



Trusted Key Entry PCIX Workstation User's Guide - SEE RESOURCE LINK FOR THE LATEST COPY OF THIS BOOK



Trusted Key Entry PCIX Workstation User's Guide - SEE RESOURCE LINK FOR THE LATEST COPY OF THIS BOOK

Note!

Before using this information and the product it supports, be sure to read the general information under "Notices" on page 391.

Fourth Edition (February 2008)

This is a major revision of SA23-2211-02.

This edition applies to Version 1 Release 9 of z/OS (5694-A01) and to all subsequent releases and modifications until otherwise indicated in new editions.

IBM® welcomes your comments. A form for readers' comments may be provided at the back of this document, or you may address your comments to the following address:

International Business Machines Corporation
MHVRCFS, Mail Station P181
2455 South Road
Poughkeepsie, NY 12601-5400
United States of America

FAX (United States & Canada): 1+845+432-9405

FAX (Other Countries):

Your International Access Code +1+845+432-9405

IBMLink™ (United States customers only): IBMUSM10(MHVRCFS)

Internet e-mail: mhvrdfs@us.ibm.com

World Wide Web: <http://www.ibm.com/servers/eserver/zseries/zos/webqs.html>

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:

- Title and order number of this document
- Page number or topic related to your comment

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 2000, 2008. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures	ix
Tables	xix
About this information	xxi
Who should read this information	xxi
How to use this information	xxi
Where to find more information	xxiii
Related Publications	xxiii
ICSF Publications	xxiv
Summary of Changes	xxv
Chapter 1. Overview	1
Trusted Key Entry Components	1
Hardware	1
Host System Software	2
TKE Hardware	2
TKE Software	3
Introducing Trusted Key Entry	3
ICSF and the Trusted Key Entry Feature	3
Cryptographic Coprocessor Feature and PCI Cryptographic Coprocessor Feature	3
PCI X Cryptographic Coprocessor and Crypto Express2 Coprocessor Features	4
Crypto Module	4
TKE Concepts and Mechanisms	4
Integrity	5
Authorities	5
Crypto Module Signature Key	6
Multi-Signature Commands	6
Access Control	7
Key-Exchange Protocol	8
Domains Controls	8
TKE Operational Considerations	8
Logically Partitioned (LPAR) Mode Considerations	8
Multiple Hosts	8
Multiple Workstations	9
Defining Your Security Policy	9
TKE Enablement for z990, z890, z9 EC, z9 BC and System z10 EC Systems	9
Welcome Page	10
TKE Navigation	11
Chapter 2. Using Smart Cards with TKE	17
Terminology	17
Preparation and Planning	18
Using the smart card reader	19
Zone Concepts	19
Authentication and Secure Communication	20
Zone creation	20
Multiple zones	21
Enrolling an entity	21
TKE smart cards	22
Steps to set up a smart card installation	22

	Chapter 3. Migration	25
I	Migrating from TKE Version 2.0 to TKE Version 5.2	25
I	Migrating from TKE Version 3.X or 4.X to TKE Version 5.2	27
	Backup TKE Configuration Files	27
	TKE Started Task	28
	Set the Workstation Clock	28
	Copy Customer Unique Data	28
	Passphrase and Smart Card Setup	29
	Passphrase Setup	29
	Smart Card Setup	34
	Enable TKE Access Control Points	41
I	Migrating from TKE Version 5.0 or 5.1 to TKE Version 5.2	42
	TKE Started Task For TKE V 3.0 and higher customers only:	42
	Passphrase and Smart Card Setup	42
	TKE Migration Utility	47
	Chapter 4. TKE Up and Running	49
	Workstation Logon: Passphrase or Smart card	50
	Passphrase and passphrase group logon	50
	Smart card and smart card group logon	52
	Automated Crypto Module Recognition	55
	Authenticating the CMID and CPM	55
	CCF	55
	PCICC/PCIXCC/CEX2C	55
	Initial Authorities	56
	Backing Up Files	57
	Workstation Files	57
	Host Files	58
	Chapter 5. Main Window	59
	Host Logon	60
	Working with Hosts	60
	Creating a Host	60
	Changing Host Entries	61
	Deleting Host Entries	62
	Working with Crypto Modules	62
	Working with Groups	63
	Creating a Group	64
	Changing a Group	65
	Comparing Groups	66
	TKE Functions Supporting Groups	68
	Function	69
	Load Authority Signature Key	69
	Define Transport Key Policy	71
	Exit	72
	Utilities	72
	Manage Workstation DES Keys	72
	Manage Workstation PKA Keys	73
	Manage smart cards	74
	Copy smart cards	75
	TKE Customization	76
	Chapter 6. Crypto Module Notebook	79
	General	79
	Intrusion Latch on the PCICC and PCIXCC/CEX2C	81
	Notebook Functions	82

Notebook Mode	83
Tabular Pages	83
Details	84
Access Control (CCF only)	85
Signature Requirements Container	85
Authority Masks Container.	88
Domain Masks Container	88
Roles (PCICC/PCIXCC/CEX2C)	88
Multi-Signature Commands	89
Single Signature Commands	90
Creating or Changing a Role	90
Deleting a Role.	93
Authorities	93
Generating Authority Signature Keys	95
Create Authority (PCICC/PCIXCC/CEX2C).	98
Change Authority	101
Delete Authority (PCICC and PCIXCC/CEX2C)	102
Domains	102
Domains General Page	103
Domain Keys Page - CCF	105
Domains Keys Page (PCICC and PCIXCC/CEX2C)	121
Domain Keys Page - PCIXCC/CEX2C	131
Domains Controls Page	151
Co-Sign	157
Chapter 7. Managing Keys: TKE and ICSF with CCF	159
Synchronizing Keys.	159
Master Key Parts	160
First-Time Startup	160
Initialize the CKDS	161
Importing Key Parts from the Queue	163
Importing Key Parts Individually	164
Importing Multiple Key Parts	164
Importing the First Master Key Part into the DES New Master Key Register	164
Importing the Intermediate Master Key Part into the DES New Master Key Register	167
Importing the Final Key Part into the DES New Master Key Register.	168
Changing Master Keys	170
Changing the Master Key Using the Master Key Panels	170
Restarting the DES Key Entry Process	174
Re-entering Master Keys After They have been Cleared	176
Setting the Master Key	177
Adding Cryptographic Coprocessors After ICSF Initialization	178
CCF	178
PCICC	179
PKA Master Key Parts.	179
Disabling PKA Services	180
Enabling PKA Services	181
Resetting PKA Master Keys.	182
Reenciphering and Activating the PKDS	182
Loading and Importing Operational Keys	184
Importing Key Parts Individually	185
Importing Multiple Key Parts	185
Importing the First Operational Key Part	185
Importing Intermediate Operational Key Parts	189
Importing the Final Operational Key Part	190

Refreshing the CKDS	192
Installing RSA Keys in the PKDS from a Dataset	193
Chapter 8. Managing Keys: TKE and ICSF with PCIXCC/CEX2C	195
Master Key Parts	195
First-Time Startup	196
Initialize the CKDS	196
Changing Master Keys	198
Changing the Master Key Using the Master Key Panels	199
Re-entering Master Keys After They have been Cleared	202
Setting the Master Key	203
Adding Cryptographic Coprocessors After ICSF Initialization	204
PCIXCC/CEX2C	204
Asymmetric-keys Master Key Parts	204
Disabling PKA Services	205
Enabling PKA Services	206
Resetting Asymmetric-Keys Master Keys	207
Reenciphering and Activating the PKDS	207
Loading Operational Keys to the CKDS	209
Refreshing the CKDS	212
Installing RSA Keys in the PKDS from a Data Set	213
Appendix A. TKE Workstation Setup and Customization	215
Installation	215
Configuring TCP/IP	215
Initializing the TKE cryptographic adapter.	219
Setting the Clock.	219
Initializing TKE for passphrase.	220
Initializing TKE for smart cards	227
Customize the TKE Application	231
Appendix B. TKE TCP/IP and Host Considerations	233
TKE TCP/IP Setup and Customization	233
TKE Host Transaction Program Setup	234
Cancel the TKE server	237
Configure 3270 Emulator Sessions for TKE	238
Appendix C. Cryptographic Node Management Utility (CNM)	241
File Menu	241
Passphrase Logon	242
Smart Card Logon	242
Group Logon	243
Logoff.	247
Crypto Node Menu	247
TKE Crypto Adapter Clock-Calendar	247
Access Control Menu	249
TKE predefined roles	250
Open or edit an existing role	250
Define a User Profile	255
Working with User Profiles	262
Master Key Menu	263
Clearing the new master key register	264
Loading a new master key from clear key parts	265
Generating master key parts to a TKE smart card	267
Loading master key parts from a TKE smart card.	268
Verifying Master Key Parts	270

Key Storage Menu	272
Reenciphering key storage	272
Smart card Menu	273
Change PIN	273
Generate TKE Crypto Adapter logon key	275
Display smart card details	276
Manage Smart Card Contents	277
Copy Smart Card	279
CNM Common Errors	282
 Appendix D. Smart Card Utility Program (SCUP)	285
Initialize and personalize the CA smart card	287
Backup a CA smart card	289
Display smart card information.	291
Initialize and enroll a TKE smart card	293
Personalize a TKE smart card	294
Unblock PIN on a TKE smart card	295
Change PIN of a CA smart card	295
Change PIN of a TKE smart card	296
Enroll a TKE cryptographic adapter	296
View current zone	304
 Appendix E. Secure Key Part Entry	305
Steps for secure key part entry	305
Entering a key part on the smart card reader	308
 Appendix F. Access Control Points and Callable Services	311
TKE Version 4.0 and Higher	311
TKE Version 3.1	312
 Appendix G. LPAR Considerations	319
Setup for CCF Systems	319
Setup for PCIXCC/CEX2C Systems.	320
 Appendix H. Auditing	323
 Appendix I. Clear RSA Key Format	325
 Appendix J. Trusted Key Entry - Workstation Cryptographic Adapter	
Initialization	327
Crypto Node Management Batch Initialization 3.10SC	327
CCA CLU 3.10SC	328
CLU Processing	328
Checking Coprocessor Status	331
Loading Coprocessor Code	331
Validating Coprocessor Code	333
Checking System Status	333
Resetting Coprocessor	333
Removing Coprocessor CCA Code and Zeroizing CCA.	333
Help Menu	334
 Appendix K. Trusted Key Entry - Utilities	335
Edit TKE Files.	335
Migrate Previous TKE Version to TKE 5.2	338
TKE File Management Utility	340
TKE Workstation Code Information	343

Appendix L. Service Management - Applications	345
Analyze Console Internal Code	345
Authorize Internal Code Changes	345
Change Console Internal Code	345
Hardware Messages	345
Rebuild Vital Product Data	347
Transmit Console Service Data	347
Appendix M. Service Management - Configuration	351
Customize Scheduled Operations	351
Appendix N. Service Management - Maintenance	357
Backup Critical Console Data	357
Lock console configuration	358
Offload Virtual RETAIN Data to DVD-RAM	360
Save Upgrade Data	362
Shutdown or Restart	363
Users and Tasks	365
View Console Events	365
View Console Information	366
View Console Service History	368
View Console Tasks Performed	371
View Licenses	371
Appendix O. Media Devices	373
Format Media	373
TKE Media Manager	376
Managing Media	377
Appendix P. Service Mode	379
Change Password Task	380
Password Requirements	381
Appendix Q. TKE Best Practices	383
Checklist for Loading a TKE Machine - Passphrase	383
Checklist for Loading a TKE Machine - Smart Card	385
Appendix R. Accessibility	389
Using assistive technologies	389
Keyboard navigation of the user interface	389
z/OS information	389
Notices	391
Trademarks	393
Index	395

Figures

1. ICSF Library	xxiv
2. Pre-login Welcome Page	10
3. Welcome Panel	11
4. Service Management for the TKE User (Alphabetized)	12
5. Primary TKE applications tasks	12
6. Service Management for the TKE User (Categorized)	14
7. Multiple zones	21
8. Migrate Previous TKE Version to TKE V 5.2.	30
9. Data Migration Progress Panel.	31
10. Crypto Adapter logon window with passphrase profiles	50
11. Enter passphrase for logon	50
12. Crypto Adapter group logon window with passphrase profiles	51
13. Enter passphrase for logon	51
14. Crypto Adapter Group logon window with passphrase profile ready	51
15. Crypto Adapter Logon Window with smart card profiles	52
16. Insert the TKE smart card	53
17. Enter smart card PIN	53
18. Crypto Adapter Group logon window with smart card profiles.	53
19. Insert the TKE smart card	54
20. Crypto Adapter Group logon window with smart card profile ready.	54
21. Authenticate Crypto Module for PCIXCC/CEX2C	56
22. TKE Preferences	59
23. Host Logon Window.	60
24. Create Host.	61
25. Main Window with Crypto Modules - CCF System	62
26. Main Window with Crypto Modules - PCIXCC/CEX2C	63
27. Create Group	65
28. Change Group - Crypto Coprocessor (PCIXCC/CEX2C)	66
29. Compare Group - CCF	67
30. Compare Group - PCIXCC/CEX2X	68
31. Select Signature Key Source	69
32. Specify Authority Index	70
33. Load Signature Key.	70
34. Load signature key from TKE smart card	71
35. Enter PIN for TKE smart card	71
36. Define Transport Policy	71
37. TKE Workstation DES Key Storage Window.	72
38. TKE Workstation PKA Key Storage Window	73
39. TKE smart card contents	74
40. Enter source TKE smart card for copy	75
41. Enter target TKE smart card for copy	75
42. Select keys to copy	76
43. CCF Crypto Module Administration Notebook - General Page	79
44. PCICC Crypto Module Administration Notebook - General Page	80
45. Crypto Coprocessor (PCIXCC/CEX2C) Crypto Module Administration Notebook - General Page	81
46. Window to Release Crypto Module	82
47. CCF Access Control Page	86
48. Change Signature Requirements Window.	87
49. Change Signature Requirements Example	88
50. PCICC Roles Page	89
51. PCICC Roles Page - Create, Change or Delete a Role.	91
52. PCICC Create New Role Page.	91
53. PCIXCC/CEX2C Create New Role Page	92

54. PCICC Authorities Page	94
55. PCIXCC/CEX2C Authorities Page.	95
56. Filled In Generate Signature Key Window.	96
57. Save Signature Key.	96
58. Select target window	97
59. Insert TKE smart card	97
60. Enter PIN	97
61. Generate signature key	97
62. Select source of signature key	98
63. Create New Authority	98
64. Insert TKE smart card	99
65. Enter PIN	99
66. Create new authority	99
67. Load Signature Key from binary file	100
68. Create New Authority with Role Container	100
69. Change Authority (PCICC/PCIXCC/CEX2C)	102
70. CCF Domains Page	103
71. CCF Domains General Page	104
72. CCF Domains Keys Page	106
73. Select Target	109
74. Save key part to TKE smart card	109
75. Enter PIN	109
76. Enter key part description	110
77. Key part saved successfully	110
78. Clear Key Warning Message	110
79. Select CCF key source - keyboard	111
80. Enter Key Value - Blind Key Entry	111
81. Enter Key Value.	112
82. Key Part Information Window	112
83. Select CCF key source - binary file.	113
84. Specify Key File.	113
85. Key Part Information Window	114
86. Select CCF key source - smart card	114
87. Select a key part	114
88. Enter PIN	115
89. Load key	115
90. Install Importer Key Part in Key Storage	116
91. Install IMP-PKA Key Part in Key Storage	117
92. Generate RSA Key.	118
93. Encipher RSA Key	119
94. Load RSA Key to PKDS.	120
95. Load RSA Key to Dataset	121
96. PCICC Domains Keys Page	122
97. PCIXCC/CEX2C Domains Keys Page.	123
98. Select Target	125
99. Save key part to smart card	125
100. Enter key part description	125
101. Save key part	126
102. Save key part success message	126
103. Select PCICC/PCIXCC/CEX2C key source - keyboard	126
104. Enter Key Value - Blind Key Entry	127
105. Enter Key	127
106. Key Part Information Window	127
107. Select PCICC/PCIXCC/CEX2C key source - binary file	128
108. Specify Key File.	128
109. Key Part Information Window	129

110. Select PCICC/PCIXCC/CEX2C key source - smart card	129
111. Select key part from TKE smart card	130
112. Clear Key Validation Message	130
113. Clear Key Successful Message	130
114. Generate Operational Key - Default ICSF Key Type	132
115. Generate Operational Key - USER DEFINED	132
116. Select Target	133
117. Save key part	133
118. Save key again	134
119. Select Source	134
120. Specify key file for binary file source	135
121. Enter key value - keyboard source for ICSF default key type	136
122. Enter key value - keyboard source for USER DEFINED key type.	136
123. Select Source	137
124. Select key part from TKE smart card	137
125. Key part information - first key part.	138
126. Key part register information	138
127. Load Operational Key Part Register - add part, keyboard source for USER DEFINED	138
128. Drop down of control vectors - add part, keyboard source for USER DEFINED	139
129. Key part information - add part	139
130. Key part information - add part with SHA-1 for combined key	139
131. Complete Operational Key Part Register - ICSF default key type.	140
132. Complete Operational Key Part Register - USER DEFINED	140
133. Key part register information - complete	141
134. View Operational Key Part Register - ICSF default key type, one key label selected	141
135. View Operational Key Part Register - ICSF default key type, all key labels selected.	142
136. View Operational Key Part Register - USER DEFINED	142
137. View key part register information - key part bit on in CV	142
138. View key part register information - complete key	143
139. View key register successful message	143
140. Warning! message for clear operational key part register.	143
141. Clear Operational Key Part Register - ICSF default key type, one key label selected	144
142. Clear Operational Key Part Register - ICSF default key type, all key labels selected	144
143. Clear Operational Key Part Register - USER DEFINED, one key label selected	145
144. Clear Key Register successful message	145
145. Install Importer Key Part in Key Storage	146
146. Install IMP-PKA Key Part in Key Storage	146
147. Generate RSA Key	148
148. Encipher RSA Key	149
149. Load RSA Key to PKDS.	150
150. Load RSA Key to Dataset	151
151. CCF Domain Controls Page - Default Setting	152
152. PCICC Domain Controls Page with Expanded ISPF Services	154
153. PCIXCC/CEX2C Domain Controls Page with Expanded ISPF Services	155
154. PCICC Domain Controls Page with Expanded API Cryptographic Services	156
155. PCICC Domain Controls Page with Expanded UDXs	157
156. PCICC Co-Sign Page	158
157. ICSF Selecting the Master Key Option on the Primary Menu Panel	161
158. Selecting the Initialize a CKDS Option on the ICSF Master Key Management Panel	162
159. ICSF Initialize a CKDS Panel	162
160. Selecting the TKE Option on the ICSF Primary Menu Panel	165
161. Selecting the DES Master Key entry on the TKE Processing Selection Panel	165
162. Selecting a Coprocessor for Master Key Entry	166
163. Selecting the Enter Key Part Option on the Enter New Master Key Panel	166
164. Enter First Master Key Part Panel with Key Part Register Status Enabled	167
165. First Panel.	167

166. Selecting the Enter Key Part Option on the Enter New Master Key Panel	168
167. Enter Intermediate Master Key Part	168
168. Middle Panel	168
169. Selecting to Enter a Final Key Part on the Enter New Master Key Panel	169
170. Enter Final Master Key Part	169
171. Final Panel	169
172. Selecting the Master Key Option on the ICSF Primary Menu Panel	171
173. Selecting the Change Master Key Option on the ICSF Master Key Management Panel	171
174. Reencipher CKDS	172
175. Selecting the Change Master Key Option on the ICSF Master Key Management Panel	173
176. Change Master Key Panel	173
177. Selecting the TKE Option on the ICSF Primary Menu Panel	174
178. Selecting the DES Master Key entry on the TKE Processing Selection Panel	174
179. Selecting a Coprocessor for Master Key Entry	175
180. Selecting the Restart Key Entry Process Option on the Enter New Master Key Panel	175
181. Confirm Restart Request Panel	176
182. ICSF Selecting the Master Key Option on the Primary Menu Panel	177
183. Selecting the Set Host Master Key Option on the ICSF Master Key Management Panel	178
184. Selecting the Administrative Control Option on the ICSF Primary Menu Panel	180
185. Disabling the PKA Callable Services	181
186. Selecting the Administrative Control Option on the ICSF Primary Menu Panel	181
187. Enabling and Disabling the PKA Callable Services	182
188. Selecting the Reencipher PKDS Option on the Master Key Management Panel	183
189. Reencipher PKDS	183
190. Selecting the Activate PKDS Option on the Master Key Management Panel.	184
191. Activate PKDS	184
192. Selecting the TKE Option on the ICSF Primary Menu Panel	185
193. Selecting the DES Operational Key entry on the TKE Processing Selection Panel	186
194. Selecting a Coprocessor for Operational Key Entry.	186
195. Operational Key Input Panel - First Key Part	187
196. Selecting a Key Type on the Key Type Selection Panel	188
197. Operational Key Input Panel - Key Part Register Status for First Part	188
198. Operational Key Input Panel	189
199. Operational Key Input Panel - Middle Key Part	190
200. Operational Key Input Panel - Key Part Register Status for Middle Part	190
201. Operational Key Input Panel - Final Key Part	191
202. Operational Key Input Panel - Key Part Register Status for Final Part	192
203. ICSF Initialize a CKDS Panel.	192
204. Selecting the TKE Option on the ICSF Primary Menu Panel	193
205. Selecting PKA Key entry on the TKE Processing Selection Panel	193
206. PKA Direct Key Load	194
207. ICSF Selecting the Master Key Option on the Primary Menu Panel	197
208. Selecting the Initialize a CKDS Option on the ICSF Master Key Management Panel	197
209. ICSF Initialize a CKDS Panel.	198
210. Selecting the Master Key Option on the ICSF Primary Menu Panel	199
211. Selecting the Reencipher CKDS Option on the ICSF Master Key Management Panel	200
212. Reencipher CKDS	200
213. Selecting the Change Master Key Option on the ICSF Master Key Management Panel	201
214. Change Master Key Panel	201
215. ICSF Selecting the Master Key Option on the Primary Menu Panel	203
216. Selecting the Set Host Master Key Option on the ICSF Master Key Management Panel	203
217. Selecting the Administrative Control Option on the ICSF Primary Menu Panel	205
218. Disabling the PKA Callable Services	206
219. Selecting the Administrative Control Option on the ICSF Primary Menu Panel	206
220. Enabling and Disabling the PKA Callable Services	207
221. Selecting the Reencipher PKDS Option on the Master Key Management Panel	208

222. Reencipher PKDS	208
223. Selecting the Activate PKDS Option on the Master Key Management Panel.	209
224. Activate PKDS	209
225. ICSF Primary Menu Panel	210
226. Coprocessor Management Panel	210
227. DES Operational Key Load Panel	211
228. DES Operational Key Load Panel	211
229. DES Operational Key Load Panel - ENC-ZERO and CV values displayed	212
230. ICSF Initialize a CKDS Panel	212
231. Selecting the TKE Option on the ICSF Primary Menu Panel	213
232. Selecting PKA Key entry on the TKE Processing Selection Panel	213
233. PKA Direct Key Load	214
234. Customize Network Settings - Identification Tab	216
235. Customize Network Settings Lan Adapters Tab	216
236. Local Area Network	217
237. Customize Network Settings - Name Services Tab	218
238. Network Diagnostic Information Task	219
239. Customize Console Date and Time Window	220
240. Crypto Adapter Initialization 1 Window	221
241. Crypto Adapter Initialization 2 Window	221
242. Crypto Adapter Initialization 3 Window	222
243. Cryptographic Node Management Utility	223
244. Passphrase logon	223
245. Crypto Adapter Initialization Confirmation Window	227
246. Crypto Adapter Initialization - Smart Card or Passphrase.	228
247. Crypto Adapter Initialization for smart card complete	228
248. Entry Example	233
249. Example of Ping Command	233
250. Example of Reserving a Port	234
251. Format of AUTHCMD.	234
252. Assign a User ID to CSFTTKE in FACILITY Class	235
253. Assign a User ID to CSFTTKE in APPL Class.	235
254. Assign a User ID to a Started Task.	235
255. Sample Startup Procedure	236
256. Start the TKE server	237
257. Cancel the TKE server	237
258. Configure 3270 Emulators	238
259. Add 3270 Emulator Session	239
260. Start or Delete a 3270 Emulator Session	239
261. CNM main window.	241
262. CNM main window - File pull down menu	242
263. Passphrase logon prompt	242
264. TKE smart card prompt	242
265. PIN prompt	243
266. Passphrase group logon - group member list	243
267. Group logon prompt	244
268. Passphrase group logon - enter passphrase prompt	244
269. Passphrase group logon - member is ready for logon	245
270. Passphrase group logon successful	245
271. Smart card group logon window	246
272. Smart card group logon — retry PIN prompt	246
273. Smart card group logon window - member is ready for logon	247
274. Smart card group logon successful.	247
275. CNM main window — Crypto Node Time sub-menu	248
276. Current Coprocessor Clock	248
277. Sync time with host window	249

278. CNM main window — Access Control menu	250
279. Role Management panel - list of roles loaded to the TKE crypto adapter for Smart Card	251
280. Open a disk-stored role - choose a file	252
281. Role Definition panel - role is displayed	253
282. Edit a role - highlight access point to permit	254
283. Edit a role - access point is moved to Permitted Operations column	254
284. Profile management panel — profile list	255
285. Define a new profile — select profile type	256
286. Profile Management panel — Passphrase profile	257
287. Profile Management panel — Passphrase profile fields filled in	258
288. Smart card profile — TKE smart card prompt	259
289. Profile management panel — smart card profile	259
290. Profile Management panel – smart card profile fields filled in	260
291. Profile Management panel — Passphrase Group profile	261
292. Profile Management panel — Smart Card Group profile filled in	262
293. CNM main window — Master Key pull-down menu	264
294. Clear New Master Key Register — confirm clearing	264
295. Clear New Master Key Register — register cleared.	264
296. Load Master Key from Clear Parts	265
297. Load Master Key from Clear Parts — key part randomly generated	266
298. Load Master Key from Clear Parts — key part successfully loaded	266
299. Smart Card Master Key Parts panel	267
300. Smart Card Master Key Parts panel — key part description prompt	267
301. Establishing a secure session between TKE Crypto Adapter and TKE smart card	267
302. Generating key part to TKE smart card	268
303. Smart Card Master Key Parts panel — key part generated to TKE smart card	268
304. Master Key Part Smart Card panel — loading a Crypto Adapter key part from TKE smart card	269
305. Establishing a secure session between Crypto Adapter TKE smart card	269
306. Loading key part from TKE smart card	269
307. Master key part successfully loaded	270
308. Master Key Verify sub-menu	271
309. Master Key Register Verification panel - verification pattern is displayed	271
310. Master Key Register VP compare successful	272
311. CNM main window — Key Storage pull-down menu	272
312. Key Storage Management Panel – key labels list	273
313. CNM main menu — Smart Card pull-down menu	274
314. Change PIN — insert TKE smart card prompt.	274
315. Change PIN — enter current PIN prompt	274
316. Change PIN — enter new PIN prompt	275
317. Generate Crypto Adapter Logon Key — insert TKE smart card	275
318. Generate Crypto Adapter Logon Key — PIN prompt	275
319. Generate Crypto Adapter Logon Key — User ID prompt	276
320. Generate Crypto Adapter Logon Key — key generated	276
321. Display Smart Card Details — insert TKE smart card prompt	276
322. Display Smart Card Details — public information displayed	277
323. Manage Smart Card contents — contents of TKE smart card are displayed	278
324. Manage Smart Card contents — confirm delete prompt	278
325. Manage Smart Card contents.	279
326. Copy Smart Card — insert source TKE smart card	280
327. Copy Smart Card — insert target TKE smart card	280
328. Copy Smart Card — TKE smart card key parts are displayed	280
329. Copy Smart Card — highlight source objects to copy to target	281
330. Copy Smart Card — source TKE smart card PIN prompt	281
331. Copy Smart Card — target TKE smart card PIN prompt	281
332. Establishing a secure session between source and target TKE smart cards	281
333. Objects are copied to the target TKE smart card.	282

334. Copy Smart Card — objects are copied to the target container	282
335. First screen of TKE Smart Card Utility Program (SCUP)	286
336. First step for initialization and personalization of the CA smart card	287
337. Message if card is not empty	287
338. Initialization message for CA smart card	288
339. Enter first PIN for CA smart card	288
340. Enter second PIN twice for CA smart card	288
341. Enter zone description for CA smart card	289
342. Enter card description for CA smart card	289
343. Building a CA smart card	289
344. Begin creation of backup CA smart card	290
345. Initialization of backup CA smart card	290
346. Continue creation of backup CA smart card	290
347. Establish secure connection for backup CA smart card	291
348. Building backup CA smart card	291
349. Display of CA smart card and TKE smart card	292
350. Initialize and enroll TKE smart card	293
351. Initializing TKE smart card	294
352. Building TKE smart card	294
353. Personalizing TKE smart card	294
354. Entering PIN for TKE smart card	295
355. Select first CA PIN.	295
356. View current zone for a TKE cryptographic adapter.	296
357. Select local zone	297
358. Certifying request for local Crypto Adapter enrollment	297
359. Message for successful Crypto Adapter enrollment	297
360. View current zone after Crypto Adapter enrollment	298
361. Crypto Adapter Enrolled	298
362. Save Enrollment Request	299
363. Enrollment Request Stored	299
364. Select remote zone	300
365. Remote zone enrollment instructions	300
366. Open enrollment request file	301
367. Verification of enrollment request	301
368. Save the enrollment certificate	302
369. Continue with remote enrollment	302
370. File Chooser Enroll Certificate	303
371. Remote Enroll Success	303
372. View current zone after Crypto Adapter enrollment	304
373. Choosing secure key part entry from the domains keys panel	305
374. Enter description panel for secure key part entry.	306
375. USER DEFINED operational key for secure key part entry	306
376. Secure key part entry — enter TKE smart card into reader	306
377. Secure key part entry — enter PIN.	307
378. Secure key part entry card identification	307
379. Secure key part entry — enter key part digits	307
380. Secure key part entry — key part information	307
381. Secure key part entry — key part information for operational key.	308
382. Secure key part entry — message for successful execution.	308
383. An Example of TKE Host and TKE Target LPARs	320
384. An Example of TKE Host and TKE Target LPARs without Domain Sharing	321
385. An Example of TKE Host and TKE Target LPARs with Domain Sharing	321
386. Crypto Node Management Batch Initialization 3.10SC Task Window	327
387. Crypto Node Management Batch Initialization 3.10SC Task Output Window.	328
388. CLU Checked Check Boxes	329
389. CLU Error	329

390. CLU View Menu	330
391. Output Log file	330
392. Command History	331
393. Successful Completion of CLU Commands	331
394. CLU File Menu	332
395. CLU Help Menu.	334
396. Edit TKE Files Task Window	335
397. Confirm Creation of a New File Prompt Window	336
398. Editor - File menu items.	336
399. Editor - Edit menu items.	337
400. Editor - Style Menu Items	338
I 401. Migrate to TKE Workstation 5.2 - Backup floppy prompt	339
I 402. Migrate to TKE Workstation 5.2 - Data migration progress window	340
403. TKE File Management Utility Task Window	341
404. TKE File Management - Directory options	342
405. Delete Confirmation Window	342
406. Window for Inputting a Filename	343
407. Completion Window	343
408. TKE Workstation Code Information window.	344
409. Hardware Messages window	346
410. Hardware Messages - Details Window	346
411. Transmit Console Service Data - prompt for DVD	347
412. Transmit Console Service Data Task Window for DVD-RAM	348
413. Transmit Console Service Data - Task Window for Diskette	348
414. Transmit Console Service Data - Successful completion	349
415. Update Problem Number for Virtual RETAIN File.	349
416. Select the Virtual RETAIN Files	350
417. Copying Data to Selected Media	350
418. Customize Scheduled Operations Task Window	351
419. Customize Scheduled Operations - Add a Scheduled Operation window	352
420. Customize Scheduled Operations - Set Date and Time window	353
421. Customize Scheduled Operations - Set Repetition of operation	354
422. Completion Window for Adding Scheduled Operation	354
423. Customize Schedule Operations.	355
424. Details View of Scheduled Operation	355
425. New Time Range window for Scheduled Operation	356
426. Backup Critical Console Data Window	357
427. Backup Console Data Progress window - in progress	357
428. Backup Console Data Progress window - Success	358
429. Service Management for the TKEUSER user (Categorized).	358
430. Prompt for Password	359
431. Error if no Password is Entered	359
432. Error if Password Entered Does not match Confirmation	360
433. Prompt to Unlock Console	360
434. Virtual RETAIN Data Offload Window	361
435. Successful Offload of Data.	361
436. Virtual RETAIN Data Offload Unformatted Media Error	361
437. Virtual RETAIN Data Offload Wrong Label Error	362
438. Save Upgrade Window	362
439. Save Upgrade Success Window.	363
440. Shutdown or Restart Task Window	364
441. Confirmation Window	364
442. Login Details Window	365
443. View Console Events Window	366
444. View Console Information Window	367
445. Internal Code Change Details Window	367

446. View Console Service History window	368
447. Problem Summary	369
448. Problem Analysis	370
449. Display Service	370
450. View Console Tasks Performed window	371
451. View Licenses window	372
452. Format Media Task Window	373
453. Format DVD-Ram Window	374
454. Format Completed Window	375
455. Format a Diskette	375
456. Specifying a Label on Diskette	376
457. Format of Diskette successfully completed	376
458. TKE Media Manager	377
459. Service Management for the Service User (Categorized).	379
460. Service Management for the Service User (Alphabetized)	380
461. Change Password Task	381
462. Change Password - Success	381

Tables

1. Smart card task checklist	23
2. TKE management system task checklist	49
3. Key Types and Actions for CCF Crypto Modules	107
4. Key Types and Actions for PCICC Crypto Modules	123
5. Key Types and Actions for PCIXCC/CEX2C Crypto Modules	124
6. TKEUSER Role	225
7. TKEADM Role	225
8. KEYMAN1 Role	226
9. KEYMAN2 Role	226
10. DEFAULT Role	227
11. SCTKEUSR Role	230
12. SCTKEADM Role	230
13. DEFAULT Role	231
14. Decimal to Hexadecimal Conversion Table	309
15. Callable service access control points.	314
16. Allowable labels when formatting DVD-RAM	374

About this information

This information introduces Version 5.2 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 5.2 of the IBM 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 program products. 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," 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," gives an explanation of the smart card support for the TKE workstation.

Chapter 3, "Migration," provides details on migrating from previous versions of TKE to TKE 5.2.

Chapter 4, "TKE Up and Running," provides preliminary setup and initialization tasks that are necessary for operation.

Chapter 5, "Main Window," explains the beginning window of the TKE program and the functions and utilities accessible from it.

Chapter 6, "Crypto Module Notebook," explains the uses of this information. The status of the master keys and key parts are displayed. This window is where the keys can be generated, loaded, reset and the key queue cleared. The domain controls are set here. The zeroize domain function is accessed from here. RSA handling is described here.

Chapter 7, “Managing Keys: TKE and ICSF with CCF,” explains how ICSF is used when loading and importing keys for CCF and PCICC.

Chapter 8, “Managing Keys: TKE and ICSF with PCIXCC/CEX2C,” explains how ICSF is used when loading and importing keys for IBM *@server* zSeries 990, 890, and PCIXCC/CEX2C.

Appendix A, “TKE Workstation Setup and Customization,” explains how to configure the TKE workstation for TCP/IP and initialize the TKE workstation.

Appendix B, “TKE TCP/IP and Host Considerations,” provides information on using TCP/IP and on the host files needed by TKE.

Appendix C, “Cryptographic Node Management Utility (CNM),” provides information on the CNM utility tasks.

Appendix D, “Smart Card Utility Program (SCUP),” provides information on the SCUP tasks.

Appendix E, “Secure Key Part Entry,” provides information on secure entry of key parts.

Appendix F, “Access Control Points and Callable Services,” provides information on their correlation to each other.

Appendix G, “LPAR Considerations,” discusses logical partitions, the TKE host and TKE targets.

Appendix H, “Auditing,” provides information on auditing.

Appendix I, “Clear RSA Key Format,” provides information on the format of RSA-entered keys.

Appendix J, “Trusted Key Entry - Workstation Cryptographic Adapter Initialization,” provides information on the TKE Workstation Cryptographic Adapter Initialization.

Appendix K, “Trusted Key Entry - Utilities,” provides information on TKE Utilities.

Appendix L, “Service Management - Applications,” provides information on Service Management Applications.

Appendix M, “Service Management - Configuration,” provides information on Service Management Configuration.

Appendix N, “Service Management - Maintenance,” provides information on Service Management Maintenance.

Appendix O, “Media Devices,” provides information on Media Devices.

Appendix P, “Service Mode,” provides information on Service Mode.

Appendix Q, “TKE Best Practices,” provides information on Checklists for Loading a TKE Machine for both Passphrase and Smart Card.

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

Notices, provides information on notices, programming interface information, and trademarks.

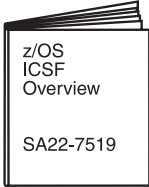
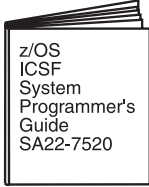
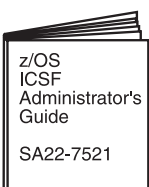
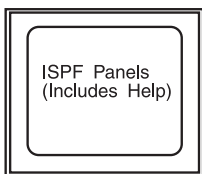
Where to find more information

The information in this book is supported by other books in the ICSF/MVS library and other system libraries. The ICSF library is shown on Figure 1 on page xxiv.

Related Publications

- *z/OS Cryptographic Services ICSF Administrator's Guide*, SA22-7521
- *z/OS Cryptographic Services ICSF System Programmer's Guide*, SA22-7520
- *z/OS Communications Server: IP Configuration Reference*, SC31-8776
- *z/OS Communications Server: New Function Summary*, GC31-8771
- *z/OS Communications Server: IP User's Guide and Commands*, SC31-8780
- *Maintenance Information for Desktop Consoles*, GC28-6847
- *PR/SM Planning Guide*, SB10-7032
- *Support Element Operations Guide*, GC28-6802
- *Communications Server System Management*, SC31-8151
- *Communications Server Network Administration*, SC31-8181

ICSF Publications

Tasks		Tasks	
 z/OS ICSF Overview SA22-7519	Evaluating Planning	 z/OS ICSF Messages SA22-7523	Administrating Application Programming Diagnosis Operating
 z/OS ICSF System Programmer's Guide SA22-7520	Customizing Diagnosis Installing Operating	 z/OS ICSF Administrator's Guide SA22-7521	Administrating
 z/OS ICSF Application Programmer's Guide SA22-7522	Application Programming	 ISPF Panels (Includes Help)	Administrating
 z/OS ICSF Writing PKCS #11 Applications SA23-2231	Application Programming		

Optional Features

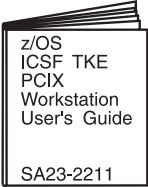
 z/OS ICSF TKE PCIX Workstation User's Guide SA23-2211	Available with the Trusted Key Entry Workstation (TKE Version 5)	 IBM Online Library: z/OS Collection Kit SK3T-4269	The ICSF Library, Trusted Key Entry Workstation User's Guide and Encryption Facility for z/OS Planning and Customizing are included on the IBM Online Library: z/OS Collection Kit SK3T-4269
---	---	---	--

Figure 1. ICSF Library

Summary of Changes

Summary of Changes for SA23-2211-03 z/OS Version 1 Release 9

This book contains information previously presented in *z/OS Cryptographic Services ICSF TKE PCIX Workstation User's Guide*, SA23-2211-01, which supports z/OS Version 1 Release 9.

New information

- Support for System z10 EC
- Support for TCP/IP V 6

Changed Information

- Floppy diskettes are read-only
 - Data can now be saved to DVD-RAMs using the TKE tasks

Deleted Information

- Key token migration for the 4753 is no longer supported

This document has been enabled for the following types of advanced searches in the online z/OS Library Center: commands, examples, tasks, concepts, and references.

You may notice changes in the style and structure of some content in this document—for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents.

This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

Summary of Changes for SA23-2211-02 z/OS Version 1 Release 9

This book contains information previously presented in *z/OS Cryptographic Services ICSF TKE PCIX Workstation User's Guide*, SA23-2211-01, which supports z/OS Version 1 Release 8.

New information

- Support for TKE 5.1 IBM System z9 GA3
 - Service Mode Support
 - Added a service user to improve user's access operations
 - Added this to maintain TKE console consistency:
 - New task layout display
- Appendix Q. TKE Best Practices

Changed Information

- Changed this to maintain TKE console consistency:
 - System Management is now Service Management

Deleted Information

- None.

This document has been enabled for the following types of advanced searches in the online z/OS Library Center: commands, examples, tasks, concepts, and references.

You may notice changes in the style and structure of some content in this document—for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents.

This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

Summary of Changes for SA23-2211-01 z/OS Version 1 Release 8

This book contains information previously presented in *z/OS Cryptographic Services ICSF TKE PCIX Workstation User's Guide*, SA23-2211-00, which supports z/OS Version 1 Release 7.

New information

- FMID HCR7731 WD#6 Support for IBM System z9 GA2
 - Access Control Points for Remote Key Loading:
 - Remote Key Export - CSNDRKX
 - Trusted Block Create - CSNDTBC
- Subtype 22 of SMF Record Type 82 to track the Trusted Block Create Service
- PKA Key Generate - Permit Regeneration Data or Permit Regeneration Data for Retained Keys must be authorized in order to use regeneration data to create a particular RSA private-public key-pair.
- Xlock Configuration Utility
- Rebuild Vital Product Data
- View Console Service History
- New TKE Crypto Adapter/CCA Code

Changed Information

- PTR Enhanced PIN Security for these callable services:
 - Clear PIN Encrypt - CSNBCPE
 - Clear PIN Generate Alternate - CSNBCPA
 - Encrypted PIN Generate - CSNBEPG
 - Encrypted PIN Translate - CSNBPTR
 - Encrypted PIN Translate enhanced further to produce return code 8,3016 - The value of the PAD data is not valid.
 - Encrypted PIN Verify - CSNBPVR

- PIN Change/Unblock - CSNBPCU

Deleted Information

- None.

This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

You may notice changes in the style and structure of some content in this document -- for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents.

Summary of Changes for SA23-2211-00 z/OS Version 1 Release 7

This document is a major revision of *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SA22-7524-07, which supports z/OS Version 1 Release 6.

New information

- New TKE Crypto Adapter/CCA Code
- System Management tasks for maintaining and servicing the TKE workstation
- Patch Process
- Migrate Previous TKE Version to TKE 5.0
- Mixed case support for RACF passwords

Changed Information

- Framework Presentation
- Invocation of TKE related tasks
- Backing up TKE related data
- File Chooser
- No command line support
- Editing TKE files

Deleted Information

- None.

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 ICSF, you can perform functions such as protecting data, verifying messages, generating and verifying signatures, and managing personal identification numbers. Cryptographic systems use a variety of keys that must be securely managed. ICSF uses a hierarchical key management approach and provides a master key to protect all the keys that are active on your system.

Trusted Key Entry (TKE) is an optional feature of ICSF that provides a basic key management system. Your key management system allows authorized persons a method for key identification, exchange, separation, update, backup, and management. It is a tool for security administrators to use in setting up and establishing the security policy and placing it into production.

Trusted Key Entry with smart card support provides an additional level of data confidentiality and security.

Trusted Key Entry Components

The Trusted Key Entry feature is a combination of workstation hardware and software network-connected to S/390, System z9 and zSeries hardware and software.

Hardware

PCI X Cryptographic Coprocessor or Crypto Express2 Coprocessor (PCIXCC/CEX2C)

The PCI X Cryptographic Coprocessor (PCIXCC) replaces the Cryptographic Coprocessor Feature and the PCI Cryptographic Coprocessor. The Crypto Express2 Coprocessor (CEX2C) provides equivalent function as the PCIXCC, but is packaged differently.

The PCIXCC is available on these servers:

- IBM @server zSeries 990 and IBM @server zSeries 890 with feature code 0868. Feature code 3863 for CP Assist for Cryptographic Functions is a prerequisite.

The CEX2C is available on these servers:

- IBM @server zSeries 990, IBM @server zSeries 890, IBM System z9 EC, z9 BC and System z10 EC with feature code 0868. Feature code 3863 for CP Assist for Cryptographic Functions is a prerequisite.

Cryptographic Coprocessor Feature (CCF)

The Cryptographic Coprocessor Feature, is a high-speed extension of the central processor and contains both DES and PKA cryptographic engines. It includes one or two cryptographic coprocessor chips protected by tamper-detection circuitry and a cryptographic battery unit.

It is available on these servers:

1. S/390 Multiprise Server with feature code 0800 plus one of these feature codes (0801, 0802, 0803, 0804, 0805)

2. IBM S/390 Parallel Enterprise Server - Generation 6: with feature code 0800 plus one of these feature codes (0811, 0812, 0813, 0814, 0815, 0832, 0833, 0834, 0835)
3. IBM @server zSeries 800 and IBM @server zSeries 900 feature code 0800 plus one of these feature codes (0874 or 0875)

PCI Cryptographic Coprocessor (PCICC)

The IBM 4758 Model 2 PCI Cryptographic Coprocessor is a programmable PCI card containing a 486-compatible microprocessor, custom hardware to perform DES and public key cryptographic algorithms and a hardware random number generator. It also has protective shields, sensors, and control circuitry to protect against a wide variety of attacks against the system.

It is available on these servers:

- IBM S/390 G6 Enterprise Server with field upgrade and with feature codes 0864 or 0865. Feature code 0860 is needed for each PCI Cryptographic Coprocessor.
- IBM @server zSeries 800 and IBM @server zSeries 900 with feature codes 0861 and 0865.

Host System Software

- For z/OS V1R3 and higher and OS/390 Release 10 without the z990 Cryptographic Support web deliverable, you will need to install APAR OW53666.
- For z990 Cryptographic CP Assist support, you will need FMID HCR7708 or later.
- For z990 PCI X Cryptographic Coprocessor support, you will need FMID HCR770A or later.
- For z990 and z890 Crypto Express2 Coprocessor support, you will need FMID HCR7720 or toleration APAR OA09157 on FMID HCR770A and HCR770B.
- For systems with FMID HCR770A and below, you need to install APAR OA07393.
- To use TKE V 4.1 or higher to load operational keys, you must be running HCR770B or higher.
- For systems with FMID HCR770B and above using TKE V 4.1 and above, you need to install APAR OA15044 if you want to load operational keys.

TKE Hardware

- TKE Workstation
- IBM 4764 Cryptographic adapter

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

Optional TKE Features

Also available with a TKE workstation are:

- Feature 0887: 2 smart card readers and 20 smart cards
- Feature 0888: 10 smart cards

Note: These optional features require at least TKE V 4.2 code - FC 853

TKE Software

This software is preinstalled on the TKE workstation:

- IBM Cryptographic Coprocessor Support Program Release 3.10SC.
- Trusted Key Entry Version 5.2 - FC 0857

Note: TKE software should not be changed without instructions from IBM service.

Introducing Trusted Key Entry

z/OS Version 1 Release 3 and higher and OS/390 Version 2 Release 10 support the Trusted Key Entry (TKE) feature. It is an optional feature and gives users an alternative method of securely loading DES and PKA master keys and operational keys.

The TKE workstation allows you to create a logical, secure channel through which master keys and operational keys can be distributed to remote locations. This logical, secure channel ensures both the integrity and the privacy of the transfer channel. It is well suited to the distributed computing environment that requires remote key management of one or more systems.

For added security, you can require that multiple security officers perform critical operations.

ICSF and the Trusted Key Entry Feature

TKE works in concert with ICSF in managing keys and requires an active TSO session on the TKE workstation or another workstation located nearby. The ICSF ISPF panels are used to load operational and master keys from the key part queue (CCF systems only), load operational keys from key part registers (PCIXCC/CEX2C only), set the master key and to initialize or reencipher the CKDS (cryptographic keys data set). The TSO session is also required to disable and enable PKA services so that the PKA master keys can be reset and changed, the PKDS (PKA keys data set) initialized and reenciphered and the PKDS activated.

Cryptographic Coprocessor Feature and PCI Cryptographic Coprocessor Feature

The Cryptographic Coprocessor Feature (CCF) provides a crypto-storage unit and crypto-computational unit on a single chip. It uses public keys and digital signatures over a public channel. The dual-control function is enhanced by means of a signature requirement array. The Cryptographic Coprocessor Feature is made secure by means of physical packaging and tamper-detection circuitry.

The PCI Cryptographic Coprocessor Feature (PCICC) provides a secure processing environment with hardware to perform DES, random number generation and modular math functions for RSA and similar public-key cryptographic algorithms. The PCI card includes sensors to protect against attacks involving probe penetration, power sequencing, radiation and temperature manipulation.

You must have at least one Cryptographic Coprocessor Feature on your system. You can order a PCICC at the time you order your zSeries (800 or 900) hardware. Multiple PCICCs are allowed on your system.

These features are not supported on the z890, z990, z9 EC, z9 BC and System z10 EC hardware.

PCI X Cryptographic Coprocessor and Crypto Express2 Coprocessor Features

The PCI X Cryptographic Coprocessor (PCIXCC) and Crypto Express2 Coprocessor (CEX2C) provide a secure processing environment with hardware to provide DES, TDES, RSA, and SHA-1 cryptographic services with the IBM Common Cryptographic Architecture (CCA) secure key management and finance-industry special function support. They also perform random number generation and modular math functions for RSA and similar public-key cryptographic algorithms. The PCIXCC/CEX2C includes sensors to protect against attacks involving probe penetration, power sequencing, radiation and temperature manipulation.

To use TKE on z990, z890, z9 EC, z9 BC and System z10 EC systems, you must have at least one PCIXCC/CEX2C on your system. The z990/z890 can support a maximum of 4 PCIXCC features. The z890, z990, z9 EC, z9 BC and System z10 EC can support a maximum of 8 CEX2C features.

Crypto Module

The Cryptographic Coprocessor Feature, the PCI Cryptographic Coprocessor Feature, the PCI X Cryptographic Coprocessor and the Crypto Express2 Coprocessor are the Host system hardware devices performing the cryptographic functions, referred to as the *crypto module*.

During the manufacturing process, several values are generated for the crypto module:

- Crypto-Module ID (CMID)
- For CCF, this is a unique 16-byte hexadecimal number generated for each crypto module. For PCICC and PCIXCC/CEX2C, this is a unique 8-byte character string generated for each crypto module. The CMID is returned in all reply messages sent by the crypto module to the TKE workstation.

- RSA Key

This is a unique 1024-bit RSA key generated for each crypto module. The public modulus part of this RSA key is called the crypto-module public modulus (CMPM).

TKE Concepts and Mechanisms

The TKE program uses these terms on its window displays:

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

Crypto Module

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

Domain

Holds master keys and operational keys. There are sixteen domains (00-15).

Authority

A person or TKE workstation that is able to issue signed commands to the crypto module. All administration of crypto modules is done by authorities.

Role (PCICC and PCIXCC/CEX2C only) Privileges assigned to one or more authorities.

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 crypto module, then integrity of the authorities, and finally, these integrity mechanisms are used as part of the process to establish secrecy.

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

In the same way, the authenticity of the reply from the crypto module to the TKE workstation is digitally signed. The reply is signed by the crypto module using its own secret RSA key and verified by the TKE workstation using the public RSA key of the crypto module.

In order to eliminate the possibility of an attacker successfully replaying a previously signed command or reply, a sequence number is included in all signed messages. Sequence numbers are maintained for each crypto module and for each authority communicating with that crypto module.

Authorities

An authority is a person who is able to issue signed commands to the crypto module.

All administration of CCF, PCICC, PCIXCC and CEX2C crypto modules is done with authorities. An authority is identified to the crypto module by the *authority index*. For CCF, there are 16 authorities for each crypto module with indices 00-15. For PCICC, PCIXCC and CEX2C, there are up to 100 authorities for each crypto module with indices 00-99. In a system with multiple crypto modules, there is no requirement that an authority have the same authority index for each crypto module. However, it is highly recommended that you do.

If your system has multiple crypto modules you will find it convenient to assign authorities the same index on each of your crypto modules. This will give each authority the ability to update all crypto modules on the system after loading their signature key. If an authority has a different index on each crypto module, they will have to change their index as they work with different crypto modules.

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

Authority Signature Key

An authority signs commands by using the secret key of its signature key pair and the crypto module verifies the signature by using the public key of the same RSA key pair.

Previous to signing and verifying command signatures, the signature key pair must be generated, the secret key associated with the authority and the public key sent to the crypto module. All authorities have a public exponent value of 65537.

Authority Default Signature Key

During the crypto module initialization, the public key of a default signature key pair is loaded into the crypto module. The secret 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 crypto module. You are able to reload the public key of a default signature key pair to the crypto module.

For CCF, the same default signature key is assigned to authorities 0-13. Authorities 14 and 15 have their own unique default signature keys.

Attention: Authorities 14 and 15 cannot be used for signing commands until their default signature keys have been changed. Either these authority signature keys must be changed or they should not be defined in the Signature Requirements Array as authorized or required to sign commands.

For PCICC and PCIXCC/CEX2C, the initialization process creates the authority 00 and assigns the authority default signature key to this authority.

Crypto Module Signature Key

The replies from each crypto module are signed by a crypto module signature key. This key is a unique RSA key for each crypto module. The public modulus part of this RSA key is called the crypto module public modulus (CMPM) and can be displayed. The public exponent for all crypto module RSA keys is a fixed value of 65537.

The RSA signature key is loaded into the crypto module during the manufacturing and initialization processes. The public part of the RSA key is sent to the TKE workstation at the very first communication between the crypto module and the workstation.

Multi-Signature Commands

All commands to the crypto module 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 multi-signature commands.

Cryptographic Coprocessor Feature

All the CCF commands are multi-signature commands. The number and identity of required signatures for each command are defined by the installation. Ten different multi-signature commands are implemented, but only six are currently used by TKE:

- Load Authorization Public Modulus (LAP)
- Load PKSC Control Block (LCB)
- Zeroize Domain (ZD)
- Load Environmental Control Mask (LEC)
- Load Key Part (LKP)
- Load and Combine PKA Master Keys (LCS/LCR)

PCI Cryptographic Coprocessor Feature / PCI X Cryptographic Coprocessor Feature / Crypto Express2 Coprocessor Feature

The PCICCC/PCIXCC/CEX2C single signature commands deal with master key management and disabling the crypto module:

- Load / combine new symmetric master key parts
- Clear new symmetric master key register
- Load / combine new asymmetric master key parts
- Clear new asymmetric master key register
- Set new asymmetric master key
- Disable crypto module

The PCICCC/PCIXCC/CEX2C multi-signature commands always require two signatures. These commands deal with:

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

PCI X Cryptographic Coprocessor and Crypto Express2 Coprocessor Feature only

The PCIXCC/CEX2C single signature commands for operational keys:

- Load first key part
- Load additional key part
- Complete key
- Clear operational key register

Access Control

Access control is administered quite differently for CCF and PCICCC/PCIXCC/CEX2C.

CCF

The access control for CCF is administered by defining the security requirements for each of the multi-signature commands. The requirement consists of a mask and a count. The mask indicates which authorities are eligible to be counted for that requirement. The count indicates how many signatures are necessary for that requirement. A pending command is not executed until all requirements for that command have been met. If the count is zero, the requirement is considered satisfied and the signature mask is ignored.

Besides the signature requirement specification, you must also specify the domains that can be changed.

Attention: Authorities 14 and 15 cannot be used for signing commands until their default signature keys have been changed. Either these authority signature keys must be changed or they should not be defined in the Signature Requirements Array as authorized or required to sign commands.

The security requirements are initially defined so that all commands can be executed by the initially created authorities 00–13.

PCICC/PCIXCC/CEX2C

The access control for PCICC/PCIXCC/CEX2C is based on roles. Each authority is assigned a role. The role definition specifies which of the PCICC/PCIXCC/CEX2C signed commands the authority can issue or co-sign and which domains the authority may change.

Initially the INITADM role is defined and the initial authority 00 is assigned to that role. This authority is allowed to create, change and delete authorities and roles.

Key-Exchange Protocol

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

For CCF, the basic transport key protects the DES master key and operational key transfer from the TKE workstation to the crypto module. The PKA transport key protects the PKA master key transfer from the TKE workstation to the crypto module.

For PCICC and PCIXCC/CEX2C, there is a single transport key used for all key transport from the TKE workstation to the crypto module.

Domains Controls

The Domains Controls settings control basic cryptographic capabilities for a selected domain. Your installation should consider the ramifications of various implementations.

TKE Operational Considerations

You can run your processor in single-image mode or physical partition mode. You can have up to two Cryptographic Coprocessor Features and multiple PCI Cryptographic Coprocessor Features on a CCF system.

On a z990, z890, z9 EC, z9 BC and System z10 EC, you must have at least one PCIXCC/CEX2C for TKE usage.

Logically Partitioned (LPAR) Mode Considerations

When you activate a logical partition, you can prepare it for running software products that work with the Cryptographic Coprocessor Feature (CCF), the PCI Cryptographic Coprocessor Feature (PCICC) or PCI X Cryptographic Coprocessor (PCIXCC)/Crypto Express2 Coprocessor (CEX2C). Both the CCF and the PCICC can be shared among several PR/SM logical partitions. The PCIXCC/CEX2C can be shared among several 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 and PKDS.

When you activate a logical partition, you prepare it for being a TKE host or a TKE target. For details, refer to Appendix G, “LPAR Considerations,” on page 319.

Multiple Hosts

One TKE workstation can be connected to several hosts.

Multiple Workstations

Several users on different workstations can have sessions with one host simultaneously. Whenever a user attempts to work with a crypto module, the system checks if another user is working with that module. The first user has a reserve on the crypto module. All other users open the crypto module in read-only mode until the first user releases the crypto module by closing 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 1 and 2? 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?

As an example, if you are using CCF, the Signature Requirements Array (SRA) could be set up to permit any two out of three security officers to issue Load Environment-Control Mask from any workstation. The SRA entry for Load PKSC Control Block, on the other hand, might be set up to require a different set of security officers and require signatures from both security officers and workstations.

TKE Enablement for z990, z890, z9 EC, z9 BC and System z10 EC Systems

If you have a z890, z990, z9 EC, z9 BC and System z10 EC system with May 2004 or later version of Licensed Internal Code (LIC) installed, TKE commands must be permitted on the Support Element before any commands issued by the TKE workstation can be executed. This is a requirement beginning with the May 2004 Licensed Internal Code. Default setting for TKE commands is **Denied**.

To permit TKE commands on the Support Element, you must perform these tasks:

1. On the PCI Cryptographic Configuration panel, highlight a PCI Cryptographic number (all PCIXCCs/CEX2Cs available on the server will be displayed) and then click on the TKE Commands button.
2. On the TKE Command Configuration panel, permit TKE commands by clicking the Permit TKE Commands check box and then press OK.

3. Repeat steps 1 and 2 for each PCIXCC/CEX2C card.

If TKE commands are not permitted on the Support Element, this Details Error will be 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.'

Note: A global zeroize issued from the Support Element will return the state of TKE Commands back to the default value of **Denied**. All PCIXCCs/CEX2Cs must have the state of the TKE Commands set to the value of **Permitted** before TKE workstation commands can be issued from the TKE workstation.

Welcome Page

The Trusted Key Entry Console automatically loads on boot up with a set of commonly used tasks. Optionally the TKE Console may be opened in Service mode. To open the TKE Console in one of these modes, close your current TKE console, and on the Welcome page select "Service and Product Engineering Access". You will be prompted for a username and password.

- For service mode, the user name is SERVICE and the default password is SERVMODE. Once logged in, it is recommended that you change this password with the Change Password task listed under the Service Management

In TKE 5.0, there were two users, including the auto-logged on user and product engineering user. The auto-logged on user selected "Launch the Trusted Key Entry Console web application" from the Pre-login menu, and the TKE user interface was brought up immediately, allowing unchallenged access to the console. When a product engineer selected "Product Engineering Access", a prompt to login with PE credentials was presented.

In TKE 5.1 and above, this link will also provide an opportunity for the "service" user to login. The new link name "Service and Product Engineering Access" reflects this change.

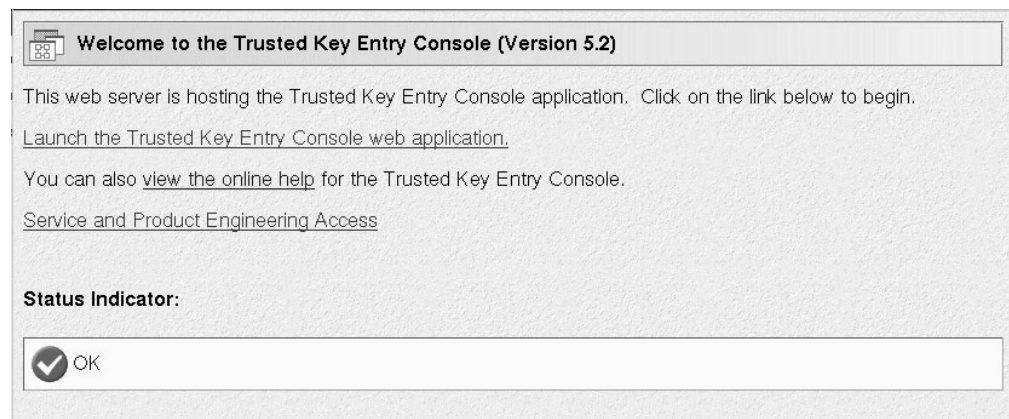


Figure 2. Pre-login Welcome Page

TKE Navigation

On startup the TKE Console will be started automatically with the Welcome panel.

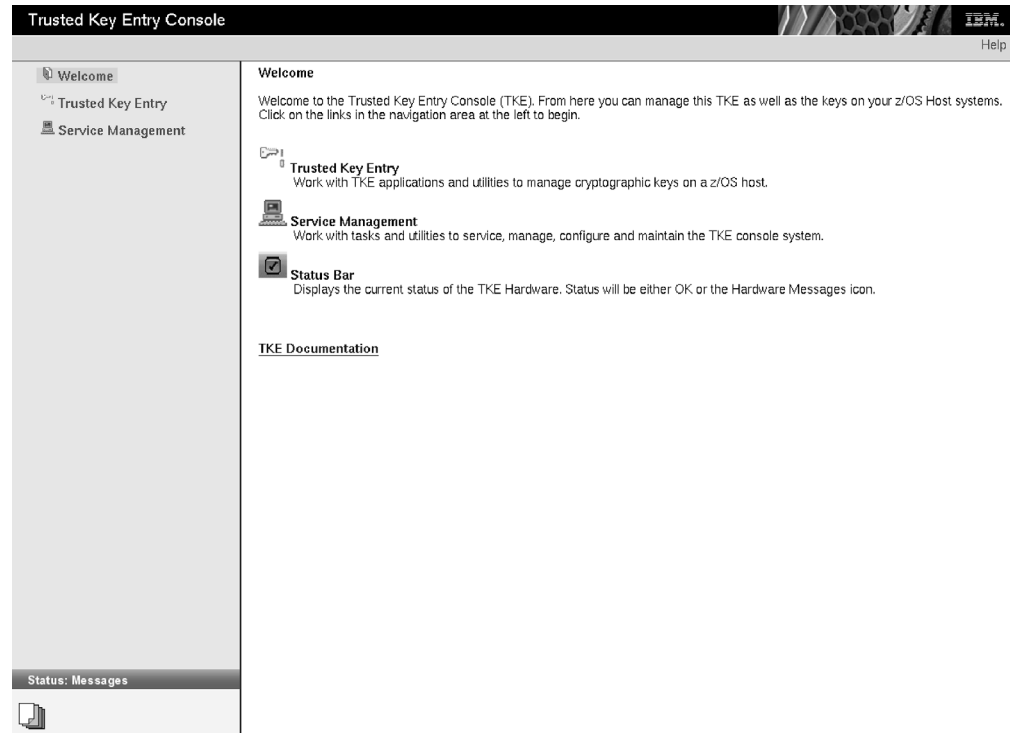


Figure 3. Welcome Panel

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 PCIX 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.

Each Category can be displayed in 2 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.

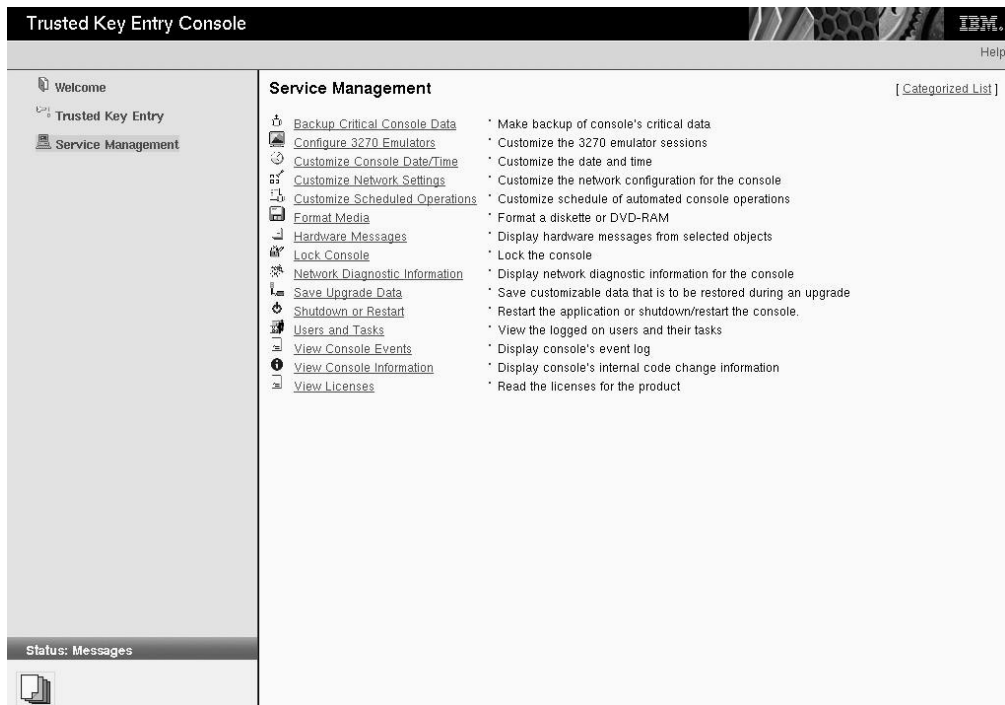


Figure 4. Service Management for the TKE User (Alphabetized)

The Applications category contains the primary TKE applications.

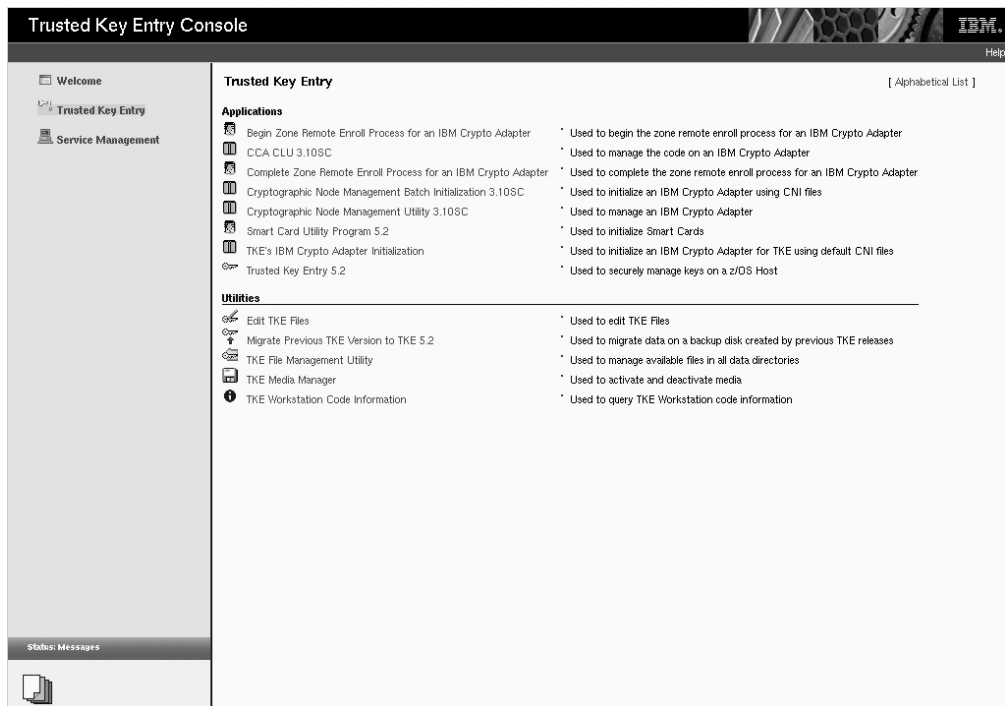


Figure 5. Primary TKE applications tasks

Applications include:

- **Begin Zone Remote Enroll Process for an IBM Crypto Adapter** - For use on the Remote TKE to begin the zone enrollment process.

- CCA CLU 3.10SC - For loading code onto the TKE V 5.2 Workstation Crypto Adapter.
- Complete Zone Remote Enroll Process for an IBM Crypto Adapter - For use on the Remote TKE to complete enrollment in a zone.
- Cryptographic Node Management Batch Initialization 3.10SC - For using a Batch interface to execute a user created CNI file. A user created CNI file can be used to initialize a TKE crypto adapter differently than the TKE's IBM Crypto Adapter Initialization task. To create the user CNI, use the Cryptographic Node Management Utility 3.10SC, CNI Editor function
- Cryptographic Node Management Utility 3.10SC - For managing the TKE workstation crypto adapter (create and manage Roles and Profiles, manage workstation master keys, etc)
- Smart Card Utility Program V 5.2 - For creating, initializing, and enrolling Smartcards and enrolling the TKE workstations.
- TKE's IBM Crypto Adapter Initialization - For initializing the TKE Workstation Crypto Adapter for Passphrase or Smartcard use.
- Trusted Key Entry V 5.2 - For managing Host cryptographic hardware use the main TKE application

The Utilities category task contains common utilities in support of TKE.

Utilities include:

- Edit TKE Files - A general purpose editor for viewing files using the floppy drive and creating/updating file using the CD/DVD drive and in TKE related directories on the hard drive
- Migrate Previous TKE Version to TKE V 5.2 - A utility for migrating TKE related information from an existing TKE workstation to a new TKE V 5.2 workstation
- TKE File Management Utility - Used to manage (copy, delete, and rename) files on Floppy Drive, CD/DVD Drive, and in TKE related data directories on the hard drive
- TKE Media Manager - For activating and deactivating media drives for use by TKE Applications and Utilities
- TKE Workstation Code Information - Provides build/change dates for the current TKE workstation code. This does not include any information for the code loaded on the Crypto Adapter

The Service Management category contains tasks and utilities to service, manage, configure and maintain the TKE console system. More Service Management tasks can be accessed under Service mode. For more information see Appendix P, "Service Mode," on page 379.

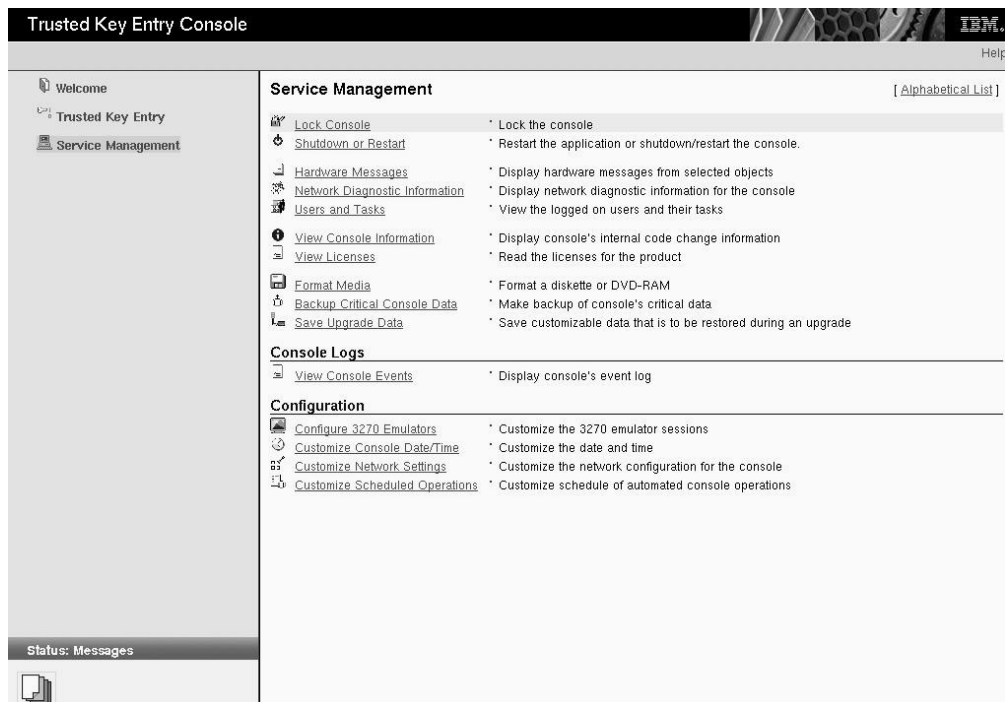


Figure 6. Service Management for the TKE User (Categorized)

The Service Management (Categorized view) workarea tasks include:

- Lock Console - Lock the TKE console
- Shutdown or Restart - Restart application, restart console, or power-off/shutdown console
- Hardware Messages - Display hardware messages
- Network Diagnostics Information - Diagnostic tools to aide in debugging connection problems
- Users and Tasks - View user details and active tasks
- View Console Information - Display consoles internal code change information
- View Licenses - View license information for applicable workstation code
- Format Media - Format diskettes or DVDs. This task cannot be run on a media type unless the TKE Media Manager task shows that the media's status is deactivated.
- Backup Critical Console Data - Backup changed TKE and system related (MCLs) data to DVD after the initial install of code. It is intended for use during a hard disk restore operation which completely replaces the contents of the hard drive using the original install CD and the Backup DVD.
- Save Upgrade Data - Saves customizable data that is to be restored during an upgrade.

The Console Logs category contains this task:

- View Console Events - Display console events log

The Configuration category contains these tasks:

- Configure 3270 Emulators - Used to configure 3270 emulator sessions
- Customize Console Date/Time - Used to set the TKE workstation Date and Time
- Customize Network Settings - Used to set up the TCPIP configuration

I

- Customize Scheduled Operations - Provides the ability to schedule automatic backups of critical console data, including MCLs applied and changes to TKE related information

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, signature keys, and TKE Crypto Adapter logon keys from ever appearing in the clear.

Smart Card support requires:

- TKE V4.2 or higher code
- TKE Smart Card Reader, feature code 0887. This feature includes 2 smart card readers and 20 smart cards.
- TKE workstation with an IBM Cryptographic Adapter Card.

Note: The 4764 card is certified at FIPS 140-2 Level 4 for the hardware, segment 0 and segment 1. The segments 2 and 3 are not certified. For TKE 5.2, card code level 3.10SC is required for segments 2 and 3.

Optional feature code 0888 includes 10 additional smart cards.

The TKE V5.2 workstation with smart card support:

- Stores ICSF (host) key parts, specifically, master and operational key parts on TKE smart cards
- Stores TKE crypto adapter workstation master key parts on TKE smart cards.
- Generates, stores, and uses a TKE authority signature key on TKE smart cards
- Generates, stores, and uses a TKE crypto adapter logon key on TKE smart cards.

Terminology

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

CNM

Cryptographic Node Management utility. This utility is a Java application that provides a graphical user interface to initialize and manage the TKE cryptographic adapter. See Appendix C, "Cryptographic Node Management Utility (CNM)," on page 241.

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 cryptographic adapter.

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 smart card readers must be attached at all times to each TKE workstation to use smart card functions.
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 and TKE smart cards and zone enrollment of the TKE crypto adapter. See Appendix D, “Smart Card Utility Program (SCUP),” on page 285.
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 20.
Entity	A member of a zone. Entities can be a CA smart card, a TKE smart card, or a cryptographic adapter.
Group Logon	Allows multiple users to co-sign the logon to the TKE cryptographic adapter. A group may have a minimum of one member and a maximum of ten members.
Certificate Authority (CA) Smart Card	An entity that establishes a zone using the Smart Card Utility Program (SCUP). Protected by two 6-digit PINs.
TKE Smart Card	Used for the storing keys and key parts; Can hold a maximum of 10 key parts, a TKE Crypto Adapter logon key and a TKE authority key. Protected by a 4-digit PIN.

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 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 smart card reader

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

Each smart card reader has two lights above the PIN pad, one green, one yellow. When opening a smart card application (SCUP, CNM or TKE), wait for the green light to come on for both smart card readers before selecting a smart card function. The green light should always be on when the readers are attached.

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 is usually white on one side and colored on the other. Half of the colored side is solid blue with a gold plated contact. Insert the gold plated contact facing you and pointing down into the smart card reader.

When prompted to insert a TKE smart card, push the smart card all the way in until the yellow light comes on. If the yellow light does not come on, remove the smart card and insert it again.

When prompted for a PIN, Enter PIN will appear on the smart card reader display window and the PIN pad cursor will flash. 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.

Other active buttons on the PIN pad are: The X button will cancel the PIN prompt; Abort will appear on the smart card reader window and the application PIN prompt will close. 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.

Zone Concepts

Smart card support provides the ability to generate and enter a cryptographic key part and then transfer the generated key parts to different smart cards. Smart card support for TKE is designed around the concept of a zone. This is done to ensure the secure transfers of key parts.

These are members of a zone:

- CA smart card
- TKE cryptographic adapter cards
- TKE smart cards

A member of a zone will be referred to as an entity. Entities have to 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) do not check the zone ID of the TKE smart card against the zone ID of the TKE cryptographic adapter. In other words, a TKE smart card from a different zone may be used to logon to the TKE cryptographic adapter in another zone, but the key parts on the TKE smart card will not be accepted in this zone (because the TKE smart card is enrolled in another zone).

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 sent with the message and protected by encryption with a public key 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 cryptographic 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).

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 cryptographic 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 or destroyed.

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 or a TKE cryptographic 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 have multiple 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.

Note that entities can only be a member of one zone at any given time.

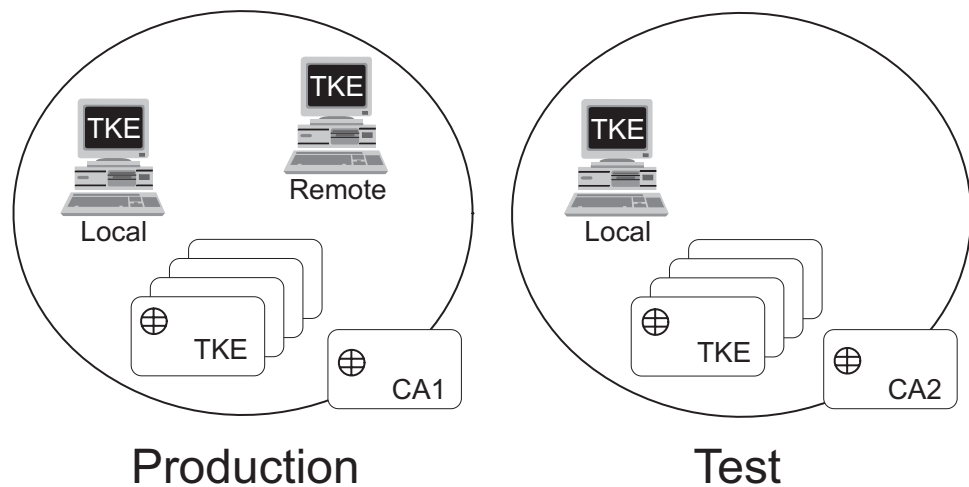


Figure 7. Multiple zones

Figure 7 shows multiple 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 cryptographic adapters
- TKE smart cards

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

During enrollment, the entity receives and stores the root certificate of the CA smart card.

A certificate is issued to the entity, enabling the entity to:

- verify that other entities have been enrolled into the same zone
- prove to other entities that it has been enrolled into the zone.

The certificate is destroyed if you initialize (zeroize) the TKE cryptographic adapter.

The entity only establishes cryptographic connections with entities that can prove they are in the same zone, by using a challenge-response protocol. It is not possible for a component or entity to be in more than one zone. Different zones cannot exchange key parts.

TKE smart cards

TKE smart cards can hold:

- A maximum of 10 key parts:
 - ICSF master key parts
 - ICSF operational key parts
 - TKE Cryptographic Adapter workstation master key parts
- One TKE Crypto Adapter logon key
- One TKE authority signature key

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 is 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.

TKE Smart Card description

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.

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.

Note: This setup is done in conjunction with Table 2 on page 49. The tasks defined here replace task 9: *Customize the TKE cryptographic adapter card*.

Table 1. Smart card task checklist

TASK	RESPONSIBLE	WHERE	COMPLETED
1. Attach the smart card readers	IBM CE	TKE workstation	
2. Initialize the crypto adapter for smart card use; see “Initializing TKE for smart cards” on page 227.	TKE Administrator	TKE workstation	
3. Create CA smart card (zone); see “Initialize and personalize the CA smart card” on page 287.	TKE Administrator	TKE workstation	
4. Backup the CA smart card; see “Backup a CA smart card” on page 289.	TKE Administrator	TKE workstation	
5. Initialize and enroll TKE smart cards into the zone; see “Initialize and enroll a TKE smart card” on page 293.	TKE Administrator	TKE workstation	
6. Personalize TKE smart cards; see “Personalize a TKE smart card” on page 294.	TKE Administrator	TKE workstation	
7. Enroll the local TKE cryptographic adapter (and any remote TKE cryptographic adapters) in the zone; see “Enroll a TKE cryptographic adapter” on page 296.	TKE Administrator	TKE workstation	
8. CNM utility - generate TKE Crypto Adapter logon keys; define and load profiles; reset default role. see Appendix C, “Cryptographic Node Management Utility (CNM),” on page 241.	TKE Administrator	TKE workstation	

Chapter 3. Migration

Migrating from TKE Version 2.0 to TKE Version 5.2

This migration includes both hardware and software. You now have a new TKE workstation with TKE V 5.2 installed and a new cryptographic adapter.

There are no migration tools provided for migrating to TKE V5.2. Personal Security Cards (PSCs) available with TKE V 2.0 are NOT usable on TKE V 5.2. Because of this, you must consider the impact on these and perform the appropriate actions described:

- **Host Definitions**

The TKE V 2.0 Host Definitions are APPC connections. You must redefine your existing hosts on TKE V 5.2 and define the relevant TCP/IP information.

- **CCF Crypto Modules, Domains, and Authority Definitions**

The TKE V 2.0 TKECM data set is not compatible with TKE V 5.2. You must redefine CCF Crypto Modules, Domains, and Authority definitions. If you plan to use the same data set name for TKE V 5.2 that you used for TKE V 2.0, you must delete the existing data set or rename it. The TKEFLAGS data set from TKE V 2.0 is no longer used in TKE V 5.2.

When the 'Send Updates' is pressed during migration, the TKECM dataset is updated. This includes:

- Description of the Crypto module
- Description of the Domain
- Optional text field of an authority definition (Name, Phone, E-mail, Address, and Description).

- **Authority Signature Keys on PSCs**

Authority signature keys saved on PSCs from TKE V 2.0 are NOT usable with TKE V 5.2. Before operating TKE V 5.2, the TKE V 2.0 user must do ONE of these:

1. If you will be using binary files for TKE V 5.2 authority signature keys
 - Generate and load new signature keys to the host. From the Authority Administration window, generate a new signature key and save it to a binary file (hard drive or diskette). Read the PM (public modulus). From the authority administration window, create a new authority and choose the signature key you just created to be used with this authority. If this is a CCF crypto module, select change authority and choose the signature key you just created. Send the updated signature key to the host. If saved to a hard drive, copy the binary file to diskette and restore the diskette files to the TKE V 5.2 workstation.
2. If you will be using the TKE V 5.2 Smart Cards for TKE V 5.2 authority signature keys:
 - Change the signature requirements so that signature keys stored on TKE V 2.0 PSCs are not required. From the Crypto Module window, update the appropriate commands with the new signature requirements. Remove any authority whose signature key was stored on TKE V 2.0 PSCs. If you do not have at least one signature key available that uses either a default key (other than authorities 14 or 15) or a signature key saved to binary file, generate and load a new signature key to the host using a binary file as in **Authority Signature Keys on PSCs**.

- From TKE V 5.2, using a default signature key or a signature key saved to a binary file, generate and load new signature keys to the host. From the Authorities Page of the Crypto Module Notebook, generate a new signature key and save it to a TKE V 5.2 smart card that has been initialized and personalized. Get the signature key. Send the updated signature key to the host. Repeat for all authorities that will be using signature keys on TKE smart cards.

Note: Each TKE smart card can hold only one authority signature key.

- After all the authority signature keys have been generated and loaded to the host, define the signature requirements for each TKE command. From the Access Control Page of the Crypto Module Notebook, update the applicable commands with the new signature requirements for authorities whose signature keys are now stored on TKE smart cards. Send the updates to the host.

For additional details on generating signatures, creating or changing authorities, and sending the updates to the Host, refer to Chapter 6, “Crypto Module Notebook,” on page 79.

- **Authority Signature Key in Workstation PKA Key Storage**

There is no direct migration for an authority signature key saved in key storage on the TKE V 2.0 4755 key storage to key storage on the TKE V 5.2 adapter card. You must perform the same tasks described previously.

- **IMP-PKA Keys in Workstation DES Key Storage**

There is no direct migration for IMP-PKA keys loaded in the TKE V 2.0 workstation key storage to the TKE V 5.2 workstation key storage. Depending on how and where the key parts were stored/loaded, the IMP-PKA keys must be reloaded to key storage on the TKE V 5.2 workstation. Follow this process for operational key parts:

- **Master and Operational Key Parts**

- Key parts saved to binary files on TKE V 2.0 hard drive
 - Copy files to diskette
 - Restore diskette files to the hard drive of the new TKE V 5.2 workstation using the TKE File Management Utility. See “TKE File Management Utility” on page 340.
- Key parts entered via the keyboard
 - Enter the key parts on the TKE V 5.2 keyboard
 - If the user wants the known key part values to be saved to a TKE V 5.2 TKE smart card, see Appendix E, “Secure Key Part Entry,” on page 305 for details.
- Key parts saved on TKE V 2.0 PSCs

Master and operational key parts stored on TKE V 2.0 PSCs are NOT usable on TKE V 5.2. The data blocks on the PSCs must be copied to binary files using the TSS HIKM utility. The utility is executed on the TKE V 2.0 workstation as follows:

1. Open a DOS window on the OS/2 desktop.
2. At the DOS command prompt, issue these commands:

```
CD WCS10\UTIL
HIKM
```

The WCS utilities are installed on the C: drive.

3. Press ENTER
4. On panel CSUCM22, press PF2 (to logon with the public profile)
5. On panel CSUCM20 select option 9 and press ENTER.
6. On panel CSUCZ20 select option 3 and press ENTER.
7. On panel CSUCZ01 select option 4 and press ENTER.
8. On panel CSUCZ07 select option 2 and press ENTER.
9. On panel CSUCR88 insert the PSC card.
10. On panel CSUCR86 select the desired data block id and press ENTER.
11. On panel CSUCZ10 select the desired profile and press ENTER.
12. On panel CSUCD03, follow the instructions to Enter the PIN on the security interface unit, then press E on the security interface unit.
13. On panel CSUCZ03 enter Type Block Token and press ENTER.
14. On panel CSUCZ09 select option 1 and press ENTER.
15. On panel CSUCR33 enter the Path for the Data File and press ENTER. Message CSUC0356I will be displayed on the screen. Press ENTER.
16. Copy the file from the hard drive to diskette.
17. Restore diskette files to hard drive of the new TKE V 5.2 workstation using the TKE File Management Utility, see "TKE File Management Utility" on page 340.

Migrating from TKE Version 3.X or 4.X to TKE Version 5.2

TKE Version 5.2 continues to allow you to manage crypto modules on your legacy machines and any PCIXCCs/CEX2Cs inside your z990, z890, z9 EC, z9 BC and System z10 EC. Migration to TKE V 5.2 requires a new TKE workstation and a new cryptographic adapter card.

Backup TKE Configuration Files

Warning: The TKE Backup Diskette MUST have a volume identifier that is either blank or ACTKEBKP. If a diskette with a blank VOLID is used, the backup program rewrites it to ACTKEBKP.

1. Perform these tasks on the existing TKE V3.X or 4.X workstation.
2. Insert the TKEWS Backup diskette into the TKE disk drive.
3. Minimize all windows until only the OS/2 Workplace is displayed.
4. Open the TKE Backup icon on the OS/2 Workplace.
5. Follow the instructions displayed on the windows to complete the backup of the TKE data. Do not remove the TKEWS Backup diskette if you will be copying user defined 4758 roles and profiles.
6. Copy any user defined 4758 roles and profiles to the TKEWS Backup diskette.
 - a. Open an OS/2 window
 - b. From the C: prompt, copy any 4758 roles and profiles that have been saved to a binary file on the hard drive
 - c. If you do not have any customer unique data to copy (step 8), exit the OS/2 window.
7. After the backup is completed and any user defined roles and profiles have been copied, remove the TKEWS Backup diskette for use on TKE V 5.2.
8. Copy customer unique data to the TKEWS Binary Key Backup diskette. If Authority Signature Keys, Master Key parts, or Operational Key parts have previously been saved to a binary file or if the customer has previously

generated and loaded a new Master Key during 4758 initialization and saved the key parts on the TKE hard drive, follow these steps:

- a. Open an OS/2 window if necessary
- b. Insert the TKEWS Binary Key Backup diskette into the TKE disk drive.
- c. From the C: prompt, copy any Authority Signature Keys, Master Key parts, or Operational Key parts that have been saved to a binary file on the hard drive.
- d. After the files have been copied, remove TKEWS Binary Key Backup diskette for use on TKE V 5.2.
- e. Exit the OS/2 window.

TKE Started Task

For TKE V 3.0, 3.1, 4.0, 4.1 and 4.2 customers only

Note: If your host system is being converted from a z900 to a z990, z9 EC, z9 BC and System z10 EC or from a z800 to a z890, the TKE V 3.0, V 3.1 V 4.0, V 4.1 and V 4.2 TKECM data set is not compatible with TKE V 5.2. If you plan to use the same data set name for TKE V 5.2 that you used for your current TKE, you must delete the existing data set or rename it.

For additional details see “TKE Host Transaction Program Setup” on page 234.

These tasks are all performed on the TKE V 5.2 workstation:

Set the Workstation Clock

1. In the left frame of the Trusted Key Entry Console click on Service Management.
2. In the right frame of the Trusted Key Entry Console click on Customize Console Date and Time.
3. Set the time and date, and if using local time, select the time zone.
4. Click on Customize. For additional details see “Setting the Clock” on page 219.

Copy Customer Unique Data

If customer unique data (authority signature keys, master key parts, or operational key parts) was copied to the TKEWS Binary Key Backup diskette and you want the files on the TKE V 5.2 hard drive, copy the files using the TKE File Management Utility.

1. In the left frame of the Trusted Key Entry Console, click on Trusted Key Entry.
2. In the right frame of the Trusted Key Entry Console, click on TKE File Management Utility.
3. Insert the TKEWS Binary Key Backup Diskette into the Floppy drive
4. Copy from the Floppy to the appropriate Data Directory. Signature keys, Host Master Key parts, and Operational Key parts should be copied to the TKE Data Directory. Cryptographic adapter Master Key parts should be copied to the CNM Data Directory.
5. Exit the File Management Utility. Click on File, then Exit.
6. Deactivate the Floppy Drive
 - a. In the right frame of the Trusted Key Entry Console, click on TKE Media Manager.

- b. From the Select Operation drop down, click on Deactivate floppy inserted in floppy drive.
 - c. Click OK. When complete, click Cancel.
7. Remove the TKEWS Binary Key Backup Diskette.

For additional details see “TKE File Management Utility” on page 340 and “TKE Media Manager” on page 376.

Passphrase and Smart Card Setup

TKE V 5.2 continues to support both passphrase and smart card usage. While it's not mandatory, it is recommended that one method be chosen and used and a mixture of methods avoided.

All predefined roles and profiles are in the CNM data directory.

Passphrase Setup

1. Run TKE's IBM Crypto Adapter Initialization task.
 - a. In the left frame of the Trusted Key Entry Console, click on Trusted Key Entry.
 - b. In the right frame of the Trusted Key Entry Console, click on TKE's IBM Crypto Adapter Initialization.
 - c. From the csulcni.sh GUI, reply 'Y' to the "Warning! The following task will initialize your cryptographic coprocessor. All modifications to the cryptographic coprocessor will be lost. Would you like to continue? (Y/N)" prompt.
 - d. Reply 'P' to the "Would you like to prepare your cryptographic coprocessor for Smart Card or Passphrase use? (S/P)" prompt.
 - e. When complete, press Enter to exit.

See “Initializing the TKE cryptographic adapter” on page 219 for additional details.

2. Load Known Master Key Parts to the Cryptographic Adapter

To be able to use migrated DES and PKA Key Storages, you must load the cryptographic adapter master key parts from your previous TKE workstation to the TKE V 5.2 workstation:

- a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 3.10SC.
 - b. Logon KEYMAN1. (Select: File => Passphrase Logon => KEYMAN1).
 - c. Load the First known cryptographic adapter master key part. ((Select: Master Key => Clear Parts => First => Enter the clear key value or select Open (if Open, select the master key part in the File Chooser => Open) => Load => OK => Cancel).

Note: If the key part was loaded from the floppy drive you need to deactivate the floppy drive before removing the floppy. You do not have to close CNM to perform this function.

- 1) In right frame of the Trusted Key Entry Console, click on TKE Media Manager.
- 2) From the select Operation drop down, click on deactivate floppy inserted in floppy drive.
- 3) Click OK. When complete, click Cancel.

- d. Logoff KEYMAN1 and logon KEYMAN2. ((Select: File => Logoff =>Yes => OK => File => Passphrase Logon => KEYMAN2).
- e. Load the Middle and Last known cryptographic adapter master key parts. (Select: Master Key = Clear Parts => Middle => Enter the clear key value or select Open (if Open, select the master key part file in the File Chooser => Open) => Load => OK => (if you have more than one Middle key part, repeat) => Last => Enter the clear key value or select Open => Load => OK => Cancel).

Note: If the key part was loaded from the floppy drive you need to deactivate the floppy drive before removing the floppy. You do not have to close CNM to perform this function.

- 1) In right frame of the Trusted Key Entry Console, click on TKE Media Manager.
 - 2) From the select Operation drop down, click on deactivate floppy inserted in floppy drive.
 - 3) Click OK. When complete, click Cancel.
- f. Set the cryptographic adapter master key. (Select: Master Key => Set).
 - g. Exit CNM.

For additional details on loading cryptographic adapter master key parts see "Loading a new master key from clear key parts" on page 265.

3. Migrate Previous TKE Version to TKE V 5.2.

Execute the Migrate Previous TKE Version to TKE V 5.2 task to migrate TKE related data (TKE Host and Group definitions, 4758 roles and profiles, DES and PKA key storages, 3270 emulator data and TCP/IP information) from your current TKE workstation to your TKE V 5.2 workstation.

- a. In the right frame of the Trusted Key Entry Console, click on Migrate Previous TKE Version to TKE V 5.2.

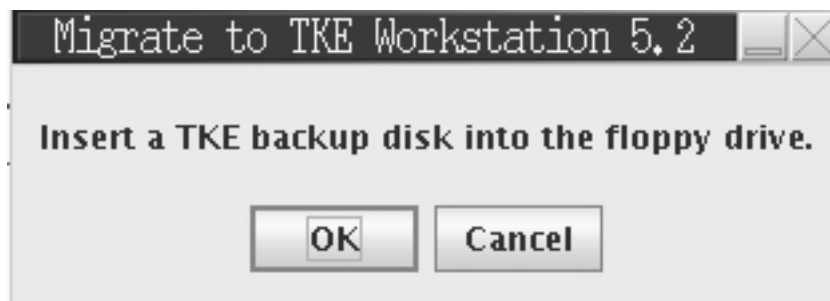


Figure 8. Migrate Previous TKE Version to TKE V 5.2.

- b. The prompt, "Insert a TKE backup disk into the floppy drive" is displayed. Insert your TKEWS Backup Diskette and select 'OK'. The 'Data Migration Progress' panel is displayed.

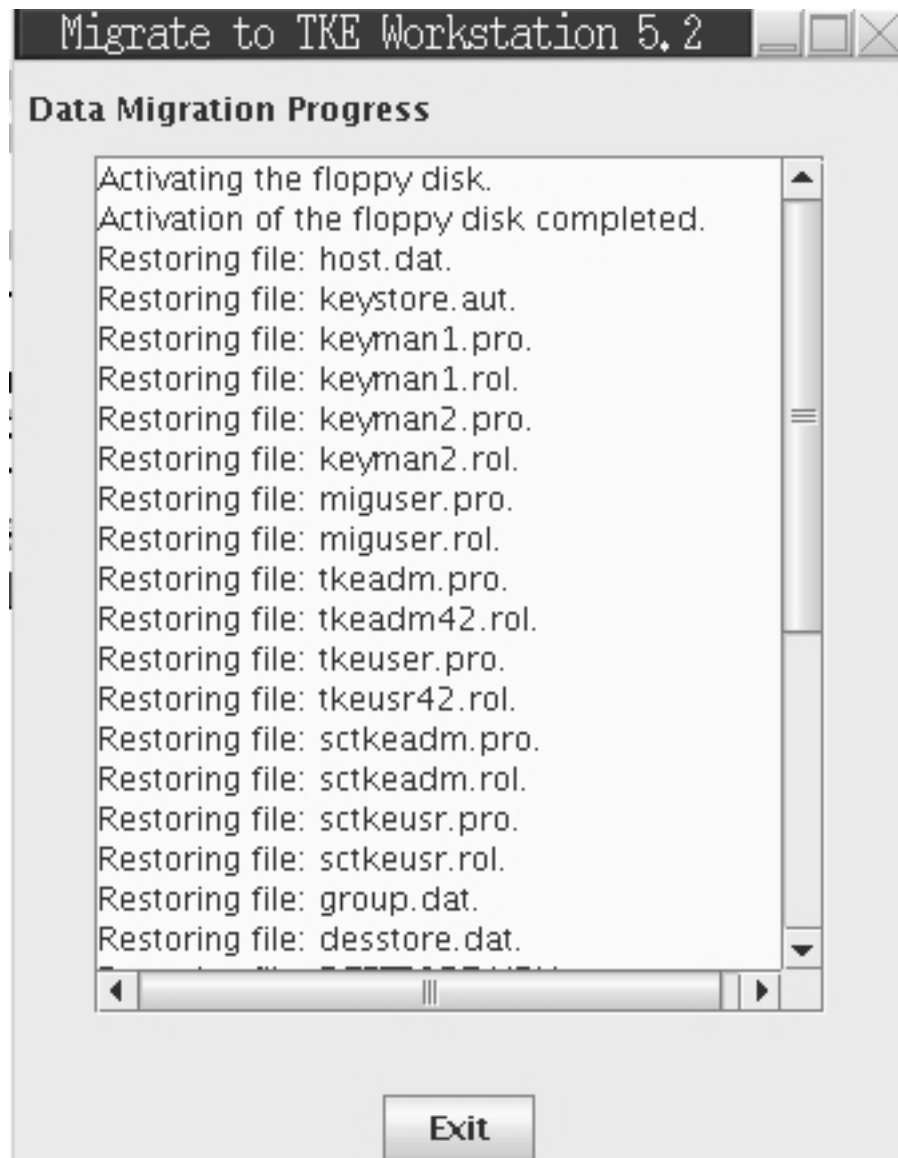


Figure 9. Data Migration Progress Panel

- c. The migrate is complete when the Exit button is no longer greyed out. When complete, click on the Exit button to close the task.
 - d. Deactivate the floppy Drive.
 - 1) In the right frame of the TKE Console, click on TKE Media Manager.
 - 2) From the Select Operation drop down, click on Deactivate floppy inserted in floppy drive.
 - 3) Click OK. When complete, click Cancel.
 - e. Remove the TKEWS Backup Diskette.
- See "Migrate Previous TKE Version to TKE 5.2" on page 338 for details.
4. Re-Initialize DES and PKA Key Storages if Master Key Parts were Unknown
 If you did not load a known master key because you did not know the key parts (Step 2), the migrated DES and PKA key storages will not be usable. You

will need to re-initialize both key storages. Any keys in DES Key Storage and the Authority Signature Key in PKA Key Storage will need to be recreated as appropriate using TKE 5.2.

- a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 3.10SC.
 - b. Logon TKEADM. (Select: File => Passphrase Logon => TKEADM).
 - c. Initialize DES Key Storage. (Select: Key Storage => DES Key Storage => Initialize => Initialize => desstore.dat (in CNM Data Directory) => Save => OK).
 - d. Initialize PKA Key Storage. (Select: Key Storage => PKA Key Storage => Initialize => Initialize => pkastore.dat (in CNM Data Directory) => Save => OK).
 - e. If loading User Defined Roles and Profiles do not exit CNM. Otherwise, exit CNM.
5. Load User Defined Roles and Profiles to the Cryptographic Adapter:
If you are currently not in CNM from Step 4, perform steps a-c, otherwise proceed to step d.
- a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 3.10SC.
 - b. Logon TKEADM (Select: File => Passphrase Logon => TKEADM)
 - c. Load Roles. (Select: Access Control => Roles => Open (File Chooser input can be either Floppy or CNM Data Directory) => Select the user defined role => Open => Load => OK). Repeat for each role to be loaded. When complete => Cancel.
 - d. Load Profiles, including any Group Profiles. (Select: Access Control => Profiles => Open (File Chooser input can be either Floppy or CNM Data Directory) => Select the user defined profile => Open => enter Passphrase, Confirm Passphrase)

Note: Group profiles do not require a passphrase to be entered and confirmed

See "Open or edit a disk-stored role" on page 250 and "Edit a Disk-Stored User Profile" on page 262 for additional details.

6. Update User Defined Roles with Applicable Access Control Points thru CNM:
- a. If Step 4 or 5 was not performed, open the Cryptographic Node Management Utility and logon to TKEADM or an equivalent profile. See Step 4 for details.
 - b. Add the applicable access control points to each user defined role.
(Select: Access Control => Roles => Select the applicable role => Edit => Based on the information below, Add the required access control points from the Restricted Operations to the Permitted Operations => Save (if desired to the floppy or CNM Data Directory) => Load => OK). Repeat for each role to be updated. When complete => Cancel.

For TKE V 4.1 or previous customers only:

If you have any user defined profiles that you want to continue to use to logon to the cryptographic adapter to use TKE, you must add several new access control points to the roles that the profiles are mapped to. The new access control points are:

- X'8002' - TKE Logon
- X'0250' - Load Diffie-Hellman key mod/gen
- X'0251' - Combine Diffie-Hellman key parts

- X'0252' - Clear Diffie-Hellman key values
- X'027A' - Unrestrict Combine key parts

If you have any user defined roles for TKE administrator functions, you must add new access control points:

- X'030B' - Reset battery low indicator
- X'0107' - One-Way Hash SHA-1

For TKE V 4.2 customers only:

If you have any user defined roles for TKE administrator functions, you must add a new access control point:

- X'0107' - One-Way Hash SHA-1

7. Create Passphrase Group Logon Profiles:

If you currently do not have passphrase group profiles defined and want to require that multiple users logon to the cryptographic adapter before either TKE or CNM can be used, define a group profile.

- If Step 4, 5, or 6 was not performed, open the Cryptographic Node Management Utility and logon to TKEADM or an equivalent profile. See Step 4 for details.
- Select: Access Control => Profiles => New. From the Profile Management pop-up, select Group.
- Enter the Group ID, update the Expiration Date. Select the role for the group profile, select passphrase profiles.
- Update the number of Group members required for Logon (minimum is 1, maximum is 10).
- Highlight the profiles from the Available profiles list that you want added to the group and select Add.
- When complete, select Load to load the group profile into the cryptographic adapter. If you also want to save the profile to the hard drive or floppy, select Save.

Note: The Role of the Group overrides the roles of the individual user profiles in the Group. It is recommended that members in the group have their individual user profiles mapped to the DEFAULT role to limit the access the user profiles have outside of the Group.

For additional details on defining group profiles, see “Define a Group Profile” on page 260.

For details on CNM passphrase group logon, see “Group Logon” on page 243.

For details on TKE group logon, see “Passphrase and passphrase group logon” on page 50.

8. Update TKE Preferences using the Preferences menu in TKE.

By default only Blind Key Entry is enabled. Only Enable Smart Card Readers requires a close and reopen of the TKE application to have the change take effect.

- In the right frame of the Trusted Key Entry Console, select **Trusted Key Entry 5.2**.
- Logon to the TKE application
- Select **Preferences** on the toolbar. Choose **Enable/Disable Blind Key Entry**, **Removable Media Only**, **Enable Tracing**, **Enable Smart Card Readers**, and **Show ZKA ECM bits** as appropriate. Preferences are enabled or disabled by clicking on the check box. A check indicates that the preference is enabled.

I

See Chapter 5, “Main Window,” on page 59 for additional details.

9. For IBM System z9 EC, z9 BC and System z10 EC Customers Only - TKE V 5.2 Additional Tasks:
 - a. Create the IBM System z9 EC, z9 BC and System z10 EC Host
 - b. Create Groups for the IBM System z9 EC, z9 BC and System z10 EC Cryptographic Coprocessors
 - c. Create roles on your host crypto modules
 - d. Create Authorities. If you want to use existing authority keys, upload the authority keys saved on floppy or in the TKE Data Directory to the host.
10. The floppy drive is read-only now. To keep all key material on one piece of media, copy over any files from the read-only floppy drive to the DVD-RAM.
 - a. Insert a blank DVD-RAM into the CD/DVD drive.
 - b. Format the DVD-RAM. Select **System Management, Format Media**.
 - c. Select **Format DVD-RAM**, select **OK**.
 - d. Select **Trusted Key Entry Data**, select **OK**.
 - e. Select **OK** on the Format Media Complete message window.
 - f. Insert the Floppy diskette with the information to be copied into the floppy drive.
 - g. Activate the diskette and the DVD-RAM. Select **Trusted Key Entry, TKE Media Manager**.
 - h. Select **Activate read only floppy inserted in the floppy drive**. Select **OK**.
 - i. Select **Activate writeable DVD-RAM disk inserted in the DVD drive**. Select **OK**.
 - j. Select **Cancel**.
 - k. Using the TKE File Management utility copy files from the diskette over to the DVD-RAM. Select **Trusted Key Entry, TKE File Management Utilities**.
 - l. Deactivate the floppy diskette and the DVD-RAM. Select **Trusted Key Entry, TKE Media Manager**.
 - m. Select **Deactivate floppy inserted in floppy drive**. Select **OK**.
 - n. Select **Deactivate media inserted in the floppy drive**. Select **OK**.

Smart Card Setup

If you will be using smart cards, several setup tasks need to be completed. If you are migrating from TKE V 4.2 and are currently using smart cards, you will be able to skip many of the steps. The steps for smart card setup are described in more detail and include:

- Activating smart card support in CNM
- Loading smart card roles to the workstation cryptographic adapter
- Initializing and personalizing a CA smart card
- Backing up a CA smart card
- Enrolling the local workstation cryptographic adapter
- Enrolling the remote workstation cryptographic adapter, if applicable
- Initializing and enrolling TKE smart cards
- Personalizing TKE smart cards
- Generating cryptographic adapter logon keys
- Defining smart card user profiles

- Defining smart card group profiles, if applicable
- Resetting the DEFAULT role
- Updating the TKE Preferences
- Generating new authority signature keys and saving them to TKE smart cards
- Uploading the new signature keys to the host.

Note: There is no migration path to get existing authority signature keys stored in binary files to TKE smart cards. New authority signature keys must be generated. Master and operational keys saved in binary files cannot be transferred to a TKE smart card unless the key part value is known. In this case, secure key part entry can be used (see Appendix E, “Secure Key Part Entry,” on page 305). If the key parts in binary files are not known, there is no migration path. If the key parts are required, you must continue to use the existing binary files. If the key parts are not required, then new key part values can be generated and saved to TKE smart cards.

Note: If you will be moving the smart card readers from your existing TKE Workstation to your TKE V 5.2 workstation, follow these steps:

1. Power down your existing TKE V 4.2 workstation and remove the smart card readers.
2. Power down your TKE V 5.2 workstation.
 - a. In the left frame of the Trusted Key Entry Console, select **Service Management**.
 - b. In the right frame of the Trusted Key Entry Console, select **Shutdown** or **restart**.
 - c. Select **Power Off/Shutdown Console** and select **OK**.
3. Plug the smart card reader cables into the correct ports.
 - a. 9 pin D-shell connector into the serial ports.
 - b. The first passthru cable/connector into the mouse PS2 port. Install the second passthru cable/connector into the first one.
 - c. Install the mouse cable into the second passthru cable/connector.
4. Power on the TKE V 5.2 Workstation.

Steps for smart card setup

The tasks are executed from the CNM utility, SCUP, and TKE. All tasks need to be completed before the TKE workstation is fully operational with smart cards.

1. Activate smart card support in CNM.
 - a. In the left frame of the Trusted Key Entry Console, select **Trusted Key Entry**.
 - b. In the right frame of the Trusted Key Entry Console, select **Cryptographic Node Management Utility 3.10SC**.
 - c. Enable smart card support. (Select: File => Enable Smart Card Readers). Smart Card support will be activated the next time you start CNM.
 - d. Exit CNM.
2. Run TKE's IBM Crypto Adapter Initialization task.
 - a. In the right frame of the Trusted Key Entry Console, click on TKE's IBM Crypto Adapter Initialization.
 - b. From the csulcni.sh GUI, reply 'Y' to the "Warning! The following task will initialize your cryptographic coprocessor. All modifications to the cryptographic coprocessor will be lost. Would you like to continue? (Y/N)" prompt.

- c. Reply '**S**' to the "Would you like to prepare your cryptographic coprocessor for Smart Card or Passphrase? (S/P)" prompt.
- d. When complete, press **Enter** to exit.

3. SCUP Initialization Tasks

Label the smart card readers 1 and 2 (for usability purposes).

- a. In the left frame of the Trusted Key Entry Console.
- b. In the right frame of the Trusted Key Entry Console, click on Smart Card Utility Program V 5.2.

Note: TKE V 4.2 customers with existing CA and TKE Smart Cards only need to execute step e and/or step f.

- c. Initialize and personalize a CA smart card. It is recommended that the first and second CA PINs be entered by different administrators and have different values. (Select: CA Smart Card => Initialize and Personalize CA Smart Card => Follow prompts).

See "Initialize and personalize the CA smart card" on page 287.

- d. Backup CA smart card. (Select: CA Smart Card => Backup CA Smart Card => Follow prompts).

See "Backup a CA smart card" on page 289.

- e. Enroll local workstation cryptographic adapter. (Select: Crypto Adapter => Enroll Crypto Adapter => Local => Follow prompts)

See "Enroll a TKE cryptographic adapter" on page 296.

- f. Enroll remote workstation cryptographic adapter if applicable.

- 1) On the remote TKE, in the right frame of the Trusted Key Entry Console, click on Begin Zone Remote Enroll Process for an IBM Crypto Adapter. Follow prompts.

- 2) Enroll the cryptographic adapter on the Local TKE

If the local TKE is TKE V 4.2 then:

- Open SCUP by clicking on the icon on the Desktop
- Select: 4758 => Enroll 4758 => Remote => Follow prompts

If the local TKE is TKE V 5.2 then:

- In the left frame of the Trusted Key Entry Console.
- In the right frame of the Trusted Key Entry Console Applications, click on Smart Card Utility Program 1.30
- Select: Cryptographic Adapter => Enroll crypto adapter => Remote => Follow prompts

- 3) On the remote TKE, in the right frame of the Trusted Key Entry Console, click on Complete Zone Remote Enroll Process for an IBM Crypto Adapter. Follow prompts.

See "Enroll a TKE cryptographic adapter" on page 296.

- g. Initialize and enroll TKE smart cards. (Select: TKE Smart Card => Initialize and enroll TKE Smart Card; Follow prompts).

See Initialize and Enroll a TKE Smart Card "Initialize and enroll a TKE smart card" on page 293.

- h. Personalize TKE smart cards. (Select: TKE smart card => Personalize TKE Smart Card; Follow prompts)

See "Personalize a TKE smart card" on page 294.

- i. Close the SCUP application.

4. Load Known Master Key Parts to the Cryptographic Adapter

To be able to use the migrated DES and PKA Key Storages, you must load the cryptographic adapter master key parts from your previous TKE workstation to the TKE V 5.2 workstation.

- a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 3.10SC.
- b. It is not necessary to logon to the workstation cryptographic adapter, as the TEMPDEFAULT role is still active.
- c. Load the First known cryptographic adapter master key part. For key parts saved on paper or in binary files: (Select: Master Key => Clear Parts => First => Enter the clear key value or select Open (if Open, select the master key part in the File Chooser => Open) => Load => OK). For key parts saved on TKE smart cards: (Select: Master Key => Smart Card Parts => Insert TKE Smart Card => First => Select the master key part you want to load => Load => Enter PIN => OK).

See Loading a new master key from clear key parts “Loading a new master key from clear key parts” on page 265 and Loading master key parts from a TKE smart card “Loading master key parts from a TKE smart card” on page 268.

Note: If the key part was loaded from the floppy drive you need to deactivate the floppy drive before removing the floppy. You do not have to close CNM to perform this function.

- 1) In right frame of the Trusted Key Entry Console, select **TKE Media Manager**.
 - 2) From the select Operation drop down, select **Deactivate floppy** inserted in floppy drive.
 - 3) Select **OK**. When complete, select **Cancel**.
- d. Load the Middle and Last known cryptographic adapter master key parts. For key parts saved on paper or in binary files: (Select: Master Key = Clear Parts => Middle => Enter the clear key value or select Open (if Open, select the master key part file in the File Chooser => Open) => Load => OK => (if you have more than one Middle key part, repeat) => Last => Enter the clear key value or select Open => Load => OK => Cancel). For key parts saved on TKE Smart Cards: (Select: Insert TKE Smart Card (if middle key part is on a different TKE Smart Card) => Middle => Select the master key part you want to load => Load => Enter PIN (if middle key part is on a different TKE Smart Card) => OK => (if you have more than one Middle key part, repeat) => Insert TKE Smart Card (if last key part is on a different TKE Smart Card) => Last => Select the master key part you want to load => Load => Enter PIN (if last key part is on a different TKE Smart Card) => OK => Cancel).

See Loading a new master key from clear key parts “Loading a new master key from clear key parts” on page 265 and Loading master key parts from a TKE smart card “Loading master key parts from a TKE smart card” on page 268.

Note: If the key part was loaded from the floppy drive you need to deactivate the floppy drive before removing the floppy. You do not have to close CNM to perform this function.

- 1) In right frame of the Trusted Key Entry Console, select **TKE Media Manager**.
- 2) From the select Operation drop down, select **Deactivate floppy** inserted in floppy drive.

- 3) Select **OK**. When complete, select **Cancel**.
 - e. Set the cryptographic adapter master key. (Select: Master Key => Set => Yes => OK).
 - f. Exit CNM
5. Migrate Previous TKE Version to TKE V 5.2.
Execute the Migrate Previous TKE Version to TKE V 5.2 task to migrate TKE related data (TKE Host and Group definitions, 4758 roles and profiles, DES and PKA key storages, 3270 emulator data and TCP/IP information) from your current TKE workstation to your TKE V 5.2 workstation.
 - a. In the left frame of the Trusted Key Entry Console, select **Trusted Key Entry**.
 - b. In the right frame of the Trusted Key Entry Console, select **Migrate Previous TKE Version to TKE V 5.2**.
 - c. The prompt, Insert a TKE backup disk into the floppy drive is displayed. Insert your TKEWS Backup Diskette and select **OK**. The Data Migration Progress panel is displayed.
 - d. The migrate is complete when the Exit button is no longer greyed out. When complete, select **Exit** to close the task.
 - e. Deactivate the Floppy Drive.
 - 1) In the right frame of the Trusted Key Entry Console, select **TKE Media Manager**.
 - 2) From the Select Operation drop down, select **Deactivate floppy** inserted in floppy drive.
 - 3) Click **OK**. When complete, click **Cancel**.
 - f. Remove the TKEWS Backup Diskette.
See "Migrate Previous TKE Version to TKE 5.2" on page 338 for details.
 6. Re-initialize DES and PKA Key Storages if the Master Key Parts were Unknown. If you did not load a known master key because you did not know the key parts (Step 3), the migrated DES and PKA key storages will not be usable. You will need to re-initialize both key storages. Any keys in DES Key Storage and the Authority Signature Key in PKA Key Storage will need to be recreated as appropriate using TKE V 5.2.
 - a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 3.10SC.
 - b. It is not necessary to logon to the workstation cryptographic adapter, as the TEMPDEFAULT role is still active.
 - c. Initialize DES Key Storage. (Select: Key Storage => DES Key Storage => Initialize => Initialize => desstore.dat (in CNM Data Directory) => Save => OK).
 - d. Initialize PKA Key Storage. (Select: Key Storage => PKA Key Storage => Initialize => Initialize => pkastore.dat (in CNM Data Directory) => Save => OK).
 - e. Exit CNM.
 7. CNM initialization tasks
 - a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 3.10SC.
 - b. It is not necessary to logon to the workstation cryptographic adapter, as the TEMPDEFAULT role is still active.

Note: TKE V 4.2 Customers Only. If you have existing roles and profiles and TKE Smart Cards with Cryptographic Adapter Logon Keys proceed to step g.

- c. It is not necessary to create any new workstation cryptographic adapter roles as SCTKEUSR and SCTKEADM are supplied with the code and provide all the required access controls for logging on the workstation cryptographic adapter for TKE, CNM and the Migration Utility respectively. However, you can create new roles as appropriate for your installation. If you do create new roles and want the user profiles that will be mapped to the roles to be suitable for workstation cryptographic adapter logon for TKE, you must permit access control point X'8002' for TKE Logon. If the role does not contain this access control point the user profile will not be displayed for logon for TKE.
- d. Generate a workstation cryptographic adapter logon key to a TKE smart card that will be used for logon to the workstation cryptographic adapter. You will need to generate a workstation cryptographic adapter logon key for each user logging on. (Select: Smart Card => Generate Crypto Adapter Logon key; Follow prompts)

See "Generate TKE Crypto Adapter logon key" on page 275.

- e. Define user profiles for the TKE smart cards that have a workstation cryptographic adapter logon key. (Select: Access Control => Profiles => New => Smart Card => Insert Smart Card => fill in fields; map to SCTKEUSR or SCTKEADM roles => Save (If desired to the floppy or CNM Data Directory => Enter File Name => Save => OK) => Load => OK)

See "Define a User Profile" on page 255. Define a User Profile.

Note: If the user profiles will be used in a group logon profile then they should be mapped to the DEFAULT role to limit the functions available to the user outside of the group.

- f. Load User Defined Roles and Profiles to the Cryptographic Adapter.
 - 1) Load Roles. (Select: Access Control => Roles => Open (File Chooser input can be either Floppy or CNM Data Directory) => Select the user defined role => Open => Load => OK). Repeat for each role to be loaded. When complete => Cancel.
 - 2) Load Profiles, including Group Profiles SCTKEADM and SCTKEUSR. (Select: Access Control => Profiles => Open (File Chooser input can be either Floppy or CNM Data Directory) => Select the user defined profile => Open => Load => OK). Repeat for each profile to be loaded. When complete => Cancel.

Note: Any smart card profiles not saved to a binary file in TKE V 4.2 will need to be created as a New Smart Card profile in TKE V 5.2. See Step f for details.

See Open or Edit a disk stored role "Open or edit an existing role" on page 250 and Edit a disk-stored user profile "Working with User Profiles" on page 262.

- g. Update User Defined Roles with Applicable Access Control Points. Add the applicable access control points to each user defined role. (Select: Access Control => Roles => Select the applicable role => Edit => Based on the information below, Add the required access control points from the Restricted Operations to the Permitted Operations => Save (if desired to the floppy or CNM Data Directory) => Load => OK). Repeat for each role to be updated. When complete => Cancel.

For TKE V 4.1 or previous customers only:

- If you have any user defined profiles that you want to continue to use to logon to the cryptographic adapter to use TKE, you must add several new access control points to the roles that the profiles are mapped to. The new access control points are:
 - X'8002' - TKE Logon
 - X'0250' - Load Diffie-Hellman key mod/gen
 - X'0251' - Combine Diffie-Hellman key parts
 - X'0252' - Clear Diffie-Hellman key values
 - X'027A' - Unrestrict Combine key parts
- If you have defined roles for TKE administrator functions, you must add new access control points:
 - X'030B' - Reset battery low indicator
 - X'0107' - One-Way Hash SHA-1

For TKE V 4.2 customers only:

- If you have defined roles for TKE administrator functions, you must add new access control points:
 - X'0107' - One-Way Hash SHA-1

h. Create Smart Card Group Logon Profiles

Note for existing TKE V 4.2 Smart Card Users:

If you have already loaded your smart card group profiles from TKE V 4.2 and will not be defining any new smart card group profiles, proceed to Step j.

Empty group profiles SCTKEADM and SCTKEUSR are provided in the CNM Data Directory. If you want to require that multiple users logon to the cryptographic adapter before either TKE or CNM can be used, update the appropriate group profile. A group may contain 1 to 10 members.

- 1) For empty group profiles sctkeusr.pro and sctkeadm.pro: (Select: Access Control => Profiles => Open) For new smart card group profiles: (Select: Access Control => Profiles => New => Group => Smart Card Profile)
- 2) Update the number of Group members required for Logon (minimum is 1, maximum is 10).
- 3) Highlight the profiles from the Available profiles list that you want added to the group and select Add.
- 4) When complete, select Load to load the group profile into the cryptographic adapter. If you also want to save the profile to the hard drive or floppy, select Save.

Note: The Role of the Group overrides the roles of the individual user profiles in the Group. It is recommended that members in the group have their individual user profiles mapped to the DEFAULT role to limit the access the user profiles have outside of the Group.

For details on defining group profiles, see “Define a Group Profile” on page 260.

For details on CNM smart card group logon, see “Smart Card Group Logon” on page 245.

For details on TKE group logon, see “Initializing TKE for smart cards” on page 227.

- i. Reset the Default role. The Default role is in the CNM Data Directory. Your TKE Workstation is not secure until the Default role is reset. (Select: Access Control => Roles => Open => default.rol => Open => Load => OK => Cancel)

See “Open or edit a disk-stored role” on page 250.

- j. Exit CNM.

8. Update TKE Preferences using the Preferences menu in TKE.

By default only Blind Key Entry is enabled. Only Enable Smart Card Readers requires a close and reopen of the TKE application to have the change take effect.

- a. In the right frame of the Trusted Key Entry Console, click on Trusted Key Entry V 5.2.
- b. Logon to TKE
- c. Click on **Preferences** on the toolbar. Choose **Enable/Disable Blind Key Entry**, **Removable Media Only**, **Enable Tracing**, **Enable Smart Card Readers**, and **Show ZKA ECM bits** as appropriate. Preferences are enabled or disabled by clicking on the check box. A check indicates that the preference is enabled.

For additional details on updating TKE Preferences, see “TKE Customization” on page 76.

9. Generate New Authority Signature Keys to TKE Smart Cards

For each authority with a signature key saved to a binary file, logon TKE and generate a new authority signature key. Save the signature key to a TKE smart card. Create or change the appropriate authority and upload the new authority signature key to the Host.

Note: Each TKE smart card can hold only one authority signature key.

10. For IBM System z9 EC, z9 BC and System z10 EC Customers Only - TKE V 5.2 Additional Tasks:

- a. Create the IBM System z9 EC, z9 BC and System z10 EC Host
- b. Create Groups for the IBM System z9 EC, z9 BC and System z10 EC Cryptographic Coprocessors
- c. Create roles on your host crypto modules
- d. Create Authorities. If you want to use existing authority keys, upload the authority keys saved on TKE smart cards to the host.

Enable TKE Access Control Points

For TKE V 3.0 Customers Only

This topic is only applicable to customers whose workstation was at TKE V 3.0 prior to the upgrade to TKE V 5.2 and whose configuration includes PCI cryptographic coprocessors. An authorized TKE Authority must enable all applicable access control points for ICSF callable services.

APAR OW46381 must be installed on z/OS V1R1 and OS/390 V2R10 systems or Access Control Failures could occur.

For TKE V 4.X Customers on z890, z990, z9 EC, z9 BC and System z10 EC

This topic is only applicable to z890, z990, z9 EC, z9 BC, and System z10 EC customers whose workstation was at TKE V4.x prior to the upgrade to TKE V5.2. If you are upgrading your ICSF level an authorized TKE authority must enable/disable access control points as appropriate.

See “Working with Domains Controls Settings (PCICC/PCIXCC/CEX2C)” on page 153.

Migrating from TKE Version 5.0 or 5.1 to TKE Version 5.2

To migrate to TKE Version 5.2 you must update the TKE workstation code. If you are adding smart card support, the smart card readers should already be attached. These steps should have been completed as part of the MES instructions. In addition, these tasks should have been performed as part of the MES upgrade:

TKE Started Task For TKE V 3.0 and higher customers only:

Note: If your host system is being converted from a z900 to a z990, z9 EC, z9 BC or System z10 EC or from a z800 to a z890, the TKE V 3.0 and higher TKECM data set is not compatible with TKE V 5.2. If you plan to use the same data set name for TKE V 5.2 that you used for your current TKE, you must delete the existing data set or rename it.

For additional details see “TKE Host Transaction Program Setup” on page 234. These tasks are all performed on the TKE V 5.2 workstation:

TKE Enablement needs to be permitted for z990, z890, z9 EC, z9 BC and System z10 EC systems.

Passphrase and Smart Card Setup

TKE V 5.2 continues to support both passphrase and smart card usage. While its not mandatory, it is recommended that one method be chosen and used and a mixture of methods avoided.

Media information

The floppy drive is read-only now. To keep all key material on one piece of media, copy over any files from the read-only floppy drive to the DVD-RAM. Follow these steps:

1. Insert a blank DVD-RAM into the CD/DVD drive.
2. Format the DVD-RAM. Select **System Management, Format Media**.
3. Select **Format DVD-RAM**, select **OK**.
4. Select **Trusted Key Entry Data**, select **OK**.
5. Select **OK** on the Format Media Complete message window.
6. Insert the Floppy diskette with the information to be copied into the floppy drive.
7. Activate the diskette and the DVD-RAM. Select **Trusted Key Entry, TKE Media Manager**.
8. Select **Activate read only floppy inserted in the floppy drive**. Select **OK**.
9. Select **Activate writeable DVD-RAM disk inserted in the DVD drive**. Select **OK**.

10. Select **Cancel**.
11. Using the TKE File Management utility copy files from the diskette over to the DVD-RAM. Select **Trusted Key Entry, TKE File Management Utilities**.
12. Deactivate the floppy diskette and the DVD-RAM. Select **Trusted Key Entry, TKE Media Manager**.
13. Select **Deactivate floppy inserted in floppy drive**. Select **OK**.
14. Select **Deactivate media inserted in the floppy drive**. Select **OK**.

Smart Card Setup - existing customers

The steps for passphrase setup include:

1. Update User Defined Roles with Applicable Access Control Points thru CNM:
 - a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 3.10SC.
 - b. Logon SCTKEADM. (Select: File => Passphrase Logon => SCTKEADM)
 - c. Add the applicable access control points to each user defined role.
(Select: Access Control => Roles => Select the applicable role => Edit => Based on the information below, Add the required access control points from the Restricted Operations to the Permitted Operations => Save (if desired to the DVD-RAM or CNM Data Directory) => Load => OK). Repeat for each role to be updated. When complete => Cancel.
 - d. Exit CNM.

Smart Card Setup

If you will be using smart cards, several setup tasks need to be completed. The steps for smart card setup are described in more detail and include:

- Activating smart card support in CNM
- Loading smart card roles to the workstation cryptographic adapter
- Initializing and personalizing a CA smart card
- Backing up a CA smart card
- Enrolling the local workstation cryptographic adapter
- Enrolling the remote workstation cryptographic adapter, if applicable
- Initializing and enrolling TKE smart cards
- Personalizing TKE smart cards
- Generating cryptographic adapter logon keys
- Defining smart card user profiles
- Defining smart card group profiles, if applicable
- Resetting the DEFAULT role
- Updating the TKE Preferences
- Generating new authority signature keys and saving them to TKE smart cards
- Uploading the new signature keys to the host.

Note: There is no migration path to get existing authority signature keys stored in binary files to TKE smart cards. New authority signature keys must be generated. Master and operational keys saved in binary files cannot be transferred to a TKE smart card unless the key part value is known. In this case, secure key part entry can be used (see Appendix E, "Secure Key Part Entry," on page 305). If the key parts in binary files are not known, there is no migration path. If the key parts are required, you must continue to use the existing binary files. If the key parts are not required, then new key part values can be generated and saved to TKE smart cards.

Steps for smart card setup:

The tasks are executed from the CNM utility, SCUP, and TKE. All tasks need to be completed before the TKE workstation is fully operational with smart cards.

1. Activate smart card support in CNM.
 - a. In the left frame of the Trusted Key Entry Console, click on Trusted Key Entry.
 - b. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 3.10SC.
 - c. Enable smart card support. (Select: File => Enable Smart Card Readers). Smart Card support will be activated the next time you start CNM.
 - d. Exit CNM.
2. Load smart card roles and profiles.
 - a. Logon to the cryptographic adapter using Passphrase Logon and TKEADM (or an equivalent passphrase profile).
 - b. Load the TEMPDEFAULT.rol (Select: Access Control => Roles => Open => tempdefault.rol => Load => OK => Cancel)
 - c. Load SCTKEUSR role (Select: Access Control => Roles => Open => sctkeusr.rol => Load => OK => Cancel)
 - d. Load SCTKEADM role (Select: Access Control => Roles => Open => sctkeadm50.rol => Load => OK => Cancel)
 - e. Load MIGUSER role (Select: Access Control => Roles => Open => miguser.rol => Load => OK => Cancel)
 - f. Logoff TKEADM
 - g. Exit CNM
3. SCUP Initialization Tasks Label the smart card readers 1 and 2 (for usability purposes).
 - a. In the right frame of the Trusted Key Entry Console, click on Smart Card Utility Program V 5.2.
 - b. Initialize and personalize a CA smart card. It is recommended that the first and second CA PINs be entered by different administrators and have different values. (Select: CA Smart Card => Initialize and Personalize CA Smart Card => Follow prompts). See "Initialize and personalize the CA smart card" on page 287.
 - c. Backup CA smart card. (Select: CA Smart Card => Backup CA Smart Card => Follow prompts). See "Backup a CA smart card" on page 289.
 - d. Enroll local workstation cryptographic adapter. (Select: Crypto Adapter => Enroll Crypto Adapter => Local => Follow prompts). See "Enroll a TKE cryptographic adapter" on page 296.
 - e. Enroll remote workstation cryptographic adapter if applicable.
 - 1) On the remote TKE, in the right frame of the Trusted Key Entry Console, click on Begin Zone Remote Enroll Process for an IBM Crypto Adapter. Follow prompts.
 - 2) Enroll the cryptographic adapter on the Local TKE.

If the local TKE is TKE V 4.2 then:

 - Open SCUP by clicking on the icon on the Desktop
 - Select: 4758 => Enroll 4758 => Remote => Follow prompts

If the local TKE is TKE V 5.0, V5.1 or V 5.2 then:

 - In the left frame of the Trusted Key Entry Console.

- In the right frame of the Trusted Key Entry Console, click on Smart Card Utility Program.
 - Select: Cryptographic Adapter => Enroll crypto adapter => Remote => Follow prompts.
- 3) On the remote TKE, in the right frame of the Trusted Key Entry Console, click on Complete Zone Remote Enroll Process for an IBM Crypto Adapter. Follow prompts. See “Enroll a TKE cryptographic adapter” on page 296.
- f. Initialize and enroll TKE smart cards. (Select: TKE Smart Card => Initialize and enroll TKE Smart Card; Follow prompts). See “Initialize and enroll a TKE smart card” on page 293.
- g. Personalize TKE smart cards. (Select: TKE smart card => Personalize TKE Smart Card; Follow prompts) See “Personalize a TKE smart card” on page 294.
- h. Close the SCUP application.
4. CNM initialization tasks:
- a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 3.10SC.
- b. It is not necessary to logon to the workstation cryptographic adapter, as the TEMPDEFAULT role is still active.
- c. It is not necessary to create any new workstation cryptographic adapter roles as SCTKEUSR, SCTKEADM, and MIGUSER are supplied with the code and provide all the required access controls for logging on the workstation cryptographic adapter for TKE, CNM and the Migration Utility respectively. However, you can create new roles as appropriate for your installation. If you do create new roles and want the user profiles that will be mapped to the roles to be suitable for workstation cryptographic adapter logon for TKE, you must permit access control point X'8002' for TKE Logon. If the role does not contain this access control point the user profile will not be displayed for logon for TKE.
- d. Generate a workstation cryptographic adapter logon key to a TKE smart card that will be used for logon to the workstation cryptographic adapter. You will need to generate a workstation cryptographic adapter logon key for each user logging on. (Select: Smart Card => Generate Crypto Adapter Logon key; Follow prompts). See “Generate TKE Crypto Adapter logon key” on page 275.
- e. Define user profiles for the TKE smart cards that have a workstation cryptographic adapter logon key. (Select: Access Control => Profiles => New => Smart Card => Insert Smart Card => fill in fields; map to SCTKEUSR or SCTKEADM roles => Save (If desired to the floppy or CNM Data Directory => Enter File Name => Save => OK) => Load => OK). See “Define a User Profile” on page 255.
- f. Load User Defined Roles and Profiles to the Cryptographic Adapter.
- 1) Load Roles. (Select: Access Control => Roles => Open (File Chooser input can be either Floppy or CNM Data Directory) => Select the user defined role => Open => Load => OK). Repeat for each role to be loaded. When complete => Cancel.
- 2) Load Profiles, including Group Profiles SCTKEADM and SCTKEUSR. (Select: Access Control => Profiles => Open (File Chooser input can be either Floppy or CNM Data Directory) => Select the user defined profile => Open => Load => OK). Repeat for each profile to be loaded. When complete => Cancel.

Note: Any smart card profiles not saved to a binary file in TKE V 4.2 will need to be created as a New Smart Card profile in TKE V 5.2. See Step f for details. See “Open or edit a disk-stored role” on page 250 and “Edit a Disk-Stored User Profile” on page 262.

g. Create Smart Card Group Logon Profiles.

Empty group profiles SCTKEADM and SCTKEUSR are provided in the CNM Data Directory. If you want to require that multiple users logon to the cryptographic adapter before either TKE or CNM can be used, update the appropriate group profile. A group may contain 1 to 10 members.

- 1) For empty group profiles sctkeusr.pro and sctkeadm.pro: (Select: Access Control => Profiles => Open) For new smart card group profiles: (Select: Access Control => Profiles => New => Group => Smart Card Profile)
- 2) Update the number of Group members required for Logon (minimum is 1, maximum is 10).
- 3) Highlight the profiles from the Available profiles list that you want added to the group and select Add.
- 4) When complete, select Load to load the group profile into the cryptographic adapter. If you also want to save the profile to the hard drive or floppy, select Save.

Note: The Role of the Group overrides the roles of the individual user profiles in the Group. It is recommended that members in the group have their individual user profiles mapped to the DEFAULT role to limit the access the user profiles have outside of the Group. For details on defining group profiles, see “Define a Group Profile” on page 260. For details on CNM smart card group logon, see “Smart Card Group Logon” on page 245. For details on TKE group logon, see “Initializing TKE for smart cards” on page 227.

h. Reset the Default role. The Default role is in the CNM Data Directory. Your TKE Workstation is not secure until the Default role is reset. (Select: Access Control => Roles => Open => default.rol => Open => Load => OK => Cancel). See “Open or edit a disk-stored role” on page 250.

i. Exit CNM.

5. Update TKE Preferences using the Preferences menu in TKE.

By default only Blind Key Entry is enabled. Only Enable Smart Card Readers requires a close and reopen of the TKE application to have the change take effect.

- a. In the right frame of the Trusted Key Entry Console, click on Trusted Key Entry 5.2.
- b. Logon to TKE
- c. Click on Preferences on the toolbar. Enable/Disable Blind key Entry, Floppy Drive Only, Enable Tracing, Enable Smart Card Readers, and Show ZKA ECM bits as appropriate. Preferences are enabled or disabled by clicking on the check box. A check indicates that the preference is enabled. For additional details on updating TKE Preferences, see “TKE Customization” on page 76.

6. Generate New Authority Signature Keys to TKE Smart Cards.

For each authority with a signature key saved to a binary file, logon TKE and generate a new authority signature key. Save the signature key to a TKE smart card. Create or change the appropriate authority and upload the new authority signature key to the Host.

Note: Each TKE smart card can hold only one authority signature key.

TKE Migration Utility

Note: APAR OA07393 must be installed on ICSF FMID HCR770A and below systems, or errors could occur during the installation of converted keys into the CKDS function of the Migration Utility process.

Chapter 4. TKE Up and Running

To use the Trusted Key Entry key management system, several complex tasks must be in place.

Table 2. TKE management system task checklist

TASK	RESPONSIBLE	WHERE	COMPLETED
1. Configure the CCF and PCICC or PCIXCC/CEX2C	IBM CE or Client Operations Representative	Support Element	
2. Load CCF and PCICC or PCIXCC/CEX2C configuration data (for PCIXCC/CEX2C , ensure LIC code has been loaded)	IBM CE or Client Operations Representative	Support Element	
3. If operating in LPAR mode, configure the processor	IBM CE or Client Operations Representative	Support Element	
4. For PCIXCC/CEX2C, permit each PCIXCC/CEX2C for TKE commands (if z990, z890, z9 EC, z9 BC or System z10 EC with May 2004 version or later of Licensed Internal Code (LIC) is installed)	IBM CE or Client Operations Representative	Support Element	
5. Update TCP/IP profiles for TKE	Client Network or VTAM personnel and ICSF Administrator	Host MVS System	
6. Customize TKE Host Program started procs (delivered with ICSF)	Client Network or VTAM personnel and ICSF Administrator	Host MVS System	
7. Ensure RACF administration is complete.	Client Security Administrator	Host MVS System	
8. Start ICSF	Client Operations or System Programmer	Host MVS System Console	
9. Customize the TKE cryptographic adapter card	TKE Administrator	TKE workstation	
10. TKE Application Customization	TKE Administrator	TKE workstation	

For more information on tasks 1 and 2, see *Support Element Operations Guide*.

For more information on tasks 3 and 4, see:

- *Support Element Operations Guide*
- *PR/SM Planning Guide*
- “TKE Enablement for z990, z890, z9 EC, z9 BC and System z10 EC Systems” on page 9.
- Appendix G, “LPAR Considerations,” on page 319.

For more information on tasks 5, 6 and 7, see Appendix B, “TKE TCP/IP and Host Considerations,” on page 233. TKE uses TCP/IP for communication between the TKE workstation and the MVS operating system.

For more information on tasks 9 and 10, see Appendix A, “TKE Workstation Setup and Customization,” on page 215.

Note: If using smart cards, refer to Table 1 on page 23.

Workstation Logon: Passphrase or Smart card

If you have installed TKE V 5.2, you must decide if you will logon with a passphrase or with a smart card. You must decide if you will use group logon. Once these decisions are made, go to the appropriate topic:

- Passphrase - see “Initializing TKE for passphrase” on page 220
- Smart card - see “Initializing TKE for smart cards” on page 227

From the Framework tree on the left hand side of the page, click on Trusted key Entry, then click on Trusted Key Entry 5.2.

The Crypto Adapter Logon window displays the profile IDs you can logon with; these are the single and group profiles previously created.

This is your starting point.

Passphrase and passphrase 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 passphrase logon.



Figure 10. Crypto Adapter logon window with passphrase profiles

Steps for logging on are:

1. Select the Profile ID that you would like to use to logon to the TKE cryptographic adapter.
2. Select **OK**

If you selected a single passphrase profile ID

1. The Passphrase Logon window will be displayed.

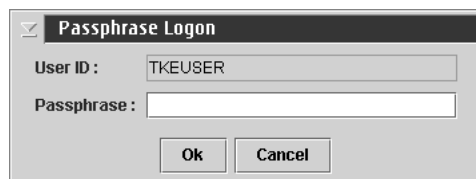


Figure 11. Enter passphrase for logon

2. Enter the passphrase for this profile ID and select **OK**.

Note: The passphrase is case sensitive.

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 12. Crypto Adapter group logon window with passphrase profiles

2. Select the member profile ID that you would like to use to logon to the TKE cryptographic adapter.
3. Select **OK**
4. Enter the passphrase for this profile ID and select **OK**.

Note: The passphrase is case sensitive.

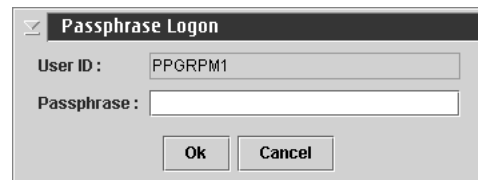


Figure 13. Enter passphrase for logon

5. Information in the Crypto Adapter Group Logon window is updated to reflect that the selected profile ID is now ready for logon

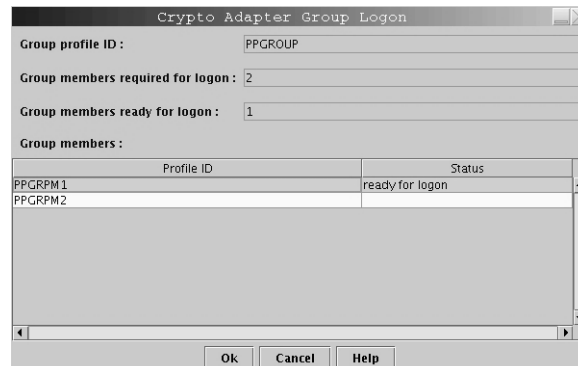


Figure 14. Crypto Adapter Group logon window with passphrase profile ready

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 Appendix C, "Cryptographic Node Management Utility (CNM)," on page 241.

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 15. 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 logon to the TKE cryptographic 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 TKE smart card that contains the TKE crypto adapter logon key for the selected profile ID and select **OK**

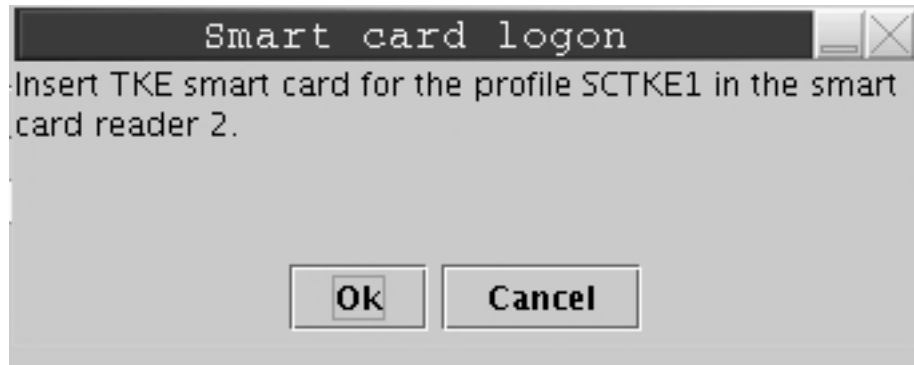


Figure 16. Insert the TKE smart card

3. Enter PIN for the TKE smart card

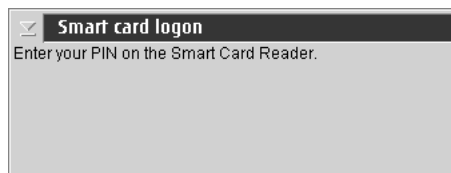


Figure 17. Enter smart card PIN

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 18. Crypto Adapter Group logon window with smart card profiles

2. Select the member profile ID that you would like to use to logon to the TKE cryptographic adapter.
3. Select **OK**
4. Insert the TKE smart card that contains the TKE crypto adapter logon key for the selected profile ID and select **OK**

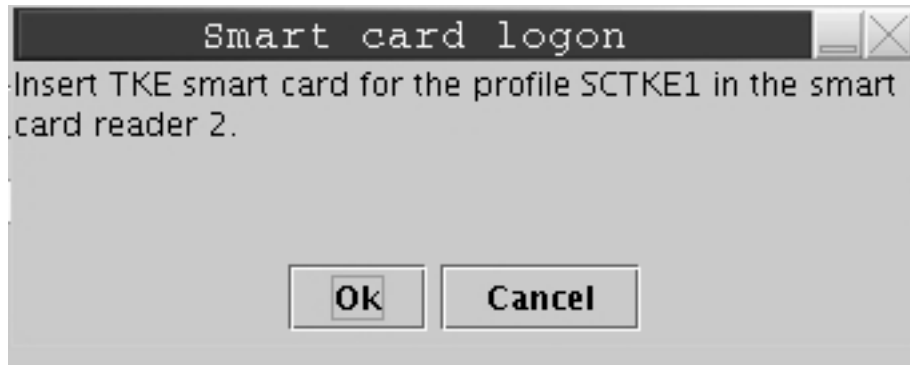


Figure 19. Insert the TKE smart card

5. Information in the Crypto Adapter Group Logon window is updated to reflect that the selected profile ID is now ready for logon



Figure 20. 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 the predefined group smart card profile, SCTKEUSR, or another user profile with 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 Appendix C, "Cryptographic Node Management Utility (CNM)," on page 241.

With either passphrase or smart card logon, if you cancel the logon, TKE operates under the DEFAULT role. Use of the DEFAULT role does not require a user profile. Any user can use the services permitted by the DEFAULT role without logging onto or being authenticated by the TKE cryptographic coprocessor. However, the DEFAULT role is limited in the operations it is allowed to perform.

Automated Crypto Module Recognition

For each host, the TKE workstation maintains a list of the installed crypto modules (CCF and PCICC or PCIXCC/CEX2C). The list contains all the information required to protect communication between the workstation and the 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 these events occur:

- A new crypto module has been installed
- A crypto module has been removed
- A crypto module has been replaced
- A crypto module had its signature key pair regenerated (PCICC/PCIXCC/CEX2C only)
- A crypto module has been moved from one slot to another (PCICC/PCIXCC/CEX2C only)

Authenticating the CMID and CMPM

The crypto module ID (CMID) and the Crypto Module Public Modulus (CMPM) are used by the TKE workstation for verification of the messages from the crypto module.

CCF

At the very first communication between a crypto module and the TKE workstation, the CMID and CMPM from the crypto module are displayed at the workstation. You are to verify the CMID against the CMID on the enablement diskette and verify that the enablement diskette was successfully loaded.

Press the **Yes** button if the CMID values are equal. The values are saved at the TKE workstation for further communication with the crypto module. The crypto module is marked as **Authenticated**.

Press the **No** button if the values differ. The crypto module is marked as **Rejected by user**. You will not be able to work with the crypto module but you are able to authenticate the module again. To re-authenticate the module, select the module. The CMID/CMPM window is displayed for you to accept or reject the values.

The confirmation process is only performed once, at the initial logon. In the event you replace your crypto chip, the confirmation process will have to be repeated.

PCICC/PCIXCC/CEX2C

For PCICC/PCIXCC/CEX2C crypto modules, the CMID and the type of the crypto module is displayed.

To verify the CMID, you need to logon to your host TSO id. From the ICSF main panel, choose option 1, Coprocessor Management. This panel will list all the PCICCs or PCIXCCs/CEX2Cs available to this host. Verify the coprocessor index and serial number with the information on the 'Authenticate crypto module' window on TKE.

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 at the TKE workstation for further communication with the 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 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.

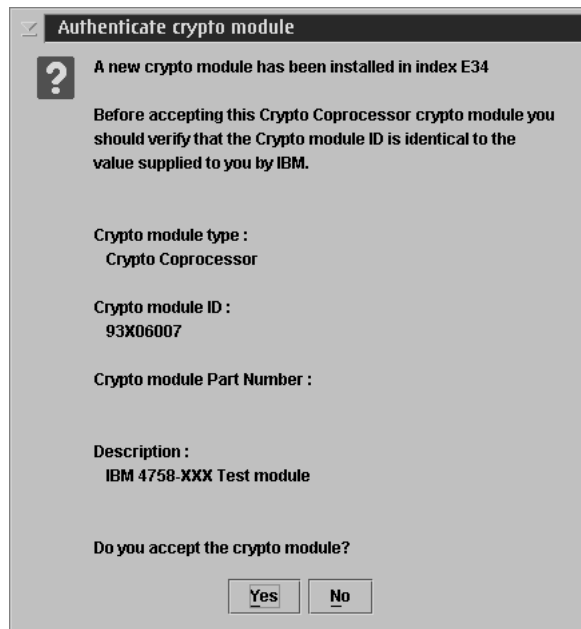


Figure 21. Authenticate Crypto Module for PCIXCC/CEX2C

Attention! The crypto module type for the PCIXCC and CEX2C on the TKE panels will be Crypto Coprocessor.

It is not necessary to authenticate the Crypto Module Public Modulus. The CMPM is authenticated by a chain of certificates. The public key of the root certificate is hardcoded into the TKE workstation code. The user is informed of the result of the verification process.

The IBM CE may need to reload code in the PCICC or PCIXCC/CEX2C card on the host for maintenance. If this is done, at the first communication with the PCICC or PCIXCC/CEX2C, it is sometimes necessary to reauthenticate the crypto module because the signature key has been regenerated.

Initial Authorities

All commands from the workstation are signed. An initial signature key relationship must be established between the workstation and the crypto modules before the first command is issued. The Default Signature Key is used for this task.

For CCF, the initialization process loads the public part of the authority default signature key to authority registers 00–13.

Attention: Authorities 14 and 15 cannot be used for signing commands until their default signature keys have been changed. Either these authority signature keys must be changed or they should not be defined in the Signature Requirements Array as authorized or required to sign commands.

For PCICC/PCIXCC/CEX2C, the initialization process creates the authority 00 and assigns the authority default signature key to this authority.

Backing Up Files

The Backup Utility supported on previous versions of TKE (which backed up host.dat, group.dat, 4758 pre-defined roles and profiles, 4758 key storages, TCP/IP information, and emulator session configurations) is no longer available. If you want to have specific files saved to DVD-RAM for backup purposes other than install/recovery (Backup Critical Console Data), files can be manually backed up using the TKE File Management Utility. This is an activity that should be performed when you have completed your initialization tasks and any time you make changes to TKE-related information. Files that should be backed up are listed here. In addition, any user defined roles and profiles, authority signature keys saved to binary files, and master and Operational key parts saved to binary files should also be backed up. A DVD-RAM is shipped with your TKE workstation for this purpose (TKEDATA) or a customer supplied DVD-RAM may be used. See “Backup Critical Console Data” on page 357 and “TKE File Management Utility” on page 340 for more information.

Workstation Files

This is a list of the TKE application specific files.

- HOST.DAT — contains definitions for the host sessions and related host data. It also contains the CMID for each crypto module and public modulus.
- GROUP.DAT — contains definitions for groups.

These files should be backed up whenever definitions are changed.

The supplied roles and profiles for the TKE crypto adapter are:

- Passphrase
 - TKEUSR52.ROL
 - TKEUSR42.ROL
 - TKEADM50.ROL
 - KEYMAN1.ROL
 - KEYMAN2.ROL
 - TKEUSER.PRO
 - TKEADM.PRO
 - KEYMAN1.PRO
 - KEYMAN2.PRO
- Smart card
 - SCTKEUSR52.ROL
 - SCTKEUSR.ROL
 - SCTKEADM50.ROL
 - SCTKEUSR.PRO
 - SCTKEADM.PRO

Any user defined roles and profiles for the TKE crypto adapter should be backed up.

- desstore.dat and desstore.NDX — DES Key Storage used to hold IMP-PKA keys for encrypting RSA keys, IMPORTER keys, and EXPORTER keys.
- pkastore.dat and pkastore.NDX — PKA Key Storage used to hold one authority signature key.

Host Files

One file on the MVS Host system should be saved. The name of the ***crypto module*** dataset is defined in the JCL used to start the TKE Host Transaction program.

- ***crypto module*** dataset — contains definitions for the Crypto Modules, Domains, and Authorities

This file is updated any time the user makes changes in the TKE application windows and crypto module notebooks for the ***crypto module***. It contains crypto module descriptions, domain descriptions and authority information (name, address, phone, e-mail, et cetera).

This file will be backed up on whatever schedule your installation uses to dump user data. Depending on this schedule, you may want to back the file up more frequently if many changes are being made.

There are other host installation files that contain the TKE programs that execute on the host. Once these files have been installed, no updates to them are required. The weekly system dumps should be sufficient for backup of these files. These are the files documented in Appendix B, “TKE TCP/IP and Host Considerations,” on page 233.

Chapter 5. Main Window

The main purpose of this window is to select a crypto module or a group of crypto modules. From the main window, you also create host definitions and group definitions.

Note: Many screen captures now show smart card as an option. If you are not using smart card support, smart card will not be an option for selection on the applicable windows.

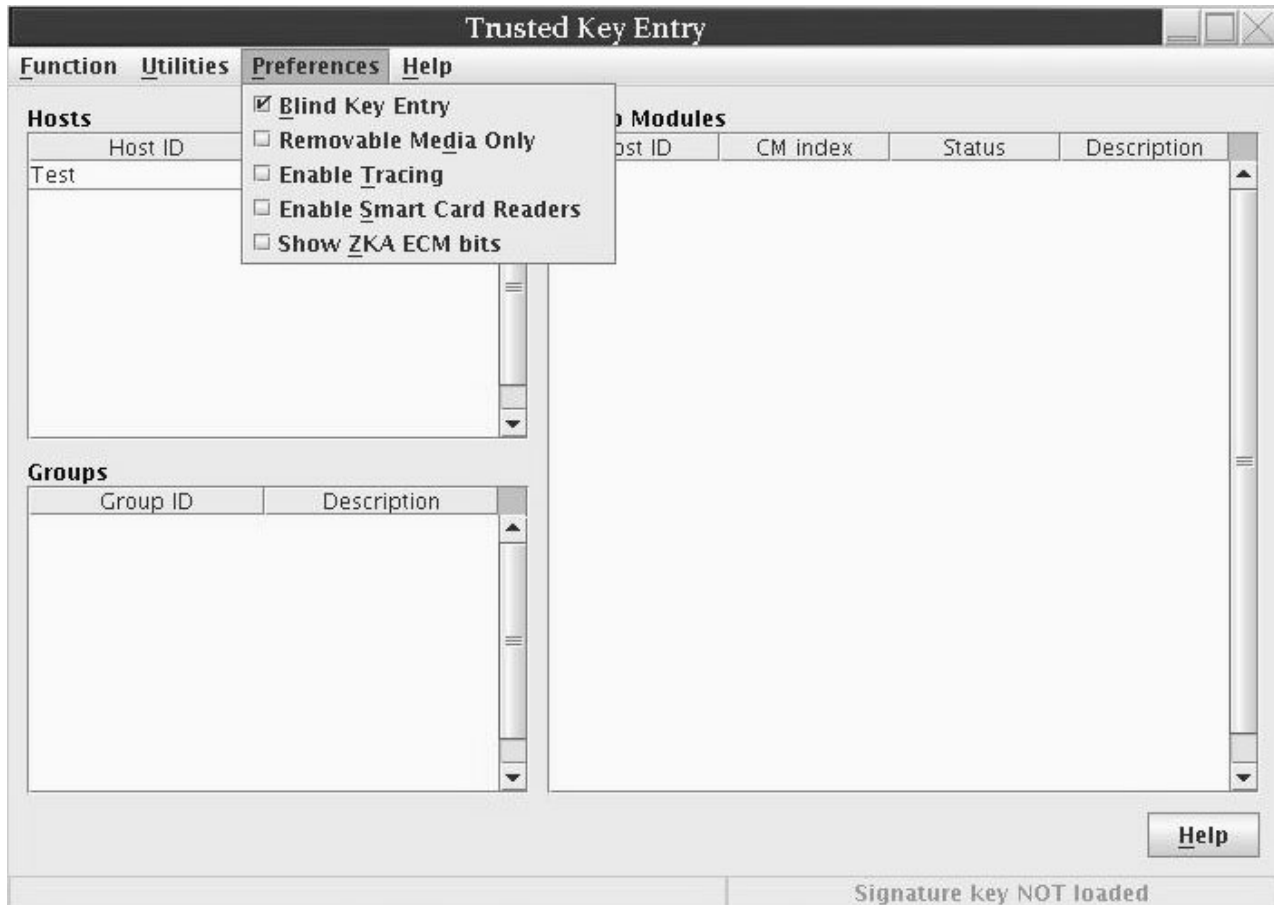


Figure 22. TKE Preferences

Update TKE Preferences using the Preferences menu in TKE. By default only Blind Key Entry is enabled. To customize the TKE workstation update the TKE Preferences using the Preferences menu in TKE. Click on Preferences on the toolbar. Enable/Disable Blind Key Entry, Removable Media Only, Enable Tracing, Enable Smart Card Readers, and Show ZKA ECM bits as appropriate. Preferences are enabled or disabled by clicking on the check box. A check indicates that the preference is enabled. For details on each of the TKE Preferences, see “TKE Customization” on page 76.

The main window has three containers labeled Hosts, Groups and Crypto Modules. All containers are blank until you create a host.

Once you have created a host, decide if you will be working with a single crypto module or a group of crypto modules. If you are working with a single crypto module, you will need to open the host defined in the Hosts container. If you are working with a group, disregard the host container and double-click or open one of the groups defined in the group container.

Note the message in the lower right corner that the signature key is not loaded. See “Load Authority Signature Key” on page 69.

Host Logon

To logon, double-click on the host entry. If working with a crypto module group, double click on the group. When you open a group in the TKE main window, you must logon to all hosts that are to be accessed within that group.

The Logon panel is displayed for the host logon.

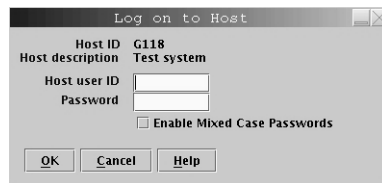


Figure 23. Host Logon Window

Enter your RACF-defined TSO host user ID and password. This 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 panel, passwords will be used as entered and will not automatically be folded to upper case. 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 upper case or you will get 'The password is incorrect' error.

Note: If your TSO password has expired, the message 'The password has expired. Change password from TSO' is displayed. Change your password and perform the logon again.

Working with Hosts

The Hosts container lists the host IDs currently defined to the workstation. You can add, change, delete or open host definitions from this container. When you select your host (by double-clicking or selecting open), the host logon window appears if you have not yet logged on. The crypto modules available for that specific host appear in the crypto module container.

Creating a Host

The TKE workstation keeps a host definition for every host it can connect to. By clicking the right mouse button in the Hosts container, a popup menu is displayed allowing you to choose **Create Host**.

The screenshot shows a standard Windows-style dialog box titled "Create New Host". It features four text input fields arranged vertically, each with a label to its left: "Host ID", "Host description", "Host Name / IP", and "Port number". Below these fields are three buttons labeled "OK", "Cancel", and "Help". In the bottom right corner of the dialog's content area, the text "Trusted Key Entry" is displayed.

Figure 24. Create Host

The host definition contains this information:

- *Host ID* — Mandatory free format text used for referencing the host within TKE.
- *Host Description* — Free-format text for your own use
- *IP address* — 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 Appendix B, "TKE TCP/IP and Host Considerations," on page 233.

LPAR Mode Considerations for CCF Systems

It is not necessary to define each logical partition to TKE. During the setup of the PR/SM environment, one partition will have *Enable modify authority* activated. It will most likely be the first partition you define, and this is the partition you must identify to TKE. The control domain for this partition will contain its own domain as well as any other domain where you want to load keys. The controlling partition will be able to load DES and PKA master keys for itself as well as for the other domains in its control.

For additional details on LPAR setup, refer to Appendix G, "LPAR Considerations," on page 319.

LPAR Mode Considerations for PCIXCC/CEX2C Systems

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 PCIXCC/CEX2C cards that it is to control.

For additional details on LPAR setup, refer to Appendix G, "LPAR Considerations," on page 319.

Changing Host Entries

Highlight the host definition in the hosts container that you want to change and click the right mouse button. A pop-up menu is displayed. Select **Change Host**.

You can change the host description, IP address and port number. 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, highlight the host you want to delete from the hosts container and right mouse click. A pop-up menu is displayed. Select **Delete Host**. A confirmation message is displayed. Select **Yes** to confirm the delete request. Select **No** to cancel the delete.

Working with Crypto Modules

The crypto module container displays the crypto modules that are available for use with the host or group you have selected. The container lists the hostID 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 25 and Figure 26 on page 63 illustrate the main window after logging onto a host. Note that in this screen capture, the signature key has not been loaded. To load a signature key, refer to “Load Authority Signature Key” on page 69.

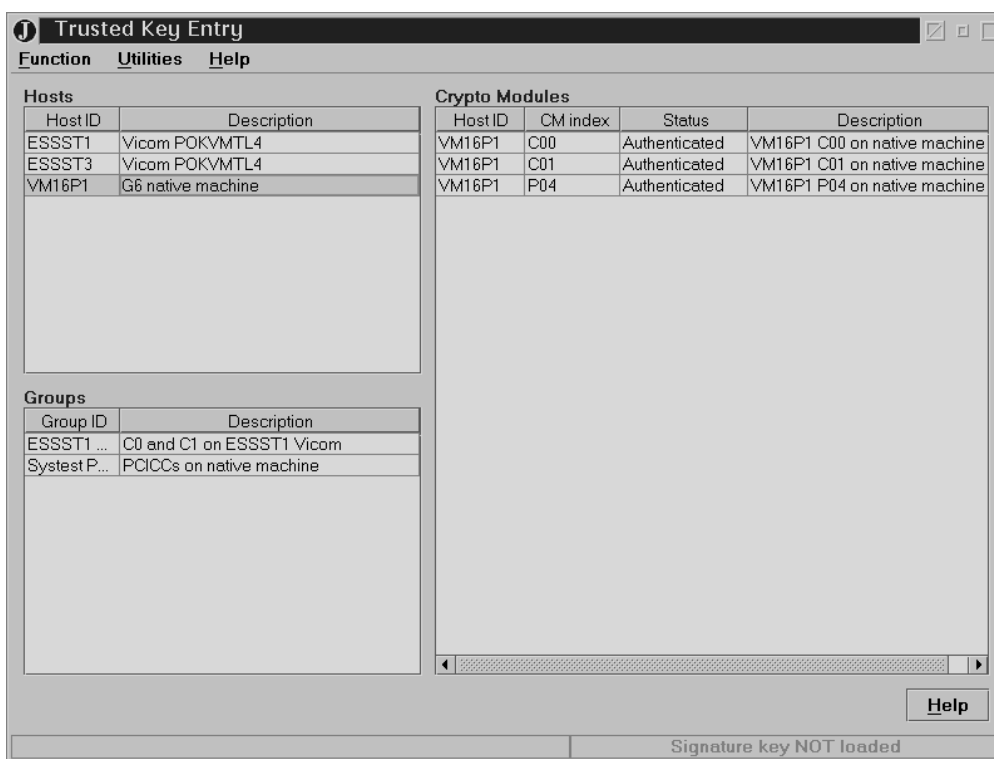


Figure 25. Main Window with Crypto Modules - CCF System

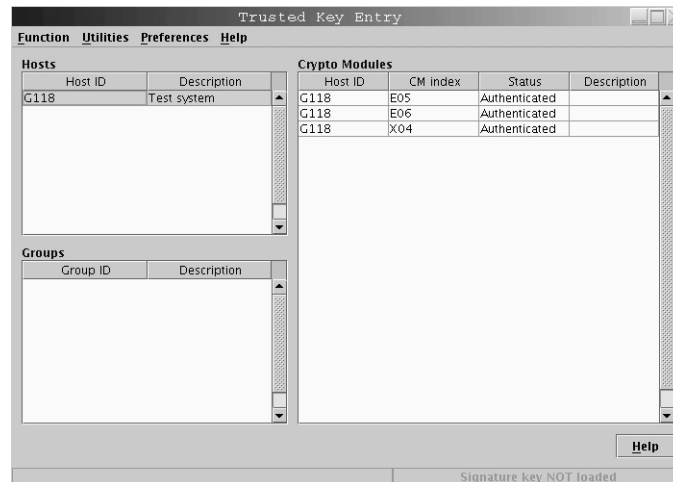


Figure 26. Main Window with Crypto Modules - PCIXCC/CEX2C

As discussed in “Automated Crypto Module Recognition” on page 55, 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.

Double-clicking on a crypto module opens the crypto module notebook.

Working with Groups

You manage groups in the TKE main window. You can add, change or delete group definitions from this container.

The group concept allows you to perform operations on a set of crypto modules as you would on a single crypto module. A group can include crypto modules from different hosts. All modules within a group must be of the same type: either all CCF crypto modules, all PCICC crypto modules or a combination of PCIXCC and CEX2C crypto modules.

Attention! The representation for the PCIXCC and CEX2C crypto modules on the TKE panels is Crypto Coprocessor.

It is highly recommended that you create groups for easier management of your cryptographic coprocessors.

In general, you work with the group as if it is a single crypto module. For example, you will see only one New Master Key register. The values displayed for a group are the values of the master crypto module. You select the master crypto module when you create the group.

It is important that the crypto modules within a group are in the same state (for example, identical signature requirements and authority signature keys for CCF crypto modules and identical roles for PCICC or PCIXCC/CEX2C crypto modules). This is achieved by always working on the crypto modules through the group

interface. When doing access control administration or loading master keys, you should always work with groups to ensure that the values are the same across all crypto modules.

For several CCF and PCIXCC/CEX2C tasks, you must create a group where only one CCF or PCIXCC/CEX2C crypto module for a host is present. This group will be used for loading operational key parts to the key part queue (CCF only), loading RSA keys to the PKDS and loading RSA keys to a host data set.

PCIXCC/CEX2C only: If a group is selected when loading operational key parts to key part registers, only the master PCIXCC/CEX2C will be loaded, even if the group contains other PCIXCCs/CEX2Cs.

When TKE performs a group operation and it is not successful, two new groups are created. One group contains the updated crypto modules and one group contains the crypto modules where the update failed. This allows you to operate on the crypto modules of the failed group until the update is successful. You may then delete the two new groups as you wish.

When you work with a group, you disregard the host container and double-click or open one of the groups defined in the group container. You will be prompted to logon to the hosts associated with the crypto module members of the group.

When you open the crypto modules of a group, a crypto module notebook is displayed.

Creating a Group

To create a new group, right-click the mouse button in the Groups container. Select **New** and the Create Group window opens.

Attention! The representation for the PCIXCC and CEX2C crypto modules on the TKE panels is Crypto Coprocessor.

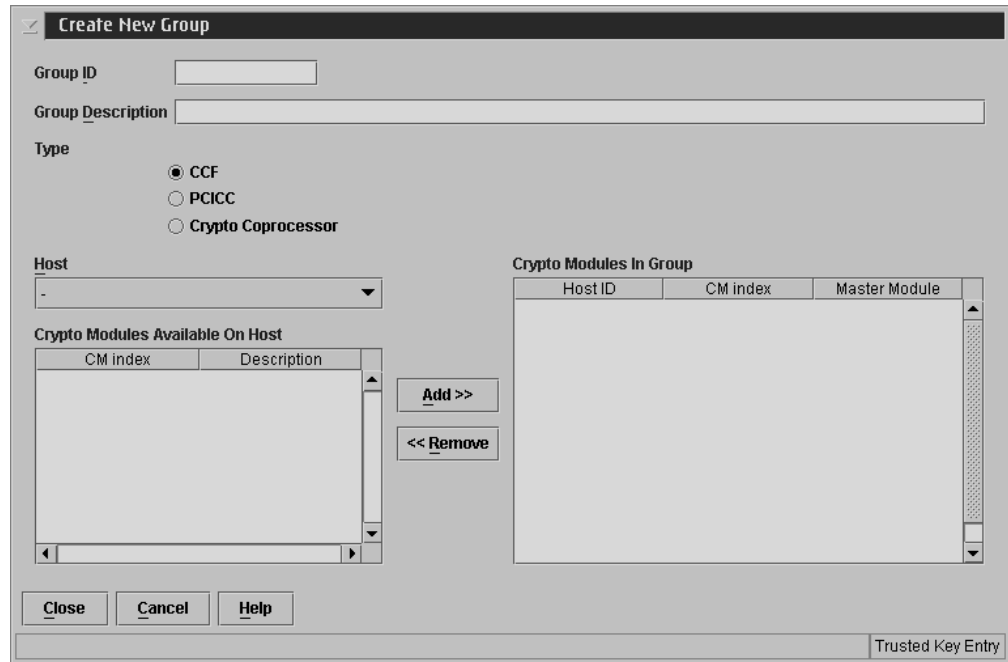


Figure 27. Create Group

Enter your information in the entry fields:

1. *Group ID* - Name of the group (mandatory)
2. *Description* - Optional free text description
3. Type of crypto modules to be in the group - CCF, PCICC or Crypto Coprocessor
4. Select the crypto modules to be in the group:
 - a. In the Host drop down list, select the host that has the crypto modules you want to include in the group.
You will be prompted to logon to the selected host if you are not currently logged on.
 - b. In the Crypto Modules Available on Host container, select the crypto modules you want in the group.
 - c. Press **Add**, and the crypto modules selected now appear in the container: Crypto Modules in Group
 - d. Repeat the prior three steps as required.
5. Select the crypto module to be the Master Module by right-clicking on the module in the Crypto Modules in Group container. **Set as Master Module** appears and sets the Master Module of the group. Unless you change it, the first crypto module added to the group becomes the master module.
6. When finished, press **Close**.

Changing a Group

To change a group, highlight the group you want to work with in the Groups container and then right-click the mouse button. Select **Change** and the Change Group window opens.

Attention! The representation for the PCIXCC and CEX2C crypto modules on the TKE panels is Crypto Coprocessor.

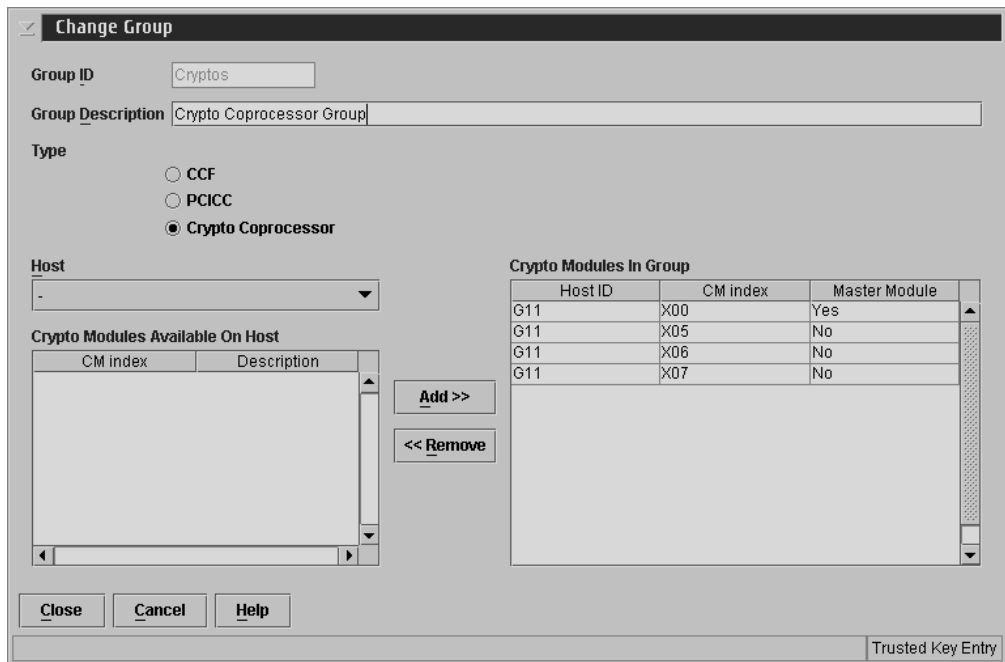


Figure 28. Change Group - Crypto Coprocessor (PCIXCC/CEX2C)

To change the description, edit the field:

- *Description* - Optional free text description

To add more crypto modules to the group:

1. In the Host drop down list, select the host that has the crypto modules you want to add to the group.
You will be prompted to logon to the selected host if you are not currently logged on.
2. In the Crypto Modules Available on Host container, select the crypto modules you want in the group.
3. Press **Add**, and the crypto modules selected now appear in the container: Crypto Modules in Group.
4. Repeat steps 1-3 as required.

To remove crypto modules from the group, select the modules in the container (Crypto Modules in Group) and press **Remove**. If you remove the master module, you are prompted to set another master module.

When finished, press **Close**.

Changing the Master Crypto Module

The Change Group window displays all the crypto modules in the group and indicates which crypto module is the master.

To change the master crypto module for a group, highlight the crypto module you want to set as the master module and right mouse click. Select **Set as Master Module**. The master module is changed.

Comparing Groups

Comparing groups is not done from the main window. It does not compare groups but compares the crypto modules within a group. To compare the crypto modules,

highlight and click on a specific group in the Groups container from the main window. The crypto module group notebook opens. Click on **Functions** and select **Compare Group**.

TKE reads and compares information from all the crypto modules in the group. The process can be cancelled at any time from the progress window display.

All crypto module data is compared, with the exception of the descriptive information for crypto modules, domains, roles and authorities. Transport key hash patterns and information unique by nature (for example, crypto module ID) are also not compared.

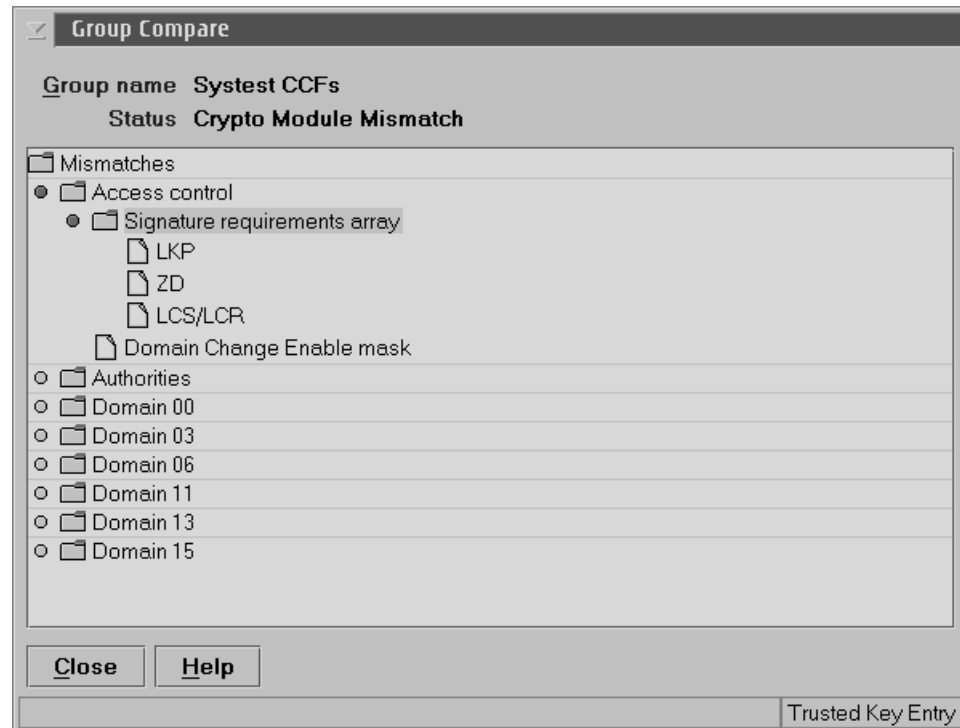


Figure 29. Compare Group - CCF

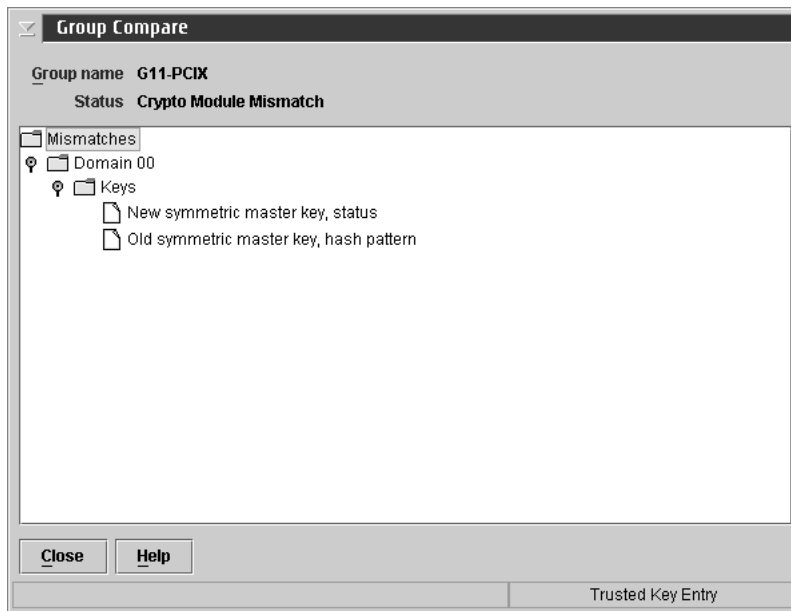


Figure 30. Compare Group - PCIXCC/CEX2X

The Group Compare window displays the 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 Groups

Attention! The representation for the PCIXCC and CEX2C crypto modules on the TKE panels is Crypto Coprocessor.

All displayed values in a notebook for a group are retrieved from the master module. You can perform these crypto module functions from a group notebook:

- Access Control maintenance (CCF group)
- Change authority
- Create and delete authority (PCICC or Crypto Coprocessor group)
- Create, change and delete role (PCICC or Crypto Coprocessor group)
- Zeroize domain
- Domain Controls
- Enable/disable crypto (PCICC or Crypto Coprocessor)
- Domain keys:
 - Load key part to new master key register
 - Load key part to key-part queue (CCF - single group)
 - Clear key register
 - Clear key-part queue (CCF - single group)
 - Set master key
 - Load RSA key to PKDS (CCF and Crypto Coprocessor - single group)
 - Load RSA key to dataset (CCF and Crypto Coprocessor - single group)

- Load operational key part to key part queue (CCF - single group)
- Load operational key part to key part register (Crypto Coprocessor)
- View operational key part registers (Crypto Coprocessor)
- Clear operational key part registers (Crypto Coprocessor)
- Co-sign
- Change signature index for notebook
- Release crypto modules

Function

These selections are available from the **Function** pull-down:

- **Load Signature Key...**
- **Define Transport Key Policy...**
- **Exit**

Load Authority Signature Key

This function is used to load the authority signature key. This signature key is active for all operations until explicitly changed by clicking on this option again to load a different authority signature key. The TKE main window displays messages in the lower right hand corner of the screen. Either SIGNATURE KEY NOT LOADED or SIGNATURE KEY LOADED is displayed.

A dialog box is displayed for the user to select the source of the signature key:



Figure 31. Select Signature Key Source

Attention: Authorities 14 and 15 cannot be used for signing commands until their default signature keys have been changed. Either these authority signature keys must be changed or they should not be defined in the Signature Requirements Array as authorized or required to sign commands.

If you specify **Key storage** or **Default key**, you then specify the authority index to be used.

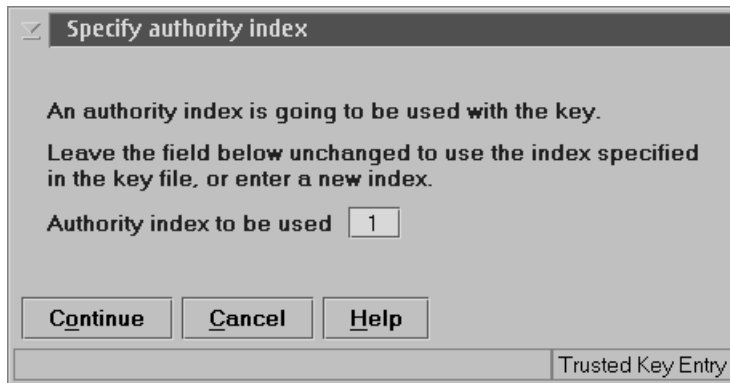


Figure 32. Specify Authority Index

Press **Continue**.

If you select **Binary file**, you must either select a file from the container or enter a file name. Additionally, you must enter a password. This assumes the signature key was previously generated and saved to a binary file.

To create a signature key, see “Generating Authority Signature Keys” on page 95.



Figure 33. Load Signature Key

You then select the authority index (Figure 32).

If you select **Smart card**, you will be prompted to insert your TKE smart card into smart card reader 2.



Figure 34. Load signature key from TKE smart card

You will be prompted to enter the PIN.

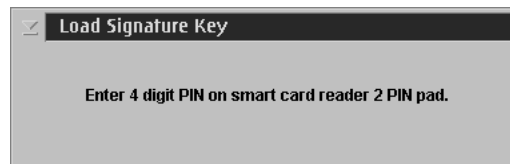


Figure 35. Enter PIN for TKE smart card

You then select the authority index (Figure 32 on page 70).

Define Transport Key Policy

The master key and operational keys are protected by encryption during the transfer between the workstation and the crypto modules. The transport encryption keys (key-encrypting keys) are established by means of a Diffie-Hellman key agreement mechanism.

This selection lets you choose the transport key policy to follow.

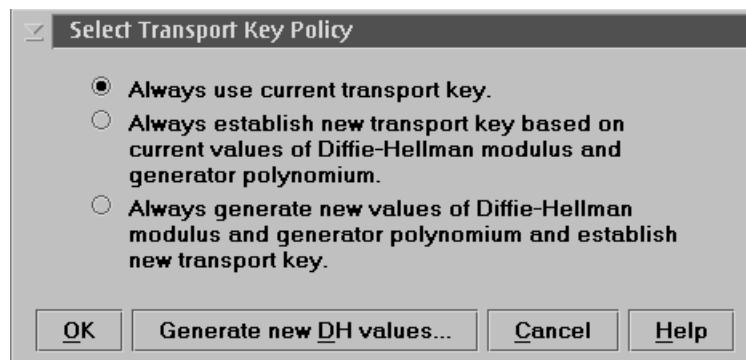


Figure 36. Define Transport Policy

The default is to use the current transport key. This choice is recommended for performance reasons. If a valid transport key is in place, the key can be reused, thus avoiding the key agreement protocol actions.

If a valid Diffie-Hellman modulus (p) and generator (g) public values exist in the workstation and you want to establish a new transport key, you can choose to reuse the existing p and g values. This avoids the time-consuming generation of these values. There are no security exposures to reusing the Diffie-Hellman modulus and generator values.

Lastly, you can choose to generate a new pair of Diffie-Hellman modulus and generator values, which in turn will be used for establishing a new transport key. Generation of a new pair of modulus and generator values is very time-consuming if the modulus size is large.

Select the required option by pressing the radio button and then press **OK**.

Anytime you wish to create new transport keys, press **Generate new DH values**.

Exit

Selecting **Exit** closes the TKE application.

Utilities

These selections are available from the **Utilities** pull-down:

- **Manage Workstation DES keys...**
- **Manage Workstation PKA keys...**
- **Manage smart card contents...**
- **Copy smart card contents...**

These utilities are used for managing the keys in the two workstation key storage areas, managing smart cards and copying smart cards. When managing DES or PKA keys is selected, a window opens displaying the keys stored in the key storage as labels and their attributes.

Manage Workstation DES Keys

TKE uses the TKE workstation DES key storage for holding the RSA key-encrypting keys (IMP-PKAs) and other key-encrypting keys.

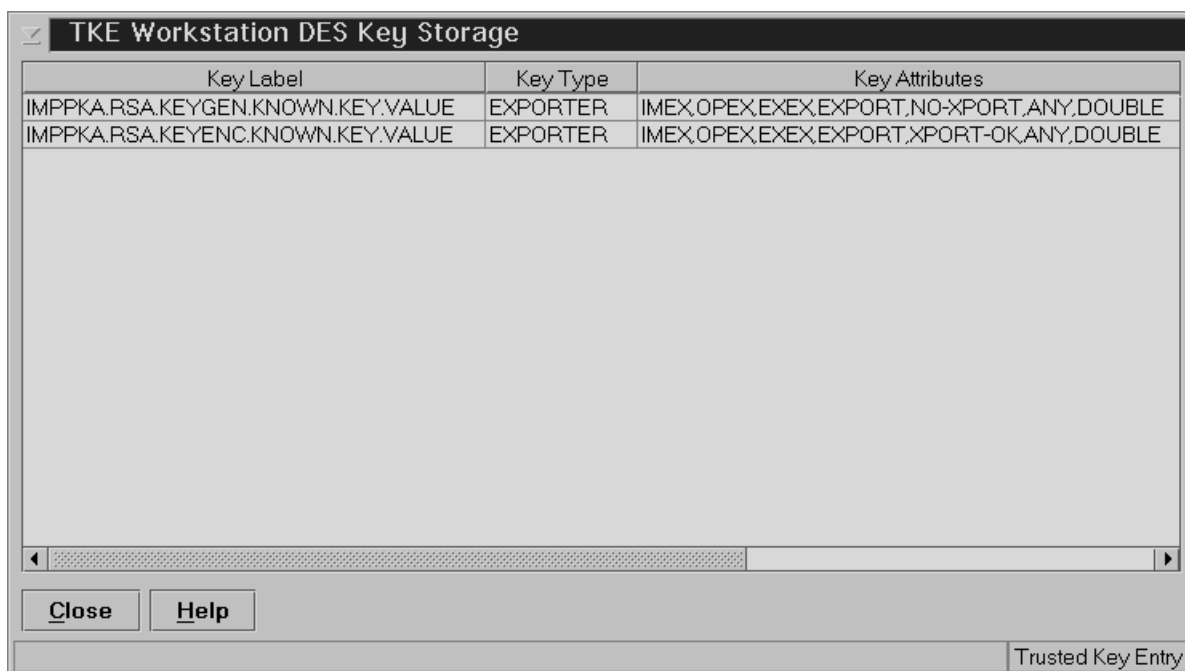


Figure 37. TKE Workstation DES Key Storage Window

The TKE Workstation DES key storage displays:

- Key label
- Key type

Key-encrypting keys written to key storage will have the key type *EXPORTER*. Keys with key type *No_Key* are empty and can be deleted. There may be other key types if the TKE cryptographic adapter card is used for purposes other than TKE.

- Key Attributes

Here is a list of some of the key words used by the TKE 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

If you select an entry, and right-click, a popup 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 signature key.

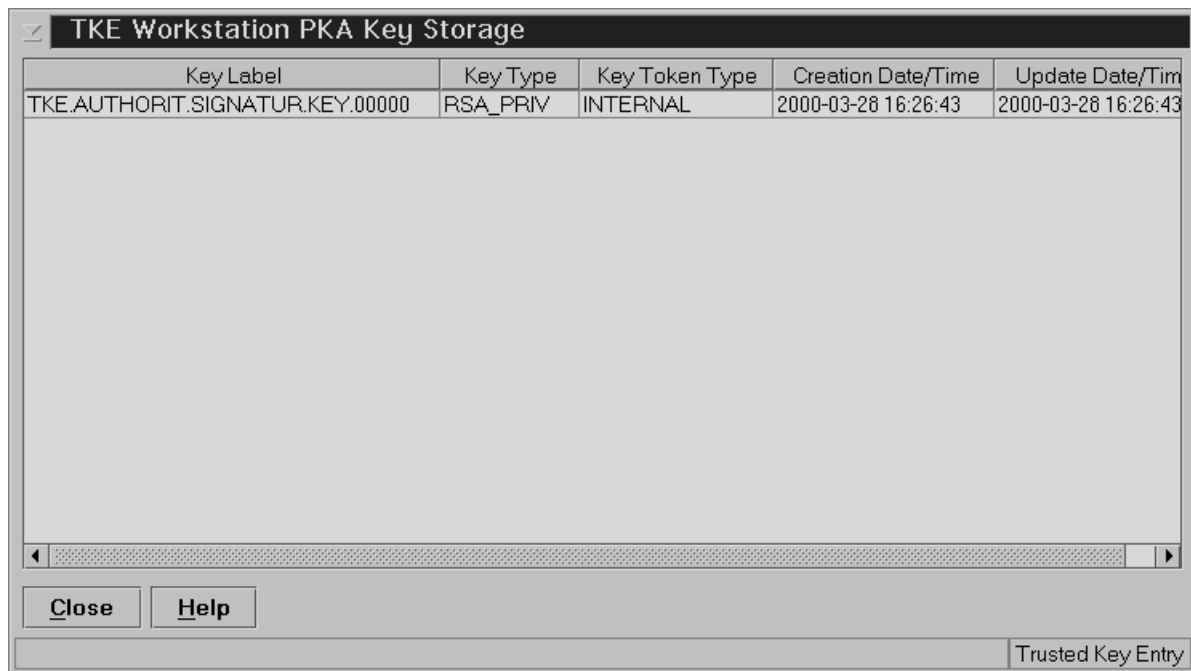


Figure 38. TKE Workstation PKA Key Storage Window

The TKE Workstation PKA key storage displays:

- Key label
- Key type
 - The type of key is one of these:
 - RSA-PRIV - A token holding the private and public key part of a PKA key pair. This is the key type for a 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 these:
 - Internal - The key token is internal and the key value is enciphered under the TKE Crypto Adapter master key.
 - External - The key token is external and the key value is either enciphered or unenciphered by a key-encrypting key.
 - No_Key - The key token is empty.
- Created date and time
- Updated date and time

Deleting an Entry

If you select an entry, and right-click, a popup menu is displayed. The only selection is **Delete key**. This allows you to permanently delete a key from key storage.

Manage smart cards

This function allows you to view or delete keys from your TKE smart card.

1. At the prompt, insert your TKE smart card into smart card reader 2.
2. The utility reads the TKE smart card contents. This may take some time. The card ID is displayed followed by the card description. Verify that this is the TKE smart card you want to work with.

Manage TKE smart card contents

Card ID 1EF574DAS
Zone description TKE50 UT
Card description

Keytype	Description	Origin	MDC4
Crypto adapter Logon key	SCTKE1	Smart card	
TKE Authority key	1, SCTKE1	Smart card	
ICSF symmetric master key part	Key part 1	Crypto adapter	9059AE7888889E8461EDACD49054EB0
ICSF symmetric master key part	Key part 2	Crypto adapter	96202900A5323083F7FF181E9B876C61
ICSF symmetric master key part	Key part 3	Crypto adapter	19E90A570FE65F9CD4FE8F994180099E
ICSF symmetric master key part	Key part 9	Crypto adapter	7E80FBE485AF6A804414448990EC09C6
ICSF symmetric master key part	Key part 4	Crypto adapter	AF0776F60E4F618F35EE9700AAA71770
ICSF symmetric master key part	Key part 5	Crypto adapter	0A1FD85992AD0766C15C4F258C6B0132
ICSF symmetric master key part	Key part 6	Crypto adapter	BEF682C11E71726B48F52CEFAF97EB5
ICSF symmetric master key part	Key part 7	Crypto adapter	59793C42829C4AF6F838733782B06339
Operational key part, DATAM	Operational Key -...	Crypto adapter	6A3EA273CF4E92B74CE5961D2A65B442

Close Help

Trusted Key Entry

Figure 39. TKE smart card contents

The information displayed for a TKE smart card is:

Card ID

Identification of TKE smart card

Card description

Description of the TKE smart card; entered when the smart card was personalized

Card contents

Key type, Description, Origin, MDC4, SHA-1, ENC-ZERO, Control Vector (for operational keys only), and Length

3. Highlight 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 and select **Delete**.
5. Confirm the delete.
6. Enter the 4-digit PIN.
7. You will get a message that the command was executed successfully.

Copy smart cards

This function allows you to copy keys and key parts from one TKE smart card to another TKE smart card. You can copy these types of keys:

- Crypto adapter logon key
- TKE authority key
- ICSF operational key parts
- ICSF master key parts
- Crypto adapter master key parts

Note: The two TKE smart cards must be enrolled in the same zone; otherwise the copy will fail. To display the zone of a TKE smart card, exit from TKE and use either the Cryptographic Node Management Utility 3.10 SC or the Smart Card Utility Program 1.30 under Trusted Key Entry Applications on the Framework. See “Crypto Node Management Batch Initialization 3.10SC” on page 327 or Appendix D, “Smart Card Utility Program (SCUP),” on page 285.

1. Insert the source and target TKE Smart Cards into the appropriate smart card readers.

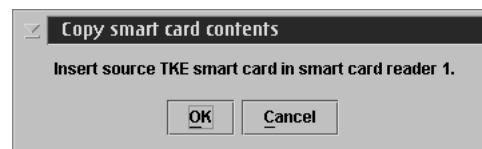


Figure 40. Enter source TKE smart card for copy

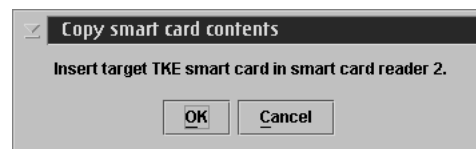


Figure 41. Enter target TKE smart card for copy

2. The utility reads the TKE smart card contents. This may take some time. The card ID is displayed followed by the card description. Verify that these are the TKE smart cards you want to work with.

This lists the information displayed for a TKE smart card:

Card ID

Identification of TKE smart card

Card description

Description of the TKE smart card; entered when the smart card was personalized

Card contents

'Key type, Description, Origin, MDC4, SHA-1, ENC-ZERO, Control Vector (for operational keys only), and Length

3. Highlight the keys that you want to copy. 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. Click on the **Copy** button or right click and select **Copy**.

Note: Smart card copy does not overwrite the target TKE smart card. If there is not enough room on the target TKE smart card, you will get an error message. You can either delete some of the keys on the target TKE smart card (see "Manage smart cards" on page 74) or use a different TKE smart card.

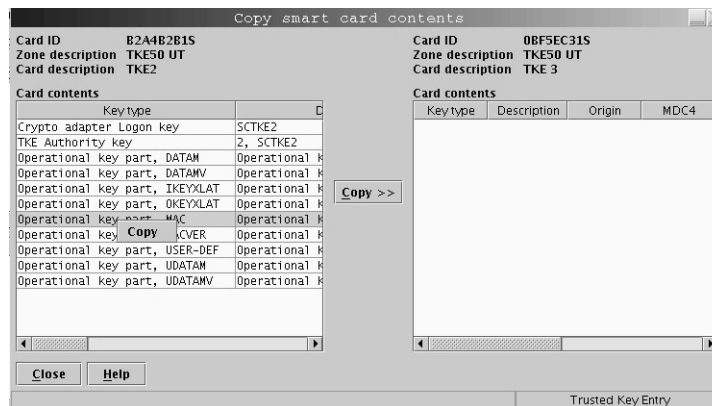


Figure 42. Select keys to copy

4. At the prompts, enter the PINs for the TKE smart cards on the smart card reader PIN pads. The keys will then be copied to the target TKE smart card. The target TKE smart card contents window is refreshed.

TKE Customization

After installation of the TKE workstation a number of parameters can be customized by using the TKE Preferences menu.

Blind Key Entry

Controls if 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.

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 an IBM 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 hide all smart card options from the user.

Note: The TKE application must be closed and reopened for this change to become effective.

ZKA Compliance

ZKA compliance requires specific TKE behavior.

Removable Media Only

Specifies where files can be retrieved and stored.

Ensure the menu item is checked if you want to restrict access to the floppy and DVD drive only; otherwise uncheck the menu item.

For ZKA compliance, this check box must be checked.

Show ZKA ECM Bits

Controls whether or not to display two additional CCF ECM (Environment Control Mask) bits when working with the CCF Domain Controls task:

- Reset Domain
- Load Clear Master Key

For ZKA compliance, this check box must be selected. Further, for the CCF Domain Controls, the only ECM bit that should remain enabled is Cryptographic functions. All other ECM selections must be disabled.

Chapter 6. Crypto Module Notebook

Once you select a crypto module or group of crypto modules, the crypto module notebook opens on the **General** tabular page.

The notebook is the central point for displaying and changing all information related to a crypto module. It is used for single crypto modules as well as groups of modules. The contents of some of the pages vary slightly depending on this. The information on the page also varies depending on the type of the modules: CCF, PCICC or PCIXCC/CEX2C.

Note: Many screen captures now show smart card as an option. If you are not using smart card support, smart card will not be an option for selection on the applicable windows.

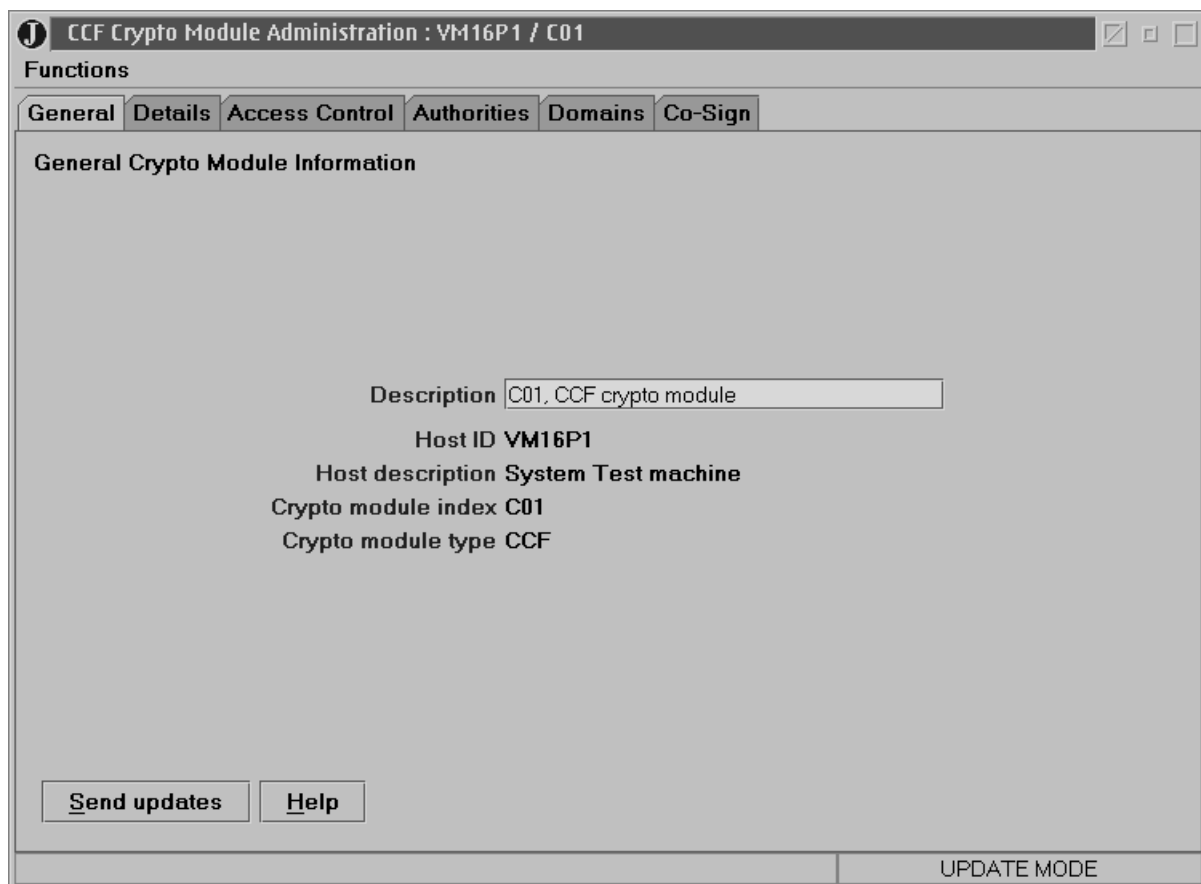


Figure 43. CCF Crypto Module Administration Notebook - General Page

General

The contents of this page are:

- Description

An optional free text description 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. In order to change the description, edit the field contents and press **Send updates**.

- Host or Group ID
- Host or Group Description
- Crypto Module Index

Together with the crypto module type, the index uniquely identifies the crypto module within a host. For CCF crypto modules, the index value is 00 or 01. For PCICC/PCIXCC/CEX2C crypto modules, the index value is 00 through 63. There is no crypto module index for a group.

- Crypto Module Type
- Status (PCICC and PCIXCC/CEX2C)

A PCICC or PCIXCC/CEX2C crypto module is either enabled or disabled. When a PCICC or PCIXCC/CEX2C crypto module is enabled, it is available for processing. From this page you change the status of the module, by pressing the appropriate button. **Enable** is a dual-signature command and another authority may need to co-sign. **Disable** is a single signature command.

Disabling a PCICC or PCIXCC/CEX2C crypto module disables all the cryptographic functions for a single PCICC or PCIXCC/CEX2C crypto module (or group of PCICC or PCIXCC/CEX2C crypto modules). This disables the crypto module for the entire system, not just the LPAR that issued the disable.

PCICC Crypto Module Administration : VM16P1 / P02

Functions

- Refresh Notebook
- Change Signature Index
- Release Crypto Module
- Compare Group
- Close

Authorities **Domains** **Co-Sign**

Description PCICC P02 on VM16P1

Host ID VM16P1

Host description System Test machine

Crypto module index P02

Crypto module type PCICC

Status Crypto module enabled

Send updates **Disable Crypto Module** **Help**

UPDATE MODE

Figure 44. PCICC Crypto Module Administration Notebook - General Page

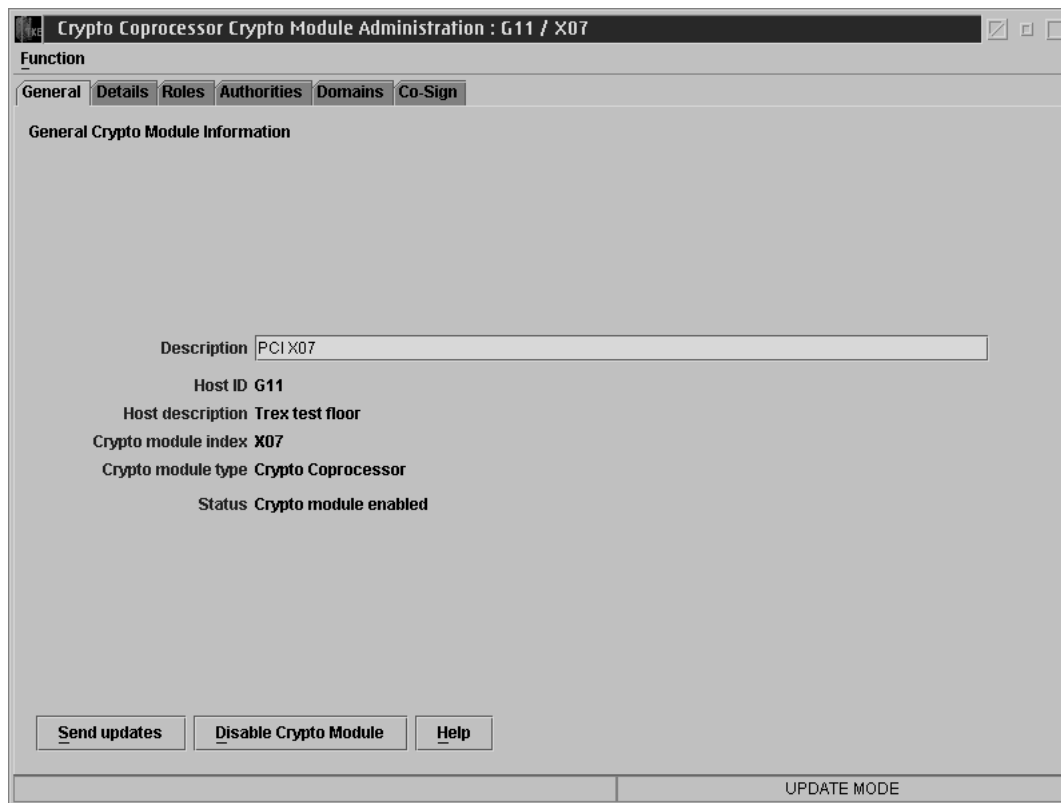


Figure 45. Crypto Coprocessor (PCIXCC/CEX2C) Crypto Module Administration Notebook - General Page

If you press **Disable Crypto Module**, a series of windows open. You are asked if you are sure you want to disable the module and then notified if the command executes successfully. The button on the screen becomes **Enable Crypto Module**.

Intrusion Latch on the PCICC and PCIXCC/CEX2C

Under normal operation, the intrusion latch on a PCICC or PCIXCC/CEX2C 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 recreated. The setting for TKE Enablement is also returned to the default value of *Denied* when the intrusion latch is tripped.

If a situation arises where a PCIXCC/CEX2C needs to be removed, for example, you need to remove your card for service, and you do not want the installation data to be cleared, perform this procedure to disable the PCIXCC/CEX2C .

There is no similar procedure for the PCICC.

This process 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 logon to your TSO user ID on the Host System where the PCIXCC/CEX2C will be removed.
2. From the ICSF Primary Option Menu on TSO, select Option 1 for Coprocessor Management.

3. Leave the Coprocessor Management panel displayed during the rest of this procedure. You will be required to hit ENTER on the Coprocessor Management panel at different times. DO NOT EXIT this panel.
4. Open the TKE Host where the PCIXCC/CEX2C will be removed. Open the PCIXCC/CEX2C . Click on Disable Crypto Module.
5. After the PCIXCC/CEX2C has been disabled from TKE, hit ENTER on the 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 PCIXCC/CEX2C from the Support Element.
7. After the card has been taken Offline, hit ENTER on the Coprocessor Management panel. The status should change to OFFLINE.
8. Remove the PCIXCC/CEX2C. Perform whatever operation needs to be done. Replace the PCIXCC/CEX2C.
9. **Configure On** the PCIXCC/CEX2C from the Support Element.
10. When the initialization process is complete, hit ENTER on the Coprocessor Management panel. The status should change to DISABLED.
11. From the TKE Workstation Crypto Module General page, click on Enable Crypto Module.
12. After the PCIXCC/CEX2C has been enabled from TKE, hit ENTER on the Coprocessor Management panel. The Status should return to its original state. If the Status was ACTIVE in step 2, when the PCIXCC/CEX2C is enabled it should return to ACTIVE.

All installation data; master keys, retained keys, roles, and authorities should still be available. The PCIXCC/CEX2C data was not cleared with the card removal because it was DISABLED first via the TKE workstation.

Notebook Functions

The selections under the **Function** pull-down are:

- **Refresh Notebook** - The content of the notebook is refreshed by reading information from the host. Performing a refresh may change the mode of the notebook.
- **Change Signature Index** - The authority signature index for the currently loaded signature key can be changed. An authority may use the same signature key on different hosts but be known by a different authority index on each host. Since the authority signature key is active until another signature key is loaded, the authority can change his/her signature index to administer different hosts.
- **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.

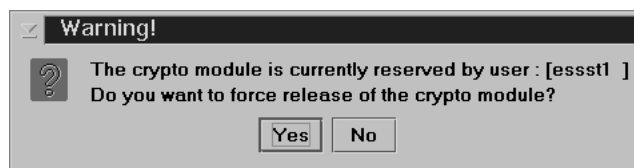


Figure 46. Window to Release Crypto Module

You can confirm release of the crypto module by pressing **Yes**.

Note: 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.

- **Compare Group** - This selection is only displayed if working with a group of modules. For more information, see “Comparing Groups” on page 66.
- **Close** - This selection closes the Crypto Module Notebook.

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 hand corner on all the 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. The notebook is currently opened by another TKE workstation.

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.

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 could not access one or more crypto modules of the group.

Tabular Pages

For the Cryptographic Coprocessor Feature (CCF), the other tabular pages available are:

- Details: see “Details” on page 84.
- Access Control: see “Access Control (CCF only)” on page 85.
- Authorities: see “Authorities” on page 93.
- Domains: see “Domain Keys Page - CCF” on page 105.
- Co-sign: see “Co-Sign” on page 157.

For the PCICC and PCIXCC/CEX2C, the other tabular pages available are:

- Details: see “Details” on page 84.
- Roles: see “Roles (PCICC/PCIXCC/CEX2C)” on page 88.
- Authorities: see “Authorities” on page 93.
- Domains: see “Domains Keys Page (PCICC and PCIXCC/CEX2C)” on page 121.
- Co-sign: see “Co-Sign” on page 157.

As discussed previously, the notebook opens on the General page.

Details

The Details page has five pages of information for CCF crypto modules and two pages for PCICC and PCIXCC/CEX2C crypto modules. No changes to the information are allowed from these pages.

For CCF, the pages and their contents are:

- Crypto module:
 - Crypto Module ID - Unique identifier burnt into the crypto module during the manufacturing process.
 - Public Modulus - Used by TKE to verify signed replies from the crypto module
 - Signature Sequence Number - Sequence number of crypto module signed reply
 - Hash pattern of Basic Transport Key - MDC-4 value of the current Diffie-Hellman DES transport key for this crypto module
 - Hash pattern of PKA Transport key - MDC-4 value of the current Diffie-Hellman PKA transport key for this crypto module
 - Crypto Module Test Mode - Indicates if the crypto module is in test mode
 - Initial PM loaded - Indicates if a manufacturing initialization public modulus is loaded or not loaded for each authority
- TKE Services: displays the list for TKE services, checking those that were enabled during crypto module initialization.
- ICRF Services: displays the list for ICRF services, checking those that were enabled during crypto module initialization.
- PKA Services: displays the list for PKA services, checking those that were enabled during crypto module initialization.
- Key Sizes: displays the maximum length of keys allowed. All key sizes are in bits. For DES keys, parity bits are not included. For Diffie-Hellman keys, the size applies to the largest modulus involved in the establishment of DH transport keys. The settings were loaded during crypto module initialization.

For PCICC and PCIXCC/CEX2C, the pages and their contents are:

- Crypto module:
 - Crypto Module ID - Unique identifier burnt into the crypto module during the manufacturing process.
 - Public Modulus - Used by TKE to verify signed replies from the crypto module
 - Signature Sequence Number - Current value of sequence number from signed, crypto module, replies
 - Hash pattern of transport key - MDC-4 value of the current Diffie-Hellman DES and PKA transport key for this crypto module
- FCV (referred to as Crypto Services on the Details page):
 - Maximum length of RSA keys used to encipher DES keys
 - Base CCA services availability
 - CDMF availability
 - 56-bit DES availability
 - Triple DES availability
 - SET services

The settings were loaded during crypto module initialization.

Access Control (CCF only)

The access control page displays the signature requirements, the authority masks and the domain masks. You define the authorities that can sign each of the multiple-signature commands as well as the number of signatures required.

Here you update which authorities can issue signed commands and which authorities can generate authority signature keys.

Attention: Authorities 14 and 15 cannot be used for signing commands until their default signature keys have been changed. Either these authority signature keys must be changed or they should not be defined in the Signature Requirements Array as authorized or required to sign commands.

If an authority is disabled in the authority signature mask, the authority cannot issue any signed commands. If an authority is signature enabled but is not change enabled, the authority can issue signed commands but a new signature key cannot be loaded for that authority.

By defining authorities to sign commands and by requiring more than one authority signature, unauthorized users are prevented from issuing commands that could change system data. Also, changes that are in error are prevented from occurring since co-signing authorities can validate if the command is required and valid.

Signature Requirements Container

The access control page lists the current signature requirements for each multiple-signature command. Signature requirements are specified as three conditions that have to be fulfilled. Each condition is a list of authorities allowed to sign the command and a count specifying the number of signatures required.

CCF Crypto Module Administration : VM16P1 / C01

Functions

General **Details** **Access Control** **Authorities** **Domains** **Co-Sign**

Access Control

Signature Requirements

Command	Count 1	Signature mask 1	Count 2	Signature mask 2	Count 3	Signature mask 3
LAP	2	+++ + + - - - - -	1	- - - - - + + - - - - -	1	- - - - - + - - - - - -
LCB	1	+++ + - - - - - + + + +	1	- - - - - + + - - - - -	1	- - - - - - - - - - - -
ZD	2	+++ - + - - - - - - -	2	- - - + + + - - - - - +	0	- - - - - - - - - - - -
LEC	1	+++ + + - - - - - - -	0	- - - - - - - - - - - -	0	- - - - - - - - - - - -
LKP	2	+++ - + - - - - - - -	0	- - - - - - - - - - - -	0	- - - - - - - - - - - -
LCS/LCR	2	+++ + + + - - - - - - -	0	- - - - - - - - - - - -	0	- - - - - - - - - - - -
XEM	0	- - - - - - - - - - - -	0	- - - - - - - - - - - -	0	- - - - - - - - - - - -
XES/XER	0	- - - - - - - - - - - -	0	- - - - - - - - - - - -	0	- - - - - - - - - - - -
RTS/RTR	0	- - - - - - - - - - - -	0	- - - - - - - - - - - -	0	- - - - - - - - - - - -
RFS/RFR	0	- - - - - - - - - - - -	0	- - - - - - - - - - - -	0	- - - - - - - - - - - -

Authority Masks

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Authority Enable ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒

Signature Key Change Enable ☐ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒

Domain Masks

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Change Enable ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒

Extraction Enable ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

Send updates **Discard changes** **Help**

UPDATE MODE

Figure 47. CCF Access Control Page

Specifying a required number of signatures equal to zero for all three conditions means that the command does not have any requirements. However, the command must be issued by an authority which can be used to issue signed commands.

The command will not be able to be executed if the required number of signatures is greater than the number of authorities allowed to sign the command.

There is one entry on the page for each of the ten multi-signature commands. The command is identified by its two or three letter acronym. The commands are:

- LAP (Load Authorization Public Modulus)
This command is issued from the Change Authority window, when sending a signature key to the crypto module.
- LCB (Load PKSC Control Block)
This command is issued from the Access Control page.
- ZD (Zeroize Domain)
This command is issued from the Domain General page when requesting the domain to be zeroized.
- LEC (Load Environment-Control Mask)
This command is issued from the Domain Controls page when updating cryptographic capabilities.
- LKP (Load Key Part)

This command is issued from the Load and Load to Queue functions (for loading a new master key or operational keys) of the Domains Keys page.

- LCS/LCR (Load and Combine PKA Master Keys)

This command is issued from the Domain window by the Load function and the reset function for loading and resetting the PKA Signature Master Key and the PKA Key Management Master Key.

- XEM (Extract and Encrypt Master Key)

Not supported by TKE.

- XES/XER (Extract and Encrypt PKA Master Keys)

Not supported by TKE.

- RTS/RTR (Reencipher to PKA Master Keys)

Not supported by TKE.

- RFS/RFR (Reencipher from PKA Master Keys)

Not supported by TKE.

Following the command acronym there are three sets of counts and masks.

The counts define the required number of signatures from the mask that follows. In the mask a check mark indicates an authority that can be used to satisfy a signature requirement.

Changing Signature Requirements

Double-clicking on one of the signature requirement entries brings up a dialog box allowing changes to the signature requirements for that command.

Signature requirements for command : Load Authorization Public Modulus	
Authority	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Signature mask	☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒
Count1	2 of ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒
Count2	0 of ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
Count3	0 of ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

OK Cancel Help

Trusted Key Entry

Figure 48. Change Signature Requirements Window

The window displays the full name of the command in question (in this case, Load Authorization Public Modulus). See the settings of the Authority Signature Mask. This is for reference only as the mask cannot be changed in this box.

The user can change the signature requirements by altering the counts and/or by selecting or unselecting authorities in the masks.

When **OK** is pressed in the dialog box, it is checked whether the number in front of each of the three rows is larger than the number of check boxes ticked in the row and enabled in the Authority Signature Mask.

If so, an error message informing the user of the problem is displayed and the change is rejected.

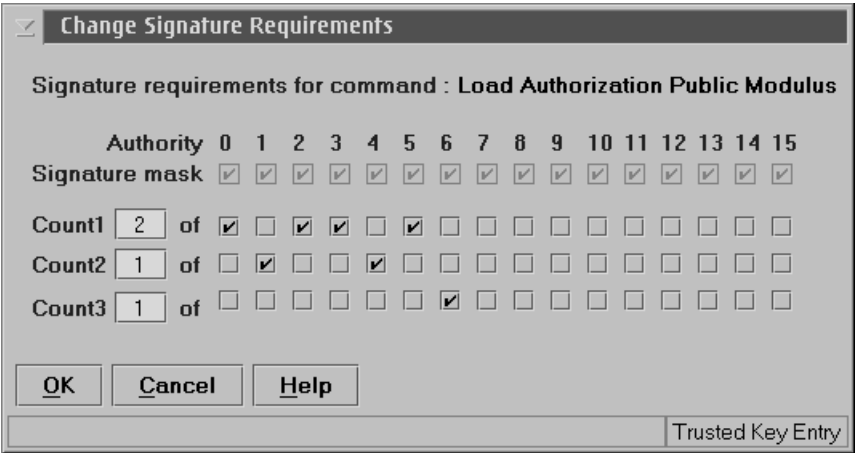


Figure 49. Change Signature Requirements Example

Using the signature requirements defined for the Load Authorization Public Modulus command in Figure 49, these authority signatures would be necessary before the LAP command would complete execution:

- Two signatures from authorities 0, 2, 3 or 5
- One signature from authorities 1 or 4
- Authority 6 MUST sign the command

Authority Masks Container

The authority mask labeled **Authority Enable** displays the authority indices that the crypto module will accept in signed commands.

The authority mask labeled **Signature Key Change Enable** displays the authorities that can have their signature key changed.

To change the mask, click on the relevant check boxes. When all changes have been made, press **Send updates**.

Domain Masks Container

The domain mask labeled **Change Enable** displays the change enable status of individual domains: whether or not it is allowed to enter keys and change enabled cryptographic functions.

The domain mask labeled **Extraction Enable** indicates if keys can be extracted from the domain. This mask should be cleared.

To change the mask, click on the relevant check boxes. When all changes have been made, press **Send updates**.

Roles (PCICC/PCIXCC/CEX2C)

The PCICC and PCIXCC/CEX2C crypto modules use role-based access control. In a role-based system, the administrator defines a set of roles, which correspond to the classes of coprocessor users. Each authority is mapped to one role. In the container, currently defined roles are displayed by their ROLE IDs and Descriptions. You can create, change or delete a role.

A role-based system is more efficient than one in which the authority is assigned individually for each user. In general, the users can be separated into just a few different categories of access rights. You can separate access to domains. You can also control the loading of a two-part key, requiring two different authorities to complete that task.

INITADM is a predefined role available on your system, assigned to authority 00. It was created with both an **issue** access control point and a **co-sign** access control point. This way, you can create the necessary roles and profiles for the PCICC or PCIXCC/CEX2C without needing someone to co-sign. This role allows you to create other roles and authorities for the PCICC and PCIXCC/CEX2C without requiring another authority to co-sign.

Once other roles and authorities are defined, you may choose to assign a different role to authority 00.

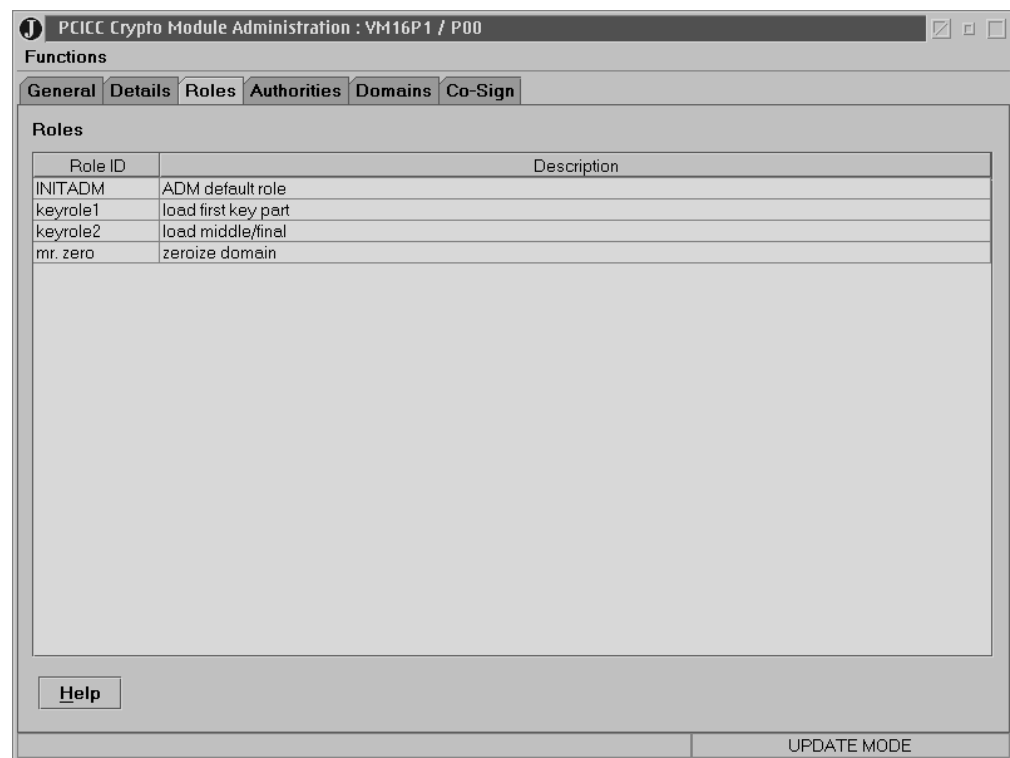


Figure 50. PCICC Roles Page

Multi-Signature Commands

Multi-signature commands for PCICC and PCIXCC/CEX2C modules always require two signatures. The authority authorized to issue the command automatically signs. A signature from the authority authorized to co-sign the command is also required.

If a role has both issue and co-sign authority for a multi-signature command, then the authority assigned to the role automatically co-signs the command after issuing it. (A role is assigned issue or co-sign authority or both when the role is created or changed.)

There are four dual-signature commands:

- Enable crypto card - This command is issued from the General page when changing the crypto module state.
- Access Control - This command is issued from:
 - Create/Change Role windows - when creating or changing a role
 - Role page - when deleting a role
 - Create/Change Authority windows - when creating or changing an authority
 - Authorities page - when deleting an authority
- Zeroize domain - This command is issued from the Domain General page when zeroizing a domain.
- Domain controls - This command is issued from the Domain Controls page when updating control settings.

Single Signature Commands

These commands require only one signature:

1. Disable crypto card
2. Load first key part - SYM-MK and ASYM-MK
3. Combine middle key parts - SYM-MK and ASYM-MK
4. Combine final key part - SYM-MK and ASYM-MK
5. Clear new master key register - SYM-MK and ASYM-MK
6. Set asymmetric master key - ASYM-MK
7. Load first key part - PCIXCC/CEX2C only (Operational Keys)
8. Load additional key part - PCIXCC/CEX2C only (Operational Keys)
9. Complete key - PCIXCC/CEX2C only (Operational Keys)
10. Clear operational key register - PCIXCC/CEX2C only (Operational Keys)

Creating or Changing a Role

When you right click in the container, a pop-up window appears and you can select **Create**, **Change** or **Delete**:

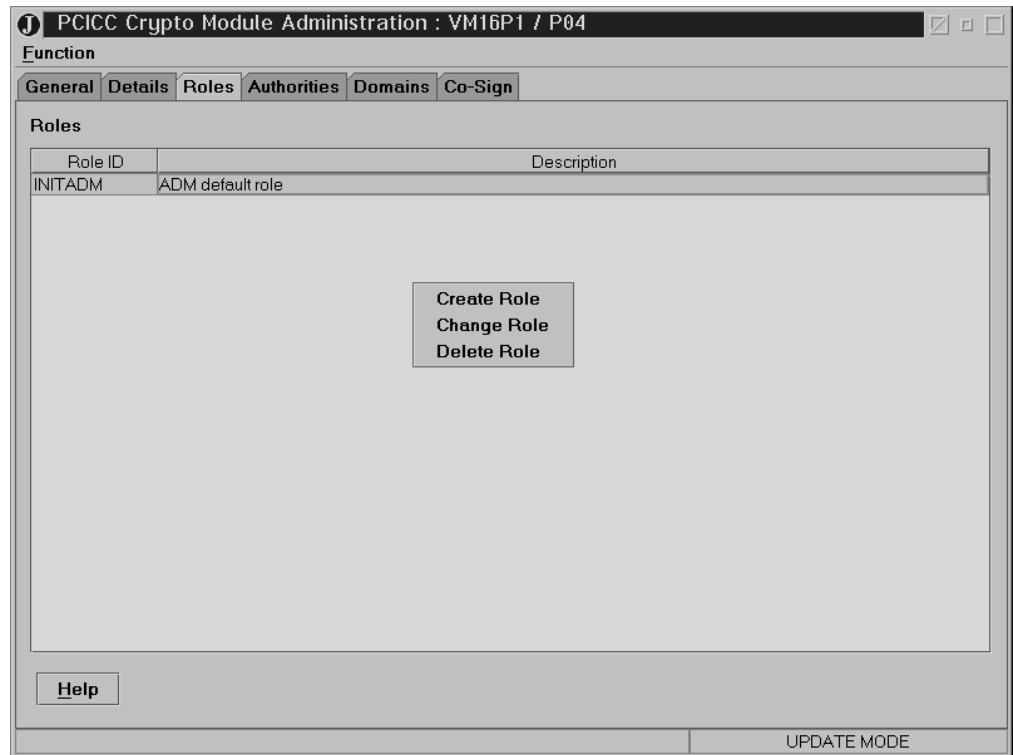


Figure 51. PCICC Roles Page - Create, Change or Delete a Role

The 'Create New Role' dialog box contains the following configuration options:

- Role ID:** [Text input field]
- Description:** [Text input field]
- Crypto Module Enable:**
 - ☐ Disable crypto card
 - ☐ Enable crypto card, issue
 - ☐ Enable crypto card, co-sign
- Access Control:**
 - ☐ Access control, issue
 - ☐ Access control, co-sign
- New Symmetric Master Key:**
 - ☐ Load first key part
 - ☐ Combine middle key parts
 - ☐ Combine final key part
 - ☐ Clear new master key register
- New Asymmetric Master Key:**
 - ☐ Load first key part
 - ☐ Combine middle key parts
 - ☐ Combine final key part
 - ☐ Clear new master key register
 - ☐ Set asymmetric master key
- Domain Zeroize:**
 - ☐ Zeroize domain, issue
 - ☐ Zeroize domain, co-sign
- Domain Controls:**
 - ☐ Domain controls change, issue
 - ☐ Domain controls change, co-sign
- Domain Access:**
 - 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
 - ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

At the bottom, there are buttons for 'Send updates', 'Cancel', and 'Help'. A 'Trusted Key Entry' button is located at the bottom right.

Figure 52. PCICC Create New Role Page

Figure 53. PCIXCC/CEX2C Create New Role Page

- **Role ID** — Enter the Role ID. If you are creating a new role you must fill in a name for that role. If you are changing a role, you cannot change this field.
- **Description** — Optional free text description.
- **Check Boxes** — Mark the boxes you require for the role. Choices must be made in these categories:
 - **Crypto Module Enable**
Choose if the role can disable the crypto card, issue the enable crypto card command, or co-sign the enable crypto card command.
 - **Access Control**
Choose if the role can issue the access control command or co-sign the access control command (needed for creating roles and profiles).
 - **New Symmetric Master Key**
Choose if the role can load the first key part, combine middle key parts, combine final key part and/or clear new master key registers.
 - **New Asymmetric Master Key**
Choose if the role can load the first key part, combine middle key parts, combine final key part, clear new master key registers and/or set the asymmetric master key.
 - **Domain Zeroize**
Choose if the role can issue a zeroize domain command or co-sign a zeroize domain command.
 - **Domain Controls**

Choose if the role can issue a domain controls change or co-sign a domain controls change (needed for administering access to ICSF panel services, access control points for ICSF callable services, and access to User Defined Extensions (UDX).

- Operational Key (PCIXCC/CEX2C only)

Choose if the role can load First and Additional key parts to key part registers, complete key part registers and clear key part registers.

- Domain Access

Choose the domains this role can access.

Press **Send Updates**. This is a dual-signature command and another authority may need to co-sign.

Deleting a Role

You can choose a crypto module and delete a role. TKE ensures that access to the crypto module is not lost when the role is deleted.

You must delete or reassign the user profile associated with a role before you delete the role.

Authorities

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.

TKE operates in exactly the same way with respect to authorities for CCF, PCICC and PCIXCC/CEX2C. However, CCF implements exactly sixteen predefined authorities while PCICC and PCIXCC/CEX2C allow a variable number of authorities.

Attention: Authorities 14 and 15 on CCF cannot be used for signing commands until their default signature keys have been changed. Either these authority signature keys must be changed or they should not be defined in the Signature Requirements Array as authorized or required to sign commands.

The purpose is to allow the user to:

- Generate a signature key for an authority and save it on a selected medium together with authority related information (name, telephone number etc).
- Upload the public part of the signature key and the authority information to the selected crypto module.
- Display and edit the authority-related information for the selected crypto module.

When you right-click in the Authorities container, you are given the opportunity to create, change or delete an authority, as well as generate a signature key. Creating and deleting authorities is only available for PCICC and PCIXCC/CEX2C crypto modules.

PCICC Crypto Module Administration : VM16P1 / P00

Functions

General **Details** **Roles** **Authorities** **Domains** **Co-Sign**

Authorities

Index	Name	Role	Phone	E-mail	Addr	Description
0		INITADM				
1	JSmith	keyrole1	555-1234	jsmith@e-mail	South Road, P...	This is JSmith's signature ...
2	MBrown	keyrole2	555-5555	mbrown@e-m...	Enterprise Dri...	This is MBrown's signatur...
3	RLewis	mr. zero	555-0000	rlewis@e-mail	5th Avenue, N...	RLewis is authorized to ze...

Help

UPDATE MODE

Figure 54. PCICC Authorities Page

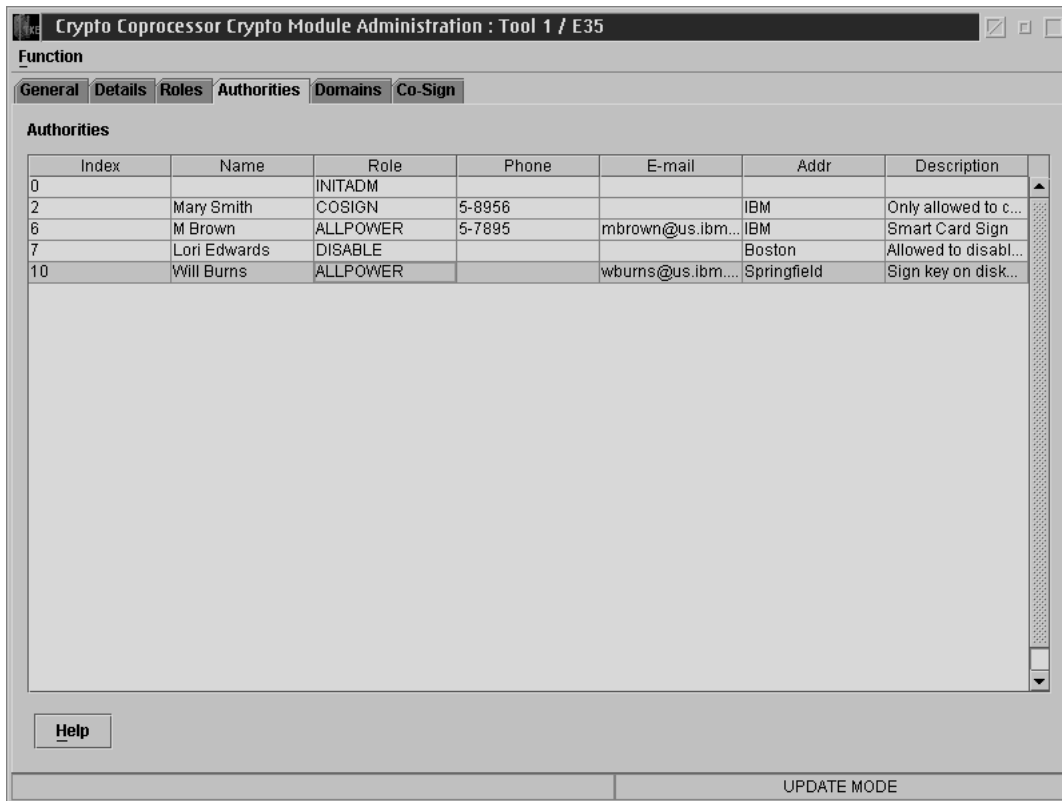


Figure 55. PCIXCC/CEX2C Authorities Page

Beginning with TKE 4.2, the representation for the PCIXCC and CEX2C crypto modules on the TKE panels will be Crypto Coprocessor.

Generating Authority Signature Keys

You generate and save a signature key by right-clicking in the Authorities container and selecting the *Generate signature key* action.

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 will be saved with the key and is called the default authority index.

Note: You can only load the signature key to a CCF module if the index is in the range 00–15. It is recommended that you use the same index across platforms and use only the first 16 indices for PCICC and PCIXCC/CEX2C.

2. 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 the **Continue** push button.



☒ **Generate Signature Key**

Authority index

Name

Phone

E-mail

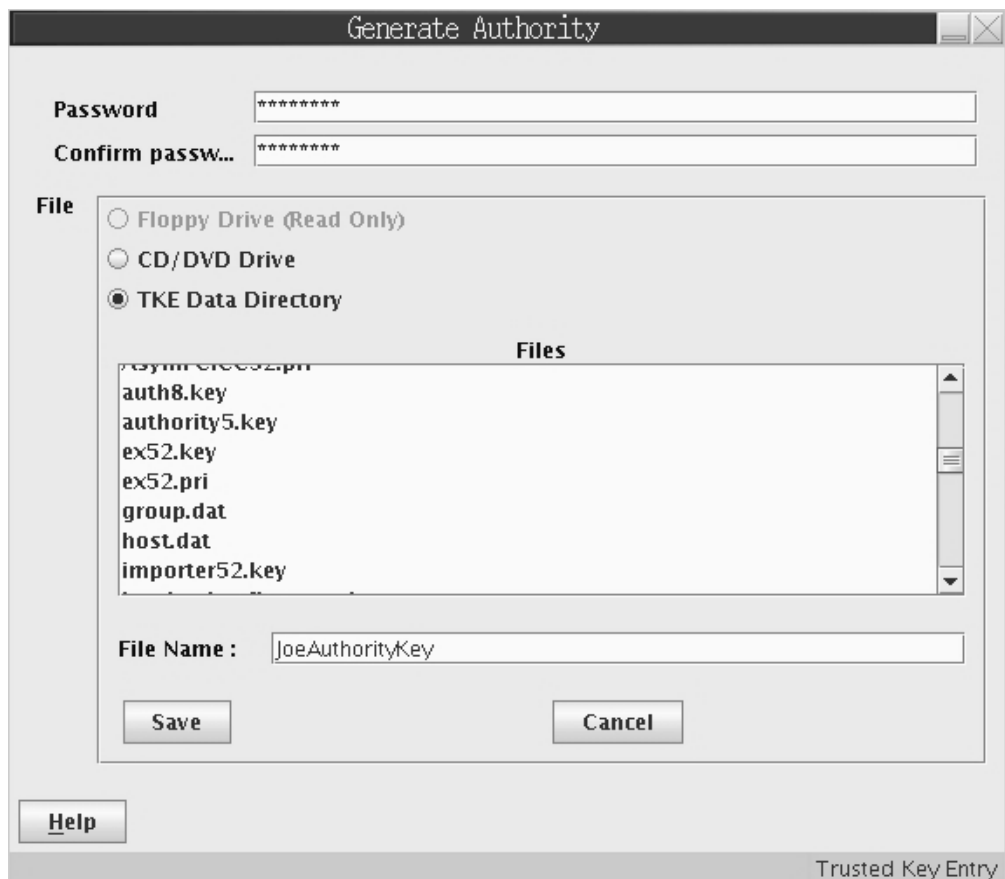
Address

Description

Trusted Key Entry

Figure 56. Filled In Generate Signature Key Window

3. When the key is generated, select the target destination. Signature keys can be saved to a **binary file, key storage, or TKE smart card**.



Generate Authority

Password

Confirm passw...

File

☐ Floppy Drive (Read Only)

☐ CD/DVD Drive

☒ TKE Data Directory

Files

symrcrc02.pri
auth8.key
authority5.key
ex52.key
ex52.pri
group.dat
host.dat
importer52.key

File Name :

Trusted Key Entry

Figure 57. Save Signature Key

4. If the keys are to be saved as a binary file on the hard drive, a password and file name are required to encrypt and save the key file. After saving 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.

Only one signature key can be stored in PKA key storage.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

5. If the keys are to be saved to a **TKE smart card**:
 - a. Select Target window is displayed after Generate Signature key window.



Figure 58. Select target window

- b. Insert the TKE smart card into smart card reader 2. Press **OK**.



Figure 59. Insert TKE smart card

- c. The user enters the PIN. When the authority signature key is saved to a TKE smart card it is protected by the PIN of the TKE smart card.

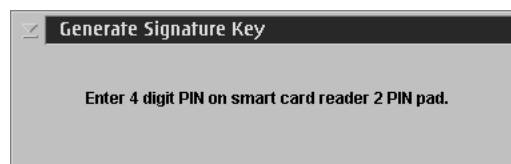


Figure 60. Enter PIN

- d. The Authority Signature Key is generated on the TKE smart card and a successful message is displayed.

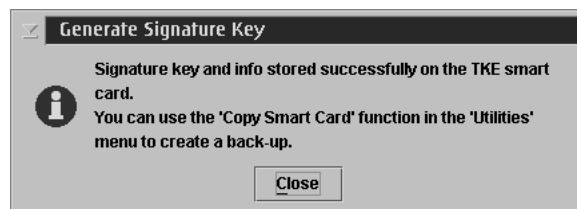


Figure 61. Generate signature key

- When saving an Authority Signature Key on a TKE smart card, the user is not given the option to save it again. The user should use the copy smart card contents utility to save the TKE authority key again. See “Copy smart cards” on page 75.

Each TKE smart card can hold only one authority signature key.

Create Authority (PCICC/PCIXCC/CEX2C)

This selection allows you to create an authority at the host and load the authority signature key public modulus. Before you can create a new authority, you need to generate a signature key (see “Generating Authority Signature Keys” on page 95) .

To create an authority, click with the right mouse button in the container on the Authorities page. Select the **Create Authority** action.

A series of windows open for you to specify the signature key source.

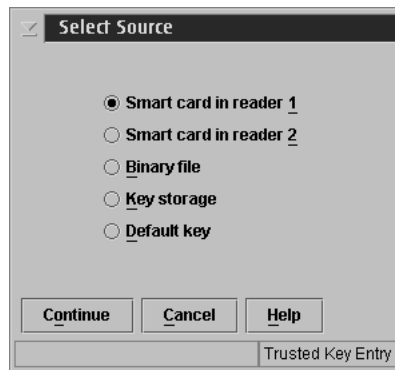


Figure 62. Select source of signature key

If you select **key storage**, the key and accompanying information you previously entered appears in the window.

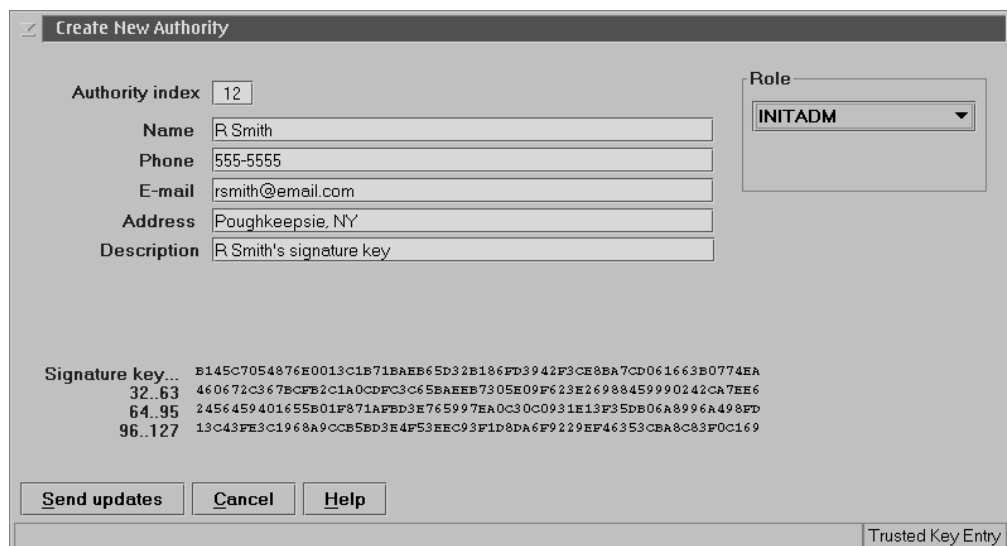


Figure 63. Create New Authority

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.



Figure 64. Insert TKE smart card

Then you are prompted to enter the TKE smart card PIN.

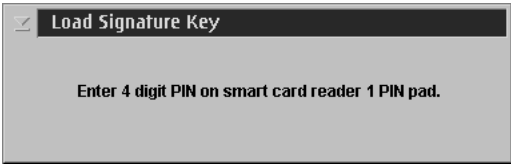


Figure 65. Enter PIN

Once the PIN has been verified, the Create New Authority window appears.

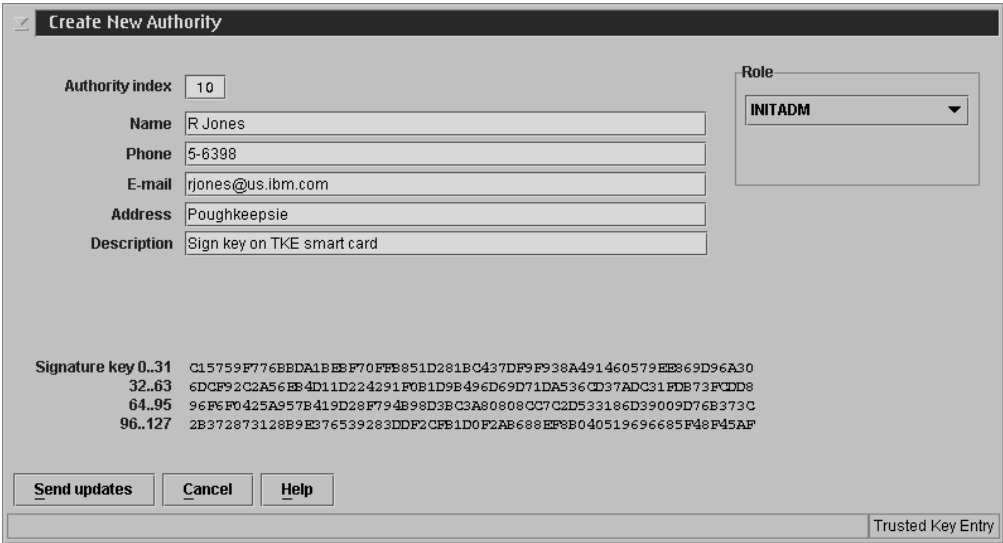


Figure 66. Create new authority

If you select **binary**, you are prompted for the signature key file to load and password before the Create New Authority window appears.

Warning: If the file is loaded from a floppy or CD/DVD, you must deactivate the floppy or CD/DVD drive before removing the diskette or disc. If the diskette is removed prior to deactivating the drive data could be lost or corrupted. For details on deactivating media see “Managing Media” on page 377.



Figure 67. Load Signature Key from binary file

If you select **default**, there is no information in the Create New Authority window. Also, there will not be any information if you did not provide any when you generated the key.

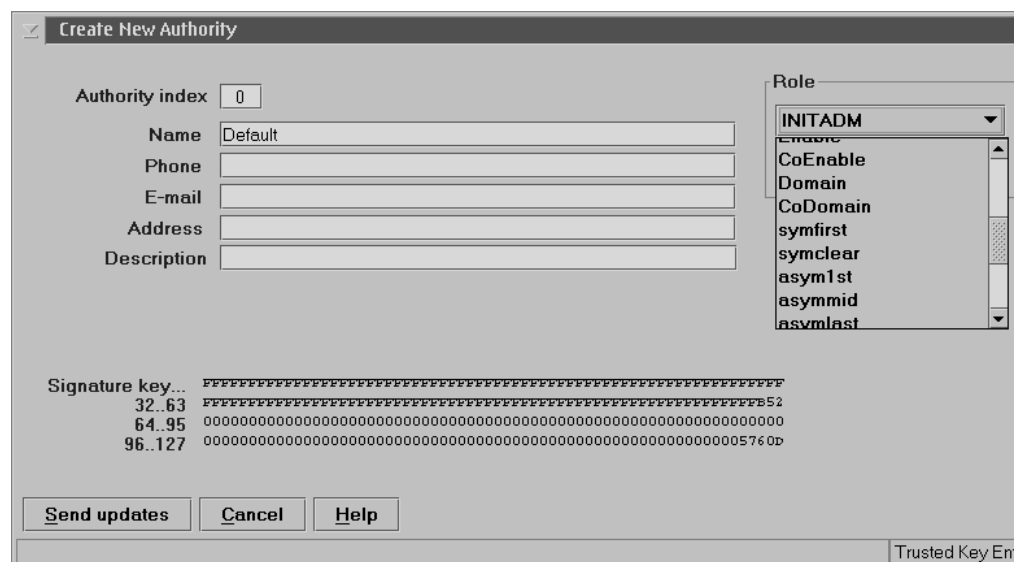


Figure 68. Create New Authority with Role Container

The Create New Authority window is opened with the authority information read from the signature key source:

- *Authority index* - This is a mandatory field with the index of the authority. Valid range is 00 through 99.

If the authorization public modulus is going to be loaded into 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* - Phone 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 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 PCICC/PCIXCC/CEX2C authority.

Press **Send updates**. This is a dual signature command and will require another authority to co-sign.

The authority information (name, phone, e-mail and address) is saved in the crypto module dataset specified in the TKE host transaction program started procedure on the host.

Change Authority

Activating this selection allows the user to change authority information and to replace the authority public modulus in the crypto module. All information except the authority index and authority TSN can be changed.

Attention: Authorities 14 and 15 on the CCF cannot be used for signing commands until their default signature keys have been changed. Either these authority signature keys must be changed or they should not be defined in the Signature Requirements Array as authorized or required to sign commands.

Change Authority

Authority index

Name

Phone

E-mail

Address

Description

Role

Domain

Authority TSN 3A586831C9EF780419C47A69021D000000100904

Signature key... 9DB400A1B89376EEAF09B3A8ABBE8AEA9B07D826C5EEBCED84FDA135165E2740

32..63 67A981DBFBCDF26D21C1FFF68BF35860EFA36546978252DB81053F6A50D2E8E0

64..95 A9E279D228620EA35A23A01E27A4CE93C9768D4DC635D1DE0CCA2C3795D472AD

96..127 74D07620BB9E985E5D299FA3D883BDE13AF6FA8237EE9B5C4B2ABA5E61743C1B

Trusted Key Entry

Figure 69. Change Authority (PCICC/PCIXCC/CEX2C)

When an authority is selected, you will be able to update the Name, Phone, E-mail and Address fields and the Authority Public Modulus. You can also change the Role definition by clicking on the pull-down menu and selecting a different role.

The **Get signature key** button opens a select source window and load signature window. The contents of the selected key file replace the contents of the Change Authority window except for the index.

The **Send updates** button 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 (PCICC and PCIXCC/CEX2C)

PCICC and PCIXCC/CEX2C operates with a variable number of TKE authorities (TKEAUTxx profiles). TKE allows a user to delete an authority from a PCICC or PCIXCC/CEX2C. 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.

Domains

The Domains page defines the domains that can have DES and PKA master keys and operational keys loaded and changed, as well as providing domains controls.

The Domains page holds general information about each domain. There are 16 tabs on the right hand side, one for each domain.

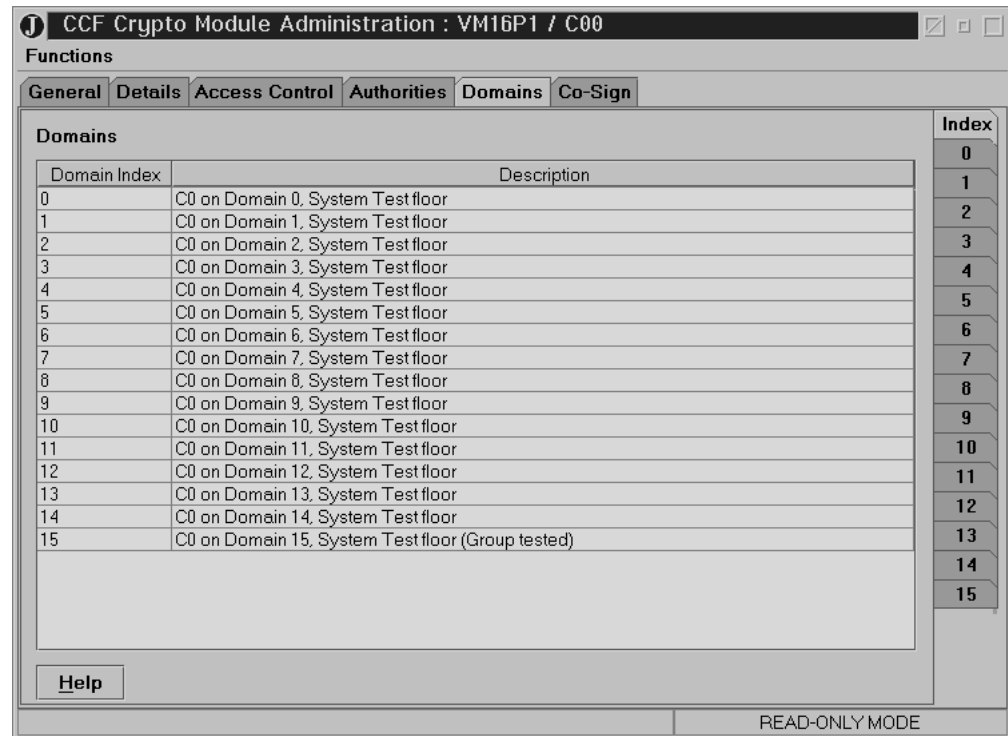


Figure 70. CCF Domains Page

Domains General Page

The Domains General page appears when you select a domain. Each domain has three associated pages: the General page, the Keys page and the Controls page.

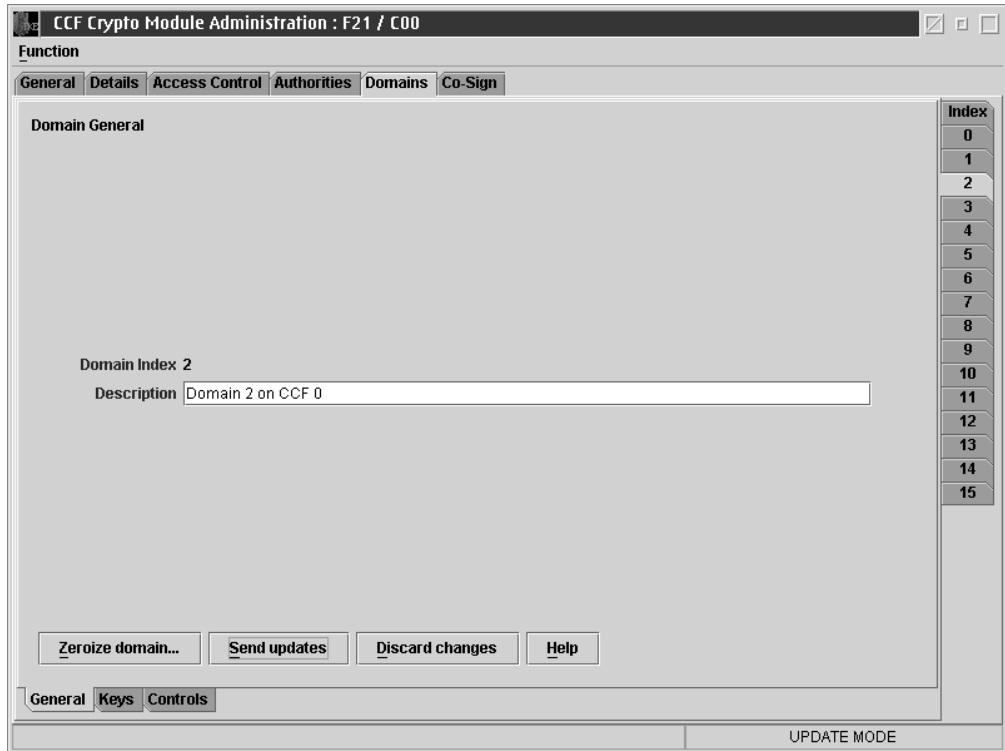


Figure 71. CCF Domains General Page

From this page, you can update the description and zeroize the domain.

To change the description, edit the entry field and press **Send updates**. The description is saved in the crypto module data set specified in the TKE host transaction program started procedure on the host.

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 informing the user that the initiated process is a destructive and irreversible process. Accepting this, the domain is zeroized. That is, all registers and keys related to this domain are set to zero or set invalid.

If you are reassigning a domain for another use, it is a good security practice to zeroize that domain before proceeding.

For CCF, once a domain has been zeroized, the cryptographic functions must be enabled from the Domains Controls page. After this has been done, DES master and PKA master keys can be loaded.

For a PCICC or PCIXCC/CEX2C, when a domain is zeroized, the domains controls are reset to their initial state whereby all services are enabled.

Note: Unlike the Global Zeroize issued from the Support Element, zeroize domain does not affect the enablement of TKE Commands on the PCIXCC/CEX2C. Refer to “TKE Enablement for z990, z890, z9 EC, z9 BC and System z10 EC Systems” on page 9.

Domain Keys Page - CCF

This page displays master key status information and allows you to generate, load and clear domain key registers.

The upper part of the window displays the status and hash patterns for the DES master key registers and for the PKA master key registers. The status and hash patterns of the entries in the key-part queue are displayed as well.

Select the key type you will be working with from the Key Type container.

These actions are available:

- **Generate:** Generate a key or key part and save it to a file or TKE smart card
- **Clear:** Clear (reset) the key register
- **Load:** Load a key or key part directly to the relevant key register
- **Load to Queue:** Load a key or key part to the key part queue
- **Load to Key Storage:** Load a key part to the TKE workstation DES key storage
- **Encipher RSA Key:** Encipher an unencrypted RSA key under an IMP-PKA key
- **Generate RSA Key:** Generate an RSA Key and encrypt it under an IMP-PKA key.
- **Load RSA Key to PKDS:** Load an RSA key to the PKDS active in the logical partition where the Host Transaction Program is started
- **Load RSA Key to Host Dataset:** Load an RSA key to a host data set
- **Secure key part entry:** Enter known key part values to a TKE smart card.

After you select a Key Type and right-click, a pop-up window appears with the available actions.

Note: The two TKE smart cards must be enrolled in the same zone; otherwise the copy will fail. To display the zone of a TKE smart card, exit from TKE and use either the Cryptographic Node Management Utility 3.10SC or the Smart Card Utility Program V 5.2 under the Trusted Key Entry Applications on the Framework. See “Crypto Node Management Batch Initialization 3.10SC” on page 327 or Appendix D, “Smart Card Utility Program (SCUP),” on page 285.

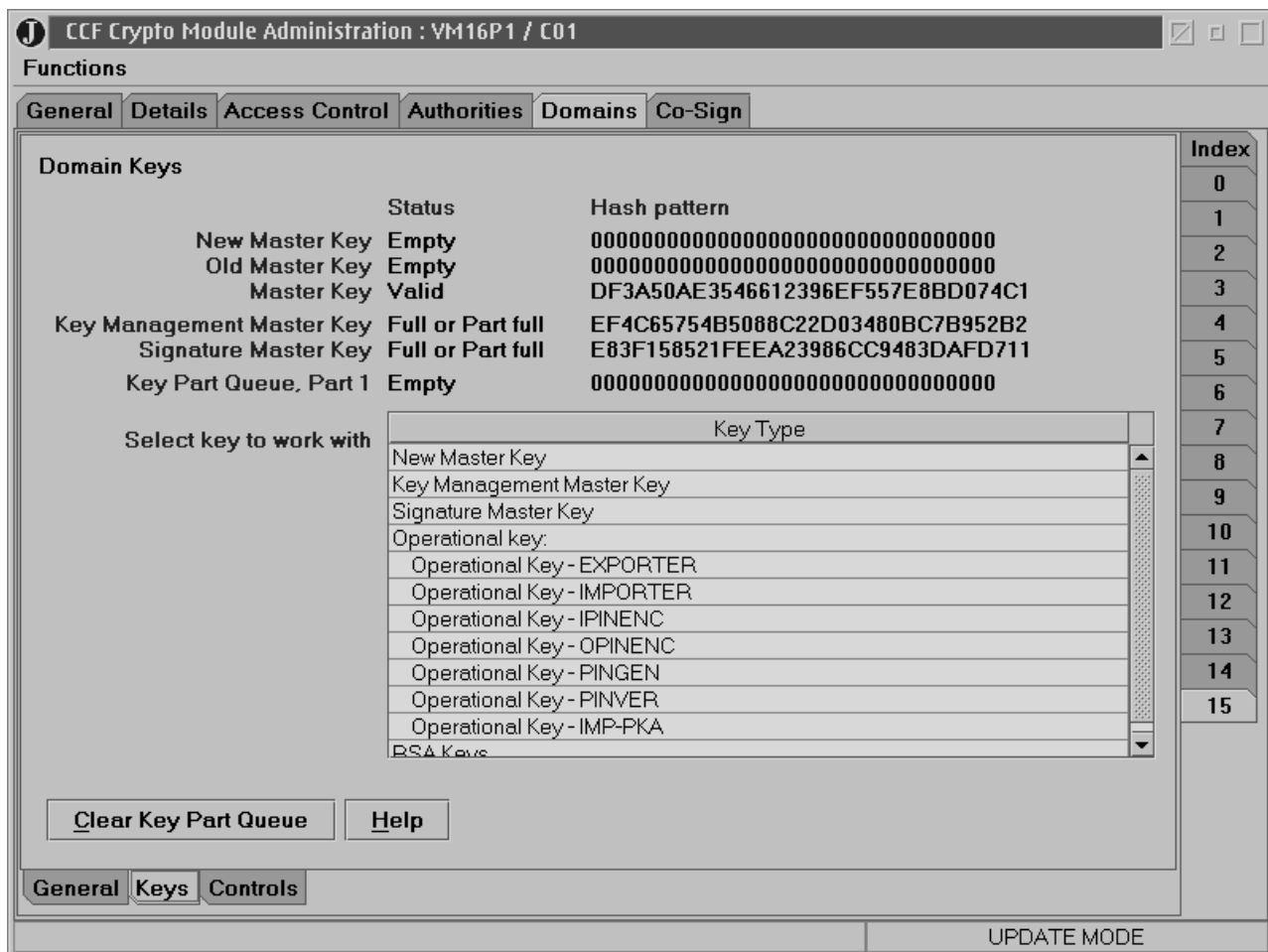


Figure 72. CCF Domains Keys Page

The key part queue permits new master key parts and operational key parts to be entered. To load keys from the key part queue and import them into the CCF crypto modules, ICSF panels must be used. See Chapter 7, “Managing Keys: TKE and ICSF with CCF,” on page 159. After each import from the ICSF panels, if you return to this page be sure to **refresh** the notebook. This will update the status of the key part queue, before you load another key part. **Refresh** is available from the Function drop-down menu.

To delete all entries in the key-part queue, press **Clear Key Part Queue**.

Not all actions are available for all key types. Table 3 on page 107 illustrates the possibilities:

Table 3. Key Types and Actions for CCF Crypto Modules

CCF			
Key Type	Popup	Sub-popup	Special Considerations
New Master Key	Generate		
	Load	First Intermediate Last Complete	Load is disabled if the New Master Key register is full. Load First and Load Complete require the register to be empty. Load Intermediate and Load Last require the register to be part full. Use Load Complete if loading only one key part.
	Load to queue	First Intermediate Last Complete	Load to queue is disabled if the queue is full. If loading just one key part, use load to queue complete. However, you must import two key parts from the key part queue from ICSF. The last key part is automatically set to zeros in the key part queue register.
	Secure key part entry		Enter known key part values to a TKE smart card; see Appendix E, "Secure Key Part Entry," on page 305.
Signature Master Key	Generate		
	Load	First Intermediate Last Complete	Load First and Load Complete require the Signature Master Key register to be empty. Load Intermediate and Load Last require the register to be part full. Use Load Complete if you are loading only one key part.
	Clear		
	Secure key part entry		Enter known key part values to a TKE smart card; see Appendix E, "Secure Key Part Entry," on page 305.
Key Management Master Key	Generate		
	Load	First Intermediate Last Complete	Load First and Load Complete require the Key Management Master Key register to be empty. Load Intermediate and Load Last require the register to be part full. Use Load Complete if you are loading only one key part.
	Clear		
	Secure key part entry		Enter known key part values to a TKE smart card; see Appendix E, "Secure Key Part Entry," on page 305.

Table 3. Key Types and Actions for CCF Crypto Modules (continued)

CCF			
Key Type	Popup	Sub-popup	Special Considerations
Operational Keys	Generate		
	Load to queue	First Intermediate Last	Load to queue is disabled if the queue is full.
	Load to key storage	First Intermediate Last	This function is only performed for Operational Key types IMPORTER or IMP-PKA.
	Secure key part entry		Enter known key part values to a TKE smart card; see Appendix E, "Secure Key Part Entry," on page 305.
RSA Key	Generate		
	Encipher		
	Load to PKDS		Loads RSA key to TKE host LPAR only.
	Load to data set		The host dataset must be preallocated.

Note: The LOAD, LOAD TO QUEUE, and CLEAR are not possible if domain change is disabled.

Operational keys are keys that are loaded to a CCF crypto module and then encrypted with the master key. The TKE workstation can be used for entry of these operational key types:

- EXPORTER
- IMPORTER
- IPINENC
- OPINENC
- PINGEN
- PINVER
- IMP-PKA

The operational keys are always loaded as key parts through the key-part queue. After each key part is loaded to queue, the key part must be imported to the CKDS using host ICSF panels. See "Loading and Importing Operational Keys" on page 184.

Generate - CCF

When you select **Generate**, a window opens whereby you specify the target.

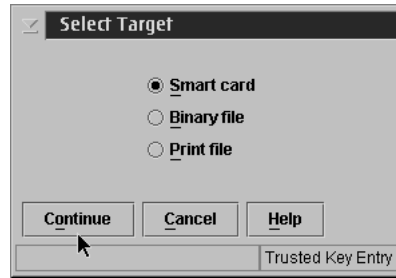


Figure 73. Select Target

Next, save the key part.

Note: If the key part is saved to a TKE smart card it cannot be saved to any other medium such as binary file or print file. If saving the key part to a binary or print file, specify either CD/DVD Drive or TKE Data Directory and the file name. With either the binary or print file option, you can save the key part to another medium, except a TKE smart card.

Note: The TKE cryptographic adapter generates the key part and securely transfers the key to the TKE smart card. You must insert a TKE smart card that is enrolled in the same zone as the TKE cryptographic adapter; otherwise the Generate will fail. To display the zone of a TKE smart card, exit from TKE and use either the Cryptographic Node Management Utility 3.10SC or the Smart Card Utility Program 5.2 under Trusted Key Entry Applications. See “Display smart card details” on page 276 or “Display smart card information” on page 291.

If you are saving to a TKE smart card, these screens appear:



Figure 74. Save key part to TKE smart card

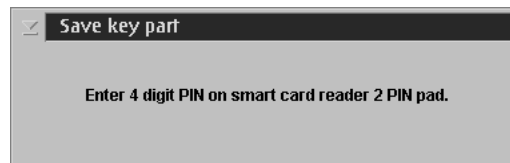


Figure 75. Enter PIN

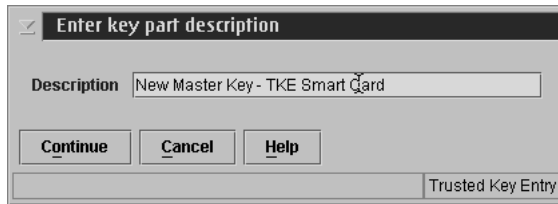


Figure 76. Enter key part description



Figure 77. Key part saved successfully

The save key part successful message appears. If you want to create a backup, see “Copy smart cards” on page 75.

Clear - CCF

Clear is only available for the SMK and KMMK. If a register is not empty or if you make a mistake during key entry, you can select **Clear**, and this window opens:

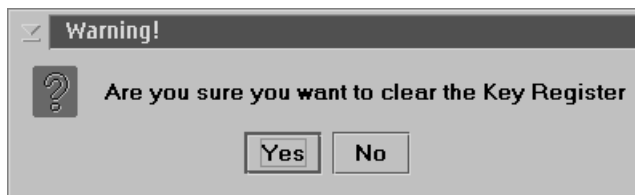


Figure 78. Clear Key Warning Message

If you press **Yes**, the command executes successfully message appears.

Load and Load to Queue - CCF

Load is available for all master keys. Load directly loads the key part to the key register. It can be used when loading DES master keys the first time (see “First-Time Startup” on page 160), but is not recommended subsequent times.

Load to Queue is only available for loading New Master Key parts or operational key parts. After successfully loading a key part to the key part queue, you must go to your TSO session and use the ICSF panels to import the key part from the key part queue to the New Master Key register or the operational key part into the CKDS. This must be done for each key part loaded to the queue from TKE. See Chapter 7, “Managing Keys: TKE and ICSF with CCF,” on page 159.

Warning

When entering a DES master key part, Load should only be selected if ICSF is NOT active in the selected domain. If ICSF is active in the target domain, Load to Queue should be used to prevent possible corruption of the CKDS or overlay of the key in the auxiliary master key register in the current domain or another domain.

Having selected **Load** or **Load to Queue**, a new menu pops up giving the user the ability to select the key part to load:

- First
- Intermediate
- Last
- Complete

You can input domain keys from the keyboard, a binary file or a TKE smart card..

Input from Keyboard:

A dialog box is displayed for selecting the input source.

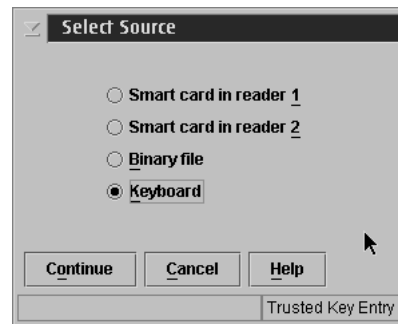


Figure 79. Select CCF key source - keyboard

If keyboard is selected as the input source an input dialog box is displayed with input fields for either a 16-byte key or a 24-byte key depending on the key type. The dialog box displayed for entering the key values depends on the installation's Blind Key Entry selection. Blind Key Entry masks the key values being entered. If your installation is using Blind Key Entry, this dialog box is displayed for entering the key values:

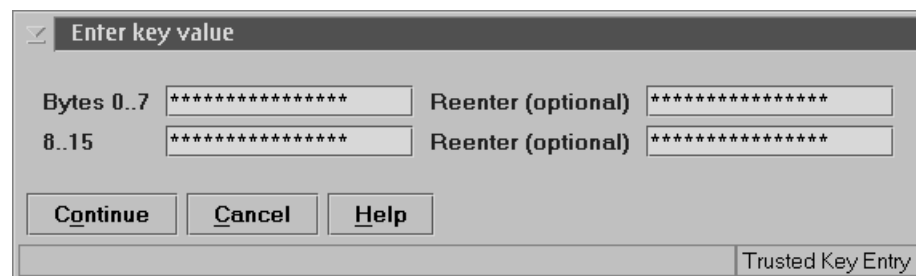


Figure 80. Enter Key Value - Blind Key Entry

An optional confirmation field can be used to confirm the key value entered.

For information on how to change the Blind Key Entry option, see “TKE Customization” on page 76.

If Blind Key Entry is not being used, this dialog box is displayed:



Figure 81. Enter Key Value

When the user presses **Continue**, the MDC-4 and ENC-ZERO is calculated and displayed, providing the user with the opportunity to visually verify the values. When Load Key is pressed, the user is asked if they would like to save the key part. If yes, a file chooser window is opened for the user to select either CD/DVD drive or TKE Data Directory and enter a File Name for saving the key part. The key part is then loaded. If no, the key part is not saved and the key is loaded.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

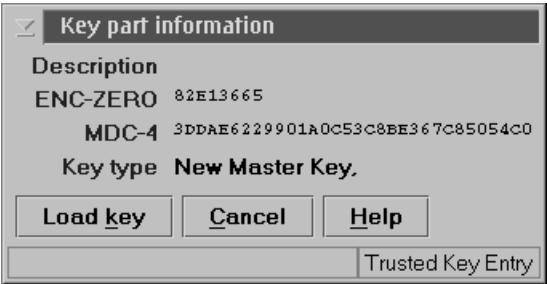


Figure 82. Key Part Information Window

If loading to queue, the key part is loaded to the key part queue on the CCF crypto module. You must go to your TSO session and import the key part from the key part queue to the New Master Key register or the CKDS. To import an NMK key part to the New Master Key register, see “Importing Key Parts from the Queue” on page 163. To import an operational key part to the CKDS, see “Loading and Importing Operational Keys” on page 184.

If loading directly and if you have not loaded the entire key, return to the Domains Keys page, refresh the notebook, and continue.

Input from Binary File:

A dialog box is displayed for selecting the input source.

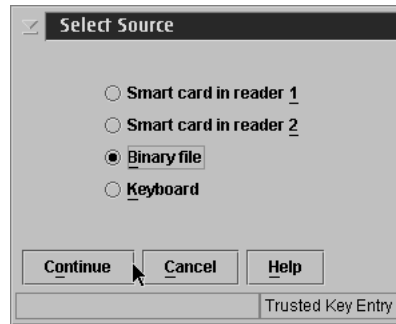


Figure 83. Select CCF key source - binary file



Figure 84. Specify Key File

Specify the file location (Floppy, CD/DVD Drive or TKE Data Directory) and file name. Select **Open**.

Warning: If the file is loaded from a floppy or CD/DVD, you must deactivate the floppy or CD/DVD drive before removing the diskette or disc. If the diskette is removed prior to deactivating the drive data could be lost or corrupted. For details on deactivating media see “Managing Media” on page 377.

The MDC-4 is calculated and displayed, providing the user with the opportunity to visually verify the MDC-4 value. The Encipher Zero VP (ENC-ZERO) is also

displayed for verification (DES master key parts and operational key parts).

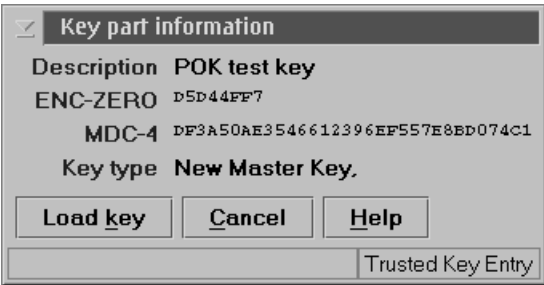


Figure 85. Key Part Information Window

Press **Load key**.

If loading directly and if you have not loaded the entire key, return to the Domains Keys page, refresh the notebook, and continue.

Input from Smart Card:

1. A dialog box is displayed for selecting the input source.

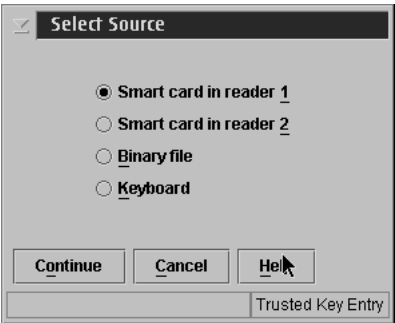


Figure 86. Select CCF key source - smart card

2. Insert the TKE smart card into the reader, highlight a key part, right click and choose select, or highlight and press OK.

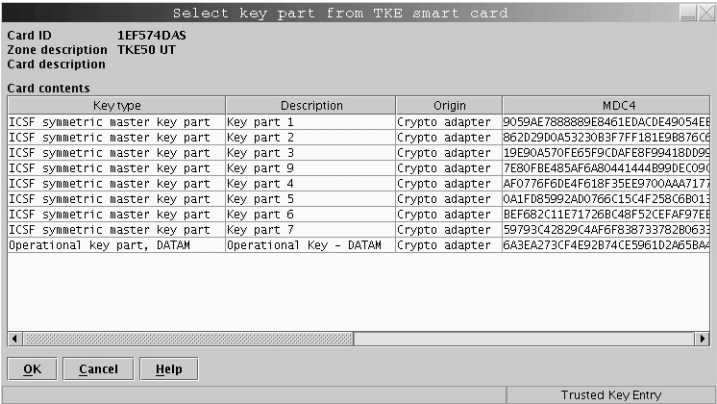


Figure 87. Select a key part

3. Enter PIN.

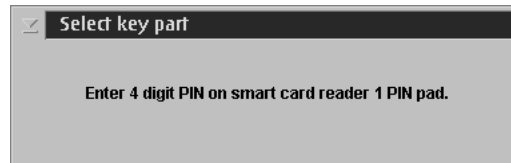


Figure 88. Enter PIN

4. The key part is read from the TKE smart card. Press Load Key.



Figure 89. Load key

5. You will get a message that the command was executed successfully.

Load or Load to Queue Complete - CCF

Use Load Complete or Load to Queue Complete if you have only one master key part. Load complete loads a complete key to the new master key register in a single load operation. The register status is full after a load complete.

Load to queue complete is only valid for loading a new DES master key to the CCF. Load to queue complete loads a key part to the key part queue. After you import the first key part, the key part on the key part queue is automatically set to zeros. You must import the final key part of zeros to the new master key register. The process is:

- Select Complete from Load to Queue pop-up menu (TKE workstation)
- Import first key part from the key part queue to the NMK register (ICSF panels)
- Import final key part from the key part queue to the NMK register (ICSF panels)

Load to Key Storage - CCF

This selection is only possible for operational IMP-PKA or IMPORTER keys. The IMP-PKA key-encrypting keys are used to protect RSA keys during transport from the workstation to ICSF whereas the IMPORTER keys are used to protect DES keys during transport from the workstation to ICSF. Having selected Load to Key Storage, the user selects which key part 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 use 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.

☒ **Install IMPORTER key part in TKE workstation key storage**

A host IMPORTER key is installed in the TKE workstation key storage as an EXPORTER key.

EXPORTER keys in TKE workstation key storage.

Key label
IMPPKA.RSA.KEYGEN.KNOWN.KEY.VALUE
IMPPKA.RSA.KEYENC.KNOWN.KEY.VALUE
MIGRATE.IMPORTER.KEY

Workstation key label

Trusted Key Entry

Figure 90. Install Importer Key Part in Key Storage

For IMP-PKA keys, you must specify additional information.

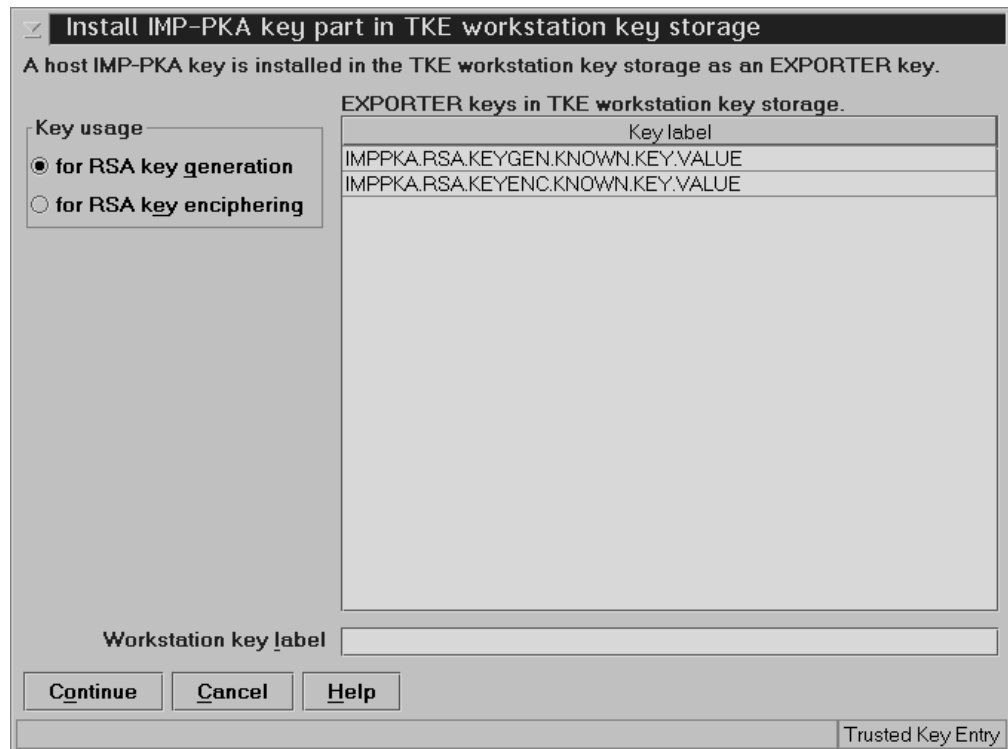


Figure 91. Install IMP-PKA Key Part in Key Storage

A window is displayed for the user to specify the workstation key label and whether this IMP-PKA KEK will be used for protecting an RSA key to be generated at the workstation or a clear RSA key to be enciphered at the workstation.

Note: For the RSA key to be loaded into the PKDS, the same IMP-PKA key value must be stored in the CKDS. If a non-odd parity key is generated, when it is loaded to key storage its parity is adjusted. However, that same non-odd parity key is sent to the MVS host system (using Load to Queue) without the parity adjusted.

Secure Key Part Entry

To save known key part values to a TKE Smart Card use secure key part entry. Refer to Appendix E, "Secure Key Part Entry," on page 305 for details on using this function.

Generate RSA Key - CCF

This selection initiates RSA key generation at the workstation. The key is protected with a previously generated IMP-PKA key encrypting key and saved in a file.

From the Domains Keys page, right-click on RSA key in the Key Types container and select Generate. The Generate RSA Key window is displayed.

Figure 92. Generate RSA Key

Specify this 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. All values from 512 to 1024 are valid. If the entered value exceeds the maximum value set by the selected crypto module an error Invalid key length specified. It must be between 512 and 1024 is displayed. You are allowed to continue but the generated RSA key cannot be loaded to this crypto module.
- *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 IMP-PKA label* — The container displays the labels of the key-encrypting keys currently in the TKE workstation key storage available for protecting RSA keys generated at a TKE workstation. Select one by clicking on it.
- *Host IMP-PKA key label* — The label of the host used to import the RSA key. The selected Workstation IMP-PKA 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 file chooser window is displayed for the user to specify the file location (CD/DVD Drive or TKE Data Directory) and file name for saving the generated RSA key.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

Encipher RSA Key - CCF

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 I, “Clear RSA Key Format,” on page 325.

Having selected the Encipher action, the Encipher RSA Key window is displayed:

☒ **Encipher RSA key**

RSA key usage control

☒ **Signature**

☐ **Key management & signature**

Key length

☐ 512

☐ 768

☐ 1024

☒ 799

Public exponent

☐ 3

☒ 65537

☐ Random

PKDS key label RSA799.key

Private key name RSA799.key

Description RSA 799 kvs

Workstation EXPORTER key label

Key label
IMPPKA.RSA.KEYENC.KNOWN.KEY.VALUE

Host IMP-PKA key label YM16P1.IMPPKA.RSA.KEYENC.KNOWN.KEY.VALUE

Encipher **Cancel** **Help**

Trusted Key Entry

Figure 93. Encipher RSA Key

Specify this 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 EXPORTER key label* — The container displays the labels of the key-encrypting keys currently in the TKE workstation key storage available for protecting RSA keys entered from a clear key file. Select one by clicking on it.
- *Host IMP-PKA key label* — The label of the host used to import the RSA key. The selected Workstation IMP-PKA 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 user presses **Encipher**, a file chooser window is displayed for the user to specify the file location (CD/DVD drive or TKE Data Directory) and file name for saving the encrypted RSA key.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

Load RSA Key to PKDS - CCF

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 LPAR. For loading RSA keys to TKE target LPARs, see “Load RSA Key to Host Dataset - CCF” on page 121.

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 94. Load RSA Key to PKDS

Specify this 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 EXPORTER key label* — Label of the workstation IMP-PKA that is used for protecting the RSA key.

- *Host IMP-PKA key label* — Label of the IMP-PKA key stored in the host CKDS that will be used to import the RSA key. Change this field as needed.

Load RSA Key to Host Dataset - CCF

This selection allows the user to load an RSA key to a host data set as an external key token. From this dataset it is possible to install the key in the PKDS by means of TSO ICSF panels.

The host dataset must be defined in advance with these attributes: recfm fixed, lrecl=1500, partitioned. Using this installation method, it is possible to load RSA keys into any PKDS in any LPAR. For information on the TSO ICSF interface, see “Installing RSA Keys in the PKDS from a Dataset” on page 193.

The steps are the same as for loading an RSA key to the PKDS (see “Load RSA Key to PKDS - CCF” on page 120), except that the user has to specify the full dataset and member name. If you don’t specify the dataset and member name in quotes, the high level qualifier for the dataset is the TSO logon of the administrator/host user ID.

Figure 95. Load RSA Key to Dataset

Domains Keys Page (PCICC and PCIXCC/CEX2C)

This page displays master key status information and allows you to generate, load, set and clear domain key registers.

The upper part of the window displays the status and hash patterns for the new symmetric master key registers and for the new asymmetric master key registers.

If you have implemented smart card support, make sure that the cryptographic adapter in the TKE workstation and the TKE smart cards are in the same zone. To display the zone of a TKE smart card, exit from TKE and use either the Cryptographic Node Management Utility 3.10SC or the Smart Card Utility Program 5.2 under Trusted Key Entry Applications. See “Display smart card details” on page 276 or Appendix D, “Smart Card Utility Program (SCUP),” on page 285.

Select the key type you will be working with from the Key Type container. These actions are available:

- **Generate:** Generate a key part and save to a file or TKE smart card
- **Clear:** Clear (reset) the key register or key part register
- **Load:** Load a key part directly to the relevant new master key register

- **Set:** Sets the new asymmetric master key. That is, the current ASYM-MK is transferred to the old ASYM-MK register, and the new ASYM-MK register is transferred to the current ASYM-MK register. The new ASYM-MK register is reset to zeros.
- **Generate RSA Key:** Generate an RSA Key and encrypt it under an IMP-PKA key.
- **Encipher RSA Key:** Encipher an unencrypted RSA key under an IMP-PKA key
- **Load RSA Key to PKDS:** Load an RSA key to the PKDS active in the logical partition where the Host Transaction Program is started
- **Load RSA Key to Host Dataset:** Load an RSA key to a host data set
- **Load to Key Storage:** Load a key part to the TKE workstation DES key storage
- **Load to Key Part Register:** Load/accumulate operational key parts in a key part register
- **View:** View key part register information
- **Secure key part entry:** Enter known key part values to a TKE smart card.

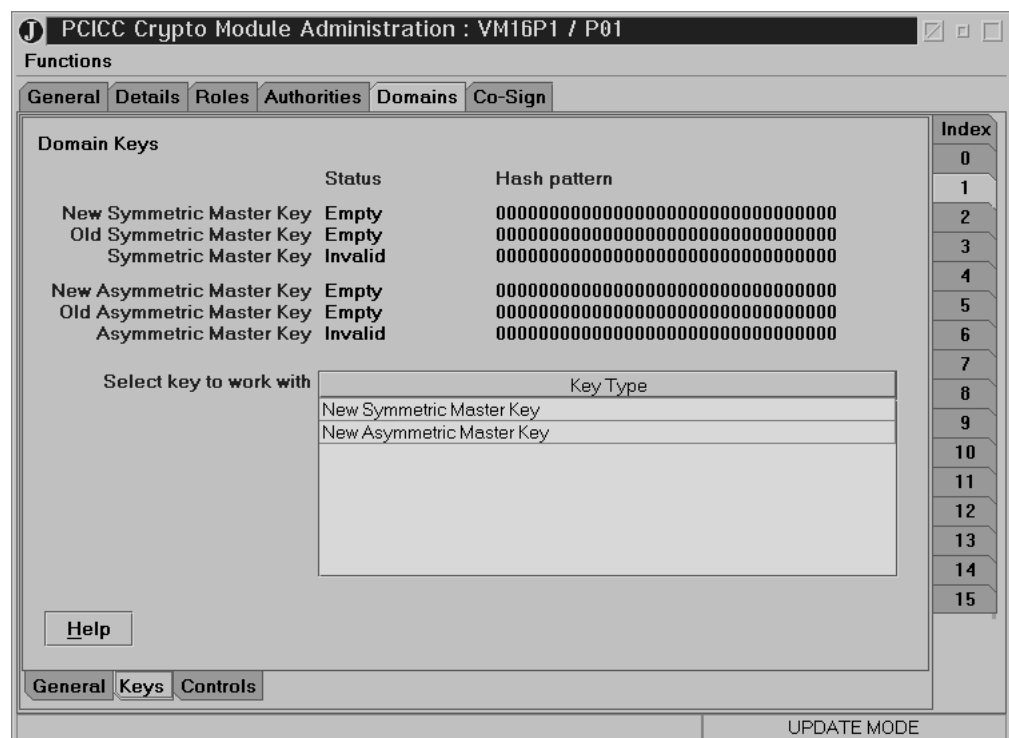


Figure 96. PCICC Domains Keys Page

Not all actions are available for all key types. Table 4 on page 123 illustrates the possibilities for the PCICC and Table 5 on page 124 illustrates the possibilities for the PCIXCC/CEX2C:

Table 4. Key Types and Actions for PCICC Crypto Modules

PCICC			
Key Type	Popup	Sub-popup	Special Considerations
New symmetric MK	Generate		
	Load	First Intermediate Last	Load First requires the register to be empty. Load Intermediate and Last require the register to be part full.
	Clear		
	Secure key part entry		Enter known key part values to a TKE smart card; see Appendix E, "Secure Key Part Entry," on page 305.
New Asymmetric MK	Generate		
	Load	First Intermediate Last	Load First requires the register to be empty. Load Intermediate and Last require the register to be part full.
	Set		
	Clear		
	Secure key part entry		Enter known key part values to a TKE smart card; see Appendix E, "Secure Key Part Entry," on page 305.

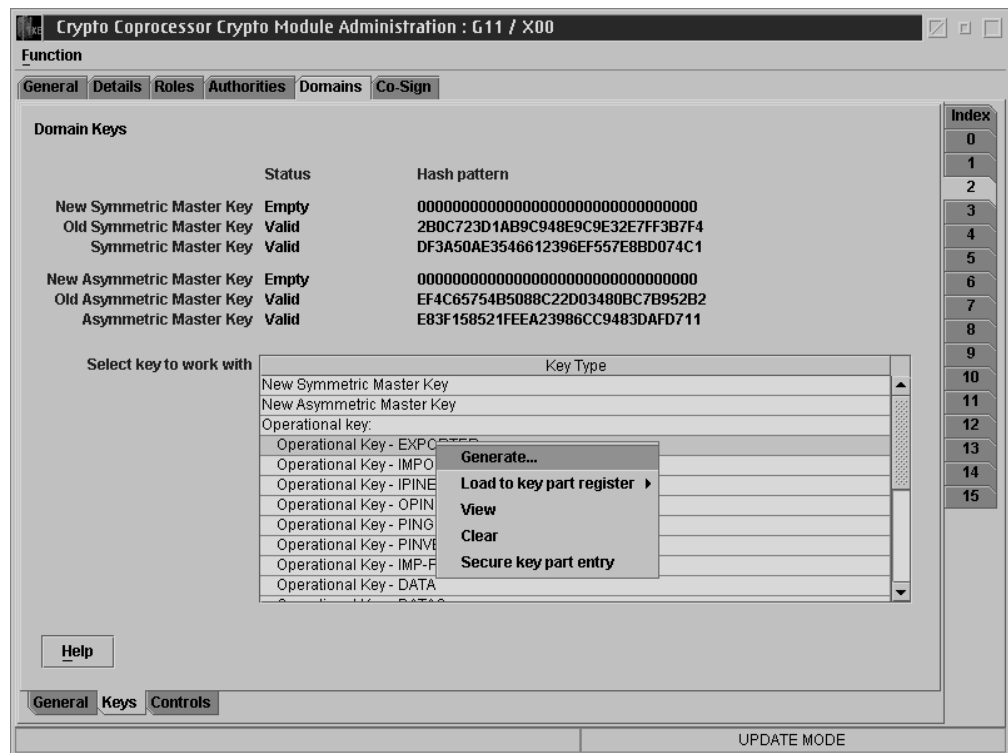


Figure 97. PCIXCC/CEX2C Domains Keys Page

Table 5. Key Types and Actions for PCIXCC/CEX2C Crypto Modules

PCIXCC			
Key Type	Popup	Sub-popup	Special Considerations
New symmetric MK	Generate		
	Load	First Intermediate Last	Load First requires the register to be empty. Load Intermediate and Last require the register to be part full.
	Clear		
	Secure key part entry		Enter known key part values to a TKE smart card; see Appendix E, "Secure Key Part Entry," on page 305.
Operational Keys	Generate		
	Load to Key Storage	First Intermediate Last	This function is only performed for operational key types IMPORTER or IMP-PKA.
	Load to Key Part register	First Add part Complete	Load First requires the key part register label to be unique. Load Add part requires a First key part loaded for the key type selected. Load Complete requires the key part register to be in the intermediate state for the key type selected.
	View		
	Clear		
	Secure key part entry		Enter known key part values to a TKE smart card; see Appendix E, "Secure Key Part Entry," on page 305.
RSA Keys	Generate...		
	Encipher		
	Load to PKDS...		
	Load to dataset		
New Asymmetric MK	Generate		
	Load	First Intermediate Last	Load First requires the register to be empty. Load Intermediate and Last require the register to be part full.
	Set		
	Clear		
	Secure key part entry		Enter known key part values to a TKE smart card; see Appendix E, "Secure Key Part Entry," on page 305.

Generate New Symmetric Master Key and New Asymmetric Master Key for PCICC/PCIXCC/CEX2C

When you select **Generate**, a window opens whereby you specify the target.

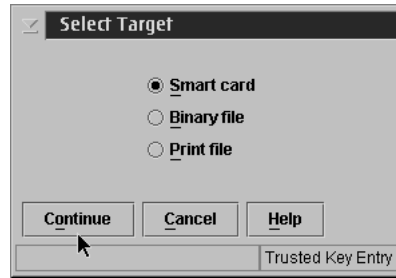


Figure 98. Select Target

Select the target: TKE smart card, binary or print file. Save the key part. If saving the key part to a binary or print file, specify the file path. to If saving the key part to a binary or print file, specify either CD/DVD Drive or TKE Data Directory and the file name.

If you are saving to a TKE smart card, these screens appear:

Note: If you have implemented smart card support, make sure that the TKE cryptographic adapter in the TKE workstation 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 3.10SC or the Smart Card Utility Program 5.2 under Trusted Key Entry Applications. See “Display smart card details” on page 276 or “Display smart card information” on page 291.

If saving the key part to a TKE smart card, it can not be saved to any other medium such as a binary or print file.



Figure 99. Save key part to smart card

After you insert the TKE smart card - press OK. Then enter the PIN onto the smart card reader PIN pad.

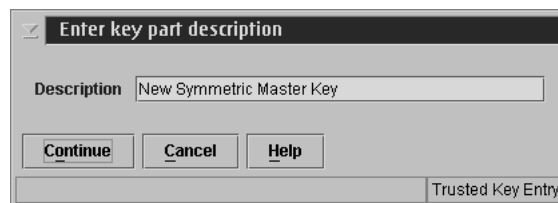


Figure 100. Enter key part description

Enter a description for the key part.

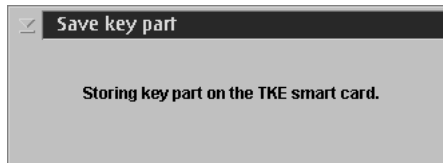


Figure 101. Save key part



Figure 102. Save key part success message

Load - PCICC/PCIXCC/CEX2C

Having selected **Load**, a new menu pops up giving the user the possibility to select which key part to load:

- First
- Intermediate
- Last

Input from Keyboard:

A dialog box is displayed for selecting the input source.

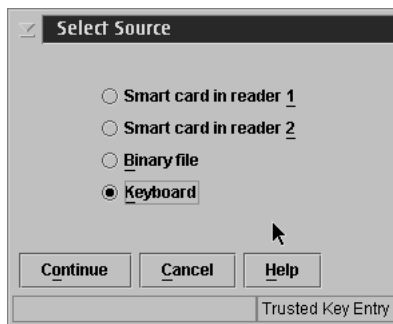


Figure 103. Select PCICC/PCIXCC/CEX2C key source - keyboard

If keyboard is selected as the input source an input dialog box is displayed with input fields for either a 16-byte key or a 24-byte key depending on the key type. The dialog box displayed for entering the key values depends on the installation's Blind Key Entry selection. Blind Key Entry masks the key values being entered. If your installation is using Blind Key Entry, this dialog box is displayed for entering the key values:

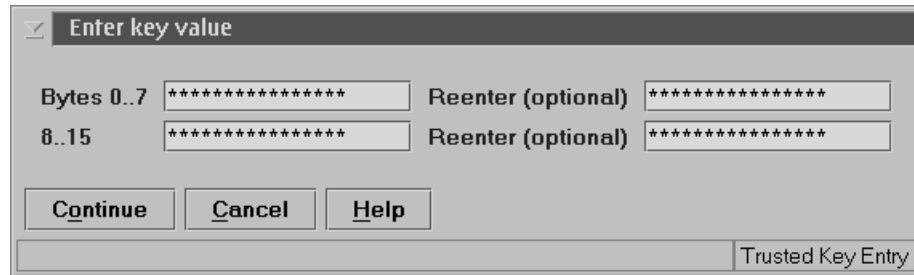


Figure 104. Enter Key Value - Blind Key Entry

An optional confirmation field can be used to confirm the key value entered.

For more information on how to change the Blind Key Entry option, see “TKE Customization” on page 76.

If Blind Key Entry is not being used, this dialog box is used:

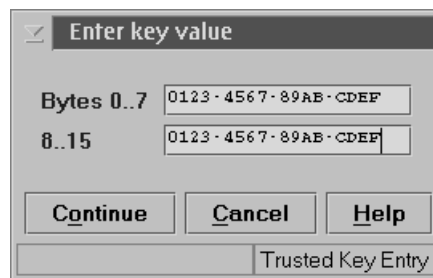


Figure 105. Enter Key

When the user presses **Continue**, the MDC-4 and the Encipher Zero VP (ENC-ZERO) are calculated and displayed, providing the user with the opportunity to visually verify the MDC-4 and ENC-ZERO values. When Load key is pressed the user is asked if they would like to save the key part. If yes, a file chooser window is opened for the use to specify the file location (CD/DVD drive or TKE Data Directory) and file name for saving the key part. Then the key part is Loaded. If no, the key part is not saved and the key part is loaded.

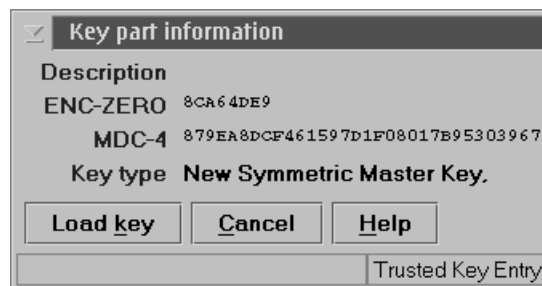


Figure 106. Key Part Information Window

Press **Load key**.

Input from Binary File:

A dialog box is displayed for selecting the input source.

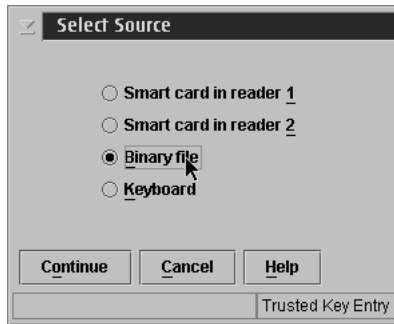


Figure 107. Select PCICC/PCIXCC/CEX2C key source - binary file



Figure 108. Specify Key File

Specify the file location (Floppy, CD/DVD Drive or TKE Data Directory) and file name. Select **Open**.

The MDC-4 is calculated and displayed, providing the user with the opportunity to visually verify the MDC-4 value.

Warning: If the file is loaded from a floppy or CD/DVD, you must deactivate the floppy or CD/DVD drive before removing the diskette or disc. If the diskette is removed prior to deactivating the drive data could be lost or corrupted. For details on deactivating media see “Managing Media” on page 377.

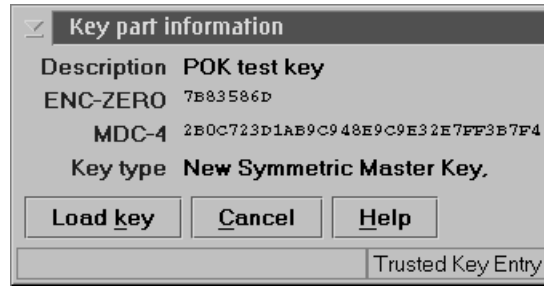


Figure 109. Key Part Information Window

Press **Load key**.

Input from TKE Smart Card:

Follow these steps:

1. A dialog box is displayed for selecting the input source.

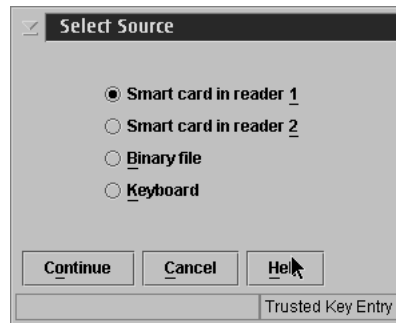


Figure 110. Select PICC/PCIXCC/CEX2C key source - smart card

Press **Continue**.

2. Insert the TKE smart card into the appropriate reader. Ensure the TKE smart card is enrolled in the same zone as the TKE cryptographic adapter; otherwise, the **Load** will fail.

Note: To display the zone of a TKE smart card, exit from TKE and use either the Cryptographic Node Management Utility 3.10SC or the Smart Card Utility Program 5.2 under Trusted Key Entry Applications. See “Display smart card details” on page 276 or “Display smart card information” on page 291.

3. The smart card contents are read and this window appears:

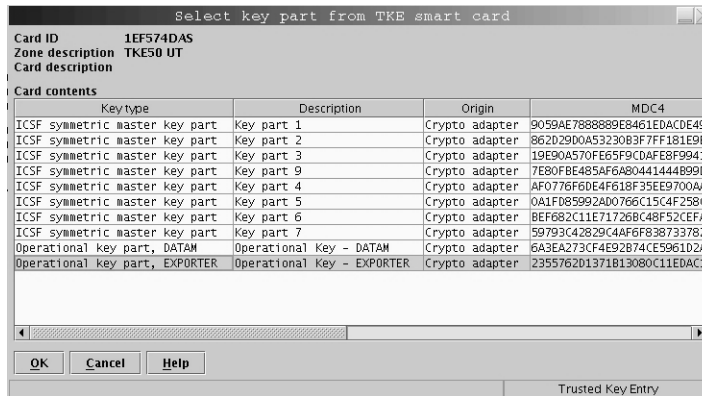


Figure 111. Select key part from TKE smart card

4. Highlight key part to load.
5. Click **OK**.
6. Enter the PIN on the smart card reader PIN pad when prompted.
7. The MDC-4 is calculated and displayed, providing the user with the opportunity to visually verify the MDC-4 value. The Encipher Zero VP (ENC-ZERO) of the new symmetric or asymmetric master key part is also displayed for verification.
8. Press Load key.
9. You will get a message that the command was executed successfully.

Clear - PCICC/PCIXCC/CEX2C

If a register is not empty or if you make a mistake during key entry, you can select **Clear**, and this window opens:

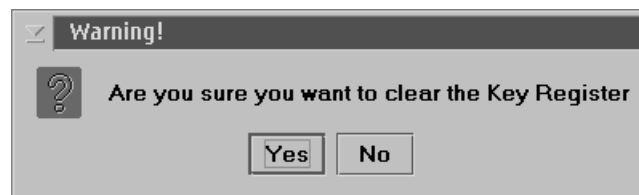


Figure 112. Clear Key Validation Message

If you press **Yes** and the command executes successfully, you will get this message:

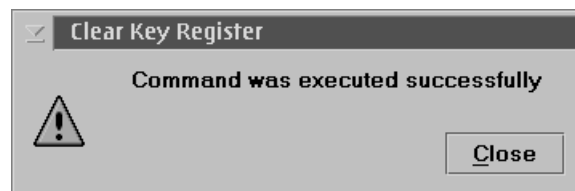


Figure 113. Clear Key Successful Message

Set (ASYM-MK only) - PCICC/PCIXCC/CEX2C

If you select SET for an asymmetric-keys master key, a message is issued warning that PKA services must be disabled before the SET is done. If you respond to continue then you get a message indicating successful execution.

SET will activate the new ASYM-MK. That is, the current ASYM-MK is transferred to the old ASYM-MK register and the new ASYM-MK register is transferred to the current ASYM-MK register. The new ASYM-MK register is reset to zeros.

Domain Keys Page - PCIXCC/CEX2C

Operational Keys (PCIXCC/CEX2C)

Beginning with TKE V4.1, operational keys can be loaded on a Crypto Coprocessor. Operational key part registers allow operational keys to be loaded and accumulated on a Crypto Coprocessor.

Note: To use TKE V4.1 or higher to load operational keys, you must be running HCR770B or higher for ICSF.

Once all the key parts have been loaded and the key is Complete, you are required to remove the key from the key part register and load it into the CKDS. This is accomplished either through ICSF panels (see “Loading Operational Keys to the CKDS” on page 209) or using an option on KGUP JCL (see *z/OS Cryptographic Services ICSF Administrator's Guide*).

Each PCIXCC/CEX2C can have a maximum of 100 key part registers distributed across all domains. A key part register can be in one of these states:

- First part entered – Load to key part register (First has completed successfully)
- Intermediate part entered – Load to key part register (Add part has completed successfully)
- Complete – Load to key part register (Complete has completed successfully)

At least two key parts must be entered and there is no maximum number of key parts.

Available tasks for Operational key part registers are:

- Load to key part register
- View
- Clear

Tasks for Load to key part register are:

- First
- Add part
- Complete

A key part register is freed when a Complete key is loaded to the CKDS from ICSF (either through the ICSF panels or KGUP JCL), when the key part register is Cleared from TKE, or a zeroize domain is issued from TKE. View of a key part register displays key part register information.

Use of the operational key part registers on the PCIXCC/CEX2C is controlled by access control points in the role definition. The access control points are:

- Load First Key Part
- Load Additional Key Part
- Complete Key
- Clear Operational Key Part Register

The Crypto Coprocessor supports all ICSF operational keys, not just Transport and PIN key types. A USER DEFINED key type is also available that allows the user to

specify their own control vector. This USER DEFINED control vector must still conform to the rules of a valid control vector. For more details on control vectors, see Appendix C in the *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

Generate Operational Key Parts: When Generate is selected for a Default Operational Key, the Generate Operational Key window is displayed showing the key type, key length, description and control vector. Only the description field may be updated. The key length and control vector fields reflect the default length and control vector for the key type selected. If the key type supports different lengths (MAC, MACVER and DATA) then the key length field can also be updated.

Figure 114. Generate Operational Key - Default ICSF Key Type

When Generate is selected for a USER DEFINED key, the Generate Operational Key window is displayed showing the key type, key length, description, and blank control vector fields. All but the key type can be updated. The control vector entered must conform to the rules for a valid control vector.

Figure 115. Generate Operational Key - USER DEFINED

In both cases, after selecting Continue on the Generate window, the user is presented with a choice of targets: Binary File, Print File or Smart Card.



Figure 116. Select Target

For either the binary file or print file option, the user must specify where the key is to be saved on the Save key part window.

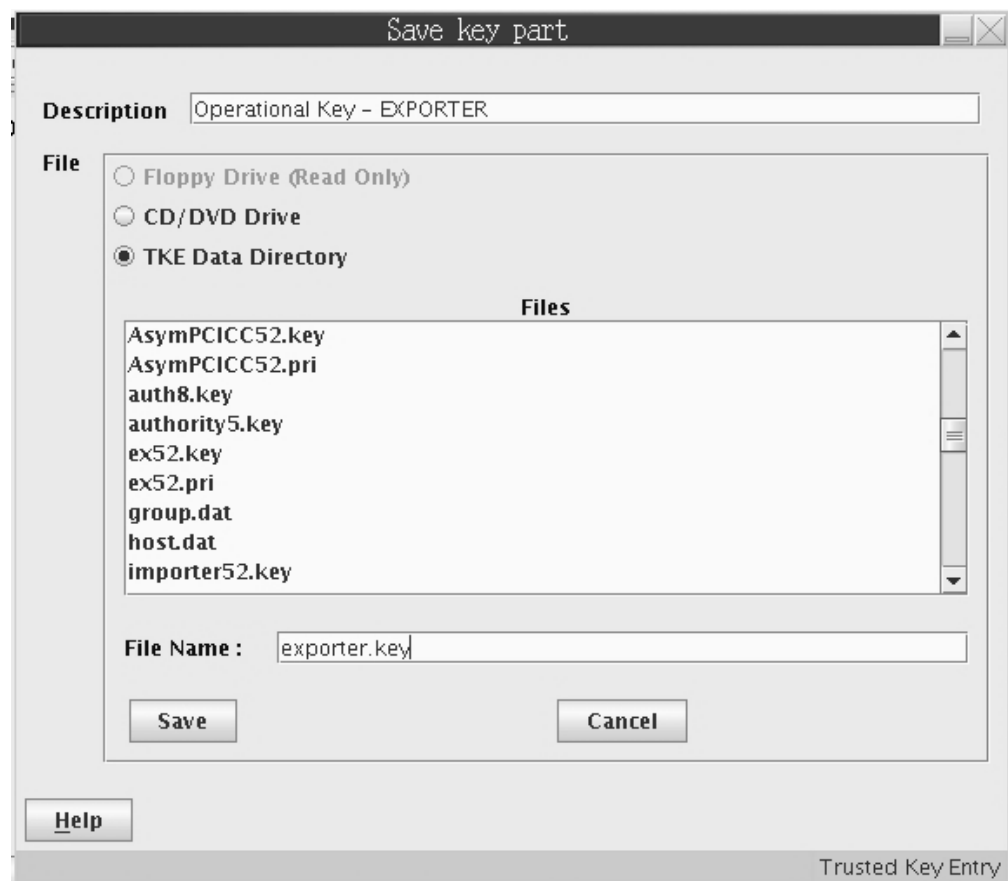


Figure 117. Save key part

After the key is saved, the user can save the same key value again in another location on the Save key again window.

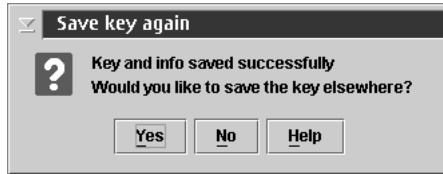


Figure 118. Save key again

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

Save key to Smart Card

Note: The TKE cryptographic adapter generates the key part and securely transfers the key to the TKE smart card. You must insert a TKE smart card that is enrolled in the same zone as the TKE cryptographic adapter; otherwise the Generate will fail. To display the zone of a TKE smart card, exit from TKE and use either the Cryptographic Node Management Utility 3.10SC or the Smart Card Utility Program 5.2 under Trusted Key Entry Applications. See “Display smart card details” on page 276, “Display smart card information” on page 291 or “View current zone” on page 304.

Steps for saving a key to a TKE smart card are:

1. When prompted, insert TKE smart card into smart card reader 2
2. Press OK
3. Enter the PIN on the smart card reader PIN pad
4. A pop up message will indicate that the key part was successfully stored on the TKE smart card.

Note: The user can use the Copy smart card contents utility to copy key parts from one TKE smart card to another. See “Copy smart cards” on page 75.

Load to Key Part Register - First: When Load to Key Part Register First is selected, the user must select the source of the key part on the Select source window.

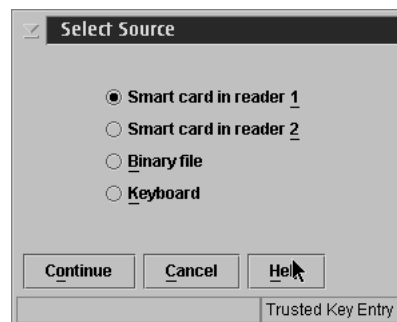


Figure 119. Select Source

If binary file is selected, the user chooses the file to load on the Specify key file window.



Figure 120. Specify key file for binary file source

If the binary file contains a key type that does not match the key type selected for loading, a warning is displayed asking for confirmation to continue. If continue is chosen, TKE will load the key part as the key type defined in the binary file and not the key type selected originally by the user.

Warning: If the file is loaded from a floppy or CD/DVD, you must deactivate the floppy or CD/DVD drive before removing the diskette or disc. If the diskette is removed prior to deactivating the drive data could be lost or corrupted. For details on deactivating media see “Managing Media” on page 377.

If keyboard is selected, the Enter key value window is displayed. When the key type is a default operational key with a fixed length (single length or double length only), the fields on the window that can be updated are the description and the key value. If the default operational key supports different lengths (DATA, MAC and MACVER), then the key length field can be updated. When the user presses Continue, the MDC-4 and ENC-ZERO is calculated and displayed, providing the user with the opportunity to visually verify the values. When Load key is pressed, the user is asked if they would like to save the key part. If yes, a file chooser window is opened for the user to select either the CD/DVD drive or the TKE Data Directory and enter a File Name for saving the key part. The key part is then loaded. If no, the key part is not saved and the key is loaded.

Enter key value

Key type: EXPORTER

Key length:
☐ 8
☒ 16
☐ 24

Description: Operational Key - EXPORTER

Control vector:
 Bytes 0..7: 00417D0003410000
 8..15: 00417D0003210000
 16..23:

Key value:
 Bytes 0..7:
 8..15:
 16..23:

Continue Cancel Help

Trusted Key Entry

Figure 121. Enter key value - keyboard source for ICSF default key type

When the key type is USER DEFINED, all the fields on the Enter Key Value window can be updated, including the control vector. The control vector entered must conform to the rules for a valid control vector. See *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

Enter key value

Key type: USER DEFINED

Key length:
☒ 8
☐ 16
☐ 24

Description: Operational Key - USER DEFINED

Control vector:
 Bytes 0..7:
 8..15:
 16..23:

Key value:
 Bytes 0..7:
 8..15:
 16..23:

Continue Cancel Help

Trusted Key Entry

Figure 122. Enter key value - keyboard source for USER DEFINED key type

1. If TKE smart card is selected, the user is prompted to insert a TKE card into the appropriate reader and select OK.

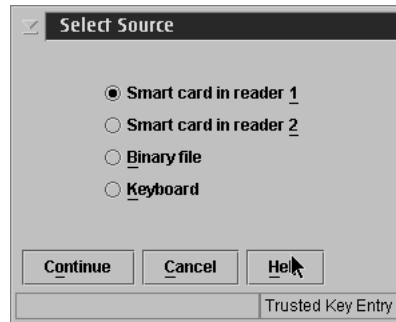


Figure 123. Select Source

2. Highlight the key part, right click and choose select; or highlight and press OK.
If the smart card contains a key type that does not match the key type selected for loading, a warning is displayed asking for confirmation to continue. If continue is chosen, TKE will load the key part as the key type defined in the smart card and not the key type selected originally by the user.

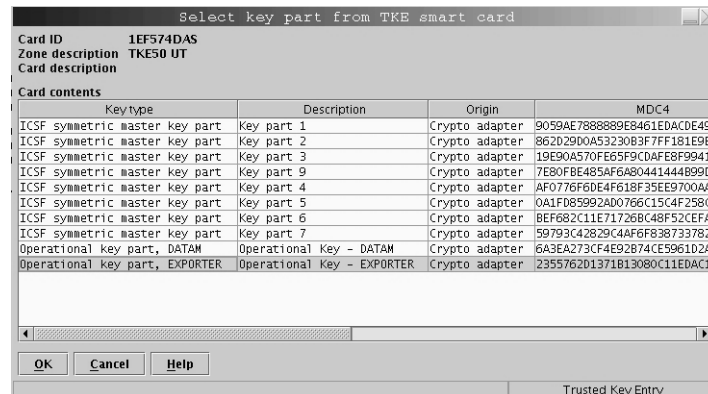


Figure 124. Select key part from TKE smart card

3. Enter PIN on PIN pad

After the binary file or TKE smart card is read or the key part is entered, the ENC-ZERO and MDC-4 values for the key part are calculated and displayed along with the description, key type, and control vector on the Key part information window. (ENC-ZERO is not displayed for 24 byte key parts.) The user must enter a key label for the key part to be loaded. When loading additional key parts, the key part register will be selected by the key label entered. The key label entered must not already exist. If it does, an error will occur. The key label must conform to valid key label names in the CKDS. It must be no more than 64 bytes with the first character alphabetic or a national (#, %, @). The remaining characters can be alphanumeric, a national character, or a period(.). When the key part is processed, the label will be converted to uppercase.



Key part information

Description: Operational Key - EXPORTER

ENC-ZERO: CP85DF3E

MDC-4: F75B19275213AD3DA3A875D23C78FC9C

Key type: Operational Key - EXPORTER

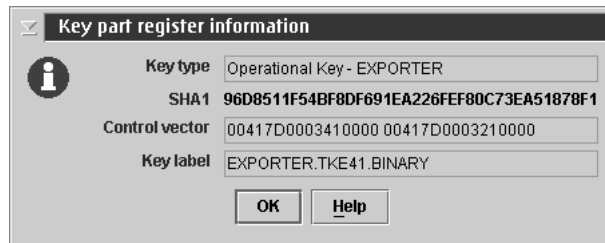
Control vector: 00417D0003410000 00417D0003210000

Key label:

Trusted Key Entry

Figure 125. Key part information - first key part

If the information presented on the Key part information panel is correct, the key part is loaded to the key part register by selecting Load Key. After the key part is successfully processed, the Key part register information window is displayed. It displays information about the Key Part Register, including the key type, SHA-1 hash of the first key part, the Control Vector and the key label. If necessary, the parity of the key part was adjusted to odd.



Key part register information

 Key type: Operational Key - EXPORTER

SHA1: 96D8511F54BF8DF691EA226FEF80C73EA51878F1

Control vector: 00417D0003410000 00417D0003210000

Key label: EXPORTER.TKE41.BINARY

Figure 126. Key part register information

After OK is selected on the Key part register information window, the Load Operational Key window is displayed, indicating that the load was processed successfully.

Load to Key Part Register - Add Part: Load to key part register Add part can be performed multiple times, but must be performed at least once. The process for loading additional parts is similar to loading the first key part.

If binary file is selected, the user chooses the file to load. If smart card in reader 1 or smart card in reader 2 is selected, the user chooses the key part to load. If keyboard is selected and the key type is a default operational key, the Enter Key Value window is displayed. If the key type is USER DEFINED then the Load Operational Key Part Register window is displayed with a drop down menu of available control vectors.



Load Operational Key Part Register

 Control vector: 0041420003480000 0041420003280000 ▼

Figure 127. Load Operational Key Part Register - add part, keyboard source for USER DEFINED

The user selects the control vector for the key part to be loaded. Note that in this display of the available control vectors, the key part bit (bit 44) is turned on indicating that the key in the key part register is a partial key and is not yet complete. This bit will be turned on automatically when the first key part is loaded regardless if the user turned it on when the control vector was defined.

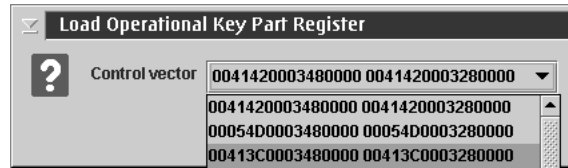


Figure 128. Drop down of control vectors - add part, keyboard source for USER DEFINED

After the control vector is selected, the Enter Key Value window is displayed. Once the binary file or key part from the TKE smart card is read or the key part is entered, the Key part information window is displayed. This window differs from the window displayed for the Load first key part in two ways: key label and key label's SHA-1.



Figure 129. Key part information - add part

The key label field is now a drop down menu for all the labels that have the same control vector and are not in a Complete state. The user selects the appropriate key label to load the key part. The key label's SHA-1 reflects the SHA-1 hash of the key parts currently loaded in the selected key part register. Load Key is selected and the key part register information window is displayed. The SHA-1 hash value displayed now represents the accumulated key parts, including the key part just loaded. If necessary, the parity of the key part just loaded was adjusted to even.



Figure 130. Key part information - add part with SHA-1 for combined key

When the add part is successfully processed, the Load Operational Key window is displayed.

Load to Key Part Register - Complete: When all the key parts have been loaded, the key part register needs to be placed in the Complete state. When load key part register complete is selected for a default operational key, the Complete Operational Key Part Register window is displayed. Only key part register labels in the intermediate state that contain keys of the same operational key type are displayed for selection. If the key type supports different key lengths (8, 16 or 24), then all key part registers of the key type selected will be displayed regardless of key length.



Figure 131. Complete Operational Key Part Register - ICSF default key type

To select one key label, select the label with the left mouse button. To select more than one key label, select the label with the left mouse button, then hold down the Control key and select additional key labels with the button. To select a range of key labels, select the first key label with the left mouse button, then hold down the Shift key and select the last key label. All key labels in between the two selected labels will be selected. To select all the key labels, hold down the Control key and type an 'a'. When only one key label is selected, the SHA-1 hash of the accumulated key in the key part register is displayed. If more than one key label is selected then the SHA-1 field on the window contains a '-'.

When load key part register complete is selected for USER DEFINED key type, the complete operational key part register window is displayed with all the domains' key part registers that are in the intermediate state.

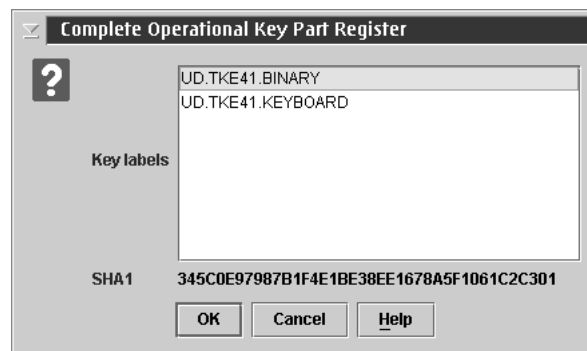


Figure 132. Complete Operational Key Part Register - USER DEFINED

After the key labels have been selected, the key part register information window is displayed for each label that was selected. The ENC-ZERO value is shown for the completed key and the state is complete. ENC-ZERO is only shown for key parts

that are not 24 bytes long.



Figure 133. Key part register information - complete

After all the key labels that were selected are processed, the load operational key window is displayed indicating that the command was executed successfully.

View: Operational Key View is used to display key part register information. When View is selected for a default operational key, the View Operational Key Part Register window is displayed. Only key part register labels that contain keys of the same operational key type are displayed for selection.



Figure 134. View Operational Key Part Register - ICSF default key type, one key label selected

To select one key label, select the label with the left mouse button. To select more than one key label, select the label with the left mouse button, then hold down the Control key and select additional key labels with the button. To select a range of key labels, select the first key label with the left mouse button, then hold down the Shift key and select the last key label. All key labels in between the two selected labels will be selected. To select all the key labels, hold down the Control key and type an 'a'. When only one key label is selected, the SHA-1 hash of the accumulated key in the key part register is displayed. If more than one key label is selected then the SHA-1 field on the window contains a '-'.



Figure 135. View Operational Key Part Register - ICSF default key type, all key labels selected

When View is selected for USER DEFINED key type, the view operational key part register is displayed with all the domains' key part registers.



Figure 136. View Operational Key Part Register - USER DEFINED

After the key labels have been selected, the key part register information window is displayed for each label that was selected. For keys that are in the First part entered or Intermediate part entered state, the SHA-1 value is displayed for the accumulated partial key value. Since the key contained in the key part register is a partial key, the key part bit (bit 44) of the control vector will be turned on. This is true for default and USER DEFINED key types.



Figure 137. View key part register information - key part bit on in CV

If the key is in the Complete state, the ENC-ZERO value of the completed key is displayed. If the key is 24 bytes, the ENC-ZERO value will be a dash ('-') rather than the actual hex number. The control vector for the completed key will have the key part bit turned off.



Figure 138. View key part register information - complete key

After all the key labels that were selected are processed, the view key register window is displayed indicating that the command was executed successfully.



Figure 139. View key register successful message

Clear: Operational Key Clear is used to clear the contents of key part registers. When Clear is selected, a **Warning!** window is displayed, prompting the user to confirm that they want to clear the key part registers.

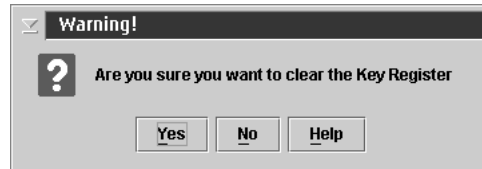


Figure 140. Warning! message for clear operational key part register

When clear is selected for a default operational key, the clear operational key part register window is displayed. Only key part register labels that contain keys of the same operational key type are displayed for selection. If the key type supports different key lengths (8, 16 or 24), then all key part registers of the key type selected will be displayed regardless of key length.



Figure 141. Clear Operational Key Part Register - ICSF default key type, one key label selected

To select one key label, select the label with the left mouse button. To select more than one key label, select the label with the left mouse button, then hold down the Control key and select additional key labels with the button. To select a range of key labels, select the first key label with the left mouse button, then hold down the Shift key and select the last key label. All key labels in between the two selected labels will be selected. To select all the key labels, hold down the Control key and type an 'a'. When only one key label is selected, the SHA-1 hash of the accumulated key in the key part register is displayed. If more than one key label is selected then the SHA-1 field on the window contains a '-'.



Figure 142. Clear Operational Key Part Register - ICSF default key type, all key labels selected

When Clear is selected for USER DEFINED key type, the clear operational key part register is displayed with all the domains' key part registers.



Figure 143. Clear Operational Key Part Register - USER DEFINED, one key label selected

After OK is selected, the key labels selected are processed, and the Clear Key Register window is displayed indicating that the command was executed successfully.



Figure 144. Clear Key Register successful message

Load to Key Storage - PCIXCC/CEX2C

This selection is only possible for operational IMP-PKA or IMPORTER keys. The IMP-PKA key-encrypting keys are used to protect RSA keys during transport from the workstation to ICSF whereas the IMPORTER keys are used to protect DES keys during transport from the workstation to ICSF. Having selected Load to Key Storage, the user selects which key part 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 use 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.

☒ **Install IMPORTER key part in TKE workstation key storage**

A host IMPORTER key is installed in the TKE workstation key storage as an EXPORTER key.

EXPORTER keys in TKE workstation key storage.

Key label
IMPPKA.RSA.KEYGEN.KNOWN.KEY.VALUE
IMPPKA.RSA.KEYENC.KNOWN.KEY.VALUE
MIGRATE.IMPORTER.KEY

Workstation key label

Trusted Key Entry

Figure 145. Install Importer Key Part in Key Storage

For IMP-PKA keys, you must specify additional information.

☒ **Install IMP-PKA key part in TKE workstation key storage**

A host IMP-PKA key is installed in the TKE workstation key storage as an EXPORTER key.

Key usage

☒ for RSA key generation

☐ for RSA key enciphering

EXPORTER keys in TKE workstation key storage.

Key label
IMPPKA.RSA.KEYGEN.KNOWN.KEY.VALUE
IMPPKA.RSA.KEYENC.KNOWN.KEY.VALUE

Workstation key label

Trusted Key Entry

Figure 146. Install IMP-PKA Key Part in Key Storage

A window is displayed for the user to specify the workstation key label and whether this IMP-PKA key will be used for protecting an RSA key to be generated at the workstation or a clear RSA key to be enciphered at the workstation.

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 to Key Part Register - First” on page 134.

Secure Key Part Entry

To save known key part values to a TKE Smart Card use secure key part entry. Refer to Appendix E, “Secure Key Part Entry,” on page 305 for details on using this function.

Generate RSA Key - PCIXCC/CEX2C

Note: On z990, z890, z9 EC, z9 BC and System z10 EC, it is strongly recommended that customers use the PKA key generate (CSNDPKG) API to generate RSA keys.

To write RSA keys to the PKDS, use PKA key record create (CSNDKRC or CSNDKRW).

For more information, see *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

This selection initiates RSA key generation at the workstation. The key is protected with a previously generated IMP-PKA key encrypting key and saved in a file.

From the Domains Keys page, right-click on RSA key in the Key Types container and select Generate. The Generate RSA Key window is displayed.

Figure 147. Generate RSA Key

Specify this 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. All values from 512 to 1024 are valid. If the entered value exceeds the maximum value set by the selected crypto module an error Invalid key length specified. It must be between 512 and 1024 is displayed. You are allowed to continue but the generated RSA key cannot be loaded to this crypto module.
- *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 IMP-PKA label* — The container displays the labels of the key-encrypting keys currently in the TKE workstation key storage available for protecting RSA keys generated at a TKE workstation. Select one by clicking on it.
- *Host IMP-PKA key label* — The CKDS key label at the host used to import the RSA key. The selected Workstation IMP-PKA 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 file chooser window is displayed for the user to specify the file location (CD/DVD or TKE Data Directory) and file name for saving the generated RSA key.

Warning: If the RSA key is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

Encipher RSA Key - PCIXCC/CEX2C

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 I, “Clear RSA Key Format,” on page 325.

Having selected the Encipher action, the Encipher RSA Key window is displayed:

Figure 148. Encipher RSA Key

Specify this 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 EXPORTER key label* — The container displays the labels of the key-encrypting keys currently in the TKE workstation key storage available for protecting RSA keys entered from a clear key file. Select one by clicking on it.
- *Host IMP-PKA key label* — The CKDS key label at the host used to import the RSA key. The selected Workstation IMP-PKA 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 (CD/DVD Drive or TKE Data Directory) and file name for saving the encrypted RSA key.

Warning: If the RSA key is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

Load RSA Key to PKDS - PCIXCC/CEX2C

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 LPAR. For loading RSA keys to TKE target LPARs, see “Load RSA Key to Host Dataset - PCIXCC/CEX2C” on page 151.

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 149. Load RSA Key to PKDS

Specify this 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 EXPORTER key label* — Label of the workstation IMP-PKA that is used for protecting the RSA key.

- *Host IMP-PKA key label* — Label of the IMP-PKA key stored in the host CKDS that will be used to import the RSA key. Change this field as needed.

Load RSA Key to Host Dataset - PCIXCC/CEX2C

This selection allows the user to load an RSA key to a host data set as an external key token. From this dataset it is possible to install the key in the PKDS by means of TSO ICSF panels.

The host dataset must be defined in advance with these attributes: recfm fixed, lrecl=1500, partitioned. Using this installation method, it is possible to load RSA keys into any PKDS in any LPAR. For information on the TSO ICSF interface, see “Installing RSA Keys in the PKDS from a Data Set” on page 213.

The steps are the same as for loading an RSA key to PKDS (see “Load RSA Key to PKDS - PCIXCC/CEX2C” on page 150), except that the user has to specify the full dataset and member name. If you don’t specify the dataset and member name in quotes, the high level qualifier for the dataset is the TSO logon of the administrator/host user ID.

Figure 150. Load RSA Key to Dataset

Domains Controls Page

The Domain Controls page displays the cryptographic functions that are in effect for the domain and allows you to make changes to them. There are different pages for the CCF crypto modules and the PCICC/PCIXCC/CEX2C crypto modules.

- To change a setting, click on it
- To upload the controls settings to the crypto module, press **Send updates**
- To leave the controls settings unaltered after you have made changes to the page, press **Discard changes**

Working with Domain Controls Settings (CCF)

You can enable or disable these functions from the TKE workstation:

- Cryptographic functions
- Special Secure mode
- Load clear new master key
- Load clear Signature master key
- Load clear Key Management master key



Figure 151. CCF Domain Controls Page - Default Setting

The *Cryptographic functions* box should always be checked. If it is not, basic cryptography is unavailable. If for some reason you must disable *cryptographic functions*, you must first disable PKA services from the ICSF panels (see “Disabling PKA Services” on page 180). PKA Services should not be enabled on the target system until **ALL** crypto modules are back online (see “Enabling PKA Services” on page 181).

The *Special Secure mode* box, when enabled, allows you to input clear keys and generate clear PINs. SSM must be enabled for the KGUP utility to permit generation or input of clear keys and to enable the secure key import or clear pin generate callable services. If you want to control the setting of SSM through the TKE workstation, SSM must be enabled in the Installation Options dataset and on the LPAR Cryptographic Control panel.

The *Load Clear New Master Key*, the *Load Clear PKA Signature Master Key* and the *Load Clear PKA Key Management Master Key* boxes, if checked, allow Clear Key Entry to be performed with the ICSF panels. These *Load clear* functions do not need to be enabled for TKE usage. Installations must decide if these functions should remain disabled.

If you disable the *Load Clear* functions from TKE, you will not be able to change the DES and PKA Master Keys if there is a hardware failure on the workstation.

To set the typical controls setting for CCF, press **Set default values**. The default setting enables cryptographic functions.

Working with Domains Controls Settings (PCICC/PCIXCC/CEX2C)

With TKE 3.1 and higher, you are able to administer access control points to ISPF Services, API Cryptographic Services and User Defined Extensions for the PCICC and PCIXCC/CEX2C from this page.

There are expandable folders for the Domain Cryptographic services. Within the folders are the services you can enable or disable:

- ISPF Services
- API Cryptographic Services
- UDXs (appears only if you have created UDXs on your system)

Note: Some services cannot be disabled because they are 'required'. This is indicated on the panel.

Whether the various services are enabled or disabled on your system is dependent upon TKE workstation installation. Prior to TKE Version 3.1, only ISPF services could be updated. With TKE Version 3.1 and later, access control points for API and UDX services can be updated.

If you have never installed a TKE workstation on your system, all services (ISPF and API) will be enabled when you first logon to the workstation. (For UDXs with access control points, enablement requires a TKE workstation.)

If, however, you have previously installed a TKE Version 3 workstation, your service settings will be the same as those for your existing system. The API settings will also be the same as those for the existing system, except for new access control points (which are disabled). The UDX access control points would all be disabled for the PCICC.

As new access control points are added, they are enabled for new, first-time, TKE installations. For existing TKE installations, API services will reflect what had been enabled/disabled in Version 3.1 and new access control points will be disabled. UDX support is implemented likewise. If your installation wants to use the new callable services, the corresponding access control point must be enabled.

PCIXCC/CEX2C have some additional access control points that are not available on the PCICC. For new TKE V5.2 users, all access control points enabled in the Default Role will be enabled on the PCIXCC/CEX2C. If migrating from TKE V4.0 or later to TKE V5.2 on a z990, z890, z9 EC, z9 BC or System z10 EC hardware, API services will reflect what had been enabled/disabled in the previous TKE release. Access control points may need to be enabled depending on the ICSF FMID installed on the above mentioned hardware.

ISPF Services: Under the ISPF Services folder, there are check boxes for the services you can enable or disable. These services are for loading and setting the Symmetric and Asymmetric Master Keys on the PCICC/PCIXCC/CEX2C through the ICSF panel interface.

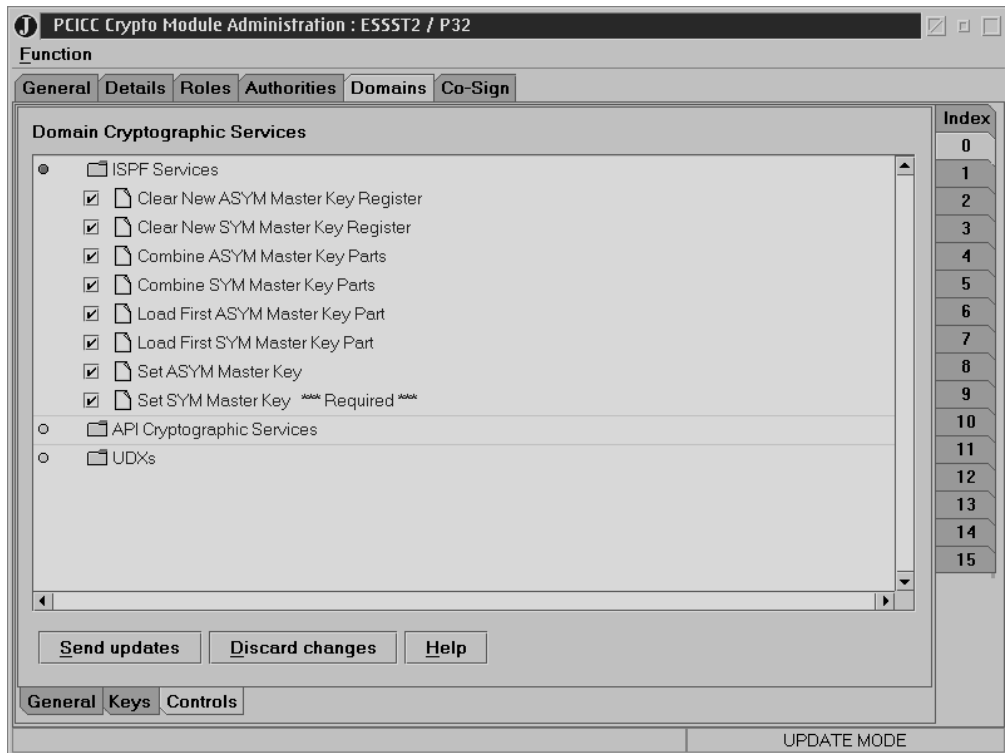


Figure 152. PCICC Domain Controls Page with Expanded ISPF Services

If you are using a TKE workstation for the first time, your settings under ISPF Services will indicate that all services are enabled.

If you previously used a TKE V3.1 or later workstation, your settings under ISPF Services will indicate the settings that were being used on that TKE workstation for the PCICC and Cryptographic Coprocessors.

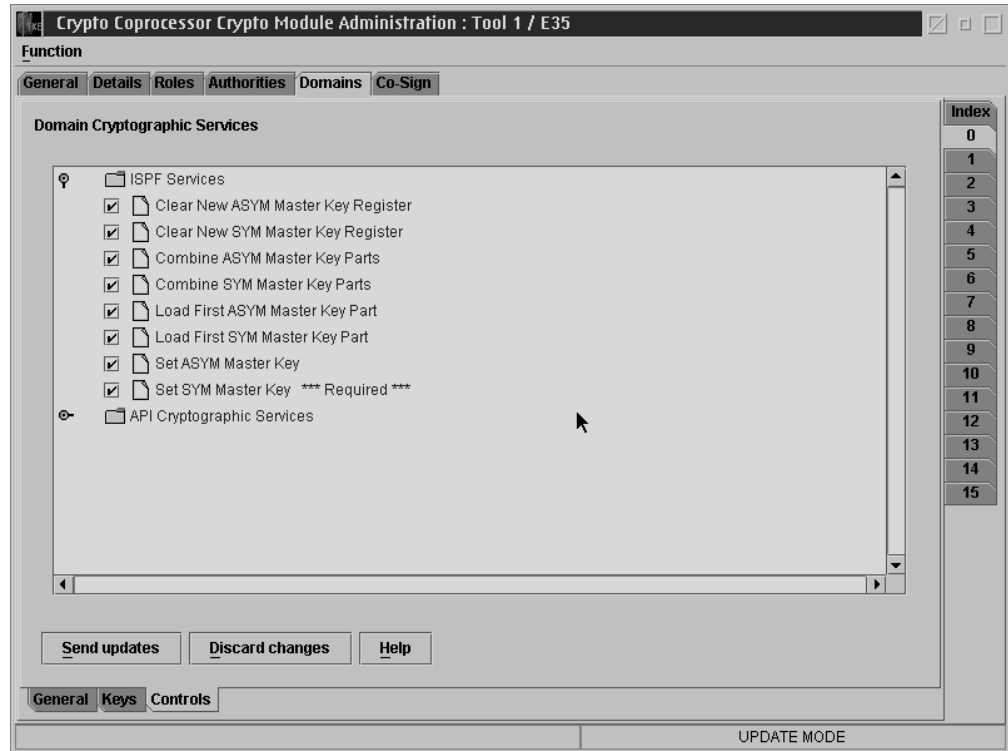


Figure 153. PCIXCC/CEX2C Domain Controls Page with Expanded ISPF Services

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 Appendix F, “Access Control Points and Callable Services,” on page 311 for the correlation between the access control point and the ICSF callable service.

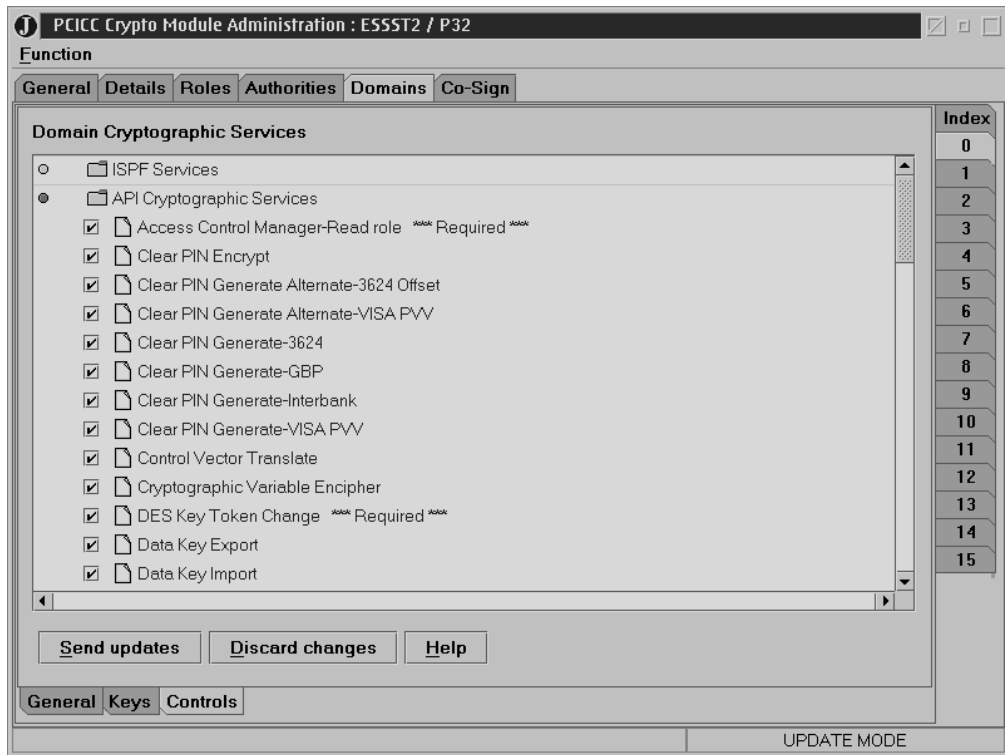


Figure 154. PCICC Domain Controls Page with Expanded API Cryptographic Services

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.

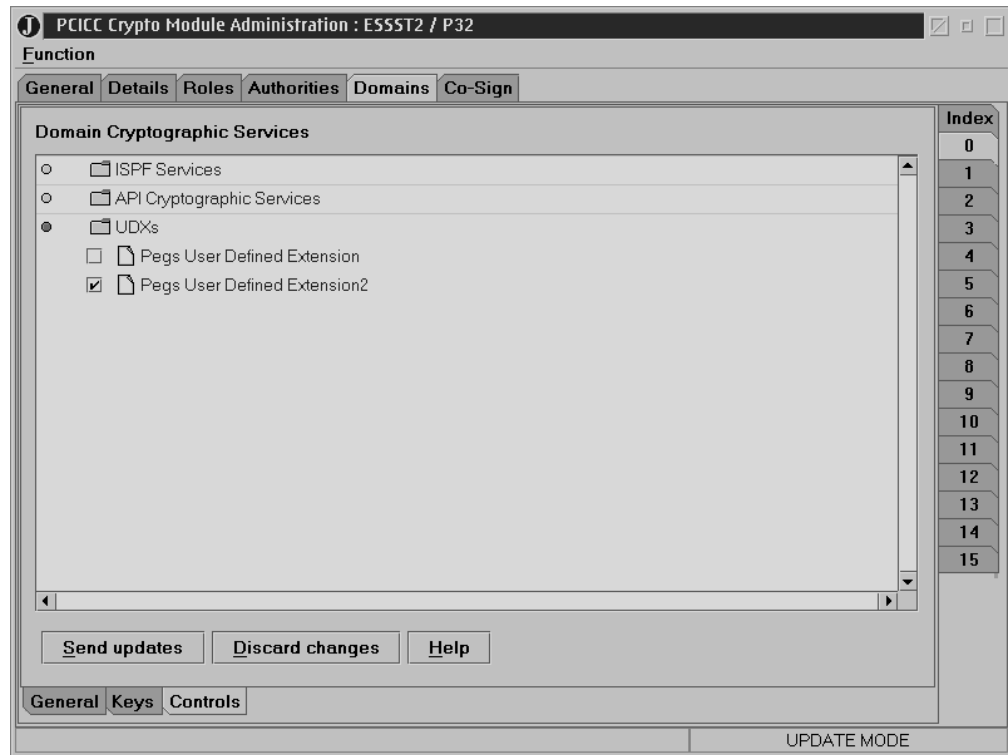


Figure 155. PCICC Domain Controls Page with Expanded UDXs

Co-Sign

For co-signing a pending command in a crypto module, open the notebook for that crypto module and select the Co-sign page. This page displays 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 CCF crypto modules, the number of required signatures is displayed for each of the three conditions together with the authority index and name of each authority allowed to sign the pending command.

For PCICC and PCIXCC/CEX2C crypto modules, exactly two signatures are required for a multi-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**.

Function																									
General Details Roles Authorities Domains Co-Sign Co-sign pending command Pending command Load authority Pending command reference 20A0832852D531FE9DCBA0D01BD6000020700808 Loading authority 2, J Roberts Pending command details <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th style="width: 15%;">Field</th> <th style="width: 85%;">Value</th> </tr> </thead> <tbody> <tr> <td>Author...</td> <td>7</td> </tr> <tr> <td>Role:</td> <td>access</td> </tr> <tr> <td>Public..</td> <td>FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF...</td> </tr> </tbody> </table>		Field	Value	Author...	7	Role:	access	Public..	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF...																
Field	Value																								
Author...	7																								
Role:	access																								
Public..	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF...																								
Signature requirements <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th style="width: 10%;">Req</th> <th style="width: 40%;">Authority</th> <th style="width: 50%;">Signed</th> </tr> </thead> <tbody> <tr> <td>1 of</td> <td>00,</td> <td></td> </tr> <tr> <td></td> <td>01, R Greene</td> <td></td> </tr> <tr> <td></td> <td>02, J Roberts</td> <td>yes</td> </tr> <tr> <td>and</td> <td></td> <td></td> </tr> <tr> <td>1 of</td> <td>00,</td> <td></td> </tr> <tr> <td></td> <td>01, R Greene</td> <td></td> </tr> <tr> <td></td> <td>03, H Ford</td> <td></td> </tr> </tbody> </table>		Req	Authority	Signed	1 of	00,			01, R Greene			02, J Roberts	yes	and			1 of	00,			01, R Greene			03, H Ford	
Req	Authority	Signed																							
1 of	00,																								
	01, R Greene																								
	02, J Roberts	yes																							
and																									
1 of	00,																								
	01, R Greene																								
	03, H Ford																								

Figure 156. PCICC Co-Sign Page

Pressing the **Co-sign** button initiates the signing of the pending command. It opens windows where you can choose the source of the signature and then choose the authority index associated with that key.

- Current key - Uses the currently loaded signature key
- Smart card - Reads a signature key from a TKE smart card
- Binary file - Reads a signature key from a hard disk or diskette
- Key storage - Reads the signature key from PKA key storage
- Default key - Uses the default signature key hardcoded into TKE

Press **Delete** if you want to delete the pending command.

Chapter 7. Managing Keys: TKE and ICSF with CCF

Master keys are used to protect all cryptographic keys that are active on your system. The number and types of master keys you need to enter depends on your hardware configuration.

- On the zSeries Model 900 eServers, on the S/390 Enterprise Servers and on S/390 Multiprise with Cryptographic Coprocessor Features, a DES master key protects DES keys and PKA master keys protect DSS and RSA keys.
- On the optional PCI Cryptographic Coprocessor, the symmetric-keys master key (SYM-MK) protects symmetric keys such as DES keys and the asymmetric-keys master key protects RSA keys. These are discussed in this topic.

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.

ICSF is required to complete some operations initiated from TKE. These operations include importing a DES key part from the key part queue to the DES master key register and importing operational key parts from the key part queue to the CKDS. ICSF is required for setting the master key, initializing/refreshing the CKDS, and installing RSA keys to the PKDS. ICSF is also required for disabling and enabling PKA services, PKDS Initialization, PKDS Reencipher and PKDS Activate.

Be prepared to switch between your TKE workstation and your ICSF host session.

This topic discusses the procedures needed for:

- Loading the master keys the first time you start ICSF (page 160)
- Importing Master Keys from the Queue (page 163)
- Changing the DES and SYM-MK master keys periodically (page 170)
- Restarting Key Entry (page 174)
- Reentering the master keys (page 176)
- Adding Additional Coprocessors (page 178)
- Changing the PKA master keys (page 179)
- Loading and Importing Operational Keys (page 184)
- Refreshing the CKDS (page 192)
- Install RSA Keys (page 193)

The types of master keys you can enter and the steps you take to enter master keys depends on your system processor and hardware features.

Synchronizing Keys

If your installation is using both CCF crypto modules and PCICC crypto modules, you must keep specific keys the same. The DES Master Key in your CCF crypto modules must be the same as the Symmetric Master Key in your PCICC crypto modules. The PKA Signature Master Key (SMK) in your CCF crypto modules must be the same as the Asymmetric Master Key in your PCICC crypto modules.

Before you set (activate) your master key, you must be sure that all your crypto modules (CCF and PCICC) have loaded the same key. If you change the DES new master key in your CCF crypto modules, you must then make the same change to the New Symmetric Master Key in your PCICC crypto modules. This also holds true for the PKA SMK key and the New Asymmetric Master Key.

Master Key Parts

Master key parts are loaded using binary files, the keyboard, or TKE smart cards. If loading key parts with the keyboard, record the key parts and the associated hash patterns.

The key parts are generated from the Domain Keys page. For more information, see “Domain Keys Page - CCF” on page 105 and “Domains Keys Page (PCICC and PCIXCC/CEX2C)” on page 121.

Note: If you are reentering master keys after they have been cleared, use the same master key part values as when you originally entered the keys. You should have saved the key part values in a secure place after you entered the master keys previously.

To enter a DES master key, you can either enter a complete key, a first key part and a final key part or a first key part, one or more intermediate key part and a final key part.

First-Time Startup

The first time you start ICSF, you must load a DES master key and initialize the CKDS. For information on creating an empty CKDS, see *z/OS Cryptographic Services ICSF System Programmer's Guide*. When you initialize the CKDS, ICSF creates a header record for the CKDS, installs the required system keys in the CKDS, and sets the master key. Keys stored in the CKDS are enciphered under the DES master key. After the master key has been set, you can generate or enter any keys you need to perform cryptographic functions.

To define a DES master key, you must load the key parts to the DES new master key register on CCF, and if running with PCICCs, you must also load the key parts to the new SYM-MK register. Since this is the first time you are starting ICSF, you may use **Load** to load directly to the register. If you use **Load to Queue**, you must additionally import the key (see “Importing Key Parts from the Queue” on page 163 for instructions).

Load and **Load to Queue** are discussed in “Domain Keys Page - CCF” on page 105.

There are four different types of system keys you can install in the CKDS:

- Required SYSTEM keys are automatically generated when you first initialize the CKDS. These include the MAC and MACVER keys that ICSF uses to generate and validate the MAC code in each CKDS record.
- NOCV-enablement keys are required for NOCV IMPORTERS and EXPORTERS. The NOCV-enablement system keys are used to twist on and twist off the CVs on external tokens during key import and key export. This allows ICSF to communicate with systems that do not use control vectors.
- ANSI system keys are required for almost all ANSI services to perform the notarization and offset that are required by ANSI X9.17.

- ESYS, or enhanced system keys, are used only in Symmetric Key Export (CSNDSYX) callable service.

You have to initialize a CKDS only the first time you start ICSF on a system. After you initialize a CKDS, you can copy the disk copy of the CKDS to create other CKDSs for use on the system. You can also share a CKDS with another ICSF system if the system has the same master key value.

If sharing a CKDS between a z890, z990, z9 EC, z9 BC, or System z10 EC system and a legacy system, the CKDS must be initialized on a legacy system.

At any time, you can read a different disk copy into storage. For information about how to read a disk copy into storage, see “Refreshing the CKDS” on page 192.

Initialize the CKDS

At this point, the DES new master key register on each CCF in this domain is full. If you have PCICC crypto modules, the new SYM-MK register on each PCICC is also full. The hash pattern of the new SYM-MK should match the hash pattern of the DES master key. If it does not, clear the register and reload the keys.

You must now initialize the CKDS (which also activates the DES master key).

From the ICSF Primary Menu on TSO:

1. Select Option 2, MASTER KEY, as shown in Figure 157.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----
OPTION ==> 2
```

Enter the number of the desired option.

- | | | | |
|---|------------------|---|--|
| 1 | COPROCESSOR MGMT | - | Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - | Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - | Installation options |
| 4 | ADMINCNTL | - | Administrative Control Functions |
| 5 | UTILITY | - | ICSF Utilities |
| 6 | PPINIT | - | Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - | TKE Master and Operational key processing |
| 8 | KGUP | - | Key Generator Utility processes |
| 9 | UDX MGMT | - | Management of User Defined Extensions |

Licensed Materials - Property of IBM

This product contains "Restricted Materials of IBM"
 5694-A01 (C) Copyright IBM Corp. 2004. All rights reserved.
 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 157. ICSF Selecting the Master Key Option on the Primary Menu Panel

2. The Master Key Management panel appears. Select Option 1, INIT/REFRESH CKDS, as shown in Figure 158 on page 162.

```

CSFMKM00 ----- ICSF - Master Key Management -----
OPTION ==> 1

Enter the number of the desired option above.

1 INIT/REFRESH CKDS - Initialize a Cryptographic Key Data Set or
                    - activate an updated Cryptographic Key Data Set
2 SET MK           - Set a DES/Symmetric-Keys master key
3 REENCIPHER CKDS  - Reencipher the CKDS prior to changing the DES
                    - /Symmetric Keys master key
4 CHANGE MK        - Change the DES/Symmetric-Keys master key and
                    - activate the reenciphered CKDS

5 INITIALIZE PKDS   - Initialize or update a PKDS Cryptographic
                    - Key Data Set header record
6 REENCIPHER PKDS   - Reencipher the PKA Cryptographic Key Data Set
7 ACTIVATE PKDS     - Activate the PKDS after it has been reenciphered
8 REFRESH CACHE     - Refresh the PKDS cache if enabled

```

Figure 158. Selecting the Initialize a CKDS Option on the ICSF Master Key Management Panel

3. The Initialize a CKDS panel now appears.

```

CSFCKD00 ----- ICSF - Initialize a CKDS -----
COMMAND ==> 1

Enter the number of the desired option.

1 Initialize an empty CKDS (creates the header and system keys)
2 NOCVKEYS - Create NOCV-Enablement keys (for keys without CVs)
3 ANSI     - Create ANSI system keys (for ANSI X9.17 services)
4 ESYS     - Create enhanced system keys (for Symmetric services)

5 REFRESH  - Activate an updated CKDS

Enter the name of the CKDS below.

CKDS ==> 'FIRST.EMPTY.CKDS'

```

Figure 159. ICSF Initialize a CKDS Panel

4. In the CKDS field at the bottom of the panel, enter the name of the empty VSAM data set that was created to use as the disk copy of the CKDS.
The name you enter should be the same name that is specified in the CKDSN installation option in the installation options data set. For information about creating a CKDS and specifying the CKDS name in the installation options data set, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.
5. Choose option 1, Initialize an empty CKDS, and press ENTER.
ICSF creates the header record in the disk copy of the CKDS. Next, ICSF sets the DES master key. ICSF then adds the required system keys to the CKDS and refreshes the CKDS. When ICSF completes all these steps the message **INITIALIZATION COMPLETE** appears. If you did not enter a master key into the new master key register previously, the message **NMK REGISTER NOT FULL** appears and the initialization process ends. You must enter a master key into the new master key register before you can initialize the CKDS.

Note: If any part of the option 1 fails, you must delete the CKDS and start over. If the failure occurs after the master key is set and before the system keys have been created, you will need to start over: initialize an empty CKDS, load a new master key and initialize the CKDS.

6. If you want ICSF to create NOCV-enablement keys after the initialization process has been completed, select option 2, NOCVKEYS, and press ENTER. The creation of NOCV-enablement keys is optional. It allows you to create NOCV keys using the key generator utility program or the Key Token Build callable service. NOCV keys allow you to send and receive keys from systems that do not use control vectors. For a description of NOCV keys, see the description of the key generator utility program NOCV keyword in *z/OS Cryptographic Services ICSF Administrator's Guide*.

Note: If you want to run the ICSF conversion program to convert a CUSP/PCF CKDS into ICSF format, the CKDS you start with must contain NOCV-enablement keys. For more information about the conversion program, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

7. To create ANSI system keys used for the ANSI X9.17 services, choose option 3, ANSI.

The creation of ANSI system keys is optional. ANSI system keys are required if you intend to also create enhanced system keys.

The message ANSI KEYS ADDED appears on the top right of the panel, if the process succeeds.

8. To create enhanced system keys, choose option 4, ESYS.

The creation of enhanced system keys is optional. To create enhanced system keys, you must have previously installed the ANSI system keys in the CKDS.

The message ESYS KEYS ADDED appears on the top right of the panel, if the process succeeds.

After you complete the entire process, a master key and CKDS exist on your system. If you want to enter keys other than PIN or transport (for example, keys using the key generate callable service or the key generator utility program), see *z/OS Cryptographic Services ICSF Administrator's Guide*.

Note: Special secure mode is required to initialize ICSF for the first time. After you perform the initialization process, you may choose to disable special secure mode.

Importing Key Parts from the Queue

This is the suggested method whereby you load the master key parts to a key part queue. You then import the keys to the new master register from the queue.

Note: Depending on your machine type, the key part queue will have room for either one or multiple entries (up to three). If your machine can only handle one entry on the key part queue, you must load and then import each key part individually. If your machine handles multiple entries, you load the key parts and then import them all.

This task is performed from your TSO logon id using the ICSF panels.

Importing Key Parts Individually

This procedure is for machines that can only handle one entry on the key part queue. Follow these steps to load and import two or more key parts into the DES new master key register:

1. Loading the first DES new master key part (TKE workstation)
2. Importing the first DES new master key part into the DES new master key register (ICSF panels)
3. Refresh the crypto notebook (TKE workstation)
4. Loading the intermediate DES new master key part (TKE workstation)*
5. Importing the intermediate DES new master key part into the DES new master key register (ICSF panels)*
6. Refresh the crypto notebook (TKE workstation)*
7. Loading the final DES new master key part (TKE workstation)
8. Importing the final DES new master key part into the DES new master key register (ICSF panels)
9. Refresh the crypto notebook (TKE workstation)

Note: * You may have one or more intermediate key parts, so these steps (4, 5 and 6) can be repeated.

Importing Multiple Key Parts

This procedure is for machines that can handle multiple entries (up to three) on the key part queue. Follow these steps to load and import two or more key parts into the DES new master key register:

1. Loading the first DES new master key part (TKE workstation)
2. Loading the intermediate DES new master key part (TKE workstation)
3. Loading the final DES new master key part (TKE workstation)
4. Importing the first DES new master key part into the DES new master key register (ICSF panels)
5. Importing the intermediate DES new master key part into the DES new master key register (ICSF panels)
6. Importing the final DES new master key part into the DES new master key register (ICSF panels)
7. Refresh the crypto notebook (TKE workstation)

Importing the First Master Key Part into the DES New Master Key Register

To begin importing the first master key part, start at the ICSF panels and follow these instructions:

1. Select option 7, TKE, on the primary menu panel, as shown in Figure 160 on page 165.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----  
OPTION ==> 7
```

Enter the number of the desired option.

- | | | |
|---|------------------|--|
| 1 | COPROCESSOR MGMT | - Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - Installation options |
| 4 | ADMINCTL | - Administrative Control Functions |
| 5 | UTILITY | - ICSF Utilities |
| 6 | PPINIT | - Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - TKE Master and Operational key processing |
| 8 | KGUP | - Key Generator Utility processes |
| 9 | UDX MGMT | - Management of User Defined Extensions |

Figure 160. Selecting the TKE Option on the ICSF Primary Menu Panel

2. Select option 1, DES Master Key entry, on the TKE Processing Selection panel, as shown in Figure 161.

```
CSF@PK00 ----- ICSF - TKE Processing Selection -----  
OPTION ==> 1
```

Enter the number of the desired option.

- | | |
|---|---------------------------|
| 1 | DES Master key entry |
| 2 | DES Operational key entry |
| 3 | PKA key entry |

Figure 161. Selecting the DES Master Key entry on the TKE Processing Selection Panel

3. The TKE Coprocessor Selection panel, similar to the one in Figure 162 on page 166, appears. Select the coprocessor for master key entry by typing the coprocessor number on the OPTION line and pressing ENTER.

Note: If you have only one coprocessor installed, or if there is only one coprocessor defined to this partition, this panel will only show one coprocessor.

```

CSFCMP20 ----- ICSF - TKE Coprocessor Selection -----
OPTION ==> 0

CRYPTO DOMAIN: 0

Enter the number of the coprocessor to be used for key entry.

REGISTER STATUS          0. COPROCESSOR C0          1. COPROCESSOR C1

Crypto Module ID         : E589C39694407A60         : C39997A396F1407A
                          : 5D40C39997A396F0         : 605D40E589C39694
New Master Key register   : EMPTY                   : EMPTY
NMK verification pattern  :                          :
Old Master Key register   : VALID                    : VALID
OMK verification pattern  : 0212570BB5E544C1         : 0212570BB5E544C1
Old/New Master Key register: 3DDAE6229901A0C5         : 5B82229C87F044C3
hash pattern             : 3C8BE367C85054C0         : DA6544F00CC43D46
Master Key register       : VALID                    : VALID
MK verification pattern   : CA6B408A02371B1D         : CA6B408A02371B1D
Master Key register       : DF3A50AE5466123A         : DF3A50AE5466123A
hash pattern             : 96EF57E8BD074557         : 96EF57E8BD074557
Special Secure Mode       : ENABLED                 : ENABLED
Environment Control Mask  : F3FEFCF0                 : F3FEFCF0

Press ENTER to select coprocessor and proceed to new master key part entry.
Press END   to exit to the previous menu.

```

Figure 162. Selecting a Coprocessor for Master Key Entry

4. The Enter New Master Key panel appears. See Figure 163. Select option 1, ENTER A KEY PART, to begin the key part entry steps.

```

CSFEKM00----- ICSF - TKE - Enter New Master Key -----
OPTION ==> 1

Coprocessor selected for new master key : C0
New master key register status          : EMPTY

Enter the number of the desired option.

1 ENTER A KEY PART          - Enter a key part into NMK register
2 ENTER A FINAL KEY PART    - Enter a final key part into NMK register
3 RESTART KEY ENTRY PROCESS - Clear the NMK register

```

Figure 163. Selecting the Enter Key Part Option on the Enter New Master Key Panel

5. The Enter First Master Key Part panel appears. See Figure 164 on page 167.


```

CSFEKP10----- ICSF - TKE - Enter First Master Key Part -----
COMMAND ==>

                Coprocessor selected for new master key      : C0
                New master key register status                : EMPTY

Press ENTER to load the key part.
Press END   to exit to the previous menu.

```

Figure 164. Enter First Master Key Part Panel with Key Part Register Status Enabled

6. Press ENTER. The panel should now appear similar to Figure 165. If successful, the message KEY PART LOADED appears in the right hand corner.

```

CSFEKP20----- ICSF - TKE - Enter First -----KEY PART LOADED
COMMAND ==>

                Coprocessor selected for new master key      : C0
                New master key register status                : PARTFULL

Verification pattern for the entered key part is:

02010E4A64E0212A          (Record and secure this pattern)

Press END   to exit to the previous menu.

```

Figure 165. First Panel

Press PF3 to exit to the previous menu.

If your machine can only enter one key part at a time, return to the TKE workstation, refresh the crypto notebook, and then load the next key part to the queue.

Otherwise, import the key part to the DES new master key register.

Importing the Intermediate Master Key Part into the DES New Master Key Register

To import the intermediate master key part, follow the instructions:

The Enter New Master Key panel appears. See Figure 166 on page 168.

1. Select option 1, ENTER A KEY PART, to begin the key part entry steps.

```
CSFEKM00----- ICSF - TKE - Enter New Master Key -----  
OPTION ==> 1  
  
Coproprocessor selected for new master key : C0  
New master key register status : PARTFULL  
  
Enter the number of the desired option above.  
  
1 ENTER A KEY PART - Enter a key part into NMK register  
2 ENTER A FINAL KEY PART - Enter a final key part into NMK register  
3 RESTART KEY ENTRY PROCESS - Clear the NMK register
```

Figure 166. Selecting the Enter Key Part Option on the Enter New Master Key Panel

2. The Enter Master Key Part panel appears. See Figure 167.

```
CSFEKP10----- ICSF - TKE - Enter Master Key Part -----  
COMMAND ==>  
  
Coproprocessor selected for new master key : C0  
New master key register status : PARTFULL  
  
Press ENTER to load the key part.  
Press END to exit to the previous menu.
```

Figure 167. Enter Intermediate Master Key Part

3. Press ENTER and the Enter Master panel appears. See Figure 168..

```
CSFEKP20----- ICSF - TKE - Enter Master ----- KEY PART LOADED  
COMMAND ==>  
  
Coproprocessor selected for new master key : C0  
New master key register status : PARTFULL  
  
Verification pattern for the entered key part is:  
  
12B42031145E212B (Record and secure this pattern)  
  
Press END to exit to the previous menu.
```

Figure 168. Middle Panel

Press PF3 to exit to the previous menu.

If your machine can only enter one key part at a time, return to the TKE workstation, refresh the crypto notebook and then load the next key part to the queue. Otherwise, import the next key part to the DES new master key register.

Importing the Final Key Part into the DES New Master Key Register

The Enter Final Master Key Part panel appears. After you enter the first key part, and any intermediate key parts, you then enter the final master key part as explained here:

1. Select option 2, Enter a Final Key Part on the Enter New Master Key panel, as shown in Figure 169, and press ENTER.

```
CSFEKM00----- ICSF - TKE - Enter New Master Key -----  
OPTION ==> 2  
  
Coprocessor selected for new master key : C0  
New master key register status : PARTFULL  
  
Enter the number of the desired option above.  
  
1 ENTER A KEY PART - Enter a key part into NMK register  
2 ENTER A FINAL KEY PART - Enter a final key part into NMK register  
3 RESTART KEY ENTRY PROCESS - Clear the NMK register
```

Figure 169. Selecting to Enter a Final Key Part on the Enter New Master Key Panel

2. The Enter Final Master Key Part panel appears. See Figure 170.

```
CSFEKP10----- ICSF - TKE - Enter Final Master Key Part -----  
COMMAND ==>  
  
Coprocessor selected for new master key : C0  
New master key register status : PARTFULL  
  
Press ENTER to load the key part.  
Press END to exit to the previous menu.
```

Figure 170. Enter Final Master Key Part

3. Press ENTER.
The Enter Final panel appears. See Figure 171.

```
CSFEKP20---- ICSF - TKE - Enter Final Master Key Part -- KEY PART LOADED  
COMMAND ==>  
  
Coprocessor selected for new master key : C0  
New master key register status : FULL  
  
Verification pattern for the entered key part is:  
02010E4A64E0212A (Record and secure this pattern)  
  
Verification pattern for the new master key is:  
A864EC4210811AA2 (Record and secure this pattern)  
  
Press END to exit to the previous menu.
```

Figure 171. Final Panel

Press PF3 to exit to the previous menu. Remember to refresh the crypto notebook.

Changing Master Keys

For security reasons your installation should change the master keys periodically. In addition, if the master keys have been cleared, you may also want to change the master keys after you reenter the cleared master keys.

Tasks necessary for changing the master key are:

1. **Load to Queue** the DES new master key (first, middle, last)
 - **Load to Queue** requires you to import the key part(s) after loading. Whether you do it after each time a key part is loaded or load multiple key parts depends on your machine. (See “Importing Key Parts from the Queue” on page 163)
2. Load new SYM-MK (first, middle, last), if running PCICC
 - The new SYM-MK (on PCICC) must equal the DES new master key (on CCF)
3. Re-encipher CKDS
4. Change master key

The step-by-step procedure for changing the DES master key, reenciphering the CKDS, and activating the new DES master key is presented in “Changing the Master Key Using the Master Key Panels.” For information on the contents of the master key registers during the key change process, and some compatibility mode considerations, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

A DES master key and a CKDS containing keys enciphered under that DES master key already exist. Before you replace this existing DES master key with the new DES master key, you must reencipher the CKDS under the new DES master key.

If you are working with the CCF and changed the DES master key before, the previous DES master key was stored in the auxiliary (or new/old) master key register. The currently active DES master key exists in the master key register. When you enter the key parts of a new DES master key, they displace the previous DES master key in the auxiliary master key register. Therefore, the previous DES master key is lost.

When the DES master key is changed, the current active DES master key is moved to the auxiliary master key register and the new DES master key is moved to the master key register. In this way, the new DES master key you have just entered becomes the current DES master key, and the previous DES master key is stored in the auxiliary master key register.

Before the new DES master key is placed into the master key register, you must reencipher all disk copies of the CKDS under the new DES master key. Then you are ready to activate the master key. When you change the master key, you have ICSF replace the in-storage copy of the CKDS with the reenciphered disk copy and make the new master key active on the system.

Changing the Master Key Using the Master Key Panels

Load the key parts of the new master key that you want to replace the current master key. The new master key parts must be loaded from TKE. When changing the DES Master Key, **Load to Queue** should be used as ICSF is active in the selected domain. For information to do this procedure, see “Load and Load to

Queue - CCF” on page 110. You must also import each key part after loading to queue (see “Importing the First Master Key Part into the DES New Master Key Register” on page 164.

If you have PCICC crypto modules, you also need to load the same key parts to the new SYM-MK register. Make sure the hash pattern of the register matches the DES new master key register. See “Load - PCICC/PCIXCC/CEX2C” on page 126.

Note: The steps for this task are performed from your TSO logon id using the ICSF panels.

The new master key register on all crypto modules (CCF and PCICC) must be full before you change the master key.

1. Select option 2, MASTER KEY, on the ICSF Primary Menu.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----  
OPTION ==> 2
```

Enter the number of the desired option.

- | | | |
|---|------------------|--|
| 1 | COPROCESSOR MGMT | - Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - Installation options |
| 4 | ADMINCNTL | - Administrative Control Functions |
| 5 | UTILITY | - ICSF Utilities |
| 6 | PPINIT | - Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - TKE Master and Operational key processing |
| 8 | KGUP | - Key Generator Utility processes |
| 9 | UDX MGMT | - Management of User Defined Extensions |

Figure 172. Selecting the Master Key Option on the ICSF Primary Menu Panel

2. Before you change the master key, you must first reencipher the disk copy of the CKDS under the new master key. Select option 3, REENCIPHER CKDS, on the Master Key Management panel, as shown in Figure 173, and press ENTER.

```
CSFMKM00 ----- ICSF - Master Key Management -----  
OPTION ==> 3
```

Enter the number of the desired option above.

- | | | |
|---|-------------------|---|
| 1 | INIT/REFRESH CKDS | - Initialize a Cryptographic Key Data Set or activate an updated Cryptographic Key Data Set |
| 2 | SET MK | - Set a DES/Symmetric-Keys master key |
| 3 | REENCIPHER CKDS | - Reencipher the CKDS prior to changing the DES /Symmetric Keys master key |
| 4 | CHANGE MK | - Change the DES/Symmetric-Keys master key and activate the reenciphered CKDS |
| 5 | INITIALIZE PKDS | - Initialize or update a PKDS Cryptographic Key Data Set header record |
| 6 | REENCIPHER PKDS | - Reencipher the PKA Cryptographic Key Data Set |
| 7 | ACTIVATE PKDS | - Activate the PKDS after it has been reenciphered |
| 8 | REFRESH CACHE | - Refresh the PKDS cache if enabled |

Figure 173. Selecting the Change Master Key Option on the ICSF Master Key Management Panel

3. The Reencipher CKDS panel appears. See Figure 174.

```
CSFCMK10 ----- ICSF - Reencipher CKDS -----  
COMMAND ==>  
  
To reencipher all CKDS entries from encryption under the current DES/  
Symmetric-Keys master key to encryption under the new master key enter  
the CKDS names below.  
  
Input CKDS ==> CKDS.CURRENT.MASTER  
  
Output CKDS ==> CKDS.NEW.MASTER
```

Figure 174. Reencipher CKDS

4. In the Input CKDS field, enter the name of the CKDS that you want to reencipher. In the Output CKDS field, enter the name of the data set in which you want to place the reenciphered keys.

Note: The output data set should already exist although it must be empty. For more information about defining a CKDS, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

Reenciphering the disk copy of the CKDS does not affect the in-storage copy of the CKDS. On this panel, you are working with only a disk copy of the CKDS.

5. Press ENTER to reencipher the input CKDS entries and place them into the output CKDS.
The message REENCIPHER SUCCESSFUL appears on the top right of the panel if the reencipher succeeds.
6. If you have more than one CKDS on disk, specify the information and press ENTER as many times as you need to reencipher all of them. Reencipher all your disk copies at this time. When you have reenciphered all the disk copies of the CKDS, you are ready to change the master key.
7. Press END to return to the Master Key Management panel.
 - a. Changing the master key involves refreshing the in-storage copy of the CKDS with a disk copy and activating the new master key.
 - b. If you are running in compatibility or co-existence mode, *do not* select option 4, the Change option. To activate the changed master key when running in compatibility or co-existence mode, you need to re-IPL MVS and start ICSF. When you re-IPL MVS and start ICSF, you activate the changed master key and refresh the in-storage CKDS. To do this, you must exit the panels at this time.
 - c. If you are running in noncompatibility mode, to change the master key select option 4 on the Master Key Management panel, as shown in Figure 175 on page 173.

```
CSFMKM00 ----- ICSF - Master Key Management -----  
OPTION ==> 4
```

Enter the number of the desired option above.

- 1 INIT/REFRESH CKDS - Initialize a Cryptographic Key Data Set or activate an updated Cryptographic Key Data Set
- 2 SET MK - Set a DES/Symmetric-Keys master key
- 3 REENCIPHER CKDS - Reencipher the CKDS prior to changing the DES /Symmetric Keys master key
- 4 CHANGE MK - Change the DES/Symmetric-Keys master key and activate the reenciphered CKDS
- 5 INITIALIZE PKDS - Initialize or update a PKDS Cryptographic Key Data Set header record
- 6 REENCIPHER PKDS - Reencipher the PKA Cryptographic Key Data Set
- 7 ACTIVATE PKDS - Activate the PKDS after it has been reenciphered
- 8 REFRESH CACHE - Refresh the PKDS cache if enabled

Figure 175. Selecting the Change Master Key Option on the ICSF Master Key Management Panel

8. When you press the ENTER key, the Change Master Key panel appears. See Figure 176.

```
CSFCMK20 ----- ICSF - Change Master Key -----  
COMMAND ==>
```

Enter the name of the new CKDS below:

New CKDS ==> CKDS.NEW.MASTER

When the master key is changed, the new CKDS will become active.

Figure 176. Change Master Key Panel

9. In the New CKDS field, enter the name of the disk copy of the CKDS that you want in storage.
You should have already reenciphered the disk copy of the CKDS under the new master key. The last CKDS name that you specified in the Output CKDS field on the Reencipher CKDS panel, which is shown in Figure 174 on page 172, automatically appears in this field.
10. Press ENTER.
ICSF loads the data set into storage where it becomes operational on the system. ICSF also places the new master key into the master key register so it becomes active.
After you press ENTER, ICSF attempts to change the master key. It displays a message on the top right of the panel. The message indicates either that the master key was changed successfully or that an error occurred that did not permit the change process to be completed. For example, if you indicate a data set that is not reenciphered under the new master key, an error message displays and the master key is not changed.

Restarting the DES Key Entry Process

If you realize you made an error when loading a key part, you can restart the process of loading the new master key. Restarting the key entry process causes the new master key register to be cleared, which means all the new master key parts you entered previously are erased.

PCICC registers can be cleared from the TKE workstation. See “Clear - PCICC/PCIXCC/CEX2C” on page 130.

This describes the procedure for clearing the DES new master key register in the CCF.

Note: When you enter the first key part, your old master key is lost, even if you restart the process.

To restart the key entry process, follow these steps using ICSF from your TSO logon id:

1. Select option 7, TKE, on the ICSF Primary Option Menu.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----  
OPTION ==> 7
```

Enter the number of the desired option.

- | | | |
|---|------------------|--|
| 1 | COPROCESSOR MGMT | - Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - Installation options |
| 4 | ADMINCTL | - Administrative Control Functions |
| 5 | UTILITY | - ICSF Utilities |
| 6 | PPINIT | - Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - TKE Master and Operational key processing |
| 8 | KGUP | - Key Generator Utility processes |
| 9 | UDX MGMT | - Management of User Defined Extensions |

Figure 177. Selecting the TKE Option on the ICSF Primary Menu Panel

2. The TKE Processing Selection panel appears. Select option 1, DES master key entry.

```
CSF0PK00 ----- ICSF - TKE Processing Selection -----  
OPTION ==> 1
```

Enter the number of the desired option.

- | | |
|---|---------------------------|
| 1 | DES Master key entry |
| 2 | DES Operational key entry |
| 3 | PKA key entry |

Figure 178. Selecting the DES Master Key entry on the TKE Processing Selection Panel

3. The Coprocessor Selection panel, which may be similar to the one in Figure 179 on page 175, appears. Select the coprocessor for master key entry by typing the coprocessor number on the OPTION line and pressing ENTER.

Note: If you have only one coprocessor installed, or if there is only one coprocessor defined to this partition, this panel will only show one coprocessor.

```

CSFCMP20 ----- ICSF - TKE Coprocessor Selection -----
OPTION ==> 0

CRYPTO DOMAIN: 0

Enter the number of the coprocessor to be used for key entry.

REGISTER STATUS          0. COPROCESSOR C0          1. COPROCESSOR C1

Crypto Module ID          : E589C39694407A60          : C39997A396F1407A
                          : 5D40C39997A396F0          : 605D40E589C39694
New Master Key register   : FULL                      : FULL
NMK verification pattern  : 0212570BB5E544C1          : 0212570BB5E544C1
Old Master Key register   : EMPTY                     : EMPTY
OMK verification pattern  :                          :
Old/New Master Key register: 3DDAE6229901A0C5          : 5B82229C87F044C3
  hash pattern           : 3C8BE367C85054C0          : DA6544F00CC43D46
Master Key register       : VALID                     : VALID
MK verification pattern   : CA6B408A02371B1D          : CA6B408A02371B1D
Master Key register       : DF3A50AE5466123A          : DF3A50AE5466123A
  hash pattern           : 96EF57E8BD074557          : 96EF57E8BD074557
Special Secure Mode       : ENABLED                   : ENABLED
Environment Control Mask  : F3FEFCF0                  : F3FEFCF0

Press ENTER to select coprocessor and proceed to new master key part entry.
Press END  to exit to the previous menu.

```

Figure 179. Selecting a Coprocessor for Master Key Entry

4. Choose option 3, the RESTART KEY ENTRY PROCESS option, on the Enter New Master Key panel, as shown in Figure 180.

```

CSFEKM00----- ICSF - TKE - Enter New Master Key -----
OPTION ==> 3

Coprocessor selected for new master key : C0
New master key register status          : FULL

Enter the number of the desired option above.

1 ENTER A KEY PART          - Enter a key part into NMK register
2 ENTER A FINAL KEY PART    - Enter a final key part into NMK register
3 RESTART KEY ENTRY PROCESS - Clear the NMK register

```

Figure 180. Selecting the Restart Key Entry Process Option on the Enter New Master Key Panel

When you choose option 3, the Confirm Restart Request panel appears. See Figure 181 on page 176.

```
CSFEKM30----- ICSF - Confirm Restart Request -----  
COMMAND ===>
```

ARE YOU SURE YOU WISH TO RESTART THE KEY ENTRY PROCESS?

Restarting the process will clear the new master key register.

Press ENTER to confirm restart request
Press END to cancel restart request

Figure 181. Confirm Restart Request Panel

This panel confirms your request to restart the key entry process.

5. If you want to restart the key entry process, press ENTER.
The restart request automatically empties the key part register and new master key register.
6. If you do not want to restart, press END.
After you make a choice, you return to Figure 180 on page 175.
7. Either begin the key entry process again or exit that panel to return to the ICSF primary menu panel.

Re-entering Master Keys After They have been Cleared

In certain situations, the Cryptographic Coprocessor Feature clears the master key registers so that the master key values are not disclosed. Master keys are cleared in these situations:

- If the Cryptographic Coprocessor Feature detects tampering
- If you issue a command from the TKE workstation to zeroize a domain
- If you issue a command from the Support Element to zeroize a domain

In these situations, the PCI Cryptographic Coprocessor Feature (PCICC) clears the master key registers so that the master key values are not disclosed:

- If the PCI Cryptographic Coprocessor Feature detects tampering (the intrusion latch is tripped), ALL installation data is cleared: master keys, retained keys for all domains, as well as roles and profiles.
- If the PCI Cryptographic Coprocessor Feature detects tampering (the secure boundary of the card is compromised), it self-destructs and can no longer be used.
- If you issue a command from the TKE workstation to zeroize a domain
This command zeroizes the data specific to a domain: master keys and retained keys.
- If you issue a command from the Support Element panels to zeroize all domains.
This command zeroizes ALL installation data: master keys, retained keys and access control roles and profiles.

Although the values of the master keys are cleared, the keys in the CKDS are still enciphered under the cleared DES master key. The RSA and DSS private key are

also each enciphered under one of the cleared PKA master keys. Therefore, to recover the keys in the CKDS, and the PKA private keys in the PKDS, you must reenter the same master keys and activate the DES master key. For security reasons, you may then want to change all the master keys.

PR/SM Considerations

If you are running in PR/SM logical partition (LPAR) mode, the Cryptographic Coprocessor Feature causes all logical partitions (LPs) to lose their master keys only for a tamper situation. In this case, you must ensure that key entry is enabled for each LP on the Change LPAR Crypto page on the support element Hardware Master Console and then reenter the master keys in each LP. If you have a PCICC, you also need to regenerate any retained keys. If you zeroize a domain using the TKE workstation, however, the master keys are cleared only in that domain. Master keys in other domains are not affected and do not need to be reentered. For more information about reentering master keys in LPAR mode, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

Setting the Master Key

After the master keys have been cleared, reenter the same master keys by following these steps:

1. Load new master key parts. For details on loading the keys, see “Load and Load to Queue - CCF” on page 110.

These values should be stored in a secure place as specified in your enterprise security process.

2. Retrieve the key parts, checksums, verification patterns, and hash patterns you used when you loaded the master keys originally. These values should have been stored in a secure place.
3. To activate the DES master key you just entered, you need to set it. On the ICSF Primary Menu panel in TSO, select option 2.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----  
OPTION ==> 2
```

Enter the number of the desired option.

- | | | |
|---|------------------|--|
| 1 | COPROCESSOR MGMT | - Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - Installation options |
| 4 | ADMINCTL | - Administrative Control Functions |
| 5 | UTILITY | - ICSF Utilities |
| 6 | PPINIT | - Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - TKE Master and Operational key processing |
| 8 | KGUP | - Key Generator Utility processes |
| 9 | UDX MGMT | - Management of User Defined Extensions |

Figure 182. ICSF Selecting the Master Key Option on the Primary Menu Panel

4. To set the DES master key, choose option 2 on the panel and press ENTER.

```

CSFMKM00 ----- ICSF - Master Key Management -----
OPTION ==> 2

Enter the number of the desired option above.

1 INIT/REFRESH CKDS - Initialize a Cryptographic Key Data Set or
                    - activate an updated Cryptographic Key Data Set
2 SET MK             - Set a DES/Symmetric-Keys master key
3 REENCIPHER CKDS   - Reencipher the CKDS prior to changing the DES
                    - /Symmetric Keys master key
4 CHANGE MK          - Change the DES/Symmetric-Keys master key and
                    - activate the reenciphered CKDS

5 INITIALIZE PKDS    - Initialize or update a PKDS Cryptographic
                    - Key Data Set header record
6 REENCIPHER PKDS    - Reencipher the PKA Cryptographic Key Data Set
7 ACTIVATE PKDS      - Activate the PKDS after it has been reenciphered
8 REFRESH CACHE      - Refresh the PKDS cache if enabled

```

Figure 183. Selecting the Set Host Master Key Option on the ICSF Master Key Management Panel

After you select option 2, ICSF checks that the states of the registers are correct. ICSF then transfers the DES master key from the new master key register to the master key register. This process sets the DES master key.

When ICSF attempts to set the DES master key, it displays a message on the top right of the Master Key Management panel. The message indicates either that the master key was successfully set, or that an error prevented the completion of the set process.

5. If your system is using two Cryptographic Coprocessor Features, ICSF sets the DES master key for each Cryptographic Coprocessor Feature whose new DES master key enciphers the in-storage CKDS. You should reenter the DES master key into the new master key register for each of the Cryptographic Coprocessor Features.

When you set the reentered DES master key, the DES master key that enciphers the existing CKDS now exists.

6. You can now change the DES master key, if you choose to, for security reasons. Continue with “Changing Master Keys” on page 170.

Adding Cryptographic Coprocessors After ICSF Initialization

There may come a time when you wish to add additional PCI Cryptographic Coprocessors (PCICC) to your system or may have one Cryptographic Coprocessor feature (CCF) and wish to add the second. 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.

Note: With TKE V4.0 or later, it is no longer necessary to exit the application to add new crypto modules.

CCF

1. Open the Host where the crypto module was added. You will be prompted to authenticate the crypto module.
2. Open the new crypto module.

3. Use the default signature key to administer access control and load authority signature keys to match the other crypto module.
4. Load the keys. Use **Load to Queue**. (You must import each key part from the key part queue from ICSF.)

Note: The keys should be the same keys that you loaded to the other crypto module.

5. If loading PKA master keys, disable PKA services (see “Disabling PKA Services” on page 180).
6. Set the master keys as outlined in “Setting the Master Key” on page 177.
7. Enable PKA Callable Services if you had previously disabled the services. Also enable PKDS Reads and Writes.
8. If desired, add the new crypto module to the group by doing a group change.

PCICC

Note: With TKE V4.0 or later, it is no longer necessary to exit the application to add new crypto modules.

1. Open the Host where the crypto module(s) were added. You will be prompted to authenticate the crypto module.
2. Open the new crypto module(s).
3. Use the authority 0 default signature key to administer access control (create the same roles and authorities for the new PCICC to match the PCICC currently on the host). Load the authority signature keys to match the other crypto modules.
4. Load a new signature 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 signature keys.
5. Load the keys. The new symmetric master key must match the DES new master key value on the CCF. The new asymmetric master key must match the SMK value on the CCF.

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 new symmetric master key on the PCICC from ICSF (see “Setting the Master Key” on page 177) when everything is the same (roles, authorities, controls, master keys).
7. Set the new asymmetric master key from TKE.
8. If desired, add the new PCICC(s) to the group by doing a group change.

PKA Master Key Parts

When you enter the PKA master keys the first time, the PKA callable services are initially disabled. Once you have entered the PKA master keys, you must enable the PKA callable services for these services to work. Before you change the PKA master keys, you need to disable the PKA callable services. To enable and disable the PKA callable services refer to “Disabling PKA Services” on page 180.

To enter a PKA master key, you can either enter a complete key, a first key part and a final key part or a first key part, an intermediate key part and a final key part.

After you enter a key part for a DES or PKA master key the Cryptographic Coprocessor Feature calculates a sixteen-byte hash pattern. The hash patterns are displayed in a pop-up window for the administrator to verify. You can use the hash pattern to verify that the key parts were entered correctly.

Tasks necessary for changing the PKA master keys are listed here. Note that steps 2 through 8 are done at the TKE workstation.

Note: You must have at least one PCICC on the system to change your PKA Master Keys. The PCICC is required to perform the PKDS Reencipher.

1. Disable PKA Services
2. Clear SMK (*if not empty*)
3. Clear KMMK (*if not empty*)
4. Load SMK — first, middle, last
5. Load KMMK — first, middle, last
6. Clear New ASYM-MK (*if not empty*)
7. Load New ASYM-MK — first, middle, last
8. Set ASYM-MK
9. PKDS Reencipher under the new PKA Master Key
10. PKDS Activate
11. Enable PKA Services
12. Enable PKDS Reads/Writes

We highly recommend that you set SMK=KMMK to maximize routing. The ASYM-MK on the PCICC must equal the SMK on the CCF.

Disabling PKA Services

When you enter or change the PKA master keys, the PKA services should first be disabled. To disable PKA services:

1. From TSO, access the user control functions by choosing option 4, ADMINCNTL, on the Primary Menu panel of ICSF, as shown in Figure 184.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----
OPTION ==> 4
```

Enter the number of the desired option.

- | | | | |
|---|------------------|---|--|
| 1 | COPROCESSOR MGMT | - | Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - | Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - | Installation options |
| 4 | ADMINCNTL | - | Administrative Control Functions |
| 5 | UTILITY | - | ICSF Utilities |
| 6 | PPINIT | - | Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - | TKE Master and Operational key processing |
| 8 | KGUP | - | Key Generator Utility processes |
| 9 | UDX MGMT | - | Management of User Defined Extensions |

Figure 184. Selecting the Administrative Control Option on the ICSF Primary Menu Panel

2. The Administrative Control Function panel appears. See Figure 185 on page 181.

```

CSFACF00 ----- ICSF Administrative Control Functions
COMMAND ==>
    Active CKDS: CSF.CKDS
    Active PKDS: CSF.PKDS
    Active TKDS: CSF.TKDS

To change the status of a control, enter the appropriate character
(E - ENABLE, D - DISABLE) and press ENTER.

      Function                                STATUS
      -----                                -
.  Dynamic CKDS Access                        ENABLED
D  PKA Callable Services                     ENABLED
.  PKDS Read Access                          ENABLED
.  PKDS Write, Create, and Delete Access      ENABLED

```

Figure 185. Disabling the PKA Callable Services

3. Type a 'D' to the left of the functions you want disabled and press ENTER.

Note: Disabling PKA Callable Services automatically disables PKDS Read/Write/Create/Delete access as well.

Enabling PKA Services

After you enter or change the PKA master keys, the PKA services should be enabled. To enable PKA services:

1. From TSO, access the user control functions by choosing option 4, ADMINCNTL, on the Primary Menu panel of ICSF, as shown in Figure 186.

```

CSF@PRIM ----- Integrated Cryptographic Service Facility -----
OPTION ==> 4

Enter the number of the desired option.

 1 COPROCESSOR MGMT - Management of Cryptographic Coprocessors
 2 MASTER KEY       - Master key set or change, CKDS/PKDS processing
 3 OPSTAT           - Installation options
 4 ADMINCNTL        - Administrative Control Functions
 5 UTILITY           - ICSF Utilities
 6 PPINIT           - Pass Phrase Master Key/CKDS Initialization
 7 TKE              - TKE Master and Operational key processing
 8 KGUP             - Key Generator Utility processes
 9 UDX MGMT         - Management of User Defined Extensions

```

Figure 186. Selecting the Administrative Control Option on the ICSF Primary Menu Panel

2. The Administrative Control Function panel appears. See Figure 187 on page 182.

```

CSFACF00 ----- ICSF Administrative Control Functions
COMMAND ===>
      Active CKDS: CSF.CKDS
      Active PKDS: CSF.PKDS
      Active TKDS: CSF.TKDS

To change the status of a control, enter the appropriate character (E - ENABLE,
D - DISABLE) and press ENTER.

      Function                                STATUS
      -----                                -
      . Dynamic CKDS Access                  ENABLED
E PKA Callable Services                     DISABLED
E PKDS Read Access                         DISABLED
E PKDS Write, Create, and Delete Access     DISABLED

```

Figure 187. Enabling and Disabling the PKA Callable Services

3. Enter the option and press ENTER.
 - To enable the PKA callable services, type an 'E' before the function. Press ENTER.
 - To enable PKDS Read Access, type an 'E' before the function. Press ENTER.
 - To enable PKDS Write Access, type an 'E' before the function. Press ENTER.

Resetting PKA Master Keys

If you realize that you have made a mistake entering key parts to either PKA master key register, you are able to reset the value in the register to zero. From the TKE workstation, access the domain window (see “Domain Keys Page - CCF” on page 105 and “Domains Keys Page (PCICC and PCIXCC/CEX2C)” on page 121). Select the appropriate PKA master key and then select **Clear**.

If changing the PKA master keys, you should clear out the current PKA key values by resetting the values to zero.

Notes:

1. Once the PKA master keys have been changed, internal tokens in the PKDS are unusable. You will need to reencipher and activate the PKDS in order to use them with the changed master key. This requires a PCICC on your system. See “Reenciphering and Activating the PKDS.”
2. For RSA keys loaded into the PKDS from the TKE workstation, the process can be repeated to load the keys under the changed PKA master keys. See “Load RSA Key to PKDS - CCF” on page 120 and “Installing RSA Keys in the PKDS from a Dataset” on page 193 for details.

Reenciphering and Activating the PKDS

For security reasons, your installation should periodically change the PKA master keys and reencipher the private keys. Reenciphering and activating the PKDS automatically refreshes the PKDS cache, as does starting ICSF.

You must have a PCICC to perform the reencipher. PKA keys should NOT be changed if a PCICC is not available.

To reencipher the PKDS after the PKA SMK and ASYM-MK have been changed, go to the Master Key Management panel and select option 6.

Note: Only keys enciphered under the SMK and the ASYM-MK are reenciphered. PKDS reencipher will not be able to reencipher private keys encrypted under the CCF key management master key (KMMK) if the KMMK does not equal the SMK.

```
CSFCMK00 ----- ICSF - Master Key Management -----
OPTION ==> 6

Enter the number of the desired option.

1 INIT/REFRESH CKDS - Initialize a Cryptographic Key Data Set or
                    - activate an updated Cryptographic Key Data Set
2 SET MK             - Set a DES/Symmetric-Keys master key
3 REENCIPHER CKDS    - Reencipher the CKDS prior to changing the DES
                    - /Symmetric Keys master key
4 CHANGE MK          - Change the DES/Symmetric-Keys master key and
                    - activate the reenciphered CKDS

5 INITIALIZE PKDS    - Initialize or update a PKDS Cryptographic
                    - Key Data Set header record
6 REENCIPHER PKDS    - Reencipher the PKA Cryptographic Key Data Set
7 ACTIVATE PKDS      - Activate the PKDS after it has been reenciphered
8 REFRESH CACHE      - Refresh the PKDS cache if enabled
```

Figure 188. Selecting the Reencipher PKDS Option on the Master Key Management Panel

The Reencipher PKDS panel appears. In the Input PKDS field, specify the name of the PKDS that you want ICSF to reencipher under the current SMK and ASYM-MK.

In the Output PKDS field, specify the name of an empty VSAM data set. ICSF writes the reenciphered keys to this data set.

```
CSFCMK11 ----- ICSF - Reencipher PKDS -----
COMMAND ==>

To reencipher all PKDS entries from encryption under the old signature/
asymmetric-keys master key to encryption under the current master key,
enter the PKDS names below.

Input  PKDS ==>

Output PKDS ==>

Press ENTER to reencipher the PKDS.
Press END  to exit to the previous menu
```

Figure 189. Reencipher PKDS

Press enter to reencipher the PKDS. Reenciphering automatically refreshes the PKDS cache. Once successful, you will then want to activate the PKDS. Return to the Master Key Management panel and select option 7.

```

CSFMKM00 ----- ICSF - Master Key Management -----
OPTION ==>7

Enter the number of the desired option.

 1 INIT/REFRESH CKDS - Initialize a Cryptographic Key Data Set or
                       activate an updated Cryptographic Key Data Set
 2 SET MK             - Set a DES/Symmetric-Keys master key
 3 REENCIPHER CKDS    - Reencipher the CKDS prior to changing the DES
                       /Symmetric Keys master key
 4 CHANGE MK          - Change the DES/Symmetric-Keys master key and
                       activate the reenciphered CKDS

 5 INITIALIZE PKDS    - Initialize or update a PKDS Cryptographic
                       Key Data Set header record
 6 REENCIPHER PKDS    - Reencipher the PKA Cryptographic Key Data Set
 7 ACTIVATE PKDS      - Activate the PKDS after it has been reenciphered
 8 REFRESH CACHE      - Refresh the PKDS cache if enabled

```

Figure 190. Selecting the Activate PKDS Option on the Master Key Management Panel

The Activate PKDS panel appears. Enter the name of the PKDS that you want ICSF to use. The PKDS must have already been reenciphered under the current Signature/Asymmetric-keys master key.

```

CSFCMK21 ----- ICSF - Activate PKA Cryptographic Key Data Set -----
COMMAND ==>

Enter the name of the new PKDS below.

New PKDS ==>

Press ENTER to activate the PKDS.
Press END to exit to the previous menu

```

Figure 191. Activate PKDS

After you press ENTER, the PKDS becomes active. Activation automatically refreshes the PKDS cache.

Loading and Importing Operational Keys

From the TKE workstation, you can load key parts for operational (PIN and transport) keys into a key part queue. To import these key parts into the CKDS, you must also use the ICSF Operational Key panel and perform a CKDS refresh.

Note: Depending on your machine type, the key part queue may only have room for one entry. You must import the key part using the ICSF panels.

When loading and importing an operational key part, a first and final key part are required. One or more intermediate key parts are optional. See “Importing the First Operational Key Part” on page 185, “Importing Intermediate Operational Key Parts” on page 189, and “Importing the Final Operational Key Part” on page 190.

Importing Key Parts Individually

This procedure involves loading and importing two or more key parts individually and is divided into these tasks:

1. Loading the first operational key part (TKE workstation)
2. Importing the first operational key part (ICSF panels)
3. Refresh the crypto notebook (TKE workstation)
4. Loading intermediate operational key part (TKE workstation)*
5. Importing intermediate operational key part (ICSF panels)*
6. Refresh the crypto notebook (TKE workstation)*
7. Loading the final operational key part (TKE workstation)
8. Importing the final operational key part (ICSF panels)
9. Refresh the crypto notebook (TKE workstation)
10. Refresh the CKDS (ICSF panels)

Note: * If you are loading more than one intermediate key part, steps 4, 5 and 6 can be repeated.

Importing Multiple Key Parts

This procedure involves loading and importing multiple key parts and is divided into these tasks:

1. Loading the first operational key part (TKE workstation)
2. Loading intermediate operational key part (TKE workstation)
3. Loading the final operational key part (TKE workstation)
4. Importing the first operational key part (ICSF panels)
5. Importing intermediate operational key part (ICSF panels)
6. Importing the final operational key part (ICSF panels)
7. Refresh the crypto notebook (TKE workstation)
8. Refresh the CKDS (ICSF panels)

Importing the First Operational Key Part

Note: The process of importing operational key parts from the key part queue is performed from your TSO logon id using the ICSF panels.

To begin importing the first operational key part, start at the ICSF main menu and follow these instructions:

1. Select option 7, TKE, on the primary menu panel, as shown in Figure 192.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----  
OPTION ==> 7
```

Enter the number of the desired option.

- | | | | |
|---|------------------|---|--|
| 1 | COPROCESSOR MGMT | - | Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - | Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - | Installation options |
| 4 | ADMINCTL | - | Administrative Control Functions |
| 5 | UTILITY | - | ICSF Utilities |
| 6 | PPINIT | - | Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - | TKE Master and Operational key processing |
| 8 | KGUP | - | Key Generator Utility processes |
| 9 | UDX MGMT | - | Management of User Defined Extensions |

Figure 192. Selecting the TKE Option on the ICSF Primary Menu Panel

- The TKE Processing Selection panel appears. Select option 2, DES Operational key entry.

Note: You must have read access to the resource CSFMVR otherwise the operation will fail.

```
CSFOPK00 ----- ICSF - TKE Processing Selection -----
OPTION ==> 2
```

Enter the number of the desired option.

- 1 DES Master key entry
- 2 DES Operational key entry
- 3 PKA key entry

Figure 193. Selecting the DES Operational Key entry on the TKE Processing Selection Panel

- The Coprocessor Selection panel appears:

```
CSFCMP20 ----- ICSF - TKE Coprocessor Selection -----
OPTION ==> 0
```

CRYPTO DOMAIN: 0

Enter the number of the coprocessor to be used for key entry.

REGISTER STATUS	0. COPROCESSOR C0	1. COPROCESSOR C1
Crypto Module ID	: E589C39694407A60	: C39997A396F1407A
	: 5D40C39997A396F0	: 605D40E589C39694
New Master Key register	: EMPTY	: EMPTY
NMK verification pattern	:	:
Old Master Key register	: VALID	: VALID
OMK verification pattern	: 0212570BB5E544C1	: 0212570BB5E544C1
Old/New Master Key register:	3DDAE6229901A0C5	: 5B82229C87F044C3
hash pattern	: 3C8BE367C85054C0	: DA6544F00CC43D46
Master Key register	: VALID	: VALID
MK verification pattern	: CA6B408A02371B1D	: CA6B408A02371B1D
Master Key register	: DF3A50AE5466123A	: DF3A50AE5466123A
hash pattern	: 96EF57E8BD074557	: 96EF57E8BD074557
Special Secure Mode	: ENABLED	: ENABLED
Environment Control Mask	: F3FEFCF0	: F3FEFCF0

Press ENTER to select coprocessor and proceed to new master key part entry.
Press END to exit to the previous menu.

Figure 194. Selecting a Coprocessor for Operational Key Entry

- Select a coprocessor. The Operational Key Input panel appears (Figure 195 on page 187).

```

CSFSCK10 ----- ICSF - TKE - Operational Key Input -----
COMMAND ==>

                                Coprocessor selected for new key   : C0

Enter the dataset name and the key specifications.

CKDS name ==> 'S09.CKDS'
Key label ==> S09.EXPORTER.KEY1
Key type ==>                               Selection panel displayed if blank
Key part ==> FIRST                          FIRST, MIDDLE or FINAL

For FINAL key part enter the following information.

Adjust parity      ==>                               YES or NO
Control Vector    ==>                               YES or NO
Installation data ==>

Press ENTER to select the dataset and the key.
Press END  to exit to the previous menu.

```

Figure 195. Operational Key Input Panel - First Key Part

All the panels for entering key parts show status information at the top. The coprocessor you selected before entering key parts, either 0 or 1, is displayed.

- a. In the CKDS name field, enter the name of the disk copy of the CKDS in which you want the key parts and, eventually, the entire key to be stored. This CKDS name field defaults to the name of the disk copy of the CKDS last used to refresh the in-storage CKDS.
- b. In the Key label field, specify the label of the entry on the CKDS in which the key parts and, eventually, the entire key will be stored.
- c. In the Key type field, enter the type of key you want to enter.

You can enter any of these types of keys:

EXPORTER	Exporter key-encrypting key
IMP-PKA	Limited Authority Importer Key
IMPORTER	Importer key-encrypting key
PINGEN	PIN generation key
PINVER	PIN verification key
IPINENC	Input PIN-encrypting key
OPINENC	Output PIN-encrypting key

If you leave the field blank and press ENTER, the Key Type Selection panel appears. See Figure 196 on page 188.

- d. Type *s* to the left of the key type you want to specify from the displayed list of key types and press ENTER.

In Figure 196 on page 188, the EXPORTER key is selected.

```

CSFCSE12 ----- ICSF - Key Type Selection Panel ----- ROW 1 OF 7
COMMAND ===> SCROLL ===> PAGE

Select one key type only
  KEY TYPE      DESCRIPTION
s EXPORTER      Export key encrypting key
  IMP-PKA       Limited Authority importer key
  IMPORTER      Import key encrypting key
  IPINENC       Input PIN encrypting key
  OPINENC       Output PIN encrypting key
  PINGEN        PIN generation key
  PINVER        PIN verification key
***** BOTTOM OF DATA *****

```

Figure 196. Selecting a Key Type on the Key Type Selection Panel

- e. In the Key part field, enter FIRST for the first key part.

Figure 197 shows an example of the Operational Key Input panel filled in for a first key part.

The Operational Key Input panel appears. See Figure 197.

```

CSFSCK30----- ICSF - TKE - Operational Key Input -----
COMMAND ===>

                                Coprocessor selected for new key      : C0

Enter a verification pattern. (optional)
VP ==> 0000000000000000

Press ENTER after the key has been entered.
Press END   to exit to the previous menu.

```

Figure 197. Operational Key Input Panel - Key Part Register Status for First Part

5. Enter the verification pattern if desired, and press ENTER.

Pressing ENTER on the Operational Key Input panel reads the key part from the key part queue and loads the key part into the CKDS.

Since you are entering the first key part, the key label on the CKDS should not already exist. ICSF will create an entry with the key label you specify.

However, if you specified a key label that already exists, the Operational Key Input panel appears. See Figure 198 on page 189.

Note: This panel will only appear if the key represented by the existing label is a null key or a partial key (the final key has not been entered). If the label represents a complete key then an error message **NOT A PARTIAL KEY** will appear in the upper right corner of the panel.

```
CSFSCK40 ----- ICSF - TKE - Operational Key Input -----  
COMMAND ===>  
  
A record with the following specifications has been found in the selected CKDS:  
  
Key label   : S09.EXPORTER.KEY1  
Key type    : EXPORTER  
  
  
  
  
  
  
  
  
  
Press ENTER to replace the existing record.  
Press END   to exit to the previous menu.
```

Figure 198. Operational Key Input Panel

This panel alerts you that even though you are entering the first key part, an entry in the CKDS under the label you specified already exists. The panel displays the key label and key type for the entry.

6. If you want to replace the existing key with the new key you are about to enter, press ENTER.

The new key value will replace the existing key under that label in the CKDS.

You have completed the process of importing the first key part. Therefore, the first key part has been transferred from the key part queue to the key label you specified on the CKDS. When you load and import the next key part, it will be combined with the first key part in the CKDS.

You are now ready to load and import a middle or final key part. A first and final key part are required for an operational key. Any intermediate key parts are optional.

If your machine can only handle one key part on the queue, return to the TKE workstation, refresh the crypto notebook, and load the next key part. Otherwise, import the next key part using the appropriate ICSF panels.

Importing Intermediate Operational Key Parts

If you have loaded an intermediate key part from TKE, follow this procedure to import the intermediate key part to the CKDS.

1. In the key part field on the Operational Key Input panel, specify MIDDLE, as shown in Figure 199 on page 190, and press ENTER.

```

CSFSCK10 ----- ICSF - TKE - Operational Key Input -----
COMMAND ==>

                                Coprocessor selected for new key      : C0

Enter the dataset name and the key specifications.

CKDS name ==> 'S09.CKDS'
Key label ==> S09.EXPORTER.KEY1
Key type  ==> EXPORTER      Selection panel displayed if blank
Key part  ==> MIDDLE        FIRST, MIDDLE or FINAL

Press ENTER to select the dataset and the key.
Press END   to exit to the previous menu.

```

Figure 199. Operational Key Input Panel - Middle Key Part

Figure 200 appears.

```

CSFSCK30----- ICSF - TKE - Operational Key Input -----
COMMAND ==>

                                Coprocessor selected for new key      : C0

Enter a verification pattern. (optional)
VP ==> 0000000000000000

Press ENTER after the key has been entered.
Press END   to exit to the previous menu.

```

Figure 200. Operational Key Input Panel - Key Part Register Status for Middle Part

2. Press enter.

If your machine can only handle one key part on the queue, return to the TKE workstation, refresh the crypto notebook, and load the next key part to the queue. Import the key part using the appropriate ICSF panels.

Importing the Final Operational Key Part

To import a final operational key part, follow these steps:

1. In the Key part field on the Operational Key Input panel, specify FINAL.


```

CSFSCK10 ----- ICSF - Operational Key Input -----
COMMAND ==>

                                Coprocessor selected for new key                : C0

Enter the dataset name and the key specifications.

CKDS name ==> 'S09.CKDS'
Key label ==> S09.EXPORTER.KEY1
Key type ==> EXPORTER      Selection panel displayed if blank
Key part ==> FINAL        FIRST, MIDDLE or FINAL

For FINAL key part enter the following information.

Adjust parity      ==> YES          YES or NO
Control Vector    ==> YES          YES or NO
Installation data ==> EXPORTER A TO B INSTALLED 03/01/99

Press ENTER to select the dataset and the key.
Press END  to exit to the previous menu.

```

Figure 201. Operational Key Input Panel - Final Key Part

2. In the Adjust parity field, specify YES if you want ICSF to adjust the parity to odd.

Any key generated on ICSF has odd parity. However, ICSF allows you to enter a key with odd or non-odd parity. A key with non-odd parity will function on ICSF but ICSF will return an even parity reason code for many functions in which the key is used. Although ICSF runs with odd or non-odd parity, your installation may choose to run with just odd parity keys.

3. In the Control Vector field, specify YES or NO.

For all types of keys except transport keys, specify YES. If you want to enter a transport key, you can specify either YES or NO. If you specify NO, the transport key is flagged for use in NOCV processing. In NOCV processing, ICSF uses the transport key itself rather than a transport key variant to encrypt keys. NOCV processing is used to exchange keys with products that do not use control vectors.

4. In the Installation data field, enter any information your installation wants to specify about the key.

This information is stored in the installation data field of the CKDS.

Figure 201 shows this panel filled in for the final key part.

5. Press ENTER. Figure 202 on page 192 appears.

```

CSFSCK30----- ICSF - TKE - Operational Key Input -----
COMMAND ==>

                                Coprocessor selected for new key      : C0

Enter a verification pattern. (optional)
VP ==> 0000000000000000

Press ENTER after the key has been entered.
Press END   to exit to the previous menu.

```

Figure 202. Operational Key Input Panel - Key Part Register Status for Final Part

6. Press enter.

Refreshing the CKDS

At any time without disrupting cryptographic functions, you can refresh the in-storage CKDS with an updated or different disk copy of the CKDS by following these steps:

1. Enter option 2, Master Key, on the ICSF Primary Menu to access the Master Key Process panel. Enter option 1, INIT/REFRESH CKDS to access the Initialize CKDS panel which is shown in Figure 203.

```

CSFCKD00 ----- ICSF - Initialize a CKDS -----
COMMAND ==> 5

Enter the number of the desired option.

1 Initialize an empty CKDS (creates the header and system keys)
2 NOCVKEYS - Create NOCV-Enablement keys (for keys without CVs)
3 ANSI     - Create ANSI system keys (for ANSI X9.17 services)
4 ESYS     - Create enhanced system keys (for Symmetric services)

5 REFRESH  - Activate an updated CKDS

Enter the name of the CKDS below.

CKDS ==> 'FIRST.EMPTY.CKDS'

```

Figure 203. ICSF Initialize a CKDS Panel

2. In the CKDS field, specify the name of the disk copy of the CKDS that you want ICSF to read into storage.
3. Choose option 5, REFRESH, and press ENTER.
ICSF reads the disk copy of the specified CKDS into storage. Partial keys that may exist when you enter keys manually are not loaded into storage during a REFRESH. Applications running on ICSF are not disrupted. A message stating that the CKDS was refreshed appears on the right of the top line on the panel.

After the CKDS is read into storage, ICSF performs a MAC verification on each record in the CKDS. If a record fails the MAC verification, a message giving the key label and type for that record is sent to the MVS security console. You can then delete the record from the CKDS using KGUP or the dynamic CKDS update services. Any other attempts to access a record that has failed MAC verification results in an invalid MAC return code and reason code.

4. Press END to return to the Primary Menu panel.

Installing RSA Keys in the PKDS from a Dataset

If you used TKE to load an RSA key into a host dataset member on MVS, you load it from the dataset to the PKDS by this method.

1. Select Option 7, TKE, on the ICSF Primary Option Menu.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----  
OPTION ==> 7
```

Enter the number of the desired option.

- | | | |
|---|------------------|--|
| 1 | COPROCESSOR MGMT | - Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - Installation options |
| 4 | ADMINCTL | - Administrative Control Functions |
| 5 | UTILITY | - ICSF Utilities |
| 6 | PPINIT | - Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - TKE Master and Operational key processing |
| 8 | KGUP | - Key Generator Utility processes |
| 9 | UDX MGMT | - Management of User Defined Extensions |

Figure 204. Selecting the TKE Option on the ICSF Primary Menu Panel

2. The TKE Processing Selection panel appears. Select option 3.

```
CSFOPK00 ----- ICSF - TKE Processing Selection -----  
OPTION ==> 3
```

Enter the number of the desired option.

- | | |
|---|---------------------------|
| 1 | DES Master key entry |
| 2 | DES Operational key entry |
| 3 | PKA key entry |

Figure 205. Selecting PKA Key entry on the TKE Processing Selection Panel

3. On the ICSF PKA Direct Key Load panel, enter the name of the pre-allocated partitioned dataset and the member name of the RSA key to be loaded into the PKDS.

```
CSFTPL00 ----- ICSF - PKA Direct Key Load -----  
Enter the data set name and the key specifications.  
Key Data Set  
Name =====> 's09.pkds(rsakey1)' _____  
  
Press ENTER to select the data set and the key.  
Press END   to exit to the previous menu.  
  
OPTION =====>
```

Figure 206. 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 8. Managing Keys: TKE and ICSF with PCIXCC/CEX2C

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.

On a z990, z890, z9 EC, z9 BC and System z10 EC with a PCI X Cryptographic Coprocessor/Crypto Express2 Coprocessor, the Symmetric-Keys Master Key (SYM-MK) protects symmetric keys such as DES keys and the Asymmetric-Keys Master Key protects RSA keys.

ICSF is required to complete some operations initiated from TKE. These operations include setting the master key, initializing/refreshing the CKDS, loading operational keys into the CKDS, and installing RSA keys to the PKDS. ICSF is also required for disabling and enabling PKA services, PKDS Initialization, PKDS Reencipher and PKDS Activate.

Be prepared to switch between your TKE workstation and your ICSF host session.

This topic discusses the procedures needed for:

- Loading the master keys the first time you start ICSF (page 196)
- Changing the SYM-MK master keys periodically (page 198)
- Reentering the master keys (page 202)
- Adding Additional Coprocessors (page 204)
- Changing the ASYM-MK master keys (page 204)
- Loading Operational Keys to the CKDS (page 209)
- Refreshing the CKDS (page 212)
- Install RSA Keys (page 213)

Master Key Parts

Master key parts are loaded using binary files, the keyboard, or secure key part entry. If loading key parts with the keyboard, record the key parts and the associated hash patterns.

The key parts are generated from the Domain Keys page. For more information, see “Domains Keys Page (PCICC and PCIXCC/CEX2C)” on page 121.

Note: If you are reentering master keys after they have been cleared, use the same master key part values as when you originally entered the keys. You should have saved the key part values in a secure place after you entered the master keys previously.

To enter a Symmetric-keys master key, you can either enter a first key part and a final key part or a first key part, one or more intermediate key part and a final key part.

First-Time Startup

The first time you start ICSF, you must load a Symmetric-Keys master key and initialize the CKDS. For information on creating an empty CKDS, see *z/OS Cryptographic Services ICSF System Programmer's Guide*. When you initialize the CKDS, ICSF creates a header record for the CKDS, installs the required system key in the CKDS, and sets the master key. Keys stored in the CKDS are enciphered under the Symmetric-Keys master key. After the master key has been set, you can generate or enter any keys you need to perform cryptographic functions.

To define a Symmetric-Keys master key, you must load the key parts to the Symmetric-Keys new master key register.

You have to initialize a CKDS only the first time you start ICSF on a system. After you initialize a CKDS, you can copy the disk copy of the CKDS to create other CKDSs for use on the system. You can also share a CKDS with another ICSF system if the system has the same master key value. If sharing a CKDS between a z990, z890 or z9 EC or z9 BC and a legacy system, the CKDS must be initialized on the legacy system. At any time, you can read a different disk copy into storage. For information about how to read a disk copy into storage, see "Refreshing the CKDS" on page 212.

Initialize the CKDS

At this point, the new symmetric-keys master key register on each PCIXCC/CEX2C in this domain is full.

You must now initialize the CKDS (which also activates the symmetric-keys master key).

From the ICSF Primary Menu on TSO:

1. Select Option 2, MASTER KEY, as shown in Figure 207 on page 197.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----  
OPTION ==> 2
```

Enter the number of the desired option.

- | | | |
|---|------------------|--|
| 1 | COPROCESSOR MGMT | - Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - Installation options |
| 4 | ADMINCTL | - Administrative Control Functions |
| 5 | UTILITY | - ICSF Utilities |
| 6 | PPINIT | - Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - TKE Master and Operational key processing |
| 8 | KGUP | - Key Generator Utility processes |
| 9 | UDX MGMT | - Management of User Defined Extensions |

Licensed Materials - Property of IBM

This product contains "Restricted Materials of IBM"
5694-A01 (C) Copyright IBM Corp. 2004. All rights reserved.
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 207. ICSF Selecting the Master Key Option on the Primary Menu Panel

2. The Master Key Management panel appears. Select Option 1, INIT/REFRESH CKDS, as shown in Figure 208.

```
CSFMKM00 ----- ICSF - Master Key Management -----  
OPTION ==> 1
```

Enter the number of the desired option above.

- | | | |
|---|-------------------|---|
| 1 | INIT/REFRESH CKDS | - Initialize a Cryptographic Key Data Set or activate an updated Cryptographic Key Data Set |
| 2 | SET MK | - Set a DES/Symmetric-Keys master key |
| 3 | REENCIPHER CKDS | - Reencipher the CKDS prior to changing the DES /Symmetric Keys master key |
| 4 | CHANGE MK | - Changing the DES/Symmetric-Keys master key and activate the reenciphered CKDS |
| 5 | INITIALIZE PKDS | - Initialize or update a PKDS Cryptographic Key Data Set header record |
| 6 | REENCIPHER PKDS | - Reencipher the PKA Cryptographic Key Data Set |
| 7 | ACTIVATE PKDS | - Activate the PKDS after it has been reenciphered |
| 8 | REFRESH CACHE | - Refresh the PKDS cache if enabled |

Figure 208. Selecting the Initialize a CKDS Option on the ICSF Master Key Management Panel

3. The Initialize a CKDS panel now appears.

```

CSFCKD10 ----- ICSF - Initialize a CKDS -----
COMMAND ==> 1

Enter the number of the desired option.

  1 Initialize an empty CKDS (creates the header and system keys)

  2 REFRESH - Activate an updated CKDS

Enter the name of the CKDS below.

CKDS ==> 'FIRST.EMPTY.CKDS'

```

Figure 209. ICSF Initialize a CKDS Panel

4. In the CKDS field at the bottom of the panel, enter the name of the empty VSAM data set that was created to use as the disk copy of the CKDS.
The name you enter should be the same name that is specified in the CKDSN installation option in the installation options data set. For information about creating a CKDS and specifying the CKDS name in the installation options data set, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.
5. Choose option 1, Initialize an empty CKDS, and press ENTER.
ICSF creates the header record in the disk copy of the CKDS. Next, ICSF sets the symmetric-keys master key. ICSF then adds the required system key to the CKDS and refreshes the CKDS. When ICSF completes all these steps the message **INITIALIZATION COMPLETE** appears. If you did not enter a master key into the new master key register previously, the message **NMK REGISTER NOT FULL** appears and the initialization process ends. You must enter a master key into the new master key register before you can initialize the CKDS.

Note: If any part of the option 1 fails, you must delete the CKDS and start over. If the failure occurs after the master key is set and before the system key has been created, you will need to reload the new master key register, delete the CKDS and start over.

After you complete the entire process, a master key and CKDS exist on your system. If you want to enter keys (for example, keys using the key generate callable service, the key generator utility program, or convert CUSP/PCF keys to ICSF keys using the conversion program), see *z/OS Cryptographic Services ICSF Administrator's Guide*.

Changing Master Keys

For security reasons your installation should change the master keys periodically. In addition, if the master keys have been cleared, you may also want to change the master keys after you reenter the cleared master keys.

Tasks necessary for changing the master key are:

1. Load new SYM-MK (first, middle, last)
2. Re-encipher CKDS
3. Change master key

The step-by-step procedure for changing the symmetric-keys master key, reenciphering the CKDS, and activating the new master key is presented in "Changing the Master Key Using the Master Key Panels" on page 199. For

information on the contents of the master key registers during the key change process, and some compatibility mode considerations, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

A symmetric-keys master key and a CKDS containing keys enciphered under that master key already exist. Before you replace this existing master key with the new master key, you must reencipher the CKDS under the new master key.

When the DES master key is changed, the current active DES master key is moved to the auxiliary master key register and the new DES master key is moved to the master key register. In this way, the new master key you have just entered becomes the current master key, and the previous master key is stored in the old master key register.

Before the new symmetric-keys master key is placed into the master key register, you must reencipher all disk copies of the CKDS under the new master key. Then you are ready to activate the master key. When you change the master key, you have ICSF replace the in-storage copy of the CKDS with the reenciphered disk copy and make the new master key active on the system.

Changing the Master Key Using the Master Key Panels

Load the key parts of the new master key that you want to replace the current master key. The new master key parts must be loaded from TKE.

Note: The steps for this task are performed from your TSO logon id using the ICSF panels.

The new symmetric-keys master key register on all PCIxCCs/CEX2Cs must be full before you change the master key.

1. Select option 2, MASTER KEY, on the ICSF Primary Menu.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----  
OPTION ==> 2
```

Enter the number of the desired option.

- | | | |
|---|------------------|--|
| 1 | COPROCESSOR MGMT | - Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - Installation options |
| 4 | ADMINCNTL | - Administrative Control Functions |
| 5 | UTILITY | - ICSF Utilities |
| 6 | PPINIT | - Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - TKE Master and Operational key processing |
| 8 | KGUP | - Key Generator Utility processes |
| 9 | UDX MGMT | - Management of User Defined Extensions |

Figure 210. Selecting the Master Key Option on the ICSF Primary Menu Panel

2. Before you change the master key, you must first reencipher the disk copy of the CKDS under the new master key. Select option 3, REENCIPHER CKDS, on the Master Key Management panel, as shown in Figure 211 on page 200, and press ENTER.

```
CSFCMK00 ----- ICSF - Master Key Management -----  
OPTION ==> 3
```

Enter the number of the desired option above.

- | | |
|---------------------|---|
| 1 INIT/REFRESH CKDS | - Initialize a Cryptographic Key Data Set or activate an updated Cryptographic Key Data Set |
| 2 SET MK | - Set a DES/Symmetric-Keys master key |
| 3 REENCIPHER CKDS | - Reencipher the CKDS prior to changing the DES /Symmetric Keys master key |
| 4 CHANGE MK | - Change the DES/Symmetric-Keys master key and activate the reenciphered CKDS |
| 5 INITIALIZE PKDS | - Initialize or update a PKDS Cryptographic Key Data Set header record |
| 6 REENCIPHER PKDS | - Reencipher the PKA Cryptographic Key Data Set |
| 7 ACTIVATE PKDS | - Activate the PKDS after it has been reenciphered |
| 8 REFRESH CACHE | - Refresh the PKDS cache if enabled |

Figure 211. Selecting the Reencipher CKDS Option on the ICSF Master Key Management Panel

3. The Reencipher CKDS panel appears. See Figure 212.

```
CSFCMK10 ----- ICSF - Reencipher CKDS -----  
COMMAND ==>
```

To reencipher all CKDS entries from encryption under the current DES/Symmetric-Keys master key to encryption under the new master key enter the CKDS names below.

Input CKDS ==> CKDS.CURRENT.MASTER

Output CKDS ==> CKDS.NEW.MASTER

Figure 212. Reencipher CKDS

4. In the Input CKDS field, enter the name of the CKDS that you want to reencipher. In the Output CKDS field, enter the name of the data set in which the reenciphered keys are written.

Note: The output data set should already exist although it must be empty. For more information about defining a CKDS, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

Reenciphering the disk copy of the CKDS does not affect the in-storage copy of the CKDS. On this panel, you are working with only a disk copy of the CKDS.

5. Press ENTER to reencipher the input CKDS entries and write them into the output CKDS.

The message REENCIPHER SUCCESSFUL appears on the top right of the panel if the reencipher succeeds.

6. If you have more than one CKDS on disk, specify the information and press ENTER as many times as you need to reencipher all of them. Reencipher all your disk copies at this time. When you have reenciphered all the disk copies of the CKDS, you are ready to change the master key.
7. Press END to return to the Master Key Management panel.
 - a. Changing the master key involves refreshing the in-storage copy of the CKDS with a disk copy and activating the new master key.
 - b. If you are running in compatibility or co-existence mode, *do not* select option 4, the Change option. To activate the changed master key when running in compatibility or co-existence mode, you need to re-IPL MVS and start ICSF. When you re-IPL MVS and start ICSF, you activate the changed master key and refresh the in-storage CKDS. To do this, you must exit the panels at this time.
 - c. If you are running in noncompatibility mode, to change the master key select option 4 on the Master Key Management panel, as shown in Figure 213.

```
CSFMKM00 ----- ICSF - Master Key Management -----
OPTION ==> 4

Enter the number of the desired option above.

 1 INIT/REFRESH CKDS - Initialize a Cryptographic Key Data Set or activate
                       an updated Cryptographic Key Data Set
 2 SET MK             - Set a DES/Symmetric-Keys master key
 3 REENCIPHER CKDS   - Reencipher the CKDS prior to changing the DES
                       /Symmetric Keys master key
 4 CHANGE MK         - Change the DES/Symmetric-Keys master key and
                       activate the reenciphered CKDS

 5 INITIALIZE PKDS   - Initialize or update a PKDS Cryptographic
                       Key Data Set header record
 6 REENCIPHER PKDS   - Reencipher the PKA Cryptographic Key Data Set
 7 ACTIVATE PKDS     - Activate the PKDS after it has been reenciphered
 8 REFRESH CACHE     - Refresh the PKDS cache if enabled
```

Figure 213. Selecting the Change Master Key Option on the ICSF Master Key Management Panel

8. When you press the ENTER key, the Change Master Key panel appears. See Figure 214.

```
CSFCMK20 ----- ICSF Change Master Key -----
COMMAND ==>

Enter the name of the new CKDS below:

New CKDS ==> CKDS.NEW.MASTER

When the master key is changed, the new CKDS will become active.
```

Figure 214. Change Master Key Panel

9. In the New CKDS field, enter the name of the disk copy of the CKDS that you want in storage.

You should have already reenciphered the disk copy of the CKDS under the new master key. The last CKDS name that you specified in the Output CKDS field on the Reencipher CKDS panel, which is shown in Figure 212 on page 200, automatically appears in this field.

10. Press ENTER.

ICSF loads the data set into storage where it becomes operational on the system. ICSF also places the new master key into the master key register so it becomes active.

After you press ENTER, ICSF attempts to change the master key. It displays a message on the top right of the panel. The message indicates either that the master key was changed successfully or that an error occurred that did not permit the change process to be completed. For example, if you indicate a data set that is not reenciphered under the new master key, an error message displays and the master key is not changed.

Re-entering Master Keys After They have been Cleared

In these situations, the PCI X Cryptographic Coprocessor (PCIXCC)/Crypto Express2 Coprocessor (CEX2C) clears the master key registers so that the master key values are not disclosed:

- If the PCIXCC/CEX2C detects tampering (the intrusion latch is tripped), ALL installation data is cleared: master keys, retained keys for all domains, operational key part registers, as well as roles and authorities.
- If the PCIXCC/CEX2C detects tampering (the secure boundary of the card is compromised), it self-destructs and can no longer be used.
- If you issue a command from the TKE workstation to zeroize a domain
This command zeroizes the data specific to a domain: master keys, retained keys and operational key part registers.
- If you issue a command from the Support Element panel to zeroize all domains.
This command zeroizes ALL installation data: master keys, retained keys, operational key part registers, and access control roles and profiles. Also, the default setting of *Denied* for all PCIXCCs/CEX2Cs set for TKE Enablement.

Although the values of the master keys are cleared, the keys in the CKDS are still enciphered under the cleared symmetric-keys master key. The RSA and DSS private key are also each enciphered under the cleared asymmetric-keys master keys. Therefore, to recover the keys in the CKDS, and the PKA private keys in the PKDS, you must reenter the same master keys and activate the symmetric-keys master key. For security reasons, you may then want to change all the master keys.

PR/SM Considerations

When running in PR/SM logical partition (LPAR) mode with PCIXCC/CEX2C, a tamper situation causes all installation data; master keys, retained keys, operational key part registers, roles and authorities to be cleared. All installation data will need to be reloaded and recreated. If you zeroize a domain using the TKE workstation, however, the master keys are cleared only in that domain. Master keys in other domains are not affected and do not need to be reentered. For more information about reentering master keys in LPAR mode, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

Setting the Master Key

After the master keys have been cleared, reenter the same master keys by following these steps:

1. Load new master key parts. For details on loading the keys, see “Load - PCICC/PCIXCC/CEX2C” on page 126.

These values should be stored in a secure place as specified in your enterprises security process.

2. Retrieve the key parts, checksums, verification patterns, and hash patterns you used when you loaded the master keys originally. These values should have been stored in a secure place.
3. To activate the symmetric-keys master key you just entered, you need to set it. On the ICSF Primary Menu panel in TSO, select option 2.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----  
OPTION ==> 2
```

Enter the number of the desired option.

- | | | |
|---|------------------|--|
| 1 | COPROCESSOR MGMT | - Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - Installation options |
| 4 | ADMINCTL | - Administrative Control Functions |
| 5 | UTILITY | - ICSF Utilities |
| 6 | PPINIT | - Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - TKE Master and Operational key processing |
| 8 | KGUP | - Key Generator Utility processes |
| 9 | UDX MGMT | - Management of User Defined Extensions |

Figure 215. ICSF Selecting the Master Key Option on the Primary Menu Panel

4. To set the Symmetric-Keys master key, choose option 2 on the panel and press ENTER.

```
CSFMKM00 ----- ICSF - Master Key Management -----  
OPTION ==> 2
```

Enter the number of the desired option above.

- | | | |
|---|-------------------|---|
| 1 | INIT/REFRESH CKDS | - Initialize a Cryptographic Key Data Set or activate an updated Cryptographic Key Data Set |
| 2 | SET MK | - Set a DES/Symmetric-Keys master key |
| 3 | RENCIPHER CKDS | - Reencipher the CKDS prior to changing the DES /Symmetric Keys master key |
| 4 | CHANGE MK | - Change the DES/Symmetric-Keys master key and activate the reenciphered CKDS |
| 5 | INITIALIZE PKDS | - Initialize or update a PKDS Cryptographic Key Data Set header record |
| 6 | RENCIPHER PKDS | - Reencipher the PKA Cryptographic Key Data Set |
| 7 | ACTIVATE PKDS | - Activate the PKDS after it has been reenciphered |
| 8 | REFRESH CACHE | - Refresh the PKDS cache if enabled |

Figure 216. Selecting the Set Host Master Key Option on the ICSF Master Key Management Panel

After you select option 2, ICSF checks that the states of the registers are correct. ICSF then transfers the symmetric-keys master key from the new master key register to the master key register. This process sets the master key.

When ICSF attempts to set the master key, it displays a message on the top right of the Master Key Management panel. The message indicates either that the master key was successfully set, or that an error prevented the completion of the set process.

5. You can now change the symmetric-keys master key, if you choose to, for security reasons. Continue with “Changing Master Keys” on page 198.

Adding Cryptographic Coprocessors After ICSF Initialization

There may come a time when you wish to add additional PCI X Cryptographic Coprocessor (PCIXCC)/Crypto Express2 Coprocessor(CEX2C) 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.

PCIXCC/CEX2C

Note: With TKE Version 4.0 and later, it is no longer necessary to exit the application to add new crypto module(s).

1. Open the Host where the crypto module(s) were added. You will be prompted to authenticate the crypto module.
2. Open the new crypto module(s).
3. Use the authority 0 default signature key to administer access control (create the same roles and authorities for the new PCIXCC/CEX2C to match the PCIXCC/CEX2C currently on the host). Load the authority signature keys to match the other crypto modules.
4. Load a new signature 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 signature keys.
5. Load the 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 asymmetric master key from TKE.
7. Set the symmetric master key on the PCIXCC/CEX2C from ICSF (see “Setting the Master Key” on page 203) when everything is the same (roles, authorities, controls, master keys).
8. If desired, add the new PCIXCC(s)/CEX2C(s) to the group by doing a group change.

Asymmetric-keys Master Key Parts

When you enter the asymmetric-keys master key the first time, the PKA callable services are initially disabled. Once you have entered the master key, you must enable the PKA callable services for these services to work. Before you change the asymmetric-keys master keys, you need to disable the PKA callable services. To enable and disable the PKA callable services refer to “Disabling PKA Services” on page 205.

To enter a asymmetric-keys master key, you can either enter a first key part and a final key part or a first key part, an intermediate key part and a final key part.

After you enter a key part for a symmetric-keys or asymmetric-keys master key the PCIXCC calculates a sixteen-byte hash pattern. The hash patterns are displayed in a pop-up window for the administrator to verify. The hash patterns check whether you entered the key part correctly.

Tasks necessary for changing the asymmetric-keys master keys are listed here. Note that steps 2 through 4 are done at the TKE workstation.

1. Disable PKA Services
2. Clear New ASYM-MK (*if not empty*)
3. Load New ASYM-MK — first, middle, last
4. Set ASYM-MK
5. PKDS Reencipher under the new PKA Master Key
6. PKDS Activate
7. Enable PKA Services
8. Enable PKDS Reads/Writes

Disabling PKA Services

When you enter or change the asymmetric-keys master keys, the PKA services should first be disabled. To disable PKA services:

1. From TSO, access the user control functions by choosing option 4, ADMINCNTL, on the Primary Menu panel of ICSF, as shown in Figure 217.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----  
OPTION ==> 4
```

Enter the number of the desired option.

- | | | |
|---|------------------|--|
| 1 | COPROCESSOR MGMT | - Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - Installation options |
| 4 | ADMINCNTL | - Administrative Control Functions |
| 5 | UTILITY | - ICSF Utilities |
| 6 | PPINIT | - Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - TKE Master and Operational key processing |
| 8 | KGUP | - Key Generator Utility processes |
| 9 | UDX MGMT | - Management of User Defined Extensions |

Figure 217. Selecting the Administrative Control Option on the ICSF Primary Menu Panel

2. The Administrative Control Function panel appears. See Figure 218 on page 206.

```

CSFACF00 ----- ICSF Administrative Control Functions
COMMAND ==>
    Active CKDS: CSF.CKDS
    Active PKDS: CSF.PKDS
    Active TKDS: CSF.TKDS

To change the status of a control, enter the appropriate character
(E - ENABLE, D - DISABLE) and press ENTER.

      Function                                STATUS
      -----                                -
.  Dynamic CKDS Access                        ENABLED
D  PKA Callable Services                     ENABLED
.  PKDS Read Access                          ENABLED
.  PKDS Write, Create, and Delete Access      ENABLED

```

Figure 218. Disabling the PKA Callable Services

3. Type a 'D' to the left of the functions you want disabled and press ENTER.

Note: Disabling PKA Callable Services automatically disables PKDS Read/Write/Create/Delete access as well.

Enabling PKA Services

After you enter or change the asymmetric-keys master keys, the PKA services should be enabled. To enable PKA services:

1. From TSO, access the user control functions by choosing option 4, ADMINCNTL, on the Primary Menu panel of ICSF, as shown in Figure 219.

```

CSF@PRIM ----- Integrated Cryptographic Service Facility -----
OPTION ==> 4

Enter the number of the desired option.

 1 COPROCESSOR MGMT - Management of Cryptographic Coprocessors
 2 MASTER KEY       - Master key set or change, CKDS/PKDS processing
 3 OPSTAT           - Installation options
 4 ADMINCNTL        - Administrative Control Functions
 5 UTILITY           - ICSF Utilities
 6 PPINIT           - Pass Phrase Master Key/CKDS Initialization
 7 TKE              - TKE Master and Operational key processing
 8 KGUP             - Key Generator Utility processes
 9 UDX MGMT         - Management of User Defined Extensions

```

Figure 219. Selecting the Administrative Control Option on the ICSF Primary Menu Panel

2. The Administrative Control Function panel appears. See Figure 220 on page 207.


```

CSFACF00 ----- ICSF Administrative Control Functions
COMMAND ==>
    Active CKDS: CSF.CKDS
    Active PKDS: CSF.PKDS
    Active TKDS: CSF.TKDS

To change the status of a control, enter the appropriate character (E - ENABLE,
D - DISABLE) and press ENTER.

      Function                                STATUS
      -----                                -
.   Dynamic CKDS Access                      ENABLED
E   PKA Callable Services                   DISABLED
E   PKDS Read Access                        DISABLED
E   PKDS Write, Create, and Delete Access    DISABLED

```

Figure 220. Enabling and Disabling the PKA Callable Services

3. Enter the option and press ENTER.
 - To enable the PKA callable services, type an 'E' before the function. Press ENTER.
 - To enable PKDS Read Access, type an 'E' before the function. Press ENTER.
 - To enable PKDS Write Access, type an 'E' before the function. Press ENTER.

Resetting Asymmetric-Keys Master Keys

If you realize that you have made a mistake entering key parts to the asymmetric-keys master key register, you are able to reset the value in the register to zero. From the TKE workstation, access the domain window (see “Domains Keys Page (PCICC and PCIXCC/CEX2C)” on page 121 and “Domain Keys Page - PCIXCC/CEX2C” on page 131). Select the asymmetric-keys master key and then select **Clear**.

Notes:

1. Once the asymmetric-keys master key has been changed, internal tokens in the PKDS are unusable. You will need to reencipher and activate the PKDS in order to use them with the changed master key. See “Reenciphering and Activating the PKDS.”
2. For RSA keys loaded into the PKDS from the TKE workstation, the process can be repeated to load the keys under the changed asymmetric-keys master keys. See “Load RSA Key to PKDS - PCIXCC/CEX2C” on page 150 and “Installing RSA Keys in the PKDS from a Data Set” on page 213 for details.

Reenciphering and Activating the PKDS

For security reasons, your installation should periodically change the asymmetric-keys master key and reencipher the private keys. Reenciphering and activating the PKDS automatically refreshes the PKDS cache, as does starting ICSF.

To reencipher the PKDS after the ASYM-MK has been changed, go to the Master Key Management panel and select option 6.

Note: If sharing a PKDS, only keys enciphered under the ASYM-MK are reenciphered. PKDS reencipher will not be able to reencipher private keys encrypted under the CCF key management key (KMMK) if the KMMK does not equal the SMK.

```
CSFMKM00 ----- ICSF - Master Key Management -----  
OPTION ==> 6
```

Enter the number of the desired option.

- | | |
|---------------------|---|
| 1 INIT/REFRESH CKDS | - Initialize a Cryptographic Key Data Set or activate an updated Cryptographic Key Data Set |
| 2 SET MK | - Set a DES/Symmetric-Keys master key |
| 3 REENCIPHER CKDS | - Reencipher the CKDS prior to changing the DES /Symmetric Keys master key |
| 4 CHANGE MK | - Change the DES/Symmetric-Keys master key and activate the reenciphered CKDS |
| 5 INITIALIZE PKDS | - Initialize or update a PKDS Cryptographic Key Data Set header record |
| 6 REENCIPHER PKDS | - Reencipher the PKA Cryptographic Key Data Set |
| 7 ACTIVATE PKDS | - Activate the PKDS after it has been reenciphered |
| 8 REFRESH CACHE | - Refresh the PKDS cache if enabled |

Figure 221. Selecting the Reencipher PKDS Option on the Master Key Management Panel

The Reencipher PKDS panel appears. In the Input PKDS field, specify the name of the PKDS that you want ICSF to reencipher under the current ASYM-MK.

In the Output PKDS field, specify the name of an empty VSAM data set. ICSF writes the reenciphered keys in this data set.

```
CSFCMK11 ----- ICSF - Reencipher PKDS -----  
COMMAND ==>
```

To reencipher all PKDS entries from encryption under the old signature/ asymmetric-keys master key to encryption under the current master key, enter the PKDS names below.

Input PKDS ==>

Output PKDS ==>

Press ENTER to reencipher the PKDS.
Press END to exit to the previous menu

Figure 222. Reencipher PKDS

Press enter to reencipher the PKDS. Reenciphering automatically refreshes the PKDS cache. Once successful, you will then want to activate the PKDS. Return to the Master Key Management panel and select option 7.

```

CSFMKM00 ----- ICSF - Master Key Management -----
OPTION ==>7

Enter the number of the desired option.

  1 INIT/REFRESH CKDS - Initialize a Cryptographic Key Data Set or activate
                        an updated Cryptographic Key Data Set
  2 SET MK             - Set a DES/Symmetric-Keys master key
  3 REENCIPHER CKDS   - Reencipher the CKDS prior to changing the DES
                        /Symmetric Keys master key
  4 CHANGE MK         - Change the DES/Symmetric-Keys master key and
                        activate the reenciphered CKDS

  5 INITIALIZE PKDS   - Initialize or update a PKDS Cryptographic
                        Key Data Set header record
  6 REENCIPHER PKDS   - Reencipher the PKA Cryptographic Key Data Set
  7 ACTIVATE PKDS     - Activate the PKDS after it has been reenciphered
  8 REFRESH CACHE     - Refresh the PKDS cache if enabled

```

Figure 223. Selecting the Activate PKDS Option on the Master Key Management Panel

The Activate PKDS panel appears. Enter the name of the PKDS that you want ICSF to use. The PKDS must have already been reenciphered under the current Signature/Asymmetric-keys master key.

```

CSFCMK21 ----- ICSF - Activate PKA Cryptographic Key Data Set -----
COMMAND ==>

Enter the name of the new PKDS below.

New PKDS ==>

Press ENTER to activate the PKDS.
Press END to exit to the previous menu

```

Figure 224. Activate PKDS

After you press ENTER, the PKDS becomes active. Activation automatically refreshes the PKDS cache.

Loading Operational Keys to the CKDS

Beginning with TKE V4.1, you can load operational key parts into key part registers on the PCIXCC/CEX2C. To load these keys into the CKDS you need to use the ICSF DES Operational Key Load panel or KGUP. For KGUP details, refer to *z/OS Cryptographic Services ICSF Administrator's Guide*.

Unlike the key part queue on the CCF, each key part register on the PCIXCC/CEX2C holds an accumulated key. Multiple key loads are not required for each key part. Therefore, when a key is loaded into the CKDS from a key part register, it is done in a single step.

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. Access control point, Key Part Import - RETRKPR, must be enabled on the selected PCIXCC/CEX2C or error message ACCESS CONTROL FAILED 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

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----
OPTION ==> 1
```

Enter the number of the desired option.

- | | | |
|---|------------------|--|
| 1 | COPROCESSOR MGMT | - Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - Installation options |
| 4 | ADMINCTL | - Administrative Control Functions |
| 5 | UTILITY | - ICSF Utilities |
| 6 | PPINIT | - Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - TKE Master and Operational key processing |
| 8 | KGUP | - Key Generator Utility processes |
| 9 | UDX MGMT | - Management of User Defined Extensions |

Figure 225. ICSF Primary Menu Panel

2. The Coprocessor Management panel appears. Put a 'K' by the PCIXCC/CEX2C that contains the key part register to load.

```
CSFGCMP0 ----- ICSF Coprocessor Management -----
COMMAND ==>
```

Select the coprocessors to be processed and press ENTER.

Action characters are: A, D, E, K, R, and S. See the help panel for details.

COPROCESSOR	SERIAL NUMBER	STATUS
-----	-----	-----
- A06		ACTIVE
- A07		DEACTIVATED
- X00	42-K0001	ONLINE
K X04	42-K0043	ACTIVE
- X05	42-K0058	DISABLED
- X06	42-K0055	DEACTIVATED

Figure 226. Coprocessor Management Panel

3. The DES Operational Key Load panel appears. The PCIXCC/CEX2C previously selected and the active CKDS are displayed at the top of the panel.

```
CSFCMP50 ----- ICSF DES Operational Key Load -----  
COMMAND ==>
```

```
Coprocessor selected for new key: X04  
CKDS name: 'CSFLPAR1.SYSPLEX.CKDS'
```

```
Enter the key label
```

```
Key label  
==> FREDS.MAC.KEY
```

```
Control Vector ==> YES YES or NO
```

Figure 227. DES 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 to Key Part Register - First” on page 134.
- 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 not exclusive-or a control vector with the key before using it. Select NO for keys that will be exchanged with a system that does not use control vectors. The default is YES.

If a record already exists in the CKDS with a label that matches the key label specified, the DES 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. Unlike the CCF, partial and complete keys can be replaced on the PCIXCC/CEX2C.

```
CSFCMP51 ----- ICSF DES Operational Key Load -----  
COMMAND ==>
```

```
A record with the following specifications has been found in the CKDS:
```

```
Key label : MY.EXISTING.LABEL.EXPORTER  
Key type : EXPORTER
```

Figure 228. DES Operational Key Load Panel

When the key has been successfully loaded the ENC-ZERO value of the key and the control vector are displayed for the user.

```

CSFCMP50 ----- ICSF DES Operational Key Load ----- KEY LOAD COMPLETE
COMMAND ==>

Coprocessor selected for new key: X04
CKDS name: 'CSFLPAR1.SYSPLEX.CKDS'

Enter the key label

Key label
==> FREDS.MAC.KEY

Control Vector ==> YES          YES or NO

ENC-ZERO VP:    01234567
Control vector: 00054D0003410000 00054D0003210000

```

Figure 229. DES Operational Key Load Panel - ENC-ZERO and CV values displayed

Refreshing the CKDS

At any time without disrupting cryptographic functions, you can refresh the in-storage CKDS with an updated or different disk copy of the CKDS by following these steps:

1. Enter option 2, Master Key, on the ICSF Primary Menu to access the Master Key process panel. Enter option 1, INIT/REFRESH CKDS to access the Initialize a CKDS panel, which is shown in Figure 230.

```

CSFCKD10 ----- ICSF - Initialize a CKDS -----
COMMAND ==> 2

Enter the number of the desired option.

  1 Initialize an empty CKDS (creates the header and system keys)
  2 REFRESH - Activate an updated CKDS

Enter the name of the CKDS below.

CKDS ==> 'FIRST.EMPTY.CKDS'

```

Figure 230. ICSF Initialize a CKDS Panel

2. In the CKDS field, specify the name of the disk copy of the CKDS that you want ICSF to read into storage.
3. Choose option 2, REFRESH, and press ENTER.
ICSF places the disk copy of the specified CKDS into storage. Partial keys that may exist when you enter keys manually are not loaded into storage during a REFRESH. Applications running on ICSF are not disrupted. A message stating that the CKDS was refreshed appears on the right of the top line on the panel.
After the CKDS is read into storage, ICSF performs a MAC verification on each record in the CKDS. If a record fails the MAC verification, a message giving the

key label and type for that record is sent to the MVS security console. You can then delete the record from the CKDS using KGUP or the dynamic CKDS update services. Any other attempts to access a record that has failed MAC verification results in an invalid MAC return code and reason code.

4. Press END to return to the Primary Menu panel.

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 on MVS (see “Loading Operational Keys to the CKDS” on page 209), you load it from the data set to the PKDS by this method.

1. Select Option 7, TKE, on the ICSF Primary Option Menu.

```
CSF@PRIM ----- Integrated Cryptographic Service Facility -----  
OPTION ==> 7
```

Enter the number of the desired option.

- | | | |
|---|------------------|--|
| 1 | COPROCESSOR MGMT | - Management of Cryptographic Coprocessors |
| 2 | MASTER KEY | - Master key set or change, CKDS/PKDS processing |
| 3 | OPSTAT | - Installation options |
| 4 | ADMINCTL | - Administrative Control Functions |
| 5 | UTILITY | - ICSF Utilities |
| 6 | PPINIT | - Pass Phrase Master Key/CKDS Initialization |
| 7 | TKE | - TKE Master and Operational key processing |
| 8 | KGUP | - Key Generator Utility processes |
| 9 | UDX MGMT | - Management of User Defined Extensions |

Figure 231. Selecting the TKE Option on the ICSF Primary Menu Panel

2. The TKE Processing Selection panel appears. Select option 3.

```
CSFOPK00 ----- ICSF - TKE Processing Selection -----  
OPTION ==> 3
```

Enter the number of the desired option.

- 1 DES Master key entry
- 2 DES Operational key entry
- 3 PKA key entry

Figure 232. Selecting PKA Key entry on the TKE Processing Selection Panel

3. 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.

```
CSFTPL00 ----- ICSF - PKA Direct Key Load -----  
Enter the data set name and the key specifications.  
Key Data Set  
Name  ====> 's09.pkds(rsakey1)' _____  
  
Press ENTER to select the data set and the key.  
Press END  to exit to the previous menu.  
  
OPTION  ====>
```

Figure 233. 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.

Appendix A. TKE Workstation Setup and Customization

This topic describes several tasks that are necessary preparation for operating your TKE workstation.

Installation

The IBM CE will install the TKE cryptographic adapter into your TKE workstation and then power it up.

Note: When using a KVM switching unit, the TKE windows may appear to be distorted. The TKE should be initialized being directly connected 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 needs to 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 needs to 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.

Configuring TCP/IP

The TKE Administrator must configure the TKE workstation for TCP/IP. 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.

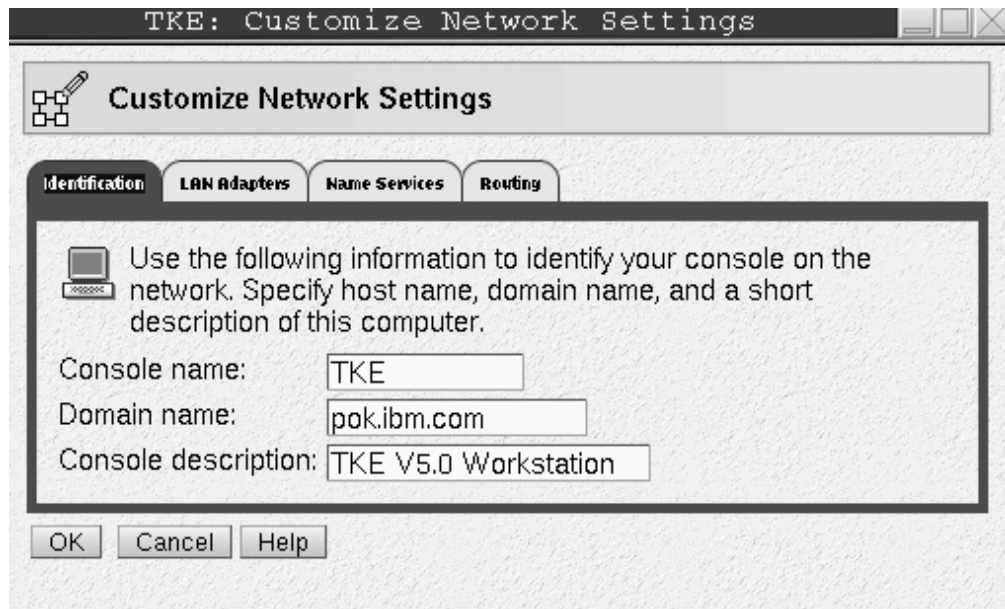


Figure 234. Customize Network Settings - Identification Tab

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.

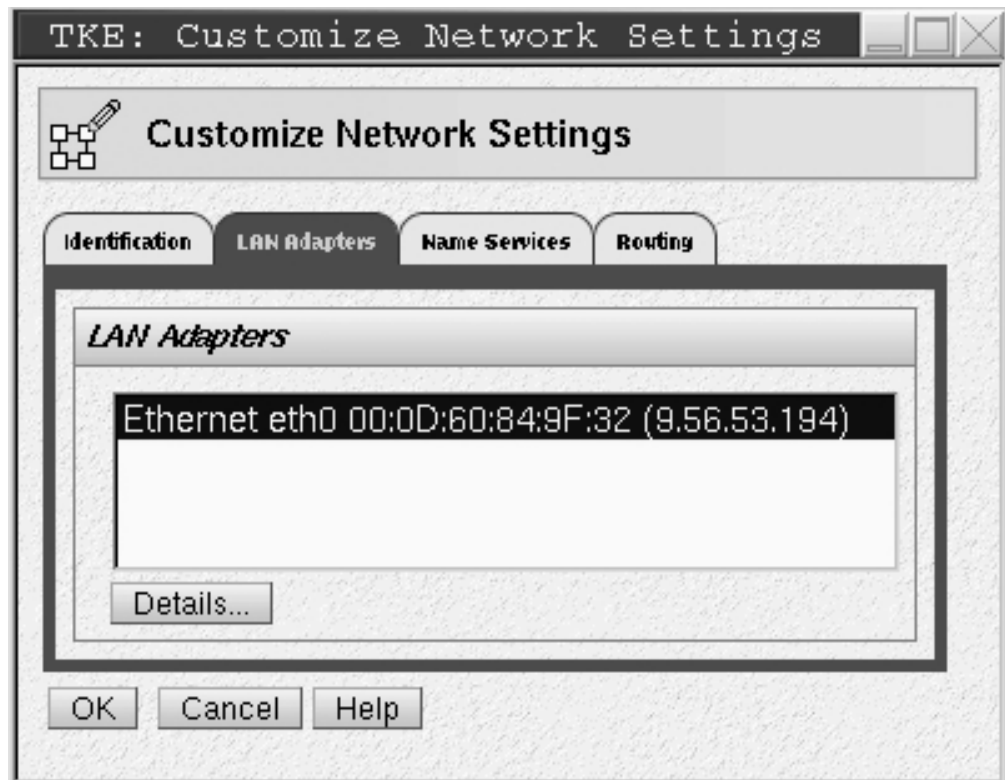


Figure 235. Customize Network Settings Lan Adapters Tab

With the Ethernet LAN adapter highlighted, click on Details.

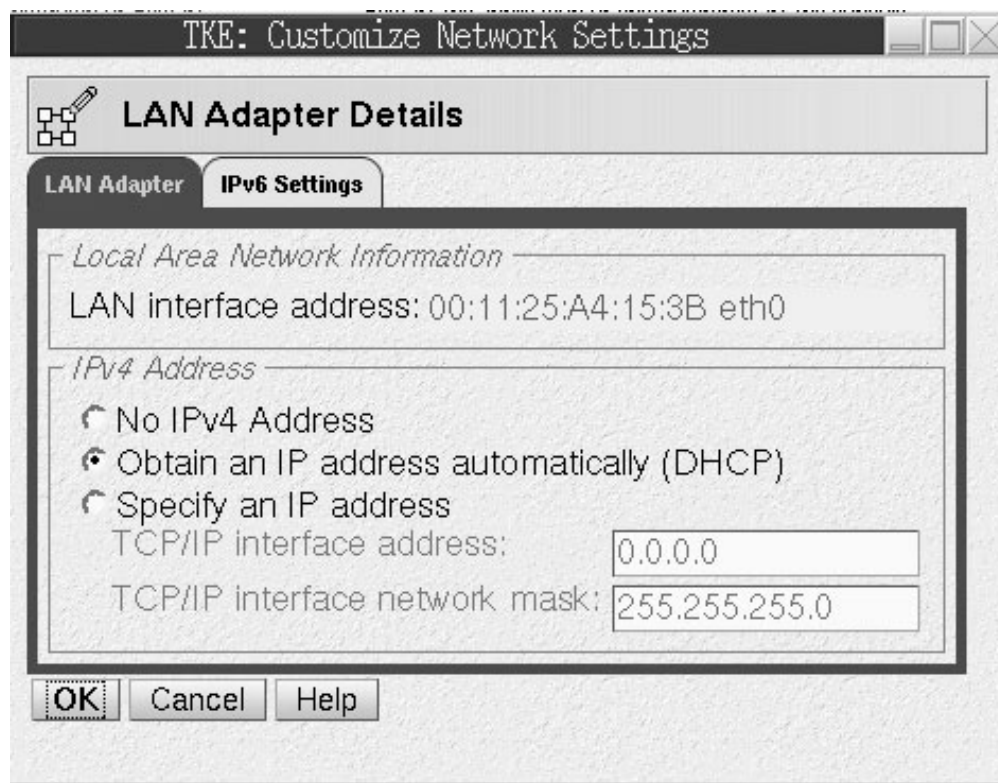


Figure 236. Local Area Network

Specify Local Area Network Information and DHCP Client/IP address information for your network. Press the OK button. If you do not have any further updates to make, click OK on the Customize Network Settings Window. To continue with updates to your network settings, click on the Name Services tab.

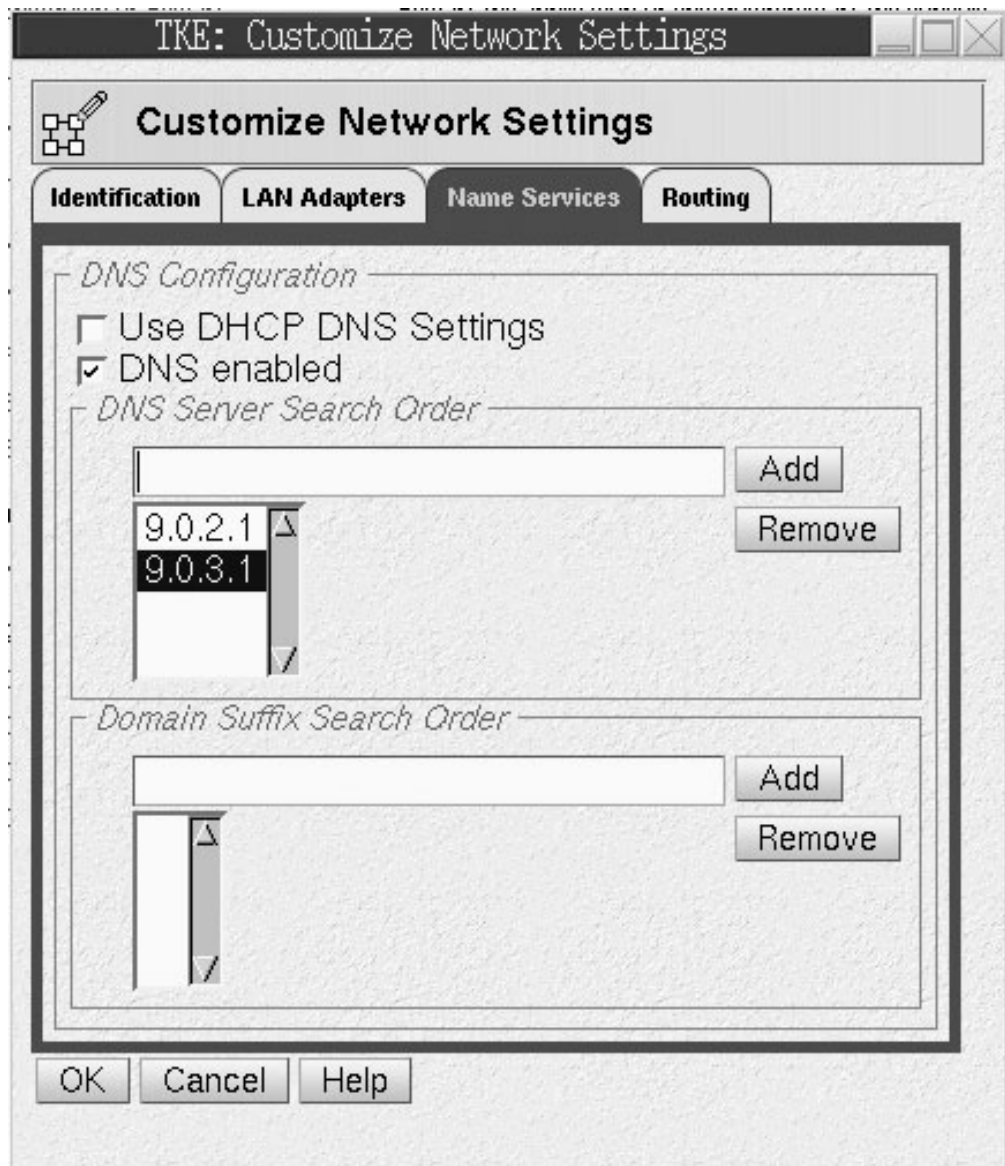


Figure 237. Customize Network Settings - Name Services Tab

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.

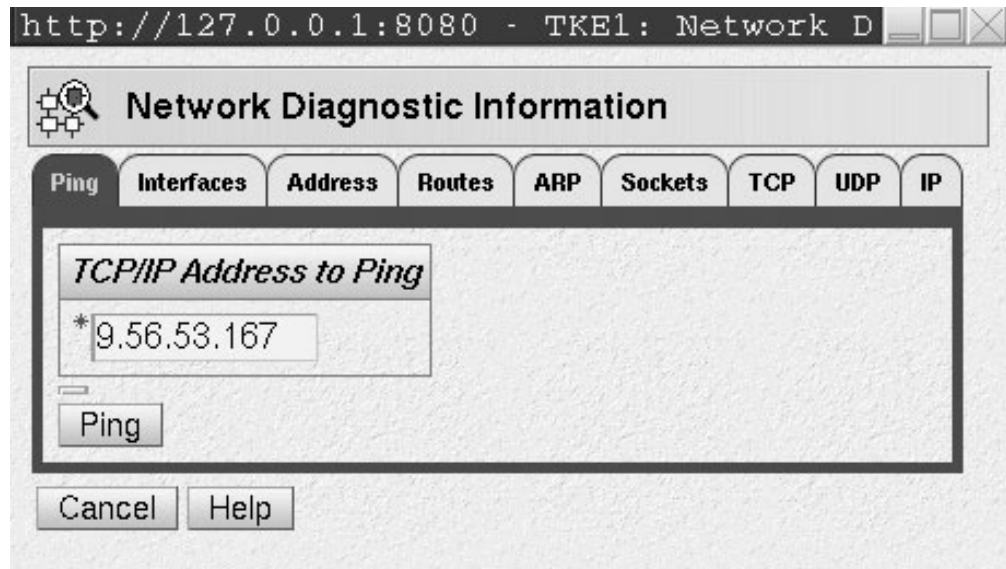


Figure 238. Network Diagnostic Information Task

Initializing the TKE cryptographic adapter

The cryptographic adapter in the TKE workstation needs to be initialized before it can be used for cryptographic functions.

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.

First, set the clock on your TKE workstation. See “Setting the Clock.”

Next, initialize the TKE cryptographic adapter using TKE’s IBM Crypto Adapter Initialization and Cryptographic Node Management Utility 3.10SC.

- If you are initializing using passphrase, see “Initializing TKE for passphrase” on page 220.
- If you are initializing using smart cards, see “Initializing TKE for smart cards” on page 227.

Setting the Clock

To set the system clock on your workstation, open the Customize Console Date/Time task under Service Management.

Changing the clock to Local or UTC

Local

Sets the time to the current time of the time zone that you selected.

UTC

Sets the time to the Greenwich Mean Time (GMT) regardless of what time zone you have chosen.

A time is required for your local system operation. Enter in either the local time or the UTC time.

Setting the assigned time for your system

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 Local clock choose a city from the list that has the same time as the one you need. Press the Customize button when finished.

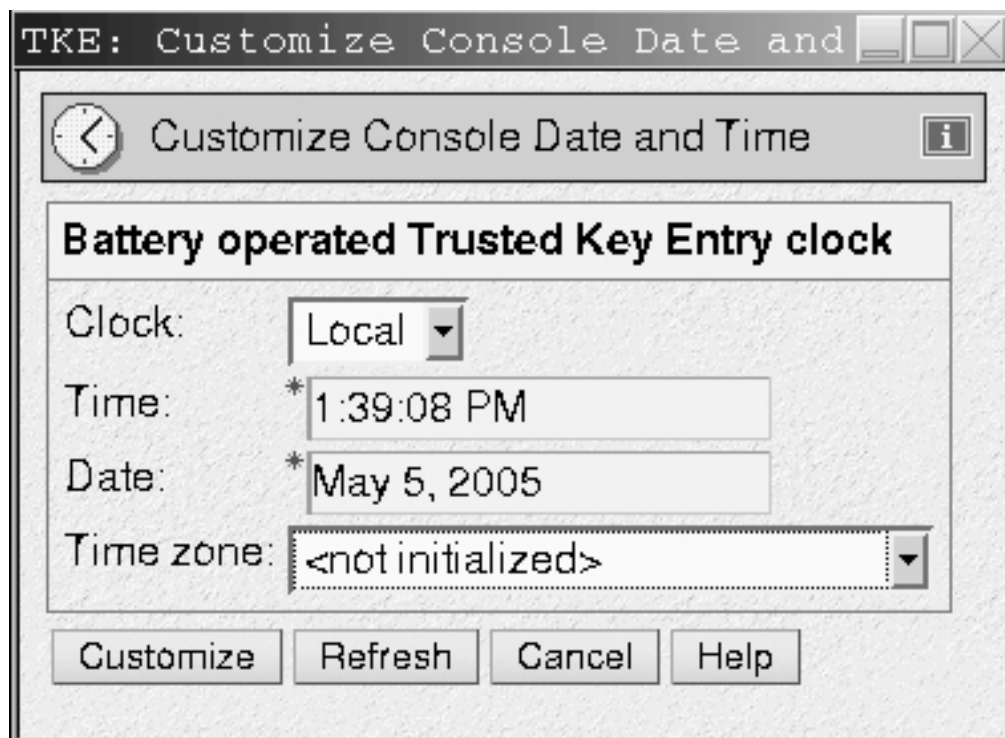


Figure 239. Customize Console Date and Time Window

Initializing TKE for passphrase

To initialize the TKE crypto adapter, click on Trusted Key Entry. Under Applications, click on TKE's IBM Crypto Adapter Initialization.



Figure 240. Crypto Adapter Initialization 1 Window

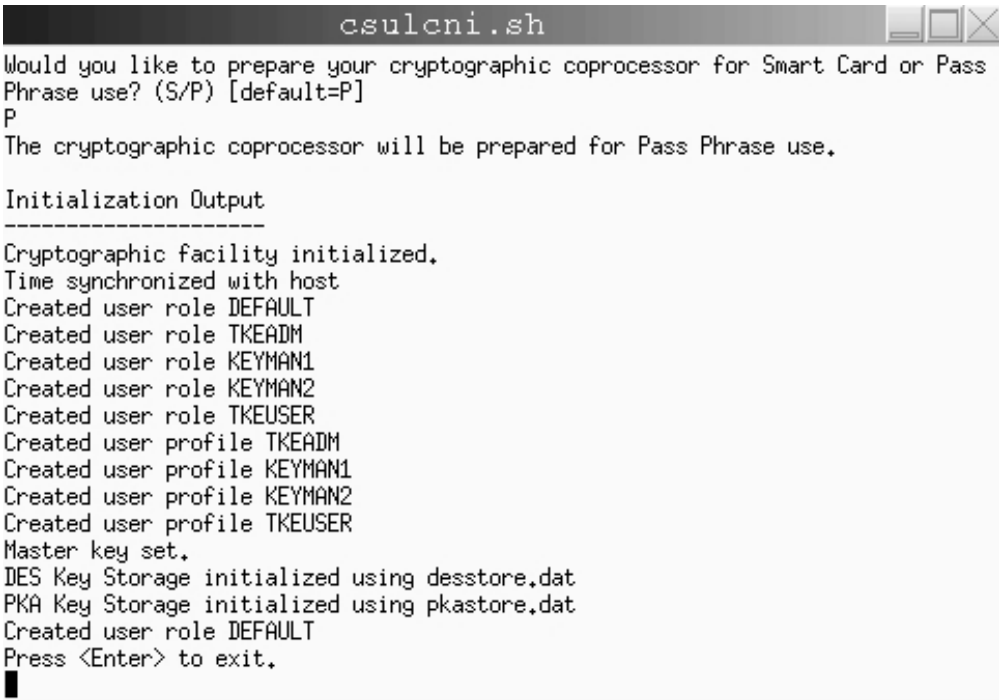
A warning will remind you that this operation will initialize your Cryptographic Coprocessor and all modifications will be lost. Select Y if you would like to continue

Select P for Passphrase.



Figure 241. Crypto Adapter Initialization 2 Window

The TKE Crypto adapter is initialized with the roles and profiles required for the passphrase environment. The time on the workstation and crypto adapter are synchronized. The crypto adapter master key is set and DES and PKA key storages are initialized.



```
csulcni.sh
Would you like to prepare your cryptographic coprocessor for Smart Card or Pass
Phrase use? (S/P) [default=P]
P
The cryptographic coprocessor will be prepared for Pass Phrase use.

Initialization Output
-----
Cryptographic facility initialized.
Time synchronized with host
Created user role DEFAULT
Created user role TKEADM
Created user role KEYMAN1
Created user role KEYMAN2
Created user role TKEUSER
Created user profile TKEADM
Created user profile KEYMAN1
Created user profile KEYMAN2
Created user profile TKEUSER
Master key set.
DES Key Storage initialized using desstore.dat
PKA Key Storage initialized using pkastore.dat
Created user role DEFAULT
Press <Enter> to exit.
```

Figure 242. Crypto Adapter Initialization 3 Window

When complete, press Enter to exit the task.

Access Control Administration

Open the CNM Utility. You can find this task under Trusted Key Entry, Applications. Click Cryptographic Node Management Utility 3.10SC to open the task.

The Cryptographic Node Management Utility is opened. The CNM utility provides a graphical user interface to use in administering access control and managing CCA master keys on the cryptographic adapter in the TKE workstation.

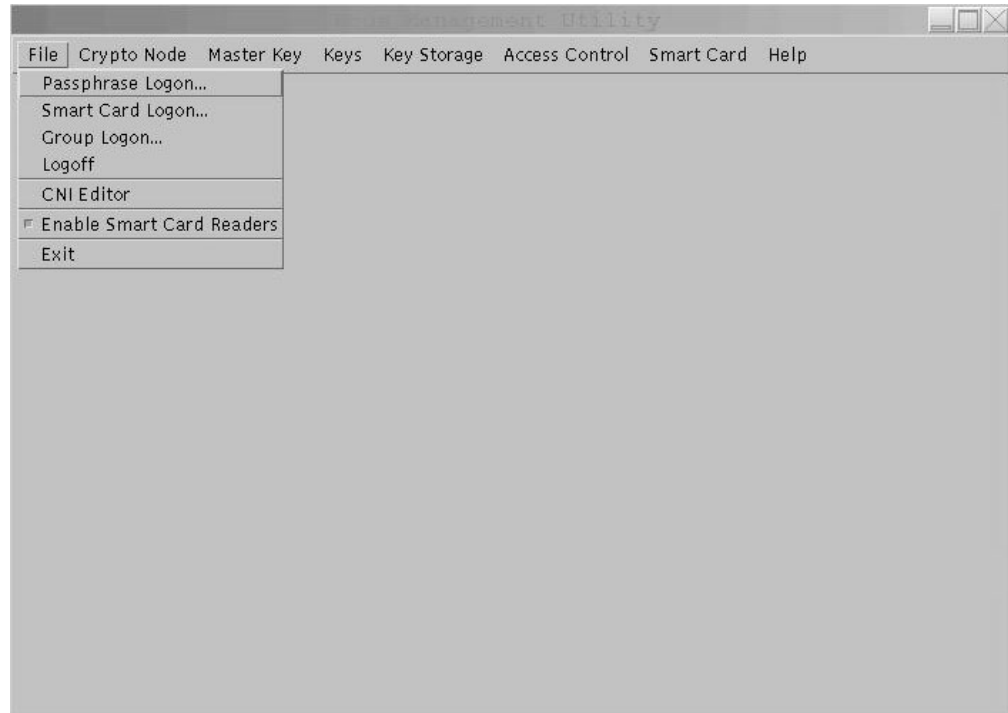


Figure 243. Cryptographic Node Management Utility

The TKE administrator must logon to the crypto node. Click on **File** and then choose **Passphrase Logon...** from the drop down menu.



Figure 244. Passphrase logon

The **Passphrase Logon** window is opened. The user ID (TKEADM) and Pass phrase (TKEADM) are set up for the TKE administrator. They are case sensitive (and must be entered in upper case). Select **Logon**.

Once successfully logged on, change the passphrase for the TKEADM profile. You may also change the Passphrase Expiration Date and the profile's Activation and Expiration dates. Refer to "Edit a User Profile loaded in the TKE Crypto Adapter" on page 263 for instructions on editing a coprocessor-stored user profile. The passphrase is case sensitive. If you save this profile to disk, remember to back up the file to DVD-RAM.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see "Managing Media" on page 377.

At this time, you should also change the passphrase for the other predefined profiles. You may want to define other profiles for the predefined roles. The access control points for each of the predefined roles are listed in "Access Control Points

for Roles” on page 225. Refer to “Define a User Profile” on page 255 for instructions on defining a user profile. Backup your profiles to DVD-RAM.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

Group Logon: Group Logon is supported with TKE V4.2 and higher. Group logon allows multiple users to co-sign a logon to the TKE cryptographic adapter. If you decide to use group logon, you need to define additional user profiles at this time. See “Define a User Profile” on page 255. You then need to define a group profile and assign the user profiles to the group profile (see “Define a Group Profile” on page 260).

Note: The group role overrides the role assigned to the individual profiles. When defining profiles, we recommend that the DEFAULT role be mapped to each of the user profiles to limit the functions that the user can perform outside of the group. The group profile should be mapped to role TKEADM or TKEUSER.

The TKEADM user ID can now logoff the crypto node. Click on **File** and then choose **Logoff** from the drop down menu.

Load First Key Part

If using passphrase logon, see “Passphrase Logon” on page 242. If using group logon, see “Group Logon” on page 243.

Logon to the crypto node as KEYMAN1. The master keys should be changed. Follow the directions in “Loading a new master key from clear key parts” on page 265 for instructions on how to load a new master key from parts. After the first key part is successfully loaded, this user must logoff the crypto node. Backup any key files to a DVD-RAM.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

Load Last Key Part

If using passphrase logon, see “Passphrase Logon” on page 242. If using group logon, see “Group Logon” on page 243.

Next, logon to the crypto node as KEYMAN2. Enter a middle key part (optional) and a last key part. Backup as necessary. You may want to verify the master key verification pattern before setting the master key. See “Verifying Master Key Parts” on page 270 for instructions on the verification procedure.

Warning: If the file is loaded from a floppy or CD/DVD, you must deactivate the floppy or CD/DVD drive before removing the diskette or disc. If the diskette is removed prior to deactivating the drive data could be lost or corrupted. For details on deactivating media see “Managing Media” on page 377.

KEYMAN2 sets the Master Key.

KEYMAN2 now re-enciphers DES and PKA key storage.

KEYMAN2 can now logoff the crypto node.

Access Control Points for Roles

These tables provide the access control points and related functions for the predefined roles.

Profiles using the TKEUSER Role are for TKE authorities.

Table 6. TKEUSER Role

Function	Access Control Point
Clear Diffie-Hellman Key values	X'0252'
Combine Diffie-Hellman Key part	X'0251'
Combine Key Part	X'001C'
Compute Verification Pattern	X'001D'
Decipher	X'000F'
Digital Signature Generate	X'0100'
Digital Signature Verify	X'0101'
Encipher	X'000E'
Export Card Device Certificate	X'02A9'
Generate Key	X'008E'
Generate MDC	X'008A'
Generate Key Set	X'008C'
Load Diffie-Hellman Key mod/gen	X'0250'
Load First Key Part	X'001B'
Load Roles and Profiles	X'0116'
PKA Clear Key Generate	X'0205'
PKA Clone Key Generate	X'0204'
PKA Key Generate	X'0103'
PKA Key Import	X'0104'
Process cleartext ICSF key parts	X'02A0'
Process enciphered ICSF key parts	X'02A1'
RNX access control point	X'02A2'
Reencipher from Master Key	X'0013'
Reencipher to Master Key	X'0012'
Session Key Master	X'02A3'
Session Key Slave	X'02A4'
TKE USER	X'8002'
Unrestrict Combine Key Parts	X'027A'

Profiles using the TKE Administration role allow the user to perform security administration for the TKE workstation. They are able to create, change and delete roles and profiles.

Table 7. TKEADM Role

Function	Access Control Point
Change Authentication Data	X'0114'
Change Profile Expiration Date	X'0113'

Table 7. TKEADM Role (continued)

Function	Access Control Point
Clear FCV	X'011A'
Compute Verification Pattern	X'001D'
Delete Role	X'0118'
Delete User Profile	X'0117'
Initialize Access Control	X'0112'
Load FCV	X'0119'
Load Roles and Profiles	X'0116'
One-Way Hash SHA-1	X'0107'
Reinitialize Device	X'0111'
Reset Battery Low Indicator	X'030B'
Reset Intrusion Latch	X'010F'
Reset Logon Failure Count	X'0115'
Set clock	X'0110'

Profiles using the TKE Key Manager 1 role allow the user to clear the TKE Crypto Adapter new master key register and load first master key parts.

Table 8. KEYMAN1 Role

Function	Access Control Point
Clear New Master Key Register	X'0032'
Compute Verification Pattern	X'001D'
Generate Key	X'008E'
Load Roles and Profiles	X'0116'
Load first Master Key Part	X'0018'

Profiles using the TKE Key Manager 2 role allow the user to load middle and last master key parts, to set the master key, and to re-encipher workstation key storage.

Table 9. KEYMAN2 Role

Function	Access Control Point
Combine Master Key Parts	X'0019'
Compute Verification Pattern	X'001D'
Generate Key	X'008E'
Load Roles and Profiles	X'0116'
PKA Key Token Change	X'0102'
Reencipher to Current Master Key	X'0090'
Set Master Key	X'001A'

The DEFAULT role allows any user to view public role and profile information. It also allows re-initialization of the TKE Crypto Adapter.

Table 10. DEFAULT Role

Function	Access Control Point
Compute Verification Pattern	X'001D'
Export Card Device Certificate	X'02A9'
Load Roles and Profiles	X'0116'
Reinitialize Device	X'0111'

Initializing TKE for smart cards

Enable Smart Card Readers in CNM

Click on Trusted Key Entry and then Cryptographic Node Management Utility 3.10SC. When the application is opened, click on the File dropdown, and click on Enable Smart Card Readers. Close the application.

Steps to initialize the TKE Crypto Adapter for smart card support

1. To initialize the TKE crypto adapter, click on Trusted Key Entry. Under Applications, click on TKE's IBM Crypto Adapter Initialization.



Figure 245. Crypto Adapter Initialization Confirmation Window

A warning will remind you that this operation will initialize your Cryptographic Coprocessor and all modifications will be lost. Select Y if you would like to continue.



```
csulcni.sh
Warning! The following task will initialize your cryptographic coprocessor.
All modifications to the cryptographic coprocessor will be lost.
Would you like to continue? (Y/N) [default=N]
y
Would you like to prepare your cryptographic coprocessor for Smart Card or Pass
Phrase use? (S/P) [default=P]
█
```

Figure 246. Crypto Adapter Initialization - Smart Card or Passphrase

Select S for Smart Card.

The TKE Crypto adapter is initialized with the roles and profiles required for the smart card environment. The time on the workstation and crypto adapter are synchronized. The crypto adapter master key is set and DES and PKA key storages are initialized.



```
csulcni.sh
Warning! The following task will initialize your cryptographic coprocessor.
All modifications to the cryptographic coprocessor will be lost.
Would you like to continue? (Y/N) [default=N]
y
Would you like to prepare your cryptographic coprocessor for Smart Card or Pass
Phrase use? (S/P) [default=P]
s
The cryptographic coprocessor will be prepared for Smart Card use.

Initialization Output
-----
Cryptographic facility initialized.
Time synchronized with host
Created user role DEFAULT
Created user role SCTKEADM
Created user role SCTKEUSR
Master key set.
DES Key Storage initialized using desstore.dat
PKA Key Storage initialized using pkastore.dat
Press <Enter> to exit.
█
```

Figure 247. Crypto Adapter Initialization for smart card complete

When complete, press Enter to exit the task.

2. SCUP initialization tasks

- a. Initialize and personalize a CA smart card.
(see “Initialize and personalize the CA smart card” on page 287)
- b. Backup CA smart card.
(see “Backup a CA smart card” on page 289)
- c. Enroll local TKE cryptographic adapter. Enroll remote TKE cryptographic adapter if applicable.
(see “Enroll a TKE cryptographic adapter” on page 296)
- d. Initialize and enroll TKE smart cards.
(see “Initialize and enroll a TKE smart card” on page 293)
- e. Personalize TKE smart cards.
(see “Personalize a TKE smart card” on page 294)

Close the SCUP application.

3. CNM initialization tasks (Appendix C)

- a. Generate Crypto Adapter logon keys to TKE smart cards that will be used to logon to the TKE cryptographic adapter.
(see “Generate TKE Crypto Adapter logon key” on page 275.)
- b. Define user profiles for the TKE smart cards which have a Crypto Adapter logon key.
(see “Define a User Profile” on page 255.)
- c. Define a group profile (optional). Empty group profiles SCTKEADM and SCTKEUSR are provided. A group may contain 1 to 10 members.
(see “Define a Group Profile” on page 260.)
- d. Reset the DEFAULT role. Your TKE workstation is not secure until you replace the TEMPDEFAULT role with the regular DEFAULT role. See “Open or edit a disk-stored role” on page 250.
- e. Logon to the TKE Crypto Adapter using a TKE smart card profile or a smart card group profile.
(see “Smart Card Logon” on page 242 or “Smart Card Group Logon” on page 245.)
- f. Generate a TKE Crypto Adapter first key part to a TKE smart card.
(see “Generating master key parts to a TKE smart card” on page 267.)
- g. Load the first key part to the new master key register.
(see “Loading master key parts from a TKE smart card” on page 268.)
- h. Generating and loading the first and last key parts should be performed by two individuals to set up a dual control security policy. Remove the TKE smart card of individual A and insert a TKE smart card from individual B. We recommend a dual control security policy for key parts. Generate a TKE Crypto Adapter last key part to the TKE smart card.
- i. Load the last key part to the new master key register. Verify the verification pattern and save it to disk for future reference.
(see “Verifying Master Key Parts” on page 270.)
- j. Set the master key.
- k. Reencipher DES/PKA key storage.
(see “Reenciphering key storage” on page 272.)

Access Control Points for Roles

These tables provide the access control points and related functions for the predefined roles.

Profiles using the SCTKEUSR Role are for TKE authorities.

Table 11. SCTKEUSR Role

Function	Access Control Point
Clear Diffie-Hellman Key values	X'0252'
Combine Diffie-Hellman Key part	X'0251'
Combine Key Part	X'001C'
Compute Verification Pattern	X'001D'
Decipher	X'000F'
Digital Signature Generate	X'0100'
Digital Signature Verify	X'0101'
Encipher	X'000E'
Export Card Device Certificate	X'02A9'
Generate Key	X'008E'
Generate MDC	X'008A'
Generate Key Set	X'008C'
Load Diffie-Hellman Key mod/gen	X'0250'
Load First Key Part	X'001B'
Load Roles and Profiles	X'0116'
One-Way Hash SHA-1	X'0107'
PKA Clear Key Generate	X'0205'
PKA Clone Key Generate	X'0204'
PKA Key Generate	X'0103'
PKA Key Import	X'0104'
Process cleartext ICSF key parts	X'02A0'
Process enciphered ICSF key parts	X'02A1'
RNX access control point	X'02A2'
Reencipher from Master Key	X'0013'
Reencipher to Master Key	X'0012'
Session Key Master	X'02A3'
Session Key Slave	X'02A4'
Unrestrict Combine Key Parts	X'027A'
TKE USER	X'8002'

Profiles using the TKE Administration role allow the user to perform security administration for the TKE workstation. They are able to create, change and delete roles and profiles.

Table 12. SCTKEADM Role

Function	Access Control Point
Change Authentication Data	X'0114'

Table 12. SCTKEADM Role (continued)

Function	Access Control Point
Change Profile Expiration Date	X'0113'
Clear FCV	X'011A'
Clear New Master Key Register	X'0032'
Combine Master Key Parts	X'0019'
Compute Verification Pattern	X'001D'
Delete Role	X'0118'
Delete User Profile	X'0117'
Initialize Access Control	X'0112'
Load FCV	X'0119'
Load Roles and Profiles	X'0116'
Load first Master Key Part	X'0018'
Master Key Extended	X'02A7'
One-Way Hash SHA-1	X'0107'
PKA Key Token Change	X'0102'
RNX access control point	X'02A2'
Reencipher to Current Master Key	X'0090'
Reinitialize Device	X'0111'
Reset Battery Low Indicator	X'030B'
Reset Intrusion Latch	X'010F'
Reset Logon Failure Count	X'0115'
Session Key Master	X'02A3'
Session Key Slave	X'02A4'
Set Master Key	X'001A'
Set clock	X'0110'
Unrestrict Combine Key Parts	X'027A'

The DEFAULT role allows any user to view public role and profile information. It also allows re-initialization of the TKE Crypto Adapter.

Table 13. DEFAULT Role

Function	Access Control Point
Compute Verification Pattern	X'001D'
Export Card Device Certificate	X'02A9'
Load Roles and Profiles	X'0116'
Reinitialize Device	X'0111'

Customize the TKE Application

1. Open the TKE Application by clicking on Trusted Key Entry and then clicking on Trusted Key Entry 5.2.
2. Logon to the TKE Crypto Adapter. See Workstation Logon: Passphrase or Smart Card on “Workstation Logon: Passphrase or Smart card” on page 50 for details.

3. Click on Preferences on the task bar.
4. Enable/Disable the Preferences as appropriate. See “TKE Customization” on page 76 for details.

Appendix B. TKE TCP/IP and Host Considerations

This topic discusses TKE TCP/IP setup and customization, host transaction program setup, and configuring 3270 emulator sessions.

TKE TCP/IP Setup and Customization

TKE uses TCP/IP for communication between the TKE workstation and the MVS operating system. We are assuming that you have TCP/IP already installed and configured. Proceed with:

1. Update the Hosts file with your IP address.

HOST : 9.117.59.140 :

Figure 248. Entry Example

TKE refers to the host by IP address, not by the host name.

Note: If a domain name server (DNS) is running, then this update is unnecessary as all hosts will be identified to the DNS.

2. Save your Hosts file and test it. If TCP/IP is started, you can test changes by opening a command window and issuing the ping command with the name you just added or go to the TKE 5.2 workstation and use the Ping option under the Network Diagnostic Information task.

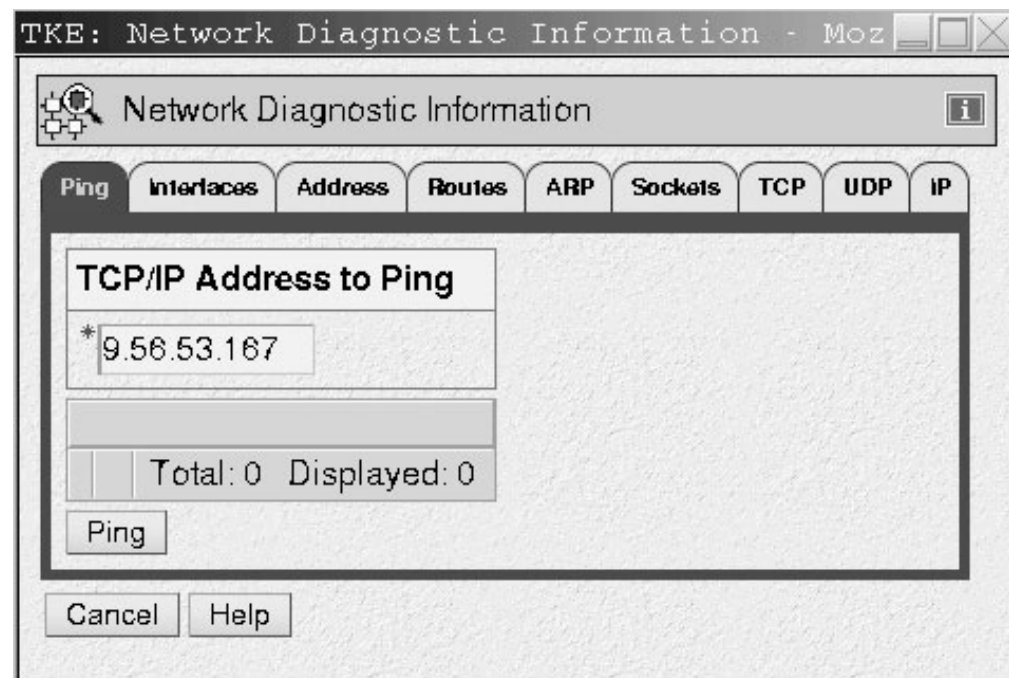


Figure 249. Example of Ping Command

You know you have a connection when you get a response from the ping command.

3. Update your TCPIP profile to reserve a port for the TKE application.

PORT 50003 TCP CSFTTCP	;ICSF TKE Server
---------------------------	------------------

Figure 250. 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 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 commands and programs member, IKJTSOxx, in the SYS1.PARMLIB data set.

AUTHCMD NAMES(	/* AUTHORIZED COMMANDS */	+
COMMAND1	/*	+
COMMAND2	/*	+
COMMAND3	/*	+
.		+
.		+
.		+
CSFTTKE	/* AUTHORIZE TKE */	+
.		+
.		+
.		+

Figure 251. Format of AUTHCMD

2. Set up system security

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 may need to work with your system programmer, since 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 252. 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 253. 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 254. 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 CSF.SAMPLIB(CSFTTCP) and included here. Copy this procedure to your proclib data set and customize it for your installation.

```

//CSFTTCP PROC LEVEL=CSF, MEMBER=CSFHTP3,
//          CPARM='PORT;1000;SET DISPLAY LEVEL;TRACE ALL'
//CLIST EXEC PGM= IKJEFT01,
//          PARM='EX ''&LEVEL..SCSFCLIO(&MEMBER)'' ''&CPARM'' EXEC'
//STEPLIB DD DSN=EZA.SEZALINK, DISP=SHR
//SYSABEND DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSEXEC DD DSN=&LEVEL..SCSFCLIO, DISP=SHR
//SYSPROC DD DSN=&LEVEL..SCSFCLIO, 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 255. Sample Startup Procedure

TKE Startup Parameters

Note: If upgrading from a legacy machine to a z990, z890, z9 EC, z9 BC or System z10 EC and upgrading to TKE 5.2, you must either delete or rename the existing TKECM dataset. The current TKE V3.0, V3.1, V4.0, V4.1, and V4.2 TKECM dataset is not compatible with a z990, z890, z9 EC, z9 BC and System z10 EC system TKECM dataset.

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 CSF.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 and Customization” on page 233).
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.

In previous versions of TCP/IP, almost all configuration data sets were implicitly allocated. Starting with TCP/IP Version 3 Release 2, 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 MVS 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 MVS System console:



```
S CSFTTCP
```

Figure 256. 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 CSFHTP3.

Cancel the TKE server

To cancel the TKE server:



```
S CSFTCTCP
```

Figure 257. Cancel the TKE server

A sample procedure CSFTCTCP is shipped in CSF.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 will default to 50003.

Note: Depending on your system setup, you may need to define the CSFTCTCP task to the RACF STARTED class in the same manner you did for the TKE started task CSFTTCP.

```
REDEFINE STARTED CSFTCTCP.CSFTCTCP STDATA(USER(userid))  
SETROPTS RACLIST(STARTED) REFRESH
```

Configure 3270 Emulator Sessions for TKE

An MVS session is required, on the host, for several tasks executed on TKE 5.2 to complete. If you do not have access to the MVS system, outside of the TKE Workstation, create access to the MVS 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.

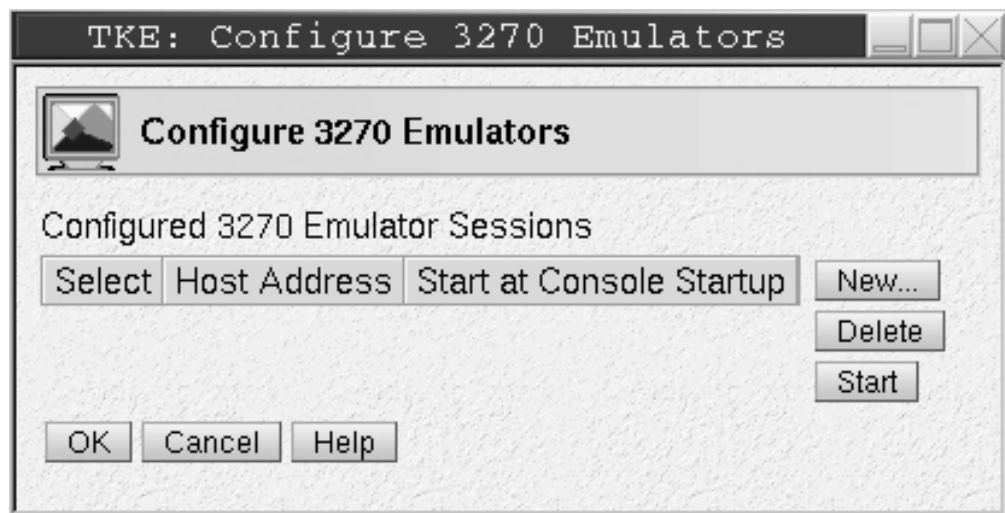


Figure 258. Configure 3270 Emulators

1. Click on the new button 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 Enable or Disable from the Start at Console Startup drop down menu.

Enabled

When the console starts this session will also be started.

Disabled

When the console starts this session will not start.

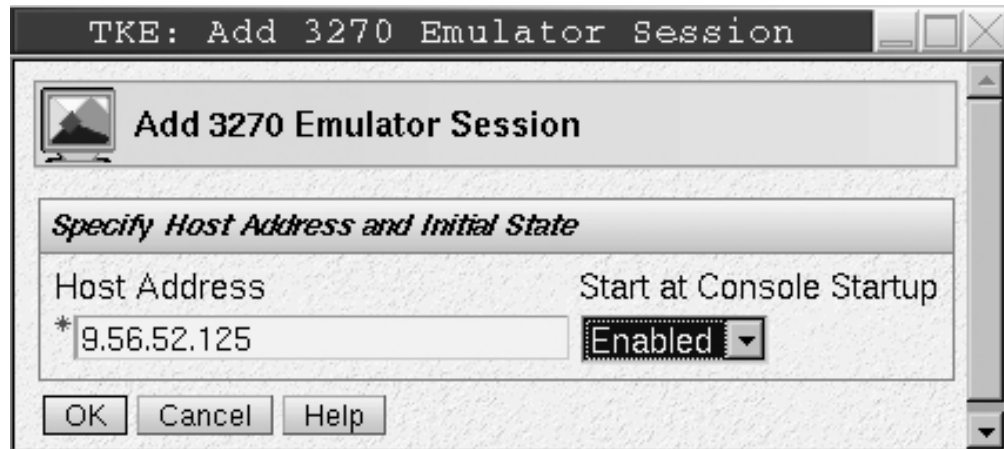


Figure 259. Add 3270 Emulator Session

5. To save the emulator session definition press OK.
6. On the Configure 3270 Emulators window press OK to save the session. Press Cancel to end without saving the session.

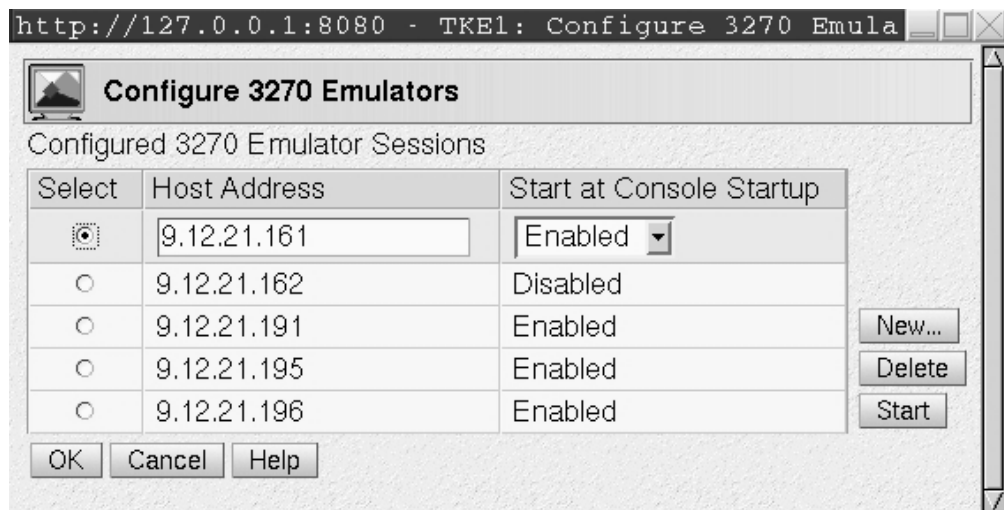


Figure 260. Start or Delete a 3270 Emulator Session

7. To Start or Delete a Host Address select the Host Address from the list and press Start or Delete.

Appendix C. 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 cryptographic 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 Crypto Adapter in the TKE workstation.

Note: Smart Card and Smart Card Group options within the CNM panels will only be available if CNM is updated to support Smart Cards. See “Initializing TKE for smart cards” on page 227.

To start CNM, go to Trusted Key Entry, Applications, and click on Cryptographic Node Management Utility 3.10SC.



Figure 261. CNM main window

File Menu

From the **File** pull-down, you can choose to logon or logoff the TKE cryptographic adapter.

Logon to the TKE cryptographic adapter: From the **File** pull-down menu, select the type of logon:

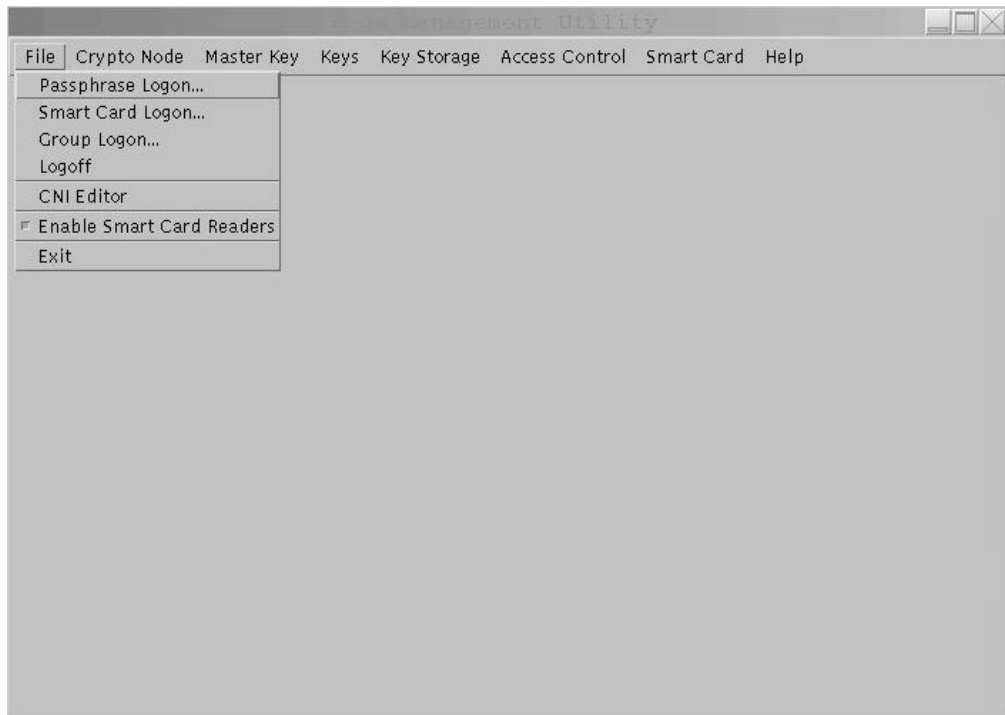


Figure 262. CNM main window - File pull down menu

Passphrase Logon

You will be prompted to enter a user ID and passphrase. They are both case sensitive.

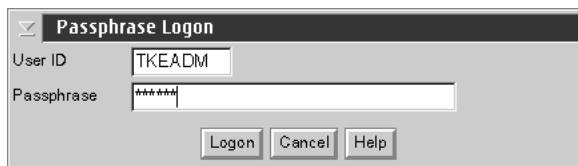


Figure 263. Passphrase logon prompt

Smart Card Logon

Follow the prompts to insert your TKE smart card into smart card reader 2 and to enter your PIN.

Note: Smart card support must be activated in CNM before logon with a TKE smart card is available. See step 1 in “Steps for smart card setup” on page 35.

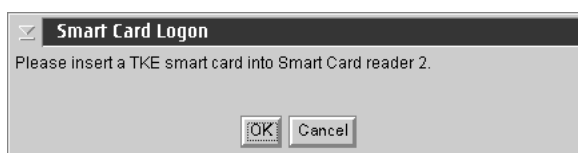


Figure 264. TKE smart card prompt

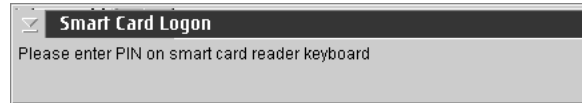


Figure 265. PIN prompt

Group Logon

Group logon allows multiple users to cosign a logon to the TKE cryptographic adapter. At the prompt, enter a group profile name for Group ID. Profile names are case sensitive.



Figure 266. Passphrase group logon - group member list

There are two types of group logon:

- Passphrase Group Logon
- Smart Card Group Logon

Passphrase Group Logon

The passphrase group logon window is displayed if a passphrase group profile name is entered at the Group Logon prompt.

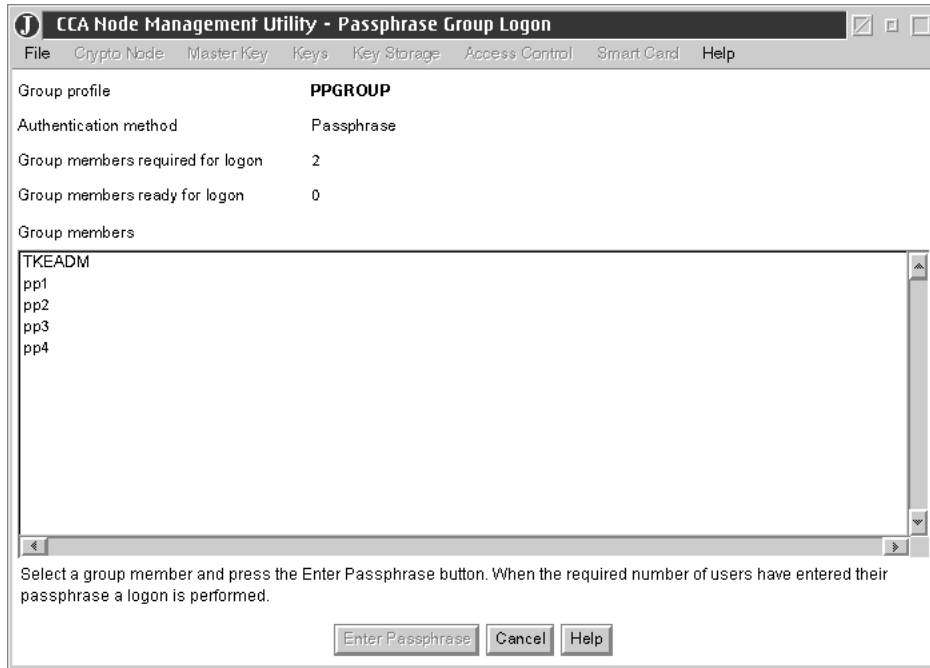


Figure 267. Group logon prompt

- The group profile name is displayed. The authentication method is Passphrase. *Group members required for logon* is the number of users that must sign the logon before the logon is performed. To sign the logon, the selected group member must enter his passphrase. *Group members ready for logon* is the number of users that have entered their passphrase. This counter is incremented each time a user signs the logon. The group members are listed. Select a group member from the list and press the *Enter Passphrase* button. The user is prompted for his passphrase.

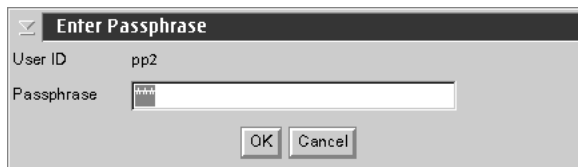


Figure 268. Passphrase group logon - enter passphrase prompt

The list is updated indicating that the user is *ready for logon*. *Group members ready for logon* is incremented.

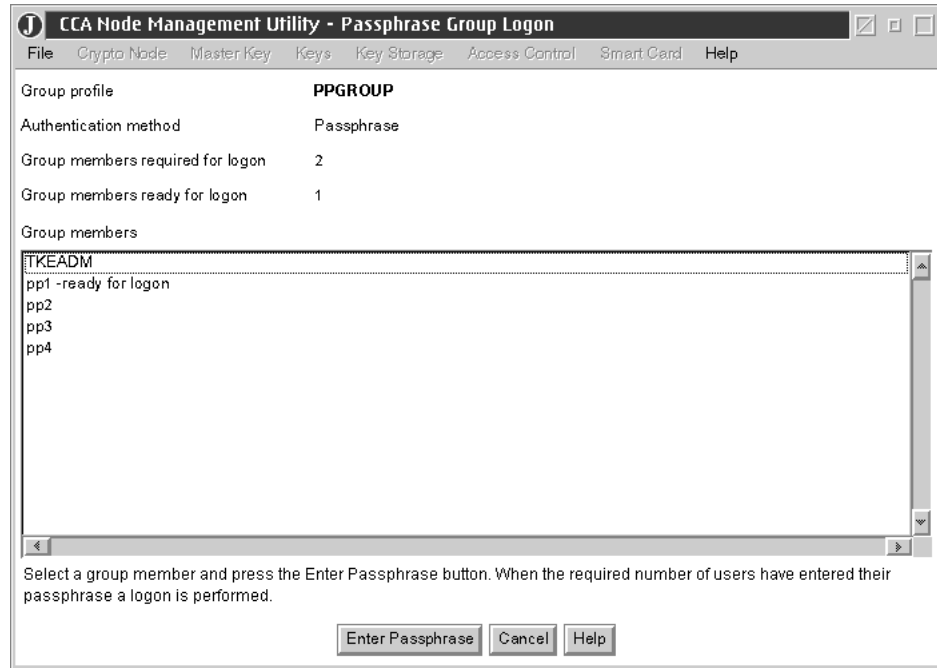


Figure 269. Passphrase group logon - member is ready for logon

When *Group members ready for logon* equals *Group members required for logon*, the logon is performed.

If the group logon is successful, *Group Logon Completed* will be displayed.



Figure 270. Passphrase group logon successful

If the group logon should fail (for example, a user profile has expired, an incorrect passphrase was entered, etc.), *Group members ready for logon* is reset to zero and group logon must start over.

Smart Card Group Logon

The smart card group logon window is displayed if a smart card group profile is entered at the Group Logon prompt.

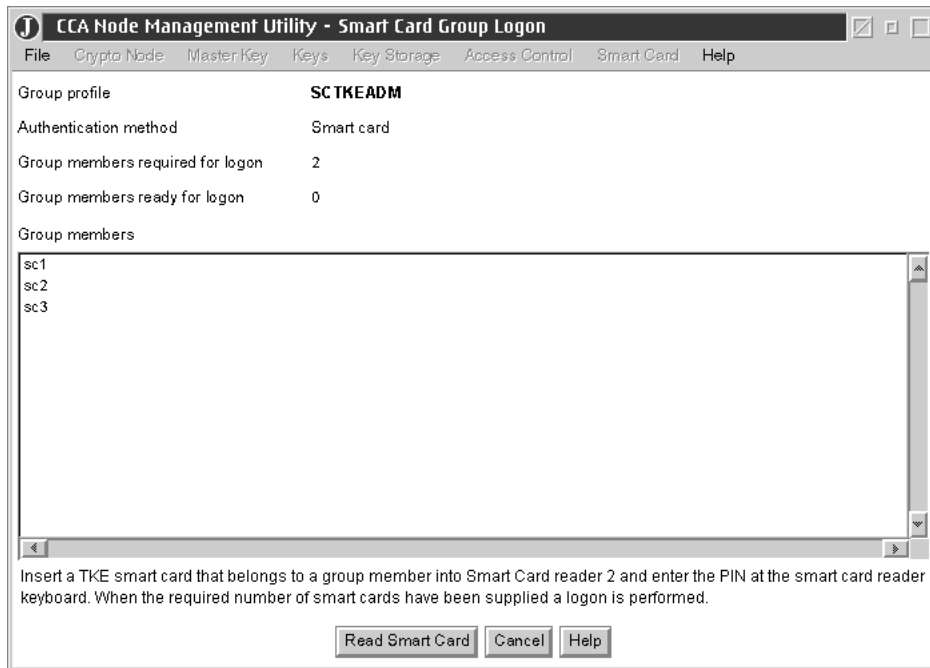


Figure 271. Smart card group logon window

The group profile name is displayed. The authentication method is Smart card.

Group members required for logon is the number of users that must sign the logon before the logon is performed. To sign the logon, the group member must insert his TKE smart card into smart card reader 2 and enter his correct PIN on the smart card reader 2 PIN pad.

Group members ready for logon is the number of users that have signed the logon with their TKE smart card and PIN. This counter is incremented each time a user signs the logon.

The group members are listed. Insert the TKE smart card for a group member and press the *Read Smart Card* button. The user is prompted for his PIN. If the PIN is correct, the list is updated indicating that the user is *ready for logon*. *Group members ready for logon* is incremented. If an incorrect PIN is entered, the user is prompted to retry another PIN or cancel.

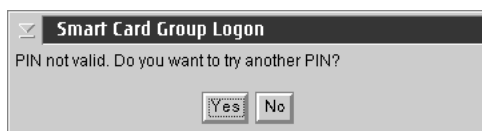


Figure 272. Smart card group logon — retry PIN prompt

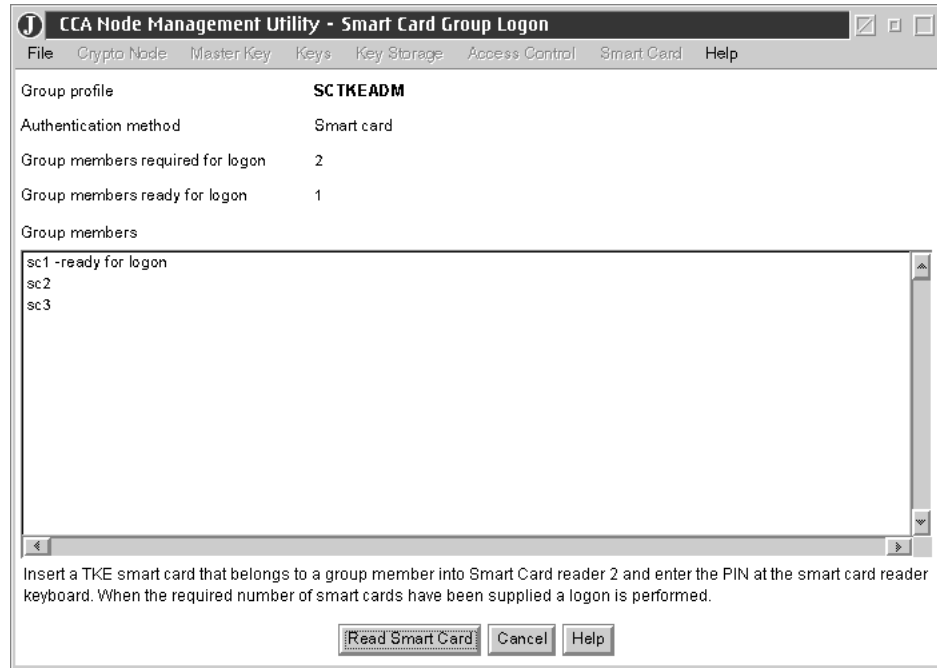


Figure 273. Smart card group logon window - member is ready for logon

Note: A TKE smart card is blocked after three incorrect PIN attempts. To unblock a PIN, you must exit from CNM and use SCUP. (Refer to “Unblock PIN on a TKE smart card” on page 295.)

When *Group members ready for logon* equals *Group members required for logon*, the logon is performed. If the group logon is successful, *Group Logon Completed* will be displayed.



Figure 274. Smart card group logon successful

If the group logon should fail (for example, a user profile has expired), *Group members ready for logon* is reset to zero and group logon must start over.

Logoff

Logoff of the TKE cryptographic adapter: From the **File** pull-down menu, select **Logoff**.

Select **Yes** to confirm logoff. A successful message is displayed.

Crypto Node Menu

TKE Crypto Adapter Clock-Calendar

The TKE Crypto Adapter uses its clock-calendar to record time and date and to prevent replay attacks in passphrase-based profile authentication.

Note: If there is more than 5 minutes difference between the TKE crypto adapter clock and the TKE workstation clock, the TKE crypto adapter cannot be used by either CNM or TKE.

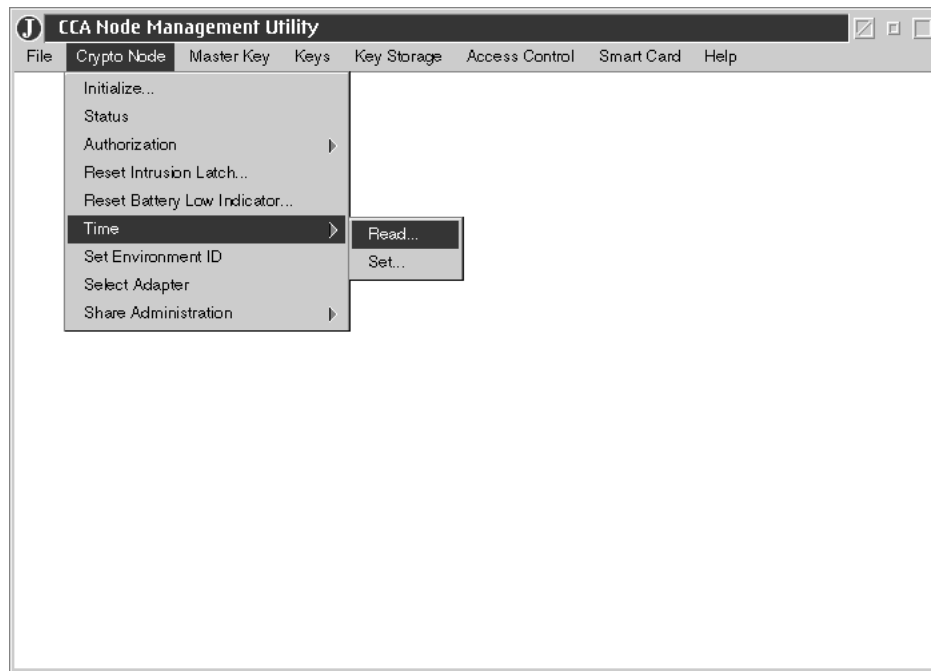


Figure 275. CNM main window — Crypto Node Time sub-menu

Read Clock-Calendar

To read the TKE 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).

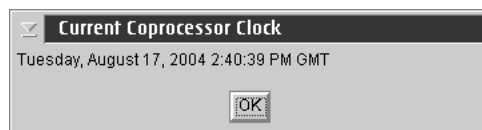


Figure 276. Current Coprocessor Clock

3. Finish the task by selecting **OK**.

Synchronize Clock-Calendar

To synchronize the TKE crypto adapter clock-calendar with the TKE workstation clock:

Note: If not already logged on, logon to the 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 prompt is displayed.



Figure 277. Sync time with host window

3. Respond **Yes** to synchronize the clock-calendar with the host.
4. Finish the task by selecting **OK**.

Note: If the time is more than 5 minutes off, the clock on the TKE workstation needs to be reset before the clock-calendar can be synchronized. See Setting the Clock “Setting the Clock” on page 219 for details.

Access Control Menu

The access control system restricts or permits the use of commands based on roles and user profiles. You create roles that correspond to the needs and privileges of assigned users.

To access the privileges assigned to a role (those that are not authorized in the default role), a user must logon to the TKE cryptographic adapter using a unique user profile. Each user profile is associated with a role. Multiple profiles can use the same role. The TKE Crypto Adapter authenticates logons using the passphrase or TKE smart card and PIN associated with the profile that identifies the user.

The TKE cryptographic adapter always has at least one role, the DEFAULT role. Use of the DEFAULT role does not require a user profile. Any user can use the functions permitted by the DEFAULT role without logging onto or being authenticated by the TKE Crypto Adapter.

A TKE administrator can manage roles and profiles from the CNM utility Access Control pull-down menu.



Figure 278. CNM main window — Access Control menu

TKE predefined roles

A role defines permissions and other characteristics of the users assigned to that role. These lists are the predefined roles supplied with TKE.

For passphrase:

- TKEUSER
- TKEADM
- KEYMAN1
- KEYMAN2

For smart card:

- SCTKEUSR
- SCTKEADM

These roles are in the CNM Data Directory. Multiple profiles can be associated with the same role.

Additional roles are not needed for TKE.

Open or edit an existing role

Use the CNM utility to:

- Open or edit a disk-stored role
- Edit a role loaded in the TKE Crypto Adapter

Open or edit a disk-stored role

Follow these steps for opening and editing a disk-stored role.

Follow these steps when you need to reload the DEFAULT or the TEMPDEFAULT role. The TEMPDEFAULT role has ACPs for all functions and is necessary for enrolling TKE cryptographic adapters. It should then be reset to the DEFAULT role.

Note: You should not edit the DEFAULT or the TEMPDEFAULT role.

To open or edit a role stored on disk:

1. From the **Access Control** pull-down menu, select **Roles**; a list of currently defined roles is displayed:

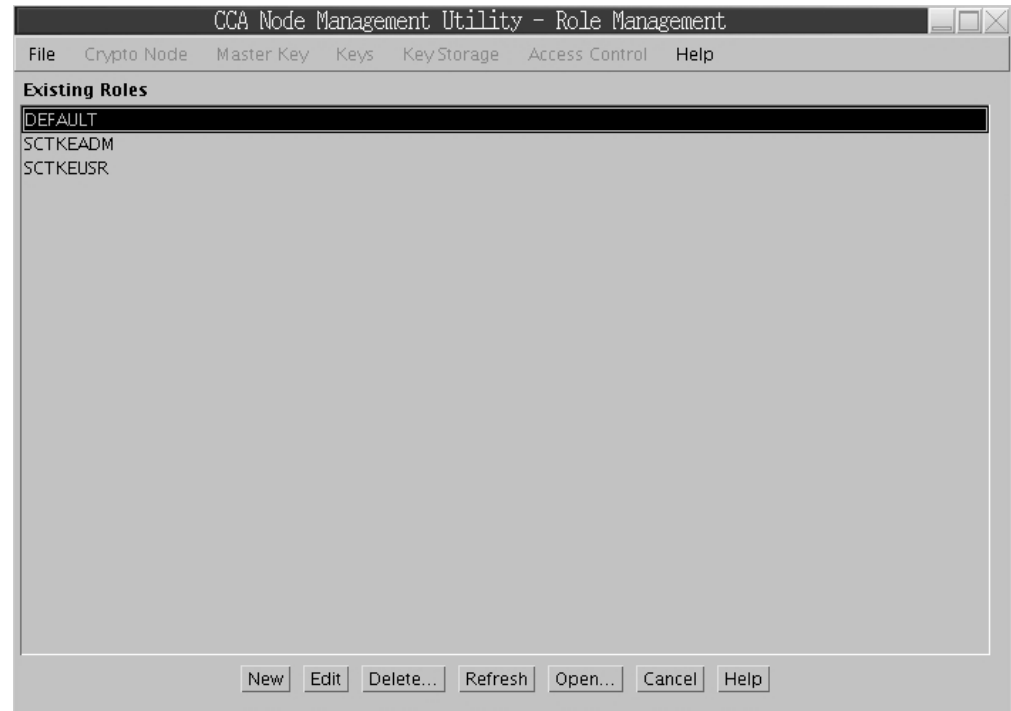


Figure 279. Role Management panel - list of roles loaded to the TKE crypto adapter for Smart Card

2. Select **Open**; you are prompted to choose a file.

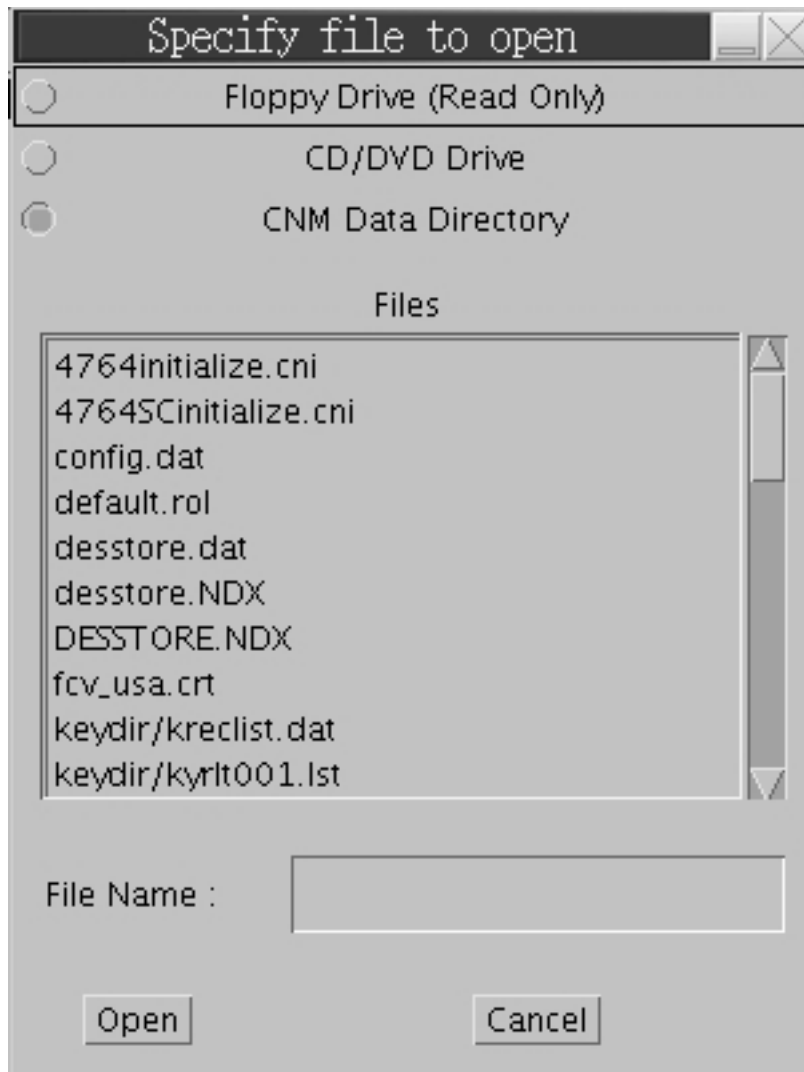


Figure 280. Open a disk-stored role - choose a file

Note: All predefined roles and profiles will be in the CNM Data Directory.

3. Open a file; data is displayed in the Role Definition panel.

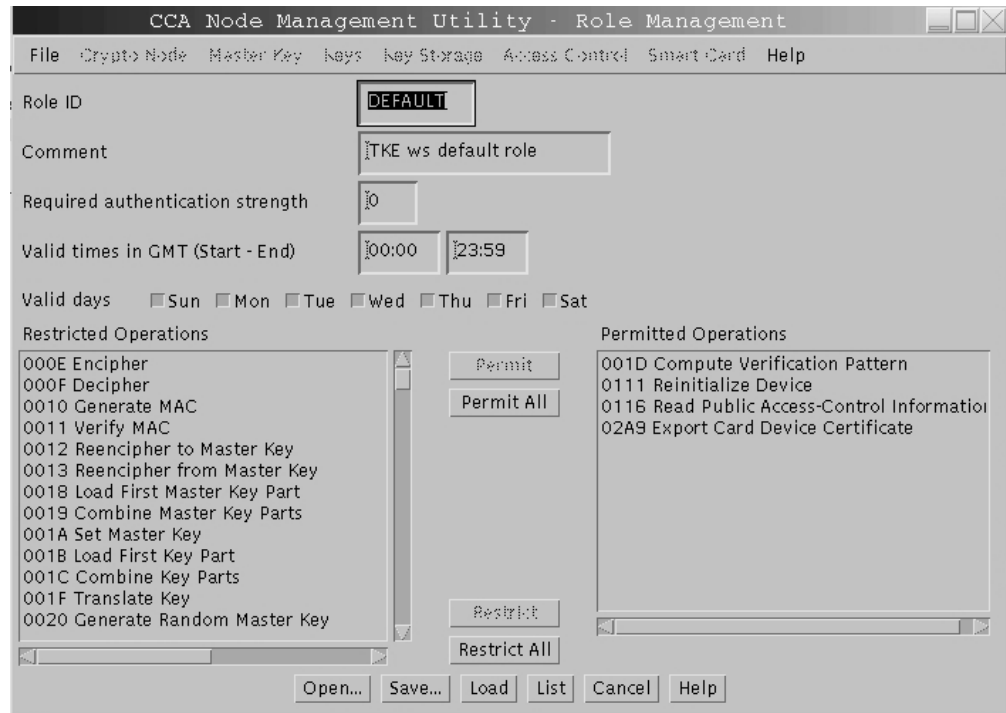


Figure 281. Role Definition panel - role is displayed

4. Select **Load** to save the new role to the TKE cryptographic adapter.
5. Role successfully loaded message appears.

Edit a role loaded in the TKE Cryptic Adapter

To edit a role loaded in the TKE cryptographic adapter:

1. From the **Access Control** pull-down menu, select **Roles**; a list of currently defined roles is displayed.
2. Highlight the role you want to edit.
3. Select **Edit**; data is displayed in the Role Definition panel.
4. Edit the role. The Restricted Operations column lists the access points that are not allowed for this role. The Permitted Operations column lists the access points that are allowed for this role. Select access point(s) from the Restricted Operations column and press Permit to move it to the Permitted Operations column.

We do not recommend deleting any access control points from the predefined roles. If you do, CNM or TKE functions may fail with an access control error.

If you are migrating from previous releases of TKE to TKE V5.2, you may need to add access control points to your roles. See Chapter 3, "Migration," on page 25.

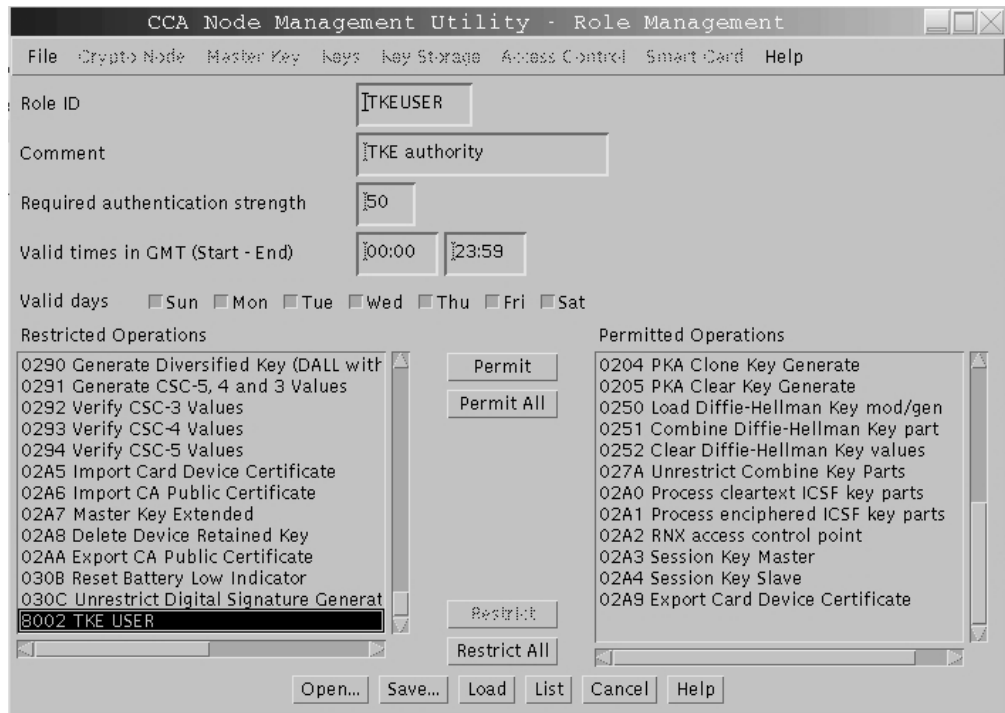


Figure 282. Edit a role - highlight access point to permit

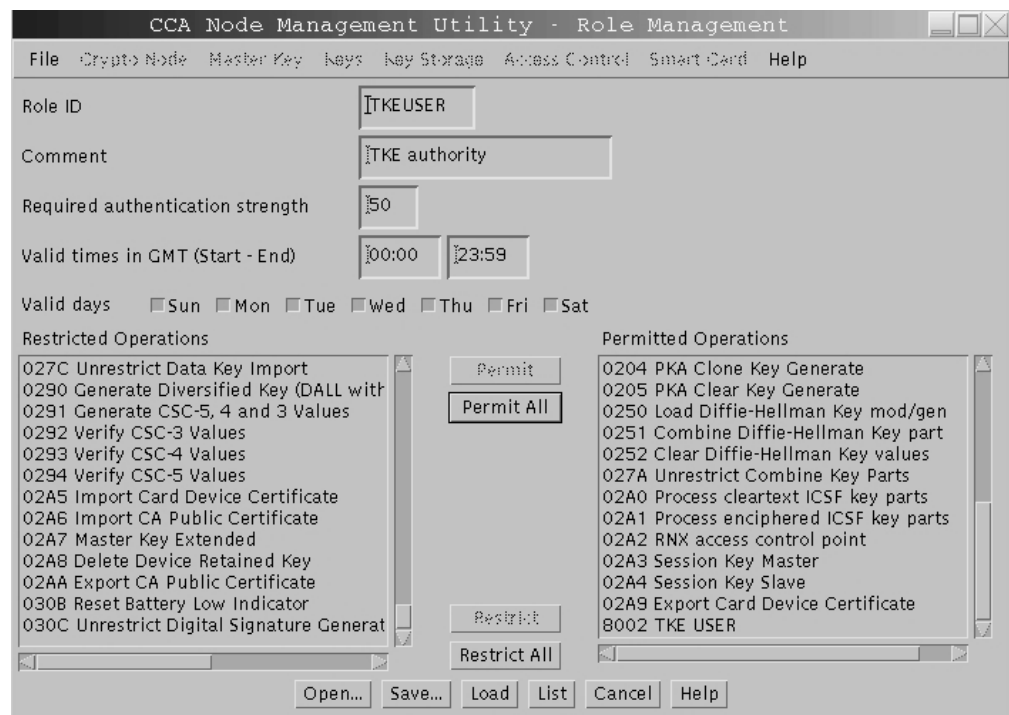


Figure 283. Edit a role - access point is moved to Permitted Operations column

5. Select Save to save the role to disk; you will be prompted for a filename. You may save the file to either the CNM data directory or the CD/DVD disk. Select Load to load the role into the TKE cryptographic adapter.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

Define a User Profile

A user profile identifies a specific user to the TKE cryptographic adapter. To define a user profile:

1. From the **Access Control** pull-down menu, select **Profiles**. A list of existing profiles is displayed.



Figure 284. Profile management panel — profile list

Passphrase profiles

TKE supplies these predefined profiles:

TKEUSER	associated with role TKEUSER; use this profile for logging onto the TKE application and performing TKE functions without smart cards.
TKEADM	associated with role TKEADM; use this profile for managing the TKE Crypto Adapter using CNM, including defining roles/profiles
KEYMAN1	associated with role KEYMAN1; use this profile to load the first master key part to the TKE Crypto Adapter new master key register
KEYMAN2	associated with role KEYMAN2; use this profile 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.

Smart card profiles

TKE supplies these predefined profiles:

SCTKEADM associated with role SCTKEADM. This is an empty group profile that can be updated to include the group members after the group member user profiles are defined. This profile allows the administration of the TKE Crypto Adapter using smart cards; including generating/loading TKE Crypto Adapter master key parts and loading roles/profiles.

SCTKEUSR associated with role SCTKEUSR. This is an empty group profile that can be updated to include the group members after the group member user profiles are defined. This profile allows all TKE application functions using smart cards.

2. Select **New** to define a new user profile. A sub-menu is displayed. Select the profile type - Passphrase, Smart Card or Group.



Figure 285. Define a new profile — select profile type

Depending on your choice, see these topics:

- “Define a Passphrase Profile”
- “Define a Smart Card Profile” on page 258
- “Define a Group Profile” on page 260

Define a Passphrase Profile

1. If Passphrase is selected as the profile type, this panel is displayed:

The screenshot shows the 'CCA Node Management Utility - Profile Management' window. It features a menu bar with options: File, Crypto Node, Master Key, Keys, Key Storage, Access Control, Smart Card, and Help. The main panel contains several input fields: 'User ID' (empty), 'Comment' (empty), 'Activation Date' (07/27/2004), 'Expiration Date' (07/27/2004), 'Role' (a dropdown menu currently showing 'DEFAULT', 'SCTKEADM', and 'SCTKEUSR'), 'Passphrase' (empty), 'Confirm Passphrase' (empty), and 'Passphrase Expiration Date' (10/27/2004). At the bottom of the window, there is a row of buttons: 'Open...', 'Save...', 'Load', 'Change Passphrase', 'List', 'Cancel', and 'Help'.

Figure 286. Profile Management panel — Passphrase profile

2. Fill in the fields on the panel:

User ID The name of the profile. A maximum of 8 characters may be specified. This field is case sensitive.

Comment An optional character string. A maximum of 20 characters may be specified.

Activation Date Determines the first date when the user can logon. This field defaults to the current date. Change this date as appropriate.

Expiration Date Determines the last date when the user can logon. This field defaults to the current date. Change this date as appropriate.

Role The name of the role that defines the permissions granted to the profile. Select a role from the list.

Note: If this user profile will be assigned to a group profile, we recommend mapping the DEFAULT role to this user profile. This limits the access this profile has outside of the group.

Passphrase The character string that the user must enter to logon to the TKE cryptographic adapter. A maximum of 64 characters may be specified. This field is case sensitive. The Passphrase and Confirm Passphrase fields must match.

Confirm Passphrase This field is identical to the Passphrase field. It is case sensitive. The Passphrase and Confirm Passphrase fields must match.

Passphrase Expiration Date The expiration date for the passphrase. This date will default to

90 days from the current date. The expiration date can be changed. Every passphrase contains an expiration date, which defines the lifetime of that passphrase. This is different from the expiration date of the profile itself.

Figure 287. Profile Management panel — Passphrase profile fields filled in

3. Select **Save** to save the profile to disk.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

4. Select **Load** to load the profile into the TKE Crypto Adapter.

Other actions and tasks available from this panel are:

- Select **Open** to work with a profile saved to disk. You will be prompted to select a file.
- Select **Change Passphrase** to change the profile’s Passphrase and Passphrase Expiration Date.
- Select **List** to return to the list of existing profiles.
- Select **Cancel** to return to the CNM main window.

Define a Smart Card Profile

1. If Smart card is selected as the profile type, you will be prompted to insert a TKE smart card into smart card reader 2.

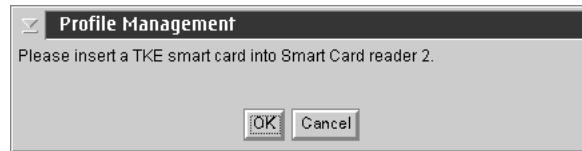


Figure 288. Smart card profile — TKE smart card prompt

2. The TKE smart card is read and the information is displayed in this panel:

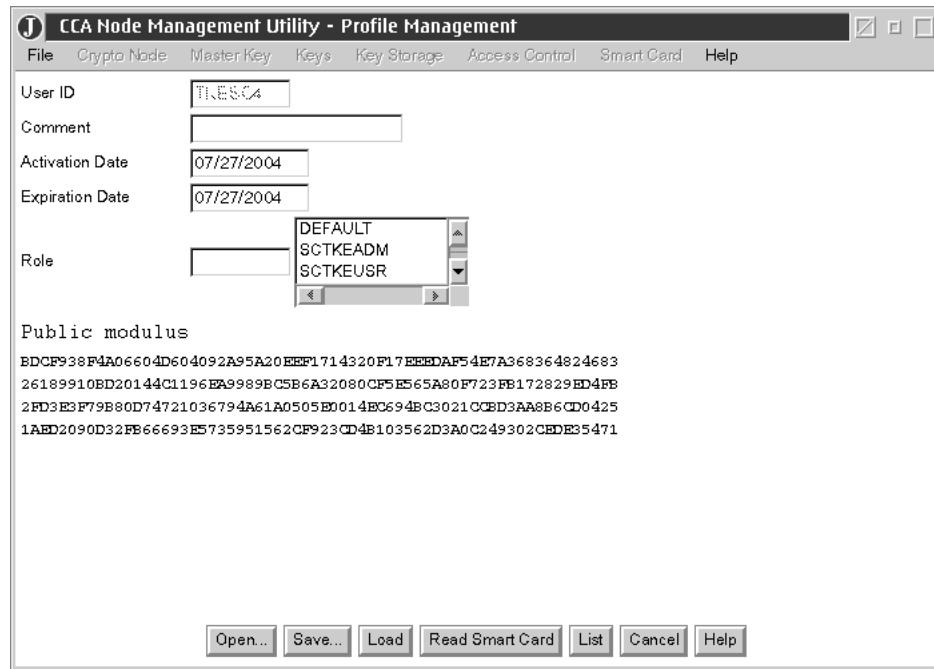


Figure 289. Profile management panel — smart card profile

3. Fill in the fields on the panel:

- | | |
|------------------------|--|
| User ID | The name of the profile. This field is read from the TKE smart card and cannot be changed. The User ID is set when the Crypto Adapter logon key is generated. (See Generate Crypto Adapter logon key). |
| Comment | An optional character string. A maximum of 20 characters may be specified. |
| Activation Date | Determines the first date when the user can logon. This field defaults to the current date. Change this date as appropriate. |
| Expiration Date | Determines the last date when the user can logon. This field defaults to the current date. Change this date as appropriate. |
| Role | The name of the role that defines the permissions granted to the profile. Select a role from the list. |

Note: If this user profile will be assigned to a group profile, we recommend mapping the DEFAULT role to this user profile. This limits the access this profile has outside of the group.

Public Modulus

This is the public modulus of the TKE Crypto Adapter login key read from the TKE smart card. This field cannot be changed. See “Generate TKE Crypto Adapter login key” on page 275.

CCA Node Management Utility - Profile Management

File Crypto Node Master Key Keys Key Storage Access Control Smart Card Help

User ID: T\ESC4

Comment: Tester 4 smart card

Activation Date: 07/27/2004

Expiration Date: 07/27/2005

Role: DEFAULT

Public modulus

EDCF938F4A06604D604092A95A20EEF1714320F17EEDAF54E7A368364824683
 26189910BD20144C1196EA9989BC5B6A32080CF5E565A80F723FB172829ED4FB
 2FD3E3F79B80D74721036794A61A0505ED014EC694BC3021CED3AA8B6CD0425
 1AED2090D32FB66693E5735951562CF923CD4B103562D3A0C249302CEDE35471

Open... Save... Load Read Smart Card List Cancel Help

Figure 290. Profile Management panel – smart card profile fields filled in

4. Select **Save** to save the profile to disk.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

5. Select **Load** to load the profile into the TKE Crypto Adapter.

Other actions and tasks available from this panel are:

- Select **Open** to work with a profile saved to disk. You will be prompted to select a file.
- Select **Read Smart Card** to read the User ID and public modulus from the TKE smart card inserted in smart card reader 2.
- Select **List** to return to the list of existing profiles.
- Select **Cancel** to return to the CNM main window.

Define a Group Profile

1. If Group is selected as the profile type, this panel is displayed:

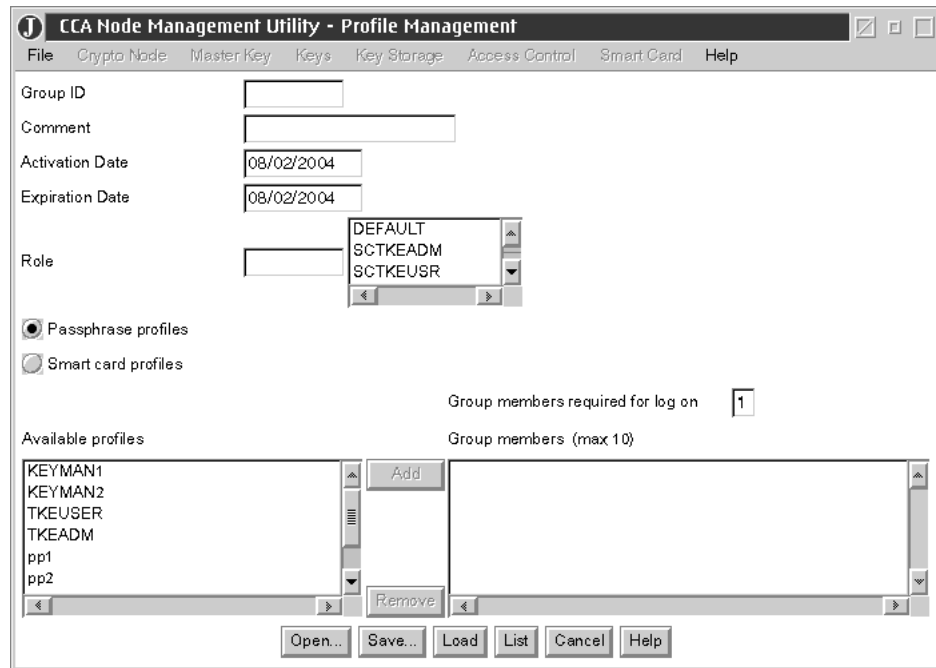


Figure 291. Profile Management panel — Passphrase Group profile

2. Fill in the fields on the panel:

Group ID The name of the profile. A maximum of 8 characters may be specified. This field is case sensitive.

Comment An optional character string. A maximum of 20 characters may be specified.

Activation Date Determines the first date when the group can logon. This field defaults to the current date. Change this date as appropriate.

Expiration Date Determines the last date when the group can logon. This field defaults to the current date. Change this date as appropriate.

Role 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 overrides the roles of the individual user profiles.

Passphrase profiles/Smart Card profiles

Select the profile type for this group profile. The profiles for the selected profile type are listed in the Available profiles container.

Available profiles

This container lists all the profiles for the selected profile type. Highlight the profiles and press the Add button to add them to the Group members container

Group members

This container lists the profiles that are members of this group. A group may have a maximum of 10 members. To remove members from the group, highlight the profiles from the Group members container and press the Remove button.

Group members required for log on

This is the number of users that must sign the logon before the logon is performed. The minimum is 1, the maximum is the number of members in the group, which cannot exceed 10.

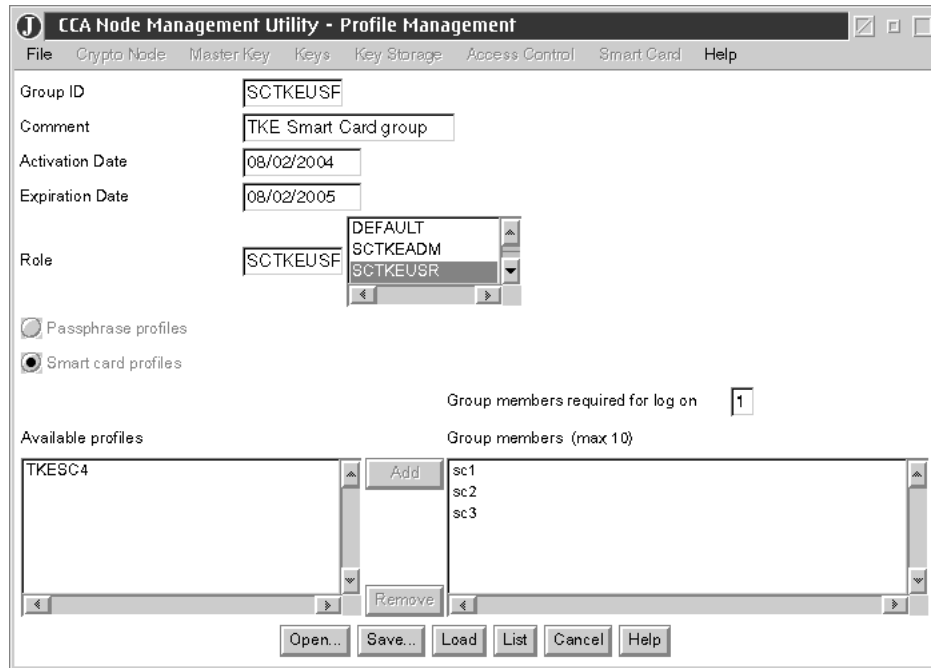


Figure 292. Profile Management panel — Smart Card Group profile filled in

3. Select **Save** to save the profile to disk.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

4. Select **Load** to load the profile into the TKE Crypto Adapter.

Other actions and tasks available from this panel are:

- Select **Open** to work with a profile saved to disk. You will be prompted to select a file.
- Select **List** to return to the list of existing profiles.
- Select **Cancel** to return to the CNM main window.

Working with User Profiles

From the Profile Management panel you can:

- Edit a disk-stored user profile
- Edit a user profile loaded in the TKE Crypto Adapter
- Delete a user profile loaded in the TKE Crypto Adapter
- Reset the user-profile-failure count (valid only for passphrase user profiles)

Edit a Disk-Stored User Profile

To edit a profile stored to disk:

1. From the **Access Control** pull-down menu, select **Profiles**; a list of existing profiles is displayed.

2. Select **Open**; you are prompted to choose a file.
3. Open a file; data is displayed in the User Profile Definition panel.
4. Edit the profile.
5. Select **Save** to save the profile to disk; select **Load** to load the profile into the TKE Crypto Adapter. Back-up any changed profiles to DVD-RAM.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

Edit a User Profile loaded in the TKE Crypto Adapter

To edit a user profile loaded in the TKE Crypto Adapter:

1. From the **Access Control** pull-down menu, select **Profiles**; a list of existing profiles is displayed.
2. Highlight the profile you want to edit.
3. Select **Edit**; data is displayed in the User Profile Definition panel.
4. Edit the profile.
5. Select **Save** to save the profile to disk; select **Replace** to load the profile into the TKE Crypto Adapter. Back-up any changed profiles to diskette.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

Delete a User Profile loaded in the TKE Crypto Adapter

To delete a user profile loaded in the TKE Crypto Adapter:

1. From the **Access Control** pull-down menu, select **Profiles**; a list of existing profiles is displayed.
2. Highlight the profile you want to delete.
3. Select **Delete**; the profile is deleted.

Reset the user-profile-failure count

To prevent unauthorized logons, the access-control system maintains a logon-attempt-failure count for each passphrase user profile. After three unsuccessful passphrase attempts, the profile is disabled.

To reset the failure count:

1. From the **Access Control** pull-down menu, select **Profiles**; a list of existing profiles is displayed.
2. Highlight the disabled profile.
3. Select **Reset FC**; a confirmation dialog box is displayed.
4. Select **Yes** to confirm; the logon-attempt-failure count is reset to zero.

This function has no effect on smart card or group profiles.

Master Key Menu

The master key is stored in the tamper resistant TKE cryptographic adapter. It is used to encipher other keys. The master key is a 168-bit key formed from three 56-bit parts. A random master key is generated and set when the TKE 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 entering key parts generated to TKE smart cards.

The TKE Crypto Adapter has three master key registers:

- The active master key is stored in the current master key register.
- The previous master key is stored in the old master key register.
- The new master key register is an interim location used to combine master key parts to form a new master key

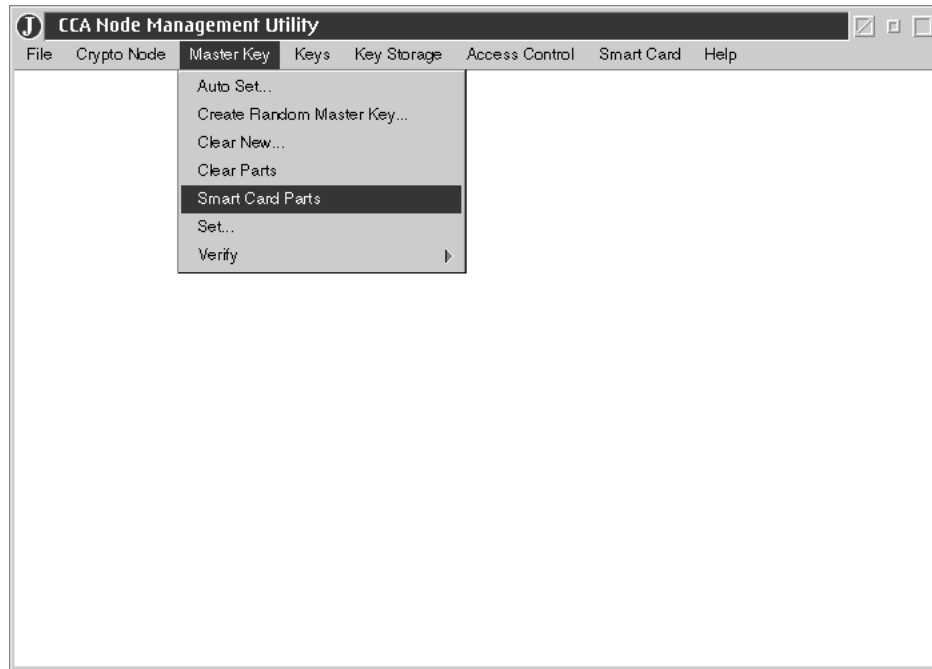


Figure 293. CNM main window — Master Key pull-down menu

Clearing the new master key register

The new master key register must be empty prior to loading a first key part. If it's not empty or if you loaded the wrong key part, you can clear the register by:

1. From the **Master Key** pull-down menu, select **Clear New...**; you will be prompted to confirm clearing the new master key register. Select Yes to confirm.



Figure 294. Clear New Master Key Register — confirm clearing

2. The new master key register is cleared. Select OK to finish.



Figure 295. Clear New Master Key Register — register cleared

Loading a new master key from clear key parts

To set a new master key into the TKE Crypto Adapter, load the first key part, any middle key parts, and the last key part into the new master key register, and then set 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 pull-down menu, select Clear Parts; the Load Master Key panel is displayed.

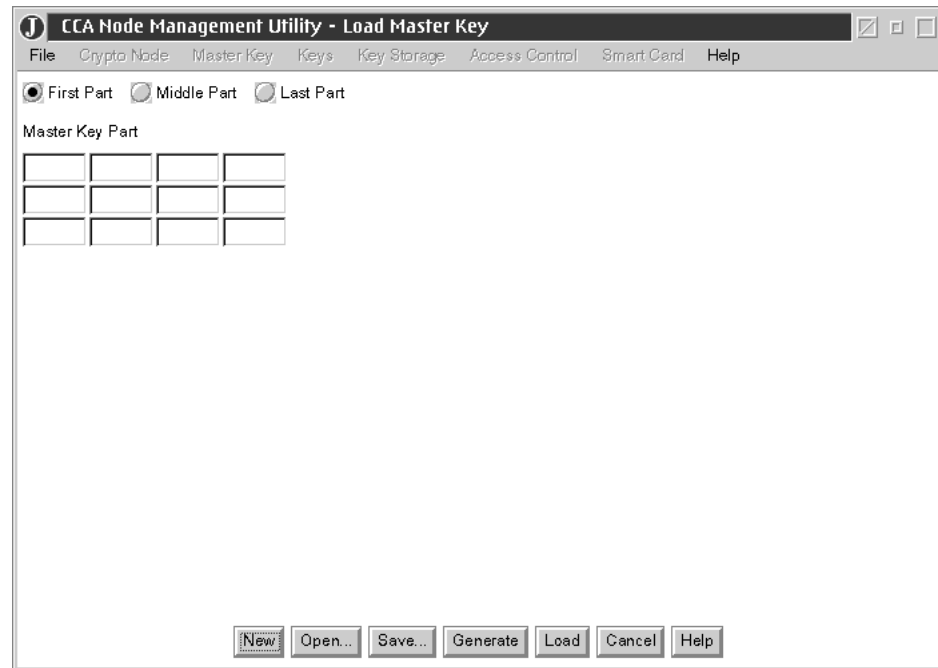


Figure 296. Load Master Key from Clear Parts

2. Select the radio button for the key part you are loading (First Part, Middle Part or Last Part).
3. Enter the clear key part by one of these:
 - a. Select **New** to clear data entered in error.
 - b. Select **Open...** to retrieve key parts saved to disk.
 - c. Select **Generate** to have the TKE Crypto Adapter randomly generate a key part.

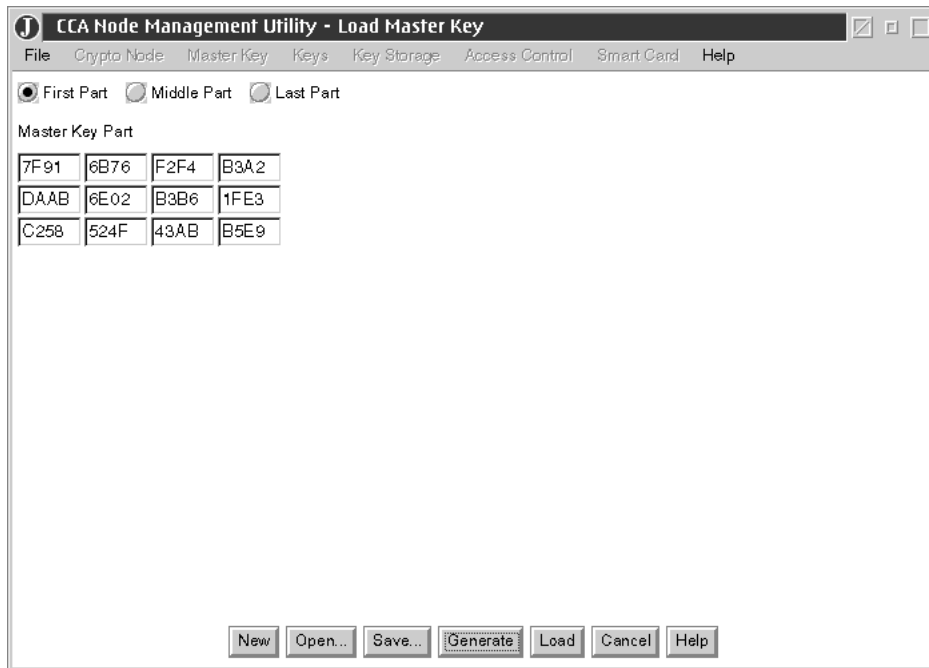


Figure 297. Load Master Key from Clear Parts — key part randomly generated

- d. Manually enter a key value into the "Master Key Part" fields; each field accepts four hexadecimal digits
4. Select **Load** to load the key part into the new master key register; select **Save...** To save the key part to disk.

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see "Managing Media" on page 377.



Figure 298. 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:
 - 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 272.)

We recommend a dual control security policy where the first and last key parts are loaded by different people.

Generating master key parts to a TKE smart card

Steps for generating master key parts to a TKE smart card are:

1. From the **Master Key** pull-down menu, select **Smart Card Parts**. You will be prompted to insert a TKE smart card into smart card reader 2. The Smart Card Master Key Parts panel is displayed. Any TKE Crypto Adapter master key parts stored on the TKE smart card are listed in the container. The TKE smart card description is displayed. Ensure this is the correct TKE smart card you want to generate the key part to.

Make sure that the cryptographic adapter in the TKE workstation and the TKE smart cards are in the same zone. To determine the zone for a TKE smart card, use CNM, see “Display smart card details” on page 276 or SCUP “Display smart card information” on page 291. To determine the zone of a TKE cryptographic adapter, use SCUP “View current zone” on page 304. To use SCUP, you must first exit from CNM.

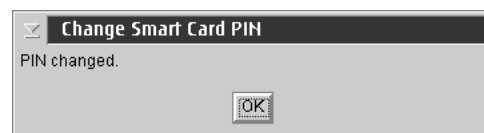


Figure 299. Smart Card Master Key Parts panel

2. Select the radio button for the key part you are generating (First Part, Middle Part, or Last Part).
3. Press the Generate & Save button. You will be prompted for an optional description for the key part you are generating. A maximum of 32 characters may be specified.

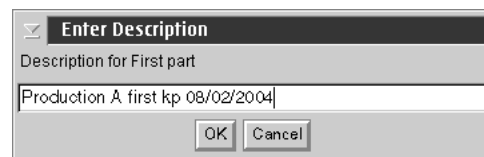


Figure 300. Smart Card Master Key Parts panel — key part description prompt

4. You will be prompted for the PIN of the TKE smart card inserted in smart card reader 2.
5. A secure session is established between the TKE Crypto Adapter and the TKE smart card. The key part is generated to the TKE smart card. The key part list is refreshed.

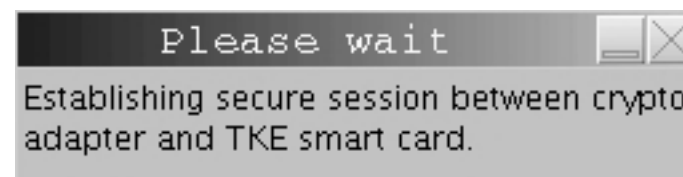


Figure 301. Establishing a secure session between TKE Crypto Adapter and TKE smart card

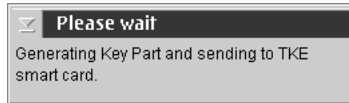


Figure 302. Generating key part to TKE smart card

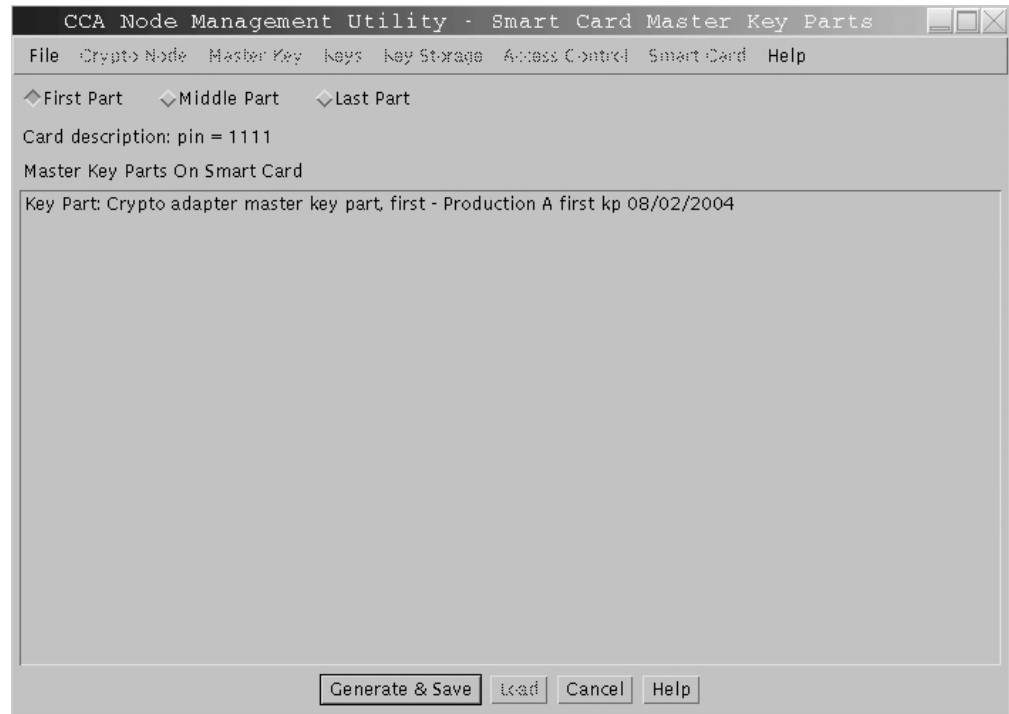


Figure 303. Smart Card Master Key Parts panel — key part generated to TKE smart card

Note: The key parts in the container 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 where the first and last key parts are generated to different TKE smart cards so that no one person has access to the complete key. At this point, we recommend that you insert a different TKE 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.

Loading master key parts from a TKE smart card

Steps for loading Crypto Adapter master key parts from a TKE smart card are:

1. From the **Master Key** pull-down menu, select **Smart Card Parts**. You will be prompted to insert a TKE smart card into smart card reader 2. The Smart Card Master Key Parts panel is displayed. Any Crypto Adapter master key parts

stored on the TKE smart card are listed in the container. The TKE smart card description is displayed. Ensure this is the correct TKE smart card you want to work with.

2. Highlight the key part you want to load to the Crypto Adapter new master key register. Press the **Load** button. You will be prompted for the PIN of the TKE smart card inserted in smart card reader 2.

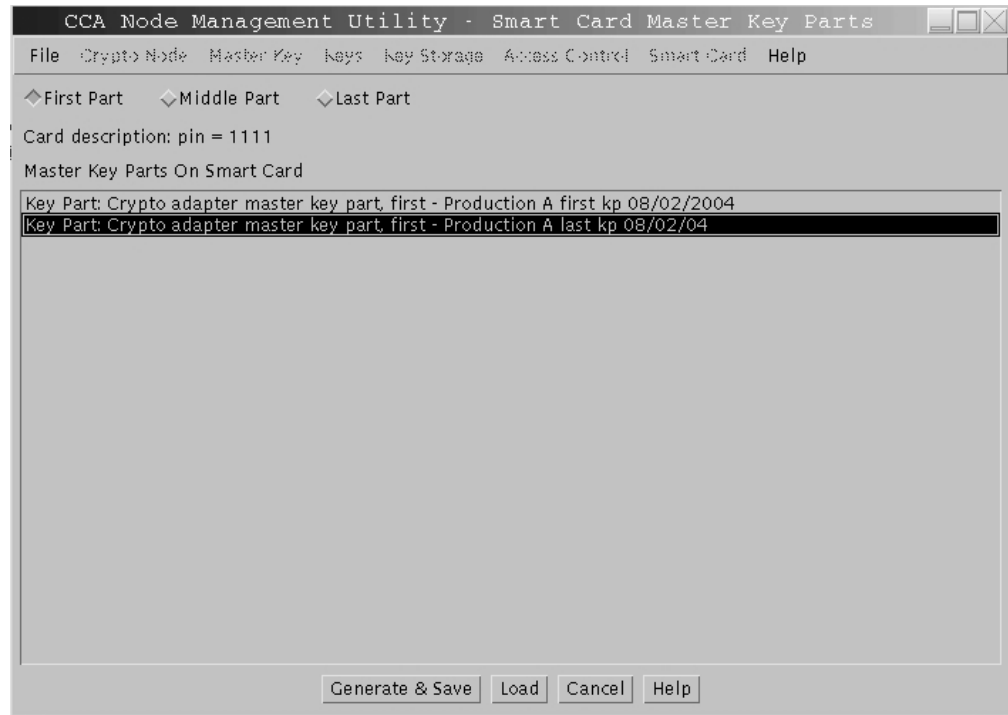


Figure 304. Master Key Part Smart Card panel — loading a Crypto Adapter key part from TKE smart card

3. A secure session is established between the Crypto Adapter and the TKE smart card. A pop-up message will display that the key part was successfully loaded.

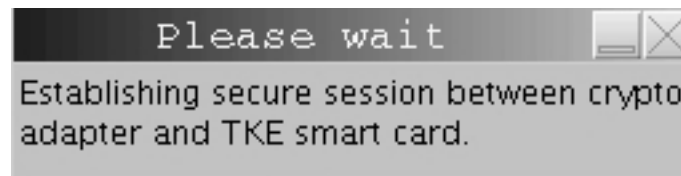


Figure 305. Establishing a secure session between Crypto Adapter TKE smart card

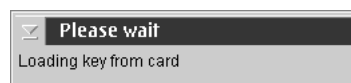


Figure 306. Loading key part from TKE smart card



Figure 307. Master key part successfully loaded

4. Repeat the preceding steps to load additional key parts to the Crypto Adapter new master key register. If key parts are on different TKE smart cards, remove the TKE smart card from smart card reader 2 and insert the TKE smart card which contains the next key part to load.

Note: Key parts must be loaded in order; 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.

5. From the **Master Key** pull-down menu, select **Set...** This will:
 - 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.
6. After setting a new master key, reencipher the keys currently in key storage. See "Reenciphering key storage" on page 272.

Verifying Master Key Parts

A verification pattern (VP) is generated for each master key stored in the master-key registers (new, current and old). The 16-byte 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 TKE 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 cryptographic 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:

1. From the **Master Key** pull-down menu, select **Verify**. A sub-menu is displayed.

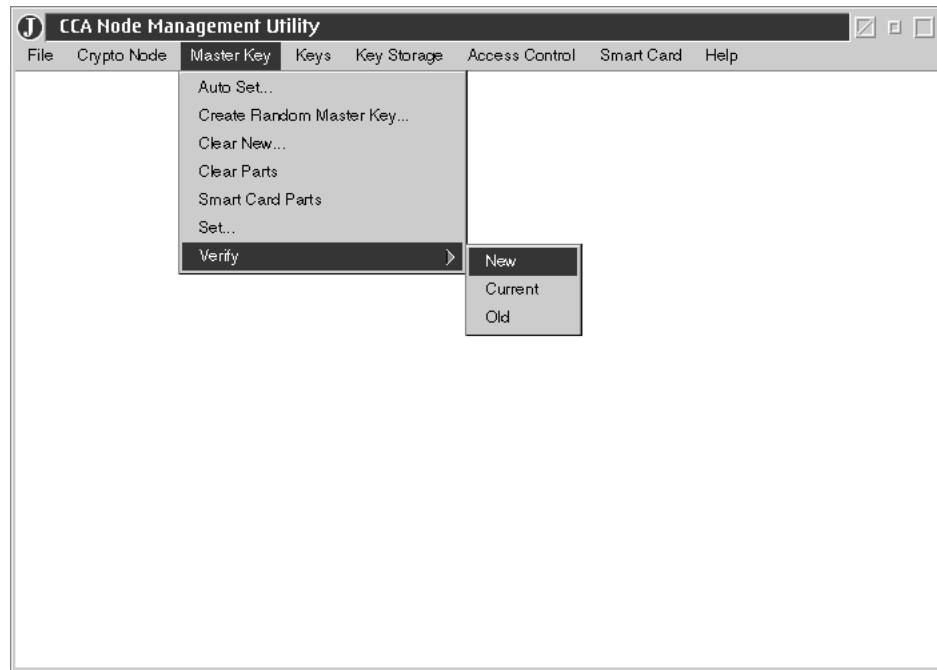


Figure 308. Master Key Verify sub-menu

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.

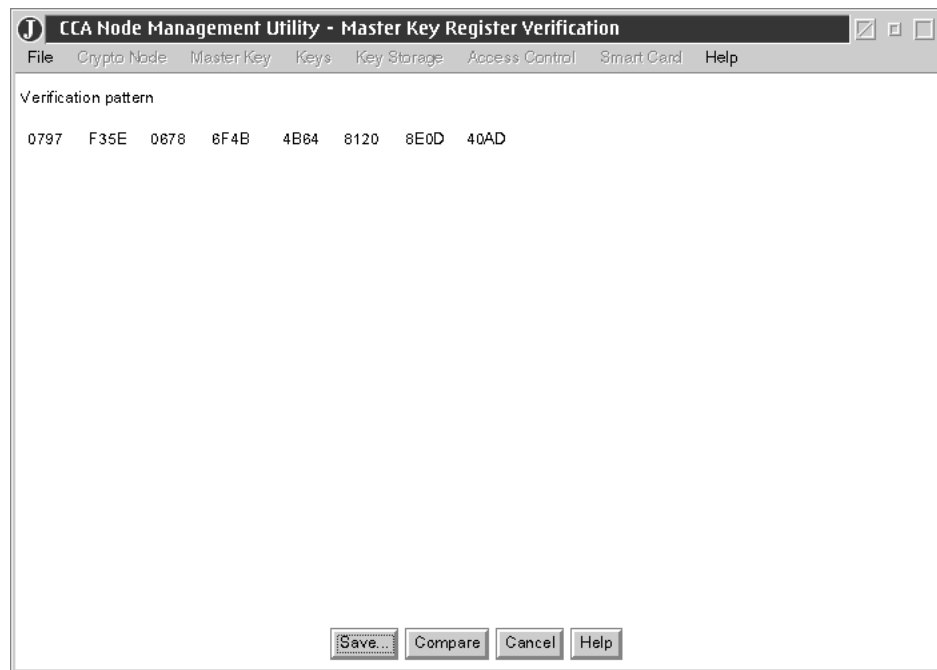


Figure 309. Master Key Register Verification panel - verification pattern is displayed

4. Select **Save** to **Save** the VP to a file. A file chooser will be displayed for the user to specify where to save the file (CD/DVD Drive or CNM Data Directory) and a file name.
Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.
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 310. Master Key Register VP compare successful

Key Storage Menu

Reenciphering key storage

Key storage is a repository of keys that you access by key label. DES keys and PKA (RSA) keys are held in separate storage systems. The keys in key storage are enciphered under the current TKE Crypto Adapter master key. When a new master key is set (becomes the current master key), the keys must be reenciphered to the current master key.



Figure 311. CNM main window — Key Storage pull-down menu

To reencipher the keys in storage:

1. From the **Key Storage** pull-down menu, select **DES Key Storage** or **PKA Key Storage**; a sub-menu is displayed.

- From the sub-menu, select **Manage**; the DES Key Storage Management or the PKA Key Storage Management panel is displayed. The panel lists the labels of the keys in key storage.

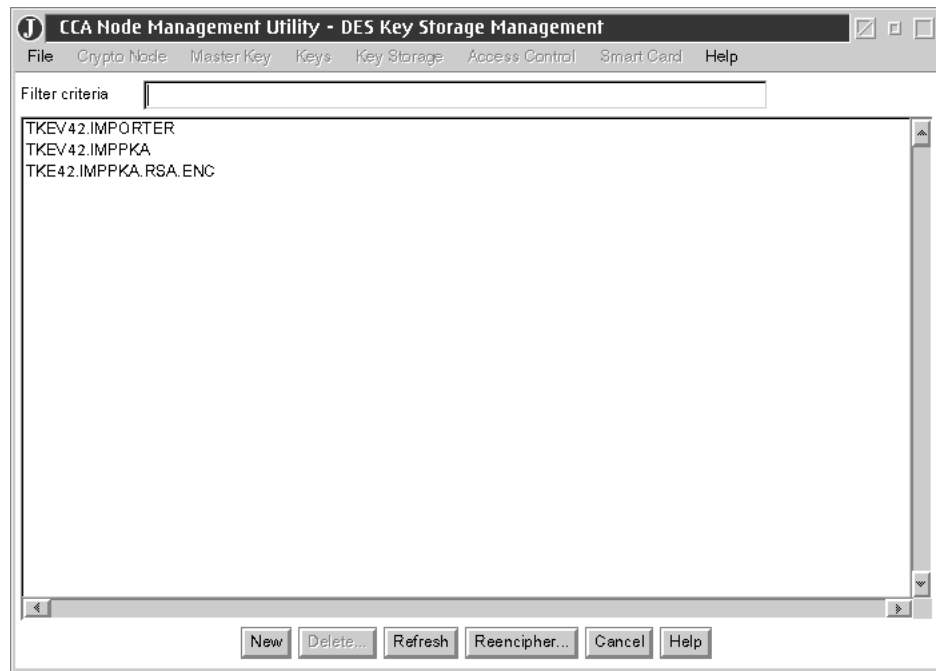


Figure 312. Key Storage Management Panel – key labels list

- Select **Reencipher...**; the keys are reenciphered using the key in the current master key register.

Smart card Menu

Change PIN

The TKE smart card is secured with a PIN. You may change your PIN using this function. You must know your current PIN. If your TKE smart card is blocked due to too many incorrect PIN attempts, this function will fail. You do not need to logon to the TKE Crypto Adapter to perform this function.



Figure 313. CNM main menu — Smart Card pull-down menu

Steps to change the PIN are:

1. From the Smart Card pull-down menu, select Change PIN; you will be prompted to insert your TKE smart card into smart card reader 2. Insert your TKE smart card and press OK to continue.



Figure 314. Change PIN — insert TKE 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 315. 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 316. Change PIN — enter new PIN prompt

4. The PIN is successfully changed on the TKE smart card.

Generate TKE Crypto Adapter logon key

A Crypto Adapter logon key allows a user to logon to the Crypto Adapter using a TKE smart card to access functions not allowed in the default role. A Crypto Adapter logon key is an RSA private key pair generated within the TKE smart card. The private key never leaves the TKE smart card. The public key is read from the TKE smart card and loaded to the Crypto Adapter when a user profile is defined. You do not need to logon to the Crypto Adapter to perform this function.

To generate a Crypto Adapter logon key:

1. From the Smart Card pull-down menu, select Generate Crypto Adapter Logon Key. You will be prompted for a TKE smart card. Insert the TKE smart card into smart card reader 2.

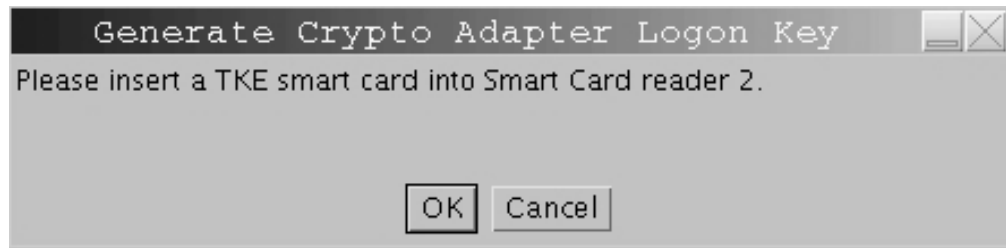


Figure 317. Generate Crypto Adapter Logon Key — insert TKE smart card

2. You will be prompted for a PIN. Enter the PIN on the smart card reader 2 PIN pad.

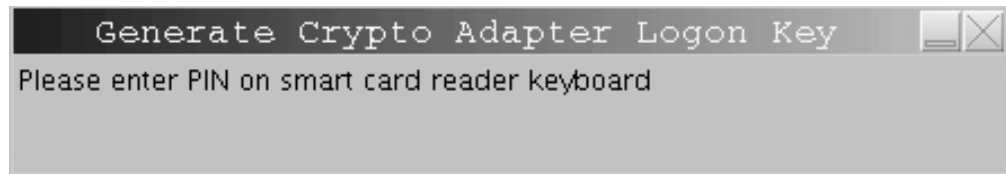


Figure 318. Generate Crypto Adapter Logon Key — PIN prompt

3. You will be prompted for a user ID for the TKE smart card. This user ID will be read from the TKE smart card when defining a smart card user profile.

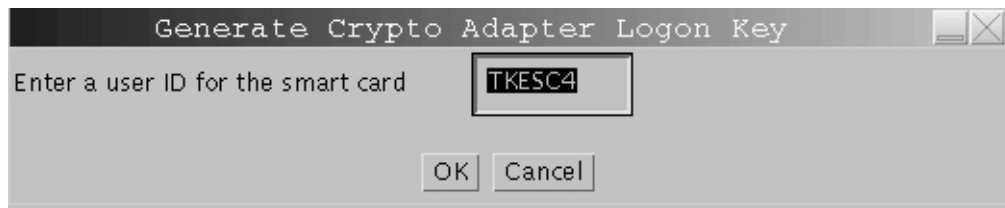


Figure 319. Generate Crypto Adapter Logon Key — User ID prompt

4. The Crypto Adapter logon key is generated.



Figure 320. Generate Crypto Adapter Logon Key — key generated

Display smart card details

Use this function to display public information about a TKE smart card. You do not need to logon to the Crypto Adapter to use this function.

1. From the **Smart Card** pull-down menu, select **Display Smart Card Details**. You will be prompted for a TKE smart card. Insert the TKE smart card into smart card reader 2.



Figure 321. Display Smart Card Details — insert TKE smart card prompt

The TKE smart card is read and the public information is displayed.

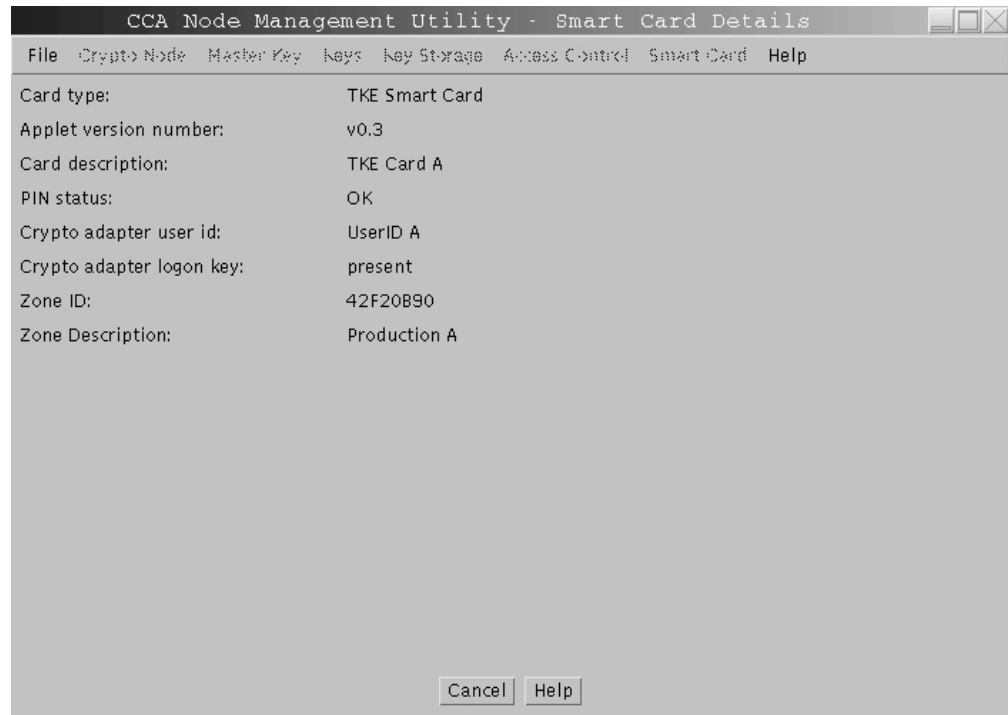


Figure 322. Display Smart Card Details — public information displayed

This information is displayed for a TKE smart card:

Card type

TKE smart card

Applet version number

Version number of applet loaded on smart card

Card description

description of the TKE smart card; entered when the smart card was personalized

PIN status

not set/OK/blocked; PIN is set when TKE smart card is personalized

Crypto Adapter user id

user id entered when a Crypto Adapter logon key is generated; may be blank if the TKE smart card does not have a Crypto Adapter logon key

Crypto Adapter logon key

not present/present

Zone ID

set when the TKE smart card is initialized

Zone Description

set when the TKE smart card is initialized

Manage Smart Card Contents

Use this function to delete keys or key parts from a TKE smart card. A TKE smart card can hold up to 10 key parts, a TKE authority signature key, and a Crypto Adapter logon key. You do not need to logon to the TKE Crypto Adapter to use this function.

1. From the **Smart Card** pull-down menu, select **Manage Smart Card contents**. You will be prompted for a TKE smart card. Insert the source TKE smart card into smart card reader 2.

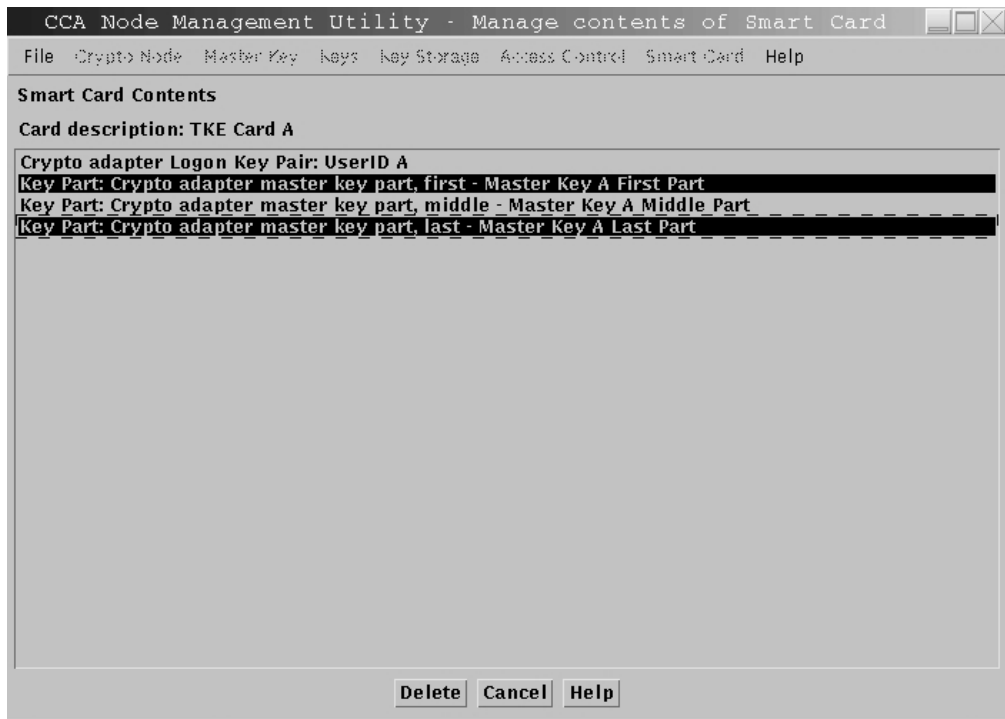


Figure 323. Manage Smart Card contents — contents of TKE smart card are displayed

2. The TKE smart card description is displayed. Ensure this is the correct TKE smart card you want to work with. Highlight the keys and/or key parts you want to delete. Press the **Delete** 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.

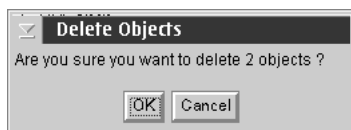


Figure 324. Manage Smart Card contents — confirm delete prompt

5. The objects are deleted and the list is refreshed.

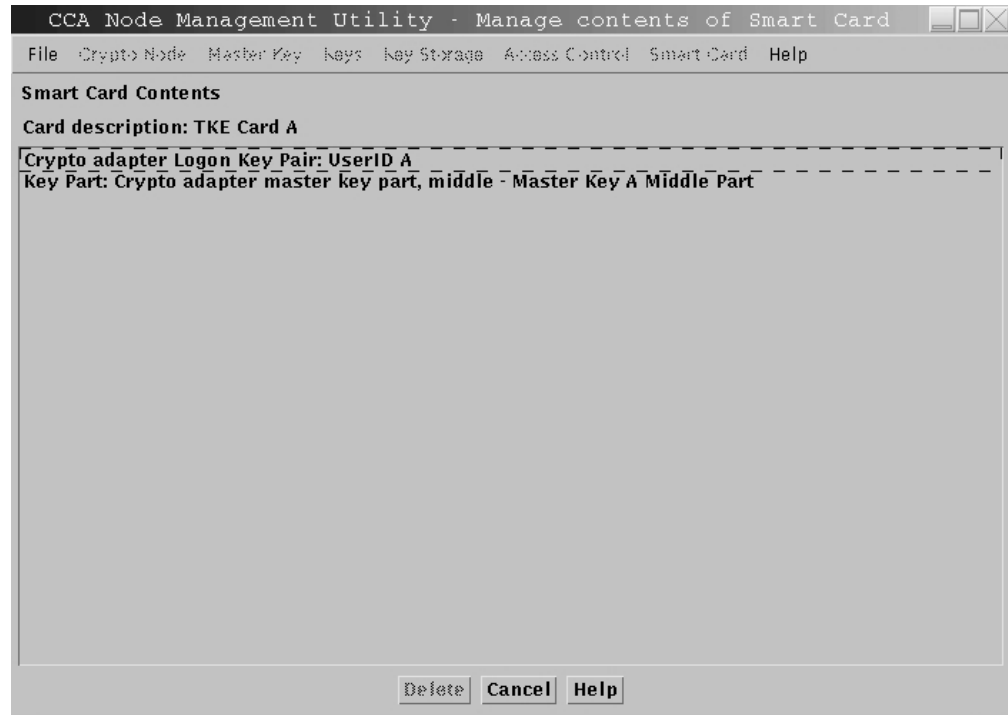


Figure 325. Manage Smart Card contents

Attention! If you delete a Crypto Adapter logon key, you will not be able to logon to the TKE Crypto Adapter until you generate a new Crypto Adapter logon key and the administrator updates your TKE Crypto Adapter user profile.

If you delete a TKE signature authority key, you will not be able to sign a TKE command until the administrator generates a new authority key and uploads it to the host.

Copy Smart Card

Use this function to copy a key or key part(s) from one TKE smart card to another. The two TKE smart cards must belong to the same zone; that is, the Zone ID of the TKE smart cards must be identical. Use **Display Smart Card Details** to verify the Zone ID of the TKE smart cards.

You do not need to logon to the TKE Crypto Adapter to use this function.

Note: Smart card copy does not overwrite the target TKE smart card. If there is not enough room on the target TKE smart card, you will get an error message. You can either delete some of the keys on the target TKE smart card (see “Manage Smart Card Contents” on page 277) or use a different TKE smart card.

1. From the Smart Card pull-down menu, select Copy Smart Card. You will be prompted for a source TKE smart card. This is the TKE smart card you want to copy from. Insert the source TKE smart card into smart card reader 1. The contents of the TKE smart card are displayed in the source container on the top.



Figure 326. Copy Smart Card — insert source TKE smart card

2. You will be prompted for a target TKE smart card. This is the TKE smart card you want to copy to. Insert the TKE smart card into smart card reader 2. The contents of the TKE smart card are displayed in the target container on the bottom. The contents of this container are greyed.



Figure 327. Copy Smart Card — insert target TKE smart card

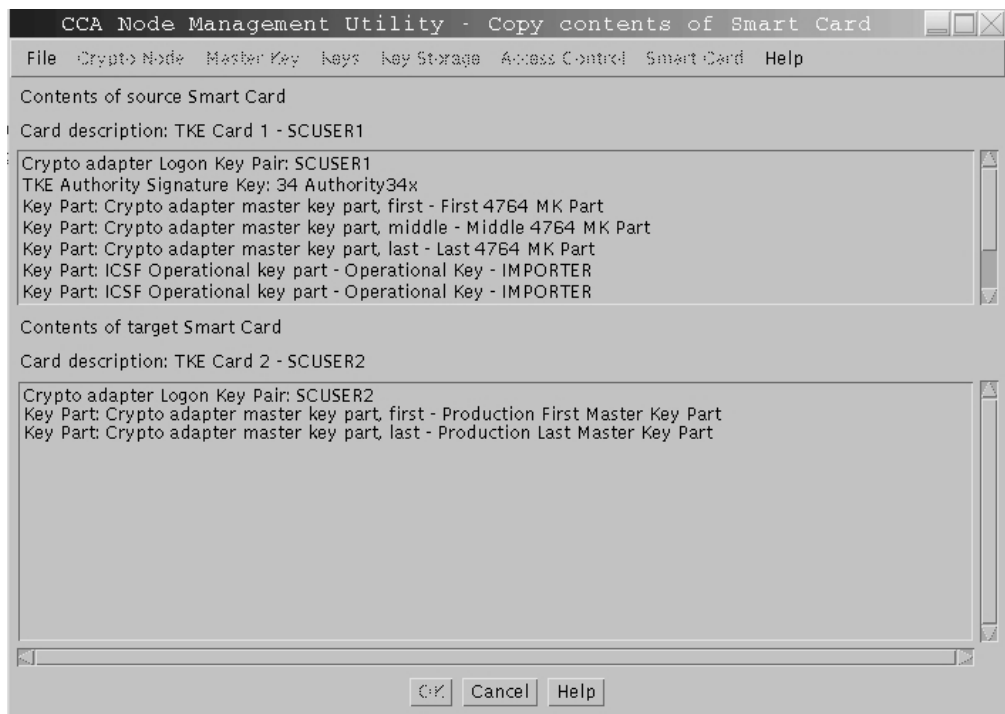


Figure 328. Copy Smart Card — TKE smart card key parts are displayed

3. Highlight the objects in the source container to copy to the target container. Press **OK** to continue.

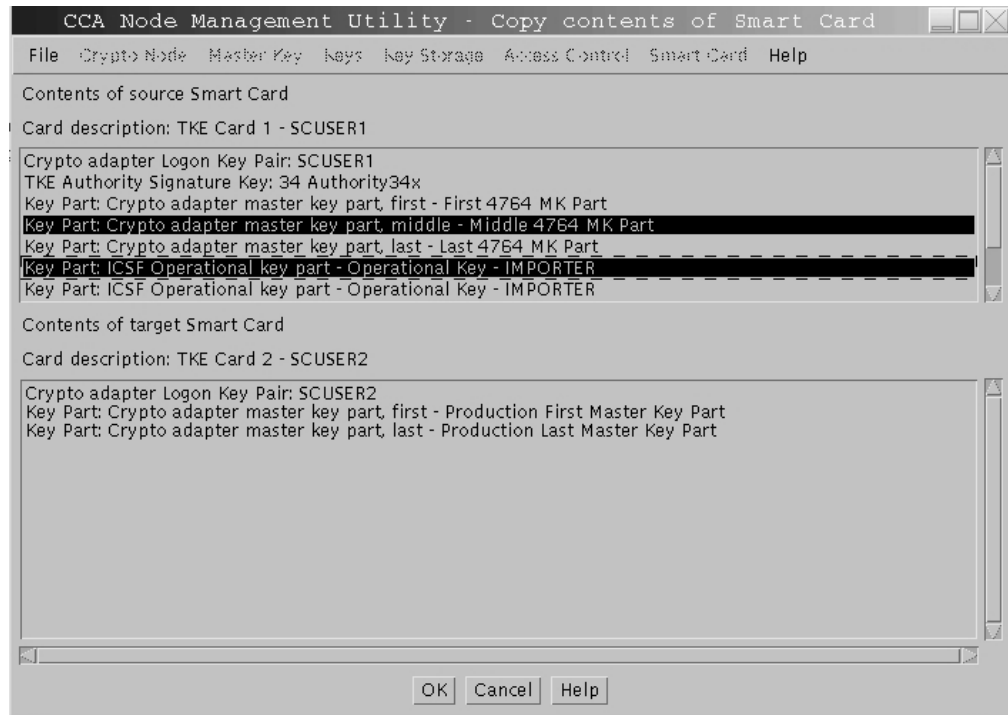


Figure 329. Copy Smart Card — highlight source objects to copy to target

4. You will be prompted for the PIN of the source TKE smart card in smart card reader 1. Enter the PIN on the smart card reader 1 PIN pad.

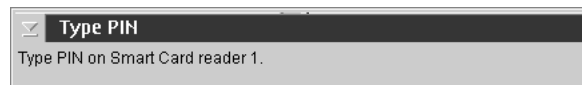


Figure 330. Copy Smart Card — source TKE smart card PIN prompt

5. You will be prompted for the PIN of the target TKE 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 TKE smart cards and the selected object(s) are copied. The contents of the target container is refreshed.

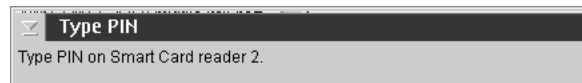


Figure 331. Copy Smart Card — target TKE smart card PIN prompt

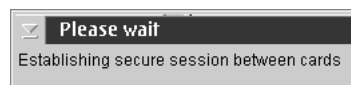


Figure 332. Establishing a secure session between source and target TKE smart cards

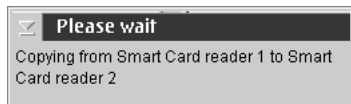


Figure 333. Objects are copied to the target TKE smart card

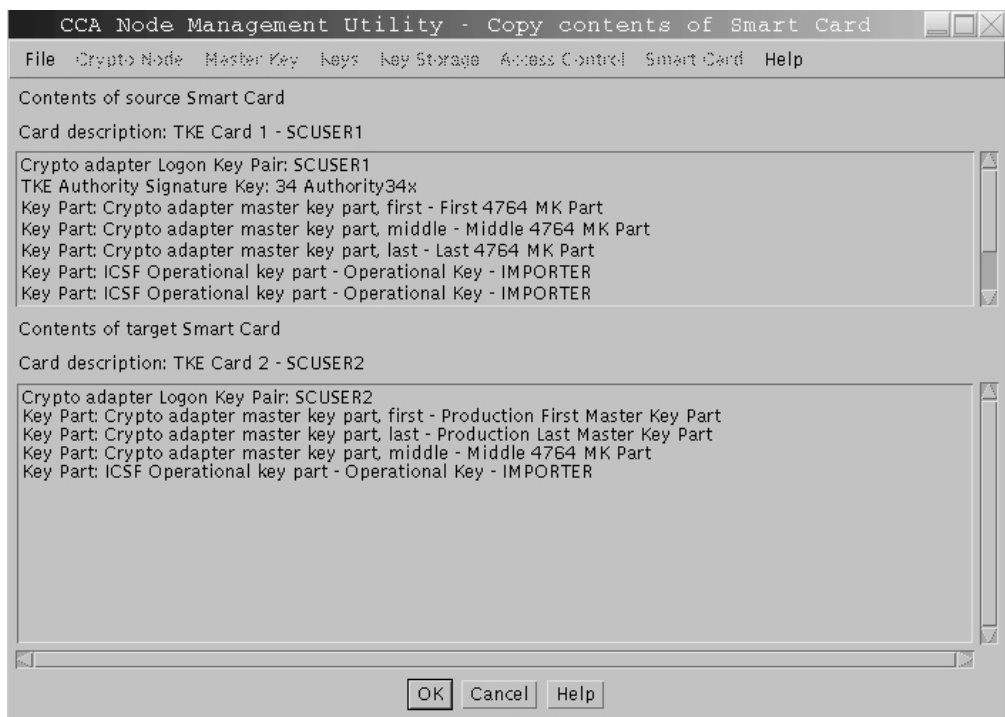


Figure 334. Copy Smart Card — objects are copied to the target container

A TKE smart card can hold a maximum of 10 key parts in addition to a workstation cryptographic adapter logon key and a TKE authority 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. Logoff the crypto module and logon using a profile associated with a role that allows this function.

Message: Time sent in your logon request was more than 5 min. off the clock in the secure module

Return Code: 8

Reason Code: 91

Explanation: The workstation clock is more than 5 minutes off the TKE Crypto Adapter clock-calendar. This occurs when the clock changes from Standard Time to Daylight Savings Time and vice-versa. Read the TKE Crypto Adapter clock-calendar (see "Read Clock-Calendar" on page 248), convert the GMT time to the current time for your area and set the workstation clock (see "Setting the Clock" on page 219). Logon to the TKE Crypto Adapter with a profile/role that allows you to set the clock (like TKEADM or SCTKEADM). Then synchronize the clock-calendar (see "Synchronize Clock-Calendar" on page 248).

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: Check that 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 (passphrase expired, profile expired, etc) and so the group logon failed. The group logon window will indicate which user failed and why. 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 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.

Appendix D. Smart Card Utility Program (SCUP)

The TKE Smart Card Utility Program (SCUP) supports the smart card system with these functions:

- Initialize and personalize the CA smart card
- Backup the CA smart card
- Initialize and enroll TKE smart cards
- Personalize TKE smart cards
- Display smart card information
- Enroll the TKE cryptographic adapter
- Unblock a TKE smart card
- Change PIN number

When you are prompted on the panel to enter PINs, the smart card reader also shows a prompt. Messages appear for certain tasks that take over a minute. Please be patient to avoid having to start the task over.

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. Under Applications, click on Smart Card Utility Program 5.2. This screen appears:

File CA Smart Card TKE Smart Card Crypto Adapter Help

Smart card reader 1

Card type: Zone enroll status:
 Card ID: Zone ID:
 Card description: Zone description:
 PIN status:
 TKE Authority key:
 Crypto Adapter Logon key:

Key parts:

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	Control vector	Length

Smart card reader 2

Card type: Zone enroll status:
 Card ID: Zone ID:
 Card description: Zone description:
 PIN status:
 TKE Authority key:
 Crypto Adapter Logon key:

Key parts:

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	Control vector	Length

Main Menu

Figure 335. First screen of TKE Smart Card Utility Program (SCUP)

Drop down menus exist for these tabs on the top of the screen:

- File
- CA Smart Card
- TKE Smart Card
- Crypto Adapter

Tasks associated with the drop down menu for **File** are:

- Display smart card information; see “Display smart card information” on page 291.
- Exit.

Tasks associated with the drop down menu for **CA Smart Card** are:

- Initialize and personalize CA smart card; see “Initialize and personalize the CA smart card” on page 287.
- Backup CA smart card; see “Backup a CA smart card” on page 289.
- Change PIN; see “Change PIN of a CA smart card” on page 295.

Tasks associated with the drop down menu for **TKE Smart Card** are:

- Initialize and enroll TKE smart card; see “Initialize and enroll a TKE smart card” on page 293.
- Personalize TKE smart card; see “Personalize a TKE smart card” on page 294.

- Unblock TKE smart card; see “Unblock PIN on a TKE smart card” on page 295.
- Change PIN; see “Change PIN of a TKE smart card” on page 296..

Tasks associated with the drop down menu for **Crypto Adapter** are:

- Enroll Crypto Adapter; see “Enroll a TKE cryptographic adapter” on page 296.
- View current zone; see “View current zone” on page 304.

Initialize and personalize the CA smart card

A zone is created when a CA smart card is initialized and personalized.

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.

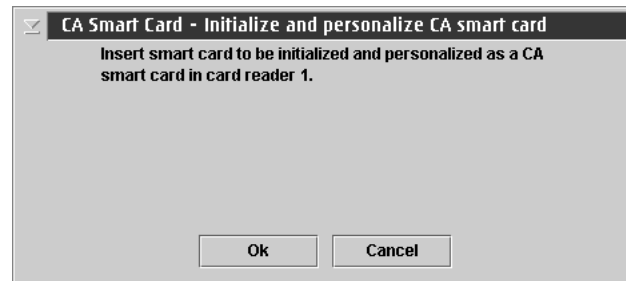


Figure 336. First step for initialization and personalization of the CA smart card

3. 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**.

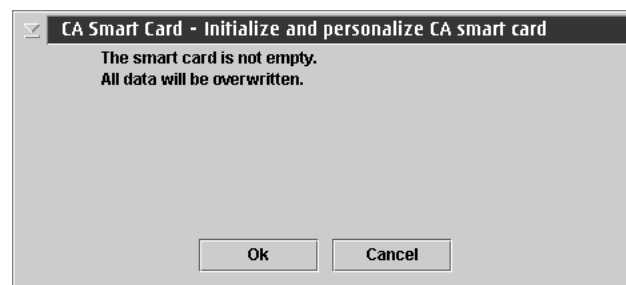


Figure 337. Message if card is not empty

4. The smart card will now be initialized.

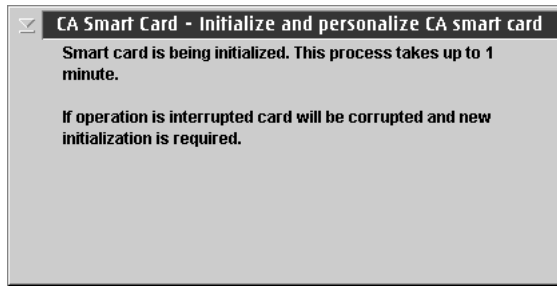


Figure 338. Initialization message for CA smart card

5. At the prompt, enter a 6-digit PIN number twice. This is the first CA smart card PIN.

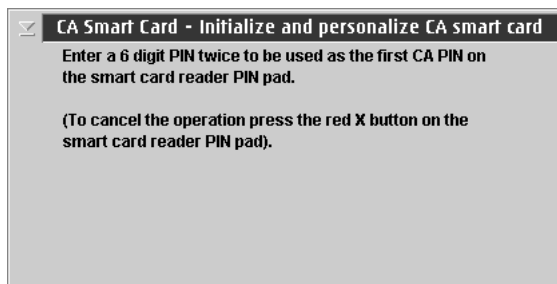


Figure 339. Enter first PIN for CA smart card

6. At the 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.

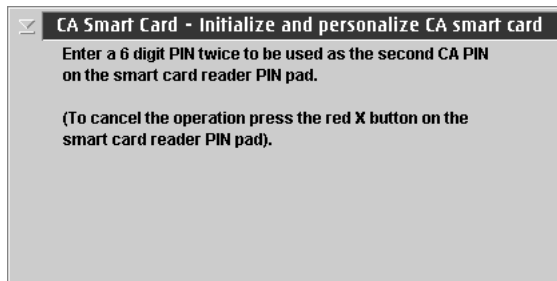


Figure 340. Enter second PIN twice for CA smart card

7. At the prompt, enter a zone description. Although this is optional, it is recommended.

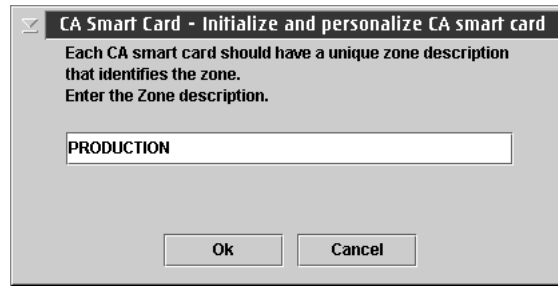


Figure 341. Enter zone description for CA smart card

8. At the prompt, enter a CA smart card description. Although this is optional, it is recommended. After the description is entered the CA Smart Card will be built.

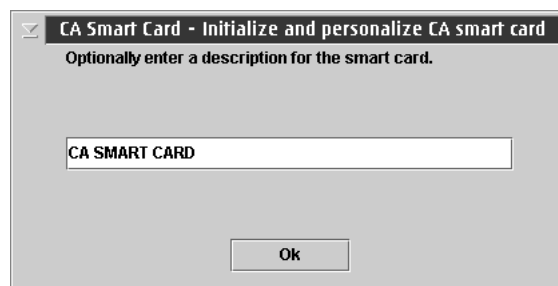


Figure 342. Enter card description for CA smart card

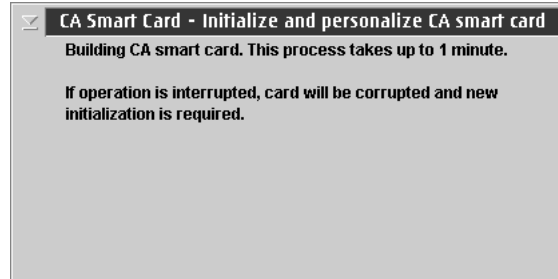


Figure 343. Building a CA smart card

9. You will get a message that a CA Smart Card was successfully created.

Backup a CA smart card

The CA smart card defines the zone. If the CA smart card is lost or blocked the administrator will not be able to initialize and enroll TKE smart cards, unblock TKE smart cards or enroll TKE cryptographic adapters in the zone. We recommend that the CA smart card be backed up and stored in a secure place.

To backup a CA smart card, follow these steps:

1. From the *CA Smart Card* drop down menu, select *Backup CA smart card* option.
2. When prompted, insert the CA smart card to be backed up into smart card reader 1.

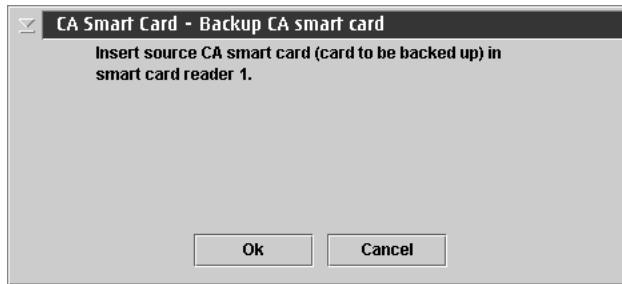


Figure 344. Begin creation of backup CA smart card

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 will be asked to overwrite all of the data on the smart card.
7. The target smart card is initialized.

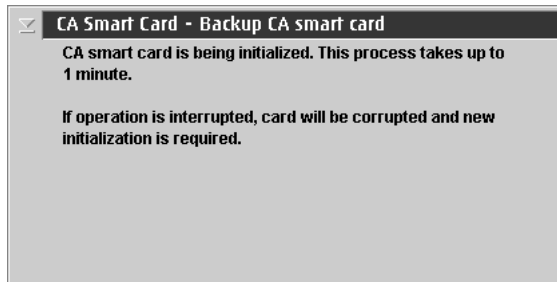


Figure 345. Initialization of backup CA smart card

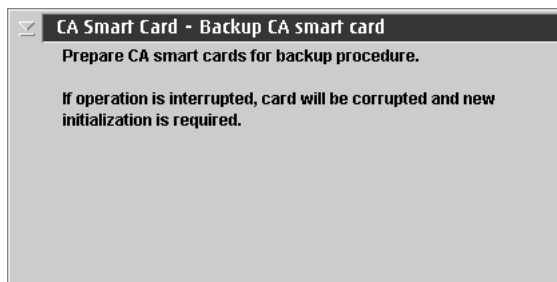


Figure 346. Continue creation of backup CA smart card

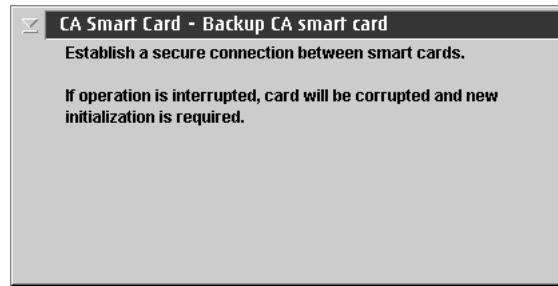


Figure 347. Establish secure connection for backup CA smart card

8. At the prompts, enter the first and second CA PINs of the original CA smart card on the smart card reader 2.

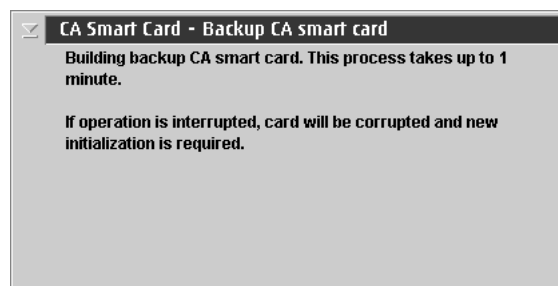


Figure 348. Building backup CA smart card

9. You will get a message that a CA Smart Card was successfully copied.

Display smart card information

After you have created a smart card, you may want to check the results. If you are copying keys from one TKE smart card to another, you may also want to see if the TKE smart cards are in the same zone.

1. Insert smart card(s) to be displayed in smart card reader 1 or 2. From the *File* menu, select *Display smart card information* option.

File CA Smart Card TKE Smart Card Cryptic Adapter Help

Smart card reader 1

Card type:	CA Smart Card v0.3	Zone enroll status:	Enrolled
Card ID:	2386A11B5	Zone ID:	42DD4E4C
Card description:	CA smart card	Zone description:	Production
PIN status:	OK		
TKE Authority key:			
Cryptic Adapter Logon key:			

Key parts:

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	Control vector	Length

Smart card reader 2

Card type:	TKE Smart Card v0.3	Zone enroll status:	Enrolled
Card ID:	754FE09B5	Zone ID:	42DD4E4C
Card description:	TKE Smart Card	Zone description:	Production
PIN status:	OK		
TKE Authority key:	45 Bob Jones		
Cryptic Adapter Logon key:	Not present		

Key parts:

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	Control vector	Length
ICSF symmetric master key	NSMF	Cryptic adap...	204F721D0C8...	F5C8DA271...	F21ED575		16
Operational key part, E...	Operation = Ke...	Cryptic adap...	5F9CC54CF3...	A4C332FC7...	3375EBE3	00417	16
Operational key part, O...	Operation = Ke...	Cryptic adap...	7AE26C34513...	893715183...	04C86C29	002477	16
Operational key part, O...	Operation = Ke...	Cryptic adap...	62C365383E...	C6CF812CD...	3CCFD358	00C000	8
Operational key part, O...	Operation = Ke...	Cryptic adap...	69BFC7C90E5...	775C5FCCF...	3651CEFE	00C000	16
Operational key part, I...	Operation = Ke...	Cryptic adap...	D4329A484a3...	8FC79FF6F...	4F54C49D	00C04	16

Main Menu

Figure 349. Display of CA smart card and TKE smart card

The panel provides this information on the smart card:

- **Card type:** This is either a CA smart card or TKE smart card.
- **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
- **TKE Authority key:** For TKE smart cards only, the authority index and name is displayed.
- **Crypto Adapter Logon Key:** For TKE smart cards only, the value can be Present or Not Present.
- **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 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 smart card. Can be 12 characters in length.
- **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
- **Control vector:** CCA control vector of operational key parts or blank for master key parts
- **Length:** 8, 16, or 24 bytes

Initialize and enroll a TKE smart card

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 a smart card to be initialized as a TKE smart card in smart card reader 2.

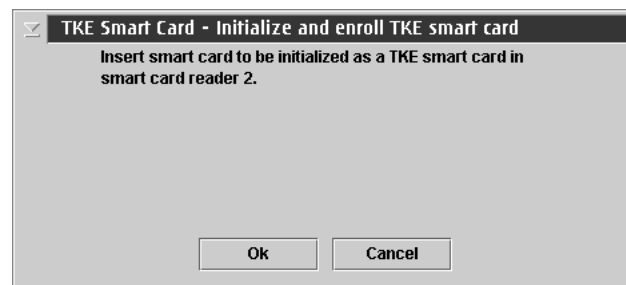


Figure 350. Initialize and enroll TKE smart card

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 these screens indicating that the smart card is being initialized and then the TKE smart card is being built.

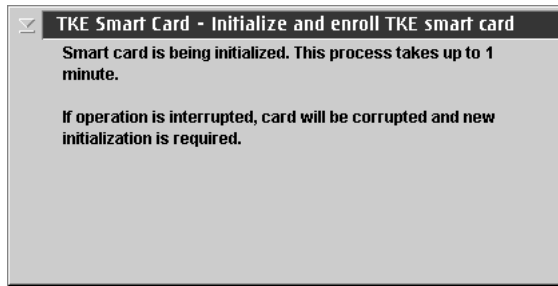


Figure 351. Initializing TKE smart card

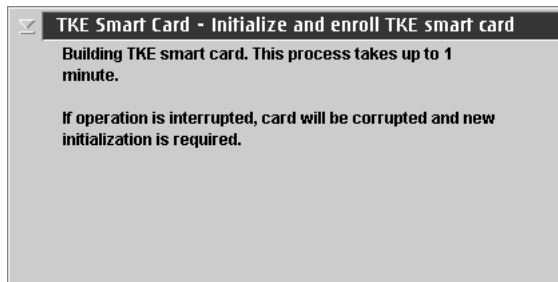


Figure 352. Building TKE smart card

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 TKE smart card

To personalize a TKE smart card, follow these steps:

1. From the *TKE Smart Card* drop down menu and select *Personalize TKE smart card* option.
2. You will be prompted to insert a TKE smart card to be personalized in smart card reader 2.

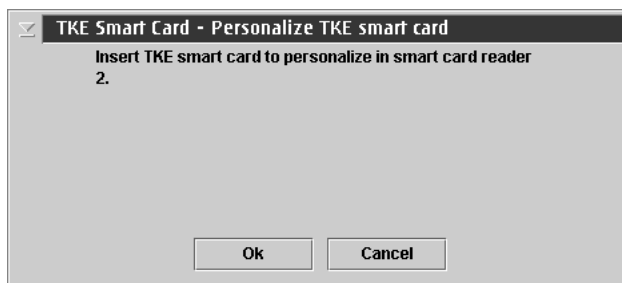


Figure 353. Personalizing TKE smart card

3. At the prompt, enter a 4-digit PIN on the PIN pad of the smart card reader 2. You will do this twice.

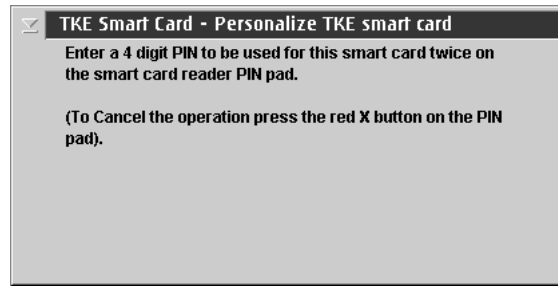


Figure 354. Entering PIN for TKE smart card

4. At the prompt, enter a description for the TKE smart card (optional).
5. When complete, you will get a message that the TKE smart card personalization was successful.

Unblock PIN on a TKE smart card

If you enter an incorrect PIN 3 times for a TKE smart card, it will become blocked and will not be usable. When you unblock the PIN, the PIN does not change. You still need to enter the correct PIN. You 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 CA smart card

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. Select either first CA PIN or second CA PIN.

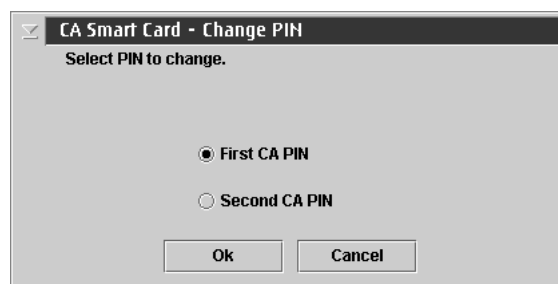


Figure 355. Select first CA PIN

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.

Change PIN of a TKE 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 4-digit PIN once.
4. At the prompt, enter the new 4-digit PIN twice.
5. You will get a message that the PIN was successfully changed.

Enroll a TKE cryptographic adapter

A TKE workstation with a cryptographic adapter can be enrolled locally or remotely.

Note: This must be done before loading key parts from the TKE smart card.

You can check if the TKE cryptographic adapter is enrolled in a zone from the Crypto Adapter drop down menu: select *View current zone* option. You will see this if it is not:



Figure 356. 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 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 must reload the TEMPDEFAULT role (see "Open or edit a disk-stored role" on page 250). 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.

For a local enrollment:

1. From the Crypto Adapter drop down menu, select Enroll Crypto Adapter option.
2. Select *local* when prompted for enrollment type.

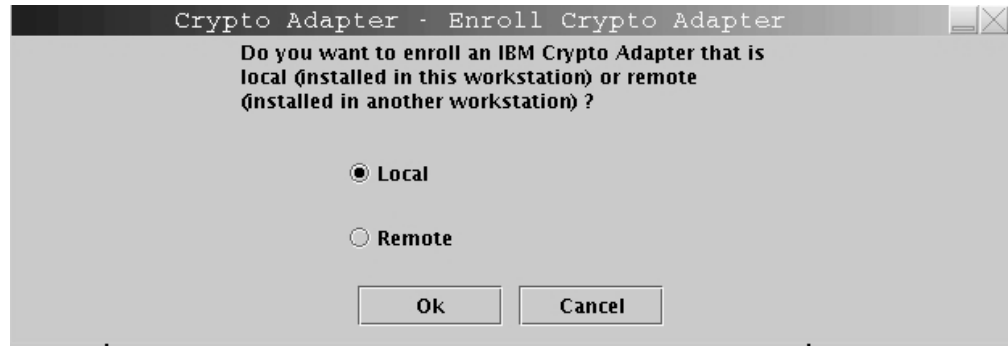


Figure 357. Select local zone

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.

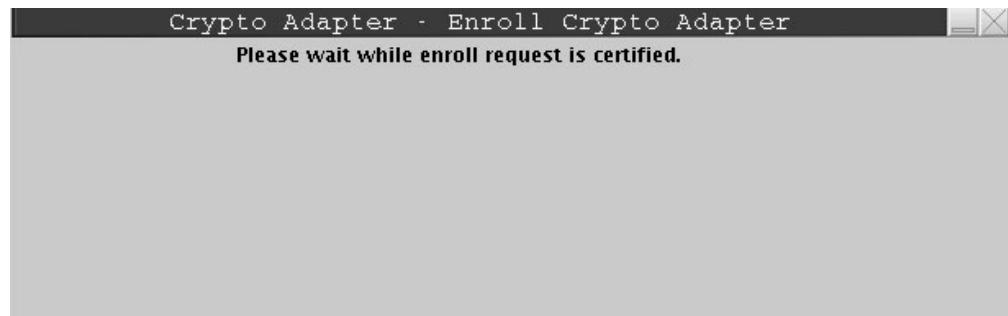


Figure 358. Certifying request for local Crypto Adapter enrollment



Figure 359. 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 360. View current zone after Crypto Adapter enrollment

For a remote/secondary enrollment:

To enroll a remote cryptographic adapter, follow these steps.

Note: If the remote workstation is TKE 4.2, refer to the TKE Workstation User's Guide, SA22-7524, on Resource Link for details.

1. On the remote workstation, click on Trusted Key Entry.
2. Click on Begin Zone Remote Enroll Process for an IBM Crypto Adapter.
3. Respond YES to this message: This program generates an enrollment request for the IBM Cryptographic card installed in this workstation Continue?? (Yes/no)
4. There is a check to see if the crypto adapter is already enrolled. If it is, the message "A device key is already present in the Crypto Adapter. After the remote enroll is completed, the device key will be replaced. Continue?" must be answered.

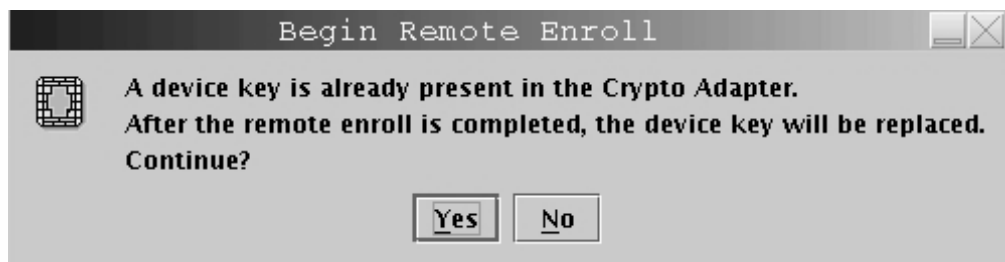


Figure 361. Crypto Adapter Enrolled

5. The restricted file chooser will open and prompt you for a file name and destination. Store the file.

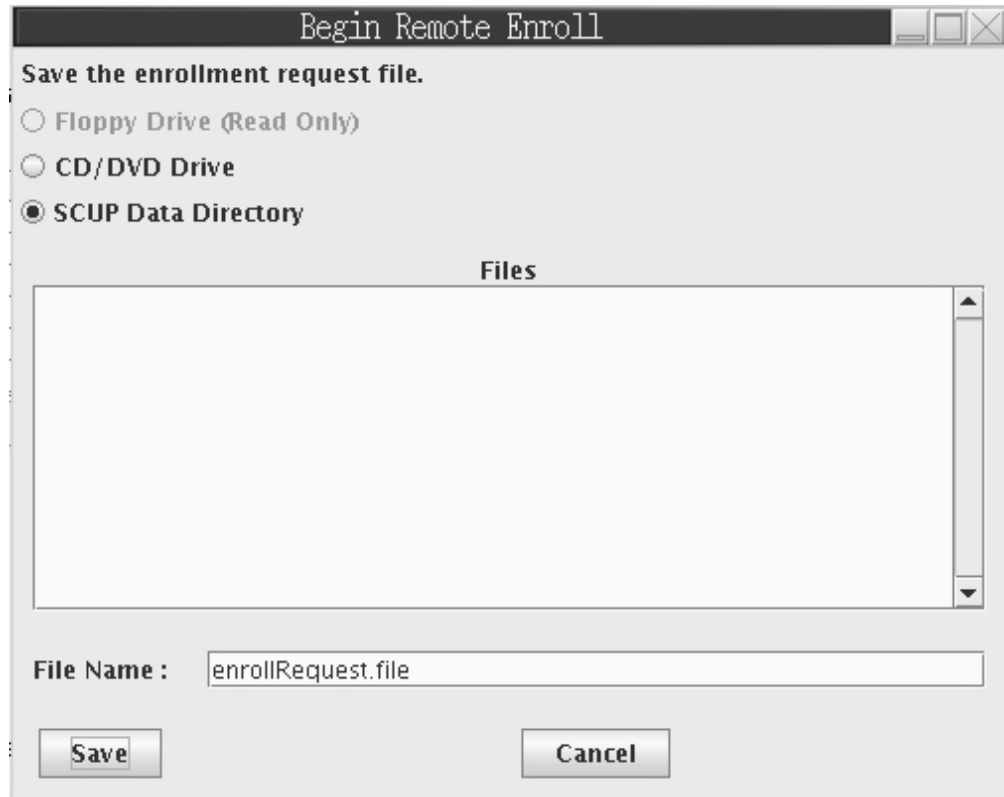


Figure 362. Save Enrollment Request

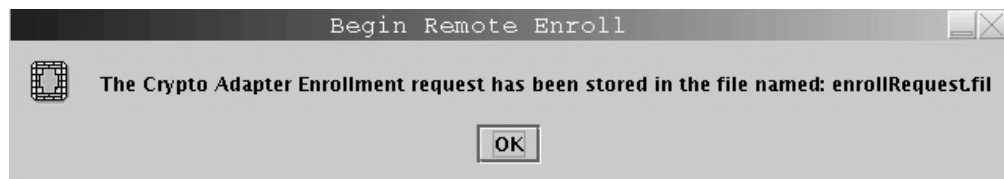


Figure 363. Enrollment Request Stored

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

6. Transport this file to the local workstation.

Note: If the local workstation is TKE 4.2, refer to the TKE Workstation User’s Guide, SA22-7524, on Resource Link for details.

7. On the local workstation, from the *Crypto Adapter* drop down menu, select *Enroll Crypto Adapter* option.
8. Select *remote* when prompted for enrollment type.

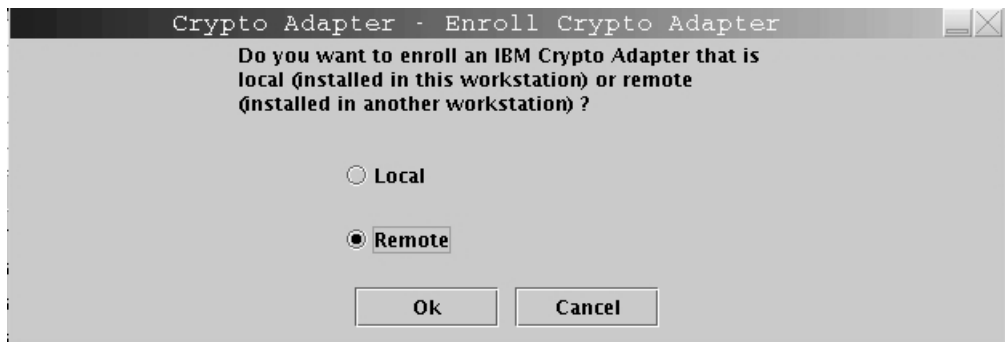


Figure 364. Select remote zone



Figure 365. Remote zone enrollment instructions

9. At the prompt, insert the CA smart card in smart card reader 1.
10. At the prompt, enter the first CA PIN on the PIN pad of smart card reader 1.
11. At the prompt, enter the second CA PIN on the PIN pad of smart card reader 1.
12. At the prompt, select the enrollment request file (created in step 5 on page 298).

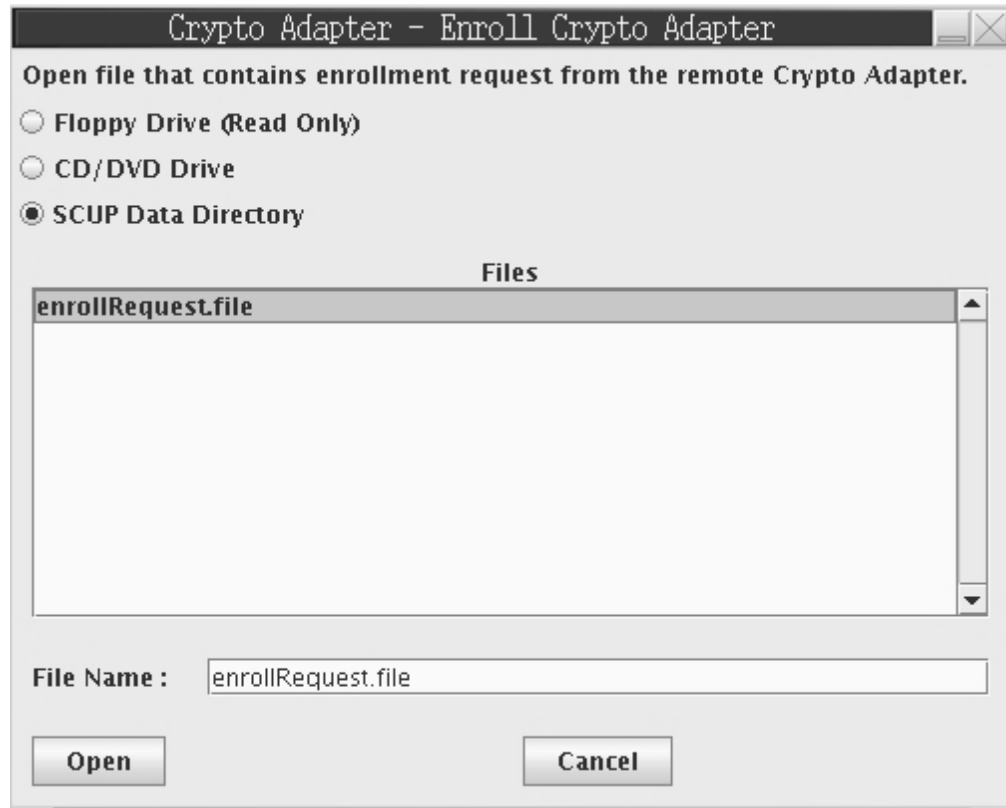


Figure 366. Open enrollment request file

13. The Crypto Adapter serial number is displayed. You are prompted to confirm this enrollment.

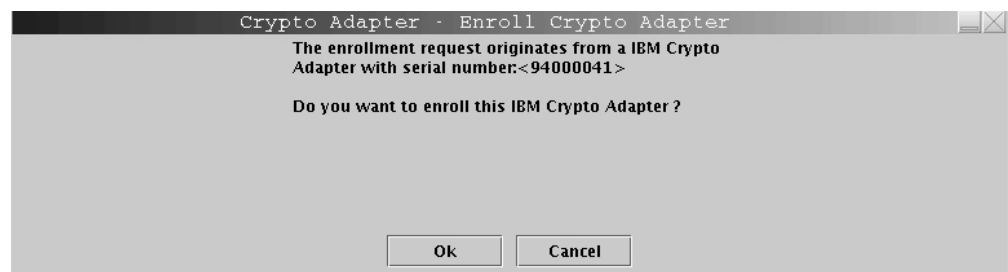


Figure 367. Verification of enrollment request

14. An enrollment certificate is created for the remote cryptographic adapter.
15. Specify a file name to save the enrollment certificate.

Note: If the remote workstation is a TKE 4.2, save the enrollment certificate on a DVD-RAM. On the TKE 4.2 workstation, the enrollment certificate needs to be copied from the DVD-RAM to a diskette.



Figure 368. Save the enrollment certificate



Figure 369. Continue with remote enrollment

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

16. Transport this file to the remote workstation.

Note: If the remote workstation is TKE 4.2, refer to the TKE Workstation User’s Guide, SA22-7524, on Resource Link for details.

17. On the remote workstation, click on Trusted Key Entry, Applications.
18. Click on Complete Zone Remote Enroll Process for an IBM Crypto Adapter.

19. Respond YES to this message: This program installs an enrollment accept in the IBM Cryptographic card installed in this workstation Continue? (Yes/no)
20. If the TKE Crypto Adapter is already enrolled, you are asked to confirm the enrollment and then asked to continue.
21. You are prompted for the file that contains the enrollment certificate (from step 15) by the restricted file chooser.

Warning: If the file is loaded from a floppy or CD/DVD, you must deactivate the floppy or CD/DVD drive before removing the diskette or disc. If the diskette is removed prior to deactivating the drive data could be lost or corrupted. For details on deactivating media see “Managing Media” on page 377.

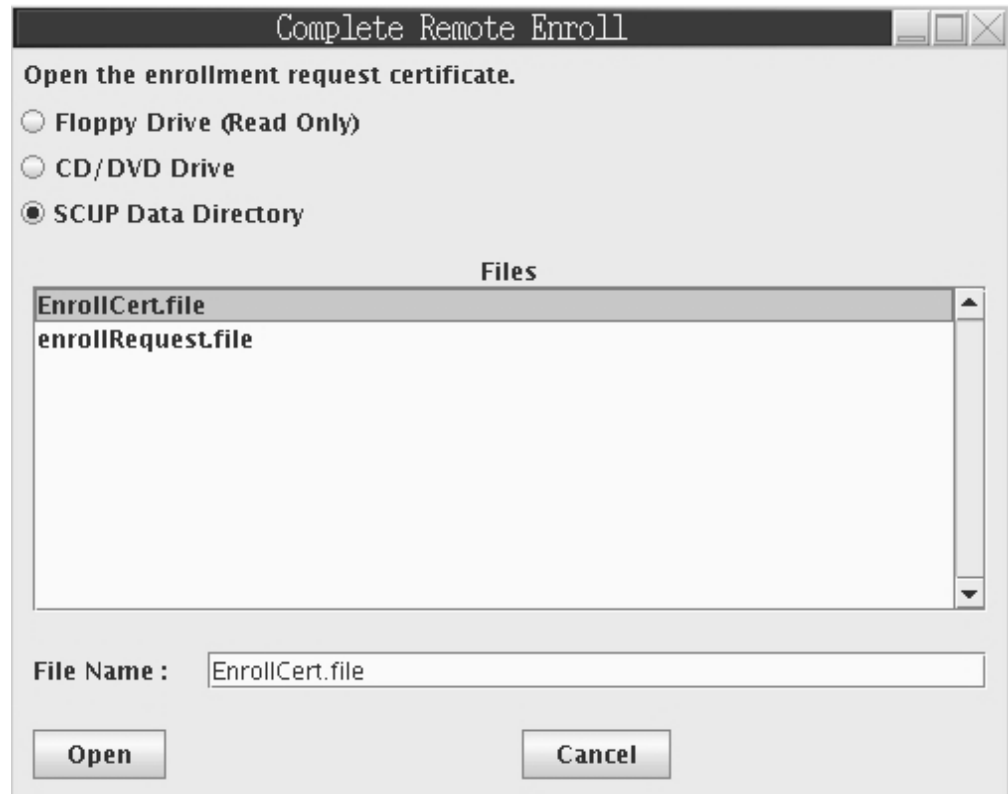


Figure 370. File Chooser Enroll Certificate

22. You will get a message that the remote Crypto Adapter has been installed in the zone (giving the zone description and ID).



Figure 371. Remote Enroll Success

View current zone

Use this function to determine the current zone of the TKE cryptographic adapter. You may want to compare it to the zone of the TKE smart card when working with key parts.

To view the current zone of the TKE cryptographic adapter, follow these steps:

1. From the *Crypto Adapter* drop down menu, select *View current zone* option.



Figure 372. View current zone after Crypto Adapter enrollment

A window is returned with the Zone ID and the Zone description (if you had previously entered one).

Appendix E. Secure Key Part Entry

This topic describes how you can enter a known key part value onto a TKE smart card.

This allows migration of existing key parts to TKE 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 securely on a TKE 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 308.

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 TKE smart card, TKE can use its existing infrastructure to securely load the key part into key storage or onto the host.

Steps for secure key part entry

Secure Key Part Entry begins from the Crypto Module Notebook by right-clicking the desired key type for entry. Right-clicking the desired key type reveals a menu where there is an entry for secure key part.

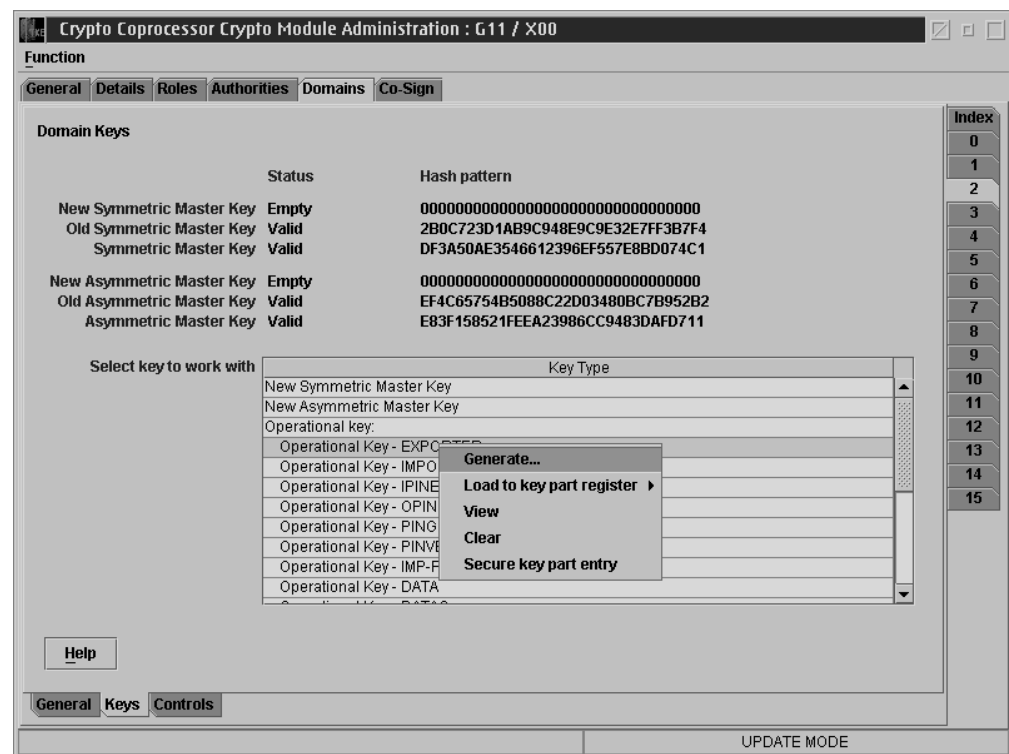


Figure 373. Choosing secure key part entry from the domains keys panel

This menu entry will be available for all four crypto module types: CCF, PCICC, PCIXCC, and CEX2C. Proceed to:

1. Select Secure key part entry.

For master keys on all coprocessors (CCF, PCICC, PCIXCC, CEX2C) and CCF operational keys, this panel appears:

Figure 374. Enter description panel for secure key part entry

For PCIXCC/CEX2C operational keys only, this panel appears:

Figure 375. USER DEFINED operational key for secure key part entry

For a USER DEFINED operational key, the user is allowed to update the description, the key length, and the control vector.

For a default operational key, only the description may be updated, unless the default key type supports multiple key lengths. In that case, the key length field can also be updated. For a default operational key, the control vector cannot be updated.

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 376. Secure key part entry — enter TKE smart card into reader

3. Enter the PIN on the smart card reader PIN pad:

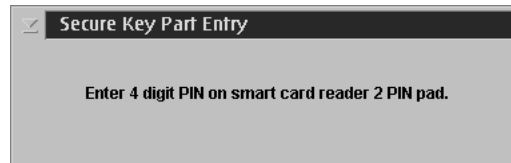


Figure 377. Secure key part entry — enter PIN

4. If the TKE smart card information is correct, press the Yes button to continue:

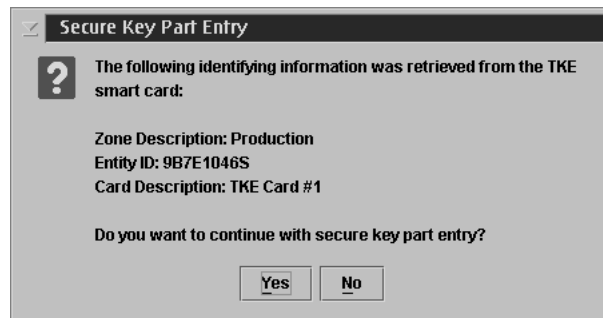


Figure 378. Secure key part entry card identification

5. Enter key part digits (see “Entering a key part on the smart card reader” on page 308) :

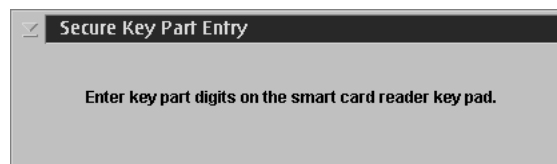


Figure 379. Secure key part entry — enter key part digits

6. After the key part value has been successfully entered on the PIN pad, a panel is displayed with information regarding the key part just entered. The ENC-ZERO, MDC-4, and SHA1 values are shown to the user for verification that the key part was entered correctly. If the key part entered was for an operational key, the CV would also be displayed on this panel. Press OK to continue



Figure 380. Secure key part entry — key part information



Figure 381. Secure key part entry — key part information for operational key

7. Successful entry



Figure 382. Secure key part entry — message for successful execution

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 14 on page 309).

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 key part registers, key part queues, or master 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 smart card reader display is updated and the current block display is reset.
- Once a block is updated with a hexadecimal digit, the values cannot be changed.
- The current decimal digit input is depicted by two lock images. One lock image flashes, indicating the position of the current decimal input that the smart card reader awaits.
- 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 entered decimal digits. It is used to stop the key entering process.

EXAMPLE

Key part type: 8-byte 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 14. 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 F. Access Control Points and Callable Services

The TKE workstation allows you to enable or disable callable service access control points. For systems that do not use the optional TKE Workstation, all access control points (current and new) are enabled in the DEFAULT Role with the appropriate licensed internal code on the PCI Cryptographic Coprocessor, PCI X Cryptographic Coprocessor, or Crypto Express2 Coprocessor

TKE Version 4.0 and Higher

Access to services that are executed on the PCI X Cryptographic Coprocessor or Crypto Express2 Coprocessor is through Access Control Points in the DEFAULT Role. To execute callable services on the PCIXCC/CEX2C, access control points must be enabled for each service in the DEFAULT Role.

New TKE users and non-TKE users have all access control points enabled. This is also true for brand new TKE V5.2 users.

Note: Access control points DKYGENKY-DALL and DSG ZERO-PAD unrestricted hash length and PTR Enhanced PIN Security are always disabled in the DEFAULT Role for all customers (TKE and Non-TKE). A TKE Workstation is required to enable these access control points. DSG ZERO-PAD and PTR Enhanced PIN Security are only applicable to the PCIXCC/CEX2C.

If you are upgrading from TKE V4.0, V4.1, V4.2, TKE V5.0, V5.1 to TKE V5.2 and your configuration includes PCIXCCs or CEX2Cs, the settings (enabled/disabled) for existing access control points remain the same as they were on TKE V4.0, V4.1, V4.2, V5.0 and V5.1. Depending on the ICSF FMID that is installed, new access control points may need to be enabled.

Access Control Point for ICSF APAR OA13764 is:

- PTR Enhanced PIN Security

Enhancements have been made to PIN security and have changed the way some PIN functions work. An access control point has been defined so that the enhancements can be enabled or disabled, at the discretion of the customer, using a TKE workstation. This PTR Enhanced PIN Security access control point is disabled by default. When disabled, the PTR Enhanced PIN Security access control point allows the cryptographic coprocessor (PCIXCC/CEX2C) to continue processing in the old manner, without the security enhancement, and to continue to be completely compatible with existing applications. If the access control point is enabled via a TKE workstation, the card switches to the enhanced, more secure mode of operation.

Access Control Points for HCR7731 are:

- Remote Key Export - Generate or export a key for use by a CCA node
- Trusted Block Create - Activate an Inactive Trusted Key Block
- Trusted Block Create - Create a Trusted Key Block in Inactive Form
- PKA Key Generate - Permit Regeneration Data
- PKA Key Generate - Permit Regeneration Data for Retained Keys

Access Control Points for HCR770B are:

- Diversified Key Generate - TDES-XOR

- Diversified Key Generate - TDESEMV2/TDESEMV4
- PIN Change/Unblock - change EMV PIN with OPINENC
- PIN Change/Unblock - change EMV PIN with IPINENC
- Transaction Validation - Generate
- Transaction Validation - Verify CSC-3
- Transaction Validation - Verify CSC-4
- Transaction Validation - Verify CSC-5
- Key Part Import - RETRKPR

Access Control Points for HCR770A are:

- CKDS Conversion Program
- Clear Key Import
- Decipher
- Digital Signature Verify
- DSG ZERO-PAD Unrestricted Hash Length
- Encipher
- Key Part Import - ADD-PART keyword
- Key Part Import - COMPLETE keyword
- NOCV Exporter
- NOCV Importer
- Prohibit Export Extended
- Public Key Encrypt

These access control points are only supported on the PCIXCC/CEX2C.

For the relationship between access control points and callable services, see Table 15 on page 314.

TKE Version 3.1

Access to services that are executed on the PCI Cryptographic Coprocessor is through Access Control Points in the DEFAULT Role. To execute callable services on the PCI Cryptographic Coprocessor, access control points must be enabled for each service in the DEFAULT Role. The ability to enable/disable access control points in the DEFAULT Role was introduced on OS/390 V2R10 through APAR OW46381 for the Trusted Key Entry Workstation. New TKE customers and Non-TKE customers have all access control points enabled. This is also true for brand new TKE V3.1 users (not converting from TKE V3.0).

Note: Access control point DKYGENKY-DALL is always disabled in the DEFAULT Role for all customers (TKE and Non-TKE). A TKE Workstation is required to enable this access control point for the Diversified Key Generate service.

For existing TKE V3.0 users, upgrading to TKE V3.1 (APAR OW46381 and its corresponding ECA), current (for the level of ICSF you are running) access control points in the DEFAULT Role are enabled. Any new access control points are disabled in the DEFAULT Role and must be enabled through TKE if the service is required.

Notes:

1. APAR OW46381 will update the TKE Host Code
2. ECA 186 will update the TKE Workstation Code

3. The latest or most current driver is required for the PCI Cryptographic Coprocessor licensed internal code for the S/390 G5 Enterprise Server or the S/390 G6 Enterprise Server
4. The latest or most current driver is required for the PCI Cryptographic Coprocessor licensed internal code for the IBM @server zSeries 900

All of the components are required for complete access control point support.

Access to services which execute on the Cryptographic Coprocessor Feature is through SAF. Disablement through SAF is sufficient to prevent execution of a service by either the Cryptographic Coprocessor Feature or the PCI Cryptographic Coprocessor. For functions which can be executed on the PCI Cryptographic Coprocessor, enablement of the function requires that the function be enabled through SAF and through the access control point in the DEFAULT Role.

If you are on OS/390 V2 R10, using a TKE V3.0 workstation, access control points for new services (requiring APARs OW46380 and OW46382) will be disabled. Existing access control points will be enabled in the DEFAULT Role. APAR OW46381 must be installed to enable the OS/390 V2 R10 interface. This will allow the TKE Administrator to enable any new access control points for ICSF services that execute in the PCI Cryptographic Coprocessor under the DEFAULT Role.

Access Control Points (requiring APARs OW46380 and OW46382) for OS/390 V2R10 are:

- DATAM Key Management Control

Note: For existing TKE installations (upgrading to TKE V3.1), it is required that this access control point be enabled. Failure to do so will result in processing errors for Double MAC keys in Key Import, Key Export, and Key Generate.

- Diversified Key Generate - Single length or same halves
- Diversified Key Generate - CLR8-ENC
- Diversified Key Generate - TDES-ENC
- Diversified Key Generate - TDES-DEC
- Diversified Key Generate - SESS-XOR
- Diversified Key Generate - DKYGENKY-DALL

Note: This access control point is always disabled in the DEFAULT Role for all customers (TKE and Non-TKE). A TKE Workstation is required to enable the function.

- MAC Generate - For existing TKE installations, it is recommended that this access control point be enabled.
- MAC Verify - For existing TKE installations, it is recommended that this access control point be enabled.

Access Control Points for z/OS V1 R2 are:

- PKA Key Token Change
- Secure Messaging for Keys
- Secure Messaging for PINs

Access Control Points for z/OS V1 R3 are:

- UKPT - PIN Verify, PIN Translate

Access Control Points for APAR OW53666 are:

- Data Key Export - Unrestricted
- Data Key Import - Unrestricted
- Key Export - Unrestricted
- Key Import - Unrestricted
- Key Part Import - Unrestricted

If an access control point is disabled, the corresponding ICSF callable service will fail during execution with an access denied error.

Table 15. Callable service access control points

Access Control Point	Callable Service
*Clear Key Import	CSNBCKI or CSNBCKM
Clear PIN Encrypt	CSNBCE
Clear PIN Generate - 3624	CSNBPGN
Clear PIN Generate - GPB	CSNBPGN
Clear PIN Generate - VISA PVV	CSNBPGN
Clear PIN Generate - Interbank	CSNBPGN
Clear Pin Generate Alternate - 3624 Offset	CSNBCPA
Clear PIN Generate Alternate - VISA PVV	CSNBCPA
Control Vector Translate	CSNBCVT
Cryptographic Variable Encipher	CSNBCVE
*CKDS Conversion Program	CSFCONV
CVV Generate	CSNBCSG
CVV Verify	CSNBCSV
DATAM Key Management Control	CSNBKGN, CSNBKIM, CSNBKEX and CSNBDKG
Data Key Export	CSNBDKX
Data Key Export - Unrestricted	CSNBDKX
Data Key Import	CSNBDKM
Data Key Import - Unrestricted	CSNBDKM
*Decipher	CSNBDEC
Digital Signature Generate	CSNDDSG
*DSG ZERO-PAD unrestricted hash length	CSNDDSG
*Digital Signature Verify	CSNDDSV
Diversified Key Generate - CLR8-ENC	CSNBDKG
Diversified Key Generate - TDES-ENC	CSNBDKG
Diversified Key Generate - TDES-DEC	CSNBDKG
Diversified Key Generate - SESS-XOR	CSNBDKG
Diversified Key Generate - single length or same halves	CSNBDKG
**Diversified Key Generate - TDES-XOR	CSNBDKG
**Diversified Key Generate - TDESEMV2/TDESEMV4	CSNBDKG
DKYGENKY - DALL	CSNBDKG

Table 15. Callable service access control points (continued)

*Encipher	CSNBENC
Encrypted PIN Generate - 3624	CSNBEPG
Encrypted PIN Generate - GPB	CSNBEPG
Encrypted PIN Generate - Interbank	CSNBEPG
Encrypted PIN Translate - Translate	CSNBPTR
Encrypted PIN Translate - Reformat	CSNBPTR
Encrypted PIN Verify - 3624	CSNBPVR
Encrypted PIN Verify - GPB	CSNBPVR
Encrypted PIN Verify - VISA PVV	CSNBPVR
Encrypted PIN Verify - Interbank	CSNBPVR
Key Export	CSNBKEX
Key Export - Unrestricted	CSNBKEX
Key Generate - OPIM, OPEX, IMEX, etc.	CSNBKGN
Key Generate - EX, IM, OP	CSNBKGN
Key Generate - CVARs	CSNBKGN
Key Generate - SINGLE-R	CSNBKGN
Key Import	CSNBKIM
Key Import - Unrestricted	CSNBKIM
*Key Part Import - ADD-PART keyword	CSNBKPI
*Key Part Import - COMPLETE keyword	CSNBKPI
Key Part Import - first key part	CSNBKPI
Key Part Import - middle and final	CSNBKPI
Key Part Import - unrestricted	CSNBKPI
Key Part Import - RETRKPR	CSNBKPI
Key Translate	CSNBKTR
MAC Generate	CSNBMGN
MAC Verify	CSNBMVR
*NOCV EXPORTER	CSNBKEX, CSNBSKM, and CSNBKGN
*NOCV IMPORTER	CSNBKIM, CSNBSKI, CSNBSKM, and CSNBKGN
**PIN Change/Unblock - change EMV PIN with OPINENC	CSNBPCU
**PIN Change/Unblock - change EMV PIN with IPINENC	CSNBPCU
PKA Decrypt	CSNDPKD
PKA Encrypt	CSNDPKE
PKA Key Generate	CSNDPKG
PKA Key Generate - Clear	CSNDPKG
PKA Key Generate - Clone	CSNDPKG
PKA Key Generate - Permit Regeneration Data	CSNDPKG

Table 15. Callable service access control points (continued)

PKA Key Generate - Permit Regeneration Data for Retained Keys	CSNDPKG
PKA Key Import	CSNDPKI
PKA Key Token Change	CSNDKTC
Prohibit Export	CSNBPEX
*Prohibit Export Extended	CSNBPEXX
PTR Enhanced PIN Security	CSNBCPE, CSNBCPA, CSNBEPG, CSNBPTR, CSNBPVR, and CSNBPCU
*Public Key Encrypt	CSNDPKE
Retained Key Delete	CSNDRKD
Retained Key List	CSNDRKL
Remote Key Export	CSNDRKX
Secure Key Import - IM	CSNBSKI or CSNBSKM
Secure Key Import - OP	CSNBSKI or CSNBSKM
Secure Messaging for Keys	CSNBSKY
Secure Messaging for PINs	CSNBSPN
SET Block Compose	CSNDSBC
SET Block Decompose	CSNDSBD
SET Block Decompose - PIN ext IPINENC	CSNDSBD
SET Block Decompose - PIN ext OPINENC	CSNDSBD
Symmetric Key Export - PKCS-1.2	CSNDSYX
Symmetric Key Export - ZERO-PAD	CSNDSYX
Symmetric Key Generate - PKA92	CSNDSYG
Symmetric Key Generate - PKCS-1.2	CSNDSYG
Symmetric Key Generate - ZERO-PAD	CSNDSYG
Symmetric Key Import - PKA92 KEK	CSNDSYI
Symmetric Key Import - PKA92 PIN Key	CSNDSYI
Symmetric Key Import - PKCS-1.2	CSNDSYI
Symmetric Key Import - ZERO-PAD	CSNDSYI
**Transaction Validation - Generate	CSNBTRV
**Transaction Validation - Verify CSC-3	CSNBTRV
**Transaction Validation - Verify CSC-4	CSNBTRV
**Transaction Validation - Verify CSC-5	CSNBTRV
Trusted Block Create - Activate an Inactive Trusted Key Block	CSNDTBC
Trusted Block Create - Create a Trusted Key Block in Inactive form	CSNDTBC
UKPT - PIN Verify, PIN Translate	CSNBPVR and CSNBPTR

Notes:

1. * indicates that the access control point is only available with a PCI X Cryptographic Coprocessor or Crypto Express2 Coprocessor.

- I
- I
2. ** indicates that the access control point is only available with a PCI X Cryptographic Coprocessor or Crypto Express2 Coprocessor and requires z990 with May 2004 or later version of Licensed Internal Code (LIC, a z890, z9 EC, z9 BC and System z10 EC with MCL 029 Stream J12220.
 3. To use PKA Key Generate - Clear or PKA Key Generate - Clone, the PKA Key Generate access control point must be enabled or the callable service will fail. PKA Key Generate - Permit Regeneration or Permit Regeneration Data for Retained Keys is optional and should be enabled as required for authorized usage. Enabling this command is not recommended for production and usage requires special consideration.
 4. To use SET Block Decompose - PIN ext IPINENC or PIN ext OPINENC, the SET Block Decompose access control point must be enabled or the callable service will fail.
 5. Diversified Key Generate - single length or same halves requires either Diversified Key Generate - TDES-ENC or Diversified Key Generate - TDES-DEC be enabled.
 6. Encrypted PIN Translate - PTR Enhanced PIN Security - enhanced further to produce return code 8,3016 - The value of the PAD data is not valid.

Appendix G. LPAR Considerations

Setup for CCF Systems

Prior to activating the Cryptographic characteristics (on the Crypto page), the cryptographic coprocessors must be selected on the Processor Page of the Customize Activation Profiles Task. Once a cryptographic coprocessor (0,1, or both) is selected for the LP, the Crypto tab is automatically displayed so cryptographic coprocessor characteristics can be defined.

In LPAR mode, only one partition can perform TKE functions at a time. The partition with this control is referred to as the TKE host. The other partitions that receive key updates from the TKE host are referred to as the TKE targets. To enable the TKE host to control the TKE targets, you need to define the control and usage domain indexes and enable specific profile options.

To configure the TKE host partition, enable these options on the Crypto page of the Customize Activation Profiles task:

- Enable public key algorithm (PKA) facility
- Enable cryptographic functions
- Enable public key secure cable (PKSC) and integrated cryptographic service facility (ICSF)
- Enable Modify authority
- Enable query signature controls
- Enable query transport control
- Enable cryptographic facility (ICRF) key entry (if you intend to use the load to queue function)
- Enable special secure mode

To configure the TKE target partitions, enable these options on the Crypto page of the Customize Activation Profiles task:

- Enable public key algorithm (PKA) facility
- Enable cryptographic functions
- Enable public key secure cable (PKSC) and integrated cryptographic service facility (ICSF)
- Enable cryptographic facility (ICRF) key entry (if you intend to use the load to queue function)
- Enable special secure mode

Note: Special secure mode must also be enabled in the installation options data set in addition to the profile options. You can then use the TKE functions to dynamically enable and disable special secure mode.

When defining the control and usage domains for the TKE host and TKE target partitions, assign the same number for both the usage domain index and the logical partition. This usage domain index and logical partition number should be the same as the domain number specified in the installation options data set for this partition. The control domain index list for the TKE host and the TKE target partitions always includes the logical partition's usage domain index. In addition, the TKE host partition's control domain index list must include the usage domain index for all the TKE target partitions for which it has control.

For example, in Figure 383 LPAR 0 is the TKE host and controls the TKE target partitions 1, 2, and 3. The control domain and usage domain on all partitions are the same number as the LPAR number. In real installations, this setup scheme is not possible because the LPAR numbering begins at one and not zero. It is used in the sample for ease of understanding. The TKE host, however, also includes control domain indexes for partitions 1, 2, and 3.

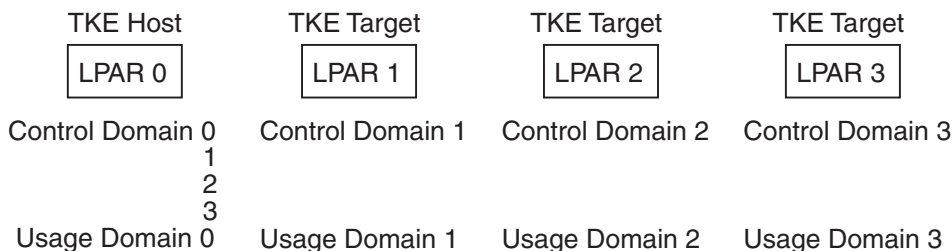


Figure 383. An Example of TKE Host and TKE Target LPARs

In this example, the TKE host workstation connects to the host system defined as LPAR 0. To update DES or PKA master keys for LPAR 0, the TKE administrator selects domain 0. To load DES or PKA master keys into any of the target LPARs, the TKE administrator changes the active selection on the TKE workstation to specify the domain of the target LPAR.

If for any reason you need to reassign a domain currently in use, you should zeroize the domain first. See “Zeroize Domain” on page 104.

Setup for PCIXCC/CEX2C Systems

On z990, z890, z9 EC, z9 BC and System z10 EC systems, there is no specific field on the LPAR Activation Profile to identify the TKE Host. You must decide which LPAR will be the TKE Host and setup the control domain and PCI Cryptographic Candidate List appropriately.

On z990, z890, z9 EC, z9 BC and System z10 EC systems, multiple TKE Target LPARs can be assigned the same domain number – provided they do not share any PCIXCCs/CEX2Cs. Therefore, the TKE Host LPAR **must** have a unique domain number. The TKE Host LPAR must also have access to all the PCIXCCs/CEX2Cs that are to be controlled on the system.

In the LPAR Activation, define the control and usage domain index for each LPAR. Assign the same number for both the usage domain and the logical partition. This usage domain index and logical partition number should be the same as the domain number specified in the installation options data set for this partition. The control domain index list for the TKE Host and the TKE target partitions always includes the logical partition’s usage domain index. In addition, the TKE Host partition’s control domain index must include the usage domain index for all the TKE target partitions for which it has control.

Additionally, the PCI Cryptographic Candidate List and PCI Cryptographic Online List must be configured in the LPAR Activation Profile. The Candidate List includes all PCIXCCs/CEX2Cs that CAN be online for the LPAR. The Online List includes all PCIXCCs/CEX2Cs that will be online when activation is complete (selections in the Online List must be selected in the Candidate List).

If TKE Target LPARs are sharing the same domain, the PCIXCCs/CEX2Cs defined in the Candidate List can not include any of the same PCIXCCs/CEX2Cs. For the TKE Host, the PCI Cryptographic Candidate List **must** include all the PCIXCCs/CEX2Cs for all the TKE target partitions for which it has control.

The example in Figure 384 has 3 LPARs and 4 PCIXCCs/CEX2Cs: 00, 01, 02, 03. There is no domain sharing. In this case, all the PCIXCCs/CEX2Cs can be specified in the Candidate List for each LPAR.

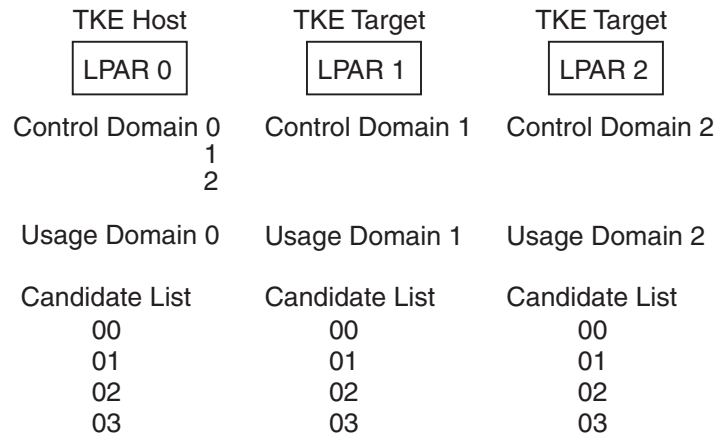


Figure 384. An Example of TKE Host and TKE Target LPARs without Domain Sharing

The example in Figure 385 has 4 LPARs, 2 sharing the same domain and 4 PCIXCCs/CEX2Cs: 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 PCIXCCs/CEX2Cs.

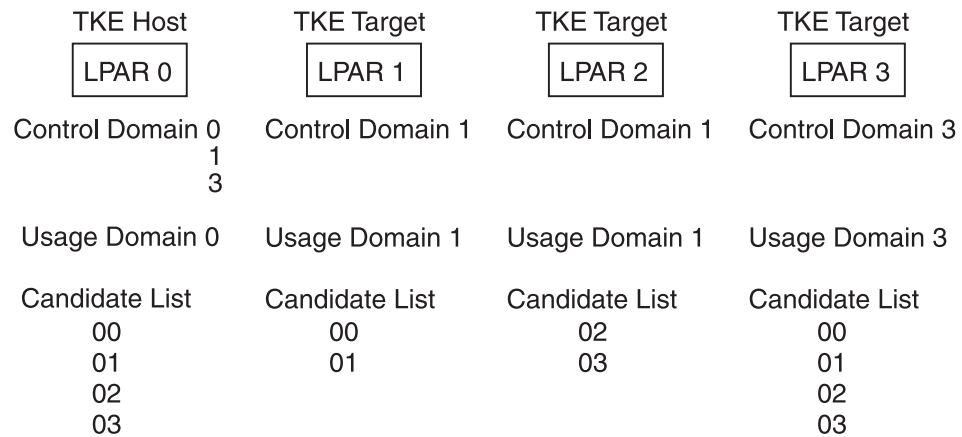


Figure 385. An Example of TKE Host and TKE Target LPARs with Domain Sharing

If the same domain is specified by more than one LPAR and the Candidate List has any of the same PCIXCCs/CEX2Cs, the first LPAR that is activated will IPL without error but the other LPARs with the same domain will fail activation.

Appendix H. Auditing

ICSF uses SMF record type 82 to record certain ICSF events. Record type 82 contains a fixed header section and subtypes.

ICSF writes to subtype 12 for every PKSC command entered through the CSFPKSC interface. Subtype 12 contains this information:

- The complete TKE request to the CCF
- The corresponding complete TKE response from the CCF

ICSF writes to subtype 16 whenever a TKE workstation either issues a command request to a PCI Cryptographic Coprocessor or PCI X Cryptographic Coprocessor or Crypto Express2 Coprocessor or receives a reply response from a PCI Cryptographic Coprocessor or PCI X Cryptographic Coprocessor or Crypto Express2 Coprocessor. Subtype 16 contains this information:

- The indicator for request or reply
- The indicator for PCICC or PCIXCC or CEX2C
- The PCI Cryptographic Coprocessor or PCI X Cryptographic Coprocessor or Crypto Express2 Coprocessor processor number
- The PCI Cryptographic Coprocessor or PCI X Cryptographic Coprocessor or Crypto Express2 Coprocessor serial number
- The PCI Cryptographic Coprocessor or PCI X Cryptographic Coprocessor or Crypto Express2 Coprocessor domain index
- The request command block or reply response block length
- The request command data block or reply response data block length
- The request or reply CPRB
- The length of the fixed audit data
- The number of relocate sections
- The function id
- The function return code
- The function description - describes the function id.

See *z/OS MVS System Management Facilities (SMF)* for details on the request and response formats.

Appendix I. 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:

[illegible]

Example 2:

0200004000030040
800000000000000001AE28DA4606D885EB7E0340D6BAAC51991C0CD0EAE835AF
D9CFF3CD7E7EA74141DADD24A6331BEDF41A6626522CCF15767D167D01A16F97
010001
0252BDAD4252BDAD425A8C6045D41AFAF746EBD5F085D574FCD9C07F0B38C2C
45017C2A1AB919ED2551350A76606BFA6AF2F1609A00A048DD719A55EDCA801

Appendix J. Trusted Key Entry - Workstation Cryptographic Adapter Initialization

Crypto Node Management Batch Initialization 3.10SC

The Crypto Node Management Batch Initialization 3.10 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 3.10SC. Open the Cryptographic Node Management Utility 3.10SC. Click on File and select CNI Editor.

All scripts must be run from the floppy or CNM Data Directory. User created scripts can be used to further initialize the TKE Crypto Adapter after passphrase or smart card initialization has been done. For details on Initializing the TKE Crypto Adapter for Passphrase or Smart Card “Initializing TKE for passphrase” on page 220 and “Initializing TKE for smart cards” on page 227.

To execute a user defined CNI script, click on Trusted Key Entry, and then Crypto Node Management Batch Initialization 3.10SC. The Select CNI file to Run window is displayed. Select the location (Floppy Drive or CNM Data Directory) and the file name of the CNI to execute. Click on Open.

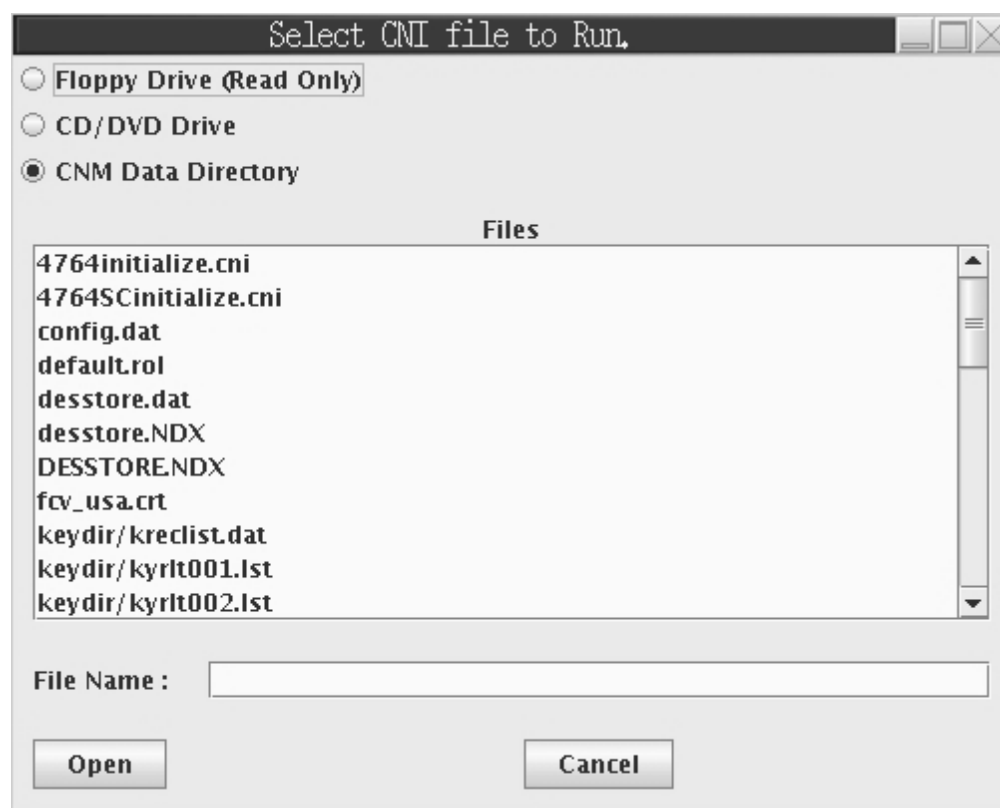


Figure 386. Crypto Node Management Batch Initialization 3.10SC Task Window

The output window shows the operations performed. Select OK to exit this task.

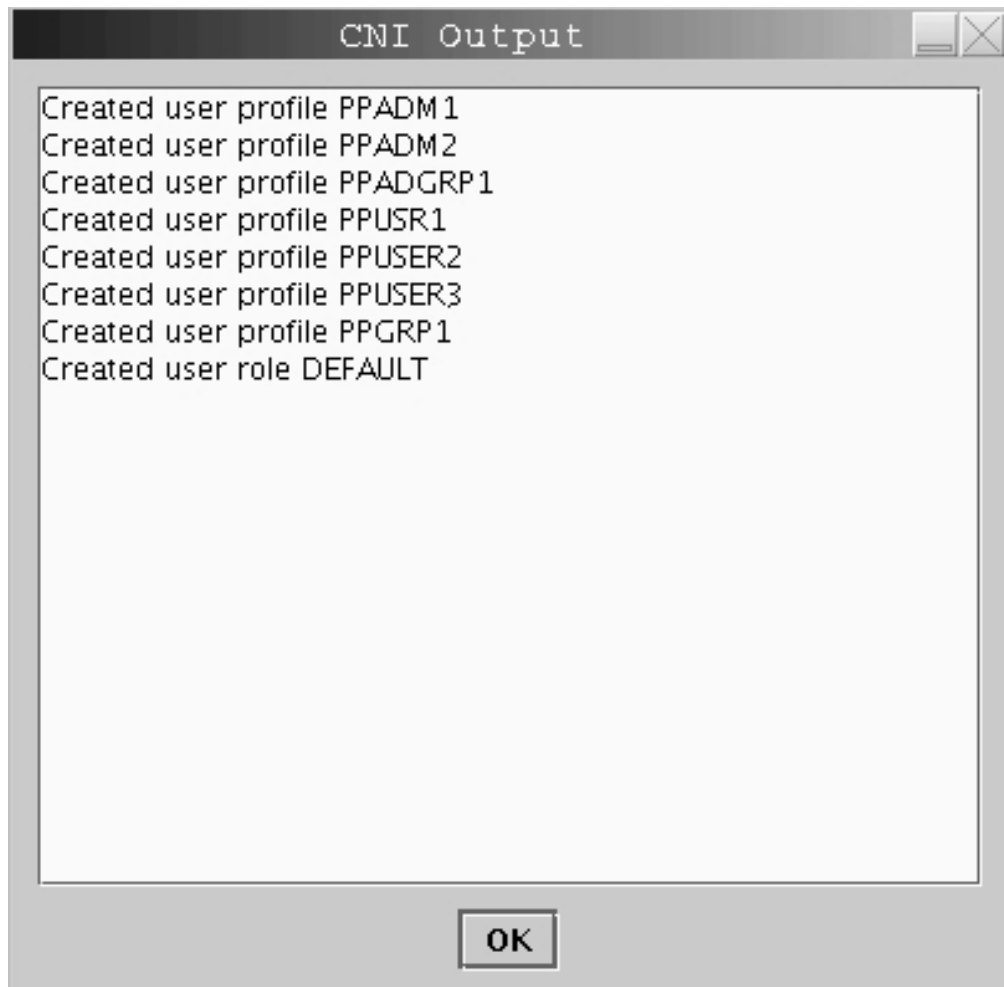


Figure 387. Crypto Node Management Batch Initialization 3.10SC Task Output Window

CCA CLU 3.10SC

The CCA CLU 3.10SC task is used for loading and checking code on the TKE Crypto Adapter.

Note: CLU should only be executed when directed by IBM support.

To invoke the CLU Utility, click on Trusted Key Entry, then select CCA CLU 3.10SC.

CLU Processing

When CLU is invoked, the Non-Factory Mode is displayed. You can select any combination of CLU command check boxes.

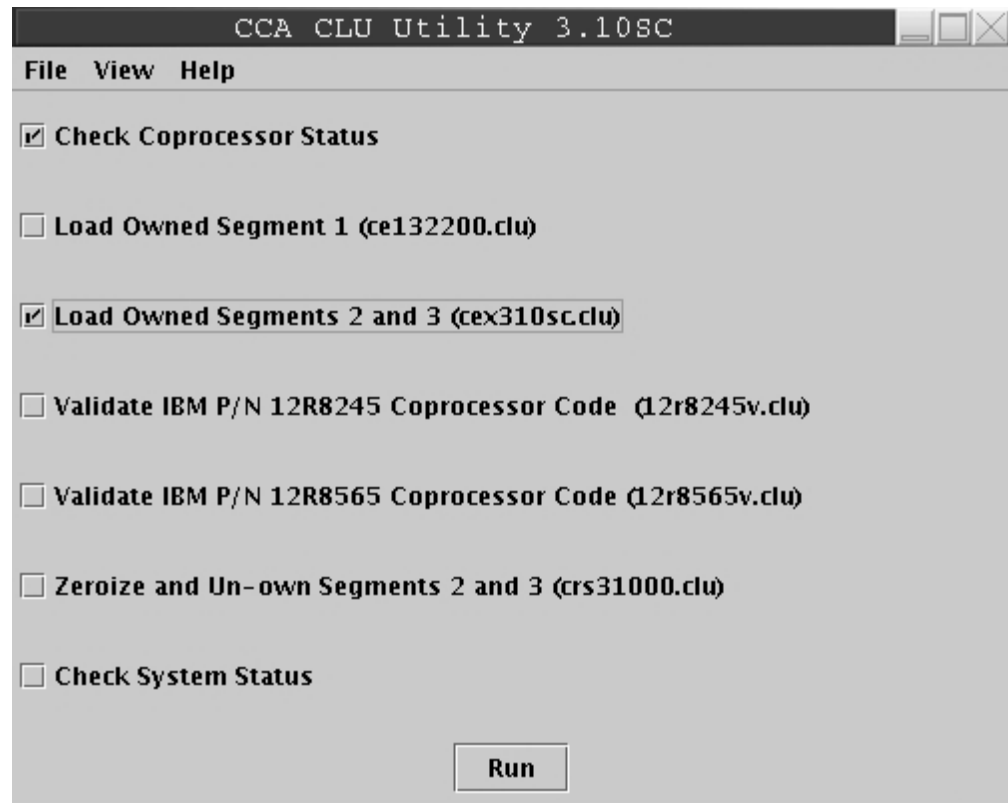


Figure 388. CLU Checked Check Boxes

When RUN is pressed, the commands will execute in the order they appear on the application window.



Figure 389. CLU Error

If a command fails, the commands checked after the failing command will not execute and will remain checked.

After pressing the RUN button view the Output Log or the Command History to check the output from the CLU commands. Both can be viewed by pressing the View menu and then selecting Output Log or Command History from the menu. The CLU output file is available to the user in the CNM Data Directory.

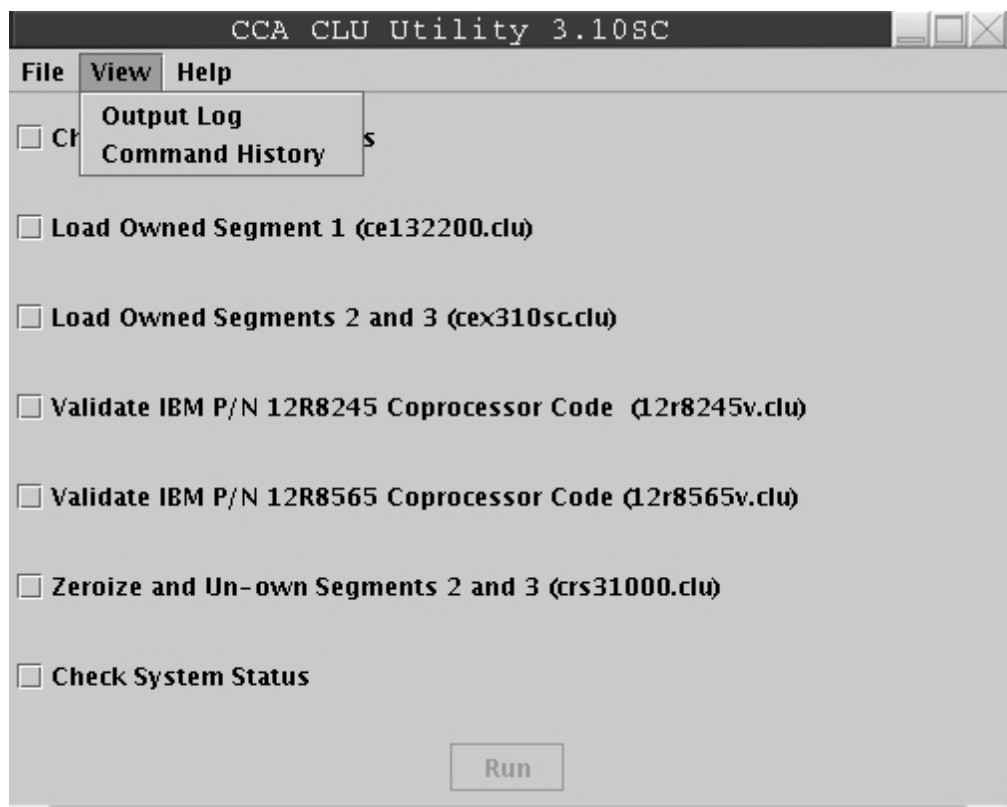


Figure 390. CLU View Menu



Figure 391. Output Log file

The CLU output log file is available to the user in the CNM Data Directory.

be displayed.

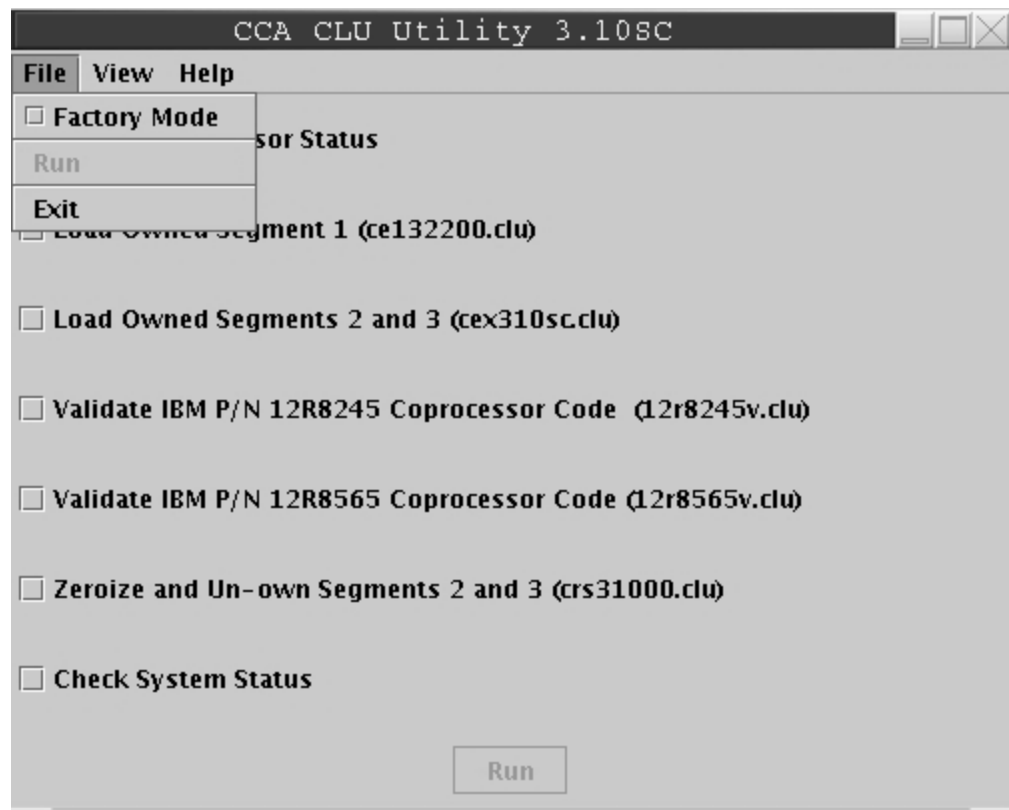


Figure 394. CLU File Menu

Reload segment 1 with the CCA segment 1 file cr132200.clu. Select the "Load Factory Segment 1 (cr132200.clu)" check box and then press the Run button.

- b. If the segment 1 image name indicates ...CCA ..., and the revision level is below 3.22, reload segment 1 with the CCA segment 1 file ce132200.clu by selecting the "Load Owned Segment 1 (ce132200.clu)" check box and then pressing the Run button.

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). For IBM 4764 Model 1 P/N 41U0441, select the "Load IBM P/N 41U0441 Factory Segments 2 and 3 (cnw310sc.clu)" check box and press the RUN button. For IBM 4764 Model 1 P/N 12R8245 and 12R8565, select the "Load IBM P/N 12R8245 and 12R8565 Factory Segments 2 and 3 (cnw310sc.12r.clu)" check box and press the RUN button.
- b. If segment 2 and 3 ROM status both indicate owner 02... For IBM 4764 Model 1 P/N 41U0441, select the "Load IBM P/N 41U0441 Owned Segments 2 and 3 (cex310sc.clu)" check box and press the RUN button. For IBM 4764 Model 1 P/N 12R8245 and 12R8565, select the "Load IBM P/N 12R8245 and 12R8565 Owned Segments 2 and 3 (cex310sc.12r.clu)".

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 will indicate that the segments contain:

Segment 1 Image: 3.22 POST1V2, MB1 V1.25 FPGA v78

Segment 2 Image: 3.10 Linux OS

Segment 3 Image: 3.10.SC CCA

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 Crypto Adapter and press the Run button.

IBM 4764 Model 01 P/N 41U0441

Validate IBM P/N 41U0441 Coprocessor Code (41u0441v.clu)

IBM 4764 Model 01 P/N 12R8245

Validate IBM P/N 12R8245 Coprocessor Code (12r8245v.clu)

IBM 4764 Model 01 P/N 12R8565

Validate IBM P/N 12R8565 Coprocessor Code (12r8565v.clu)

View the results in the Output Log or Command History.

Checking System Status

If you want to check the system status of your Crypto Adapter, use the CLU utility check system status command (SS). Select the "Check System Status" check box and then press the Run button.

View the results in the Output Log or Command History.

Resetting Coprocessor

If you need to reset the Crypto Adapter use the CLU utility reset coprocessor command (RS). You must enter Factory mode by clicking "Factory Mode" menu item under the File menu. Then select the "Reset Coprocessor" check box and press the Run button.

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 (crs31000.clu)" check box and then press the Run button. 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 contents of Help, select Contents from the HELP menu.

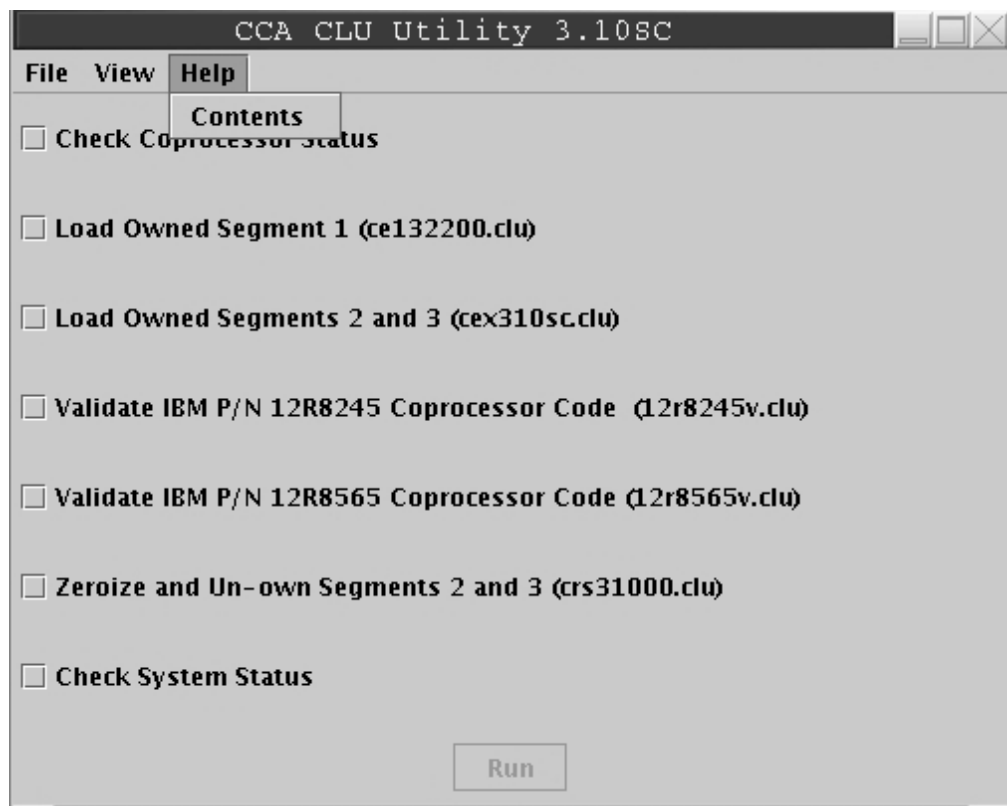


Figure 395. CLU Help Menu

Appendix K. Trusted Key Entry - Utilities

Edit TKE Files

The Edit TKE Files task provides a way to edit/browse files on diskette, CD/DVD, and 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

To open the Edit TKE Files task, click on Trusted Key Entry and then click on Edit TKE Files.

To edit, select a file from the displayed list. If you enter a File Name manually that does not exist, a new file by that name will be created in the location specified.

Note: Files on a CD can only be browsed. Writing to a CD is not supported.

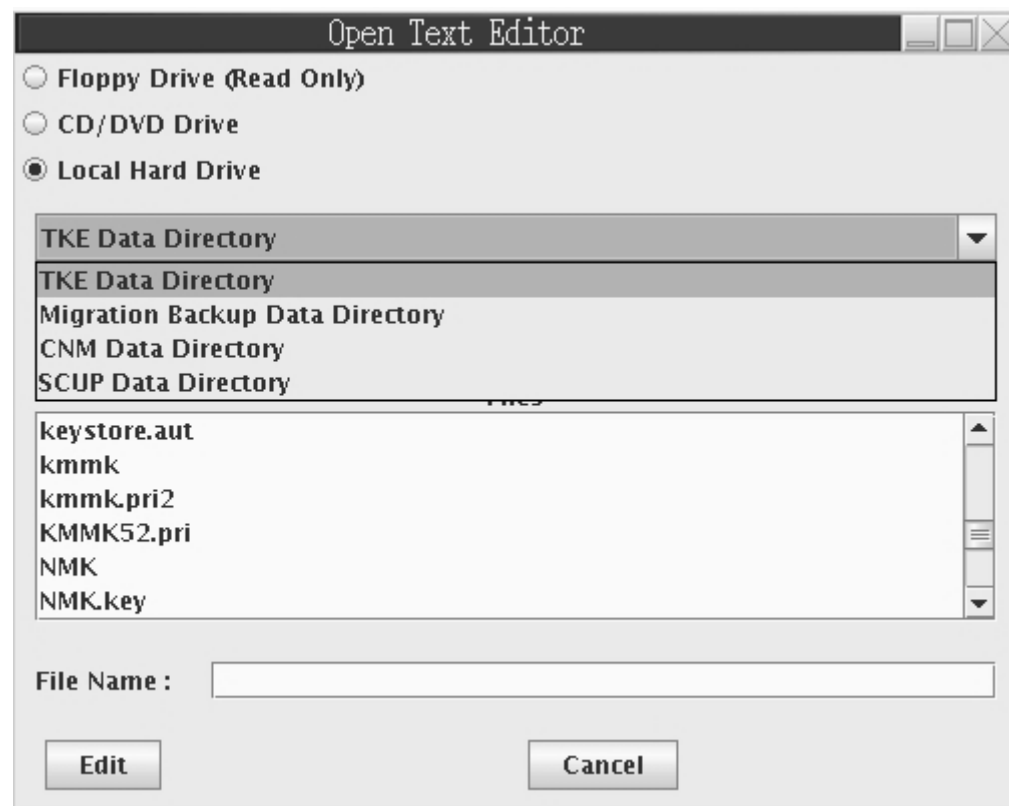


Figure 396. Edit TKE Files Task Window

You will be prompted to confirm creation of a new file.



Figure 397. Confirm Creation of a New File Prompt Window

In this case, a file was created using the name Test.txt. You can edit the file within the edit text box and use File -> Save menu item to save the file.

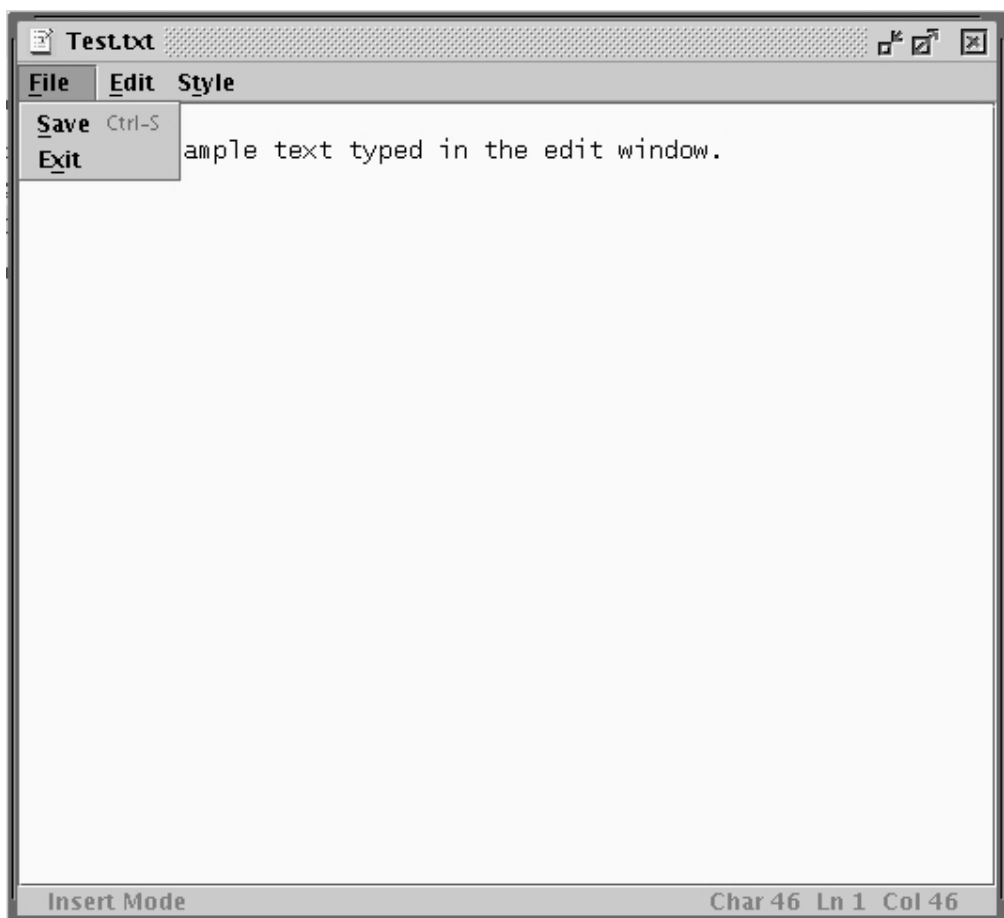


Figure 398. Editor - File menu items

Warning: If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “Managing Media” on page 377.

The editor provides options for Undo, Cut, Copy, Paste, along with Line Selection and Search/Replace.

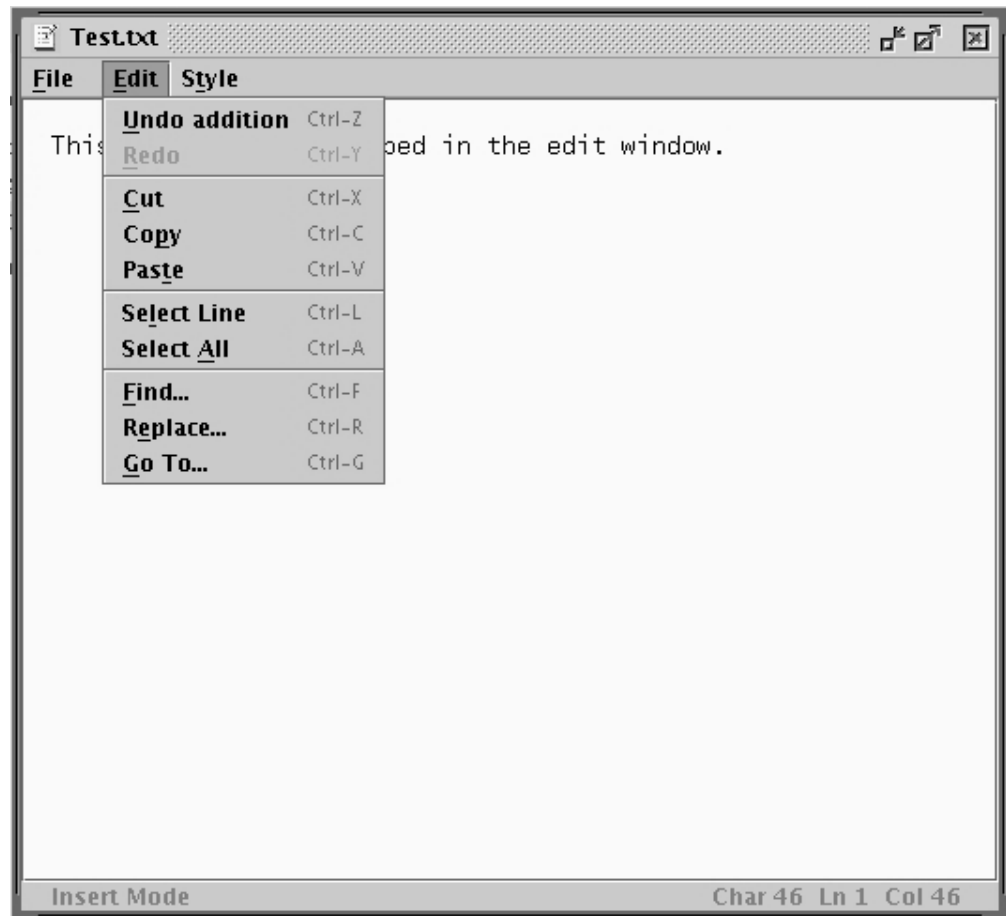


Figure 399. Editor - Edit menu items

In addition, there are options for Fonts, line wrap, and background.

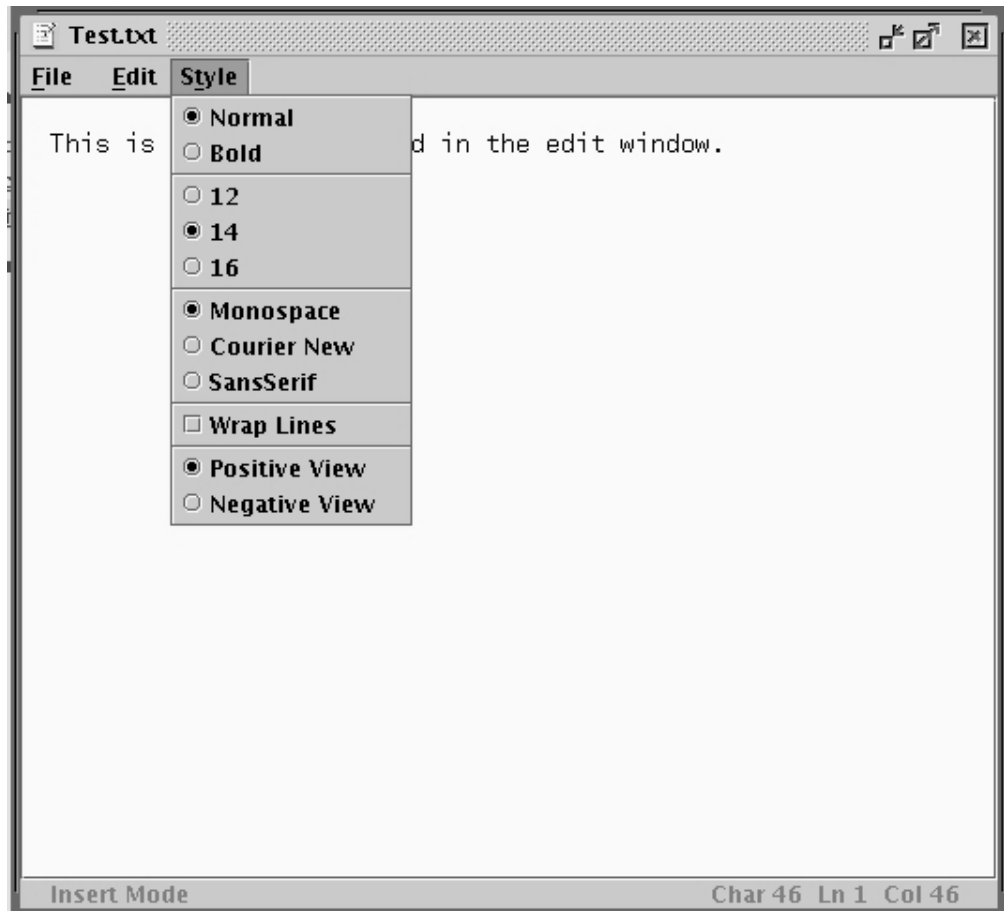


Figure 400. Editor - Style Menu Items

Migrate Previous TKE Version to TKE 5.2

This task is executed only when you have an existing TKE 3.0, 3.1, 4.0, 4.1, or 4.2 workstation and are migrating to TKE Version 5.2. It will migrate the default passphrase and smart card roles and profiles, DES and PKA Key storages, Host.dat, Group.dat, 3270 emulator sessions, FCV, and TCP/IP information. Prior to executing this task, you must execute the 'TKE Backup' on your existing TKE Workstation. After the TKE Backup has been executed, if you have Customer defined roles and profiles for your 4758 crypto adapter stored on the hard drive and you want them migrated, manually copy the files to the TKE Backup diskette.

Note: Authority signature keys, Master key parts, and Operational key parts cannot be migrated with this task.

Note: The floppy drive must be deactivated to successfully execute this task. Check TKE Media Manager to ensure the floppy drive is deactivated.

To invoke this task, click on Trusted Key Entry and then click on Migrate Previous TKE Version TKE 5.2.

You will be requested to insert the TKE Backup diskette from the workstation you are migrating from. Click OK.

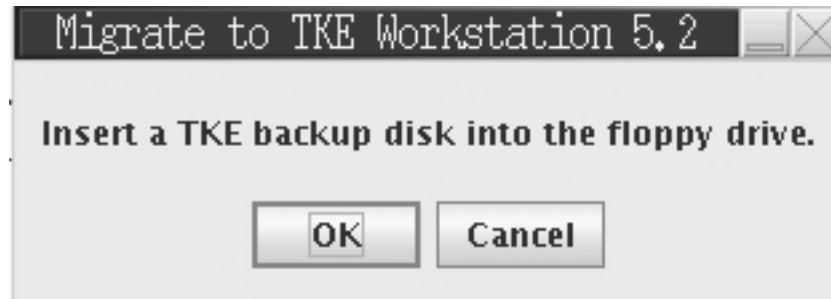


Figure 401. Migrate to TKE Workstation 5.2 - Backup floppy prompt

Files migrated will be displayed in the Migrate to TKE Workstation 5.2 window.

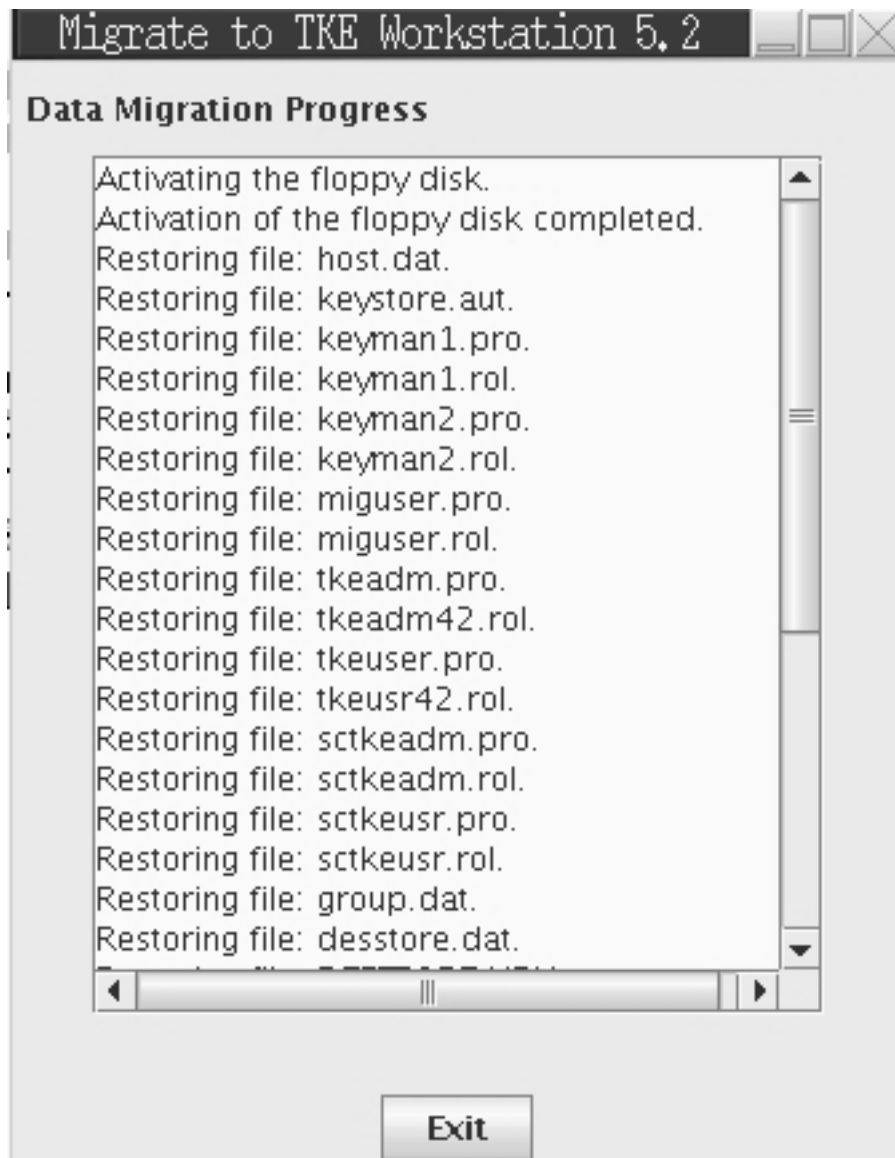


Figure 402. Migrate to TKE Workstation 5.2 - Data migration progress window

The task is complete when the 'Exit' button is no longer greyed out.

TKE File Management Utility

The TKE File Management Utility task allows you to manage files on diskette, CD/DVD, or within the Supported Data directories. It provides the ability to Delete, Rename, and Copy files.

To invoke this task, click on Trusted Key Entry and then click on TKE File Management Utility.

When the TKE File Management Utility is opened the user is presented with this task window.

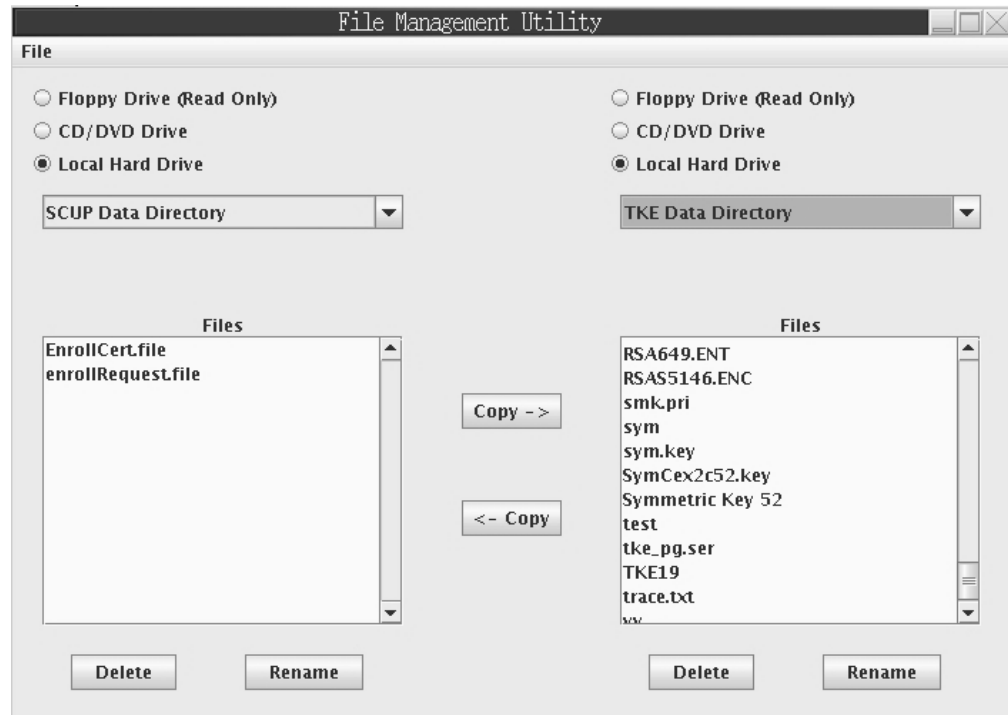


Figure 403. TKE File Management Utility Task Window

Selecting the hard drive for either Source or Target will allow the user to select from one of four data directories:

- TKE Data Directory
- Migration Backup Data Directory
- CNM Data Directory
- SCUP Data Directory

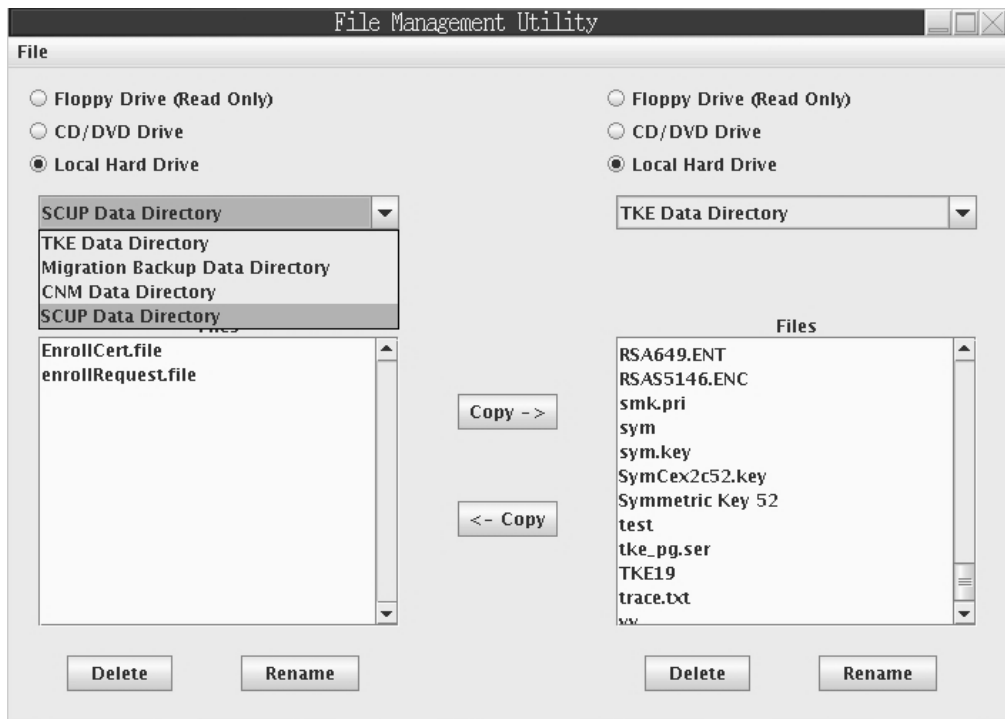


Figure 404. TKE File Management - Directory options

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 it.
- 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'.

Selecting 'Delete' will present a confirmation window.



Figure 405. Delete Confirmation Window

Rename will present a window for inputting a filename.

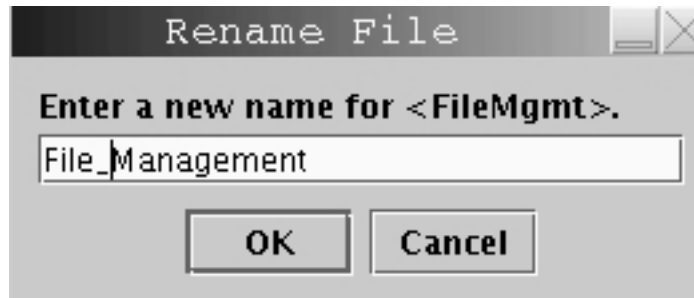


Figure 406. Window for Inputting a Filename

Completion of Delete, Rename, or Copy will present a window similar to this:

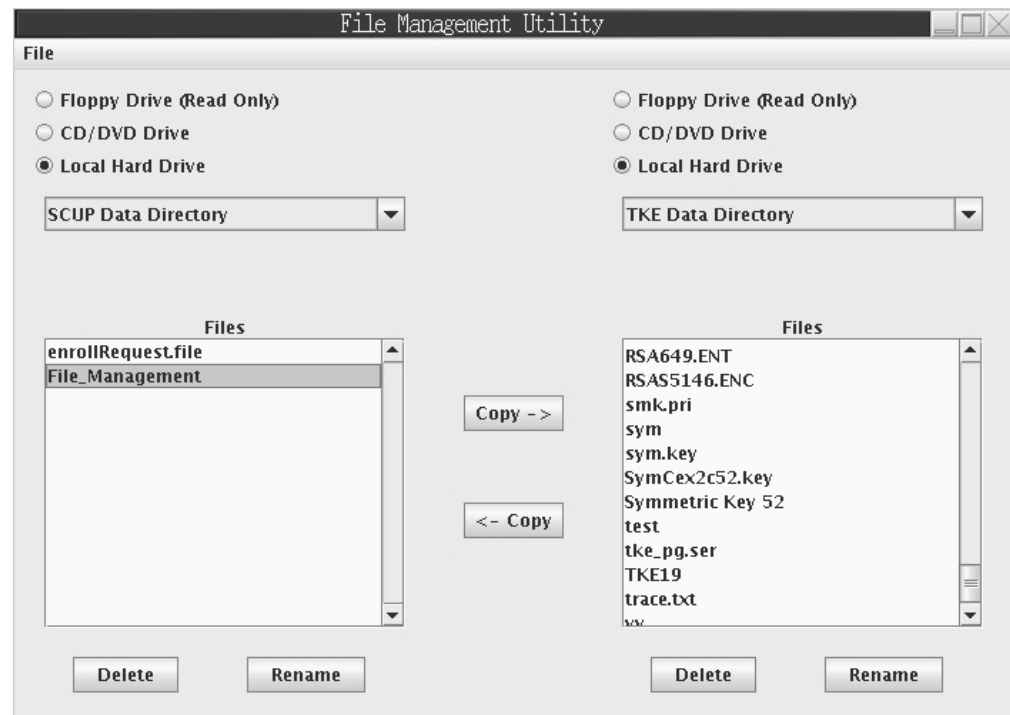


Figure 407. Completion Window

Warning: If updates are done to the floppy drive or DVD-RAM, the media must be deactivated before it is removed. Otherwise the updates may be lost.

TKE Workstation Code Information

This task window shows information concerning the code used by the TKE applications. This information can be useful in problem determination. Updates to TKE Application code will be reflected within this window. This task does not give information regarding the code on crypto card.

To invoke this task, click on Trusted Key Entry and then click on TKE Workstation Code Information.

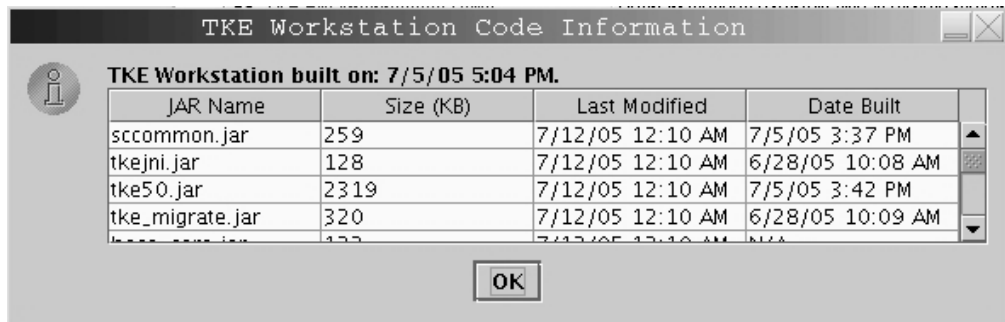


Figure 408. TKE Workstation Code Information window

Appendix L. Service Management - Applications

Analyze Console Internal Code

Note: This task will only be displayed when logged on as the SERVICE id.

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.

For details, refer to *Maintenance Information for Desktop Consoles*, GC28-6847.

Authorize Internal Code Changes

Note: This task will only be displayed when logged on as the SERVICE id.

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.

For details, refer to *Maintenance Information for Desktop Consoles*, GC28-6847.

Change Console Internal Code

Note: This task will only be displayed when logged on as the SERVICE id.

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.

For details, refer to *Maintenance Information for Desktop Consoles*, GC28-6847.

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.

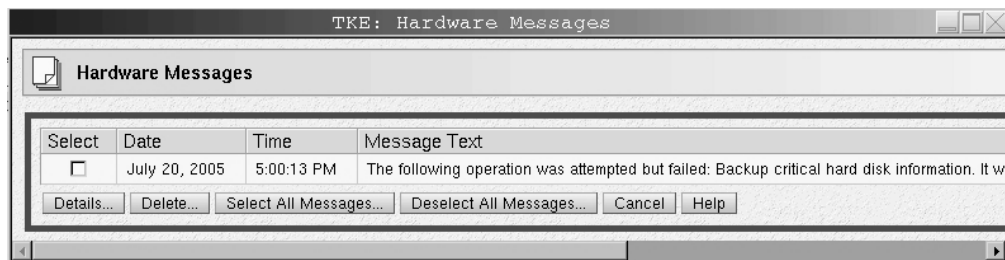


Figure 409. Hardware Messages window

Hardware messages notify you of events that involve or affect the TKE workstation hardware or internal code.

To promptly view, act on, and delete messages:

1. Select a message, then click Details to display details.

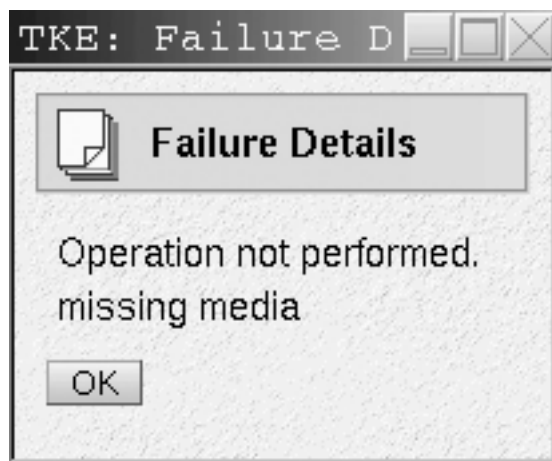


Figure 410. Hardware Messages - Details Window

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 of displaying new messages as they are received.

Rebuild Vital Product Data

Note: This task will only be displayed when logged on as the SERVICE id.

This task is used to rebuild the Vital Product Data for the TKE machine.

Transmit Console Service Data

Note: This task will only be displayed when logged on as the SERVICE id.

This task is used to select the types of service data and the method to send the data to aid in the problem determination.

To invoke this task, click on Service Management and then click on Transmit Console Service Data.

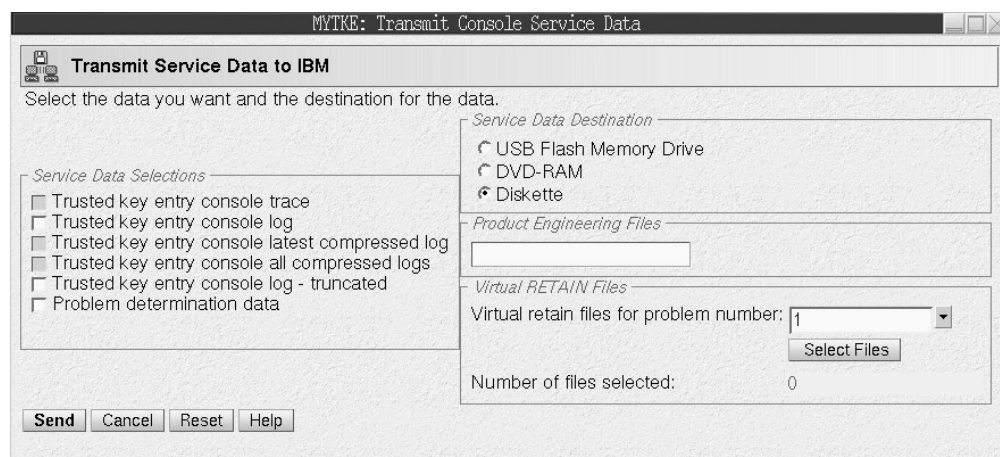


Figure 411. Transmit Console Service Data - prompt for DVD

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 this window only when directed by your service representative or IBM Support Center. Select the service data categories requested by IBM. Service data in selected categories is collected in a file or group of files for transmission to IBM.

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 IBM.

Service Data Destination

Use this topic to specify how your service data is sent to IBM.

Virtual RETAIN Files

Use this topic to copy to diskette or DVD-RAM selected virtual RETAIN files for the specified problem number.

Note: You can select and copy virtual RETAIN files to diskette or DVD-RAM for only a single problem number at a time.

Note: When using a DVD-RAM for service data it must first be formatted specifically for Service Data. See “Format Media” on page 373 for details.

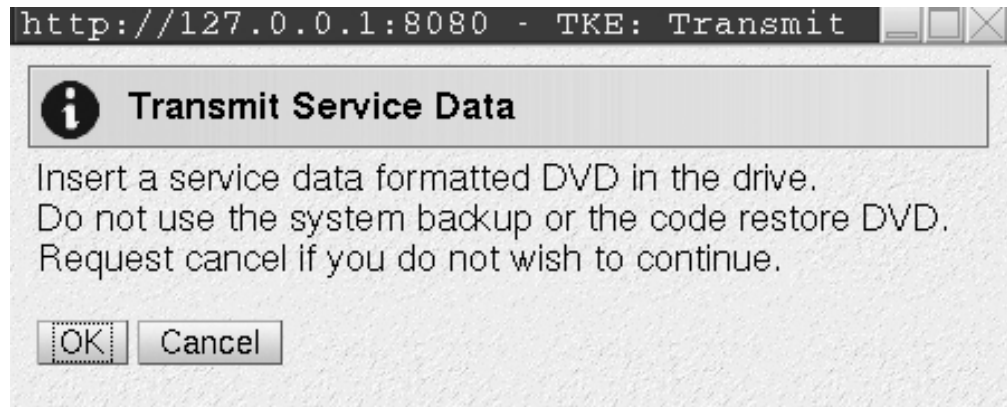


Figure 412. Transmit Console Service Data Task Window for DVD-RAM

If Diskette was chosen for the Service Data Destination, this will be displayed:



Figure 413. Transmit Console Service Data - Task Window for Diskette

Successful completion will present this window.



Figure 414. 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.

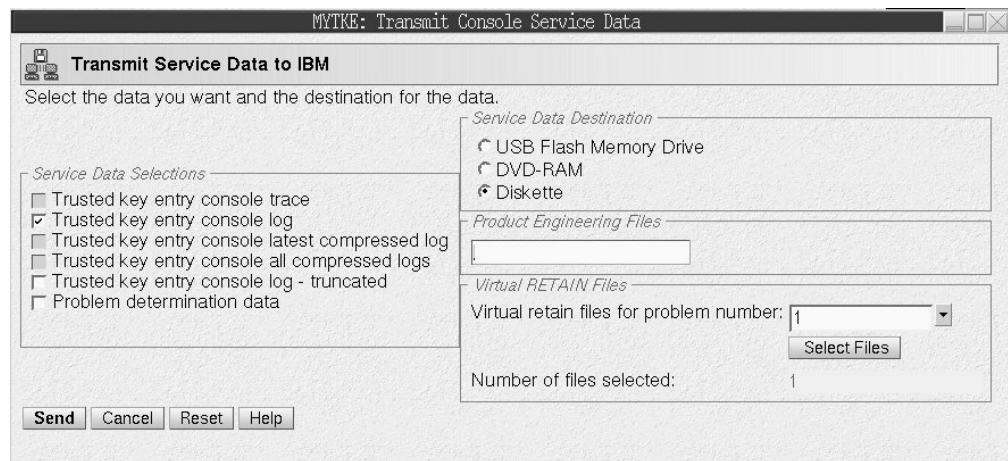


Figure 415. Update Problem Number for Virtual RETAIN File

Select the applicable Virtual RETAIN Files and click OK.

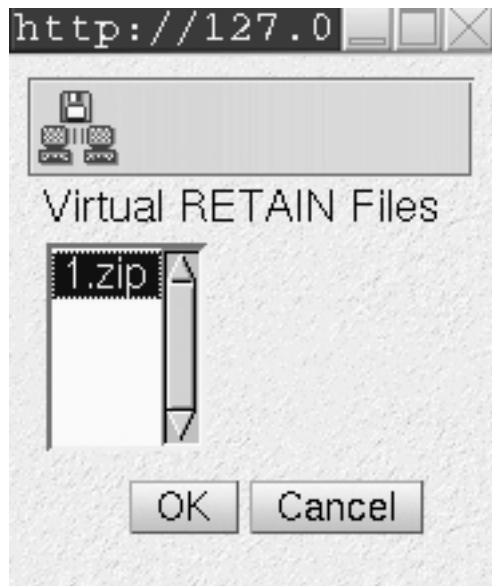


Figure 416. Select the Virtual RETAIN Files

Select the Service Data Destination, Diskette or DVD-RAM on the Transmit Service Data to IBM window.

Click on Send to transmit the selected Virtual RETAIN files to Media.

Insert the selected media when prompted.

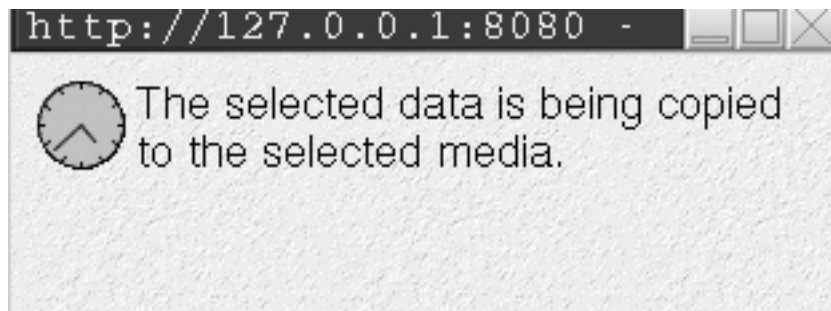


Figure 417. Copying Data to Selected Media

Successful completion will present the window displayed in Figure 414 on page 349.

Appendix M. Service Management - Configuration

Customize Scheduled Operations

Use this task to customize a schedule for backing up critical hard disk information to DVD.

It is very important to backup critical console data on a regular basis so the latest system changes and updates are available for recovery situations.

Note: The DVD used for the Backup Critical hard disk information must be formatted as ACTBKP. See Format Media for details.

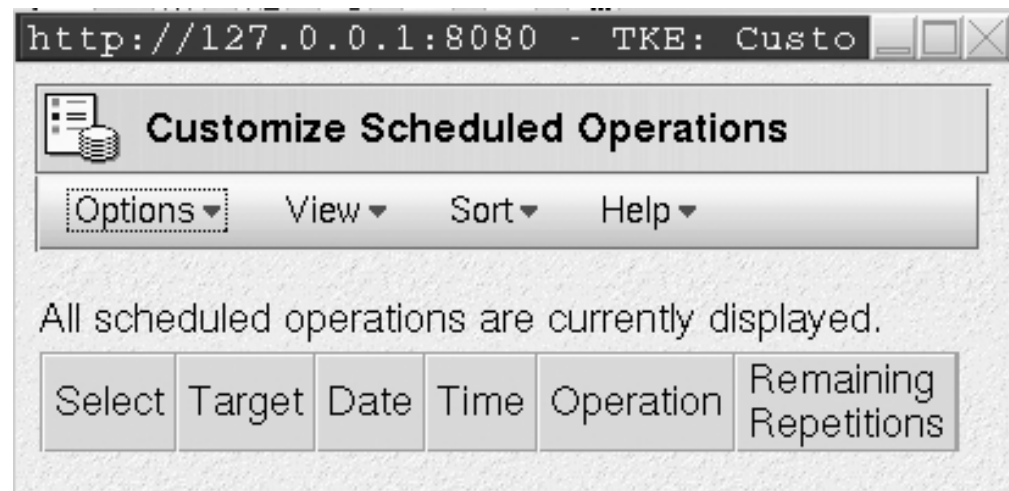


Figure 418. Customize Scheduled Operations Task Window

The Backup DVD is intended for use only during a hard disk restore operation which completely replaces the contents of the hard 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 DVD.

Included on the Backup DVD are any Microcode Fixes (MCFs) and Microcode Loads (MCLs) that have been applied to the system. Also included is TKE related data. After the restore/reload the system is back to the Service 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 to perform the operation. A schedule can be set for one operation or repeated many times.

To open this task, click on Service Management and then click on Customize Scheduled Operations.

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 currently displayed

Deselect All

to deselect 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 screen is displayed.

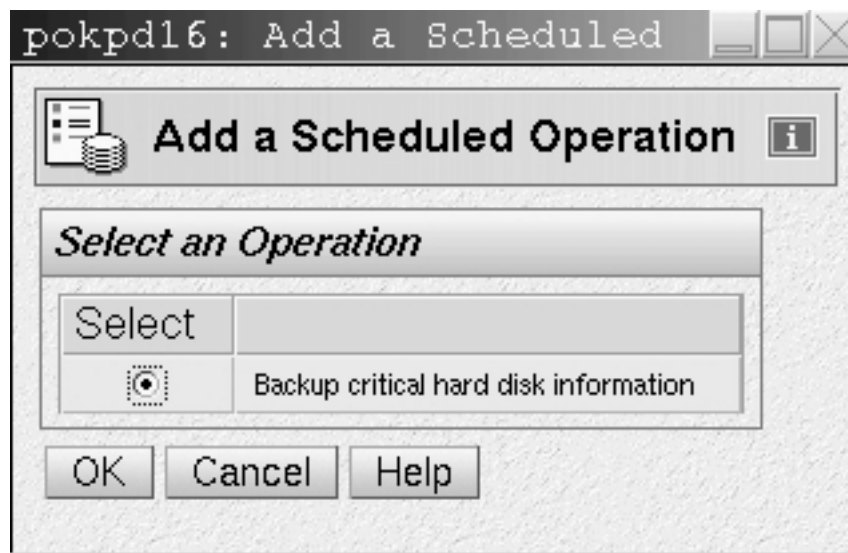


Figure 419. Customize Scheduled Operations - Add a Scheduled Operation window

Clicking on the 'OK' button will present this screen where the Time, Date, and Repetition of the operation can be specified.

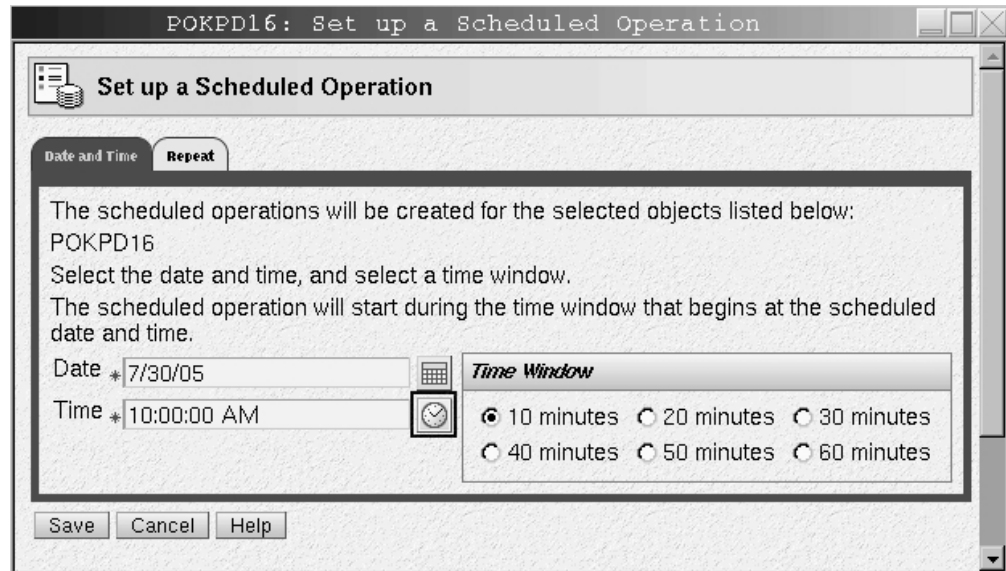


Figure 420. Customize Scheduled Operations - Set Date and Time window

Enter the date and time for a scheduled operation on the Date and Time window. The time window defines the time frame in which the scheduled operation must start.

After you have entered the Date, Time, and selected the Time Window, click on the Repeat tab.

Select whether the operation is a single occurrence or will be repeated. Select the Days of the Week, you want to perform the operation. The Interval is the number of weeks to elapse before the scheduled operation is executed again. Repetitions is the number of times you want the scheduled operations performed.

POKPD16: Set up a Scheduled Operation

Set up a Scheduled Operation

Date and Time Repeat

The scheduled operations will be created for the selected objects listed below:
POKPD16

Single or Repeated

☐ Set up a single scheduled operation
☒ Set up a repeated scheduled operation

Days of the Week

☐ Monday ☐ Friday
☐ Tuesday ☒ Saturday
☐ Wednesday ☐ Sunday
☐ Thursday

Options

Interval: 1 [up/down] 1 to 26 weeks

Repetitions: 1 [up/down] 1 to 100

☒ Infinite repetitions

Save Cancel Help

Figure 421. Customize Scheduled Operations - Set Repetition of operation

After all the information is selected, press the Save button to complete the scheduling of the operation.

pokpd16: Customize Scheduled Operations - Mozilla

Customize Scheduled Operations

Options ▾ View ▾ Sort ▾ Help ▾

All scheduled operations are currently displayed.

Select	Target	Date	Time	Operation	Remaining Repetitions
☐	pokpd16	Jun 22, 2005	9:42:47 AM	Backup critical hard disk information	1

Figure 422. Completion Window for Adding Scheduled Operation

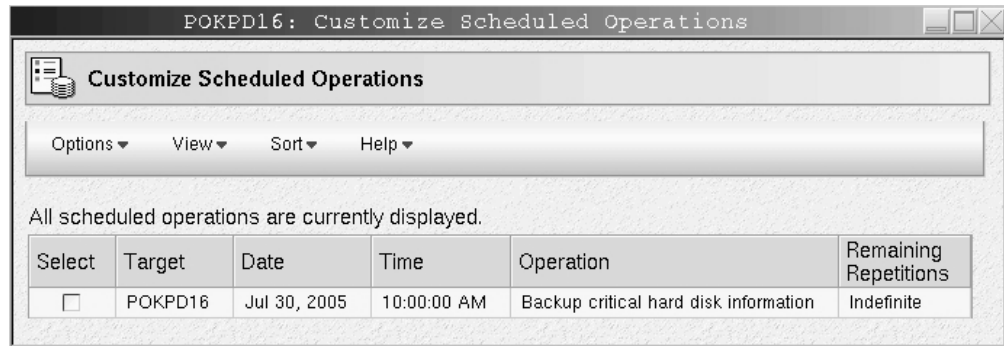


Figure 423. Customize Schedule Operations

Click Sort on the menu bar to sort how you want to view the list of scheduled operations; By Date and Time, By Object, or By Operation. Date and time will sort the list according to date in descending order with the most recent operation at the top. By Object and By Operation 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

to display schedule information for the selected scheduled operation. For TKE, Object and Operation are not relevant.

New Time Range

to specify a definite time range (days, weeks, months, or displayed scheduled operations) for the selected operation.

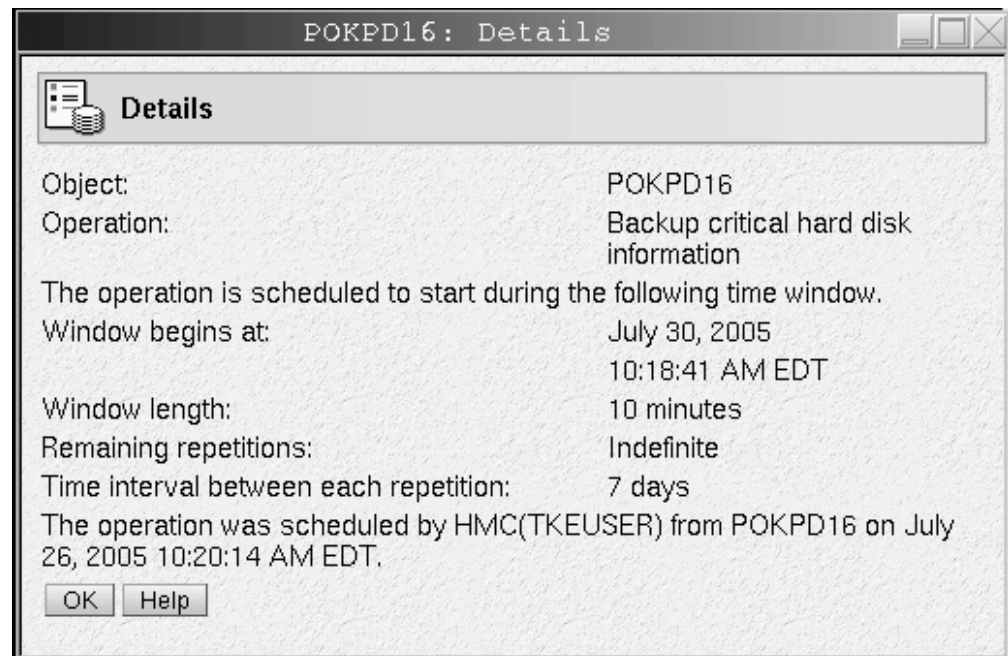


Figure 424. Details View of Scheduled Operation

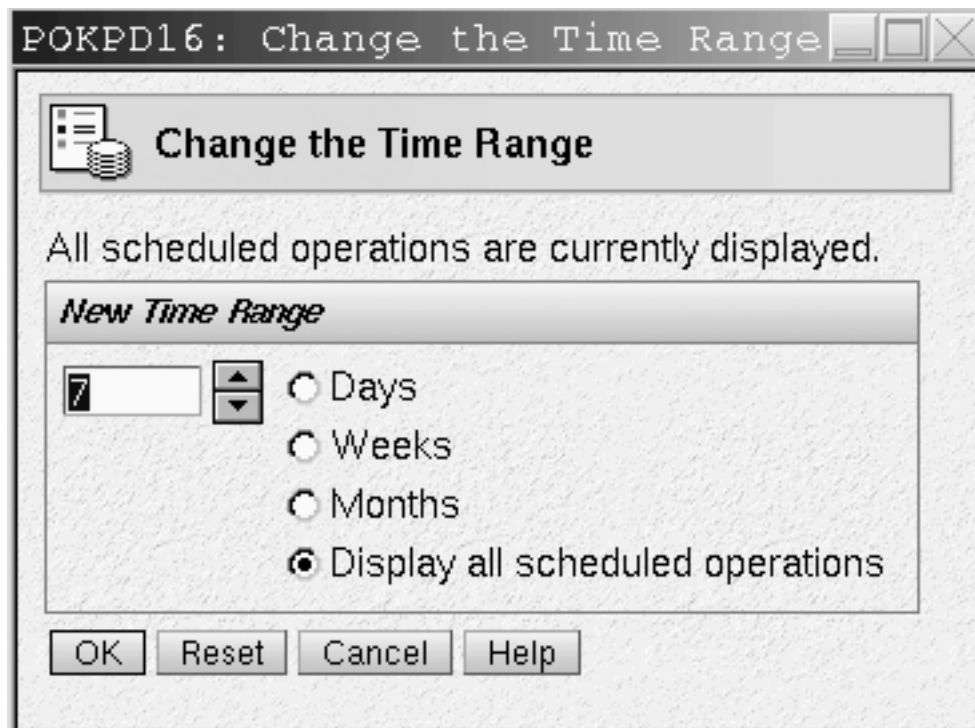


Figure 425. New Time Range window for Scheduled Operation

Appendix N. Service Management - Maintenance

Backup Critical Console Data

This task performs the same function as the Customize Scheduled Operations for Backup Critical Hard Disk Information. Rather than executing it as a scheduled operation, this task will execute the Backup immediately. The backup critical data operation copies critical files from the Trusted Key Entry workstation to the Backup DVD-RAM.

To invoke this task, click on Service Management and then click on Backup Critical Console Data.

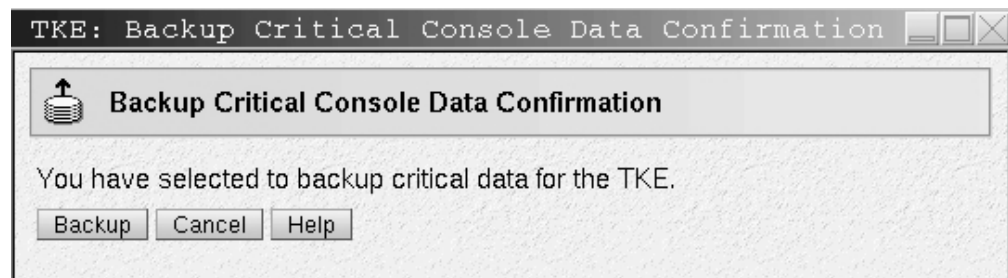


Figure 426. Backup Critical Console Data Window

The DVD-RAM for the Backup Critical Console Data task must be formatted with a volume identification of ACTBKP, using the Format Media task.

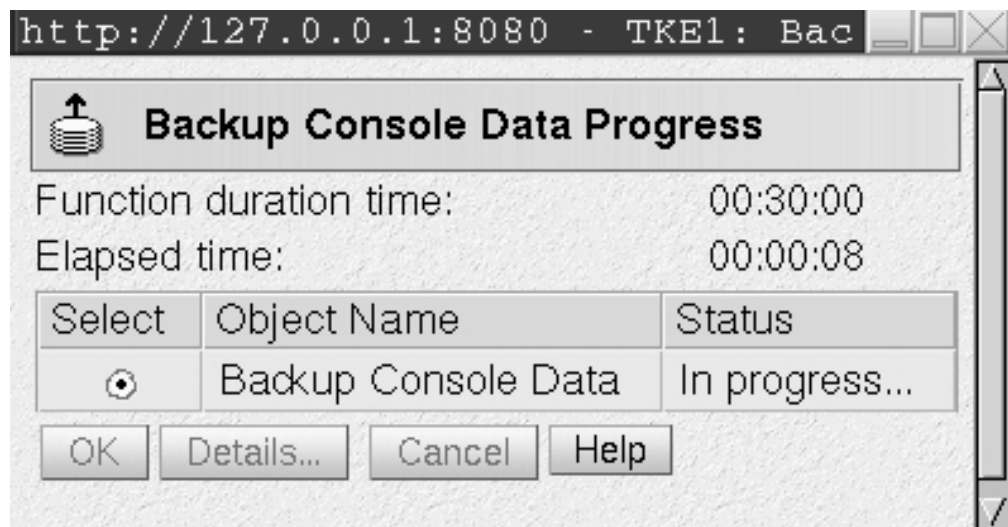


Figure 427. Backup Console Data Progress window - in progress

When the operation is complete the Status will be updated to indicate Success.

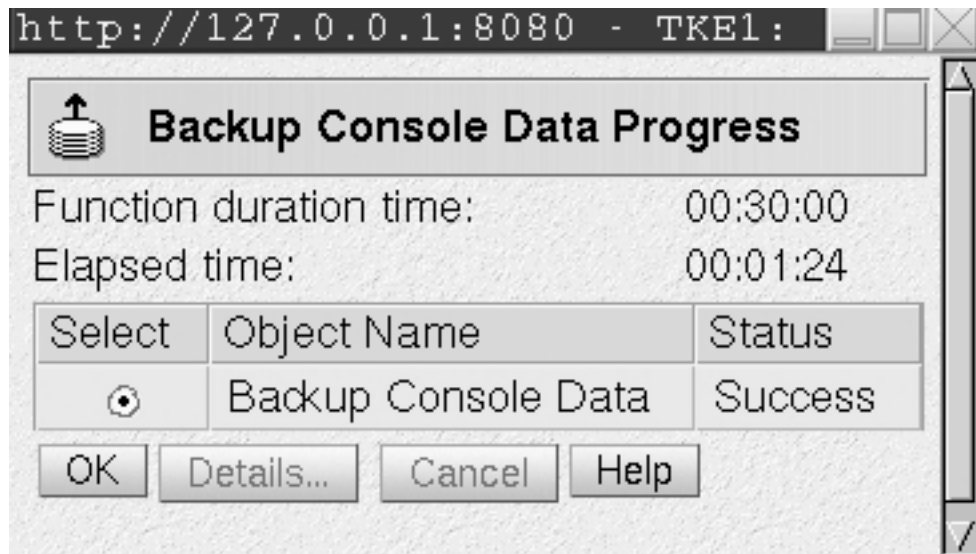


Figure 428. Backup Console Data Progress window - Success

Lock console configuration

This task is used to allow customers to lock the TKE console.

To invoke this task, click on Service Management and then click on Lock Console.

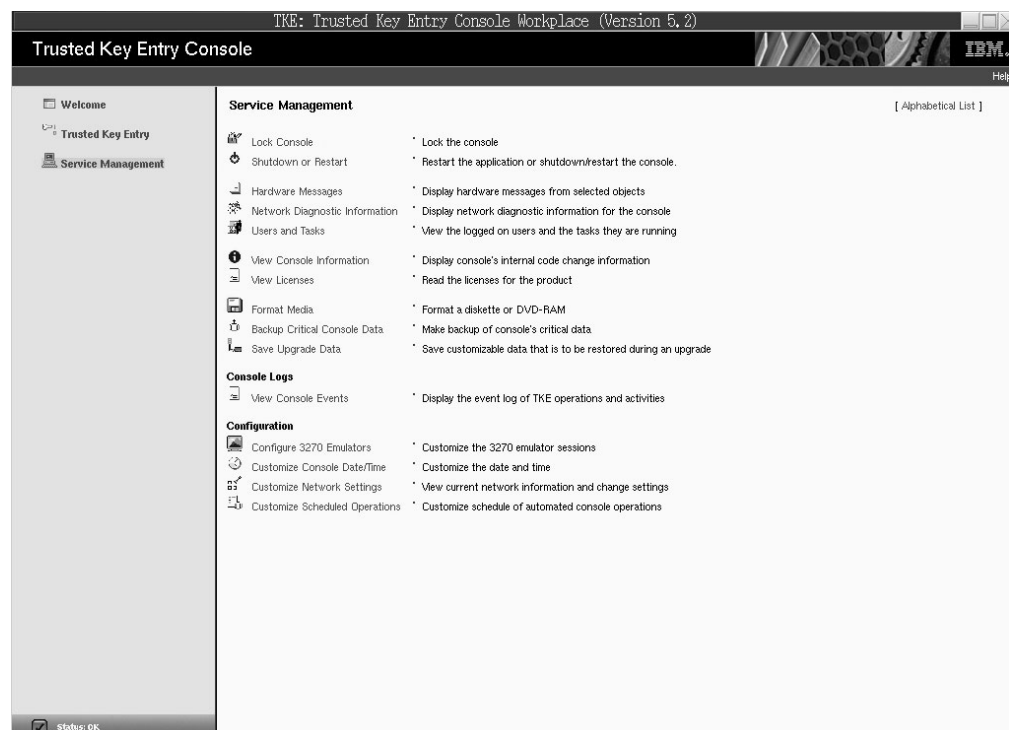


Figure 429. Service Management for the TKEUSER user (Categorized)

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.

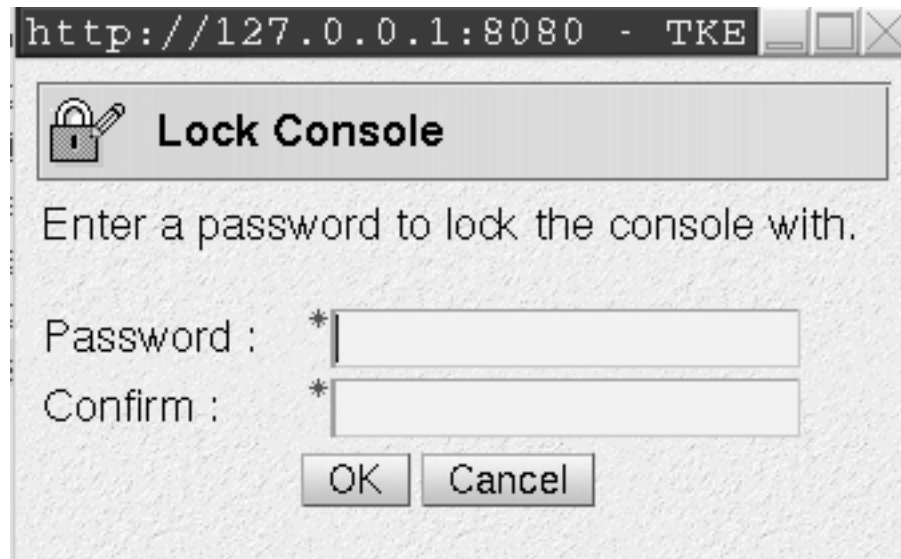


Figure 430. Prompt for Password

The user must enter a password and confirm it. If either field is not entered this error is displayed:



Figure 431. Error if no Password is Entered

If the password value entered does not match the value in the confirmation box this error is displayed:

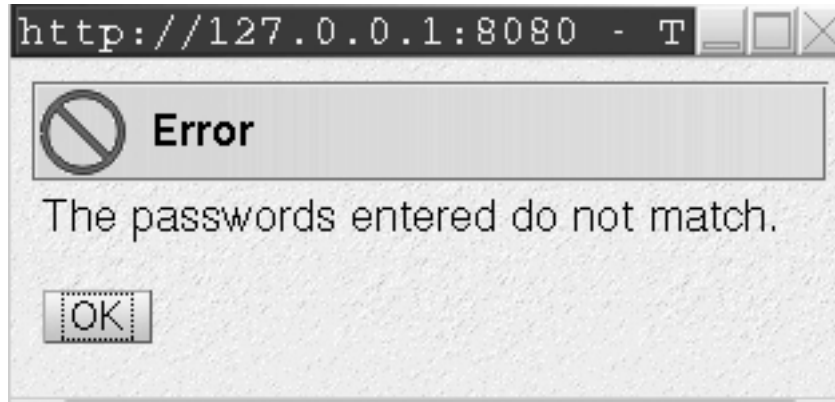


Figure 432. Error if Password Entered Does not match Confirmation

Once you've entered a password value, confirmed it, and selected the OK button, 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.

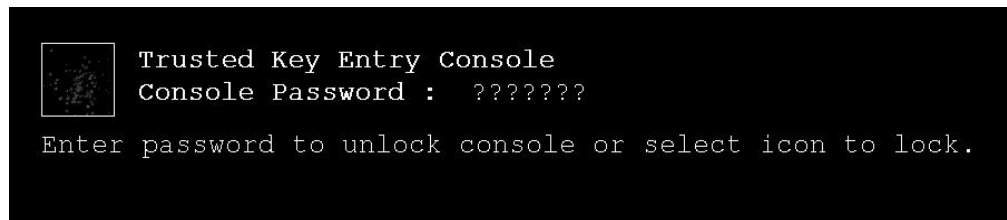


Figure 433. Prompt to Unlock Console

Each keystroke appears as a question mark on the password prompt. If the correct password is entered, the user returns back to the TKE console. If an incorrect password is entered, an error message will be displayed informing the user.

Offload Virtual RETAIN Data to DVD-RAM

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 DVD-RAM.

To invoke this task, click on Service Management and then click on Offload Virtual RETAIN Data to DVD-RAM.

Note: The DVD-RAM must be formatted with volume identification label VIRTRET, using the Format Media task.

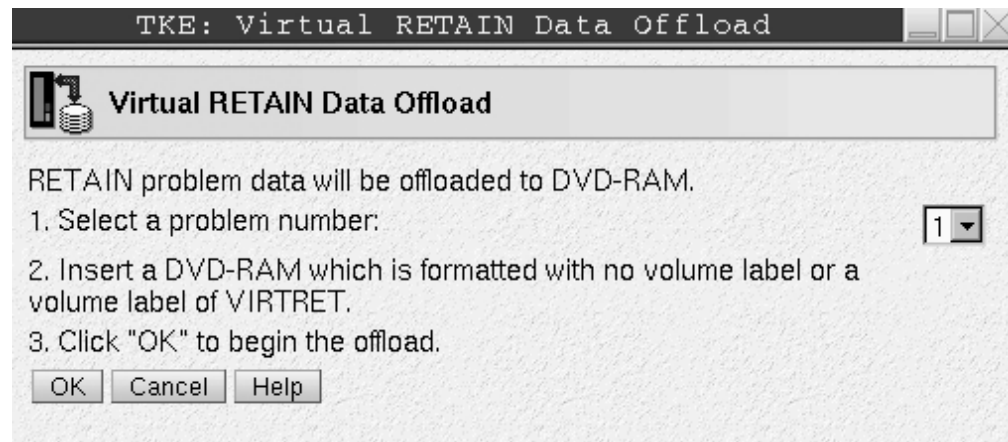


Figure 434. Virtual RETAIN Data Offload Window

After selecting the Problem Number click on OK. The selected virtual RETAIN data is off-loaded to the DVD-RAM.

When the virtual RETAIN data is offloaded successfully, this is displayed.



Figure 435. Successful Offload of Data

If you insert a DVD-RAM that has not been formatted or has the wrong label, these errors will be displayed, respectively.

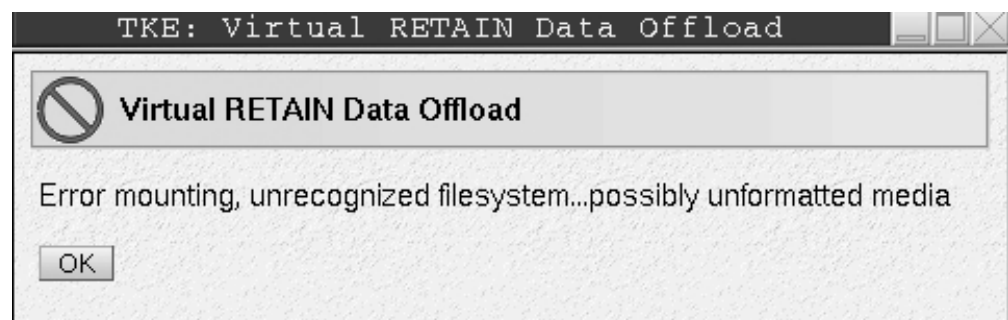


Figure 436. Virtual RETAIN Data Offload Unformatted Media Error

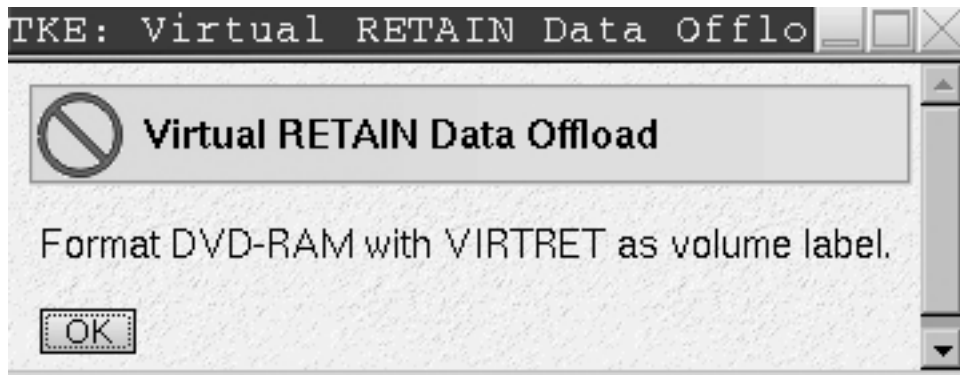


Figure 437. Virtual RETAIN Data Offload Wrong Label Error

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.

All data pertinent to the TKE workstation (ie. TKE related data directories, emulator sessions, TCP/IP information, etc.) 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.

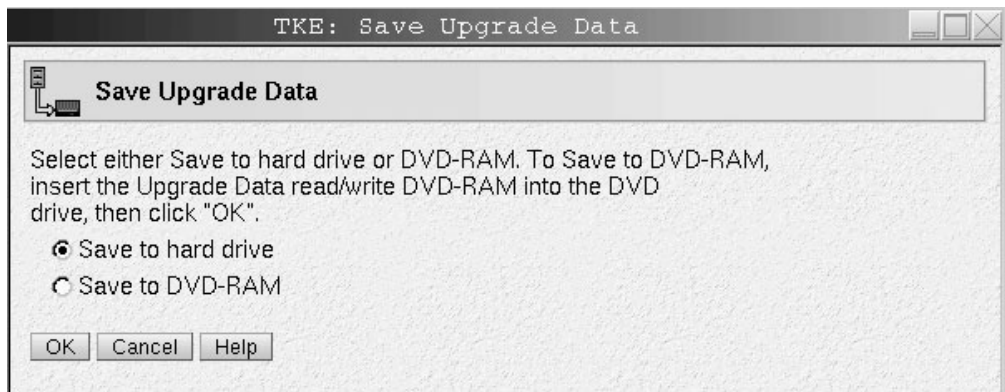


Figure 438. Save Upgrade Window

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 DVD-RAM for this task must be formatted with a volume identification label of ACTUPG, using the Format Media task.

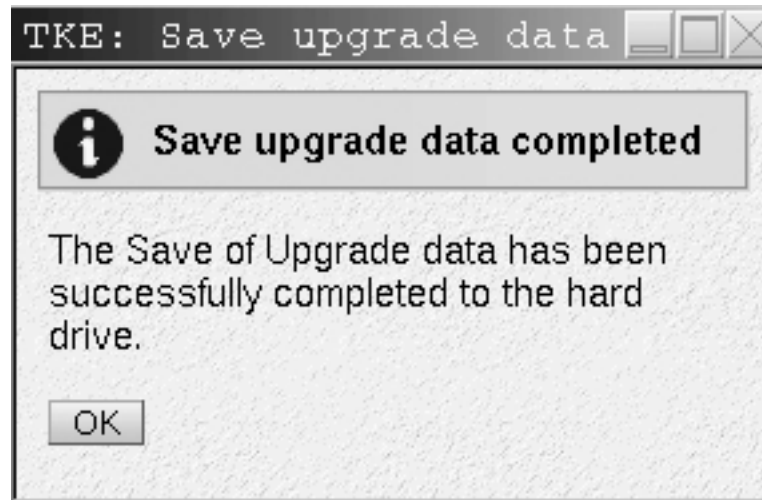


Figure 439. Save Upgrade Success Window

Note: While the Save to DVD-RAM option is available for Save Upgrade Data, it should not be used. The restore of Upgrade Data from a DVD-RAM is currently not supported.

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.

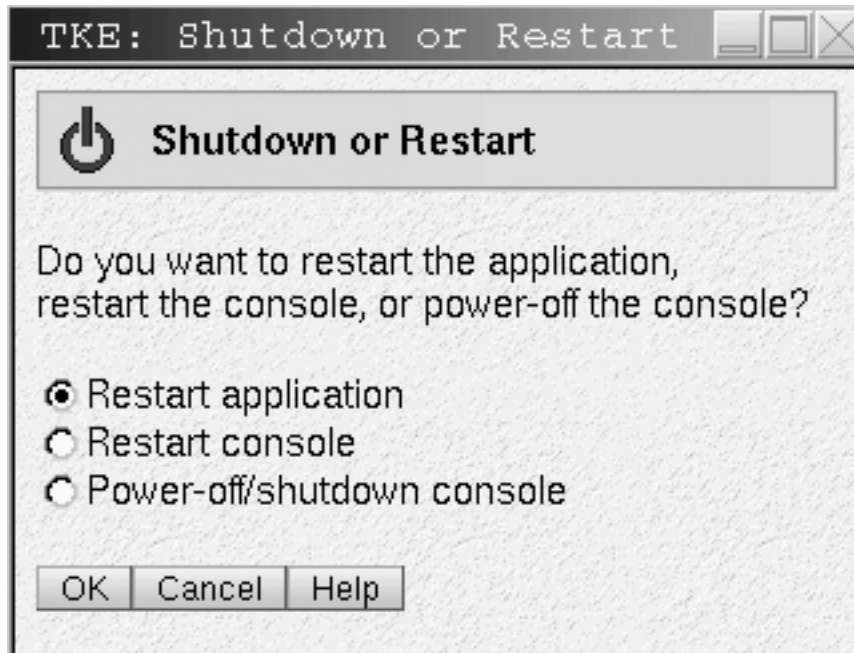


Figure 440. Shutdown or Restart Task Window

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/Shutdown Console

To close the Trusted Key Entry workstation, shut down the operating system, and power-off the hardware, select Power-off/shutdown console.

Selecting any option will present you with a confirmation window similar to Figure 441.

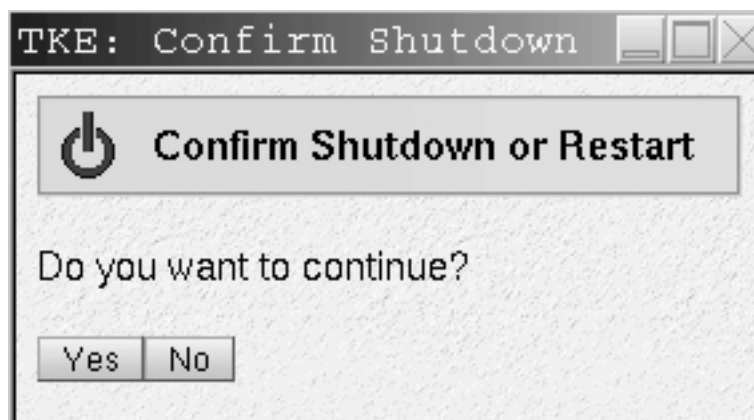


Figure 441. Confirmation Window

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 won't 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 3.10SC task. If you attempt to terminate CLU from this task you will be presented with a window stating 'You can not 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.'

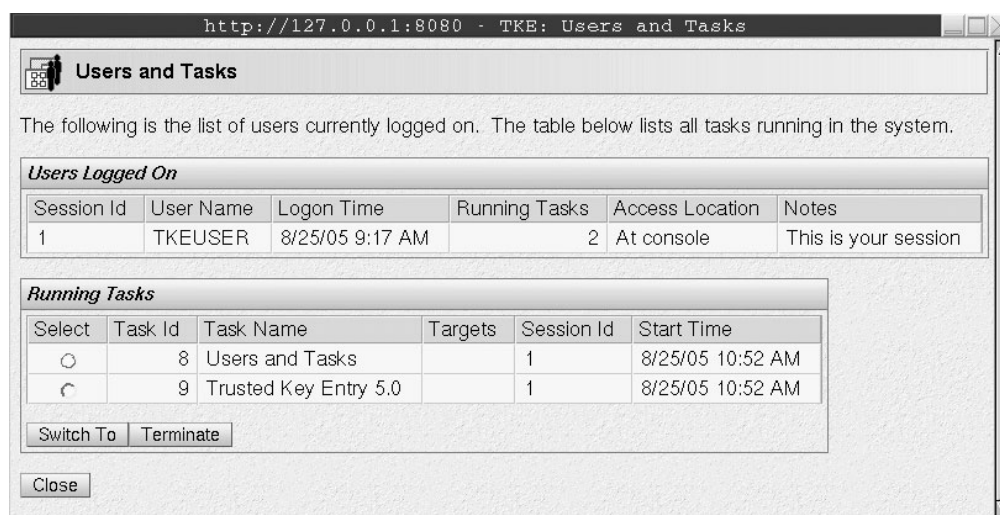


Figure 442. Login Details Window

View Console Events

This task displays console events logged by the Trusted Key Entry.

To invoke this task, click on Service Management and then click View Console Events.

Date	Time	Console Event
05/06/2005	15:54:56.230	Upgrade data was saved.
05/06/2005	15:41:43.150	Backup critical data ended.
05/06/2005	15:13:10.790	Backup critical data started.
05/06/2005	11:57:36.660	Backup critical data ended.
05/06/2005	11:34:16.020	Backup critical data started.
05/06/2005	00:01:00.410	Root password on LINUX updated.
05/05/2005	14:31:52.750	An Authorize Internal Code Changes request of Enable for HMC TKE ZZZZZZZZ and all its defined objects
05/05/2005	13:16:46.780	User TKEUSER was logged on automatically.
05/05/2005	13:16:46.510	User TKEUSER has logged on in TKEUSER mode.
05/05/2005	13:16:36.100	The Hardware Management Console Application (HWMCA) was initialized.
05/05/2005	13:16:36.080	Root password on LINUX updated.
05/05/2005	13:16:35.390	A user password was changed.
05/04/2005	17:02:57.940	User TKEUSER with sessionid util.hmcsession.1 has requested to Power-off the Console.
05/04/2005	11:12:46.790	User TKEUSER was logged on automatically.
05/04/2005	11:12:46.520	User TKEUSER has logged on in TKEUSER mode.
05/04/2005	11:12:36.290	Root password on LINUX updated.
05/04/2005	11:12:35.970	The Hardware Management Console Application (HWMCA) was initialized.
05/04/2005	11:12:35.360	A user password was changed.
05/03/2005	17:23:15.110	User TKEUSER with sessionid util.hmcsession.1 has requested to Power-off the Console.
05/03/2005	17:19:26.500	User TKEUSER was logged on automatically.

Page 1 of 11 1 Go Total: 205 Displayed: 20

Figure 443. 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 initially displays all console events currently logged and lists them in reverse order of occurrence (from the most recent event to the oldest event). The options under View on the menu bar allow you to change the number of events listed or to change the order the events are listed, select your preference:

- To change how many events are listed change list's time range, by selecting Using a different time range
- To list events from the oldest event to the most recent, select In order of occurrence
- To list events from the most recent event to the oldest event, select In reverse order of occurrence
- To close the window, select Exit.

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 in problem determination.

To invoke this task, click on Service Management and then click on View Console Information.

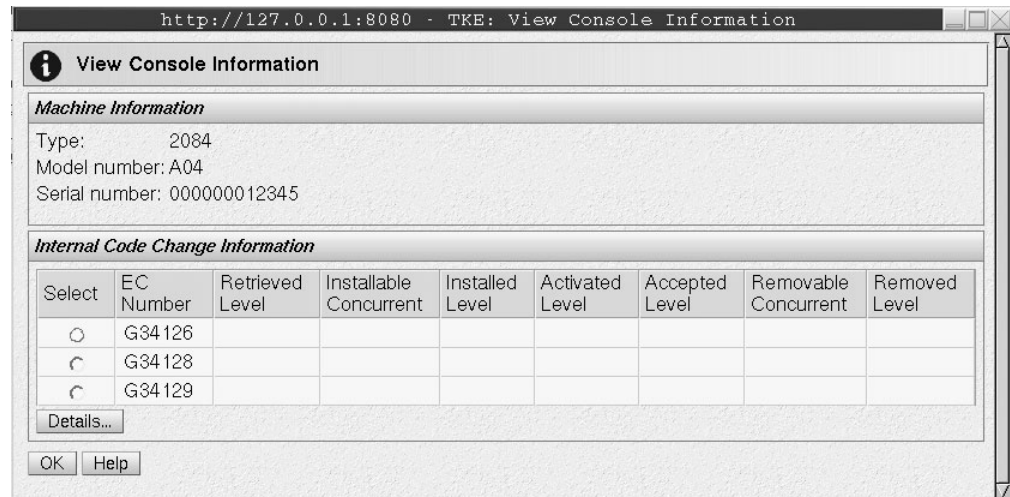


Figure 444. View Console Information Window

For additional information about an internal code change, select an EC number, then click Details.

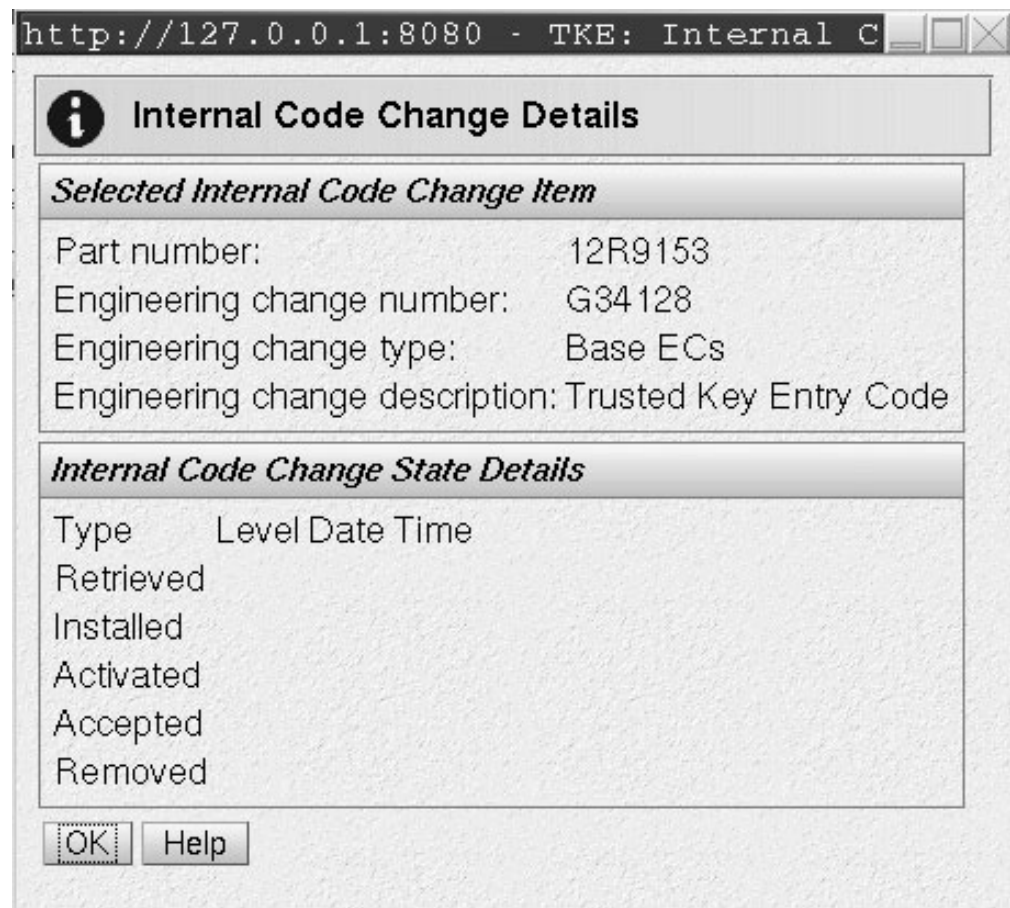


Figure 445. Internal Code Change Details Window

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.

Installed Level

Displays the internal code change level that was most recently prepared for activation as a working part of the licensed internal code of the 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 the console, from the current installed level down to and including the removable concurrent level, and then activate the change level that remains installed without disrupting the operations of this console.

Removed Level

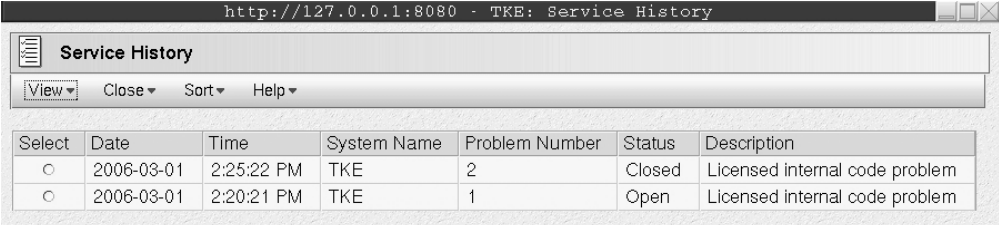
Displays the internal code change level that will remain installed and become activated when the console is activated again, while the installation of all more recent change levels is undone.

View Console Service History

Note: This task will only be displayed when logged on as the SERVICE id.

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.



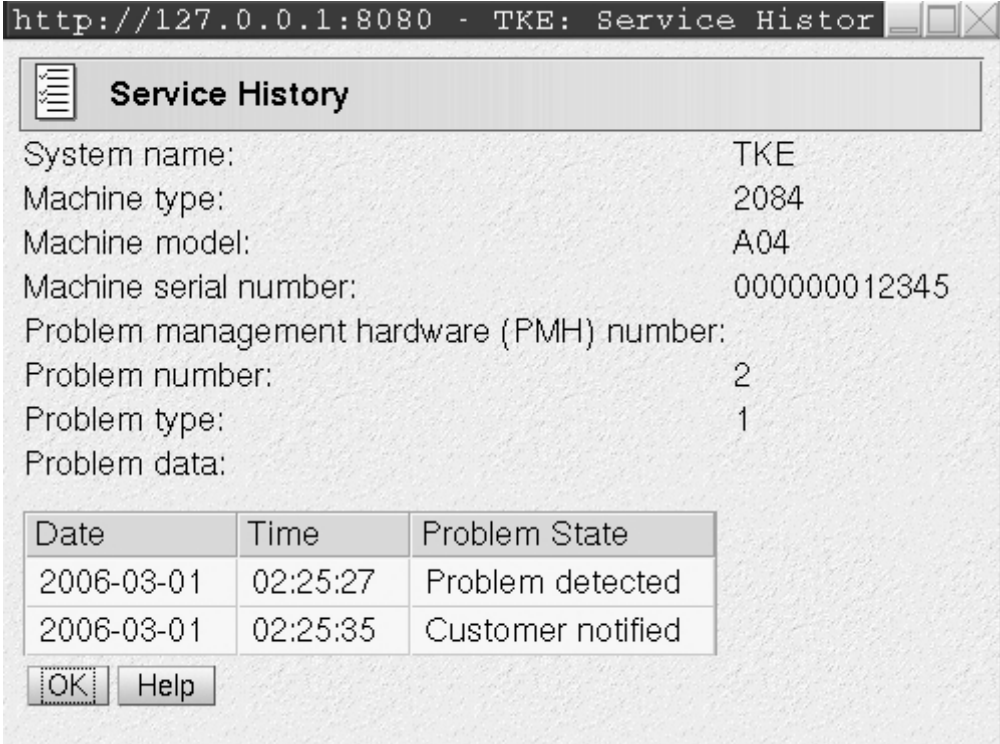
Select	Date	Time	System Name	Problem Number	Status	Description
☐	2006-03-01	2:25:22 PM	TKE	2	Closed	Licensed internal code problem
☐	2006-03-01	2:20:21 PM	TKE	1	Open	Licensed internal code problem

Figure 446. 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.



The screenshot shows a web browser window titled "http://127.0.0.1:8080 - TKE: Service Histor". Inside the browser is a "Service History" panel. The panel contains the following text:

System name: TKE
Machine type: 2084
Machine model: A04
Machine serial number: 000000012345
Problem management hardware (PMH) number:
Problem number: 2
Problem type: 1
Problem data:

Date	Time	Problem State
2006-03-01	02:25:27	Problem detected
2006-03-01	02:25:35	Customer notified

At the bottom of the panel are two buttons: "OK" and "Help".

Figure 447. Problem Summary

- Problem Analysis Panel shows System Name, Date and Time, Problem Description, Corrective Actions that a user can take and impact of repair.

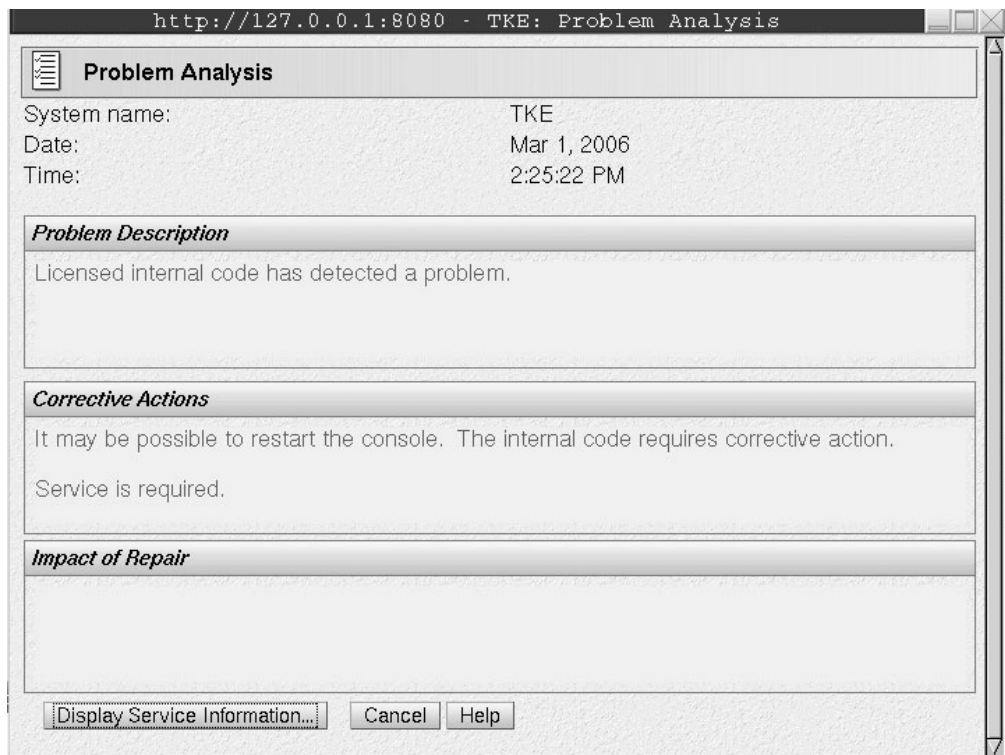


Figure 448. Problem Analysis

If you click Display Service Information you will see this window.

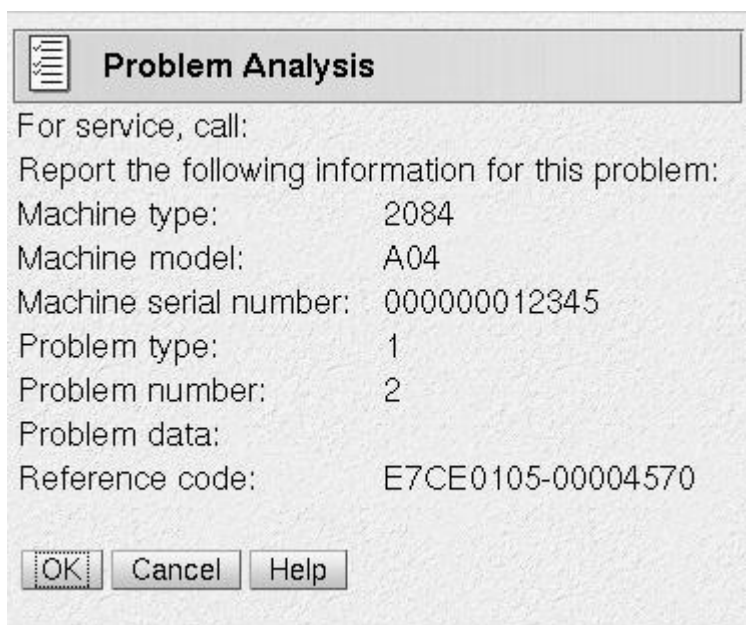


Figure 449. Display Service

- Cancel exits this task and returns to the Trusted Key Entry Console.

Click Close on the menu bar and then select this:

- Selected Problem changes the status of a problem from Open to Closed

- All Problem changes the status of all open problems to closed.

View Console Tasks Performed

Note: This task will only be displayed when logged on as the SERVICE id.

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.

You must scroll the display to the right until you see the inner right hand scroll bar for moving the display up and down.

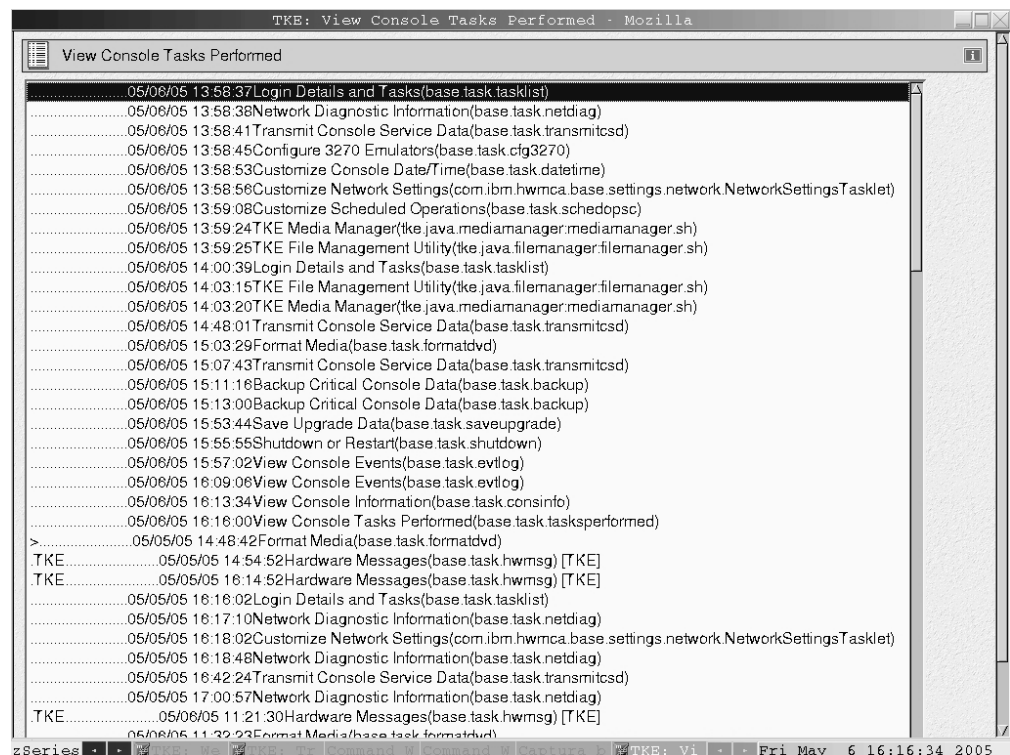


Figure 450. View Console Tasks Performed window

View Licenses

This task is used to view the open source licenses for the Trusted Key Entry Console.

Licenses that can be viewed include:

- Embedded Operating System Readme File
- Eclipse Help System Readme File
- Adobe Reader License

- Mozilla Firefox Browser License
- Opera Browser License
- International License Agreement for Non-Warranted Programs
- Additional License Information

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 thru this task, the first TKE related task that you invoke will display the license information. This will only be done once.

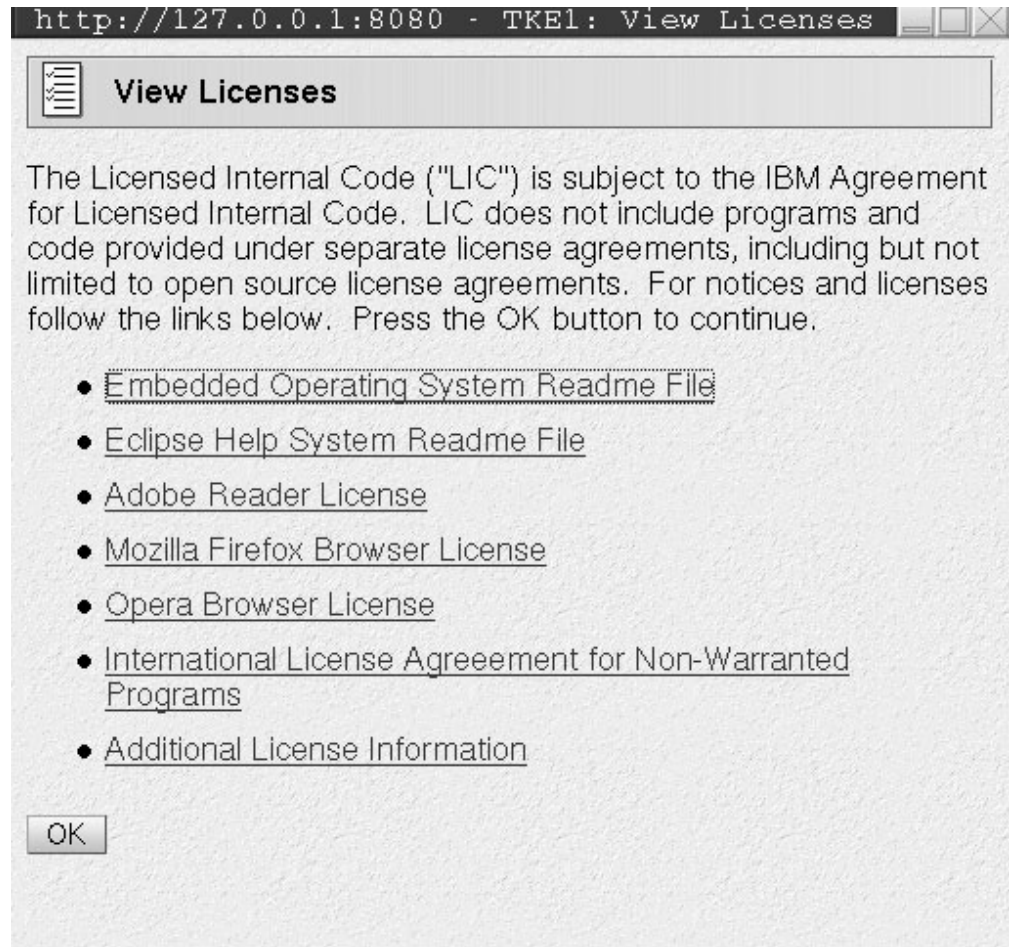


Figure 451. View Licenses window

Appendix O. Media Devices

Format Media

Warning: Prior to formatting any media, ensure that the applicable Floppy or DVD-RAM drive is deactivated in the TKE Media Manager. If the media is not deactivated, the format will fail.

To invoke this task, click on System Management, Maintenance, and then click on Format Media.

Note: Format Media is also available under System Management, Service Applications.

The Format Media task is used to format DVD-RAMs and diskettes only.

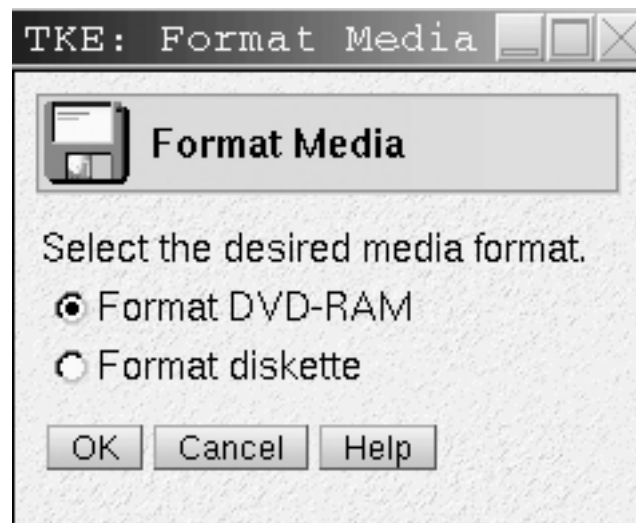


Figure 452. Format Media Task Window

Depending on what the DVD-RAM will be used for will determine how the DVD-RAM is formatted and what label is written on it.

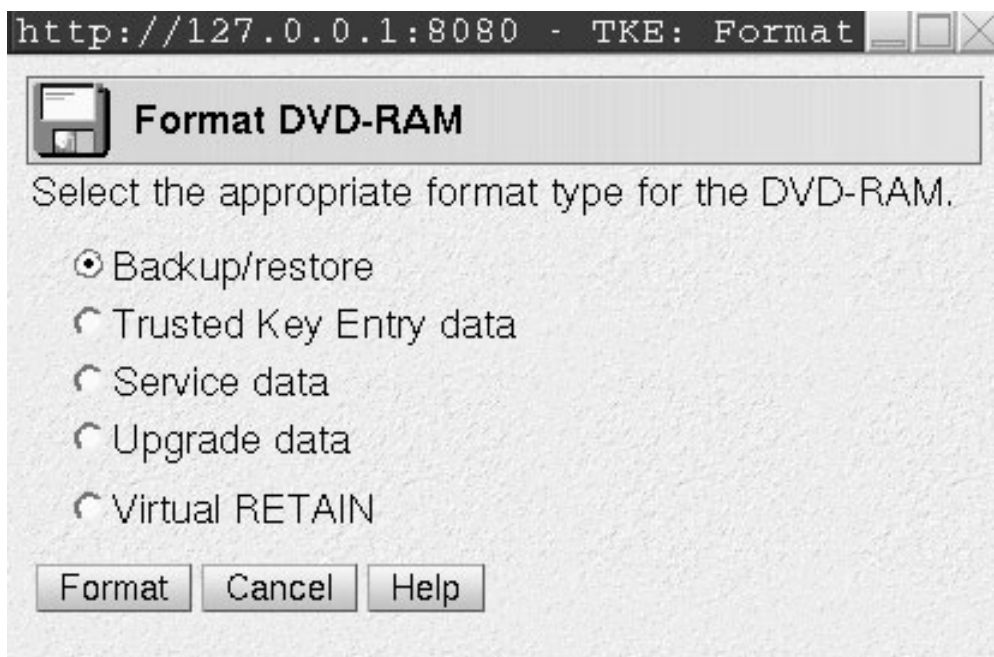


Figure 453. Format DVD-Ram Window

Table 16. Allowable labels when formatting DVD-RAM

Format	Label
Backup/restore	ACTBKP
Trusted Key Entry data	TKEDATA
Service data	SRVDAT
Upgrade data	ACTUPG
Virtual RETAIN	VIRTRET

The DVD-RAM label is automatically written to the DVD.

ACTBKP

This formatted DVD-RAM is used in the Backup Critical Console Data task and the Customize Scheduled Operations task. To choose this format type, select Backup/restore.

TKEDATA

This formatted DVD-RAM is used in the TKE applications and tasks. TKE data can be related to TKE, SCUP, CNM, or user defined. To choose this format type, select Trusted Key Entry data.

SRVDATA

This formatted DVD-RAM is used in the Transmit Console Service Data task. To choose this format type, select Service data.

ACTUPG

This formatted DVD-RAM is used in the Save Upgrade Data task. To choose this format type, select Upgrade data.

VIRTRET

This formatted DVD-RAM is used in the Offload Virtual RETAIN Data to DVD-RAM task. To choose this format type, select Virtual RETAIN.

If the DVD-RAM is not inserted into the DVD drive when the format is selected, you will get the error 'DVD-RAM not ready. DVD is not properly inserted.' Insert the DVD-RAM and click Format.

After the format is completed this screen will be presented.

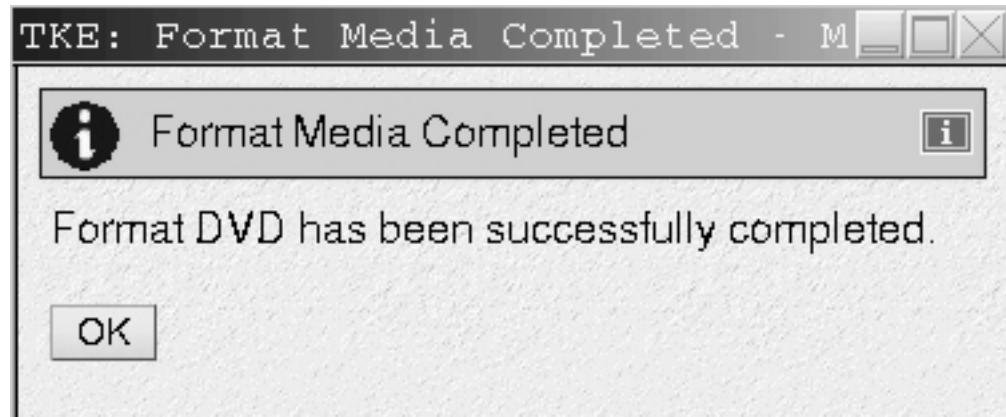


Figure 454. Format Completed Window

To format a diskette simply select 'Format diskette' on the Format Media screen.

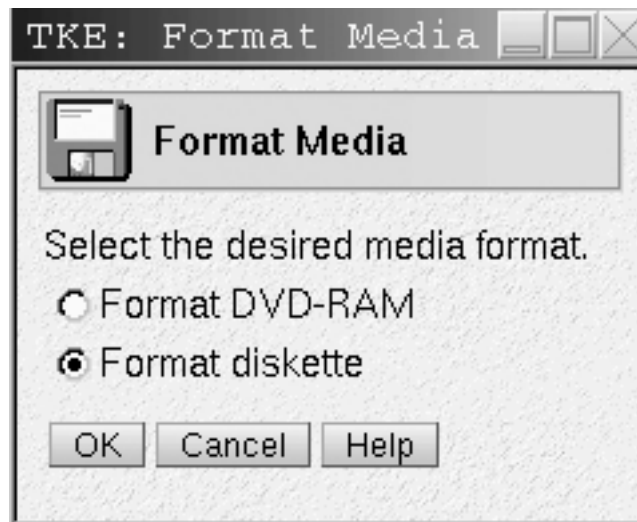


Figure 455. Format a Diskette

You can either specify your own label or choose to have no label on the diskette. To specify your own label enter up to 11 characters in the Label field. If you do not want a label on the diskette, leave the Label field blank. Click on 'Format' button.

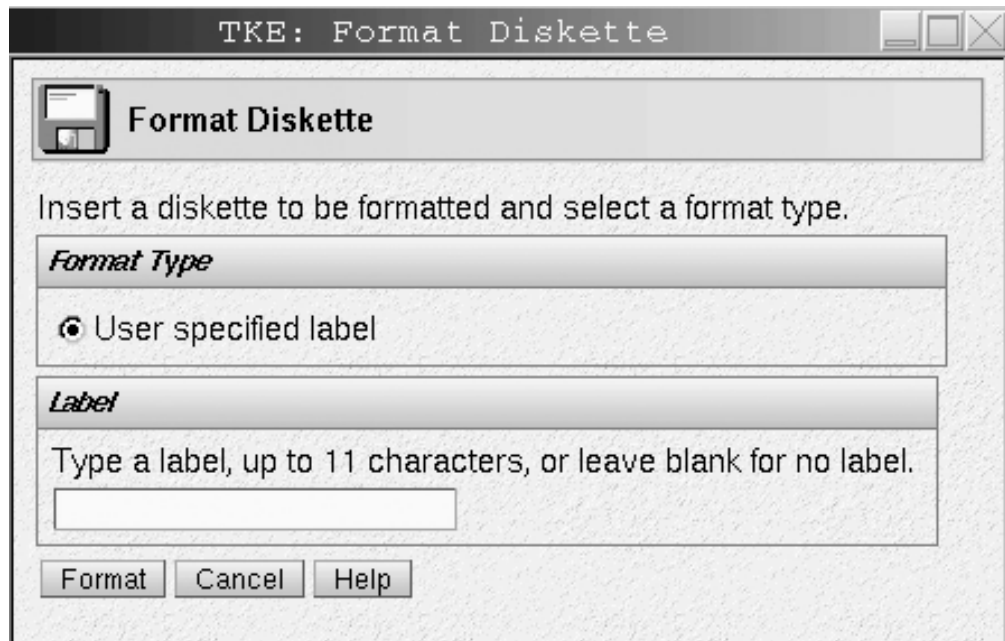


Figure 456. Specifying a Label on Diskette

After the format is completed, this screen will be presented.



Figure 457. Format of Diskette successfully completed

TKE Media Manager

The TKE Version 5.2 workstation allows the use of these media devices:

- Floppy Disk (read-only)
- Compact Disc (read-only)
- DVD-RAM Disc

TKE 5.2 is shipped with one TKEDATA DVD-RAM disc and one Backup DVD-RAM disc. The TKEDATA DVD-RAM disc is provided for saving and backing up TKE related files in the TKE data directories. The Backup DVD-RAM disc should be used to backup critical console data only.

To invoke this task, click on Trusted Key Entry and then click on TKE Media Manager.

Managing Media

Before accessing or updating an inserted floppy or DVD-RAM/CD-ROM media from any of the Trusted Key Entry (Applications and Utilities) tasks, the media must first be activated using the TKE Media Manager. The TKE Media Manager is located under Trusted Key Entry Utilities. From the **Select operation** drop down menu, you can activate media that is currently deactivated, or deactivate media that is currently active by selecting the desired operation and clicking **OK**. After the operation is finished, the TKE Media Manager will update the status of the corresponding drive. Select the cancel button to exit the TKE Media Manager.

Note: To execute the Migrate Previous TKE Version to TKE 5.0, the floppy drive must **NOT** be activated. If it is, the migrate will fail.

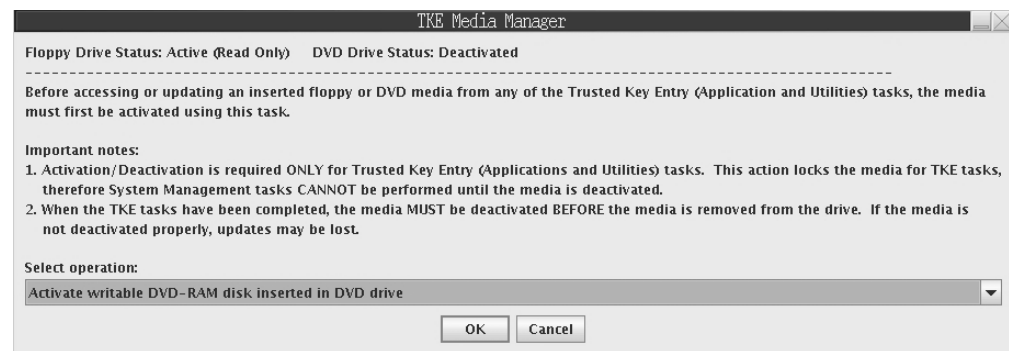


Figure 458. TKE Media Manager

Important Notes:

1. Only DVD-RAM and CD-ROM disks are supported. The DVD-RAM is R/W while the CD-ROM is R/O. DVD-RAM format is single-sided Type II (4.7GB).
2. Activation / Deactivation are required only for Trusted Key Entry (Applications and Utilities) tasks. This action locks the media for TKE tasks; therefore System Management Tasks cannot be performed until the media is deactivated.
3. When the TKE tasks have been completed, the media must be deactivated before the media is removed from the drive. If the media is not deactivated properly, updates may be lost.

Note: If the CD/DVD aren't deactivated the drive will remain locked and cannot be used by any System Management tasks.

4. If a media device is inserted but not activated, and you select to use the device with a TKE application, the application will attempt to activate the device. Even though the media was not activated directly with the TKE Media Manager, the media must still be deactivated using the TKE Media Manager before it is removed.
5. Any media activated in the CD/DVD drive will not eject until the drive is deactivated. You must use the TKE Media Manager to deactivate a drive.
6. If a floppy disk is ejected without deactivating the drive, your disk may become corrupted. It is necessary that you deactivate the floppy drive before you eject your floppy disk.

Note: The TKE 5.2 floppy is read-only.

Warning: Even if you are using the media for input only, the media must be deactivated before it is removed. If the media is not deactivated before it is removed, new media inserted may not be handled correctly.

Appendix P. Service Mode

A service user has been added in order to remove access to service-related tasks from the auto-logged on user.

The Trusted Key Entry Console automatically loads on boot up with a set of commonly used tasks. Optionally the TKE Console may be opened in Service mode. To open the TKE Console in one of these modes, close your current TKE console, and on the Welcome page select "Service and Product Engineering Access". You will be prompted for a username and password.

- For service mode, the user name is SERVICE and the default password is SERVMODE. Once logged in, it is recommended that you change this password with the Change Password task listed under the Service Management

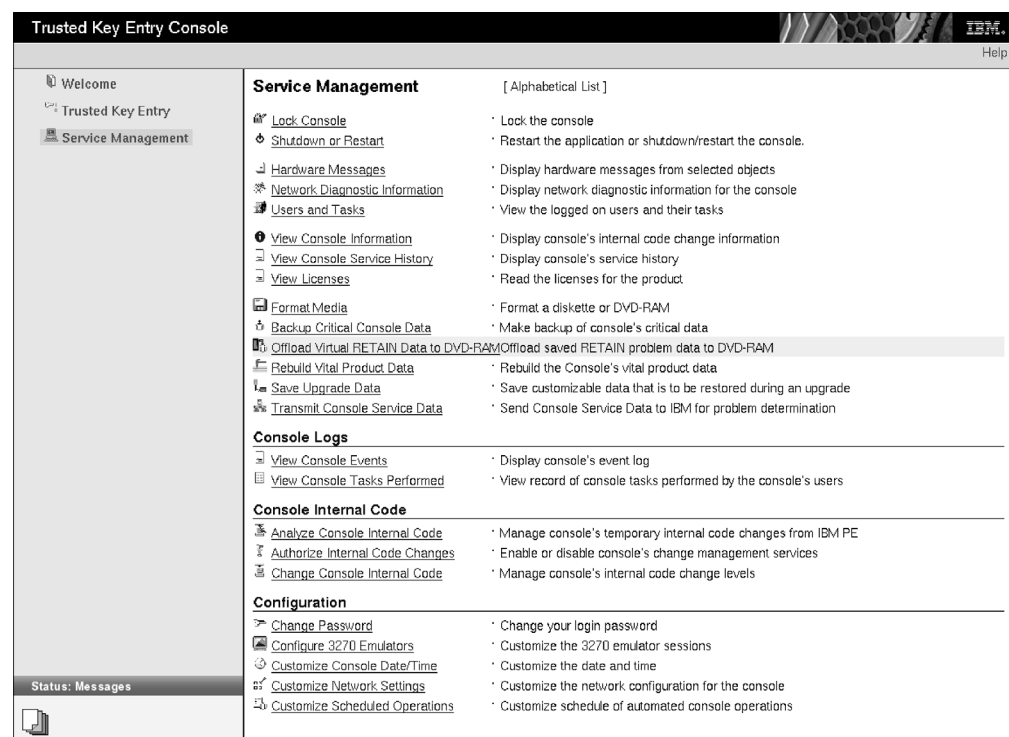


Figure 459. Service Management for the Service User (Categorized)

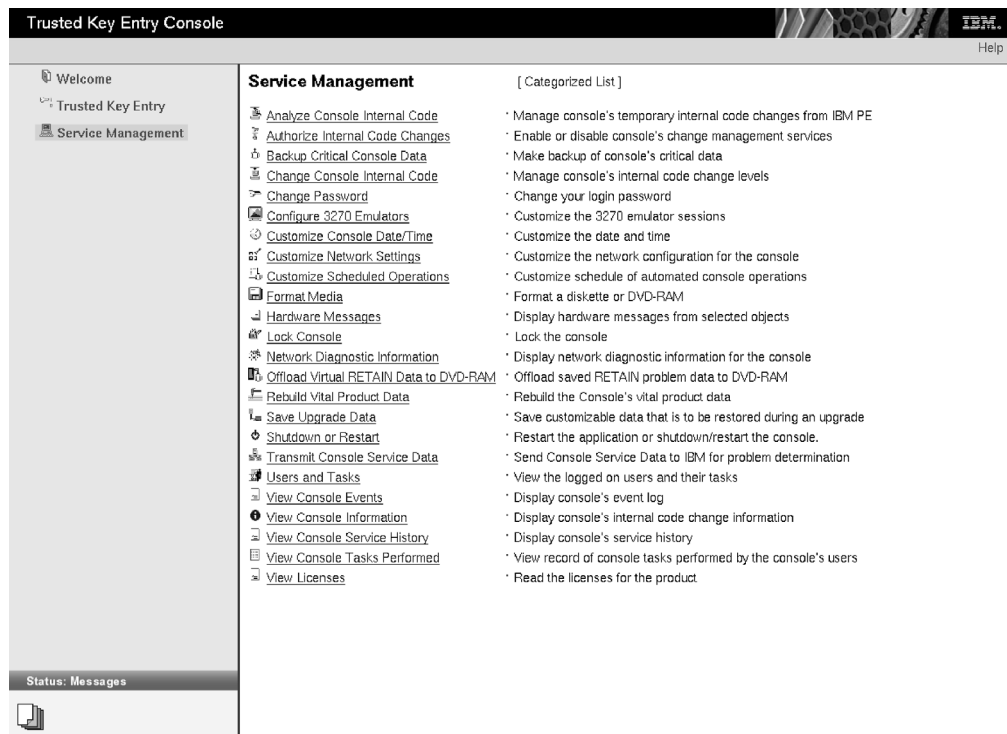
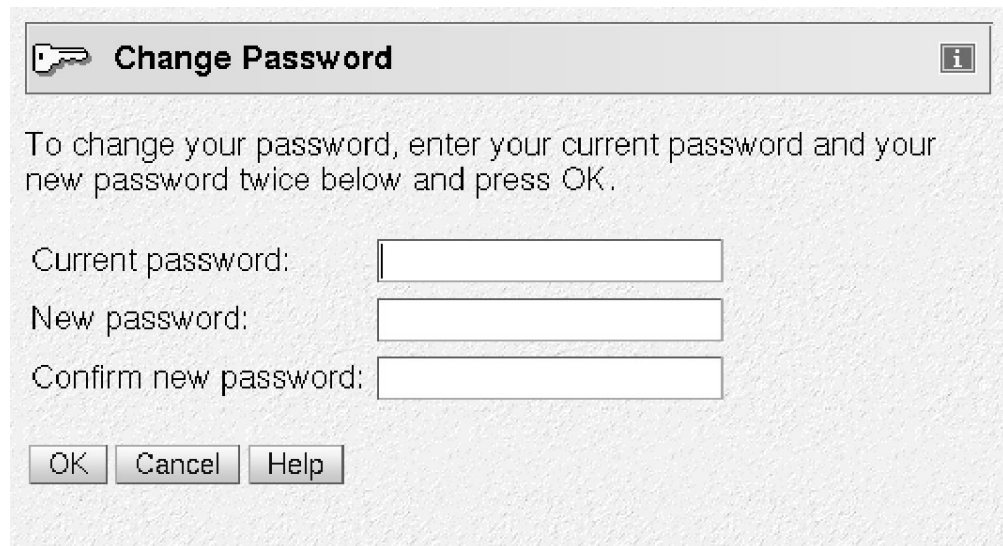


Figure 460. Service Management for the Service User (Alphabetized)

Change Password Task

The Change Password task has been added for TKE 5.1 and later as a result of adding the service user. This task is only used by the service mode user id.

The service user's default out-of-box password is "servmode". The service user must use this password to login the first time. The user should then change it using the Change Password task found within the Configuration category in the Service Management workarea. Figure 461 shows the task being executed.



Change Password

To change your password, enter your current password and your new password twice below and press OK.

Current password:

New password:

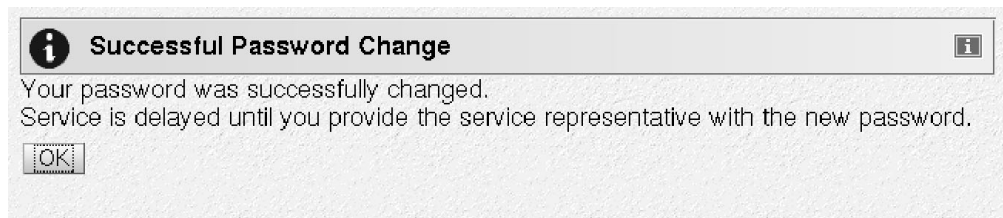
Confirm new password:

OK Cancel Help

Figure 461. Change Password Task

When the task is executed, the user is required to enter the current password and then the desired new password twice. When done successfully and the new password conforms to the password rules, the user is then presented with a success dialog, OK is selected and the task ends.

Note: The user's password is upgraded when the TKE code is upgraded.



Successful Password Change

Your password was successfully changed.
Service is delayed until you provide the service representative with the new password.

OK

Figure 462. Change Password - Success

Password Requirements

Password requirements for the service user's password are "basic". This is not subject to change as an administrative user does not exist on TKE. These rules apply to this "basic" role:

- 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.

Appendix Q. TKE Best Practices

Checklist for Loading a TKE Machine - Passphrase

Expectations

- You are working on a PCIXCC/CEX2C card
- TKE is enabled on the card(s) on the Host machine
- LPARs are established
- TKE CD is loaded on the workstation
- Card code is loaded on the crypto adapter on the workstation
- TKE started task is edited and started in the Host TKE LPAR
- ICSF is started in each LPAR

Setup

- 2 TKEs both running the same level of software
 - 1 for production
 - 1 for backup
- 2 CECs cards being shared
 - 1 Test LPARs (Domain 0)
 - 3 Production LPARs (Domain 1, 2, 3)

TKE can load the master key in groups if the domains are the same across machines.
- Host TKE LPAR 1

When defining the LPAR activation profile, the usage domain will be 1 & the control domain will be 0, 1, 2, 3.

User IDs are used to restrict access to the TKE workstation crypto adapter

- TKEUSER - Logs on to TKE application
- TKEADM - Creates and updates user roles and profiles
- KEYMAN1 - Clears new master key register and loads first master key part
- KEYMAN2 - Loads middle and last master key parts and reenciphers workstation key storage

Authorities are used to restrict access to the CCF, PCICC, PCIXCC, and CEX2C cards on the Host machine.

One way to control access to the Crypto Cards on the host is with a minimum of 7 authority key users.

- ISSUER
 - Disable crypto card
 - Enable crypto card issue
 - Access control issue
 - Zeroize domain issue
 - Domain control change issue
- CONSIGN
 - Access control co-sign
 - Enable crypto card co-sign

- Zeroize domain co-sign
- Domain control change co-sign
- MFIRST
 - Symmetric/asymmetric load first key part
 - Clear new master key register
- MMIDDLE
 - Symmetric/asymmetric combine middle key parts
- MLAST
 - Symmetric/asymmetric combine final key part
 - Set asymmetric master key
- 1STCLEAR
 - Load first key part
 - Clear operational key register
- ADDCOMP
 - Load additional key part
 - Complete key
- TKE 1
 1. Customize Network Settings
 2. Customer Console Date/Time
 3. Initialize the crypto adapter in the workstation
 - a. All predefined roles and profiles are loaded
 - b. Crypto Adapter master key is set and the DES and PKA Key Storage is initialized.
 4. Logon to CNM with KEYMAN1 - OPTIONAL
 - a. Clear master key register
 - b. Enter known first master key part
 - c. Logoff
 5. Logon to CNM with KEYMAN2 - OPTIONAL
 - a. Enter known middle and last master key parts
 - b. Reencipher DES and PKA key storage
 - c. Logoff
 6. Logon to CNM with TKEADM
 - a. Create user defined profiles - OPTIONAL
 - b. Create user defined roles - 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. Logon to TKE 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
 - Floppy Drive only

- c. Create a Host
 - d. Create groups - OPTIONAL
 - e. Logon to host with VM id
 - f. Create role(s)
 - g. Generate authority key(s) and save them to binary file(s)
 - h. Create different authorities using the different authority key(s) that were just generated.
 - i. 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 DVD
 10. Customize Scheduled Operations to schedule the backup critical console data task

Checklist for Loading a TKE Machine - Smart Card

Expectations

- You are working on a PCIXCC/CEX2C card
- TKE is enabled on the Host machine you are using
- LPARs are established (set up and predefined)
- TKE CD is loaded on the workstation
- Card code is loaded on the crypto adapter on the workstation
- TKE started task is created and started on the Host machine
- SC readers are attached

Setup

- 2 TKEs both running the same level of software
 - 1 for production
 - 1 for backup
- 2 CECs cards being shared
 - 1 Test LPARs (Domain 0)
 - 3 Production LPARs (Domain 1, 2, 3)

TKE can load the master key in groups if the domains are the same across machines.

- Host TKE LPAR 1

When defining the LPAR activation profile, the usage domain will be 1 & 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 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 - Logs on to TKE application
- SCTKEADM - Logs on to CNM to create and update user roles and profiles

Authorities are used to restrict access to the CCF, PCICC, PCIXCC, and CEX2C cards on the Host machine.

One way to control access to the cards with a minimum of 7 authority key users (only 1 authority key can be stored on each smart card):

- ISSUER
 - Disable crypto card
 - Enable crypto card issue
 - Access control issue
 - Zeroize domain issue
 - Domain control change issue
- CONSIGN
 - Access control co-sign
 - Enable crypto card co-sign
 - Zeroize domain co-sign
 - Domain control change co-sign
- MFIRST
 - Symmetric/asymmetric load first key part
 - Clear new master key register
- MMIDDLE
 - Symmetric/asymmetric combine middle key parts
- MLAST
 - Symmetric/asymmetric combine final key part
 - Set asymmetric master key
- 1STCLEAR
 - Load first key part
 - Clear operational key register
- ADDCOMP
 - Load additional key part
 - Complete key
- Steps to set up the TKE workstation for smart card use:
 1. Customize Network Settings
 2. Customer Console Date/Time
 3. Initialize the crypto adapter in the workstation for Smart Card use
 - a. All predefined roles and profiles are loaded.
 - b. Crypto Adapter master key is set and the DES and PKA Key Storage is initialized.
 4. Open the SCUP application
 - a. Set the PINs - this will be done by an administrator
 - b. Backup CA smart cards
 - c. Create TKE smart card(s)
 - d. Personalize TKE smart card(s) by setting the PIN (done by the user of the TKE smart card)
 - e. Enroll the TKE adapter with the CA card
 5. Open CNM

Note: You do not have to logon because the temp default key is loaded and has full access to do everything on the crypto adapter.

 - a. Enter known master key - OPTIONAL

- You want to do this if you are going to save authority keys or operational keys in the key storage on the workstation, so you will have a known master key to use again.
- b. Reencipher DES and PKA key storage - OPTIONAL
 - Do this ONLY if you entered your own master key.
- c. Generate TKE crypto adapter logon keys for each smart card that will be logging on to the TKE or CNM applications
- d. Create new profile(s) for the smart cards under the Access Control menu. The roles for these profiles are loaded in the Crypto Adapter when TKE's IBM Crypto Adapter Initialization task is run.
- e. Create group(s) and add users

Note: Group members should already be defined.

- f. Load the default role
 - When the Crypto Card in the TKE workstation is initialized the TEMPDEFAULT role is loaded. You need to load the regular DEFAULT role to secure the TKE workstation.
- 6. Logon to the TKE application with SCTKEUSR profile or another profile with the same authority.
 - a. Enable Smart Card Readers via the TKE preferences menu
 - Select Enable Smart Card Readers
 - b. Close the TKE application
- 7. Logon to TKE with 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
 - Floppy Drive only
 - c. Create a Host
 - d. Create groups - OPTIONAL
 - e. Logon to host with VM id
 - f. Create role(s)
 - g. Generate an authority key(s) and save them to a TKE smart card
 - h. Create different authorities using the different authority key(s) that were just generated.
 - i. 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.
- 8. Configure 3270 Emulators
- 9. Backup Critical Console Data
- 10. Customize Scheduled Operations to schedule the backup critical console data task
- 11. If using the same set of smart cards on another TKE, you need to use the Remote Enroll feature for TKE.

Appendix R. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS™ enable users to:

- Use assistive technologies such as screen readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using such products to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Vol I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

z/OS information

z/OS information is accessible using screen readers with the BookServer/Library Server versions of z/OS books in the Internet library at:

<http://www.ibm.com/servers/eserver/zseries/zos/bkserv/>

Notices

This information was developed for products and services offered in the USA.

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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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
Mail Station P300
2455 South Road
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 information 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.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

- IBM
- IBMLink
- PR/SM
- RACF
- Resource Link
- System z9
- VTAM
- z/OS
- zSeries

The e-business logo is a trademark of IBM.

Other company, product and service names may be trademarks or service marks of others.

Index

Numerics

4764 cryptographic adapter
 enroll local 296
 enroll remote 298
 installation 215
 local enrollment 296
 remote enrollment 298
 temperature warning 215
 view zone 304

A

access control
 administration 222
 CCF 7, 85
 PCICC 8
 PCIXCC/CEX2C 8
access control menu
 CNM 249
access control page 85
access control points
 DEFAULT 227
 KEYMAN1 226
 KEYMAN2 226
 SCTKEUSR 230
 TKEADM 225, 230
 TKEUSER 225
accessibility 389
Activate PKDS panel 184, 209
adding cryptographic coprocessor 178, 204
Administrative Control Functions panel 181, 182, 206, 207
API cryptographic services
 PCICC/PCIXCC/CEX2C 155
auditing 323
authorities 5, 93
 changing 101
 creating 98
 deleting 102
authorities page 93
authority administration
 generating signature keys 95
authority default signature key 6
authority signature key 5
 load 69
authority signature keys
 generating 95
automated recognition
 crypto module 55

B

backup
 CA smart card 289
 host files 58
 workstation files 57
bibliography xxiv

blind key entry
 inputting CCF keys 111
 inputting PCICC/PCIXCC/CEX2C keys 126
books, ICSF xxiv

C

CA smart card 20
 backup 289
 change PIN 295
 display 291
 initialize 287
 personalize 287
cancel TKE server 237
CCF
 access control 7
 authenticating crypto modules 55
 description 1
 domains general page 103
 domains keys page 105
 encipher RSA key 119
 generate RSA key 117
 key types and actions 107
 load 110
 load complete 115
 load RSA key to host dataset 121
 load RSA key to PKDS 120
 load to key storage 115
 load to queue 110
 load to queue complete 115
CEX2C
 description 1
Change Master Key panel 173, 201
change PIN
 CNM 273
change signature index 82
changing entries
 authorities 101
 host 61
changing master keys 170, 198
 using panels 170, 199
checklist
 before using TKE 49
CKDS (cryptographic key data set)
 initializing 160, 161, 196
 panel option 161, 196
 reenciphering 172, 200
 refreshing 192, 212
clear
 PCIXCC/CEX2C 143
clear (CCF) 110
clear (PCICC/PCIXCC/CEX2C) 130
clearing new master key register
 CNM 264
clock
 setting 219
clock-calendar
 read 248

- clock-calendar (*continued*)
 - synchronize 248
- CMID 4
- CMPM
 - description 6
- cni list
 - smart cart 227
- cnm
 - errors 282
- CNM
 - access control menu 249
 - change PIN 273
 - clearing new master key register 264
 - crypto node menu 247
 - define a role 250
 - define group profile 260
 - define passphrase profile 256
 - define smart card profile 258
 - define user profile 255
 - delete user profile loaded in the 4764 263
 - description 241
 - display smart card details 276
 - edit a disk-stored role 251
 - edit a role loaded in the 4764 253
 - edit disk-stored user profile 262
 - edit existing user profile 262
 - edit icon 227
 - edit user profile loaded in the 4764 263
 - file menu 241
 - generate 4764 logon key 275
 - generating master key parts to a TKE smart card 267
 - group logon 243
 - key storage menu 272
 - loading a new master key from key parts 265
 - loading master key parts from a TKE smart card 268
 - manage smart card contents 277
 - master key menu 263
 - passphrase group logon 243
 - passphrase logon 242
 - read clock-calendar 248
 - reenciphering key storage 272
 - reset user profile failure count 263
 - smart card group logon 245
 - smart card logon 242
 - smart card menu 273
 - starting 241
 - synchronize clock-calendar 248
 - verifying master key parts 270
- co-sign page
 - description 157
- commands
 - multi-signature 6
- configuring
 - TCP/IP 215
- Confirm Restart Request panel 176
- Coprocessor Management panel 210
- coprocessor selection panel 166, 175, 186
- creating entries
 - authorities 98

- creating entries (*continued*)
 - crypto module groups 64
- Crypto Express2 Coprocessor 4
 - description 1
- crypto module
 - authenticating 55
 - automated recognition 55
 - description 4
 - groups 63
 - master 66
 - RSA key 5
 - signature key 6
 - using 62
- crypto module ID 4, 55
- crypto module notebook
 - access control page 85
 - authorities page 93
 - authority masks container 88
 - change signature index 82
 - changing signature requirements 87
 - co-sign page 157
 - compare group 82
 - description 79
 - details page 84
 - domain masks container 88
 - domains controls 151
 - domains keys page 105
 - domains page 102
 - functions 82
 - general page 79
 - modes 83
 - multi-signature commands 86
 - refresh notebook 82
 - release crypto module 82
 - roles 88
 - signature requirements 85
 - tabular pages 83
- crypto module public modulus 55
- crypto node menu
 - CNM 247
- cryptographic coprocessor
 - adding 178, 204
- cryptographic coprocessor feature 3

D

- default signature key 56
 - CCF 6
 - CEX2C 6
 - PCICC 6
 - PCIXCC 6
- define a role
 - CNM 250
- define groupe profile
 - CNM 260
- define passphrase profile
 - CNM 256
- define smart card profile
 - CNM 258
- define user profile
 - CNM 255

- delete user profile loaded in the 4764
 - CNM 263
- deleting entries
 - authorities 102
 - DES key storage 73
 - host 62
 - PKA key storage 74
- DES key storage 72
 - deleting an entry 73
- DES master key
 - initializing 160
- DES master key parts
 - importing 163
- DES Operational Key Load panel 211, 212
- disability 389
- disabling PCIXCC/CEX2C 81
- disabling PKA callable services 179, 204
- disabling PKA services 180, 205
- display
 - CA smart card information 291
- display smart card details
 - CNM 276
- domain controls 8
- domain keys page
 - PCIXCC/CEX2C 131
- domain keys page (CCF)
 - clear 110
 - clear key-part queue 106
 - encipher RSA key 119
 - generate RSA key 117
 - load 110
 - load RSA key to host dataset 121
 - load RSA key to PKDS 120
 - load to key storage 115
 - load to queue 110
- domain keys page (PCICC/PCIXCC/CEX2C)
 - generate 124
 - load 126
 - set 130
- domain keys page (PCICC/PCIXCCCEX2C)
 - clear 130
- domain keys page (PCIXCC/CEX2C)
 - encipher RSA key 149
 - generate RSA key 147
 - load RSA key to host dataset 151
 - load RSA key to PKDS 150
- domain keys page PCIXCC/CEX2C)
 - load to key storage 145
- domains
 - domains general page 103
 - domains keys page 105
- domains controls page
 - CCF 151
 - description 151
 - PCICC/PCIXCC/CEX2C 153
- domains general page
 - CCF 103
 - zeroize domain 104
- domains keys page (CCF)
 - generate 108
- domains keys page (PCICC/PCIXCC/CEX2C) 121

- domains page 102

E

- edit an existing role
 - CNM 250
- edit disk-stored user profile
 - CNM 262
- edit existing user profile
 - CNM 262
- edit user profile loaded in the 4764
 - CNM 263
- emulator session
 - configuring 238
- enabling PKA services 181, 206
- encipher RSA key 119, 149
- enrolling an entity
 - description 21
- enter final master key part panel 169
- enter first master key part panel 167
- enter master key part panel 168, 169
- enter new master key panel 166, 168, 169, 175
- entering a key part
 - smart card reader 308

F

- file menu
 - CNM 241
- files
 - backing up 57

G

- general page 79
- generate 4764 logon key
 - CNM 275
- generate RSA key
 - PCIXCC/CEX2C 147
- generate RSA key (CCF) 117
- generating
 - authority signature keys 95
 - CCF keys 108
 - PCICC/PCIXCC/CEX2C keys 124
- generating master key parts to a TKE smart card
 - CNM 267
- group logon
 - CNM 243
- groups
 - changing crypto module 65
 - comparing crypto module 66
 - creating crypto module 64
 - supporting functions 68
 - using crypto module 63

H

- host
 - changing 61
 - creating 60

- host (*continued*)
 - deleting 62
 - logon 60
- host files
 - backing up 58
- host transaction program
 - installation 234

I

- importing
 - DES master key parts 163
 - final master key part 168
 - final operational key part 190
 - first master key part 164
 - first operational key part 185
 - intermediate master key part 167
 - intermediate operational key parts 189
- initial authorities 56
- initialize a CKDS panel 162, 192, 198, 212
- initializing
 - CKDS 161, 196
 - DES master key 160
 - symmetric keys master key 196
 - TKE 4764 cryptographic adapter 219
- integrity 5
- intrusion latch
 - PCICC/PCIXCC/CEX2C 81
- ISPF services
 - PCICC/PCIXCC/CEX2C 153

K

- key part
 - description 179, 205
- key part queue
 - importing DES master key parts 163
- key part queue (CCF)
 - clearing 106
- key storage menu
 - CNM 272
- key synchronization 159
- Key Type Selection Panel 188
- key-exchange protocol 8
- keyboard 389
 - inputting CCF keys 111
 - inputting PCICC/PCIXCC/CEX2C keys 126

L

- load (CCF) 110
 - complete 115
 - input from binary file 112
 - input from keyboard 111
 - input from smart card 114
- load (PCICC/PCIXCC/CEX2C) 126
 - input from binary file 127
 - input from keyboard 126
 - input from TKE smart card 129
- load RSA key to host dataset 121, 151
- load RSA key to PKDS 120, 150

- load to key part register - add part
 - PCIXCC/CEX2C 138
- load to key part register - complete
 - PCIXCC/CEX2C 140
- load to key part register - first
 - PCIXCC/CEX2C 134
- load to key storage (CCF) 115
- load to key storage (PCIXCC/CEX2C) 145
- load to queue 110
- load to queue (CCF)
 - complete 115
 - input from binary file 112
 - input from keyboard 111
 - input from smart card 114
- loading a new master key from key parts
 - CNM 265
- loading master key parts from a TKE smart card
 - CNM 268
- LPAR considerations 8, 319
 - CCF systems 61
 - PCIXCC/CEX2C systems 61

M

- main window 59
 - function menu 69
 - load authority signature key 69
 - utilities 72
- manage smart card contents
 - CNM 277
- master crypto module
 - changing 66
 - setting 65
- master key
 - importing 164
 - initializing 160, 196
 - panel option 164
 - setting 177, 203
- master key management panel 162, 171, 173, 178, 197, 200, 201, 203
- Master Key Management panel 183, 184, 208, 209
- master key menu
 - CNM 263
- master key part
 - importing first 164
 - importing intermediate 167
 - importing last 168
- master key parts 160, 195
- master keys
 - changing 170, 198
 - re-entering 176, 202
- migration
 - TKE V 2.0 to TKE V 5.2 25
 - TKE V 3.0 to TKE V 5.2 27
- mode
 - locked read-only 83
 - pending command 83
 - read-only 83
 - update 83
- modifying entries
 - groups 65

- multi-signature commands 86
 - CCF 6
 - description 6
 - PCICC 7
 - PCIXCC/CEX2C 7
- multiple hosts 8
- multiple workstations 9
- multiple zones 21

N

- Notices 391

O

- Operational Key Input panel 187, 188, 189, 190, 191, 192
- operational key parts
 - generate 132
- operational keys
 - importing 184
 - importing final 190
 - importing first 185
 - importing intermediate 189
 - loading 184
- opkey
 - panel option 185

P

- panels
 - CSF@PRIM — Primary Menu 161, 165, 171, 174, 177, 180, 181, 185, 193, 197, 199, 203, 205, 206, 210, 213
 - CSFACF00 — Administrative Control
 - Functions 181, 182, 206, 207
 - CSFCKD00 — Initialize a CKDS 162, 192, 198, 212
 - CSFCMK10 — Reencipher CKDS 172, 200
 - CSFCMK11 — Reencipher PKDS 183, 208
 - CSFCMK20 — Change Master Key 173, 201
 - CSFCMK21 — Activate PKDS 209
 - CSFCMK21 — Activate PKDS 184
 - CSFCMP20 — Coprocessor Selection 166
 - CSFCMP50 — DES Operational Key Load 211, 212
 - CSFCMP51 — DES Operational Key Load 211
 - CSFCSE12 — Key Type Selection Panel 188
 - CSFEKM00 — Enter New Master Key 166, 168, 169, 175
 - CSFEKM30 — Confirm Restart Request 176
 - CSFEKP10 — Enter First Master Key Part 167
 - CSFEKP10 — Enter Master Key Part 168, 169
 - CSFEKP20 — Enter Final 169
 - CSFEKP20 — Enter First 167
 - CSFEKP20 — Enter Master 168
 - CSFGCMP0 — Coprocessor Management 210
 - CSFMKM00 — Master Key Management 162, 171, 173, 178, 183, 184, 197, 200, 201, 203, 208, 209
 - CSFMKP10 — Coprocessor Selection 175, 186
 - CSFOPK00 — TKE Processing Selection 165, 174, 186, 193, 213

- panels (*continued*)

- CSFSCK10 — Operational Key Input 187, 190, 191
- CSFSCK30 — Operational Key Input 188, 190, 192
- CSFSCK40 — Operational Key Input 189
- parity
 - adjusting a key's parity using ICSF panels 191
- passphrase
 - access control administration 222
 - access control points 225
 - DEFAULT role 227
 - initialize 220
 - KEYMAN1 role 226
 - KEYMAN2 role 226
 - load first key part 224
 - load last key part 224
 - TKEADM role 225
 - TKEUSER role 225
- passphrase group logon
 - CNM 243
- passphrase logon
 - CNM 242
- PCI cryptographic coprocessor feature 3
- PCI X Cryptographic Coprocessor 4
 - description 1
- PCICC
 - access control 8
 - description 2
- PCICC/PCIXCC/CEX2C
 - API cryptographic services 155
 - API cryptographicSPF services 153
 - authenticating crypto modules 55
 - generating keys 124
 - load 126
 - multi-signature commands 89
 - roles 88
 - set ASYM-MK 130
 - single signature commands 90
 - UDXs 156
- PCICC/PCIXCCCEX2C
 - clear 130
- PCIXCC
 - description 1
- PCIXCC/CEX2C
 - access control 8
 - clear 143
 - disabling 81
 - domain keys page 131
 - encipher RSA key 149
 - generate operational key parts 132
 - generate RSA key 147
 - load RSA key to host dataset 151
 - load RSA key to PKDS 150
 - load to key part register - add part 138
 - load to key part register - complete 140
 - load to key part register - first 134
 - load to key storage 145
 - operational keys 131
- PKA callable services
 - disabling before entering PKA master keys 179, 204
- PKA key storage 73

- PKA key storage *(continued)*
 - deleting an entry 74
- PKDS
 - activating 182, 207
 - reenciphering 182, 207
- PR/SM considerations 177, 202
- primary menu panel 161, 165, 174, 180, 193, 197, 205, 210, 213
- Primary Menu panel 171, 174, 177, 181, 185, 199, 203, 206
- publications
 - ICSF xxiv
 - related xxiii

R

- re-entering master keys 176, 202
- reencipher CKDS panel 172, 200
- Reencipher PKDS panel 183, 208
- reenciphering key storage
 - CNM 272
- refresh notebook 82
- refreshing the CKDS
 - using panels 192, 212
- release crypto module 82
- remote 4764 cryptographic adapter
 - enroll 298
- reset user profile failure count
 - CNM 263
- resetting PKA master keys 182, 207
- restarting the DES key entry process 174
- role
 - edit 251, 253
- roles
 - access control points (passphrase) 225
 - access control points (smart card) 230
 - changing 90
 - creating 90
 - deleting 93
 - description 88
- RSA key 4
 - crypto module 5
 - encipher 119, 149
 - generate 117, 147
 - installing in the PKDS 193, 213
 - load to host dataset 121, 151
 - load to PKDS 120, 150

S

- SCUP
 - backup the CA smart card 289
 - change PIN of a CA smart card 295
 - change PIN of a TKE smart card 296
 - description 285
 - display smart card 291
 - enroll a 4764 cryptographic adapter 296
 - initialize and enroll a TKE smart card 293
 - initialize and personalize the CA smart card 287
 - personalize a TKE smart card 294
 - unblock PIN on a TKE smart card 295

- SCUP *(continued)*
 - view zone 304
- secure key part entry
 - description 305
 - entering a key part 308
 - steps 305
- security policy
 - defining 9
- setting master key 177, 203
- shortcut keys 389
- signature requirements
 - changing 87
- smart card
 - access control points 230
 - cni list 227
 - edit CNM icon 227
 - initialize 227
 - SCTKEUSR role 230
 - TKEADM role 230
- smart card group logon
 - CNM 245
- smart card logon
 - CNM 242
- smart card menu
 - CNM 273
- smart card reader
 - secure key part entry 308
 - using 19
- smart card support
 - authentication 20
 - CA smart card 20
 - description 19
 - enrolling an entity 21
 - multiple zones 21
 - preparation and planning 18
 - requirements 17
 - setting up 22
 - terminology 17
 - TKE smart card 22
 - using the smart card reader 19
 - zone creation 20
 - zone description 20
 - zone identifier 20
- start TKE server 237
- symmetric keys master key
 - initializing 196
- synchronizing keys 159

T

- TCP/IP
 - configure 215
 - setup 233
- TKE
 - host transaction program 234
 - smart card support 17
- TKE 4764 cryptographic adapter
 - initialize 219
- TKE enablement
 - z990, z890, z9-109, z9 EC, z9 BC, System z10 EC 9

TKE processing selection panel 165, 174, 186, 193, 213

TKE smart card

change PIN 296

description 22

initialize and enroll 293

personalize 294

unblock PIN 295

TKE Version 5.0

migrating to 25

TKE Version 5.2

migrating to 27

transport key policy

defining 71

trusted key entry

access control 7

activating the host 60

authorities 5

authority default signature key 6

authority signature key 5

checklist before using 49

concepts 4

Crypto Express2 Coprocessor 4

crypto module signature key 6

cryptographic coprocessor feature 3

exiting 72

integrity 5

interaction with ICSF 159, 195

introducing 3

key-exchange protocol 8

LPAR 8, 61

main window 59

multi-signature commands 6

operational considerations 8

optional pc hardware 2

pc hardware 2

pc software 3

PCI cryptographic coprocessor feature 3

PCI X Cryptographic Coprocessor 4

smart card hardware 2

synchronizing keys 159

system hardware 1

system software 2

terms 4

workstation logon 50

TSS HIKM

using 26

U

UDXs

PCICC/PCIXCC/CEX2C 156

utilities

copying smart card contents 75

managing DES keys 72

managing PKA keys 73

managing smart card contents 74

V

verification pattern

description 180, 205

verifying master key parts

CNM 270

W

workstation

logon 50

workstation files

backing up 57

workstation logon

passphrase 50

smart card 50

Z

z9 BC 9

z9 EC 9

z990, z890 z9-109, z9 EC and z9 BC

TKE enablement 9

zeroize domain 104

zone creation 20

zone description 20

zone identifier 20

Readers' Comments — We'd Like to Hear from You

z/OS

Cryptographic Services

ICSF

Trusted Key Entry PCIX Workstation User's Guide - SEE RESOURCE LINK FOR THE LATEST COPY OF THIS BOOK

Publication No. SA23-2211-03

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:

- Send your comments to the address on the reverse side of this form.
- Send your comments via e-mail to: mhvrfs@us.ibm.com

If you would like a response from IBM, please fill in the following information:

Name

Address

Company or Organization

Phone No.

E-mail address



Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape



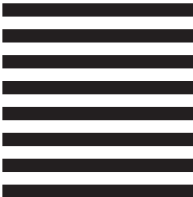
NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie, NY
12601-5400



Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line



Program Number: 5694-A01

Printed in USA

SA23-2211-03

