you must use IA and KPH smart cards with an applet version of 0.3 or greater. Earlier IA and KPH applet versions do not support the type of OA proxy signature used for these crypto module types.

Restriction on CCA User Defined Extensions (UDXs)

Customized functions can be added to a CCA crypto module by creating a user defined extension (UDX). User defined extensions can be written by IBM or by a selected set of contractors. A user defined extension is a separate segment 3 code load for the CCA crypto module and a separate host library to communicate with the crypto module.

When a user defined extension is installed on a CCA crypto module for the first time, ownership of the CCA crypto module must be surrendered. This erases all secrets on the crypto module and returns the crypto module to an initialized state. This prevents any secrets on the CCA crypto module from potentially being exposed by the user defined extension.

Similarly, ownership of the CCA crypto module must be surrendered when removing a UDX and when installing a different UDX. Installing an updated version of the same UDX or an updated version of the base CCA code does not require surrendering ownership.

To prevent a potential security exposure, configuration migration using the Configuration Migration Tasks application is not allowed if the segment 3 owner id of the source crypto module is different from the segment 3 owner id of the target crypto module. An error is signaled during an apply if the owner ids are different. Every user defined extension has a unique owner id that is different from the owner id for the base CCA code.

Service Management tasks

The Service Management category contains tasks and utilities to service, manage, configure and maintain the TKE console. The tasks vary with the user name used to log on.

The following tasks are displayed if you are logged in as **Service**:

- “Analyze console internal code” on page 351
- “Authorize internal code changes” on page 351
- “Change console internal code” on page 352
- “Offload virtual RETAIN data to removable media” on page 363
- “Transmit console service data” on page 366
- “View console service history” on page 371
- “Rebuild vital product data” on page 363

The following tasks are displayed if you are logged in as **Auditor**:

- “Archive security logs” on page 351
- “View security logs” on page 375

The following tasks are displayed for multiple user names:

- “Audit and log management” on page 360

- “Backup critical console data” on page 351
- “Change password ” on page 353
- “Configure 3270 emulators” on page 93
- “Customize console date and time” on page 83
- “Customize network settings” on page 81
- “Customize scheduled operations” on page 353
- “Format media” on page 358
- “Hardware messages” on page 360
- “Lock console ” on page 362
- “Manage print screen files” on page 362
- “Network diagnostic information” on page 363
- “Password protect console” on page 364
- “Save/restore customizable console data” on page 364
- “Save upgrade data” on page 364
- “Shutdown or restart” on page 365
- “Users and tasks” on page 368
- “View console events” on page 369
- “View console information” on page 370
- “View console tasks performed” on page 373
- “View licenses” on page 374

Analyze console internal code

This task is used to work with temporary internal code fixes or to debug problems if errors occur during a code fix install. This task should only be invoked by your IBM Customer Engineer or when directed by IBM Product Engineering. You must log on with a console user name of SERVICE to use this task.

For details, see *Z Service Guide for TKE Workstations*.

Archive security logs

This task saves the TKE console's default security log to a USB flash memory drive, then erases up to 80 percent of the oldest entries to make room for additional audit records. You must log on with a console user name of AUDITOR to use this task.

See “Archive security logs” on page 235 for more information.

Authorize internal code changes

This task is used to verify or change the setting that allows using this TKE workstation to perform installation and activation of internal code changes and other subsequent operations. This task should only be invoked by your IBM Customer Engineer or when directed by IBM Product Engineering. You must log on with a console name of SERVICE to use this task.

For details, see *Z Service Guide for TKE Workstations*.

Backup critical console data

This task performs the same operation as the 'Backup critical hard disk information' operation in the **Customize Scheduled Operations** task. This task performs the operation immediately rather than at a scheduled date and time. The operation copies critical files from the Trusted Key Entry workstation to a USB flash memory drive, an FTP server, or both.

To invoke this task, log on as either ADMIN or SERVICE, click on Service Management and then click on Backup Critical Console Data.

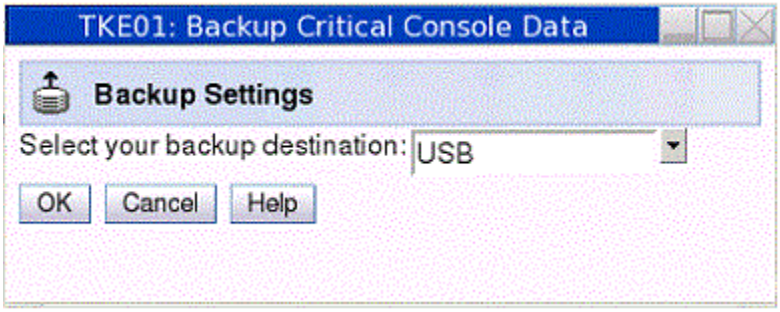


Figure 317. Backup Critical Console Data -- select backup destination

You are asked to select the destination of the backup data. You can select a USB flash memory drive, an FTP server, or both. If a USB flash memory drive is selected as a backup destination, it must be formatted with a volume identification of ACTBKP using the **Format Media** task. To select an FTP server as a backup destination, you must first configure the server using the **Configure Backup and Upgrade Settings** task.

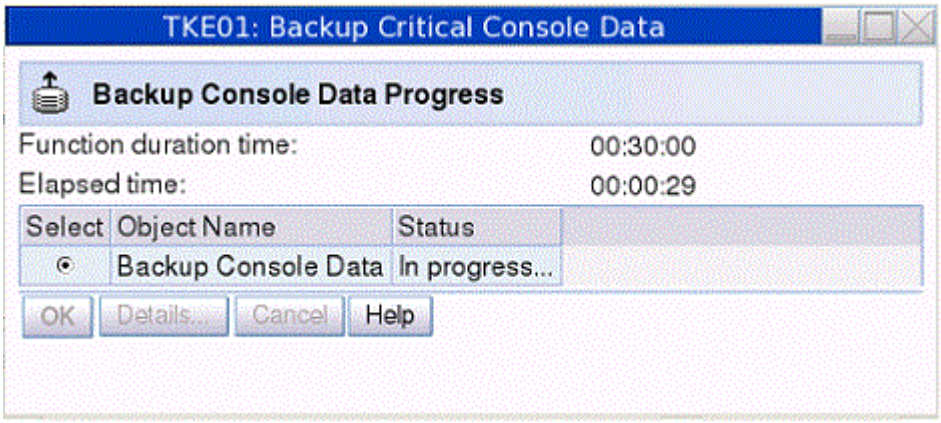


Figure 318. Backup Critical Console Data -- in progress

When the operation is complete, the status field will be updated to indicate success.

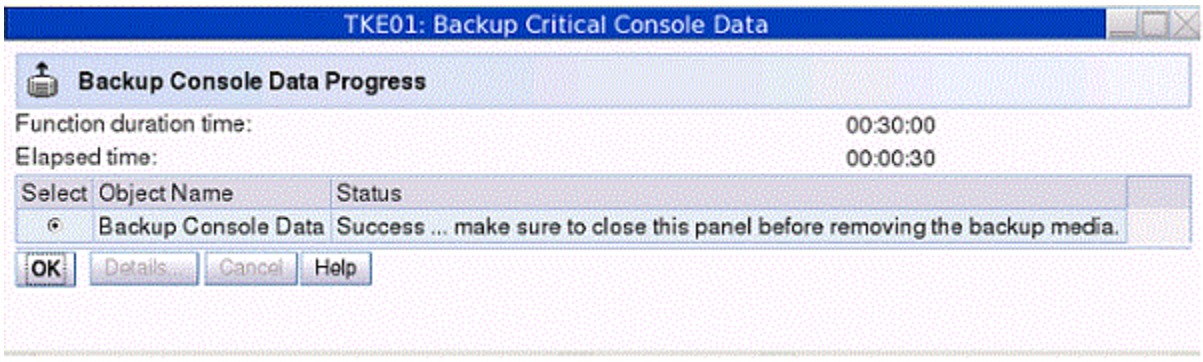


Figure 319. Backup Critical Console Data -- final status

Change console internal code

This task is used to work with internal code changes for the TKE workstation. Code changes can be retrieved, installed and activated, removed, and accepted. **This task should only be invoked by your IBM Customer Engineer or when directed by IBM Product Engineering.** You must log on with a console name of SERVICE to use this task.

For details, see *Z Service Guide for TKE Workstations*.

Change password

The Trusted Key Entry workstation is shipped with predefined console user names and default passwords. The Change Password task appears in the Service Management tree when you are logged on as any of the following Privileged Mode Access user IDs.

- ADMIN - the default password is PASSWORD
- AUDITOR - the default password is PASSWORD
- SERVICE - the default password is SERVMODE

After logging on the first time with one of these console user names, the user should change the password by selecting **Service Management** and **Change Password**.

If you are logged on as ADMIN, you can change the ADMIN, AUDITOR, and SERVICE passwords. If you are logged on as AUDITOR or SERVICE, you can change only your own password.

When the task is executed, the user is required to enter the current password and then the new password twice. When done successfully, and if the new password conforms to the password rules, the task ends.

Note: When the TKE workstation is migrated to a new version, the password values are preserved. They do not revert to the default values.

Password requirements

Password requirements for the user's password are as follows:

- Password must be between 4 and 8 characters.
- The password may be alphanumeric but may not contain any special characters.

No other restrictions, such as password history rules or repeating characters, apply.

Customize scheduled operations

Use this task to customize a schedule for backing up critical hard disk information to USB flash memory drive. You must log on with a console user name of SERVICE or ADMIN to use this task.

It is important to back up critical console data regularly so that the latest system changes and updates are available for recovery situations.

Note: The USB flash memory drive that is used for the backup must be formatted with the label ACTBKP. See “Format media” on page 358 for details.

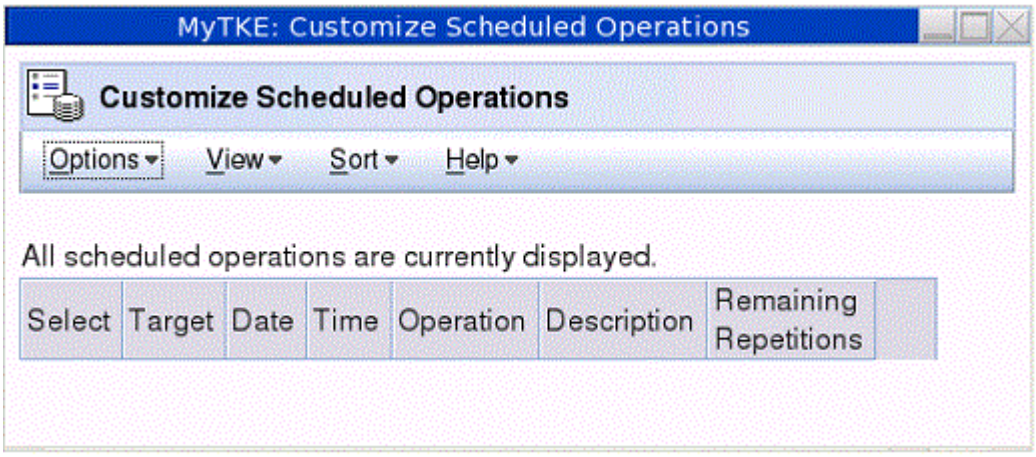


Figure 320. Customize Scheduled Operations task window

The backup USB flash memory drive is intended for use only during a hard disk restore operation, which completely replaces the contents of the hard disk drive. The hard disk restore operation loads the system

image from the installation DVD (shipped with your TKE workstation) and then restores the data from the backup USB flash memory drive.

The backup USB flash memory drive includes any microcode fixes (MCFs) and microcode loads (MCLs) that were applied to the system. Also included is TKE-related data. After the restore/reload operation the system is back to the service level and TKE level of the last backup.

Scheduled operations are helpful for situations where automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance. A schedule can be set for one operation or repeated many times.

To open this task, click **Service Management** and then click **Customize Scheduled Operations**.

The **Customize Scheduled Operations** window opens.

Click **Options** on the menu bar to select:

New
To create a new scheduled operation

Delete
To remove a scheduled operation

Refresh
To update the current list of scheduled operations

Select All
To choose all scheduled operations that are currently displayed

Deselect All
To clear all scheduled operations that were currently selected

Exit
To exit this task

When **New** is selected from the **Options** menu, the **Add a Scheduled Operation** window opens.

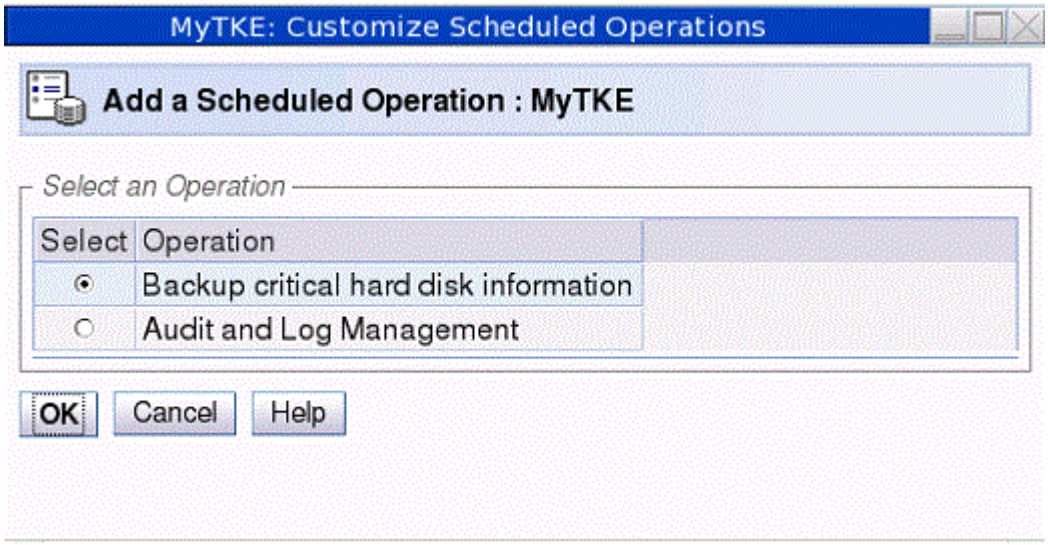


*Figure 321. Customize Scheduled Operations - **Add a Scheduled Operation** window*

Clicking **OK** opens a window in which the time, date, and repetition rate of the operation can be specified.

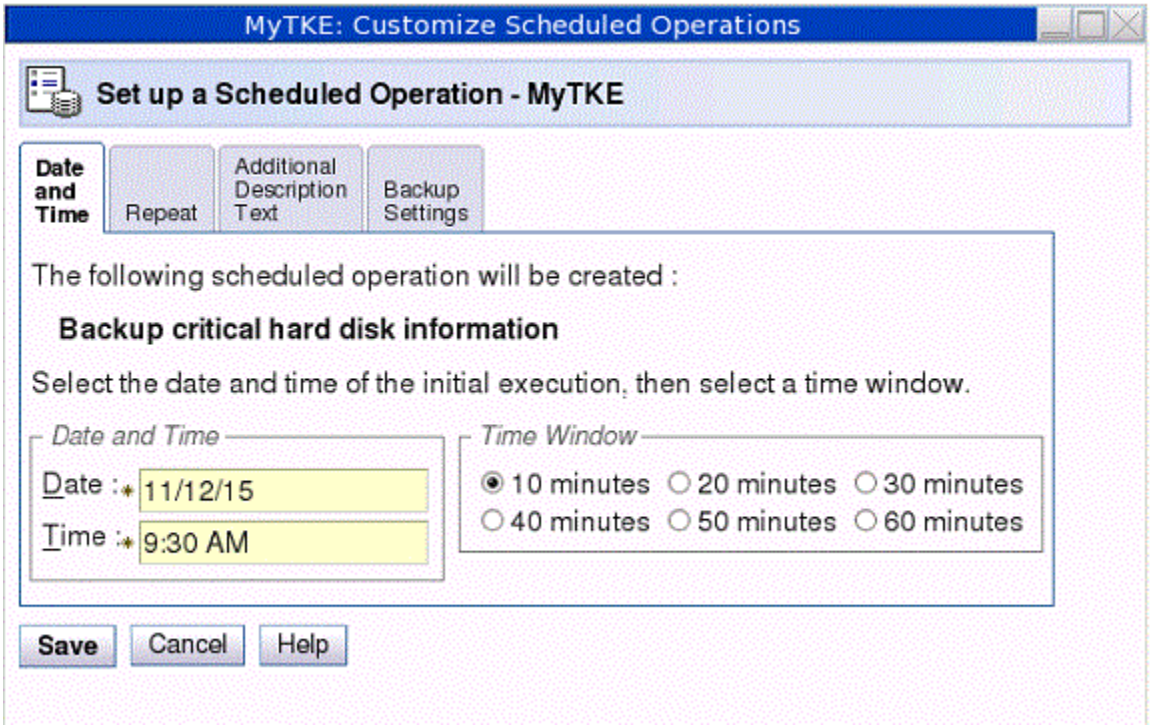


Figure 322. Customize Scheduled Operations - Set Date and Time window

Enter the date and time for a scheduled operation in the **Date and Time** area. The **Time Window** area defines the time frame in which the scheduled operation must start.

After you specify the date, time, and time window, click the **Repeat** tab.

Select whether the operation is a single occurrence or repeats. Select the days of the week you want to perform the operation. The **Interval** field specifies the number of weeks to elapse before the scheduled operation is performed again. The **Repetitions** field specifies the number of times you want the scheduled operations to be performed.

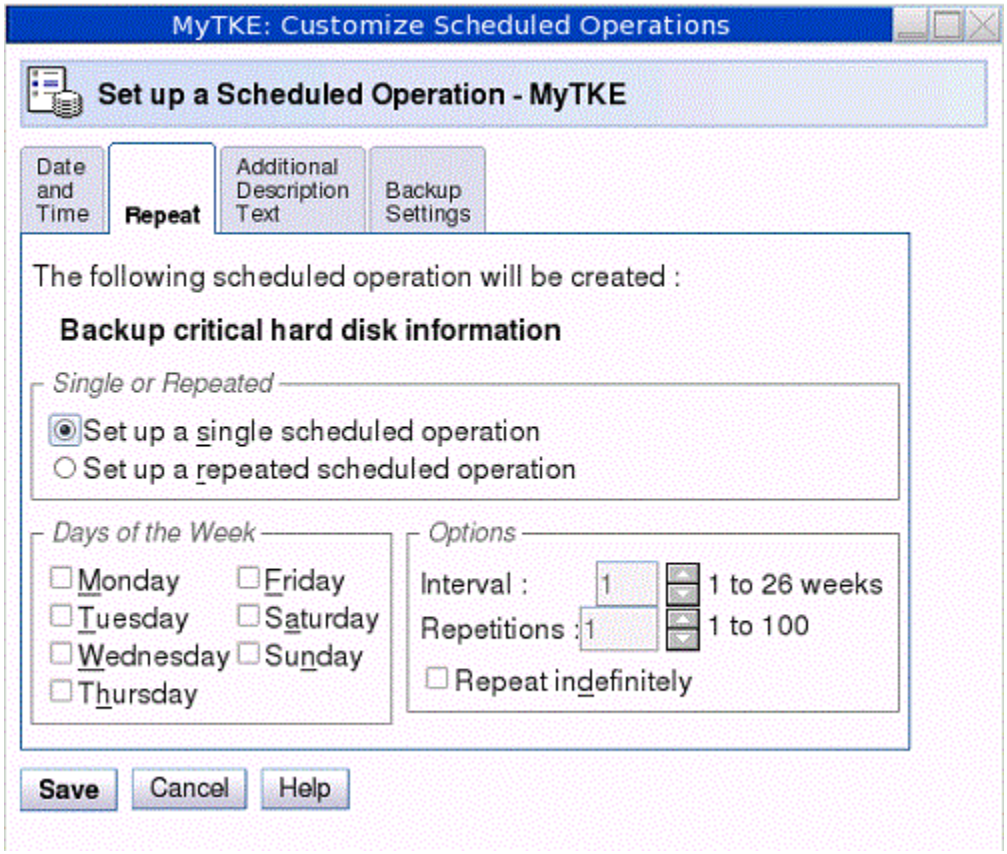


Figure 323. Customize Scheduled Operations - Set repetition of operation

After all the information is selected, click **Save** to complete the scheduling of the operation.

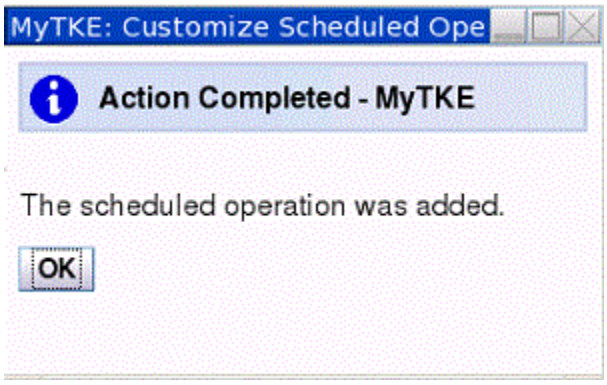


Figure 324. Completion window for Adding Scheduled Operation

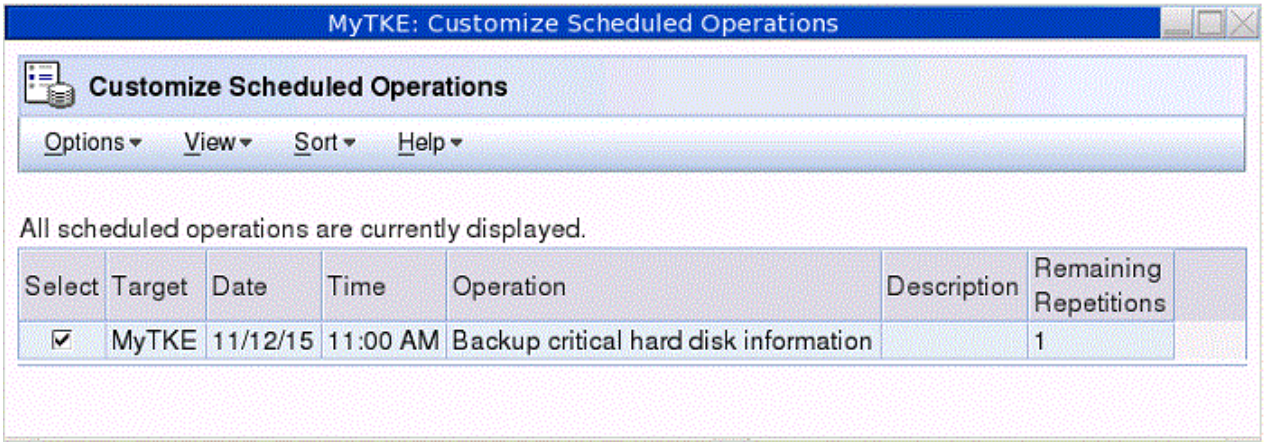


Figure 325. Customize Scheduled Operations

Click **Sort** on the menu bar to specify how you want to view the list of scheduled operations: by date and time, by object, or by operation. The **Date and time** option sorts the list according to date in descending order with the most recent operation at the top. The **By Object** and **By Operation** options have no meaning for TKE. The only object is TKE and the only operation is Backup Critical Console Data.

Click **View** on the menu bar to select:

Schedule Details
Used to display schedule information for the selected scheduled operation. For TKE, Object and Operation are not relevant.

New Time Range
Used to specify a definite time range (days, weeks, months, or displayed scheduled operations) for the selected operation.

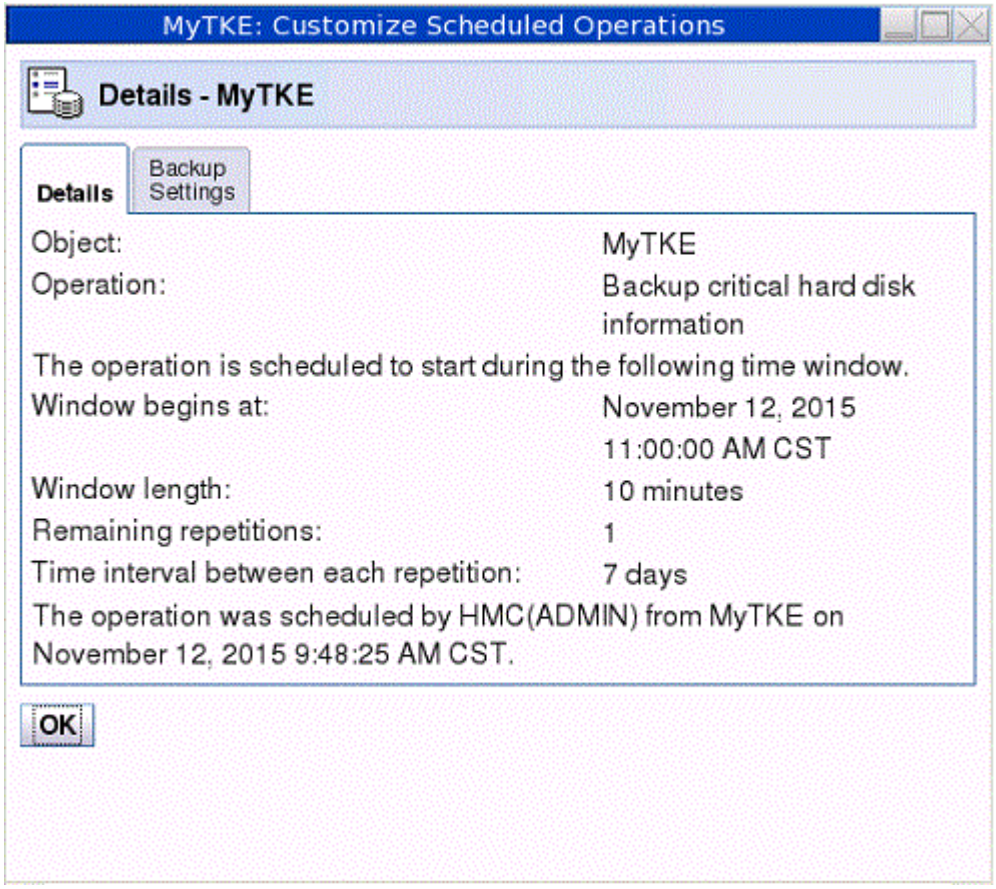


Figure 326. Details view of scheduled operation

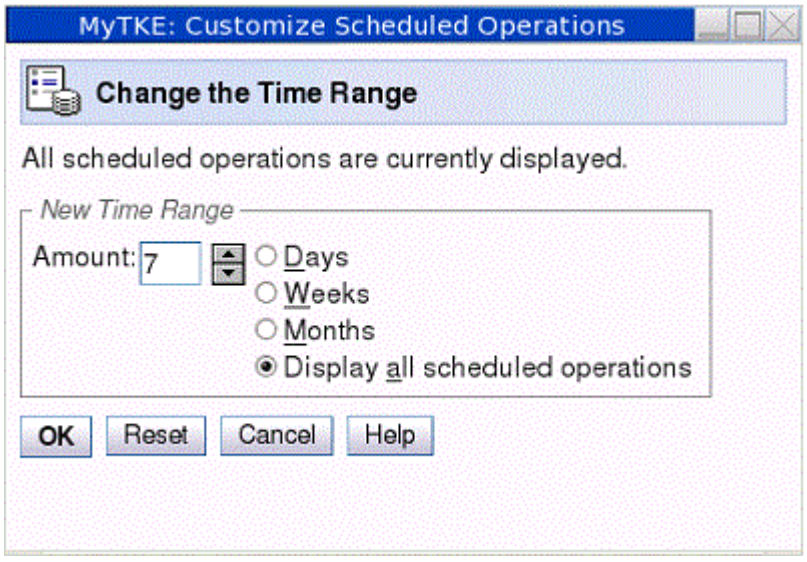


Figure 327. New time range window for scheduled operation

Format media

The Format Media task is used to format USB flash memory drives.

1. To invoke this task, click on **Service Management** and then click on **Format Media**.

   The Format Media dialog is displayed.

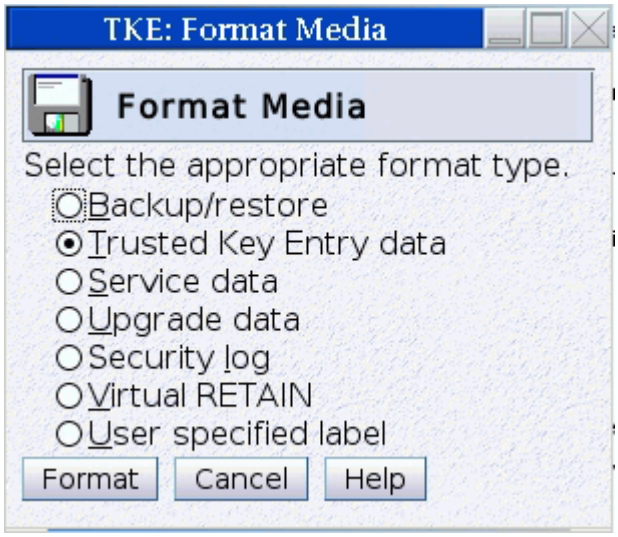


Figure 328. Format Media dialog

2. In the Format Media dialog, select the appropriate format type from the list. The format type you select will determine how the media is formatted and what label is written on it.

Table 38. Allowable labels when formatting USB flash memory

Format	Label	Description:
Backup/restore	ACTBKP	This formatted media is used in the Backup Critical Console Data task and the Customize Scheduled Operations task. To choose this format type, select Backup/restore.
Trusted Key Entry data	TKEDATA	This formatted media is used in the TKE applications and tasks. TKE data can be related to TKE, SCUP, CNM, the Migration utility, or user defined. To choose this format type, select Trusted Key Entry data.
Service data	SRVDAT	This formatted media is used in the Transmit Console Service Data task. To choose this format type, select Service data.
Upgrade data	ACTUPG	This formatted media is used in the Save Upgrade Data task. To choose this format type, select Upgrade data.
Security log	ACTSECLG	This formatted media is used in the Archive Security Logs or the Log Offload Support for Customer Audit tasks. To choose this format type, select Security log.

Table 38. Allowable labels when formatting USB flash memory (continued)		
Format	**Label**	**Description:**
Virtual RETAIN	VIRTRET	This formatted media is used in the Offload Virtual RETAIN Data to Removable Media task. To choose this format type, select Virtual RETAIN.
User-specified label		

3. In the Format Media dialog, click the **Format** push button. If you selected "User specified label", a dialog will prompt you for a label name. Type in the name, and click the **Format** push button.

   The Select Media Device dialog is displayed.

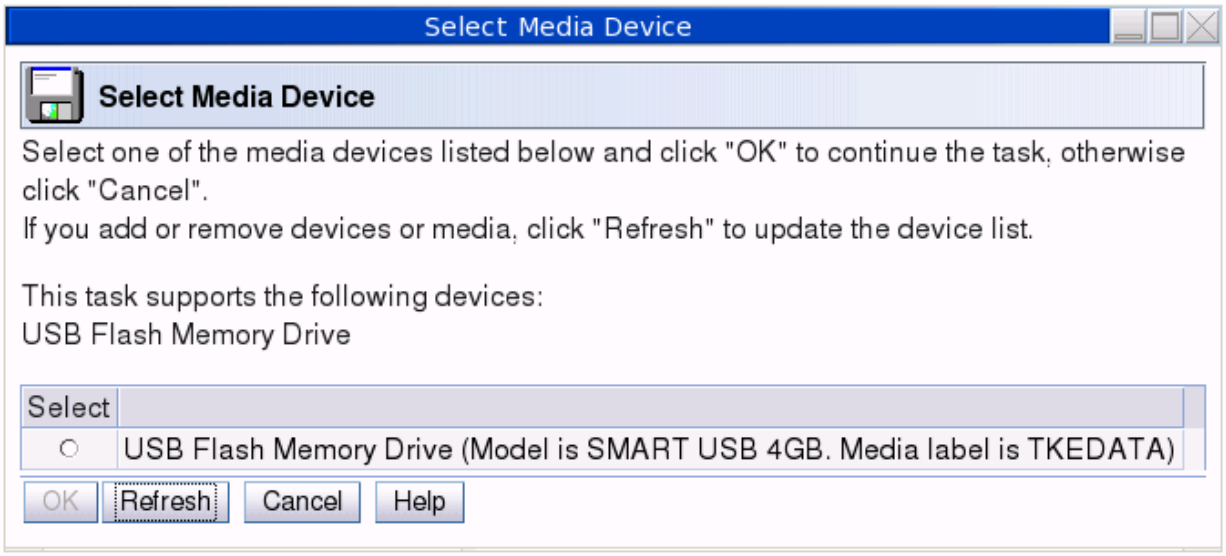


Figure 329. Select Media Device

4. In the Select Media Device dialog, select the radio button for the desired device, and click the **OK** push button.

   A confirmation dialog displays a warning that the format media action will remove all data on the removable media selected.

5. If you wish to continue the format media action, click the confirmation dialog's **Yes** push button.

   An informational window will display when the Format Media action has completed.

Audit and log management

This task copies the TKE console's default security log to an ASCII format file on a USB flash memory drive. The default security log on the TKE console is not changed. You must logon with a console user name of AUDITOR to use this task. See “Audit and log management” on page 231 for more information.

Hardware messages

This task displays messages about hardware activity on the Trusted Key Entry workstation.

When the green 'Status OK' icon (lower left corner of the TKE Console), changes to the blue 'Status Messages' icon it indicates that a Hardware Message is pending. The message can be viewed by clicking on the Status icon or by invoking this task.

To invoke the Hardware Messages task, click on Service Management and then click on Hardware Messages.

Messages are listed from the oldest to the newest message, with the oldest message displayed at the top of the list.

Date
Displays the date the message was sent.

Time
Displays the time the message was sent.

Message Text
Displays the message.

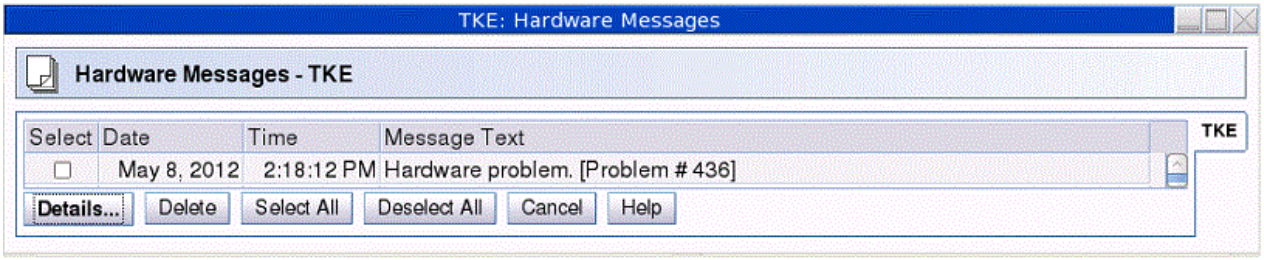


Figure 330. Hardware Messages window

Hardware messages notify you of events that involve or affect the TKE workstation hardware or internal code.

To promptly view, act on, or delete messages:

1. Select a message, then click Details to display details.

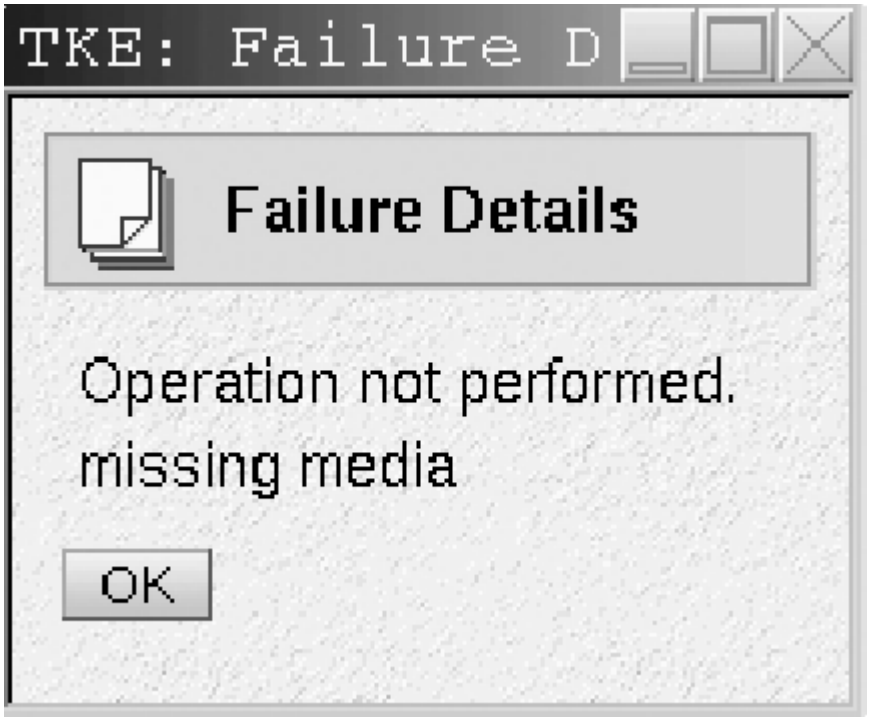


Figure 331. Hardware Messages - details window

2. If messages details are available and intervention is required, perform the action recommended in the details.
3. To delete the selected message, click Delete.

A message is displayed until an action causes it to be deleted.

Some messages are deleted automatically after the message or its details are displayed, if available. These messages generally provide information only, and are deleted automatically because no further action is required.

Messages that require further action provide message details that include a recommended action. The message and its details remain available until it is deleted manually. This allows reviewing the message details to assist intervention. But the message must be deleted when its information is no longer required.

Deleting messages provides greater assurance that new messages will be displayed as they are received.

Lock console

This task is used to allow customers to lock the TKE console. The Lock Console task appears in the Service Management tree when you are logged in as ADMIN, SERVICE, AUDITOR, or TKEUSER.

To invoke this task, click on Service Management and then click on Lock Console.

This task prompts the user for a password in order to lock the TKE console. Passwords can be up to any 12 characters except a space, backspace (\), *, and -. If any of these characters are entered you will receive an error message.

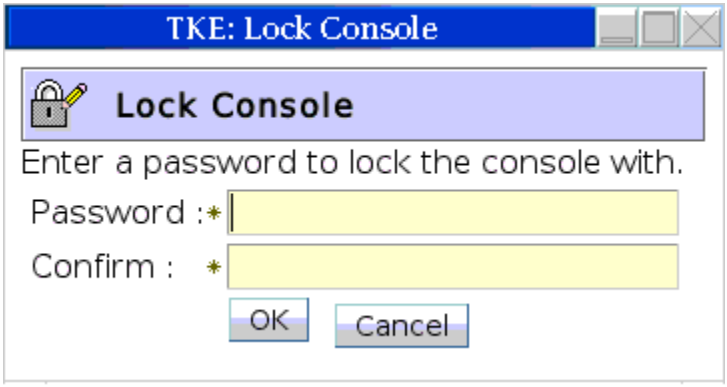


Figure 332. Prompt for password

The user must enter a password and confirm it.

Once you have entered a password value, confirmed it, and selected **OK**, a screen saver will lock the TKE Console. To unlock the console, move the mouse or touch the keyboard and you will be prompted for the password.

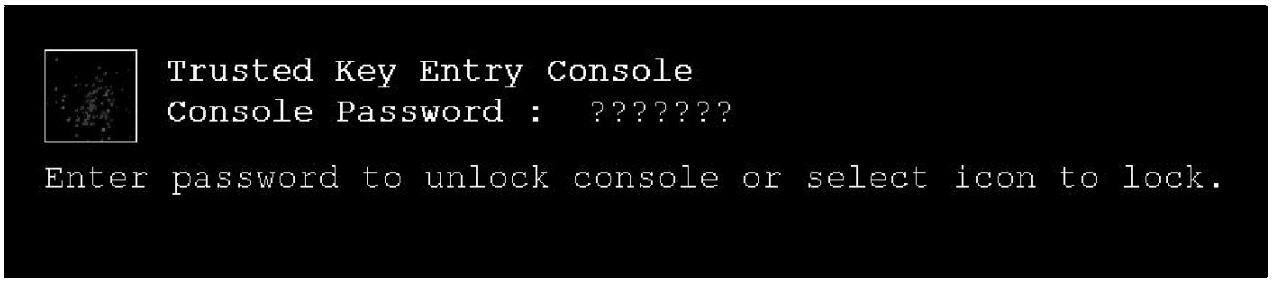


Figure 333. Prompt to unlock console

At the Console Password prompt, each keystroke appears as a question mark on the password prompt. If the correct password is entered, the user returns to the TKE console. If an incorrect password is entered, an error message will be displayed informing the user.

Manage print screen files

The Manage Print Screen Files task can be used to print individual windows on the TKE console to a file or to print the entire screen. Print screen files can be viewed, copied to a USB flash memory drive, and deleted using this task.

Network diagnostic information

The Network Diagnostic Information task displays network information such as TCP/IP addresses and Ethernet settings. It can test network connections by sending an echo request (ping) to a remote host.

Rebuild vital product data

This task is used to rebuild the Vital Product Data for the TKE machine.

Note: This task will only be displayed when logged on with the SERVICE user name.

Offload virtual RETAIN data to removable media

Note: This task will only be displayed when logged on as the SERVICE ID.

This task is used to select, by problem number, specific virtual RETAIN data to offload to a USB flash memory drive.

To invoke this task, click on Service Management and then click on Offload Virtual RETAIN Data to removable media.

Note: The removable media must be formatted with volume identification label VIRTRET, using the Format Media task.

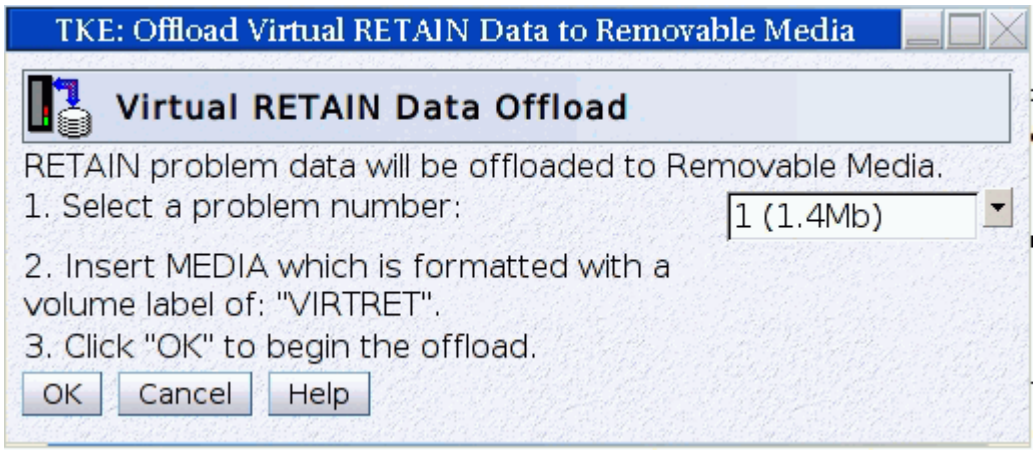


Figure 334. Virtual RETAIN Data Offload window

In the Virtual RETAIN Data Offload window, select the Problem Number and click OK. The selected virtual RETAIN data is off-loaded to the removable media.

When the virtual RETAIN data is offloaded successfully, a message is displayed indicating the offload was successful.

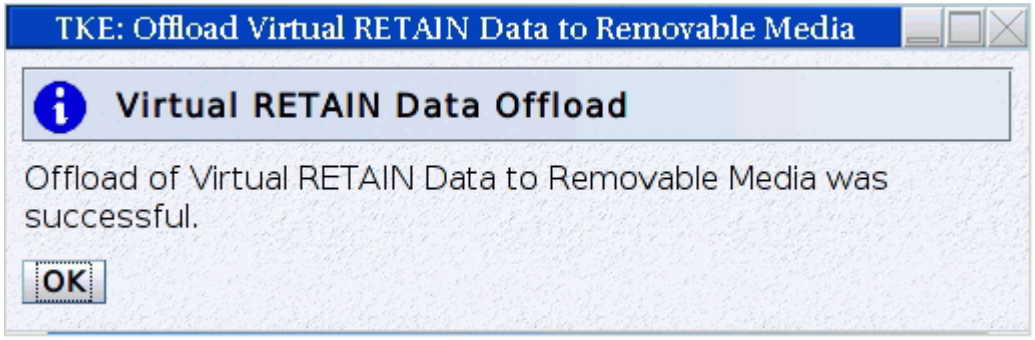


Figure 335. Successful offload of data

If you insert removable media that has not been formatted or that has the wrong label, an error message is displayed.



Figure 336. Virtual RETAIN Data Offload incorrect media error

Password protect console

This task allows you to require a password for the default console user and to specify the password value.

You can also use this task to change the current password for the default console user or to specify that a password is no longer required.

Save/restore customizable console data

This task allows you to save and restore console data using USB memory or an FTP server. You can select to save or restore console user passwords, TKE data files, or both.

This task can be used to transfer console data to a different TKE or to recover console data after an install. You must be logged on the console as ADMIN or SERVICE to use this task.

Save upgrade data

The Save Upgrade Data task is used when a customer is upgrading to a new TKE image. The task should only be executed when an engineering change (EC) upgrade or miscellaneous equipment specification (MES) instructs you to save the Trusted Key Entry workstation's upgrade data. You must log on with a console user name of ADMIN or SERVICE to use this task.

All data pertinent to the TKE workstation (for example, TKE-related data directories, emulator sessions, and TCP/IP information) will be saved. Upgrading the Trusted Key Entry workstation requires saving its upgrade data before installing new EC or MES code, then restoring the upgrade data afterwards.

To invoke this task, click on Service Management and then click on Save Upgrade Data.

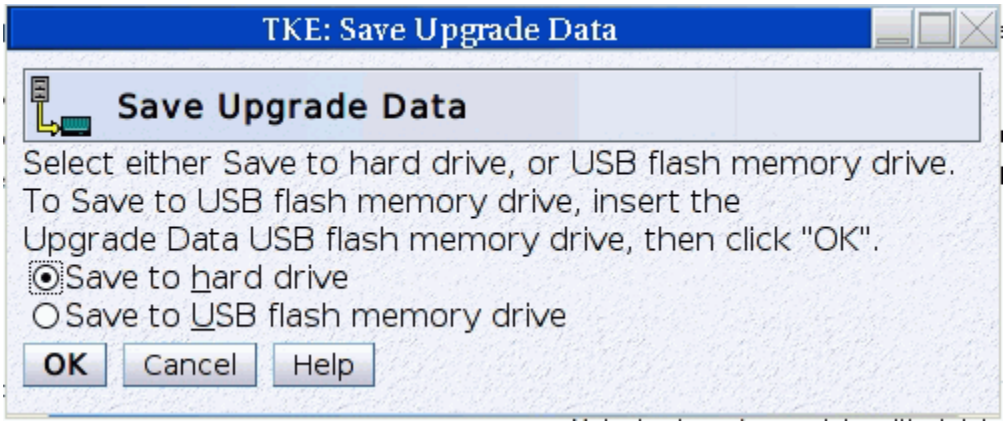


Figure 337. Save Upgrade window

Some upgrade procedures save and restore the Trusted Key Entry workstation's upgrade data automatically, and there is no need to use this console action. Otherwise, if you are following an upgrade

procedure that instructs you to save the Trusted Key Entry workstation's upgrade data, you must use this console action to save it manually.

Note: The USB flash memory drive for this task must be formatted with a volume identification label of ACTUPG, using the Format Media task.

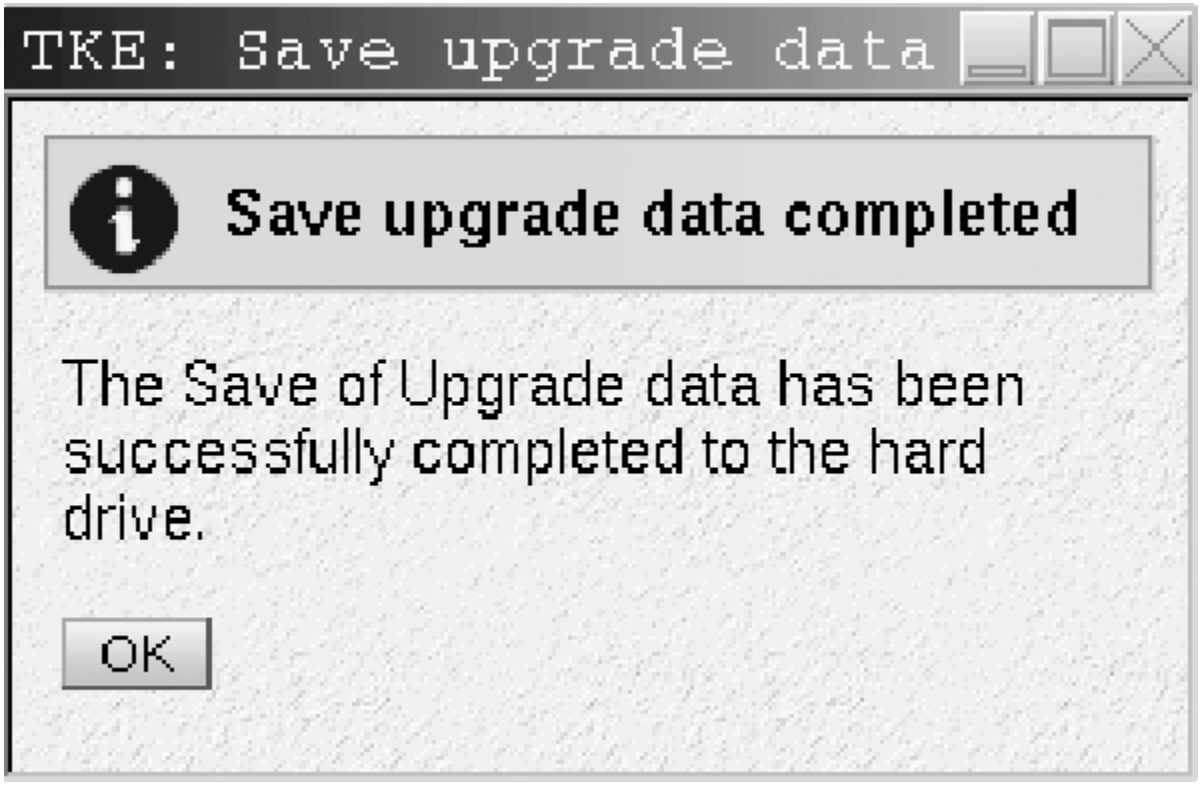


Figure 338. Save upgrade success window

Shutdown or restart

This task allows you to restart the application/console or power off.

To invoke this task, click on Service Management and then click on Shutdown or Restart.

The Shutdown or Restart dialog displays.

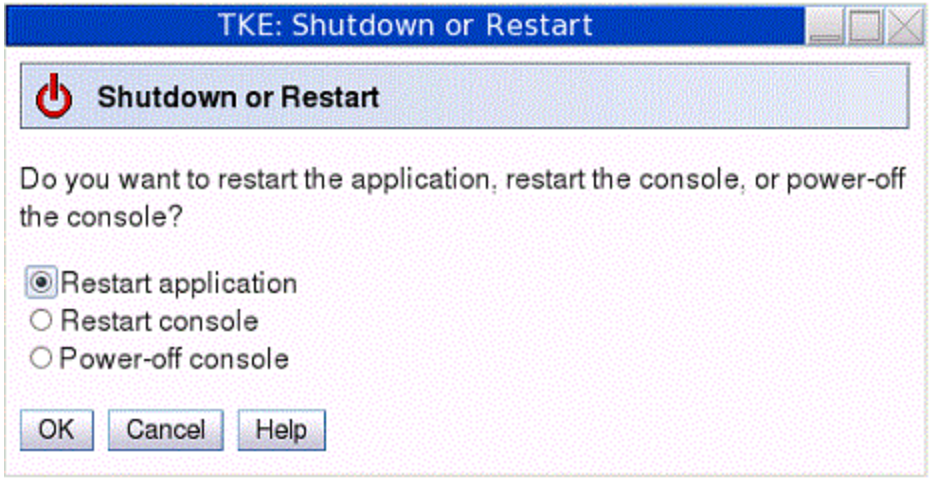


Figure 339. Shutdown or Restart task window

Select one of the following options from the dialog and press **OK**.

Restart Application
To close the Trusted Key Entry workstation and restart the application, select Restart application.

Restart Console
To close the Trusted Key Entry workstation, perform a system power-on reset, and restart the console, select Restart console.

Power-off console
To close the Trusted Key Entry workstation, shut down the operating system, and power-off the hardware, select Power-off console.

Selecting any option will present you with a confirmation window. Press **Yes** to continue.

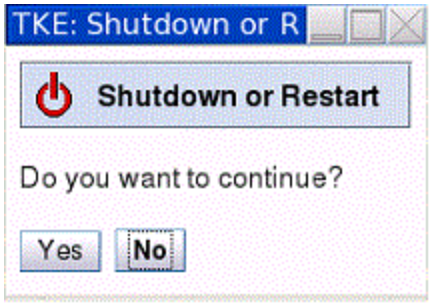


Figure 340. Confirmation window

Transmit console service data

This task is used to select the types of service data and the method to send the data to aid in the problem determination. You must log on with a console user name of SERVICE to use this task.

To invoke this task, click on Service Management and then click on Transmit Console Service Data.

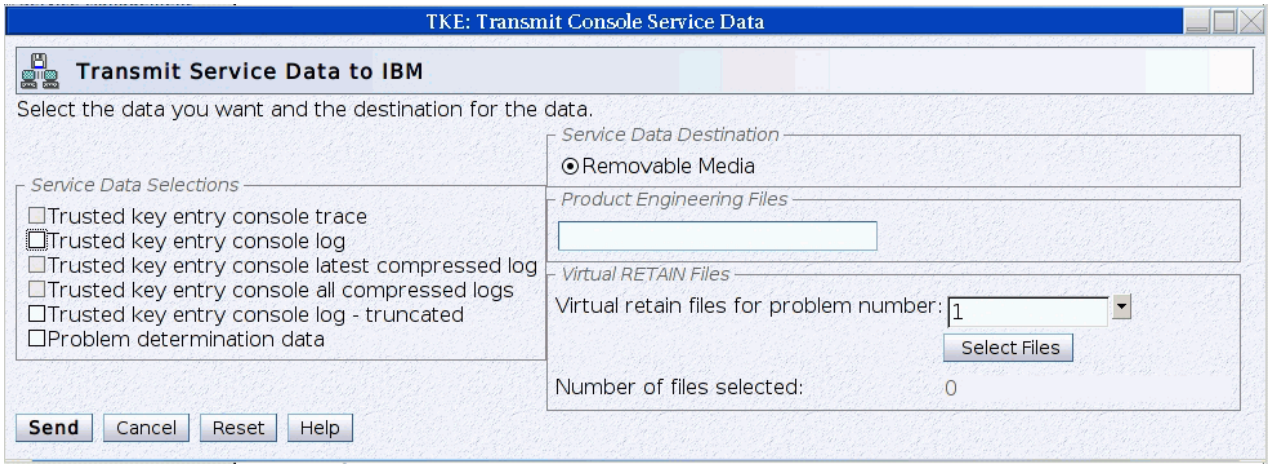


Figure 341. Transmit Console Service Data

Service data is a set of program and event traces and storage dumps. The data in the traces and the contents of storage assists in servicing the system.

Use the Transmit Console Service Data window only when directed by your service representative or support system. Select the service data categories requested by the support system. Service data in selected categories is collected in a file or group of files for transmission to the support system.

Note: Some service data categories may not be available for selection. Such categories appear grayed. This indicates that no data is available for that category.

Service Categories:

Service Data Selections
Use the displayed categories in this topic to select the types of service data to send to the support system.

Service Data Destination
Use this topic to specify how your service data is sent to the support system.

Virtual RETAIN Files
Use this topic to copy to a USB flash memory drive selected virtual RETAIN files for the specified problem number.

Note: You can select and copy virtual RETAIN files to a USB flash memory drive for only a single problem number at a time.

Note: When using a USB flash memory drive for service data it must first be formatted specifically for Service Data. See “Format media” on page 358 for details.

Successful completion will present the following window.

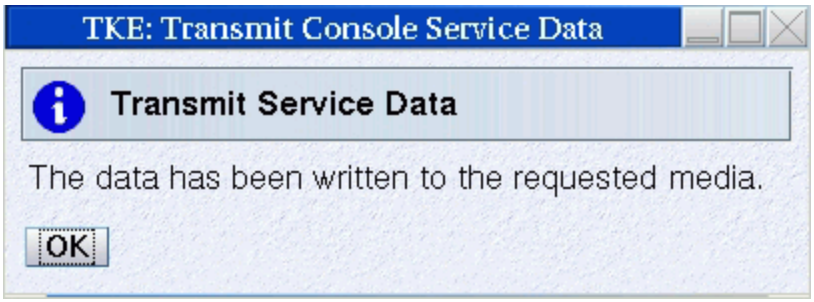


Figure 342. Transmit Console Service Data - successful completion

For Virtual RETAIN Files, enter the problem number in the Virtual RETAIN Files for Problem Number field and click on Select Files.

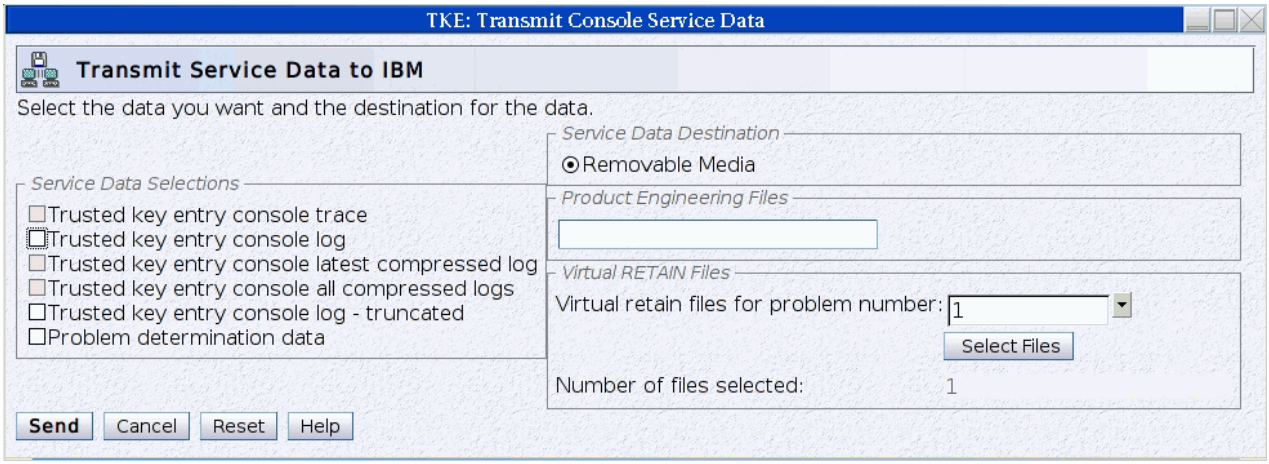


Figure 343. Update problem number for virtual RETAIN file

Select the applicable Virtual RETAIN Files and click OK.

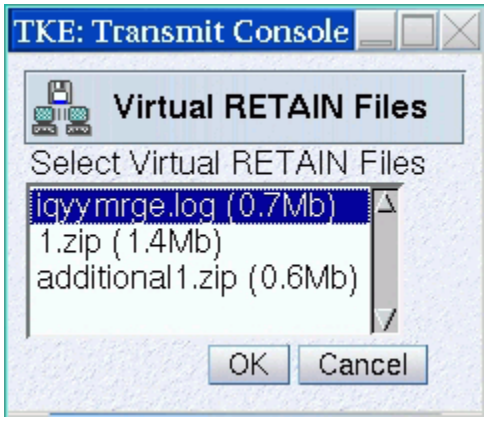


Figure 344. Select the virtual RETAIN files

Click on Send to transmit the selected Virtual RETAIN files to Media.

Insert the selected media when prompted.

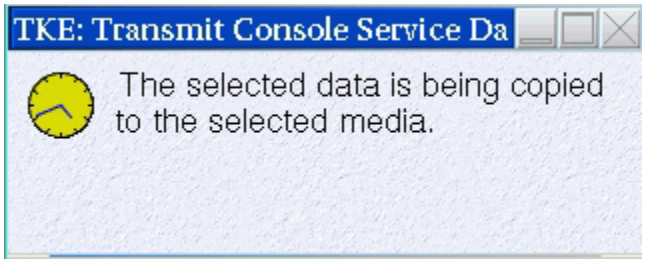


Figure 345. Copying data to selected media

An information window will display when the data has been written to the required media.

Users and tasks

The Users and Tasks task window displays the users and running tasks on the TKE Workstation and allows you to switch to a currently running task or terminate a task that perhaps will not complete.

You can only switch to Service Management type tasks. If you attempt to switch to a Trusted Key Entry task (Applications and Utilities) you will be presented with a window stating 'This function is not available for Trusted Key Entry tasks. Switch To only works with Service Management tasks'.

The Terminate option can be used to terminate either Trusted Key Entry tasks or Service Management tasks. The only exception is the Trusted Key Entry CCA CLU task. If you attempt to terminate CLU from this task you will be presented with a window stating 'You cannot terminate the CCA CLU Utility from the Login Details and Task menu. If you need to terminate CLU you must use the Exit option of the CLU Utility.'

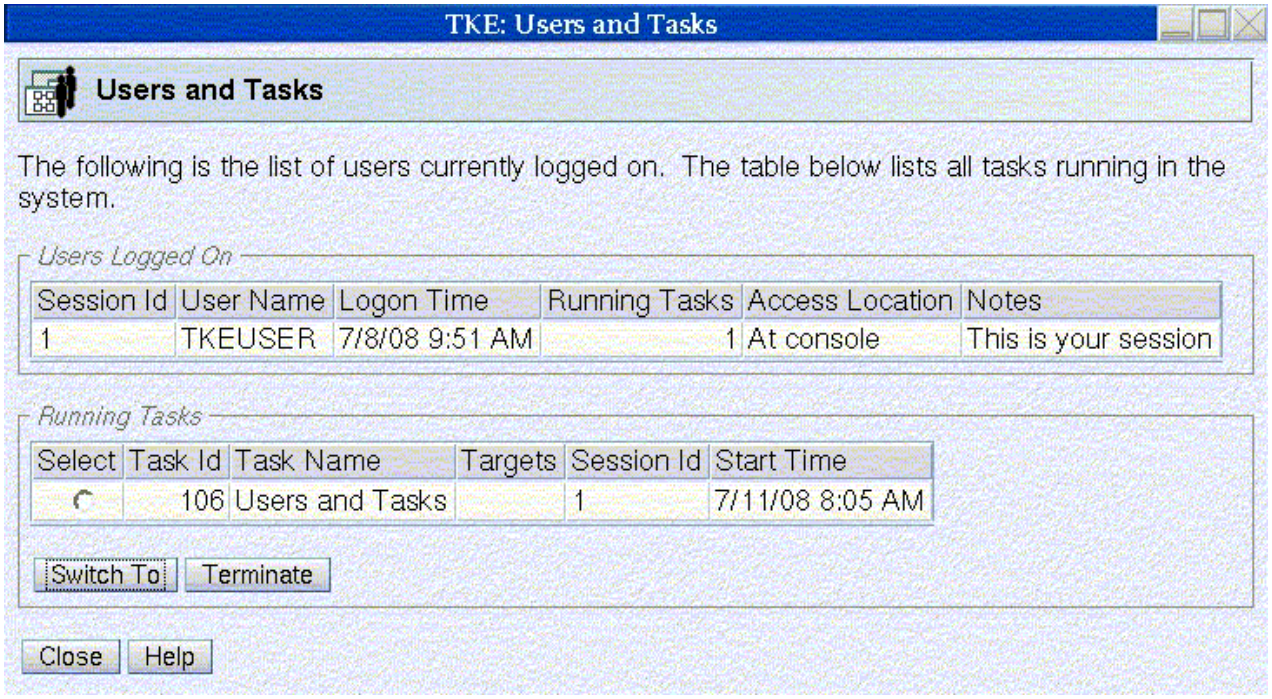


Figure 346. Users and Tasks window

View console events

This task displays console events logged by the Trusted Key Entry workstation.

To invoke this task, click on Service Management and then click View Console Events.

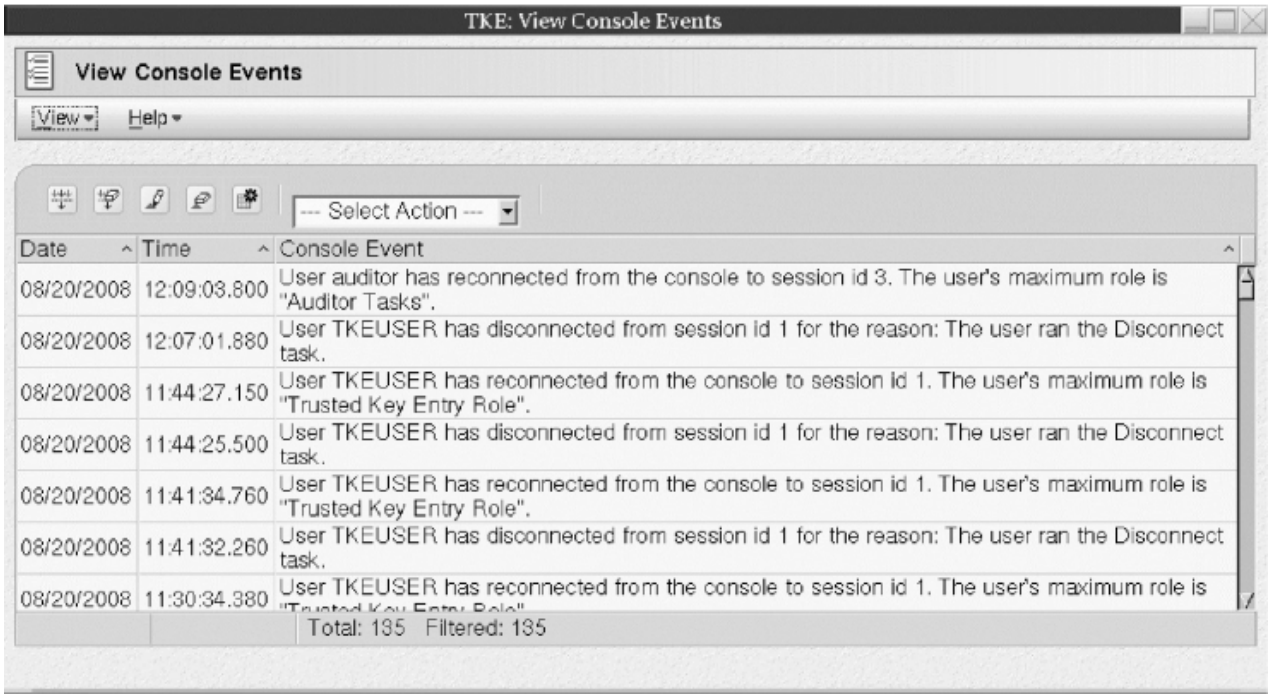


Figure 347. View Console Events window

The Trusted Key Entry workstation automatically keeps a log of significant operations and activities, referred to as console events, that occur while the application is running.

This window displays all console events currently logged and lists them in reverse order of occurrence, from the most recent event to the oldest event. You can select a different time and date range for the events displayed using an option on the View pull-down menu.

View console information

This task shows the Machine Information (Type, Model Number, and Serial Number) and the Internal Code Change History. The information contained here may be useful for problem determination.

To invoke this task, click on Service Management and then click on View Console Information.

The View Console Information window is displayed.

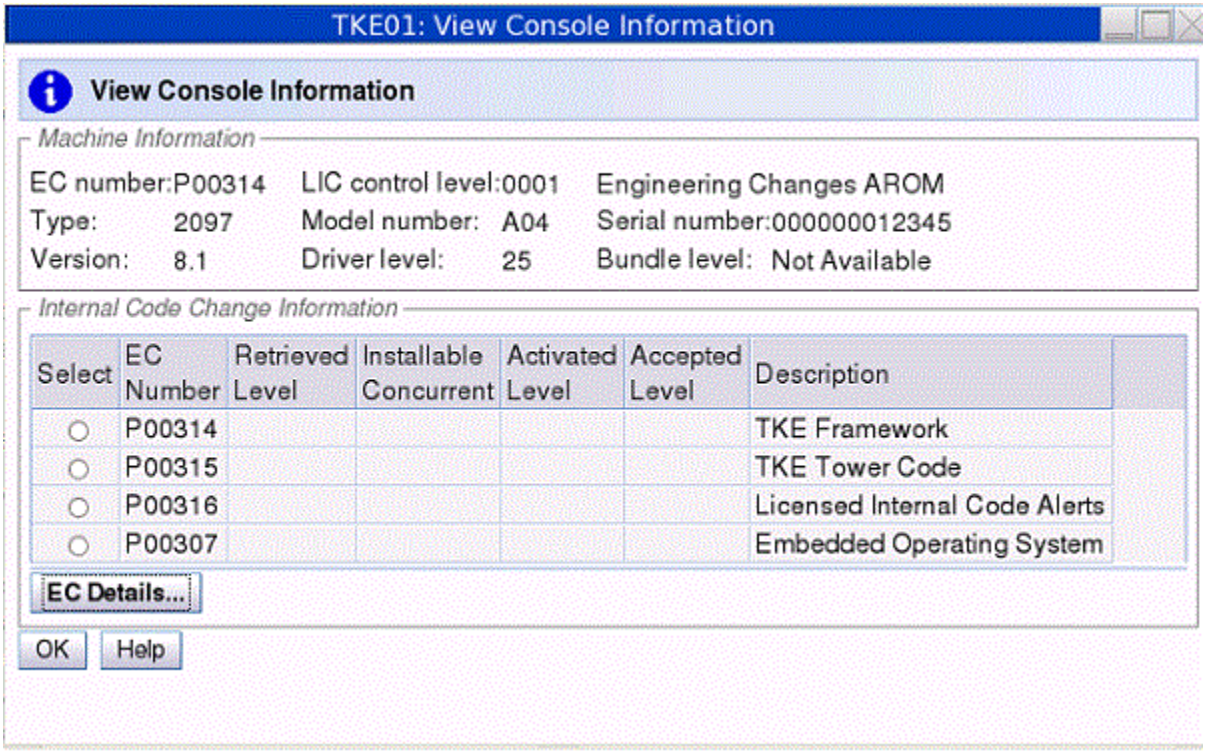


Figure 348. View Console Information window

For additional information about an internal code change, select an EC number, then click **EC Details**.

The Internal Code Change Details window is displayed.

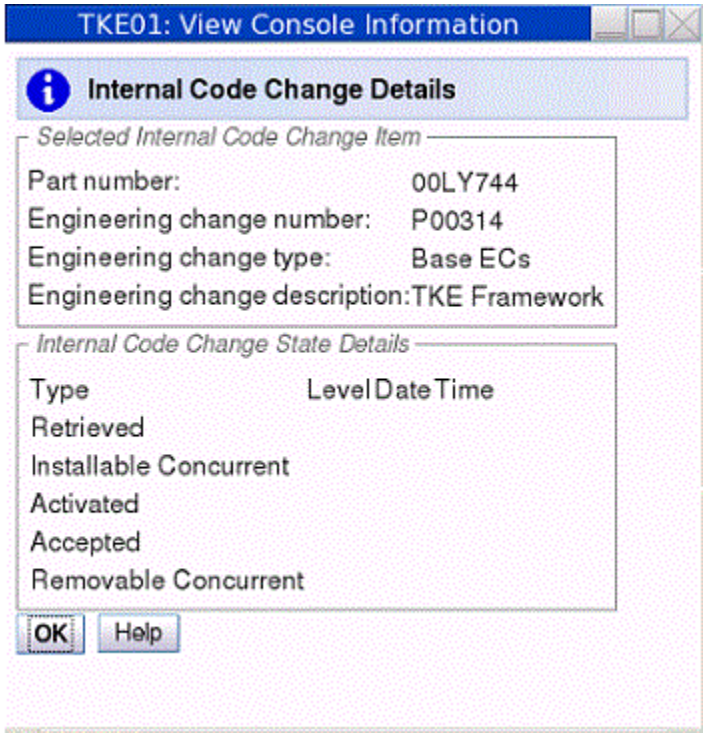


Figure 349. Internal Code Change Details window

The View Console Information window contains the following information.

EC Number
Displays the engineering change (EC) number of the internal code change.

Retrieved Level
Displays the internal code change level that was most recently copied to the console, making it available for installation.

Installable Concurrent
Displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for this console, from the current installed level up to and including the installable concurrent level, without disrupting the operations of this console.

Activated Level
Displays the internal code change level that was most recently activated as a working part of the licensed internal code of the console.

Accepted Level
Displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the console.

Removable Concurrent
Displays the lowest installed internal code change level that can be removed such that the remaining installed change level can be activated concurrently. That is, you can remove all change levels installed for this console, from the current installed level down to and including the removable concurrent level, without disrupting the operations of this console.

View console service history

The View Console Service History is used to review or close problems that are discovered by Problem Analysis. A problem is opened when Problem Analysis determines service is required to correct a problem.

To invoke this task, click on Service Management and then click on View Console Service History.

The View Console Service History window is displayed.

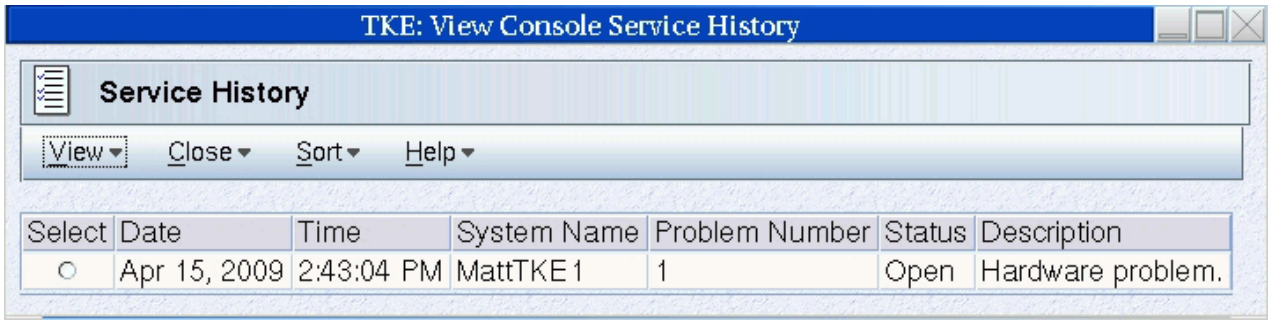


Figure 350. View Console Service History window

Each record of a problem includes detailed information about the problem and indicates whether the service required to correct the problem is still pending (Open), is already completed (Closed), or no longer needed (Closed).

View on the menu bar:

- **Problem summary** lists information about the problem and what actions are needed to diagnose and correct it.

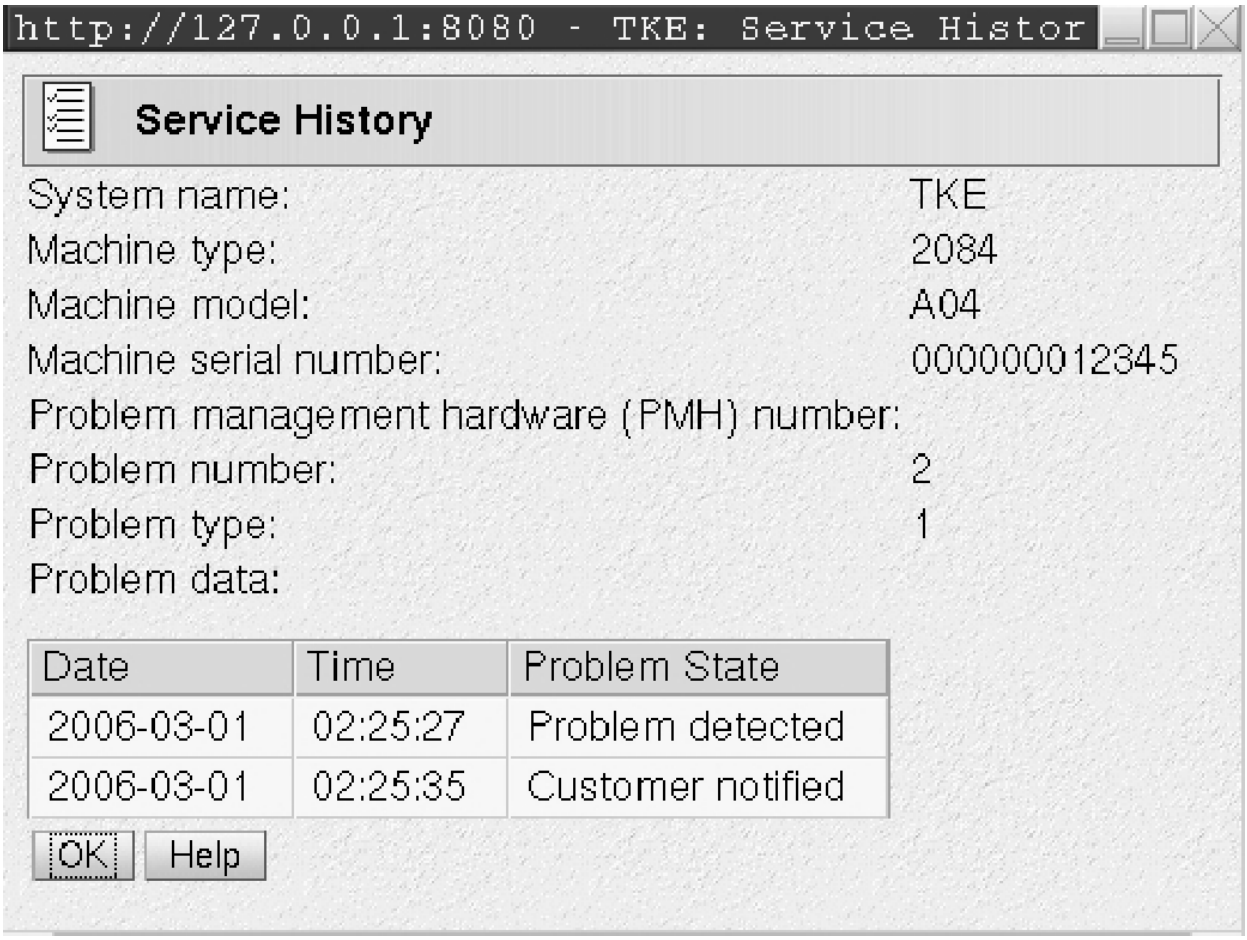


Figure 351. Problem summary

- The **Problem Analysis Panels** show System name, Date, Time, Problem Description, and Corrective Actions that a user can take.

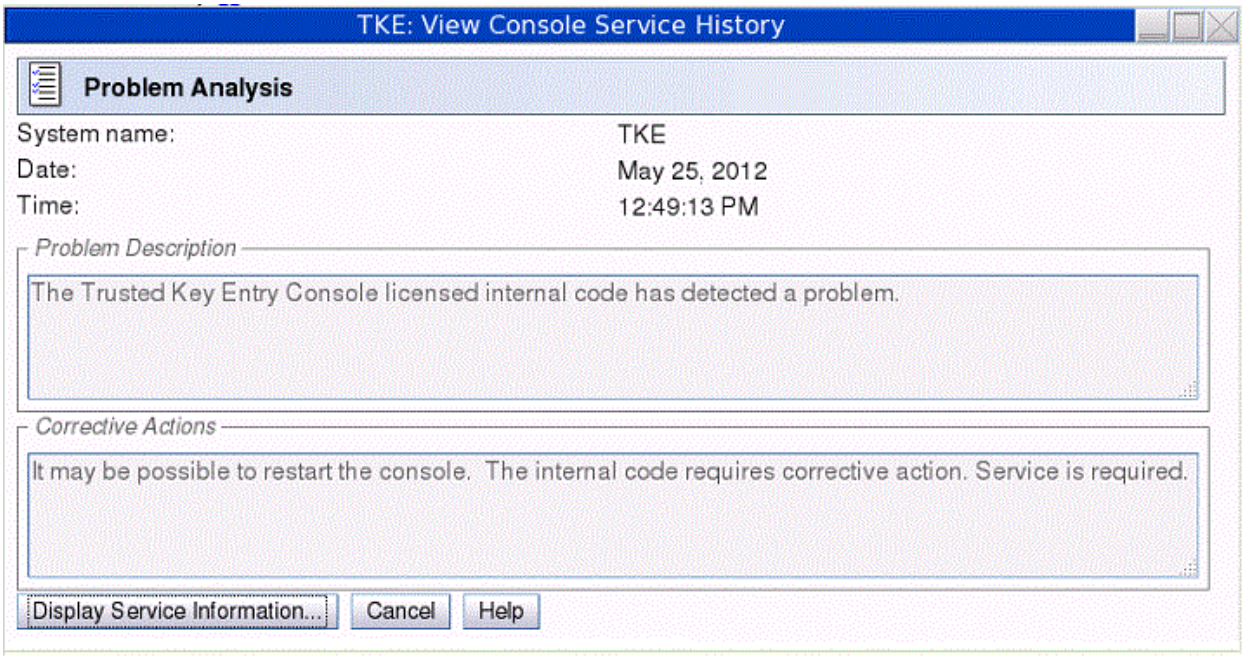


Figure 352. Problem Analysis

- **Cancel** exits this task and returns to the Trusted Key Entry Console.

Clicking **Close** on the menu bar brings up two options:

- **Selected Problem** changes the status of the selected problem to Closed.
- **All Problems** changes the status of all open problems to Closed.

View console tasks performed

The View Console Tasks Performed task window shows a summary of the console tasks performed with the date and time associated with each task. The most recent tasks invoked are appended to the bottom of the list. This information is useful in determining past activity performed on the TKE Workstation for auditing or problem determination.

To invoke this task, click on Service Management and then click on View Console Tasks Performed. The View Console Tasks Performed window is displayed.

You must scroll the display to the right until you see the inner right scroll bar for moving the display up and down.

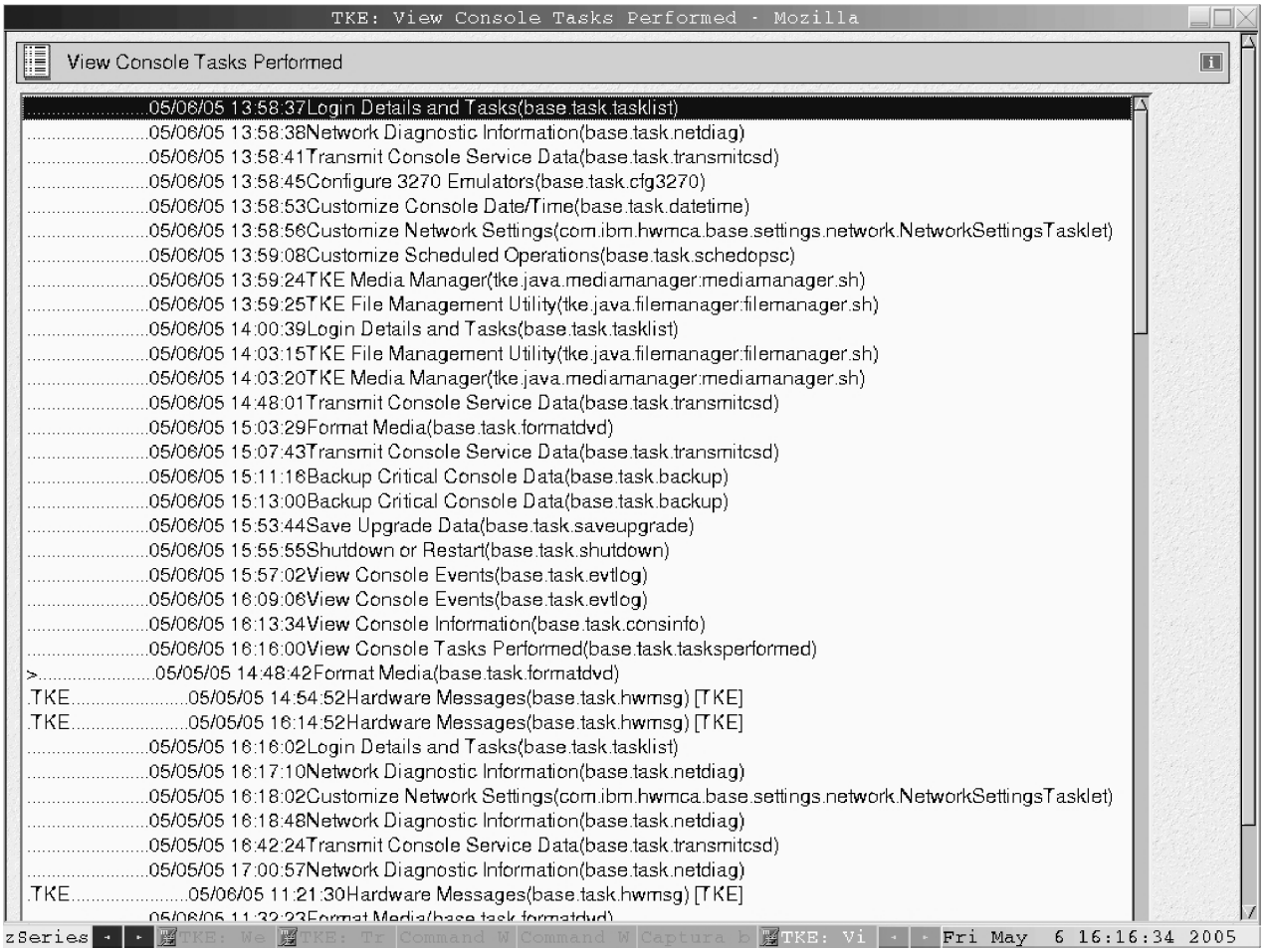


Figure 353. View Console Tasks Performed window

View licenses

This task is used to view the open source licenses for the Trusted Key Entry Console.

To view a specific license, click on it. When you are done viewing the license information click on **OK** to exit.

If you have not viewed any license information through this task, the first TKE related task that you invoke will display the license information. This will only be done once.

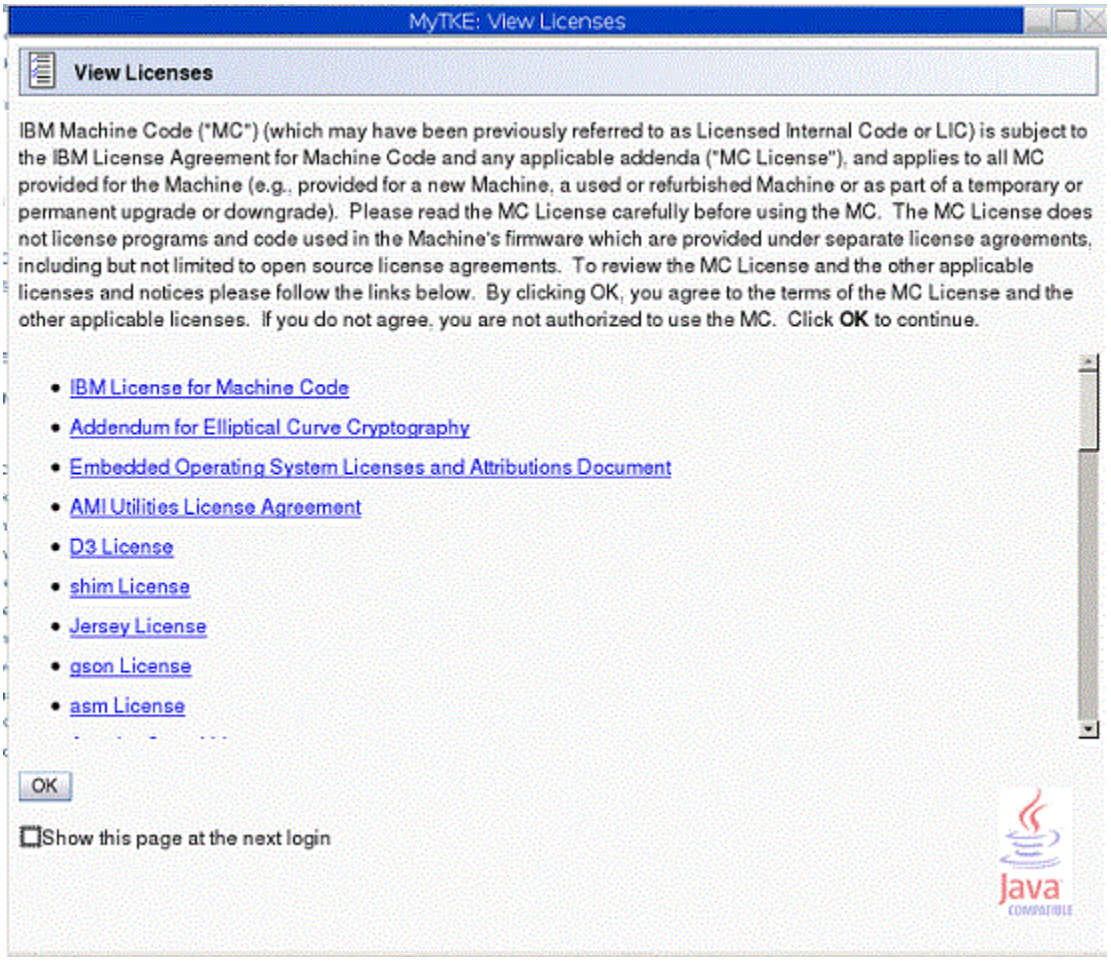


Figure 354. View Licenses window

View security logs

This task displays the TKE console's default security log. The security log is a record of the security-relevant events that have occurred on or have been initiated by the TKE workstation. You must log on with a console user name of AUDITOR to use this task.

See “View security logs” on page 230 for more information.

Appendix F. TKE best practices

This information describes the setup required for TKE to manage host crypto modules, and a set of setup steps to perform on the TKE workstation. TKE workstations initialized for passphrase and initialized for smart card use are considered separately.

Checklist for loading a TKE machine - passphrase

Expectations

- You are working with CCA host crypto modules
- The support element has enabled TKE on these host crypto modules
- LPARs are established
- TKE licensed internal code (LIC) is loaded on the TKE workstation
- Segments 1, 2, and 3 have been loaded on the TKE workstation crypto adapter
- The TKE host transaction program has been configured and started in the host TKE LPAR
- ICSF is started in each LPAR

Setup

- 2 TKEs both running the same level of software
  - One for production
  - One for backup
- 2 Central electronic complex (CEC) cards being shared
  - One Test LPARs (Domain 0)
  - Three Production LPARs (Domain 1, 2, 3)

  TKE can load the master key in a group of domains as defined by a domain group.
- Host TKE LPAR 1

  When defining the LPAR activation profile, the usage domain will be 1 and the control domain will be 0, 1, 2, 3.

The following User IDs are used to restrict access to the TKE workstation crypto adapter:

- TKEUSER - can run the main TKE application
- TKEADM - can create and update TKE roles and profiles
- KEYMAN1 - can clear TKE new master keys and load first master key parts
- KEYMAN2 - can load TKE middle and last key parts and reencipher TKE workstation key storage

Authorities are used to restrict access to the CCA crypto modules on the host machine.

One way to control access to CCA host crypto modules is with a minimum of seven host authorities.

- ISSUER
  - Disable host crypto module
  - Enable host crypto module issue
  - Access control issue
  - Zeroize domain issue
  - Domain control change issue
- COSIGN

© Copyright IBM Corp. 2000, 2021

  - Access control co-sign
  - Enable host crypto module co-sign
  - Zeroize domain co-sign
  - Domain control change co-sign
- MKFIRST
  - AES, DES, ECC (APKA), or RSA load first master key part
  - Clear new master key register
  - Clear old master key register
- MKMIDDLE
  - AES, DES, ECC (APKA), or RSA combine middle master key parts
- MKLAST
  - AES, DES, ECC (APKA), or RSA combine final master key part
  - Set RSA master key
- FIRSTCLEAR
  - Load first operational key part
  - Clear operational key register
- ADDCOMP
  - Load additional operational key part
  - Complete key

The following tasks should be run using the TKE workstation to set up the TKE workstation and the host crypto modules for use. Be aware that the Service Management tasks available to you will vary depending on the console user name you used to log on. Refer to "Service Management tasks" on page 350 for more information.

1. Customize Network Settings
2. Customize Console Date/Time
3. Initialize the TKE workstation crypto adapter for passphrase use
   a. Predefined TKE roles and profiles are loaded.
   b. The TKE master keys are set and TKE key storages are initialized.
4. Logon to CNM with KEYMAN1 - OPTIONAL
   a. Clear the new DES/PKA and AES master key registers
   b. Enter known first master key parts for the DES/PKA and AES master keys.
   c. Logoff
5. Logon to CNM with KEYMAN2 - OPTIONAL
   a. Enter known middle and last master key parts for the DES/PKA and AES master keys.
   b. Reencipher DES, PKA, and AES key storage
   c. Logoff
6. Logon to CNM with TKEADM
   a. Create user defined roles - OPTIONAL
   b. Create user defined profiles - OPTIONAL
   c. Create groups and add users - OPTIONAL

      Note: Group members should already be defined.
   d. Change the passphrases for all of the predefined profiles - TKEADM, TKEUSER, KEYMAN1, and KEYMAN2

7. Log on to the main TKE application with TKEUSER profile or another profile with the same authority
    a. Load the default authority key for key index 0
    b. Change these options of your security policy via the TKE preferences menu
        - Blind Key Entry
        - Removable media only
    c. Create a Host
    d. Create domain groups - OPTIONAL
    e. Open a host or a domain group (requires host logon)
    f. Open a crypto module notebook or domain group notebook
    g. Create role or roles
    h. Generate authority key or keys and save them to binary file or files
    i. Create different authorities using the different authority key or keys that were just generated.
    j. Delete the authority 00 or change the authority key to a key that is not the default key. If you delete authority 00 make sure that you have 2 other known authority keys that have the Domain control change issue and co-sign.
8. Configure 3270 Emulators
9. Backup Critical Console Data onto a USB flash memory drive.
10. Customize Scheduled Operations to schedule the backup critical console data task

Checklist for loading a TKE machine - smart card

Expectations:

- You are working with CCA or EP11 host crypto modules.
- The support element has enabled TKE on these host crypto modules.
- LPARs are established (set up and predefined).
- TKE licensed internal code (LIC) is loaded on the TKE workstation.
- Segments 1, 2, and 3 have been loaded on the TKE workstation crypto adapter.
- The TKE host transaction program has been configured and started in the host TKE LPAR.
- ICSF is started in each LPAR.
- Smart card readers are attached.

Setup

- 2 TKEs both running the same level of software
    - One for production
    - One for backup
- 2 CECs cards being shared
    - One Test LPARs (Domain 0)
    - Three Production LPARs (Domain 1, 2, 3)

  TKE can load the master key in a group of domains as defined by a domain group.
- Host TKE LPAR 1

  When defining the LPAR activation profile, the usage domain will be 1 and the control domain will be 0, 1, 2, 3.

Profiles and roles are used to restrict access to the TKE workstation crypto adapter. There are two roles, listed below, that are needed to use the TKE and CNM applications. Profiles are created by first generating a crypto adapter logon key and then creating a profile using the crypto adapter logon key.

- SCTKEUSR - can run the main TKE application
- SCTKEADM - can run CNM to create and update TKE roles and profiles

Authorities are used to restrict access to the CCA crypto modules on the host machine.

Administrators are used to restrict access to the EP11 crypto modules on the host machine.

One way to control access to the CCA host crypto modules is with a minimum of seven host authorities.

- ISSUER
  - Disable host crypto module
  - Enable host crypto module issue
  - Access control issue
  - Zeroize domain issue
  - Domain control change issue
- COSIGN
  - Access control co-sign
  - Enable host crypto module co-sign
  - Zeroize domain co-sign
  - Domain control change co-sign
- MKFIRST
  - AES, DES, ECC (APKA), or RSA load first master key part
  - Clear new master key register
  - Clear old master key register
- MKMIDDLE
  - AES, DES, ECC (APKA), or RSA combine middle master key parts
- MKLAST
  - AES, DES, ECC (APKA), or RSA combine final master key part
  - Set RSA master key
- FIRSTCLEAR
  - Load first operational key part
  - Clear operational key register
- ADDCOMP
  - Load additional operational key part
  - Complete key

The steps to set up the TKE workstation for smart card use are as follows. Be aware that the Service Management tasks available to you will vary depending on the console user name you used to log on. Refer to "Service Management tasks" on page 350 for more information.

1. Customize Network Settings.
2. Customize Console Date/Time.
3. Initialize the TKE workstation crypto adapter for smart card use:
   a. Predefined TKE roles and profiles are loaded.
   b. The TKE master keys are set and TKE key storages are initialized.
4. Open the SCUP application.
   a. Create a CA smart card.
   b. Backup CA smart cards.

c. Create TKE smart cards.

   Note: In general, smart cards created on a particular TKE release cannot be used on TKE workstations that are at prior release levels. There are exceptions. See “Smart card usage” on page 47.

d. Create EP11 smart cards.

e. Enroll the TKE workstation crypto adapter with the CA card.

5. Open CNM.

   Note: Choose the "Default Logon". The temp default role will be used, and has full access to do everything on the crypto adapter.

   a. Enter known DES/PKA and AES master keys. (Optional)

      - Do this only if you want to have known master keys to use again.

   b. Reencipher DES, PKA, and AES key storage. (Optional)

      - Do this only if you entered your own master keys.

   c. Generate TKE workstation crypto adapter logon keys for each smart card that will be logging on to the TKE or CNM applications.

   d. Create new profile or profiles for the smart cards under the Access Control menu. The roles for these profiles are loaded in the crypto adapter when TKE's Crypto Adapter Initialization task is run.

   e. Create group or groups and add users.

      Note: Group members should already be defined.

   f. Load the default role.

      - When the TKE workstation crypto adapter is initialized the TEMPDEFAULT role is loaded. You need to load the DEFAULT role to secure the TKE workstation.

6. Log on to the main TKE application with the SCTKEUSR profile or another profile with the same authority.

   a. Load the default authority key for key index 0.

   b. Change these options of your security policy via the TKE preferences menu

      - Blind Key Entry
      - Removable media only

   c. Create a Host.

   d. Create domain groups. (Optional)

   e. Open a host or a domain group (requires host logon).

   f. Open a crypto module notebook or domain group notebook.

   g. For CCA host crypto modules:

      i) Create roles.

      ii) Generate authority keys and save them to TKE smart cards.

      Note: You can generate and save 1024-bit and 2048-bit RSA keys and BP-320 ECC keys on TKE smart cards. Authorities with 2048-bit RSA keys are supported starting with the CEX3C. Authorities with BP-320 ECC keys are supported starting with the CEX5C.

      iii) Create different authorities using the different authority keys that were just generated.

      iv) Delete the authority 00 or change the authority key to a key that is not the default key. If you delete authority 00 make sure that you have 2 other known authority keys that have the Domain control change issue and cosign.

   h. For EP11 host crypto modules:

      i) Generate administrator keys and save them to EP11 smart cards.

ii) Zeroize the host crypto module or the set of domains you want to administer. Zeroizing a host crypto module or domain puts it in "imprint mode", where administrators can be added without using signed commands.

iii) Add crypto module and domain administrators.

iv) Set the signature threshold and revocation signature threshold on each crypto module and domain. This ends imprint mode.

7. Configure 3270 Emulators.
8. Backup Critical Console Data.
9. Customize Scheduled Operations to schedule the backup critical console data task.
10. If using the same set of smart cards on another TKE, you need to use the Remote Enroll feature for TKE.

Appendix G. TKE hardware support and migration information

This information includes the following topics:

- "TKE release and feature codes available by CEC levels" on page 383
- "Smart card readers and smart cards orderable by TKE release" on page 383
- "TKE (LIC) upgrade paths" on page 385
- "Host cryptographic modules managed by TKE" on page 386

TKE release and feature codes available by CEC levels

Table 39 on page 383 shows the TKE licensed internal code (LIC) that is orderable based on the date and type of your CEC.

Most of the time, a new version of the TKE workstation is released at the same time as a new CEC. When you order a new TKE workstation, you receive the latest TKE hardware with the latest TKE licensed internal code (LIC) installed on it. For example, if you had placed an order for a new TKE workstation between September of 2012 and September of 2013, you would have received TKE 7.2 (or, in order words, hardware feature code 0841 with LIC feature code 0850).

Table 39. TKE release and feature codes available by CEC level

TKE release (LIC)	Feature codes			CEC information												
	Hardware	LIC	Initial release date	z9-109 z9EC 2094	z9BC 2096	z10 EC 2097	z10 BC 2098	z10 EC GA3 z10 BC GA2	z196	z114	zEC12	zBC12	z13	z13s	z14	z15
TKE 5.3	0839	0854	Oct 2008	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
TKE 6.0	0840	0858	Nov 2009	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
TKE 7.0	0841	0860	Sept 2010	N/A	N/A	Yes	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A
TKE 7.1	0841	0867	Sept 2011	N/A	N/A	Yes	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A
TKE 7.2	0841	0850	Sept 2012	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A
TKE 7.3	0842	0872	Sept 2013	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
TKE 8.0	0847	0877	Feb 2015	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes	Yes	Yes
TKE 8.1	0847 or 0097	0878	Feb 2016	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes	Yes	Yes
TKE 9.0	0085 or 0086	0879	Sept 2017	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes	Yes
TKE 9.1	0085 or 0086	0880	Nov 2018	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes
TKE 9.2	0085 or 0086	0881	Sept 2019	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes

Your host cryptographic environment determines the level of TKE LIC that you can use. To determine which host cryptographic modules are supported by your TKE, see Table 42 on page 386.

Smart card readers and smart cards orderable by TKE release

Table 40 on page 384 shows the smart card readers and smart cards that can be ordered for each TKE release.

© Copyright IBM Corp. 2000, 2021

Table 40. Smart card readers and smart cards orderable by TKE release				
TKE release (LIC)	**Smart card reader**		**Smart card**	
	Feature code	**Type**	**Feature code**	**Part number**
TKE 5.3	0885	Omnikey/HID	0884	45D3398
TKE 6.0	0885	Omnikey/HID	0884	45D3398
				74Y0551* #
TKE 7.0	0885	Omnikey/HID	0884	45D3398
				74Y0551* #
TKE 7.1	0885	Omnikey/HID	0884	45D3398
				74Y0551*
TKE 7.2	0885	Omnikey/HID	0884	74Y0551*
TKE 7.3	0885	Omnikey/HID	0884	74Y0551*
TKE 8.0	0885 or 0891	Omnikey/HID	0884 or 0892	00JA710
TKE 8.1	0885 or 0891 @	Omnikey/HID/ Gemalto	0884 or 0892	00JA710
TKE 9.0	0885 or 0891 @	Omnikey/HID/ Gemalto/IDENTIV	0892	00JA710
TKE 9.1	0891	IDENTIV	0900	00RY790
TKE 9.2	0891	IDENTIV	0900	00RY790

*****
Part number 74Y0551 replaced part number 45D3398 in feature code 0884.

#
An MCL is required to support part number 74Y0551 on TKE 6.0 and TKE 7.0.

@

- Clients in the United States, Canada, and European Union (EU) might receive Gemalto CT700 readers.
- With Gemalto smart card readers, you must press the green Enter button after you enter the PIN or a character during the secure key entry process.

There are restrictions on what smart card part numbers can be used to create different smart card types. For more information, see “Smart card compatibility issues” on page 44.

DATAKEY smart cards are not supported on TKE 7.0 or later. If you are upgrading from TKE 6.0 to TKE 7.0 or later and have DATAKEY smart cards, you need to back up your CA smart cards by using a more current smart card part number and copy keys and key parts from your TKE smart cards onto TKE smart cards that are created from a more current smart card part number. See “Datakey card usage” on page 48 for information on migrating data to a new smart card.

To identify the part number of your smart card, look for the following:

DATAKEY
Has blue and orange art work and DATAKEY printed on them.

45D3398
Are white and do not have any part number printed on them.

74Y0551
Has part number 74Y0551 printed on them.

00JA710
Has part number 00JA710 printed on them.

TKE (LIC) upgrade paths

Table 41 on page 385 shows which TKE licensed internal code (LIC) can be upgraded to a new LIC level.

Table 41. Summary of when a TKE workstation can be upgraded

Starting point			Upgradable to TKE LIC level									
TKE release (LIC)	**Hard-ware feature code**	**TKE crypto adapte r type**	**TKE 6.0 (FC 0858)**	**TKE 7.0 (FC 0860)**	**TKE 7.1 (FC 0867)**	**TKE 7.2 (FC 0850)**	**TKE 7.3 (FC 0872)**	**TKE 8.0 (FC 0877)**	**TKE 8.1 (FC 0878)**	**TKE 9.0 (FC 0879)**	**TKE 9.1 (FC 0880)**	**TKE 9.2 (FC 0881)**
TKE 5.3	0839	4764	Yes	No	No	No	No	No	No	No	No	No
TKE 6.0	0839	4764	**Base***	No	No	No	No	No	No	No	No	No
	0840											
TKE 7.0	0841	4765	N/A	**Base***	Yes	Yes	Yes	No	No	No	No	No
TKE 7.1	0841	4765	N/A	N/A	**Base***	Yes	Yes	No	No	No	No	No
TKE 7.2	0841	4765	N/A	N/A	N/A	**Base***	Yes	No	No	No	No	No
TKE 7.3	0841	4765	N/A	N/A	N/A	N/A	**Base***	No	No	No	No	No
	0842	4765	N/A	N/A	N/A	N/A	**Base***	Yes	Yes	Yes	Yes	Yes
TKE 8.0	0847	4767	N/A	N/A	N/A	N/A	N/A	**Base***	Yes	Yes	Yes	Yes
TKE 8.1	0847	4767	N/A	N/A	N/A	N/A	N/A	N/A	**Base***	Yes	Yes	Yes
	0097											
TKE 9.0	0085	4768	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**Base***	Yes	Yes
	0086											
TKE 9.1	0085	4768	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**Base***	Yes
	0086											
TKE 9.2	0085	4768	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**Base***
	0086											

Base*
The initial TKE LIC level installed on the TKE workstation before it was shipped.

Note: In general, you cannot upgrade the LIC level of your TKE workstation if the new LIC level requires a new TKE crypto adapter type. An exception is that upgrades from TKE 7.3 with hardware feature code 0842 to TKE 8.0 or TKE 8.1 are permitted, but the TKE crypto adapter must be replaced.

Notes about upgrading to TKE 9.0

- When TKE workstation feature 0842 or 0847 is upgraded to TKE 9.0, it becomes workstation feature 0849.
- When TKE workstation feature 0097 is upgraded to TKE 9.0, it becomes workstation feature 0080.
- When TKE workstation feature 0098 is upgraded to TKE 9.0, it becomes workstation feature 0081,

The upgrade to TKE 9.0 does not include the new secure workstation features of TKE. You must purchase a new TKE 9.0 workstation to obtain the new capability.

When you upgrade the LIC level of your TKE workstation, you can keep your user data. See Chapter 3, “TKE upgrade and migration actions,” on page 55 for more information.

Host cryptographic modules managed by TKE

TKE manages host cryptographic modules on any CEC where that particular host cryptographic module is supported. In other words, for example, TKE is unaware whether a CEX3C module is running on an IBM System z10, IBM zEnterprise 196, IBM zEnterprise 114, IBM zEnterprise EC12, IBM zEnterprise BC12, IBM z13, IBM z13s, IBM z14, or IBM z15.

Table 42 on page 386 identifies the host cryptographic modules that each TKE release can manage.

Table 42. Host cryptographic modules managed by TKE LIC

TKE release (LIC)	Host cryptographic modules supported by TKE release							
	CEX2C	CEX3C	CEX4C	CEX4P	CEX5C	CEX5P	CEX6C	CEX6P
TKE 5.2	Yes	No	No	No	No	No	No	No
TKE 5.3	Yes	Yes	No	No	No	No	No	No
TKE 6.0	Yes	Yes	Sometimes*	No	No	No	No	No
TKE 7.0	Yes	Yes	Sometimes*	No	No	No	No	No
TKE 7.1	Yes	Yes	Sometimes*	No	No	No	No	No
TKE 7.2	Yes	Yes	Yes	Yes#	No	No	No	No
TKE 7.3	Yes	Yes	Yes	Yes#	No	No	No	No
TKE 8.0	Yes	Yes	Yes	Yes#	Yes@,+	Yes#, $	No	No
TKE 8.1	Yes	Yes	Yes	Yes#	Yes@,+	Yes#, $	No	No
TKE 9.0	Yes	Yes	Yes	Yes#	Yes@,+	Yes#, $	Yes	Yes#
TKE 9.1	Yes	Yes	Yes	Yes#	Yes@,+	Yes#, $	Yes	Yes#
TKE 9.2	Yes	Yes	Yes	Yes#	Yes@,+	Yes#, $	Yes	Yes#

+

TKE 8.1 with the TKE Tower Code level of 3 or higher is required to manage a CEX5C at level CCA 5.3. The TKE Tower Code is include in TKE LIC Control Level 004 and beyond.

*****

A Crypto Express4 that is running in Common Cryptographic Architecture (CCA) mode as a CEX4C is only supported when running ICSF FMID HCR7790 or lower with the toleration APAR OA39075 that allows the CEX4C to report in as a CEX3C. In this case, ICSF sees the module as a CEX3C and manages it as a CEX3C.

#

Modules running in EP11 mode require smart cards to hold administrator certificates and master key material. Smart card readers must be attached to the TKE workstation to administer these host crypto module types.

@

You must be using one of the following levels of ICSF:

- ICSF FMID HCR77B0.
- ICSF FMID HCR77A1, HCR77A0, HCR7790, or HCR7780 in toleration mode (APAR OA45547) and also have the new function APAR OA44910.

$

You must be using one of the following levels of ICSF:

- ICSF FMID HCR77B0.
- ICSF FMID HCR77A1 in toleration mode (APAR OA45547) and also have the new function APAR OA44910.

Some host cryptographic configurations (in other words, specific cryptographic features or combinations of the CEC, host cryptographic module, CCA or EP11 level, and ICSF) require minimum levels of TKE to support the environment.

Appendix H. Hardware Security Module (HSM) event log entries that CCA version 6.0.3 supports

Table 43 on page 387 shows all the possible Hardware Security Module (HSM) event log entries that CCA version 6.0.3 supports.

Table 43. Hardware Security Module (HSM) event log entries

Event ID	Description	Notes for the event type
0	Initialize card-scoped role inactive.	
1	Initialize card-scoped role activate.	
2	Initialize domain-scoped role inactive.	
3	Initialize domain-scoped role activate.	
4	Replace card-scoped role inactive.	
5	Replace card-scoped role activate.	
6	Replace domain-scoped role inactive.	
7	Replace domain-scoped role activate.	
8	Initialize card-scoped profile inactive.	
9	Initialize card-scoped profile activate.	
10	Initialize domain-scoped profile inactive.	
11	Initialize domain-scoped profile activate.	
12	Change expiration date card-scoped profile.	
13	Change expiration date domain-scoped profile.	
14	Passphrase change card-scoped profile.	
15	Passphrase change domain-scoped profile.	
16	Reset failed logon count card-scoped profile.	
17	Reset failed logon count domain-scoped profile.	
18	Replace card-scoped profile inactive.	
19	Replace card-scoped profile activate.	
20	Replace domain-scoped profile inactive.	
21	Replace domain-scoped profile activate.	
22	Delete card-scoped role inactive.	
23	Delete card-scoped role activate.	
24	Reserved.	
25	Delete domain-scoped role inactive.	

© Copyright IBM Corp. 2000, 2021

Table 43. Hardware Security Module (HSM) event log entries (continued)		
Event ID	**Description**	**Notes for the event type**
26	Delete domain-scoped role activate.	
27	Delete card-scoped profile inactive.	
28	Delete card-scoped profile activate.	
29	Reserved.	
30	Delete domain-scoped profile inactive.	
31	Delete domain-scoped profile activate.	
32	Failed logon count exceeded.	
33	Logon failed.	
34	Clear range card-scoped audit log inactive.	
35	Clear range card-scoped audit log activate.	
36	Clear range domain-scoped audit log inactive.	
37	Clear range domain-scoped audit log activate.	
38	Clear all card-scoped audit log inactive.	
39	Clear all card-scoped audit log activate.	
40	Clear all domain-scoped audit log inactive.	
41	Clear all domain-scoped audit log activate.	
42	Firmware update.	The log message contains three (32-bit) integer fields. Each field corresponding to the image revision codes of segments 1, 2, and 3.
43	Set AES master key.	
44	Load first AES master key part.	
45	Load middle AES master key part.	
46	Load last AES master key part.	
47	Clear new AES master key register.	
48	Clear old AES master key register.	
49	Set APKA (ECC) master key.	
50	Load first APKA (ECC) master key part.	
51	Load middle APKA (ECC) master key part.	
52	Load last APKA (ECC) master key part.	
53	Clear new APKA (ECC) master key register.	
54	Clear old APKA (ECC) master key register.	
55	Set DES master key.	
56	Load first DES master key part.	
57	Load middle DES master key part.	

Table 43. Hardware Security Module (HSM) event log entries (continued)		
Event ID	**Description**	**Notes for the event type**
58	Load last DES master key part.	
59	Clear new DES master key register.	
60	Clear old DES master key register.	
61	Generate random new DES master key.	
62	Set RSA master key.	
63	Load first RSA master key part.	
64	Load middle RSA master key part.	
65	Load last RSA master key part.	
66	Clear new RSA master key register.	
67	Clear old RSA master key register.	
68	Generate random new RSA master key.	
69	Set DES and AES master keys.	
70	Load first DES and AES master key part.	
71	Load middle DES and AES master key part.	
72	Load last DES and AES master key part.	
73	Clear new DES and AES master key registers.	
74	Clear old DES and AES master key registers.	
75	Generate random new DES and AES master key.	
76	Load Function Control Vector.	
77	Clear Function Control Vector.	
78	Set clock.	
79	Load decimalization table or tables.	
80	Delete decimalization table or tables.	
81	Enter imprint mode inactive.	
82	Enter PCI-compliant mode inactive.	
83	Enter PCI-compliant mode activate.	
84	Remove PCI-compliant mode inactive.	
85	Remove PCI-compliant mode activate.	
86	Enter migration mode inactive.	
87	Enter migration mode activate.	
88	Start secure audit log wrap.	
89	Start secure audit log nowrap.	
90	Stop secure audit log.	

Table 43. Hardware Security Module (HSM) event log entries (continued)		
Event ID	**Description**	**Notes for the event type**
91	Load certificate inactive.	
92	Load certificate activate.	
93	Load first DES operational key part.	
94	Load additional DES operational key part.	
95	Complete DES operational key.	
96	Clear DES operational key part register.	
97	Load first AES operational key part.	
98	Load additional AES operational key part.	
99	Complete AES operational key.	
100	Clear AES operational key part register.	
101	Load first AES operational key part (VAR-AES).	
102	Load additional AES operational key part (VAR-AES).	
103	Complete AES operational key (VAR-AES).	
104	Clear AES operational key part register (VAR-AES).	
105	Load first HMAC operational key part.	
106	Load additional HMAC operational key part.	
107	Complete HMAC operational key.	
108	Clear HMAC operational key part register.	
109	Diffie-Hellman key load, load 4096-bit RSA.	
110	Diffie-Hellman key load, combine 4096-bit RSA.	
111	Diffie-Hellman key load, clear 4096-bit RSA.	
112	Diffie-Hellman key load, load ECC.	
113	Diffie-Hellman key load, combine ECC.	
114	Diffie-Hellman key load, clear ECC.	
115	Start access control tracking.	
116	Stop access control tracking.	
117	Clear access control tracking data.	
118	Collect configuration data, card.	
119	Collect configuration data, domain.	
120	Apply configuration data, card.	This audit record will not be cut if the auditing level is off both before and after the apply operation.

Table 43. Hardware Security Module (HSM) event log entries (continued)		
Event ID	**Description**	**Notes for the event type**
121	Apply configuration data, domain.	This audit record will not be cut if the auditing level is off both before and after the apply operation.
122	Manual create of secure log entry.	
123	Exit migration mode inactive.	
124	Exit migration mode activate.	
125	Exit migration mode, timer expired.	
126	Reserved.	
127	Enter imprint mode activate.	
128	Initialize card-scoped role.	
129	Initialize card-scoped profile.	
130	Replace card-scoped profile.	
131	Delete card-scoped role.	
132	Delete card-scoped profile.	
133	Activate decimalization table or tables.	
134	Load weak PIN value or values.	
135	Delete weak PIN value or values.	
136	Activate weak PIN value or values.	
137	Delete all weak PIN values.	
138	Exit imprint mode.	

Appendix I. Multi-Factor Authentication (MFA) and the TKE

On a system using Multi-Factor Authentication (MFA), you use an alternative authentication mechanism, such as RSA SecureID, to get a one-time use token instead of using a password. The token is used to authenticate your user ID to the z/OS application to which you are running. Since the token is one-time use, any authentication after that would require a new token.

If you use Multi-Factor Authentication (MFA) with the TKE:

- After a TKE OPEN HOST is done, the TKE replays the user ID and password credentials for some commands sent to the HOST.
- You must run some of the commands that require the replay while you configure host crypto modules.
- By default, MFA uses one-time use only credentials and will not allow you to replay the same credential multiple times.

Therefore, you cannot use a one-time use MFA credential to open a host and configure crypto modules on that host.

There are two ways to handle the TKE replay issue for MFA:

1. You can use the IBM Multi-Factor Authentication Out-of-band server to get a token that allows replay and is valid for the time needed to configure crypto modules on that host. You pick a timeout value that makes sense to you (for example, one hour or one day). When the token expires, you have to close the host and reopen it with a new token. For more information, see "Out-of-Band cache token credential (CTC)" on page 393.
2. You can add the TKE RACF Authorization application (CSFTTKE) to the application exclusion list for MFA to exclude the TKE RACF Authorization application from MFA processing so that only the user ID and RACF password are needed. For more information, see "Bypassing MFA" on page 394.

For more information about IBM MFA, Out-of-Band, the cache token credential, and exclusion list support, see:

- IBM Multi-Factor Authentication for z/OS Installation and Customization (www.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R3sc278447/$file/azfi100_v1r3.pdf)
- IBM Multi-Factor Authentication for z/OS User's Guide (www.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R3sc278448/$file/azfu100_v1r3.pdf)

Out-of-Band cache token credential (CTC)

A cache token credential (CTC) allows reuse of an MFA token for a limited time. A CTC is generated by providing a token from an application such as RSA SecureID to an IBM MFA Out-of-Band server. The CTC returned by the Out-of-Band server can then be used and reused instead of having to provide a new token for every transaction requiring authentication.

To specify that a CTC is going to be used for a given length of time, create an MFA policy such as the one below:

```
FACTORS = AZFSIDP1
TOKEN TIMEOUT = 00003600
REUSE = YES
```

Where:

TOKEN TIMEOUT
Sets the length of time (in seconds) that an IBM MFA Out-of-Band token is valid once the token is generated. The value can be between 1 - 86400 (the number of seconds in a day). The timeout given

© Copyright IBM Corp. 2000, 2021

in the example above is one hour, which is the recommended value for the TKE. The default token timeout is 300 seconds (five minutes).

REUSE
Determines whether the IBM MFA Out-of-Band token can be reused by an application. Possible values are YES or NO. The default is NO.

Bypassing MFA

By running some RACF commands, you can bypass MFA processing when an open host is done from a TKE. For example:

```
RDEF MFADEF MFABYPASS.APPL.CSFTTKE UACC(NONE)
PE  MFABYPASS.APPL.CSFTTKE  CLASS(MFADEF) ID(TKEMFA) ACC(READ)
SETR RACLIST(MFADEF) REFRESH
```

Notes:

- The RACF RDEF (Define General Resource) command adds the TKE RACF Authorization module (CSFTTKE) to the MFA excluded application list.
- The RACF UACC operand specifies Universal Access Authority. In this example, NONE is specified, which is the default.
- The RACF PE (Permit) command is used to allow the user, TKEMFA, to bypass MFA processing. Specify your own list of users for your installation.
- You can remove a user from the permitted list with the following set of commands (in this example, the user TKEMFA is removed. You would specify your own users to remove):

  ```
  PE  MFABYPASS.APPL.CSFTTKE  CLASS(MFADEF) ID(TKEMFA) DELETE
  SETR RACLIST(MFADEF) REFRESH
  ```

- You can also remove the TKE RACF Authorization application (CSFTTKE) from the excluded application list with the following set of commands (these commands remove all users):

  ```
  RDEL MFADEF MFABYPASS.APPL.CSFTTKE
  SETR RACLIST(MFADEF) REFRESH
  ```

Appendix J. Accessibility

Accessible publications for this product are offered through IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSLTBW/welcome).

If you experience difficulty with the accessibility of any z/OS information, send a detailed message to the Contact the z/OS team web page (www.ibm.com/systems/campaignmail/z/zos/contact_z) or use the following mailing address.

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
United States

Accessibility features

Accessibility features help users who have physical disabilities such as restricted mobility or limited vision use software products successfully. The accessibility features in z/OS can help users do the following tasks:

- Run assistive technology such as screen readers and screen magnifier software.
- Operate specific or equivalent features by using the keyboard.
- Customize display attributes such as color, contrast, and font size.

Consult assistive technologies

Assistive technology products such as screen readers function with the user interfaces found in z/OS. Consult the product information for the specific assistive technology product that is used to access z/OS interfaces.

Keyboard navigation of the user interface

You can access z/OS user interfaces with TSO/E or ISPF. The following information describes how to use TSO/E and ISPF, including the use of keyboard shortcuts and function keys (PF keys). Each guide includes the default settings for the PF keys.

- *z/OS TSO/E Primer*
- *z/OS TSO/E User's Guide*
- *z/OS ISPF User's Guide Vol I*

Dotted decimal syntax diagrams

Syntax diagrams are provided in dotted decimal format for users who access IBM Knowledge Center with a screen reader. In dotted decimal format, each syntax element is written on a separate line. If two or more syntax elements are always present together (or always absent together), they can appear on the same line because they are considered a single compound syntax element.

Each line starts with a dotted decimal number; for example, 3 or 3.1 or 3.1.1. To hear these numbers correctly, make sure that the screen reader is set to read out punctuation. All the syntax elements that have the same dotted decimal number (for example, all the syntax elements that have the number 3.1)

© Copyright IBM Corp. 2000, 2021

are mutually exclusive alternatives. If you hear the lines `3.1 USERID` and `3.1 SYSTEMID`, your syntax can include either `USERID` or `SYSTEMID`, but not both.

The dotted decimal numbering level denotes the level of nesting. For example, if a syntax element with dotted decimal number 3 is followed by a series of syntax elements with dotted decimal number 3.1, all the syntax elements numbered 3.1 are subordinate to the syntax element numbered 3.

Certain words and symbols are used next to the dotted decimal numbers to add information about the syntax elements. Occasionally, these words and symbols might occur at the beginning of the element itself. For ease of identification, if the word or symbol is a part of the syntax element, it is preceded by the backslash (\) character. The `*` symbol is placed next to a dotted decimal number to indicate that the syntax element repeats. For example, syntax element `*FILE` with dotted decimal number 3 is given the format `3 \* FILE`. Format `3* FILE` indicates that syntax element `FILE` repeats. Format `3* \* FILE` indicates that syntax element `* FILE` repeats.

Characters such as commas, which are used to separate a string of syntax elements, are shown in the syntax just before the items they separate. These characters can appear on the same line as each item, or on a separate line with the same dotted decimal number as the relevant items. The line can also show another symbol to provide information about the syntax elements. For example, the lines `5.1*, 5.1 LASTRUN, and 5.1 DELETE` mean that if you use more than one of the `LASTRUN` and `DELETE` syntax elements, the elements must be separated by a comma. If no separator is given, assume that you use a blank to separate each syntax element.

If a syntax element is preceded by the % symbol, it indicates a reference that is defined elsewhere. The string that follows the % symbol is the name of a syntax fragment rather than a literal. For example, the line `2.1 %OP1` means that you must refer to separate syntax fragment `OP1`.

The following symbols are used next to the dotted decimal numbers.

? indicates an optional syntax element
The question mark (?) symbol indicates an optional syntax element. A dotted decimal number followed by the question mark symbol (?) indicates that all the syntax elements with a corresponding dotted decimal number, and any subordinate syntax elements, are optional. If there is only one syntax element with a dotted decimal number, the ? symbol is displayed on the same line as the syntax element, (for example `5? NOTIFY`). If there is more than one syntax element with a dotted decimal number, the ? symbol is displayed on a line by itself, followed by the syntax elements that are optional. For example, if you hear the lines `5 ?, 5 NOTIFY`, and `5 UPDATE`, you know that the syntax elements `NOTIFY` and `UPDATE` are optional. That is, you can choose one or none of them. The ? symbol is equivalent to a bypass line in a railroad diagram.

! indicates a default syntax element
The exclamation mark (!) symbol indicates a default syntax element. A dotted decimal number followed by the `!` symbol and a syntax element indicate that the syntax element is the default option for all syntax elements that share the same dotted decimal number. Only one of the syntax elements that share the dotted decimal number can specify the ! symbol. For example, if you hear the lines `2? FILE, 2.1! (KEEP), and 2.1 (DELETE)`, you know that `(KEEP)` is the default option for the `FILE` keyword. In the example, if you include the `FILE` keyword, but do not specify an option, the default option KEEP is applied. A default option also applies to the next higher dotted decimal number. In this example, if the `FILE` keyword is omitted, the default `FILE(KEEP)` is used. However, if you hear the lines `2? FILE, 2.1, 2.1.1! (KEEP)`, and `2.1.1 (DELETE)`, the default option KEEP applies only to the next higher dotted decimal number, `2.1` (which does not have an associated keyword), and does not apply to `2? FILE`. Nothing is used if the keyword `FILE` is omitted.

*** indicates an optional syntax element that is repeatable**
The asterisk or glyph (*) symbol indicates a syntax element that can be repeated zero or more times. A dotted decimal number followed by the * symbol indicates that this syntax element can be used zero or more times; that is, it is optional and can be repeated. For example, if you hear the line `5.1* data area`, you know that you can include one data area, more than one data area, or no data area. If you hear the lines `3* , 3 HOST, 3 STATE`, you know that you can include `HOST, STATE`, both together, or nothing.

Notes:

1. If a dotted decimal number has an asterisk (*) next to it and there is only one item with that dotted decimal number, you can repeat that same item more than once.
2. If a dotted decimal number has an asterisk next to it and several items have that dotted decimal number, you can use more than one item from the list, but you cannot use the items more than once each. In the previous example, you can write `HOST STATE`, but you cannot write `HOST HOST`.
3. The * symbol is equivalent to a loopback line in a railroad syntax diagram.

+ indicates a syntax element that must be included

The plus (+) symbol indicates a syntax element that must be included at least once. A dotted decimal number followed by the + symbol indicates that the syntax element must be included one or more times. That is, it must be included at least once and can be repeated. For example, if you hear the line `6.1+ data area`, you must include at least one data area. If you hear the lines `2+, 2 HOST,` and `2 STATE`, you know that you must include `HOST, STATE,` or both. Similar to the * symbol, the + symbol can repeat a particular item if it is the only item with that dotted decimal number. The + symbol, like the * symbol, is equivalent to a loopback line in a railroad syntax diagram.

Notices

This information was developed for products and services that are offered in the USA or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

This information could include missing, incorrect, or broken hyperlinks. Hyperlinks are maintained in only the HTML plug-in output for the Knowledge Centers. Use of hyperlinks in other output formats of this information is at your own risk.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Site Counsel
2455 South Road

© Copyright IBM Corp. 2000, 2021

Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or

reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's name, email address, phone number, or other personally identifiable information for purposes of enhanced user usability and single sign-on configuration. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at ibm.com/privacy and IBM's Online Privacy Statement at ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at ibm.com/software/info/product-privacy.

Policy for unsupported hardware

Various z/OS elements, such as DFSMSdfp, JES2, JES3, and MVS™, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those

products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (www.ibm.com/software/support/systemsz/lifecycle)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and Trademark information (www.ibm.com/legal/copytrade.shtml).

Index

Numerics

3270 emulation session 95
3270 emulation session, TLS (SSL) 94

A

access control menu
    CNM 253
access control tracking 189
accessibility
    contact IBM 395
    features 395
add
    DES operational key part 176
adding cryptographic coprocessor 244
AES
    operational keys 178
AES key storage
    deleting an entry 129
alternate zone
    enroll 304
    remove 304
API cryptographic services 189
assistive technologies 395
auditing 227
authorities
    changing 154
    creating 150, 155
    deleting 154
    guided create 155
authorities page 146
authority administration
    generating signature keys 147
authority default signature key 6
authority signature key
    load 122
    unload 124
authority signature keys
    generating 147
auto-accept
    hosts 108
automated recognition
    crypto module 102

B

back up
    CA smart card 301
backup
    host files 104
binary file key part
    copy to smart card 132

C

CA smart card
    back up 301
    change PIN 302
    initialize 299
    personalize 299
callable services
    controls for key wrapping behavior of 189
cancel TKE server 77
CCA CLU utility 324
CCA crypto module notebook 137
CCA host crypto module
    API cryptographic ISPF services 188
    API cryptographic services 189
    clear 180
    disabling 140
    domain keys page 170
    encipher RSA key 185
    generate operational key parts 171, 334
    generate RSA key 183
    generating keys 164
    load 164
    load RSA key to host data set 187
    load RSA key to PKDS 186
    load to key part register - add part 174
    load to key part register - complete 177
    load to key part register - first 173
    load to key storage 181
    operational keys 170
    roles 142
    UDXs 189
CCA key parts
    create 133
change PIN
    CNM 281
change signature index 138
changing entries
    authorities 154
    host 107
changing master keys 243
clear 180
clearing new master key register
    CNM 272
clock
    setting 83
clock-calendar
    read 252
    synchronize 253
closing 108
CLU (Code Load utility) 324
CMID 3
CNM
    access control menu 253
    change PIN 281
    check group profiles 271
    clearing new master key register 272

CNM *(continued)*
crypto node menu 252
description 251
display smart card details 282
errors 288
file menu 252
generate crypto adapter logon key 282
generating master key parts to a smart card 274
initialize 253
key storage menu 279
load user profiles 270
load user roles 270
loading a new master key from key parts 273
loading master key parts from a smart card 276
manage smart card contents 283
master key menu 271
read clock-calendar 252
reenciphering key storage 279
save user profiles 270
save user roles 270
smart card menu 280
starting 251
synchronize clock-calendar 253
TKE crypto adapter group profiles 271
TKEGRPMB role 271
verifying master key parts 277
co-sign page
description 196
Code Load utility (CLU) 324
commands
dual-signature 7, 143
single-signature 7
configuration migration
all data 343, 345
domain-only apply 343, 345
public data 344
configuring
TCP/IP 81
contact
z/OS 395
Coprocessor Management panel, ICSF 246
copy
binary file key part to smart card 132
copy and paste
domains 109
create
CCA key parts 133
creating entries
authorities 150
crypto adapter
remove current zone 310
crypto adapter, TKE workstation
initializing 84
local enrollment 305
remote enrollment 306
roles and profiles 16
view zone 310
crypto module group 122
crypto module ID 3, 102
crypto module notebook, CCA
authorities page 146
change signature index 138
co-sign page 196
compare group 138
crypto module notebook, CCA *(continued)*
description 137
details page 141
domain controls 187
domains page 155
functions 138
general page 139
modes 137
refresh notebook 138
release crypto module 138
roles 142
tabular pages 139
crypto module notebook, EP11
description 209
domain administrators page 221
domain attributes page 221
domain control points page 225
domain general page 220
domain keys page 223
domains page 219
function menu 211
modes 210
module administrators page 215
module attributes page 217
module details page 214
module general tab 212
crypto module, host
authenticating 102
automated recognition 102
index values 196
signature key 7
using 112
crypto module, releasing 345
crypto modules 108
crypto node menu
CNM 252
cryptographic adapters supported 3
cryptographic coprocessor
adding 244

D

datakey smart card 48
decimalization tables, managing 190
default signature key 6, 103
deleting entries
AES key storage 129
authorities 154
DES key storage 127
host 107
PKA key storage 128
DES key storage
deleting an entry 127
disabling crypto module 140
display
crypto module settings 138, 211
smart card information 294
display smart card details
CNM 282
domain access 143
domain audit log page 195
domain authorities page 195
domain certificates page 193
domain controls and domain control points 9

domain controls pages
  description 187
domain group
  changing 116
  checking overlap 119
  comparing 121
  creating 114
  viewing 118
  working with in TKE main window 112
domain groups 108
domain keys page
  clear 169
  encipher RSA key 185
  generate 164
  generate RSA key 183
  load 164
  load RSA key to host data set 187
  load RSA key to PKDS 186
  load to key storage 181
domain modes
  changing 157
domain roles page 194
domain-only apply 343, 345
domains
  copy and paste 109
  domain general page 156
domains general page
  zeroize domain 157
domains keys page 158
domains page 155
dual-signature commands 7, 143
duplicate
  EP11 smart cards 134
  TKE smart cards 134
DVD-RAM 55, 56

E

emulation session, 3270 TLS (SSL) 94
emulator session
  configuring 93
encipher RSA key 185
enrolling an entity
  description 51
entering a key part
  smart card reader 318
EP11
  transport key policy 334
EP11 crypto module notebook 209
EP11 master key parts
  generate 134
EP11 smart card
  description 52
EP11 smart cards
  duplicate 134

F

feedback xxxi
file menu
  CNM 252
files
  backing up 103
flash memory drives
  shipped with TKE 2
  USB 307
  using with TKE 56, 333

G

Gemalto smart card reader
  using 43
general page 139
generate
  EP11 master key parts 134
  key parts 173
generate RSA key 183
generate TKE crypto adapter logon key
  CNM 282
generating
  administrator signature keys 216
  authority signature keys 147
  master key parts 164
  operational key parts 171, 334
generating master key parts to a smart card 274
groups
  crypto module 122
  domain 112
guided create authorities 155
guided create roles 145

H

hardware for trusted key entry 1
hash display, truncated 334
HMAC
  operational keys 178
host
  ACP for managing 92
  changing 107
  creating 106
  deleting 107
  logon 107
host crypto module
  description 3
  RSA key 4
host files
  backing up 104
host transaction program
  installation 74
hosts
  auto-accept 108
  working with 106
hosts, multiple 10

I

imprint mode
  CCA 9
  EP11 210
INITADM role 142
initial authorities 103
initializing
  TKE workstation crypto adapter 84
installation
  recovery 70

integrity 4
intrusion latch 140, 213
ISPF services 188

K

key part
    DES operational 176
key parts
    generate multiple 173
    load 179
key storage menu
    CNM 279
key wrapping behavior of ICSF callable services, controls for 189
key-exchange protocol 9
keyboard
    input from keyboard 166
    navigation 395
    PF keys 395
    shortcut keys 395
keys, master
    changing 243

L

load
    key parts 179
load new
    input from binary file 167
    input from keyboard 166
    input from TKE smart card 165
load RSA key to host data set 187
load RSA key to PKDS 186
load to key part register - add part 174
load to key part register - complete 177
load to key part register - first 173
load to key storage
    AES 182
    DES 181
loading a new master key from key parts
    CNM 273
loading master key parts from a smart card 276
loading to CKDS
    operational keys 170
logon key
    for crypto adapter, generating 282
LPAR considerations 10, 106

M

main window
    function menu 122
    load authority signature key 122
    unload authority signature key 124
    utilities 126
Manage Host List ACP 92
manage smart card contents
    CNM 283
master key
    coordinated change 169, 170, 225
    set 169
    set, immediate 169
master key menu
    CNM 271
master keys
    changing 243
migration
    of configuration data 344
mode
    locked read-only 137
    pending command 137
    read-only 137
    update 137
module policy
    setup 146, 155, 217
multiple hosts 10
multiple workstations 10
multiple zones 50

N

navigation
    keyboard 395
normal mode 9

O

OA signature key 7
operational keys
    clear 180
    generate key part 171
    load key part 173
    load to host CKDS 245
    load to TKE key storage 181, 182
    view 179
outbound authentication 7

P

panels
    ICSF Coprocessor Management 246
    ICSF Operational Key Load 247, 248
    ICSF Primary Menu 246, 249
password protect console 364
PCI-compliant mode 9
PCI-HSM
    improved security 5
    overview 4
    requirements 4, 5
PIN
    changing 281
    disallowing values for 192
PKA key storage
    deleting an entry 128
primary menu panel, ICSF 246, 249
printer support 335

R

recovery installation 70
reenciphering key storage
    CNM 279
refresh notebook 138
release crypto module 138, 345
remote cryptographic adapter

remote cryptographic adapter *(continued)*
enroll 306
remove current zone
crypto adapter 310
roles
changing 144
creating 144, 145
deleting 145
description 142
guided create 145
RSA key
encipher 185
generate 183
host crypto module 4
installing in the PKDS 248
load to host data set 187
load to PKDS 186

S

SCUP
back up the CA smart card 301
change PIN of a CA smart card 302
change PIN of a smart card 304
description 291
display smart card 294
enroll a TKE cryptographic adapter 305
initialize and enroll a smart card 302
initialize and personalize the CA smart card 299
personalize a smart card 303
unblock PIN on a smart card 303
view zone 310
secure key part entry
description 311
entering a key part 318
steps 311
security policy
defining 10
sending to IBM
reader comments xxxi
setup
module policy 146, 155, 217
Setup wizard for the workstation
introduction 78
loading and saving customer roles and profiles 80
overview 79
running 80
shortcut keys 395
signature collection 346
signature threshold 346
single-signature commands 7
smart card
copying key from one to another 285
display information 294
managing contents 283
smart card menu
CNM 280
smart card reader
considerations 44
secure key part entry 318
using 42, 43
smart card support
authentication 49
CA smart card 50
smart card support *(continued)*
considerations 44
description 49
enrolling an entity 51
EP11 smart card 52
managing contents 129
multiple zones 50
preparation and planning 42
requirements 41
setting up 52
terminology 41
TKE smart card 51
using the Gemalto smart card reader 43
using the smart card reader 42, 43
zone creation 49
zone description 50
zone identifier 50
start TKE server 77
support element, description 11

T

TCP/IP
configure 81
setup 73
TKE
host transaction program 74
smart card support 41
TKE enablement 11
TKE policy wizards
starting point 293
TKE smart card
change PIN 304
description 51
initialize and enroll 302
personalize 303
unblock PIN 303
TKE smart card wizard 298
TKE smart cards
duplicate 134
TKE workstation crypto adapter
initializing 84
local enrollment 305
remote enrollment 306
roles and profiles 16
view zone 310
TKE Workstation Logon Profile wizard 271
TKE Workstation Setup wizard
loading and saving customer roles and profiles 80
overview 79
running 80
TKE zone wizard 298
TKEDATA DVD-RAM files 55, 56
TLS (SSL) 3270 emulation session 94
trademarks 402
transport key policy
CCA 124
EP11 334
trusted key entry
activating the host 107
authorities 5
authority default signature key 6
authority signature key 6
concepts 3

trusted key entry *(continued)*
crypto module signature key 7
exiting 125, 126
hardware 1
integrity 4
interaction with ICSF 243
key-exchange protocol 9
LPAR 10
main window 105
operational considerations 10
software 2
system hardware 1
terms 3
workstation logon 97

U

UDXs 189
USB flash memory drives
formatting for Trusted Key Entry data 307
shipped with TKE 2
using with TKE 56, 333
user interface
ISPF 395
TSO/E 395
utilities
copying smart card contents 131
managing AES keys 129
managing DES keys 126
managing PKA keys 127
managing smart card contents 129

V

V2R2 changed information TKE 8.1 xxxviii
V2R2 deleted information TKE 8.1 xxxviii
V2R2 new information TKE 8.1 xxxvii
V2R3 changed information TKE 9.0 xxxvii
V2R3 changed information TKE 9.1 xxxvi
V2R3 deleted information TKE 9.0 xxxvii
V2R3 deleted information TKE 9.1 xxxvi
V2R3 new information TKE 9.0 xxxvi
V2R3 new information TKE 9.1 xxxv
V2R4 deleted information TKE 9.2 xxxv
V2R4 new information TKE 9.2 xxxiii
verifying master key parts
CNM 277
view
role 145

W

wizard
for workstation setup 78
TKE Workstation Logon Profile 271
workstation
logon 97
workstation logon
passphrase 97
Workstation Setup wizard
loading and saving customer roles and profiles 80
overview 79
running 80

Z

zeroize domain 157
zone
concepts 49
creation 49
description 42
zone description 50
zone identifier 50



SC14-7511-09

