



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





# Trusted Key Entry 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 361.

**Seventh Edition**

This is a major revision of SA23-2211-05.

This edition applies to Version 1 Release 12 of z/OS (5694-A01) and to all subsequent releases and modifications until otherwise indicated in new editions.

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 IBM Corporation 2000, 2010.

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



# Contents

<b>Figures</b> . . . . .	ix
<b>Tables</b> . . . . .	xvii
<b>About this information</b> . . . . .	xix
Who should read this information . . . . .	xix
How to use this information . . . . .	xix
Where to find more information . . . . .	xx
Related Publications . . . . .	xx
ICSF Publications . . . . .	xxi
<b>Summary of Changes</b> . . . . .	xxiii
<b>Chapter 1. Overview</b> . . . . .	1
Trusted Key Entry Components . . . . .	1
Supported Host Cryptographic Cards . . . . .	1
TKE Hardware . . . . .	1
TKE Software . . . . .	2
Introducing Trusted Key Entry . . . . .	2
ICSF and the Trusted Key Entry Feature . . . . .	2
Supported Host Cryptographic Card Features . . . . .	3
Host Crypto Module . . . . .	3
TKE Concepts and Mechanisms . . . . .	3
Integrity . . . . .	4
Authorities . . . . .	4
Crypto Module Signature Key . . . . .	5
Multi-Signature Commands . . . . .	5
Access Control . . . . .	6
Key-Exchange Protocol . . . . .	6
Domain Controls . . . . .	6
TKE Operational Considerations . . . . .	6
Logically Partitioned (LPAR) Mode Considerations . . . . .	6
Multiple Hosts . . . . .	7
Multiple Workstations . . . . .	7
Defining Your Security Policy . . . . .	7
TKE Enablement . . . . .	7
Trusted Key Entry Console . . . . .	8
Trusted Key Entry Console Navigation . . . . .	11
<b>Chapter 2. Using Smart Cards with TKE</b> . . . . .	13
Terminology . . . . .	13
Preparation and Planning . . . . .	14
Using the OmniKey smart card reader . . . . .	15
Smart Card Compatibility Issues . . . . .	15
Zone Concepts . . . . .	17
Authentication and Secure Communication . . . . .	18
Zone creation . . . . .	18
Multiple zones . . . . .	19
Enrolling an entity . . . . .	19
TKE smart cards . . . . .	20
Steps to set up a smart card installation . . . . .	21
<b>Chapter 3. Migration</b> . . . . .	23

Migrating from TKE Version 2.0 to TKE Version 7.0 . . . . .	23
Migrating from TKE Version 3.X or 4.X to TKE Version 7.0 . . . . .	25
Backup TKE Configuration Files . . . . .	25
TKE Started Task . . . . .	26
Set the Workstation Clock . . . . .	26
Copy Customer Unique Data . . . . .	26
Passphrase and Smart Card Setup . . . . .	27
Passphrase Setup . . . . .	27
Smart Card Setup — Migrating from TKE previously using smart cards . . . . .	33
Smart Card Setup — Migrating from a TKE NOT previously using smart cards. . . . .	37
Migrating from TKE Version 5.0, 5.1, 5.2, 5.3, or 6.0 to TKE Version 7.0 . . . . .	42
TKE Started Task . . . . .	42
Passphrase and Smart Card Setup . . . . .	43
Smart Card Setup — Migrating from TKE previously using smart cards . . . . .	48
Smart Card Setup — Migrating from TKE NOT previously using smart cards . . . . .	52
Migrating Data from One Smart Card to Another . . . . .	57
Migrate Data on DataKey Smart Cards to NXP JCOP 4.1 Smart Cards . . . . .	57
 <b>Chapter 4. TKE Setup and Customization . . . . .</b>	 59
TKE TCP/IP Setup . . . . .	59
TKE Host Transaction Program Setup . . . . .	60
Cancel the TKE server . . . . .	63
TKE Workstation Setup and Customization . . . . .	64
Configuring TCP/IP . . . . .	64
Initializing the TKE Workstation Crypto Adapter . . . . .	69
Configure 3270 Emulators . . . . .	82
 <b>Chapter 5. TKE Up and Running . . . . .</b>	 85
Crypto Adapter Logon: Passphrase or Smart card . . . . .	85
Passphrase and passphrase group logon . . . . .	85
Smart card and smart card group logon . . . . .	87
Automated Crypto Module Recognition . . . . .	90
Authenticating the CMID and CPM . . . . .	91
Initial Authorities . . . . .	92
Backing Up Files . . . . .	92
Workstation Files . . . . .	92
Host Files . . . . .	93
 <b>Chapter 6. Main Window . . . . .</b>	 95
Host Logon . . . . .	96
Working with Hosts . . . . .	96
Creating a Host . . . . .	97
Changing Host Entries . . . . .	97
Deleting Host Entries . . . . .	97
Working with Crypto Modules . . . . .	98
Working with Crypto Module Groups . . . . .	98
Creating a Crypto Module Group . . . . .	100
Changing a Crypto Module Group . . . . .	101
Comparing Crypto Module Groups . . . . .	103
TKE Functions Supporting Crypto Module Groups . . . . .	104
Working with Domain Groups . . . . .	105
Creating a Domain Group . . . . .	106
Changing a Domain Group . . . . .	108
Viewing a Domain Group . . . . .	108
Checking Domain Group Overlap . . . . .	109

Comparing Groups . . . . .	111
TKE Functions Supporting Domain Groups . . . . .	112
Function Menu . . . . .	113
Load Signature Key. . . . .	113
Display signature key information. . . . .	115
Define Transport Key Policy. . . . .	115
Exit. . . . .	116
Exit and logoff. . . . .	116
Utilities Menu . . . . .	117
Manage Workstation DES Keys . . . . .	117
Manage Workstation PKA Keys . . . . .	118
Manage smart cards . . . . .	119
Copy smart cards . . . . .	120
TKE Customization . . . . .	121
<b>Chapter 7. Crypto Module Notebook.</b> . . . .	123
Crypto Module Notebook General Tab . . . . .	123
Intrusion Latch . . . . .	124
Notebook Mode . . . . .	125
Crypto Module Notebook Function Menu . . . . .	125
Tabular Pages. . . . .	126
Crypto Module Notebook Details Tab . . . . .	126
Crypto Module Notebook Roles Tab. . . . .	127
Multi-Signature Commands . . . . .	127
Single Signature Commands . . . . .	128
Creating or Changing a Role . . . . .	128
Deleting a Role . . . . .	131
Crypto Module Notebook Authorities Tab . . . . .	131
Generating Authority Signature Keys . . . . .	132
Create Authority . . . . .	134
Change Authority . . . . .	137
Delete Authority . . . . .	138
Crypto Module Notebook Domains Tab . . . . .	138
Domains General Page . . . . .	139
Domains Keys Page . . . . .	140
Operational Keys . . . . .	149
RSA Keys . . . . .	168
Domains Controls Page . . . . .	173
Crypto Module Notebook Co-Sign Tab . . . . .	174
<b>Chapter 8. Auditing</b> . . . . .	175
TKE Audit Configuration Utility. . . . .	175
Service Management Auditing Functions . . . . .	179
View Security Logs . . . . .	179
Archive Security Logs . . . . .	181
Format Security Logs to DVD-RAM . . . . .	182
TKE Audit Record Upload Configuration Utility . . . . .	183
Starting TKE Audit Record Upload Configuration Utility. . . . .	183
Configure TKE for Audit Data Upload . . . . .	184
Uploading Audit Records. . . . .	185
Enabling and Disabling Automatic Audit Record Upload . . . . .	186
<b>Chapter 9. Managing Keys</b> . . . . .	187
Master Key Parts . . . . .	187
First-Time Startup . . . . .	188
Initialize the CKDS . . . . .	188

Changing Master Keys . . . . .	190
Changing the Master Key Using the Master Key Panels . . . . .	191
Re-entering Master Keys After They have been Cleared . . . . .	194
Setting the Master Key . . . . .	195
Adding Host Crypto Modules After ICSF Initialization . . . . .	196
Asymmetric-keys Master Key Parts . . . . .	196
Disabling PKA Services . . . . .	197
Enabling PKA Services . . . . .	198
Resetting Asymmetric Master Keys . . . . .	199
Reenciphering and Refreshing the PKDS . . . . .	199
Loading Operational Keys to the CKDS . . . . .	201
Refreshing the CKDS . . . . .	204
Updating the CKDS with the AES master key . . . . .	205
Installing RSA Keys in the PKDS from a Data Set . . . . .	207
 <b>Chapter 10. Cryptographic Node Management Utility (CNM)</b> . . . . .	209
Passphrase Logon . . . . .	209
Smart Card Logon . . . . .	210
Group Logon . . . . .	210
Passphrase Group Logon . . . . .	211
Smart Card Group Logon . . . . .	212
File Menu . . . . .	214
Exit. . . . .	214
Exit and Logoff . . . . .	215
Crypto Node Menu . . . . .	215
TKE Crypto Adapter Clock-Calendar . . . . .	215
Access Control Menu . . . . .	216
TKE predefined roles . . . . .	217
Open or edit an existing role . . . . .	217
Define a User Profile . . . . .	222
Working with User Profiles . . . . .	230
Master Key Menu . . . . .	231
Clearing the new master key register . . . . .	232
Loading a new master key from clear key parts . . . . .	233
Generating master key parts to a TKE smart card . . . . .	235
Loading master key parts from a TKE smart card . . . . .	237
Verifying Master Key Parts . . . . .	238
Key Storage Menu . . . . .	240
Reenciphering key storage . . . . .	241
Smart card Menu . . . . .	242
Change PIN . . . . .	243
Generate TKE Crypto Adapter logon key . . . . .	244
Display smart card details . . . . .	245
Manage Smart Card Contents . . . . .	246
Copy Smart Card . . . . .	248
CNM Common Errors . . . . .	251
 <b>Chapter 11. Smart Card Utility Program (SCUP)</b> . . . . .	253
General Information. . . . .	253
File Menu Functions . . . . .	255
Display smart card information. . . . .	255
Display smart card key identifiers. . . . .	256
CA Smart Card Menu Functions . . . . .	258
Initialize and personalize the CA smart card. . . . .	258
Backup a CA smart card . . . . .	261
Change PIN of a CA smart card . . . . .	262

TKE Smart Card Menu Functions . . . . .	263
Initialize and enroll a TKE smart card . . . . .	263
Personalize a TKE smart card . . . . .	264
Unblock PIN on a TKE smart card . . . . .	265
Change PIN of a TKE smart card . . . . .	265
Crypto Adapter Menu Functions . . . . .	265
Enroll a TKE cryptographic adapter . . . . .	265
View current zone . . . . .	274
<b>Appendix A. Secure Key Part Entry . . . . .</b>	<b>275</b>
Steps for secure key part entry . . . . .	275
Entering a key part on the smart card reader . . . . .	278
<b>Appendix B. Access Control Points and Callable Services . . . . .</b>	<b>281</b>
<b>Appendix C. LPAR Considerations . . . . .</b>	<b>291</b>
Setup for CEX2C/CEX3C Systems . . . . .	291
<b>Appendix D. Trusted Key Entry - Workstation Cryptographic Adapter</b>	
<b>Initialization . . . . .</b>	<b>293</b>
Cryptographic Node Management Batch Initialization 4.1.0 . . . . .	293
CCA CLU 4.1.0 . . . . .	294
CLU Processing . . . . .	294
Checking Coprocessor Status . . . . .	297
Loading Coprocessor Code . . . . .	297
Validating Coprocessor Code . . . . .	299
Checking System Status . . . . .	299
Resetting Coprocessor . . . . .	299
Removing Coprocessor CCA Code and Zeroizing CCA. . . . .	299
Help Menu . . . . .	299
<b>Appendix E. Clear RSA Key Format . . . . .</b>	<b>301</b>
<b>Appendix F. Trusted Key Entry Applications and Utilities . . . . .</b>	<b>303</b>
Trusted Key Entry Applications and Utilities . . . . .	304
Begin Zone Remote Enroll Process . . . . .	305
CCA CLU 4.1.0 . . . . .	305
Complete Zone Remote Enroll Process . . . . .	305
Cryptographic Node Management Batch Initialization 4.1.0 . . . . .	305
Cryptographic Node Management Utility 4.1.0 . . . . .	305
Edit TKE Files. . . . .	305
Migrate Previous TKE Version to TKE 7.0 . . . . .	309
Smart Card Utility Program 7.0 . . . . .	311
TKE Audit Configuration Utility . . . . .	311
TKE Audit Record Upload Configuration Utility . . . . .	311
TKE File Management Utility . . . . .	311
TKE Media Manager . . . . .	313
TKE Workstation Code Information . . . . .	315
Configuration Migration . . . . .	315
Service Management Tasks. . . . .	321
Analyze Console Internal Code . . . . .	322
Archive Security Logs . . . . .	322
Authorize Internal Code Changes . . . . .	323
Backup Critical Console Data . . . . .	323
Change Console Internal Code . . . . .	324
Change Password . . . . .	325

Customize Scheduled Operations . . . . .	326
Format Media . . . . .	331
Log Offload Support for Customer Audit . . . . .	334
Hardware Messages . . . . .	334
Lock console . . . . .	335
Manage Print Screen Files . . . . .	336
Network Diagnostic Information . . . . .	336
Rebuild Vital Product Data . . . . .	336
Offload Virtual RETAIN Data to Removable Media . . . . .	337
Save Upgrade Data. . . . .	338
Shutdown or Restart . . . . .	339
Transmit Console Service Data . . . . .	340
Users and Tasks . . . . .	343
View Console Events . . . . .	344
View Console Information . . . . .	345
View Console Service History . . . . .	347
View Console Tasks Performed . . . . .	349
View Licenses. . . . .	350
View Security Logs . . . . .	351
<b>Appendix G. TKE Best Practices . . . . .</b>	<b>353</b>
Checklist for Loading a TKE Machine - Passphrase . . . . .	353
Checklist for Loading a TKE Machine - Smart Card . . . . .	355
<b>Appendix H. Accessibility . . . . .</b>	<b>359</b>
Using assistive technologies . . . . .	359
Keyboard navigation of the user interface. . . . .	359
z/OS information . . . . .	359
<b>Notices . . . . .</b>	<b>361</b>
<b>Trademarks . . . . .</b>	<b>363</b>
<b>Index . . . . .</b>	<b>365</b>

# Figures

1. ICSF Library . . . . .	xxi
2. TKE Console - initial panel. . . . .	9
3. TKE Console - pre-login panel . . . . .	10
4. Log on with other console user names . . . . .	10
5. Trusted Key Entry for ADMIN - catagorized . . . . .	11
6. Service Management for TKEUSER (Categorized) . . . . .	12
7. Multiple zones . . . . .	19
8. Migrate Previous TKE Version to TKE V7.0. . . . .	29
9. Data Migration Progress Panel. . . . .	29
10. Entry Example. . . . .	60
11. Example of Reserving a Port . . . . .	60
12. Format of AUTHCMD . . . . .	60
13. Assign a User ID to CSFTTKE in FACILITY Class . . . . .	61
14. Assign a User ID to CSFTTKE in APPL Class . . . . .	61
15. Assign a User ID to a Started Task . . . . .	61
16. Sample Startup Procedure . . . . .	62
17. Start the TKE server . . . . .	63
18. Cancel the TKE server. . . . .	63
19. Login with ADMIN user name . . . . .	64
20. Customize Network Settings - Identification Tab . . . . .	65
21. Customize Network Settings Lan Adapters Tab . . . . .	66
22. Local Area Network . . . . .	67
23. Customize Network Settings - Name Services Tab . . . . .	68
24. Network Diagnostic Information Task . . . . .	69
25. Customize Console Date and Time Window . . . . .	70
26. Configure NTP settings . . . . .	71
27. Add a Network Time Server. . . . .	71
28. Cryptographic Node Management Utility . . . . .	72
29. Cryptographic Node Management Utility . . . . .	78
30. Configure 3270 Emulators . . . . .	83
31. Add 3270 Emulator Session. . . . .	83
32. Start or Delete a 3270 Emulator Session . . . . .	84
33. Crypto Adapter logon window with passphrase profiles . . . . .	85
34. Enter passphrase for logon . . . . .	86
35. Crypto Adapter group logon window with passphrase profiles . . . . .	86
36. Enter passphrase for logon . . . . .	86
37. Crypto Adapter Group logon window with passphrase profile ready . . . . .	87
38. Crypto Adapter Logon Window with smart card profiles . . . . .	87
39. Insert the TKE smart card . . . . .	88
40. Enter smart card PIN . . . . .	88
41. Crypto Adapter Group logon window with smart card profiles. . . . .	89
42. Insert the TKE smart card . . . . .	89
43. Crypto Adapter Group logon window with smart card profile ready. . . . .	90
44. Authenticate Crypto Module . . . . .	91
45. TKE Preferences . . . . .	95
46. Host Logon Window. . . . .	96
47. Create Host. . . . .	97
48. Main Window . . . . .	98
49. Main Window - working with crypto module groups . . . . .	99
50. Create New Group. . . . .	100
51. Change Group . . . . .	102
52. Group Compare. . . . .	104
53. Main Window - working with domain groups . . . . .	105

	54. Create Domain Group . . . . .	107
	55. Change Domain Group . . . . .	108
	56. View Domain Group . . . . .	109
	57. Check Domain Group Overlap . . . . .	110
	58. Domain Group Overlap Details . . . . .	111
	59. Compare Group . . . . .	112
I	60. Select Authority Signature Key Source . . . . .	113
	61. Specify Authority Index . . . . .	114
	62. Load Signature Key . . . . .	115
	63. Select Transport Key Policy . . . . .	116
	64. TKE Workstation DES Key Storage Window . . . . .	117
	65. TKE Workstation PKA Key Storage Window . . . . .	118
	66. TKE smart card contents . . . . .	119
	67. Select keys to copy . . . . .	121
	68. Crypto Coprocessor Crypto Module Administration Notebook - General Page . . . . .	123
	69. Window to Release Crypto Module . . . . .	126
	70. Create New Role Page . . . . .	129
	71. Authorities Page . . . . .	131
	72. Filled In generate signature key window . . . . .	132
	73. Save authority signature key . . . . .	133
I	74. Generate signature key . . . . .	134
	75. Key saved status message . . . . .	134
I	76. Select source of authority signature key . . . . .	135
I	77. Create new authority . . . . .	135
	78. Load Signature Key from binary file . . . . .	136
	79. Create New Authority with Role Container . . . . .	137
	80. Change Authority . . . . .	138
	81. Domains General Page . . . . .	139
	82. Domains Keys Page . . . . .	140
	83. Select Target . . . . .	142
	84. Save key part to smart card . . . . .	143
	85. Enter key part description . . . . .	143
	86. Save key part . . . . .	143
	87. Save key part success message . . . . .	143
	88. Select key source - smart card . . . . .	144
	89. Select key part from TKE smart card . . . . .	144
	90. Select key source - keyboard . . . . .	145
	91. Enter Key Value - Blind Key Entry . . . . .	145
	92. Enter Key Value . . . . .	146
	93. Key Part Information Window . . . . .	146
	94. Key Part Information Window . . . . .	146
	95. Select key source - binary file . . . . .	147
	96. Specify Key File . . . . .	147
	97. Key Part Information Window . . . . .	148
	98. Clear new or old master key register validation message . . . . .	148
	99. Clear new or old new master key successful message . . . . .	149
	100. Generate Operational Key - predefined EXPORTER Key Type . . . . .	151
	101. Generate Operational Key - USER DEFINED . . . . .	151
	102. Select Target . . . . .	152
	103. Save key part . . . . .	152
	104. Save key again . . . . .	153
	105. Select Source . . . . .	154
	106. Specify key file for binary file source . . . . .	154
	107. Enter key value - keyboard source for predefined EXPORTER key type . . . . .	155
	108. Enter key value - keyboard source for USER DEFINED key type . . . . .	156
	109. Select Source . . . . .	156



110. Select key part from TKE smart card . . . . .	157
111. Key part information - first DES key part. . . . .	157
112. DES key part register information . . . . .	158
113. Load Operational Key Part Register - add part, keyboard source for USER DEFINED . . . . .	158
114. Drop down of control vectors - add part, keyboard source for USER DEFINED . . . . .	158
115. DES Key part information - add part . . . . .	159
116. DES Key part register information - add part with SHA-1 for combined key . . . . .	159
117. AES key part information - add part . . . . .	160
118. AES key part register information . . . . .	160
119. Complete DES Operational Key Part Register - predefined EXPORTER key type. . . . .	160
120. Complete DES Operational Key Part Register - USER DEFINED key type . . . . .	161
121. Complete AES Operational Key Part Register - predefined DATA key type . . . . .	161
122. AES Key part register information - predefined DATA key type in Complete state . . . . .	161
123. DES Key part register information - predefined EXPORTER key type in Complete state . . . . .	162
124. View DES Operational Key Part Register - EXPORTER, one key label selected . . . . .	162
125. View DES Operational Key Part Register - EXPORTER, all key labels selected . . . . .	163
126. View DES Operational Key Part Register - USER DEFINED . . . . .	163
127. View DES key part register information - key part bit on in CV. . . . .	163
128. View DES key part register information - complete key . . . . .	164
129. View key register successful message . . . . .	164
130. Warning! message for clear operational key part register. . . . .	164
131. Clear Operational Key Part Register - EXPORTER key type, one key label selected . . . . .	165
132. Clear DES Operational Key Part Register - EXPORTER key type, all key labels selected . . . . .	165
133. Clear DES Operational Key Part Register - USER DEFINED, one key label selected . . . . .	166
134. Clear Key Register successful message . . . . .	166
135. Install Importer Key Part in Key Storage . . . . .	167
136. Install IMP-PKA Key Part in Key Storage . . . . .	168
137. Generate RSA Key . . . . .	169
138. Encipher RSA Key . . . . .	170
139. Load RSA Key to PKDS. . . . .	172
140. Load RSA Key to Dataset . . . . .	173
141. Default settings for auditing . . . . .	176
142. Auditing is off. . . . .	177
143. Example of expanded auditing points . . . . .	178
144. Viewing the security logs . . . . .	180
145. Viewing additional details of the security logs . . . . .	181
146. Archiving the security logs . . . . .	181
147. Formatting the security logs . . . . .	182
148. Formatting the security logs message. . . . .	182
149. Formatting the security logs complete message . . . . .	182
150. TKE Audit Record Upload Configuration Utility . . . . .	183
151. Specify Host Information dialog . . . . .	184
152. Other hosts and associated timestamps . . . . .	184
153. Specify Host Login Information . . . . .	185
154. ICSF Selecting the Master Key Option on the Primary Menu Panel . . . . .	189
155. Selecting the Initialize a CKDS Option on the ICSF Master Key Management Panel . . . . .	189
156. ICSF Initialize a CKDS Panel . . . . .	190
157. Selecting the Master Key Option on the ICSF Primary Menu Panel . . . . .	191
158. Selecting the Reencipher CKDS Option on the ICSF Master Key Management Panel . . . . .	192
159. Reencipher CKDS . . . . .	192
160. Selecting the Change Master Key Option on the ICSF Master Key Management Panel . . . . .	193
161. Change Master Key Panel . . . . .	193
162. ICSF Selecting the Master Key Option on the Primary Menu Panel . . . . .	195
163. Selecting the Set Host Master Key Option on the ICSF Master Key Management Panel . . . . .	195
164. Selecting the Administrative Control Option on the ICSF Primary Menu Panel . . . . .	197
165. Disabling the PKA Callable Services . . . . .	198

166. Selecting the Administrative Control Option on the ICSF Primary Menu Panel . . . . .	198
167. Enabling and Disabling the PKA Callable Services . . . . .	199
168. Selecting the Reencipher PKDS Option on the Master Key Management Panel . . . . .	200
169. Reencipher PKDS . . . . .	200
I 170. Selecting the Refresh PKDS Option on the Master Key Management Panel. . . . .	201
171. Refresh PKDS . . . . .	201
172. ICSF Primary Menu Panel . . . . .	202
173. Coprocessor Management Panel . . . . .	202
174. Operational Key Load Panel . . . . .	202
175. Operational Key Load Panel . . . . .	203
176. Operational Key Load Panel - ENC-ZERO and CV values displayed . . . . .	203
177. Operational Key Load Panel - AES control vector values displayed . . . . .	204
178. ICSF Initialize a CKDS Panel . . . . .	204
179. Selecting the Master Key option on the primary menu panel . . . . .	205
180. ICSF Master Key Management Panel. . . . .	206
181. ICSF Initialize a CKDS Panel if AES master keys are supported . . . . .	206
182. ICSF Initialize a CKDS Panel . . . . .	207
183. Selecting the TKE Option on the ICSF Primary Menu Panel . . . . .	207
184. Selecting PKA Key entry on the TKE Processing Selection Panel . . . . .	207
185. PKA Direct Key Load . . . . .	208
186. CNM main window. . . . .	209
187. Passphrase logon prompt . . . . .	210
188. TKE smart card prompt . . . . .	210
189. PIN prompt . . . . .	210
190. Passphrase group logon - group member list . . . . .	210
191. Group logon prompt . . . . .	211
192. Passphrase group logon - enter passphrase prompt . . . . .	211
193. Passphrase group logon - member is ready for logon . . . . .	212
194. Passphrase group logon successful . . . . .	212
195. Smart card group logon window . . . . .	213
196. Smart card group logon — retry PIN prompt . . . . .	213
197. Smart card group logon window - member is ready for logon . . . . .	214
198. Smart card group logon successful. . . . .	214
199. CNM main window — Crypto Node Time sub-menu . . . . .	215
200. Current Coprocessor Clock . . . . .	215
201. Sync time with host window . . . . .	216
202. CNM main window — Access Control menu . . . . .	217
203. Role Management panel - list of roles loaded to the TKE crypto adapter for Smart Card . . . . .	218
204. Open a disk-stored role - choose a file . . . . .	219
205. Role Definition panel - role is displayed . . . . .	220
206. Edit a role - highlight access point to permit . . . . .	221
207. Edit a role - access point is moved to Permitted Operations column . . . . .	221
208. Profile management panel — profile list . . . . .	222
209. Profile Management panel — Passphrase profile . . . . .	223
210. Profile Management panel — Passphrase profile fields filled in . . . . .	225
211. Smart card profile — TKE smart card prompt . . . . .	226
212. Profile management panel — smart card profile . . . . .	226
213. Profile Management panel — smart card profile fields filled in . . . . .	227
214. Profile Management panel — Passphrase Group profile . . . . .	228
215. Profile Management panel — Smart Card Group profile filled in . . . . .	229
216. CNM main window — Master Key pull-down menu . . . . .	232
217. Clear New Master Key Register — confirm clearing . . . . .	232
218. Clear New Master Key Register — register cleared. . . . .	233
219. Load Master Key from Clear Parts . . . . .	233
220. Load Master Key from Clear Parts — key part randomly generated. . . . .	234
221. Load Master Key from Clear Parts — key part successfully loaded . . . . .	234

222. Smart Card Master Key Parts panel . . . . .	235
223. Smart Card Master Key Parts panel — key part description prompt . . . . .	236
224. Establishing a secure session between TKE crypto adapter and TKE smart card . . . . .	236
225. Generating key part to TKE smart card . . . . .	236
226. Smart Card Master Key Parts panel — key part generated to TKE smart card . . . . .	236
227. Master Key Part Smart Card panel — loading a Crypto Adapter key part from TKE smart card . . . . .	237
228. Establishing a secure session between Crypto Adapter and TKE smart card . . . . .	238
229. Loading key part from TKE smart card . . . . .	238
230. Master key part successfully loaded . . . . .	238
231. Master Key Verify sub-menu . . . . .	239
232. Master Key Register Verification panel - verification pattern is displayed . . . . .	240
233. Master Key Register VP compare successful . . . . .	240
234. CNM main window — Key Storage pull-down menu . . . . .	241
235. Key Storage Management Panel – key labels list . . . . .	242
236. CNM main menu — Smart Card pull-down menu . . . . .	243
237. Change PIN — insert TKE smart card prompt. . . . .	243
238. Change PIN — enter current PIN prompt . . . . .	244
239. Change PIN — enter new PIN prompt . . . . .	244
240. Generate Crypto Adapter Logon Key — insert TKE smart card . . . . .	244
241. Generate Crypto Adapter Logon Key — PIN prompt . . . . .	244
242. Generate Crypto Adapter Logon Key — User ID prompt . . . . .	245
243. Generate Crypto Adapter Logon Key — key generated . . . . .	245
244. Display Smart Card Details — insert TKE smart card prompt . . . . .	245
245. Display Smart Card Details — public information displayed . . . . .	246
246. Manage Smart Card contents — contents of TKE smart card are displayed . . . . .	247
247. Manage Smart Card contents — confirm delete prompt . . . . .	247
248. Manage Smart Card contents. . . . .	248
249. Copy Smart Card — insert source TKE smart card . . . . .	249
250. Copy Smart Card — insert target TKE smart card . . . . .	249
251. Copy Smart Card — TKE smart card key parts are displayed . . . . .	249
252. Copy Smart Card — highlight source objects to copy to target . . . . .	250
253. Copy Smart Card — source TKE smart card PIN prompt . . . . .	250
254. Copy Smart Card — target TKE smart card PIN prompt . . . . .	250
255. Establishing a secure session between source and target TKE smart cards . . . . .	250
256. Objects are copied to the target TKE smart card. . . . .	251
257. Copy Smart Card — objects are copied to the target container . . . . .	251
258. First screen of TKE Smart Card Utility Program (SCUP) . . . . .	254
259. Display of CA smart card and TKE smart card . . . . .	255
260. Display of smart card key identifiers . . . . .	257
261. First step for initialization and personalization of the CA smart card . . . . .	258
262. Zone key length window. . . . .	258
263. Message if card is not empty . . . . .	259
264. Initialization message for CA smart card . . . . .	259
265. Enter first PIN for CA smart card . . . . .	259
266. Enter second PIN twice for CA smart card . . . . .	260
267. Enter zone description for CA smart card . . . . .	260
268. Enter card description for CA smart card . . . . .	260
269. Building a CA smart card . . . . .	260
270. Begin creation of backup CA smart card . . . . .	261
271. Initialization of backup CA smart card . . . . .	261
272. Continue creation of backup CA smart card . . . . .	262
273. Establish secure connection for backup CA smart card . . . . .	262
274. Building backup CA smart card . . . . .	262
275. Select first CA PIN. . . . .	263
276. Initialize and enroll TKE smart card . . . . .	264
277. Initializing TKE smart card . . . . .	264

278. Building TKE smart card . . . . .	264
279. Personalizing TKE smart card . . . . .	265
280. View current zone for a TKE cryptographic adapter. . . . .	266
281. Select local zone . . . . .	266
282. Certifying request for local Crypto Adapter enrollment . . . . .	267
283. Message for successful Crypto Adapter enrollment . . . . .	267
284. View current zone after Crypto Adapter enrollment . . . . .	267
285. Remote Zone Key Length . . . . .	268
286. Remote Zone Key Length is 2048 . . . . .	268
287. Crypto Adapter Enrolled . . . . .	268
288. Save Enrollment Request . . . . .	269
289. Enrollment Request Stored . . . . .	269
290. Select remote zone . . . . .	270
291. Remote zone enrollment instructions . . . . .	270
292. Open enrollment request file . . . . .	271
293. Verification of enrollment request . . . . .	271
294. Save the enrollment certificate . . . . .	272
295. Continue with remote enrollment . . . . .	272
296. File Chooser Enroll Certificate . . . . .	273
297. Remote Enroll Success . . . . .	274
298. View current zone after Crypto Adapter enrollment . . . . .	274
299. Choosing secure key part entry from the domains keys panel . . . . .	275
300. Enter description panel for secure key part entry. . . . .	276
301. USER DEFINED operational key for secure key part entry . . . . .	276
302. Secure key part entry — enter TKE smart card into reader . . . . .	276
303. Secure key part entry — enter PIN. . . . .	277
304. Secure key part entry card identification . . . . .	277
305. Secure key part entry — enter PIN. . . . .	277
306. Secure key part entry — DES key part information for a master key . . . . .	278
307. Secure key part entry — AES key part information for a master key . . . . .	278
308. Secure key part entry — DES key part information for operational key. . . . .	278
309. Secure key part entry — message for successful execution. . . . .	278
310. An Example of TKE Host and TKE Target LPARs without Domain Sharing . . . . .	292
311. An Example of TKE Host and TKE Target LPARs with Domain Sharing . . . . .	292
I 312. Cryptographic Node Management Batch Initialization 4.1.0 Task Window. . . . .	293
313. Cryptographic Node Management Batch Initialization Task Output Window . . . . .	294
314. CLU Command Check Boxes. . . . .	295
315. CLU Error . . . . .	295
316. CLU View Menu . . . . .	296
317. Output Log file . . . . .	296
318. CLU Command History . . . . .	297
319. Successful Completion of CLU Commands. . . . .	297
320. CLU File Menu . . . . .	298
321. Edit TKE Files Task Window . . . . .	306
322. Editor - File menu items. . . . .	307
323. Editor - Edit menu items. . . . .	308
324. Editor - Style Menu Items . . . . .	309
I 325. Migrate to TKE Workstation 7.0 - Backup floppy prompt . . . . .	310
I 326. Migrate to TKE Workstation 7.0 - Data migration progress window . . . . .	310
327. TKE File Management Utility Task Window. . . . .	312
328. TKE File Management - Directory options . . . . .	312
329. Delete Confirmation Window . . . . .	313
330. Window for Inputting a Filename . . . . .	313
331. TKE Media Manager . . . . .	314
332. TKE Workstation Code Information window. . . . .	315
I 333. Configuration Migration Tasks panel . . . . .	317

334. Backup Critical Console Data Window . . . . .	323
335. Backup Console Data Progress window - in progress . . . . .	324
336. Backup Console Data Progress window - Success . . . . .	324
337. Change Password Task . . . . .	325
338. Change Password - Success . . . . .	325
339. Customize Scheduled Operations Task Window . . . . .	326
340. Customize Scheduled Operations - Add a Scheduled Operation window . . . . .	327
341. Customize Scheduled Operations - Set Date and Time window . . . . .	328
342. Customize Scheduled Operations - Set Repetition of operation . . . . .	329
343. Completion Window for Adding Scheduled Operation . . . . .	329
344. Customize Schedule Operations. . . . .	330
345. Details View of Scheduled Operation . . . . .	330
346. New Time Range window for Scheduled Operation . . . . .	331
347. Format Media Dialog . . . . .	332
I 348. Select Media Device . . . . .	333
349. Hardware Messages window . . . . .	334
350. Hardware Messages - Details Window . . . . .	335
351. Prompt for Password . . . . .	336
352. Prompt to Unlock Console . . . . .	336
353. Virtual RETAIN Data Offload Window . . . . .	337
354. Successful Offload of Data. . . . .	337
355. Virtual RETAIN Data Offload Incorrect Media Error . . . . .	338
356. Save Upgrade Window . . . . .	338
357. Save Upgrade Success Window. . . . .	339
358. Shutdown or Restart Task Window . . . . .	339
359. Confirmation Window . . . . .	340
360. Transmit Console Service Data . . . . .	340
361. Transmit Console Service Data Task Window for DVD-RAM . . . . .	341
362. Transmit Console Service Data - Successful completion . . . . .	342
363. Update Problem Number for Virtual RETAIN File. . . . .	342
364. Select the Virtual RETAIN Files . . . . .	343
365. Copying Data to Selected Media . . . . .	343
366. Users and Tasks Window . . . . .	344
367. View Console Events Window . . . . .	345
368. View Console Information Window . . . . .	346
369. Internal Code Change Details Window . . . . .	346
370. View Console Service History window . . . . .	347
371. Problem Summary . . . . .	348
372. Problem Analysis . . . . .	349
373. View Console Tasks Performed window . . . . .	350
374. View Licenses window . . . . .	351



## Tables

I	1. Applet version by TKE release . . . . .	16
I	2. CA smart card usage . . . . .	16
I	3. TKE smart card usage . . . . .	17
	4. Smart card task checklist . . . . .	21
	5. TKE management system task checklist . . . . .	59
	6. TKEUSER Role . . . . .	74
	7. TKEADM Role. . . . .	75
	8. KEYMAN1 Role . . . . .	76
	9. KEYMAN2 Role . . . . .	77
	10. DEFAULT Role . . . . .	77
	11. SCTKEUSR Role. . . . .	80
	12. SCTKEADM Role . . . . .	81
	13. DEFAULT Role . . . . .	82
	14. Key types and actions for the supported crypto modules . . . . .	141
	15. Decimal to Hexadecimal Conversion Table . . . . .	279
I	16. Callable service access control points. . . . .	284
	17. Tasks, applications and utilities accessible by console user name . . . . .	303
I	18. Allowable labels when formatting DVD-RAM or USB flash memory drive . . . . .	332





---

## About this information

This information introduces Version 7.0 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 7.0 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 7.0.

Chapter 4, "TKE Setup and Customization," provides information on using TCP/IP and on the host files needed by TKE. It also explains how to configure the TKE workstation for TCP/IP and initialize the TKE workstation.

Chapter 5, "TKE Up and Running," provides preliminary setup and initialization tasks that are necessary for operation.

Chapter 6, "Main Window," explains the beginning window of the TKE program and the functions and utilities accessible from it.

Chapter 7, "Crypto Module Notebook," explains how to work with crypto modules. The status of the master keys and key parts are displayed. This window is where

the keys can be generated, loaded and cleared. The domain controls are set here. The zeroize domain function is accessed from here. RSA handling is described here.

Chapter 8, “Auditing,” provides information on auditing.

Chapter 9, “Managing Keys,” explains how ICSF is used when loading and importing keys to a CEX2C or CEX3C on an IBM System z9, IBM System z10, or IBM zEnterprise 196.

Chapter 10, “Cryptographic Node Management Utility (CNM),” provides information on the CNM utility tasks.

Chapter 11, “Smart Card Utility Program (SCUP),” provides information on the SCUP tasks.

Appendix A, “Secure Key Part Entry,” provides information on secure entry of a known key part onto a TKE smart card.

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

Appendix C, “LPAR Considerations,” discusses host setup considerations for managing CEX2Cs and CEX3Cs across multiple logical partitions.

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

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

Appendix F, “Trusted Key Entry Applications and Utilities,” provides information on TKE console applications and utilities and Service Management tasks.

Appendix G, “TKE Best Practices,” provides information on Checklists for Loading a TKE Machine for both passphrase and smart card.

Appendix H, “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.

---

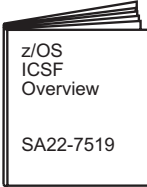

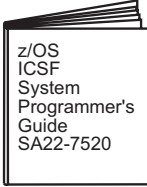
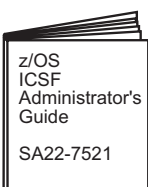

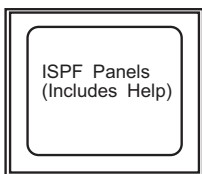
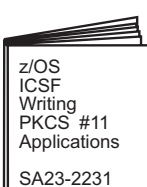
## Where to find more information

The information in this book is supported by other books in the ICSF/MVS library and other system libraries.

## Related Publications

- *z/OS Cryptographic Services ICSF Administrator's Guide*
- *z/OS Cryptographic Services ICSF System Programmer's Guide*
- *System z Service Guide for Trusted Key Entry Workstations*, GC28-6901
- *PR/SM Planning Guide*, SB10-7153

# ICSF Publications

Tasks		Tasks	
	Evaluating Planning		Administrating Application Programming Diagnosis Operating
	Customizing Diagnosis Installing Operating		Administrating
	Application Programming		Administrating
	Application Programming		

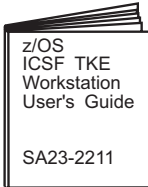

Optional Features			
	Available with the Trusted Key Entry Workstation (TKE Version 7)		The ICSF Library, Trusted Key Entry Workstation User's Guide and Encryption Facility for z/OS Planning and Customizing are included on the IBM Online Library: z/OS Collection Kit SK3T-4269

Figure 1. ICSF Library



---

# Summary of Changes

## **Summary of Changes for SA23-2211-06 z/OS Version 1 Release 12**

This book contains information previously presented in *z/OS Cryptographic Services ICSF TKE PCIX Workstation User's Guide*, SA23-2211-05, which supports z/OS Version 1 Release 11.

### **New information**

- Improved tools to capture host crypto adapter configuration data – including roles, authorities, domain control settings, and master keys -- securely to a file, and re-apply the data to another host crypto module or crypto module group. These tools simplify the task of installing new or replacement host crypto adapters, and can be used for backup and disaster recovery as well. See “Configuration Migration” on page 315 for more information on migration wizard tools.
- New utility for sending TKE workstation security audit records to a System z host, where they will be saved in the z/OS System Management Facilities (SMF) dataset. For more information, refer to “TKE Audit Record Upload Configuration Utility” on page 183.
- Support for IBM zEnterprise 196 (z196) hardware.
- Support for AES master keys and operational keys.
- Support for ECC master keys.
- Ability to save key parts, backup data, and other files to a USB flash memory drive.
- New access control points described in Appendix B, “Access Control Points and Callable Services,” on page 281.

### **Changed Information**

- DataKey smart cards no longer supported. You should back up your DataKey CA smart cards, and make copies of your DataKey TKE smart cards, using NXP JCOP 4.1 smart cards. Copying a DataKey smart card is the only action still supported. See “Copy Smart Card” on page 248
- A TKE smart card initialized using TKE 7.0 (applet version 0.6) is now protected by a 6-digit PIN. Smart cards initialized on earlier versions of TKE are protected by a 4-digit PIN.
- Stronger passphrase requirements for the TKE workstation crypto adapter logon passphrase profiles.

## **Summary of Changes for SA23-2211-05 z/OS Version 1 Release 11**

This book contains information previously presented in *z/OS Cryptographic Services ICSF TKE PCIX Workstation User's Guide*, SA23-2211-04, which supports z/OS Version 1 Release 10.

### **New information**

- Crypto Express3 Coprocessor (CEX3C) support.

- New access control points described in Appendix B, “Access Control Points and Callable Services,” on page 281.
- New utility for saving and restoring crypto adapter configuration data described in “Migrate IBM Host Crypto Module Public Configuration Data” on page 316.
- Added support for grouping of domains. This support enables you to perform operations on a set of crypto module domains as you would a single crypto module domain.
- Enhanced zone certificate length.

#### **Changed Information**

- Removed information on CCF and PCICC. TKE V5.3 and later do not support the CCF and PCICC.

#### **Summary of Changes for SA23-2211-04 z/OS Version 1 Release 10**

This book contains information previously presented in *z/OS Cryptographic Services ICSF TKE PCIX Workstation User's Guide*, SA23-2211-03, which supports z/OS Version 1 Release 9.

#### **New information**

- ADMIN user name
- AUDITOR user name
- Audit configuration utility
- Audit logging of TKE workstation activity
- Support for USB (OmniKey) smart card readers
- Support for IBM System z10 BC
- Support for AES master keys and operational keys

#### **Changed Information**

- Panel changes for support of the AES master key, AES operational keys and SHA-256 Hash
- TKE V5.3 does not support the CCF and PCICC.

#### **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 IBM 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.





---

## 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 (PINs). Cryptographic systems use cryptographic keys. A cryptographic key instructs the cryptographic function in its operation. The security of the cryptographic service and its results depend on safeguarding the cryptographic keys.

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

Trusted Key Entry (TKE) is an optional 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 z10, or z196 and zSeries hardware and software.

### Supported Host Cryptographic Cards

The supported host cryptographic cards for TKE 7.0 are:

- the Crypto Express2 Coprocessor (CEX2C)
- the Crypto Express3 Coprocessor (CEX3C)

The Crypto Express3 Coprocessor (CEX3C) is available on z10 and z196 servers with feature code 0864. Feature code 3863 for CP Assist for Cryptographic Functions is a prerequisite. To administer a CEX3C card on a z10 or z196, you must have ICSF FMID HCR7770 or later installed.

The Crypto Express2 Coprocessor (CEX2C) is available on z10 and z196 servers with feature code 0863. Feature code 3863 for CP Assist for Cryptographic Functions is a prerequisite.

**Note:** Secure AES keys are only supported on a CEX2C running on a z10 server, or on a CEX3C running on a z10 or z196 server with IBM Cryptographic Coprocessor Support Program with the November, 2008 or later licensed internal code (LIC).

### TKE Hardware

- TKE Workstation
- IBM 4765 Cryptographic adapter

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

### Optional TKE Features

Also available with a TKE 7.0 workstation are:

- Feature 0885: 2 OmniKey smart card readers and 20 NXP smart cards
- Feature 0884: 10 NXP smart cards

#### Notes:

1. OmniKey smart card readers require TKE 5.3 or higher code - FC 0854 with the November, 2008 or later licensed internal code (LIC).
2. Kobil smart card readers are not supported and not usable with TKE 7.0 or later.
3. DataKey smart cards are no longer usable with TKE 7.0.
4. Older smart cards must be reinitialized on TKE 7.0 or later to be able to store ECC master keys.
5. TKE 7.0 requires the new TKE workstation, FC 0841. TKE 7.0 requires the IBM 4765 Cryptographic adapter. Previous TKE workstations do not support the IBM 4765 Cryptographic Adapter.

## TKE Software

This software is preinstalled on the TKE workstation:

- IBM Cryptographic Coprocessor Support Program Release 4.10.
- Trusted Key Entry Version 7.0 - FC 0860

#### Notes:

1. TKE software should not be changed without instructions from IBM Service.
2. TKE 6.0 software, FC 0858, can only be installed on TKE workstations FC 0859, FC 0839, or FC 0840.
3. TKE 7.0 software, FC 0860, can only be installed on a TKE 7.0 workstation, FC 0841 or greater.

---

## 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, AES, ECC, 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 panels are used to load operational keys from key part registers, set the master

key, and 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 and the PKDS (PKA Cryptographic Key Data Set) can be initialized, reenciphered and refreshed.

---

## Supported Host Cryptographic Card Features

The host cryptographic cards supported with TKE 7.0 are the Crypto Express2 Coprocessor (CEX2C) and the Crypto Express3 Coprocessor (CEX3C). These host cryptographic cards:

- provide a secure processing environment with hardware to provide DES, AES, TDES, RSA, SHA-1 and SHA-256 cryptographic services with the IBM Common Cryptographic Architecture (CCA) secure key management and finance-industry special function support.
- perform random number generation and modular math functions for RSA and similar public-key cryptographic algorithms.
- include sensors to protect against attacks involving probe penetration, power sequencing, radiation and temperature manipulation.

**Note:** Secure AES keys are only supported on a CEX2C running on z10 servers, or on a CEX3C running on a z10 or z196 server with the November, 2008 or later licensed internal code (LIC).

To use TKE with z10 and z196 systems, you must have at least one supported host cryptographic card on your system.

## Host Crypto Module

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

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

- **Crypto-Module ID (CMID)**  
This is a unique 8-byte character string generated for each host crypto module. The CMID is returned in all reply messages sent by the host crypto module to the TKE workstation.
- **RSA Key**  
This is a unique RSA key generated for each host crypto module. The public modulus part of this RSA key is called the crypto-module public modulus (CMPM). For the CEX2C, this is a 1024-bit key. For the CEX3C, this is a 4096-bit key.

---

## 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.

**Host 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 (0-15).

**Authority**

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

**Role** 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 host 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 host 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 host crypto module using the public RSA key of the authority previously loaded into the host crypto module.

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

All administration of host crypto modules is done with authorities. An authority is identified to the host crypto module by the *authority index*. There are up to 100 authorities for each supported host 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 host 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 host crypto modules. This will give each authority the ability to update all host crypto modules on the system after loading their signature key. If an authority has a different index on each host 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 to create crypto module groups or domain groups, then everything relating to the host crypto modules (authority index, authority signature keys, signing requirements, roles, etc) within the group needs to be the same.

**Authority Signature Key**

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

Prior to signing and verifying command signatures, the signature key pair must be generated and the public key sent to the host crypto module. All authorities have a public exponent value of 65537.

1024-bit, 2048-bit, and 4096-bit authority signature keys can be saved to key storage or binary files. 1024-bit and 2048-bit authority signature keys can be saved to smart cards. The CEX2C does not support authority signature keys greater than 1024-bits.

### **Authority Default Signature Key**

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

The length of the default signature key is 1024-bits.

For the CEX2C and CEX3C, 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 host crypto module are signed by a signature key. This signature key is associated with a signature key certificate containing the public component of an RSA key pair. This certificate is part of a certificate chain leading to the Card Class certificate. The Card Class certificate is signed by the crypto card device private key, which is loaded into the host crypto module during the manufacturing process.

When the host crypto module is first opened, the certificate chain is validated by the TKE. Once the certificate chain is validated, TKE uses the public modulus within the signature key certificate to validate all signed replies from the host crypto module.

## **Multi-Signature Commands**

All commands to the host 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.

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

- Clear old symmetric DES or AES master key register
- Clear old asymmetric master key register
- Load / combine new symmetric DES or AES master key parts
- Clear new symmetric DES or AES master key register
- Load / combine new asymmetric master key parts
- Clear new asymmetric master key register
- Set new asymmetric master key
- Clear old ECC master key
- Clear new ECC master key
- Load / combine new ECC master key parts
- Disable crypto module

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

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

The single signature commands for operational keys:

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

## Access Control

The access control for the supported crypto modules is based on roles. Each authority is assigned a role. The role definition specifies which of the 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 transport key between the workstation and the host crypto module. One or more key parts can then be encrypted under the transport key.

## Domain Controls

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

---

## TKE Operational Considerations

On a z10 EC and z10 BC, you must have at least one CEX2C or CEX3C for TKE usage. On the z196, you must have at least one CEX3C 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 Crypto Express2 Coprocessor (CEX2C) and Crypto Express3 Coprocessor (CEX3C). These supported crypto modules 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 C, “LPAR Considerations,” on page 291.

## Multiple Hosts

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

## Multiple Workstations

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

---

## TKE Enablement

If you have a z10 or z196 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 host crypto modules 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 host crypto module.



If TKE commands are not permitted on the Support Element, the following 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 supported host cryptographic cards 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.

---

## Trusted Key Entry Console

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

Most tasks require an additional logon to the TKE Workstation Crypto Adapter. You log on with your workstation crypto adapter profile. The profile is defined for your workstation when TKE is configured and customized. See “Define a User Profile” on page 222 for more information.

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

- TKEUSER -- default console user name.
- ADMIN -- provides access to administrative functions, such as migration utilities, the code load utility, and the crypto adapter initialization utility.
- AUDITOR -- provides access to audit functions, such as the Audit Configuration Utility, the Audit Record Upload Configuration Utility, and utilities to view and archive security logs.
- SERVICE -- provides access to service functions, such as managing the console code level, setting the date and time, and saving upgrade data.

Appendix F, “Trusted Key Entry Applications and Utilities,” on page 303 describes the applications and utilities available to each console user name.

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



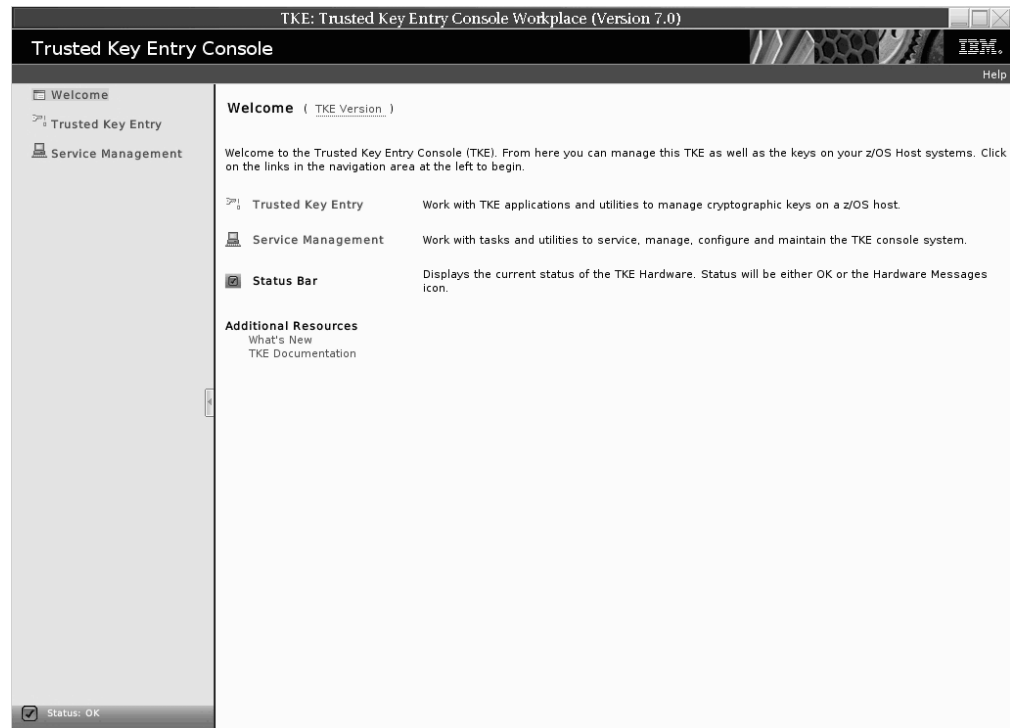


Figure 2. TKE Console - initial panel

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

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

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

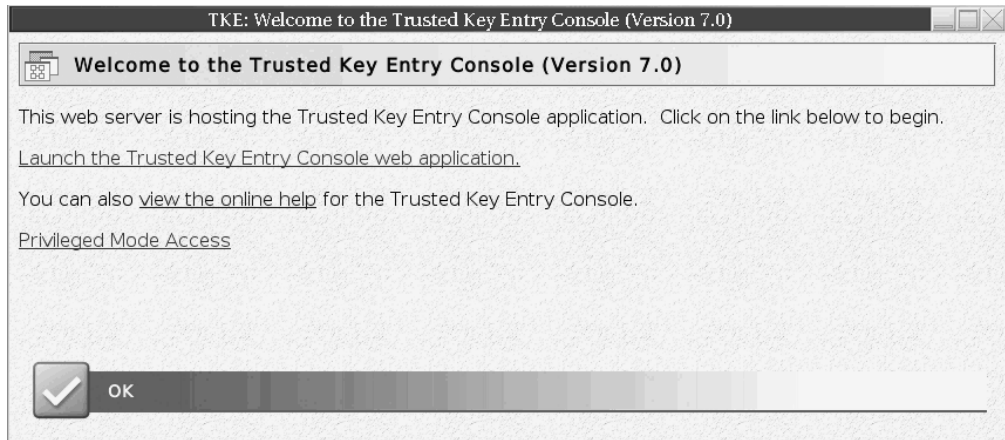


Figure 3. TKE Console - pre-login panel

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

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

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

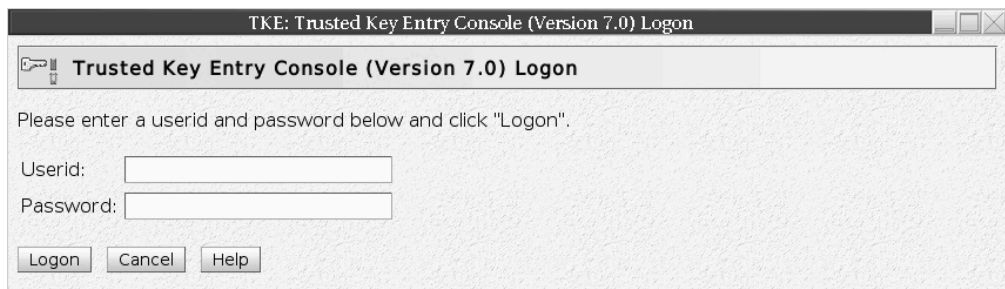


Figure 4. Log on with other console user names

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

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

After logging on with the new user name, an initial panel appears. In the upper right hand corner, to the left of the word Help, the user name is displayed. When logged on as TKEUSER, no user name is displayed. This initial panel provides access to applications and utilities when you are using a console user name. It is identical to the TKEUSER initial panel with the same options:

- Clicking on **Trusted Key Entry** provides access to the applications and utilities available with the console user name you used to log on.
- Clicking on **Service Management** provides access to service functions available with the console user name you used to log on.

- Clicking on **Status Bar** displays the current status of the TKE Hardware.
- Clicking on **TKE Documentation** provides access to a version of this document on the TKE workstation.

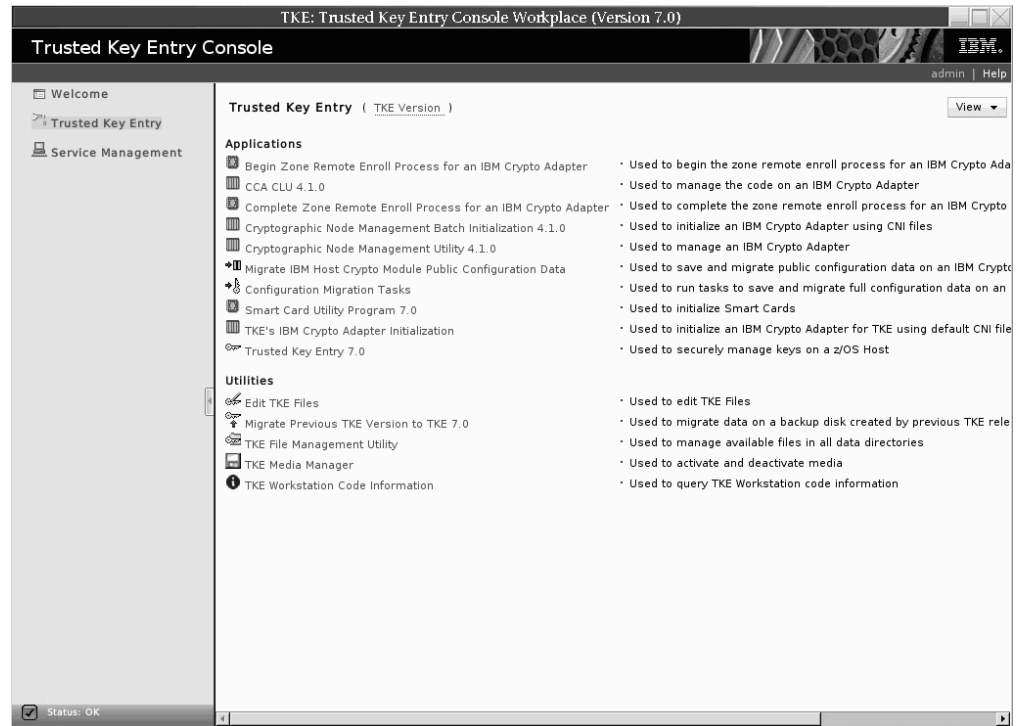


Figure 5. Trusted Key Entry for ADMIN - categorized

After logging in the first time, it is recommended that you change the password with the Change Password task. See “Change Password” on page 325.

## Trusted Key Entry Console Navigation

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

There are three presentation options:

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

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

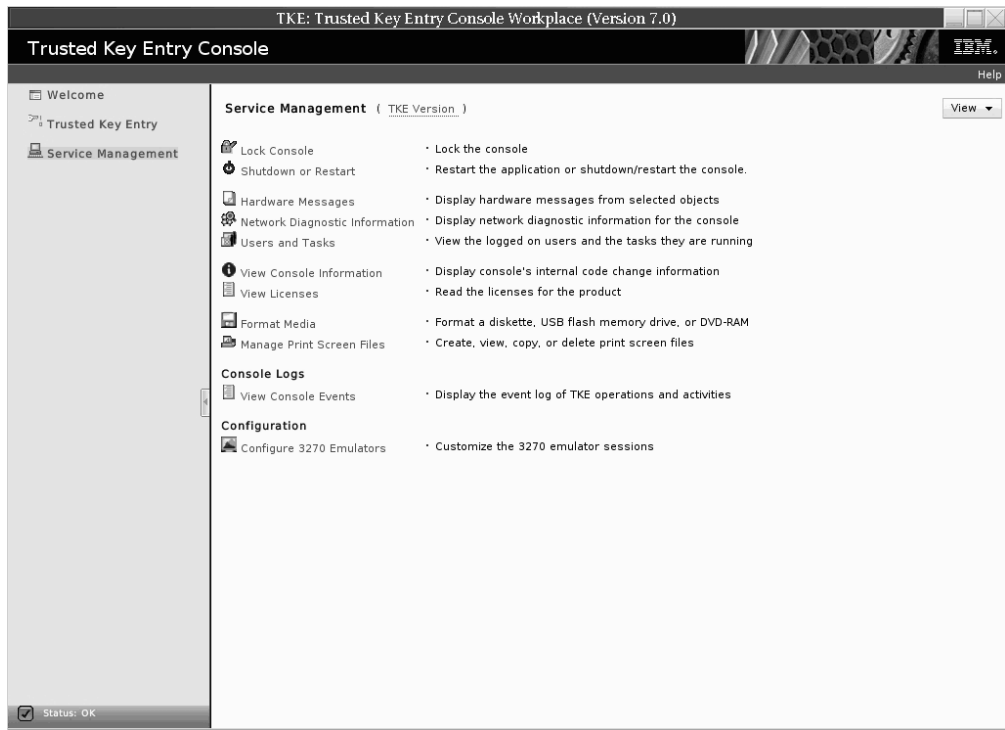


Figure 6. Service Management for TKEUSER (Categorized)

---

## Chapter 2. Using Smart Cards with TKE

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

Smart Card support gives the user the ability to keep all key parts, authority 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 Readers. For TKE 7.0, only OmniKey smart card readers are supported.
- TKE workstation with an IBM cryptographic adapter.

**Note:** The 4765 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 V7.0, the 4.10 level of the licensed internal code (LIC) is required for segments 2 and 3.

The TKE 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 workstation crypto adapter. See Chapter 10, “Cryptographic Node Management Utility (CNM),” on page 209.

### CNI

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

### 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. Two OmniKey readers need to be attached.

**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 Chapter 11, "Smart Card Utility Program (SCUP)," on page 253.

**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 18.

**Entity**

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

**Group Logon**

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

**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 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 6-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 OmniKey smart card reader

**Note:** Beginning with TKE 7.0, Omnikey smart card readers are the only supported smart card reader type.

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

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

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

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

When prompted to insert a TKE smart card, push the smart card all the way in until the right side of the reader displays a solid colored box. If a blank box displays, you have not inserted the smart card correctly.

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

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

The other buttons on the PIN pad are not operational.

## Smart Card Compatibility Issues

Features added in recent TKE releases (such as AES key support added in TKE V5.3, 2048-bit RSA key support added in TKE V6.0, and ECC and increased PIN length support added in TKE 7.0) have required changes to the CA and TKE smart card applets. Because of these changes, there are restrictions on which smart cards can be used with a particular TKE release.

### Applet Version

When a new TKE or CA smart card is created, an applet is loaded onto the smart card. This occurs when initializing and enrolling a TKE smart card in a zone, when initializing and personalizing a CA smart card, and when creating a backup CA smart card. The applet version depends on the TKE release as shown in the following table.

Table 1. Applet version by TKE release

	CA Smart Card	TKE Smart Card
TKE 5.2 or before	applet version = 0.3	applet version = 0.3
TKE 5.3	applet version = 0.3	applet version = 0.4
TKE 6.0	applet version = 0.4	applet version = 0.5
TKE 7.0	applet version = 0.4	applet version = 0.6

In general, smart cards created on a particular TKE release cannot be used on TKE workstations that are at prior release levels. TKE 5.2 applets are not usable on TKE 7.0 because they can only be installed on DataKey smart cards, and DataKey smart cards are not supported.

## Zone Key Length

Beginning in TKE V6.0, users can select the length of the RSA keys used to establish secure communication within a zone. The zone key length is selected when initializing and personalizing a CA smart card. This zone key length is used for any TKE smart cards created in the zone and any TKE workstations enrolled in the zone. Key lengths of 1024-bits and 2048-bits are allowed.

Prior to TKE V6.0, the zone key length is 1024-bits. For smart cards, the zone key length can be displayed using the Smart Card Utility Program.

## Smart Card Usage

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

Table 2. CA smart card usage

	Use on TKE 5.2 or before	Use on TKE 5.3	Use on TKE 6.0	Use on TKE 7.0
Created on TKE 5.2 or before	Yes	Yes	Yes	No
Created on TKE 5.3	No	Yes	Yes	Yes <sup>1</sup>
Created on TKE 6.0, 1024-bit zone key	No	Yes	Yes	Yes <sup>1</sup>
Created on TKE 6.0, 2048-bit zone key	No	No	Yes	Yes
Created on TKE 7.0	No	No	No	Yes

<sup>1</sup> Only CA smart cards created with these releases that are NXP cards work for TKE 7.0. Datakey cards are not supported in TKE 7.0

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



authority signature key or crypto adapter logon key on the smart card. The authority signature key and the crypto adapter logon key are not subject to zone constraints.

Table 3. TKE smart card usage

	Use on TKE 5.2 or before	Use on TKE 5.3	Use on TKE 6.0	Use on TKE 7.0
Created on TKE 5.2 or before	Yes	Yes	Yes	No
Created on TKE 5.3	No	Yes	Yes	Yes <sup>2</sup>
Created on TKE 6.0, 1024-bit zone key	No	Yes <sup>1</sup>	Yes	Yes <sup>2</sup>
Created on TKE 6.0, 2048-bit zone key	No	No	Yes	Yes
Created on TKE 7.0	No	No	No	Yes
<sup>1</sup> 2048-bit TKE authority keys created on TKE 6.0 cannot be used on TKE 5.3. 2048-bit cryptographic adapter logon keys created on TKE 6.0 cannot be used on TKE 5.3. The size of a cryptographic adapter logon key created on TKE 6.0 depends on the type of smart card and smart card reader used (2048-bits for NXP JCOP 4.1 and OmniKey, 1024-bits otherwise).				
<sup>2</sup> Only TKE smart cards generated on NXP cards will work with TKE 7.0.				

## NXP Smart Cards Required for TKE 7.0

Beginning with TKE 7.0, NXP JCOP 4.1 smart cards must be used for all operations on the TKE workstation. DataKey smart cards are no longer supported.

The only operations on the TKE 7.0 workstation that permit the use of DataKey smart cards are creating a backup CA smart card and copying the contents of a TKE smart card. DataKey smart cards can be used as the source card for these operations.

You can back up CA smart cards using the Smart Card Utility Program.

To make a copy of a TKE smart card, take the following steps:

1. Using the Smart Card Utility Program, initialize and enroll a new TKE smart card in the same zone as the TKE smart card you want to copy.
2. Using the Smart Card Utility Program, personalize the new TKE smart card (set the card description and PIN).
3. Using the Cryptographic Node Management Utility, copy all keys from the original TKE smart card to the new TKE smart card.

---

## Zone Concepts

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

These are members of a zone:

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

A member of a zone is 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 key, TKE authority signature key) do not check the zone ID of the TKE smart card against the zone ID of the TKE workstation crypto adapter. In other words, a TKE smart card from a different zone may be used to logon to the TKE workstation crypto adapter in another zone, but the key parts on the TKE smart card cannot be exchanged in this zone (because the TKE smart card is enrolled in another zone).

## Authentication and Secure Communication

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

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

## Zone creation

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

### CA Smart Cards

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

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

### Zone description

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

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

### Zone identifier (ID)

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

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

## Multiple zones

It may be desirable to 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.

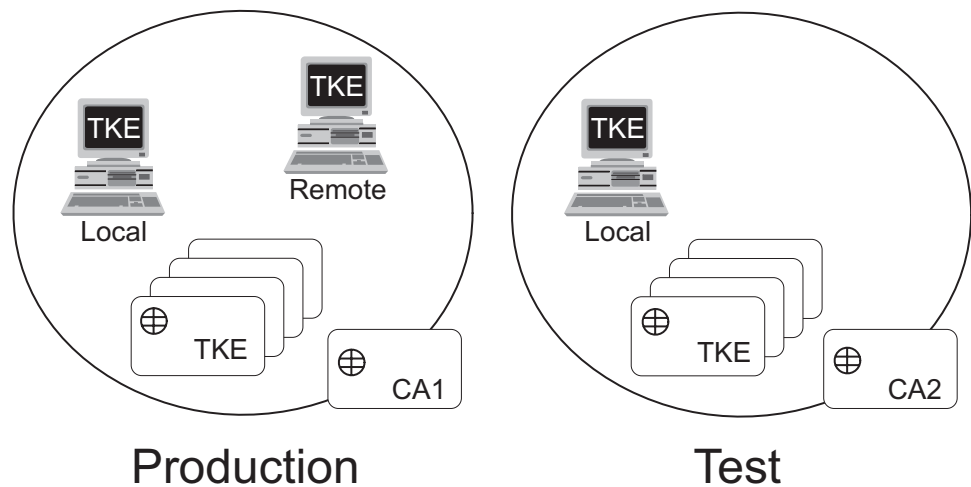


Figure 7. Multiple zones

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 workstation crypto adapters
- TKE smart cards

For TKE workstation crypto 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. The root certificate is then used to verify other entities enrolled in the same zone.

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

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

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

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. TKE crypto adapter logon keys generated on TKE 7.0 are 2048-bits long. TKE crypto adapter logon keys generated on earlier versions of the TKE workstation may be 1024-bits long.
- One authority signature key. When generating an authority signature key and saving it to a smart card, you can select whether the key size is 1024-bits or 2048-bits.

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

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

The zone environment is the primary security feature of the TKE smart cards (not the PIN). Even if an attacker gets access to several TKE smart cards containing all key parts for a certain key and manages to get access to the PIN's of those smart cards, there will not be any access to the key parts. The TKE smart card will only export its key parts to other entities in the same zone and the key parts will always be encrypted during such transfers.

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

### 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.

### Notes:

1. This setup is done in conjunction with Table 5 on page 59. The tasks defined here replace task 9: *Customize the TKE cryptographic adapter card*.
2. You must be logged in as ADMIN for this task.

Table 4. Smart card task checklist

TASK	RESPONSIBLE	WHERE	COMPLETED
1. Attach the smart card readers	IBM CE	TKE workstation	
2. Initialize the TKE workstation crypto adapter for smart card use; see "Initializing TKE for smart cards" on page 77.	TKE Administrator	TKE workstation	
3. Create CA smart card (zone); see "Initialize and personalize the CA smart card" on page 258.	TKE Administrator	TKE workstation	
4. Backup the CA smart card; see "Backup a CA smart card" on page 261.	TKE Administrator	TKE workstation	
5. Initialize and enroll TKE smart cards into the zone; see "Initialize and enroll a TKE smart card" on page 263.	TKE Administrator	TKE workstation	
6. Personalize TKE smart cards; see "Personalize a TKE smart card" on page 264.	TKE Administrator	TKE workstation	
7. Enroll the local TKE workstation crypto adapter (and any remote TKE cryptographic adapters) in the zone; see "Enroll a TKE cryptographic adapter" on page 265.	TKE Administrator	TKE workstation	
8. CNM utility - generate TKE crypto adapter logon keys; define and load profiles; reset default role. see Chapter 10, "Cryptographic Node Management Utility (CNM)," on page 209.	TKE Administrator	TKE workstation	



## Chapter 3. Migration

### Migrating from TKE Version 2.0 to TKE Version 7.0

This migration includes both hardware and software. You now have a new TKE workstation with TKE V7.0 installed and a new TKE workstation cryptographic adapter.

There are no migration tools provided for migrating to TKE V7.0. Personal Security Cards (PSCs) available with TKE V2.0 are NOT usable on TKE V7.0. Because there are no tools provided for migration to the TKE V7.0, you must consider the impact on these and perform the appropriate actions described.

TKE V7.0 cannot manage any of the same host servers that TKE V2.0 can manage. For this reason, this section will discuss only how to migrate key material from TKE V2.0 to TKE V7.0.

- **Host Definitions**

The TKE V2.0 Host Definitions are APPC connections. TKE V7.0 cannot manage any of the same host servers that TKE 2.0 can manage.

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

TKE V7.0 cannot manage any of the same host servers that TKE 2.0 can manage.

- **Authority Signature Keys on PSCs**

Authority signature keys saved on PSCs from TKE V2.0 are NOT usable with TKE V7.0. Before operating TKE V7.0, the TKE V2.0 user must do ONE of the following:

1. **Binary File:** If you will be using binary files for TKE V7.0 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 public modulus (PM). From the authority administration window, create a new authority and choose the authority signature key you just created to be used with this authority. If this is a CCF crypto module, select change authority and choose the authority signature key you just created. Send the updated authority 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 V7.0 workstation.
2. **Smart Cards:** If you will be using the TKE V7.0 Smart Cards for TKE V7.0 authority signature keys:
  - Change the signature requirements so that signature keys stored on TKE V2.0 PSCs are not required. From the Crypto Module window, update the appropriate commands with the new signature requirements. Remove any authority whose authority signature key was stored on TKE V2.0 PSCs. If you do not have at least one authority signature key available that uses either a default key (other than authorities 14 or 15) or an authority signature key saved to binary file, generate and load a new authority signature key to the host using a binary file as in **Authority Signature Keys on PSCs**.
  - From TKE V7.0, using a default authority signature key or an authority signature key saved to a binary file, generate and load new authority signature keys to the host. From the Authorities Page of the Crypto Module Notebook, generate a new authority signature key and save it to a

TKE V7.0 smart card that has been initialized and personalized. Get the authority signature key. Send the updated authority signature key to the host. Repeat for all authorities that will be using authority 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 authority 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 7, “Crypto Module Notebook,” on page 123.

- **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 V2.0 4755 key storage to key storage on the TKE V7.0 workstation crypto adapter. 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 V2.0 workstation key storage to the TKE V7.0 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 V7.0 workstation. Follow this process for operational key parts:

- **Master and Operational Key Parts**

- **Saving key parts to binary files on TKE V2.0 hard drive**

- Copy files to diskette
- Restore diskette files to the hard drive of the new TKE V7.0 workstation using the TKE File Management Utility. See “TKE File Management Utility” on page 311.

- **Entering key parts via the keyboard**

- Enter the key parts on the TKE V7.0 keyboard
- If the user wants the known key part values to be saved to a TKE V7.0 TKE smart card, see Appendix A, “Secure Key Part Entry,” on page 275 for details.

- **Saving key parts on TKE V2.0 PSCs**

Master and operational key parts stored on TKE V2.0 PSCs are NOT usable on TKE V6.0. The data blocks on the PSCs must be copied to binary files using the TSS HIKM utility. The utility is executed on the TKE V2.0 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 the hard drive of the new TKE V7.0 workstation using the TKE File Management Utility. See "TKE File Management Utility" on page 311.

---

## Migrating from TKE Version 3.X or 4.X to TKE Version 7.0

TKE Version 7.0 continues to allow you to manage any CEX2C/CEX3Cs inside your z10 EC and z10 BC. Older host crypto modules and machines are unsupported by TKE 7.0 and will require you keep your older TKE to manage those host crypto modules. Migration to TKE V7.0 requires a new TKE workstation and a new TKE Workstation cryptographic adapter.

**Note:** This process will require a USB floppy drive for the TKE 7.0 workstation.

## 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.

Perform the following tasks on the existing TKE V3.X or 4.X workstation.

1. Insert the TKEWS Backup diskette into the TKE disk drive.
2. Minimize all windows until only the OS/2 Workplace is displayed.
3. Open the TKE Backup icon on the OS/2 Workplace.
4. 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.
5. 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 7), exit the OS/2 window.
6. After the backup is completed and any user defined roles and profiles have been copied, remove the TKEWS Backup diskette for use on TKE V7.0.
7. 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 you have 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 V7.0.
- e. Exit the OS/2 window.

## TKE Started Task

### For TKE V3.0, 3.1, 4.0, 4.1 and 4.2 customers only

**Note:** If your host system is being converted from a z900 to z10 EC or z/10 BC, the TKE V3.0, V3.1 V4.0, V4.1 and V4.2 TKECM data set is not compatible with TKE V7.0. If you plan to use the same data set name for TKE V7.0 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 60.

## Set the Workstation Clock

Perform this task on the TKE V7.0 workstation.

You must be logged in as the ADMIN console user in order to set the time.

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. Click on either **Customize Date and Time** or **Configure NTP Settings** and set the time and date. For additional details see “Customize Console Date/Time” on page 69.

## 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 V7.0 hard drive, copy the files using the TKE File Management Utility.

Perform this task on the TKE V7.0 workstation.

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. TKE workstation crypto adapter Master Key parts should be copied to the CNM Data Directory.
5. Exit the File Management Utility. Click on File, then Exit and Logoff.

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 311 and “TKE Media Manager” on page 313.

## Passphrase and Smart Card Setup

TKE V7.0 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. You should choose only one of the sets of setup instructions based on a particular migration scenario.

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

## Passphrase Setup

Perform this task on the TKE V7.0 workstation.

In order to initialize the TKE workstation crypto adapter you must be logged in as the ADMIN console user.

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 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 Workstation Crypto Adapter” on page 69 for additional details.
2. Load Known Master Key Parts to the TKE workstation crypto adapter.
 

To be able to use migrated DES and PKA Key Storages, you must load the TKE workstation crypto adapter master key parts from your previous TKE workstation to the TKE V7.0 workstation as follows:

  - a. In the right frame of the Trusted Key Entry Console, click on **Cryptographic Node Management Utility 4.1.0**.
  - b. The crypto adapter logon window appears. Select **Passphrase logon** and logon as KEYMAN1.
  - c. Load the First known TKE workstation crypto 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 the 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 to KEYMAN2. Select File -> Exit and Logoff.
  - e. Open the Cryptographic Node Management Utility 4.1.0 again. The crypto adapter logon window appears.
  - f. Select **Passphrase Logon**. Logon as KEYMAN2.
  - g. Load the Middle and Last known TKE workstation crypto 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 the 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.
- h. Set the TKE workstation crypto adapter master key. (Select: Master Key => Set).
  - i. Exit and logoff CNM.

For additional details on loading TKE workstation crypto adapter master key parts, see "Loading a new master key from clear key parts" on page 233.

### 3. Migrate Previous TKE Version to TKE V7.0.

Execute the Migrate Previous TKE Version to TKE V7.0 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 V7.0 workstation.

- a. In the right frame of the Trusted Key Entry Console, click on Migrate Previous TKE Version to TKE V7.0.

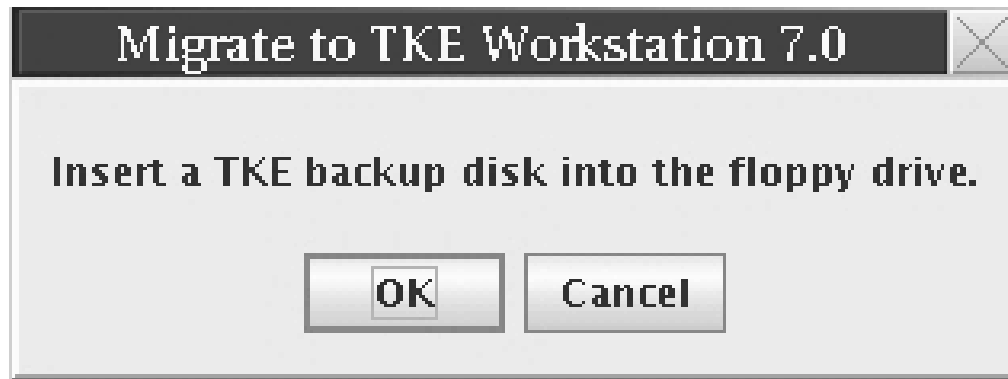


Figure 8. Migrate Previous TKE Version to TKE V7.0.

- 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.

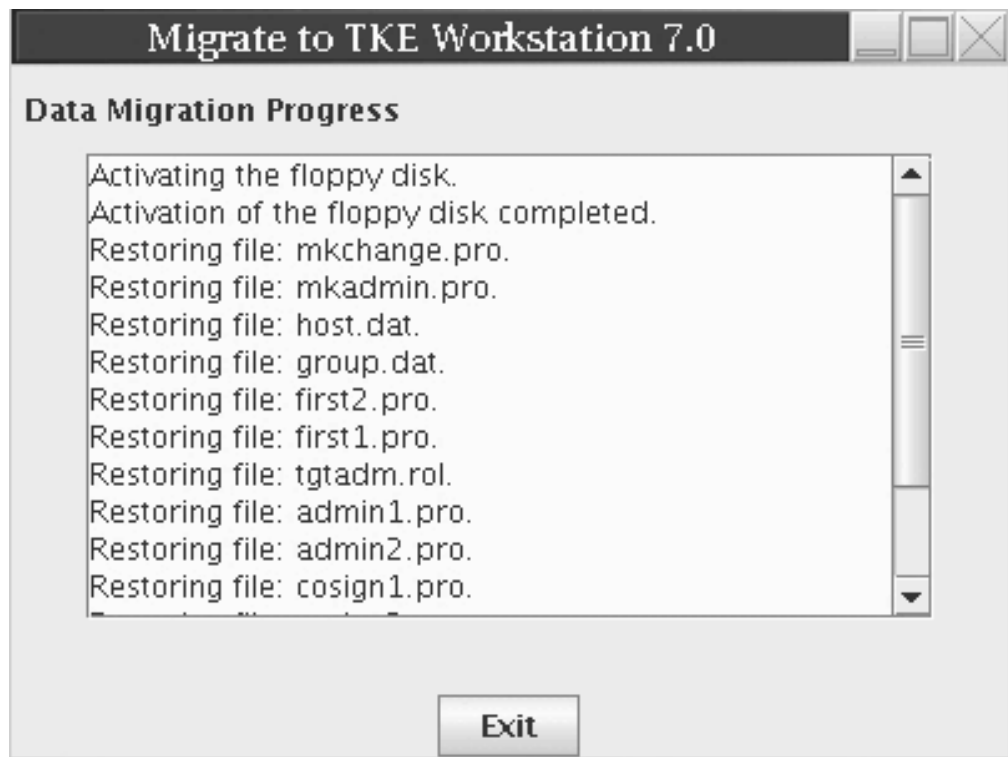


Figure 9. Data Migration Progress Panel

- 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 7.0” on page 309 for details.

4. Reinitialize 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 7.0.
  - a. In the right frame of the Trusted Key Entry Console, click on **Cryptographic Node Management Utility 4.1.0**.
  - b. The crypto adapter logon window appears. Select **Passphrase logon** and logon as 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 and logoff CNM.
5. Load User Defined Roles and Profiles to the TKE workstation crypto 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 4.1.0**.
  - b. The crypto adapter logon window appears. Select **Passphrase logon** and logon as TKEADM.
  - c. Load Roles. (Select: Access Control => Roles => Open (File Chooser input can be either CD/DVD or CNM Data Directory) => Select the user defined role => Open => Load => OK). Repeat for each role to be loaded. When complete => Cancel.

**Note:** Due to new TKE 7.0 capability, 5 new “Required” ACPs will be added to each role automatically if they were not already included in the role.
  - d. Load Profiles, including any Group Profiles. (Select: Access Control => Profiles => Open (File Chooser input can be either CD/DVD drive 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.
6. Update User Defined Roles with Applicable Access Control Points through CNM:
  - a. If CNM is not open, 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 CD/DVD or CNM Data Directory) => Load => OK). Repeat for each role to be updated. When complete => Cancel.

- If you have any user defined profiles that you want to continue to use to logon to the TKE Workstation crypto adapter that are intended to be used to manage host crypto modules through the TKE application you may need to add new ACPs to enable the new capabilities of TKE 7.0. Make sure the role tied to the user defined profile contains AT LEAST the ACPs in Table 6 on page 74. Add any missing ACPs to the role.
- If you have any user defined profiles that you want to continue to use to logon to the TKE Workstation crypto adapter that are intended to be used for administration of the TKE workstation (managing CNM etc) you may need to add new ACPs to enable the new capabilities of TKE 7.0. Make sure the role tied to the user defined profile contains AT LEAST the ACPs in Table 7 on page 75. Add any missing ACPs to the role.

#### 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 TKE workstation crypto adapter before either TKE or CNM can be used, define a group profile.

- a. If CNM is not open, open the Cryptographic Node Management Utility and logon to TKEADM or an equivalent profile. See Step 4 for details.
- b. Select: Access Control => Profiles => New. From the Profile Management pop-up, select Group.
- c. Enter the Group ID, update the Expiration Date. Select the role for the group profile, select passphrase profiles.
- d. Update the number of Group members required for Logon (minimum is 1, maximum is 10).
- e. Highlight the profiles from the Available profiles list that you want added to the group and select Add.
- f. When complete, select Load to load the group profile into the TKE workstation crypto 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 228.

For details on CNM passphrase group logon, see “Group Logon” on page 210.

For details on TKE group logon, see “Passphrase and passphrase group logon” on page 85.

#### 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, select **Trusted Key Entry 7.0**.
- b. Logon to the TKE application
- c. 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.

See Chapter 6, “Main Window,” on page 95 for additional details.

9. For IBM System z10 EC, z10 BC, and z196 Customers Only - TKE V7.0

Additional Tasks:

- a. Create the IBM System z10 EC, z10 BC, and z196 host crypto modules.
- b. Create Groups for the IBM System z10 EC, z10 BC, and z196 host crypto modules.
- c. Create roles on your host crypto modules.
- d. Create Authorities. If you want to use existing authority signature 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 or USB flash memory drive.

- To copy to 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 **Trusted Key Entry Data**, select **OK**.
- d. Select the DVD-RAM, 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**.

- To copy to USB Flash memory drive:

- a. Insert a blank USB Flash memory drive into an available USB port.
- b. Format the USB Flash Memory Drive. To do this select **System Management, Format Media**.
- c. Select **Trusted Key Entry Data**, select **OK**.
- d. Select the USB Flash memory drive, 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. Select **Trusted Key Entry, TKE Media Manager**.



- h. Select **Activate read only floppy inserted in the floppy drive**. Select **OK**.
- i. Select **Cancel**.
- j. Using the TKE File Management utility copy files from the diskette over to the USB Flash Memory Drive. Select **Trusted Key Entry, TKE File Management Utilities**.
- k. Deactivate the floppy diskette. Select **Trusted Key Entry, TKE Media Manager**. (The USB Flash Memory drive is deactivated automatically when the copy is completed.)
- l. Select **Deactivate floppy inserted in floppy drive**. Select **OK**.

### Note for TKE V4.X Users on z10 EC and z10 BC

This note applies only to z10 EC and z10 BC customers whose workstation was at TKE V4.x prior to the upgrade to TKE V7.0. If you are upgrading your ICSF level, an authorized TKE authority must enable/disable access control points as appropriate. See Appendix B, "Access Control Points and Callable Services," on page 281 as well as "Working with Domains Controls Settings" on page 173 for more details.

## Smart Card Setup — Migrating from TKE previously using smart cards

These setup steps are for users who are migrating from a previous version of TKE that used smart cards to a new TKE 7.0 that will continue to use smart cards.

**Note:** There is no migration path to obtain 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 A, "Secure Key Part Entry," on page 275). 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

You must be logged in as the ADMIN console user.

The following 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. Run TKE's IBM Crypto Adapter Initialization task, as follows.
  - a. In the right frame of the Trusted Key Entry Console, click on **TKE 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.
2. Activate smart card support in CNM as follows:
  - 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 4.1.0**.
  - c. The crypto adapter logon window appears. Select **Default Logon**.
  - d. Enable smart card support. (Select: File => Enable Smart Card Readers). Smart Card support will be activated the next time you start CNM.
  - e. Exit and logoff CNM
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, select **Trusted Key Entry**.
  - b. In the right frame of the Trusted Key Entry Console, click on **Smart Card Utility Program 7.0**.
  - c. The crypto adapter logon window appears. Select the Profile ID **Use Default Role** and logon to the TKE workstation crypto adapter.
  - d. If the current smart cards are datakey smart cards, see “Migrate Data on DataKey Smart Cards to NXP JCOP 4.1 Smart Cards” on page 57. If the new capability of TKE 7.0 is desired, see “Migrating Data from One Smart Card to Another” on page 57. (Smart card capability can be determined by reviewing information in Chapter 2, “Using Smart Cards with TKE,” on page 13).
- Note:** Cards initialized in TKE 7.0 cannot be used on previous versions of TKE. This should be considered when initializing smart cards if older TKE's are going to be using the same set of smart cards.
- e. Enroll local workstation cryptographic adapter. (Select: Crypto Adapter => Enroll Crypto Adapter => Local => Follow prompts)  
See “Enroll a TKE cryptographic adapter” on page 265.
  - f. Enroll remote workstation cryptographic adapter if applicable.  
See “Enroll a TKE cryptographic adapter” on page 265.
  - g. Close the SCUP application.
4. Load Known Master Key Parts to the TKE workstation crypto adapter
- To be able to use the migrated DES and PKA Key Storages, you must load the TKE workstation crypto adapter master key parts from your previous TKE workstation to the TKE V7.0 workstation.
- a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 4.1.0
  - b. The crypto adapter logon window appears. Select **Default logon** and logon as the TEMPDEFAULT role.
  - c. Load the known TKE workstation crypto adapter master key parts.  
See “Loading a new master key from clear key parts” on page 233 and “Loading master key parts from a TKE smart card” on page 237.
  - d. Set the TKE workstation crypto adapter master key. (Select: Master Key => Set => Yes => OK).
  - e. Exit and logoff CNM
5. Migrate Previous TKE Version to TKE V7.0.
- Execute the Migrate Previous TKE Version to TKE V7.0 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 V7.0 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 V7.0**.
- 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. (A USB floppy drive is needed for this task as the TKE 7.0 does not have a floppy drive.)
- 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 7.0" on page 309 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 4), 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 V7.0.
  - a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 4.1.0.
  - b. The crypto adapter logon window appears. Select **Default logon** and logon as the TEMPDEFAULT role.
  - 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 and logoff CNM
7. CNM initialization tasks
  - a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 4.1.0.
  - b. The crypto adapter logon window appears. Select **Default logon** and logon as the TEMPDEFAULT role.
  - c. Load any User Defined Roles and Profiles to the TKE workstation crypto 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.

**Note:** Due to new TKE 7.0 capability, 5 new "Required" ACPs will be added to each role automatically if they were not already included in the role.

- 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 V4.2 will need to be created as a New Smart Card profile in TKE V7.0. See “Define a Smart Card Profile” on page 225 for details.

See “Open or edit an existing role” on page 217 and “Working with User Profiles” on page 230 for additional details.

- d. 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 CD/DVD, USB Flash Memory Drive or CNM Data Directory) => Load => OK). Repeat for each role to be updated. When complete => Cancel.
  - If you have any user defined profiles that you want to continue to use to logon to the TKE Workstation crypto adapter that are intended to be used to manage host crypto modules through the TKE application you may need to add new ACPs to enable the new capabilities of TKE 7.0. Make sure the role tied to the user defined profile contains AT LEAST the ACPs in Table 11 on page 80. Add any missing ACPs to the role.
  - If you have any user defined profiles that you want to continue to use to logon to the TKE Workstation crypto adapter that are intended to be used for administration of the TKE workstation (managing CNM etc) you may need to add new ACPs to enable the new capabilities of TKE 7.0. Make sure the role tied to the user defined profile contains AT LEAST the ACPs in Table 12 on page 81. Add any missing ACPs to the role.
- e. Create Smart Card Group Logon Profiles

**Note:** If you have already loaded your smart card group profiles from the old TKE and will not be defining any new smart card group profiles, proceed to Step g.

Empty group profiles SCTKEADM and SCTKEUSR are provided in the CNM Data Directory. If you want to require that multiple users logon to the TKE workstation crypto 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 TKE workstation crypto adapter. If you also want to save the profile to the hard drive, DVD-RAM, USB flash memory 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 228.

For details on CNM smart card group logon, see “Smart Card Group Logon” on page 212.

For details on TKE group logon, see “Initializing TKE for smart cards” on page 77.

- f. 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\_70.rol => Open => Load => OK => Cancel)

See “Open or edit a disk-stored role” on page 218.

- g. 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 V7.0.
- 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 121.

9. For IBM System z10 EC, z10 BC, and z196 Customers Only - TKE V7.0 Additional Tasks:

- a. Create the IBM System z10 EC, z10 BC, and z196 Host
- b. Create Groups for the IBM System z10 EC, z10 BC, and z196 host crypto modules.
- 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.

**Note for TKE V4.X Users on z10 EC and z10 BC:** This note applies only to z10 EC and z10 BC customers whose workstation was at TKE V4.x prior to the upgrade to TKE V7.0. If you are upgrading your ICSF level, an authorized TKE authority must enable/disable access control points as appropriate. See Appendix B, “Access Control Points and Callable Services,” on page 281 as well as “Working with Domains Controls Settings” on page 173 for more details.

## Smart Card Setup — Migrating from a TKE NOT previously using smart cards

These setup steps are for users that are migrating from a previous version of TKE that used the passphrase setup, and now want to use smart cards with their new TKE 7.0.

**Note:** There is no migration path to obtain 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 A, "Secure Key Part Entry," on page 275). 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

You must be logged in as the ADMIN console user.

The following 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. Run TKE's IBM Crypto Adapter Initialization task, as follows.
  - a. In the right frame of the Trusted Key Entry Console, click on **TKE 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.
2. Activate smart card support in CNM as follows:
  - 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 4.1.0**.
  - c. The crypto adapter logon window appears. Select **Default Logon**.
  - d. Enable smart card support. (Select: File => Enable Smart Card Readers). Smart Card support will be activated the next time you start CNM.
  - e. Exit and logoff CNM
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, select **Trusted Key Entry**.
  - b. In the right frame of the Trusted Key Entry Console, click on **Smart Card Utility Program 7.0**.
  - c. The crypto adapter logon window appears. Select the Profile ID **Use Default Role** and logon to the TKE workstation crypto adapter.
  - d. 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 258.

**Note:** Cards initialized in TKE 7.0 cannot be used on previous versions of TKE. This should be considered when initializing smart cards if older TKE's are going to be using the same set of smart cards.

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



- See "Backup a CA smart card" on page 261.
- f. Enroll local workstation cryptographic adapter. (Select: Crypto Adapter => Enroll Crypto Adapter => Local => Follow prompts)
  - See "Enroll a TKE cryptographic adapter" on page 265.
- g. Enroll remote workstation cryptographic adapter if applicable.
  - See "Enroll a TKE cryptographic adapter" on page 265.
- h. 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 263.
- i. Personalize TKE smart cards. (Select: TKE smart card => Personalize TKE Smart Card; Follow prompts)
  - See "Personalize a TKE smart card" on page 264.
- j. Close the SCUP application.
- 4. Load Known Master Key Parts to the TKE workstation crypto adapter
 

To be able to use the migrated DES and PKA Key Storages, you must load the TKE workstation crypto adapter master key parts from your previous TKE workstation to the TKE V7.0 workstation.

  - a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 4.1.0
  - b. The crypto adapter logon window appears. Select **Default logon** and logon as the TEMPDEFAULT role.
  - c. Load the known TKE workstation crypto adapter master key parts.
    - See "Loading a new master key from clear key parts" on page 233 and "Loading master key parts from a TKE smart card" on page 237.
  - d. Set the TKE workstation crypto adapter master key. (Select: Master Key => Set => Yes => OK).
  - e. Exit and logoff CNM
- 5. Migrate Previous TKE Version to TKE V7.0.
 

Execute the Migrate Previous TKE Version to TKE V7.0 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 V7.0 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 V7.0**.
  - 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. (A USB floppy drive is needed for this task as the TKE 7.0 does not have a floppy drive.)
  - 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 7.0” on page 309 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 4), 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 V7.0.
  - a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 4.1.0.
  - b. The crypto adapter logon window appears. Select **Default logon** and logon as the TEMPDEFAULT role.
  - 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 and logoff CNM
7. CNM initialization tasks
  - a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 4.1.0.
  - b. The crypto adapter logon window appears. Select **Default logon** and logon as the TEMPDEFAULT role.
  - c. Load any User Defined Roles and Profiles to the TKE workstation crypto adapter.

**Note:** Due to new TKE 7.0 capability, 5 new “Required” ACPs will be added to each role automatically if they were not already included in the role.

See “Open or edit an existing role” on page 217 for additional details.

- d. 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 CD/DVD, USB Flash Memory Drive or CNM Data Directory) => Load => OK). Repeat for each role to be updated. When complete => Cancel.
  - If you have any user defined profiles that you want to continue to use to logon to the TKE Workstation crypto adapter that are intended to be used to manage host crypto modules through the TKE application you may need to add new ACPs to enable the new capabilities of TKE 7.0. Make sure the role tied to the user defined profile contains AT LEAST the ACPs in Table 11 on page 80. Add any missing ACPs to the role.
  - If you have any user defined profiles that you want to continue to use to logon to the TKE Workstation crypto adapter that are intended to be used for administration of the TKE workstation (managing CNM, for example) you may need to add new ACPs to enable the new capabilities of TKE 7.0. Make sure the role tied to the user defined profile contains AT LEAST the ACPs in Table 12 on page 81. Add any missing ACPs to the role.
- e. Generate a workstation cryptographic adapter logon key to a TKE smart card that will be used for logon to the TKE workstation cryptographic



adapter. You will need to generate a TKE crypto 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 244.

- f. Define user profiles for the TKE smart cards that have a TKE workstation crypto adapter logon key. (Select: Access Control => Profiles => New => Smart Card => Insert Smart Card => fill in fields; map to SCTKEUSR, SCTKEADM, or a user-defined role => Save (If desired to the CD/DVD, USB flash memory drive, or CNM Data Directory => Enter File Name => Save => OK) => Load => OK)

See "Define a User Profile" on page 222. 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.

Empty group profiles SCTKEADM and SCTKEUSR are provided in the CNM Data Directory. If you want to require that multiple users logon to the TKE workstation crypto adapter before an application requiring crypto adapter logon 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 TKE workstation crypto adapter. If you also want to save the profile to the hard Drive, DVD-RAM, or USB Flash Memory, 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 228.

For details on CNM smart card group logon, see "Smart Card Group Logon" on page 212.

For details on TKE group logon, see "Initializing TKE for smart cards" on page 77.

- g. 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\_70.rol => Open => Load => OK => Cancel)

See "Open or edit a disk-stored role" on page 218.

- h. 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 V7.0.
- 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 121.

9. Generate New Authority Signature Keys to TKE Smart Cards if needed. For each authority with an authority signature key saved to a binary file, logon TKE and generate a new authority signature key. Save the authority 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 z10 EC, z10 BC, and z196 Customers Only - TKE V7.0 Additional Tasks:
  - a. Create the IBM System z10 EC, z10 BC, and z196 Host
  - b. Create Groups for the IBM System z10 EC, z10 BC , and z196 host crypto modules.
  - 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.

**Note for TKE V4.X Users on z10 EC and z10 BC:** This note applies only to z10 EC and z10 BC customers whose workstation was at TKE V4.x prior to the upgrade to TKE V7.0. If you are upgrading your ICSF level, an authorized TKE authority must enable/disable access control points as appropriate. See Appendix B, “Access Control Points and Callable Services,” on page 281 as well as “Working with Domains Controls Settings” on page 173 for more details.

---

## Migrating from TKE Version 5.0, 5.1, 5.2, 5.3, or 6.0 to TKE Version 7.0

TKE Version 7.0 continues to allow you to manage any CEX2C/CEX3Cs inside your z10 EC and z10 BC and now allows the managing of CEX3Cs running inside the z196. Older host crypto modules and machines are unsupported by TKE 7.0 and will require you keep your older TKE to manage those host crypto modules. Migration to TKE V7.0 requires a new TKE workstation and a new TKE Workstation cryptographic adapter. If you are adding smart card support, the smart card readers should already be attached. The installing of the software on the TKE and the TKE Workstation crypto adapter as well as the moving of relevant data from the older TKE to the new TKE 7.0 should have been completed as part of the Miscellaneous Equipment Specification (MES) instructions.

The instructions below will guide the completion of the migration process based on the type of setup that will be run on this TKE (smart card or passphrase).

### TKE Started Task

**Note:** If your host system is being converted from a z900 to a z10 EC and z10 BC, the TKECM data set is not compatible with TKE V7.0. If you plan to use the

same data set name for TKE V7.0 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 60.

## Passphrase and Smart Card Setup

TKE V7.0 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. You should choose only one of the sets of setup instructions based on the particular migration scenario.

All predefined roles and profiles as well as any user defined roles and profiles that were saved to a file on the old TKE are now in the CNM data directory.

### Passphrase Setup

Perform this task on the TKE V7.0 workstation.

In order to initialize the TKE workstation crypto adapter you must be logged in as the ADMIN console user.

1. Backup the TKE Workstation key storages so we can put them back after the TKE Workstation crypto adapter initialization.
  - 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 the **TKE File Management Utility**.
  - c. The crypto adapter logon window appears. Select the Profile ID **Use Default Role** and logon to the TKE Workstation crypto adapter.
  - d. Copy the following files from the CNM Data Directory to the Migration Backup Data Directory: **desstore.dat**, **desstore.dat.NDX**, **pkastore.dat**, **pkastore.dat.NDX**. For more information on using the File Management Utility see “TKE File Management Utility” on page 311.
  - e. Select File => Exit from the TKE File Management Utility.
2. 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 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 Workstation Crypto Adapter” on page 69 for additional details.

**If the Master Key Parts for the TKE Workstation Master Key are known, or stored in files or on smart cards, do Steps 3 and 4 and then skip Step 5. or else if the Master Key Parts for the TKE Workstation Master Key are Unknown and NOT saved in files or on smart cards, skip Steps 3 and 4 and go directly to Step 5.**

3. Load the Known Master Key Parts to the TKE Workstation crypto adapter. To be able to use migrated DES and PKA Key Storages, you must load the TKE Workstation crypto adapter master key parts from your previous TKE workstation to the TKE V7.0 workstation as follows:
  - a. In the right frame of the Trusted Key Entry Console, click on **Cryptographic Node Management Utility 4.1.0**.
  - b. The crypto adapter logon window appears. Select **Passphrase logon** and logon as KEYMAN1.
  - c. Load the First known TKE workstation crypto 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 the 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 to KEYMAN2. Select File -> Exit and Logoff.
  - e. Open the Cryptographic Node Management Utility 4.1.0 again. The crypto adapter logon window appears.
  - f. Select **Passphrase Logon**. Logon as KEYMAN2.
  - g. Load the Middle and Last known TKE workstation crypto 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 the 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.
- h. Set the TKE workstation crypto adapter master key. (Select: Master Key => Set).
  - i. Exit and logoff CNM.

For additional details on loading TKE workstation crypto adapter master key parts see "Loading a new master key from clear key parts" on page 233.

4. Restore the saved TKE Workstation Key storages
  - 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 the **TKE File Management Utility**.

- c. The crypto adapter logon window appears. Select the Profile ID **Use Default Role** and logon to the TKE Workstation crypto adapter.
  - d. Copy the following files from the Migration Backup Data Directory to the CNM Data Directory: **desstore.dat**, **desstore.dat.NDX**, **pkastore.dat**, **pkastore.dat.NDX**. This will be overwriting the files that are currently in the CNM Data Directory. For more information on using the File Management Utility see "TKE File Management Utility" on page 311.
  - e. Select File => Exit from the TKE File Management Utility.
5. Reinitialize 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 (Steps 3 and 4), 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 7.0.
  - a. In the right frame of the Trusted Key Entry Console, click on **Cryptographic Node Management Utility 4.1.0**.
  - b. The crypto adapter logon window appears. Select **Passphrase logon** and logon as 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 and logoff CNM.
6. Load User Defined Roles and Profiles to the TKE Workstation crypto adapter: If you are currently not in CNM, 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 4.1.0**.
  - b. The crypto adapter logon window appears. Select **Passphrase logon** and logon as TKEADM.
  - c. Load Roles. (Select: Access Control => Roles => Open (File Chooser input can be either CD/DVD or CNM Data Directory) => Select the user defined role => Open => Load => OK). Repeat for each role to be loaded. When complete => Cancel.

**Note:** Due to new TKE 7.0 capability, 5 new "Required" ACPs will be added to each role automatically if they were not already included in the role.

  - d. Load Profiles, including any Group Profiles. (Select: Access Control => Profiles => Open (File Chooser input can be either CD/DVD drive 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 218 and "Edit a Disk-Stored User Profile" on page 230 for additional details.
7. Update User Defined Roles with Applicable Access Control Points through CNM:

- a. If CNM is not already open, open the Cryptographic Node Management Utility and logon to TKEADM or an equivalent profile. See Step 6 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 CD/DVD or CNM Data Directory) => Load => OK). Repeat for each role to be updated. When complete => Cancel.
  - If you have any user defined profiles that you want to continue to use to logon to the TKE workstation crypto adapter that are intended to be used to manage host crypto modules through the TKE application, you may need to add new ACPs to enable the new capabilities of TKE 7.0. Make sure the role tied to the user defined profile contains AT LEAST the ACPs in Table 6 on page 74. Add any missing ACPs to the role.
  - If you have any user defined profiles that you want to continue to use to logon to the TKE Workstation crypto adapter that are intended to be used for administration of the TKE workstation (managing CNM for example), you may need to add new ACPs to enable the new capabilities of TKE 7.0. Make sure the role tied to the user defined profile contains AT LEAST the ACPs in Table 7 on page 75. Add any missing ACPs to the role.
8. 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 TKE Workstation crypto adapter before either TKE or CNM can be used, define a group profile.
  - a. If CNM is not open, open the Cryptographic Node Management Utility and logon to TKEADM or an equivalent profile.
  - b. Select: Access Control => Profiles => New. From the Profile Management pop-up, select Group.
  - c. Enter the Group ID, update the Expiration Date. Select the role for the group profile, select passphrase profiles.
  - d. Update the number of Group members required for Logon (minimum is 1, maximum is 10).
  - e. Highlight the profiles from the Available profiles list that you want added to the group, and select Add.
  - f. When complete, select Load to load the group profile into the TKE workstation crypto 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 228.

For details on CNM passphrase group logon, see “Group Logon” on page 210.

For details on TKE group logon, see “Passphrase and passphrase group logon” on page 85.

9. For IBM System z10 EC, z10 BC, and z196 Customers Only - TKE V7.0 Additional Tasks:



- a. Create the IBM System z10 EC, z10 BC, and z196 Hosts if new host(s) are available.
  - b. Create Groups for the IBM System z10 EC, z10 BC, and z196 host crypto modules.
  - c. Create roles on your host crypto modules
  - d. Create Authorities. If you want to use existing authority signature keys, upload the authority signature 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 or USB Flash Memory Drive.
- To copy to 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 **Trusted Key Entry Data**, select **OK**.
    - d. Select the DVD-RAM, 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**.
  - To copy to USB Flash memory drive:
    - a. Insert a blank USB Flash memory drive into an available USB port.
    - b. Format the USB Flash Memory Drive. To do this, select **System Management, Format Media**.
    - c. Select **Trusted Key Entry Data**, select **OK**.
    - d. Select the USB Flash memory drive, 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. Select **Trusted Key Entry, TKE Media Manager**.
    - h. Select **Activate read only floppy inserted in the floppy drive**. Select **OK**.
    - i. Select **Cancel**.

- j. Using the TKE File Management utility, copy files from the diskette over to the USB Flash Memory Drive. Select **Trusted Key Entry, TKE File Management Utilities**.
  - k. Deactivate the floppy diskette. Select **Trusted Key Entry, TKE Media Manager**. (The USB Flash Memory drive is deactivated automatically when the copy is completed.)
  - l. Select **Deactivate floppy inserted in floppy drive**. Select **OK**.
11. Check the Host ACPs if ICSF level is upgraded. If you are upgrading your ICSF level an authorized TKE authority must enable/disable access control points as appropriate. See Appendix B, "Access Control Points and Callable Services," on page 281 as well as "Working with Domains Controls Settings" on page 173 for more details.

## Smart Card Setup — Migrating from TKE previously using smart cards

These setup steps are for users that are migrating from a previous version of TKE that used smart cards to a new TKE 7.0 that will continue to use smart cards.

**Note:** There is no migration path to obtain 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 A, "Secure Key Part Entry," on page 275). 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

You must be logged in as the ADMIN console user.

The following 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. Backup the TKE Workstation key storages so we can put them back after the TKE Workstation crypto adapter initialization.
  - 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 the **TKE File Management Utility**.
  - c. The crypto adapter logon window appears. Select the Profile ID **Use Default Role** and logon to the TKE Workstation crypto adapter.
  - d. Copy the following files from the CNM Data Directory to the Migration Backup Data Directory: **desstore.dat**, **desstore.dat.NDX**, **pkastore.dat**, **pkastore.dat.NDX** For more information on using the File Management Utility see "TKE File Management Utility" on page 311.
  - e. Select File => Exit from the TKE File Management Utility.
2. Run TKE's IBM Crypto Adapter Initialization task.
  - a. In the right frame of the Trusted Key Entry Console, click on **TKE 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 use? (S/P)" prompt.
- d. When complete, press **Enter** to exit.
- 3. Activate smart card support in CNM as follows (should already be enabled, but just in case):
  - 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 4.1.0**.
  - c. The crypto adapter logon window appears. Select **Default Logon**.
  - d. Enable smart card support. (Select: File => Enable Smart Card Readers). Smart Card support will be activated the next time you start CNM.
  - e. Exit and logoff CNM

#### 4. 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, select **Trusted Key Entry**.
- b. In the right frame of the Trusted Key Entry Console, click on **Smart Card Utility Program 7.0**.
- c. The crypto adapter logon window appears. Select the Profile ID **Use Default Role** and logon to the TKE workstation crypto adapter.
- d. If the current smart cards are datakey smart cards, see "Migrate Data on DataKey Smart Cards to NXP JCOP 4.1 Smart Cards" on page 57. If the new capability of TKE 7.0 is desired see "Migrating Data from One Smart Card to Another" on page 57. (Smart card capability can be determined by reviewing information in Chapter 2, "Using Smart Cards with TKE," on page 13).

**Note:** Cards initialized in TKE 7.0 cannot be used on previous versions of TKE. This should be considered when initializing smart cards if older TKE's are going to be using the same set of smart cards.

- e. Enroll local workstation cryptographic adapter. (Select: Crypto Adapter => Enroll Crypto Adapter => Local => Follow prompts)  
See "Enroll a TKE cryptographic adapter" on page 265.
- f. Enroll remote workstation cryptographic adapter if applicable.  
See "Enroll a TKE cryptographic adapter" on page 265.
- g. Close the SCUP application.

**If the Master Key Parts for the TKE Workstation Master Key are known, or stored in files or on smart cards, do Steps 5 and 6 and then skip Step 7 or else if the Master Key Parts for the TKE Workstation Master Key are Unknown and NOT saved in files or on smart cards, skip Steps 5 and 6 and go directly to Step 7.**

- 5. Load Known Master Key Parts to the TKE workstation crypto adapter  
To be able to use the migrated DES and PKA Key Storages, you must load the TKE workstation crypto adapter master key parts from your previous TKE workstation to the TKE V7.0 workstation.
  - a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 4.1.0
  - b. The crypto adapter logon window appears. Select **Default logon** and logon as the TEMPDEFAULT role.

- c. Load the known TKE workstation crypto adapter master key parts.  
See “Loading a new master key from clear key parts” on page 233 and “Loading master key parts from a TKE smart card” on page 237.
  - d. Set the TKE workstation crypto adapter master key. (Select: Master Key => Set => Yes => OK).
  - e. Exit and logoff CNM
6. Restore the saved TKE Workstation Key storages
- 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 the **TKE File Management Utility**.
  - c. The crypto adapter logon window appears. Select the Profile ID **Use Default Role** and logon to the TKE Workstation crypto adapter.
  - d. Copy the following files from the Migration Backup Data Directory to the CNM Data Directory: **desstore.dat**, **desstore.dat.NDX**, **pkastore.dat**, **pkastore.dat.NDX** This will be overwriting the files that are currently in the CNM Data Directory. For more information on using the File Management Utility see “TKE File Management Utility” on page 311.
  - e. Select File => Exit from the TKE File Management Utility.
7. Reinitialize 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 (Steps 5), 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 7.0.
- a. In the right frame of the Trusted Key Entry Console, click on **Cryptographic Node Management Utility 4.1.0**.
  - b. The crypto adapter logon window appears. Select **Default logon** and logon as TEMPDEFAULT role.
  - 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 and logoff CNM.
8. CNM initialization tasks
- a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 4.1.0.
  - b. The crypto adapter logon window appears. Select **Default logon** and logon as the TEMPDEFAULT role.
  - c. Load any User Defined Roles and Profiles to the TKE workstation crypto 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.

**Note:** Due to new TKE 7.0 capability, 5 new “Required” ACPs will be added to each role automatically if they were not already included in the role.

- 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 on the previous TKE at the time of the migration will need to be created as a New Smart Card profile in TKE V7.0. See “Define a Smart Card Profile” on page 225 for details.

See Open or Edit a disk stored role “Open or edit an existing role” on page 217 and Edit a disk-stored user profile “Working with User Profiles” on page 230 for additional details.

- d. 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 CD/DVD, USB Flash Memory Drive or CNM Data Directory) => Load => OK). Repeat for each role to be updated. When complete => Cancel.
  - If you have any user defined profiles that you want to continue to use to logon to the TKE Workstation crypto adapter that are intended to be used to manage host crypto modules through the TKE application you may need to add new ACPs to enable the new capabilities of TKE 7.0. Make sure the role tied to the user defined profile contains AT LEAST the ACPs in Table 11 on page 80. Add any missing ACPs to the role.
  - If you have any user defined profiles that you want to continue to use to logon to the TKE Workstation crypto adapter that are intended to be used for administration of the TKE workstation (managing CNM for example) you may need to add new ACPs to enable the new capabilities of TKE 7.0. Make sure the role tied to the user defined profile contains AT LEAST the ACPs in Table 12 on page 81. Add any missing ACPs to the role.
- e. Create Smart Card Group Logon Profiles

**Note:** If you have already loaded your smart card group profiles from the old TKE and will not be defining any new smart card group profiles, proceed to Step g.

Empty group profiles SCTKEADM and SCTKEUSR are provided in the CNM Data Directory. If you want to require that multiple users logon to the TKE workstation crypto 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 TKE workstation crypto adapter. If you also want to save the profile to the hard drive, DVD-RAM, USB Flash Memory 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 228.

For details on CNM smart card group logon, see “Smart Card Group Logon” on page 212.

For details on TKE group logon, see “Initializing TKE for smart cards” on page 77.

- f. 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\_70.rol => Open => Load => OK => Cancel)

See “Open or edit a disk-stored role” on page 218.

- g. Exit CNM.

9. For IBM System z10 EC, z10 BC, and z196 Customers Only - TKE V7.0 Additional Tasks:

- a. Create the IBM System z10 EC, z10 BC, and z196 Hosts if new hosts are available.
- b. Create Groups for the IBM System z10 EC, z10 BC, and z196 host crypto modules.
- 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.

10. Check the Host ACPs if ICSF level, is upgraded. If you are upgrading your ICSF level, an authorized TKE authority must enable/disable access control points as appropriate. See Appendix B, “Access Control Points and Callable Services,” on page 281 as well as “Working with Domains Controls Settings” on page 173 for more details.

## Smart Card Setup – Migrating from TKE NOT previously using smart cards

These setup steps are for users that are migrating from a previous version of TKE that used the passphrase setup, and now want to use smart cards with their new TKE 7.0.

**Note:** There is no migration path to obtain 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 A, “Secure Key Part Entry,” on page 275). 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

You must be logged in as the ADMIN console user.

The following 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. Backup the TKE Workstation key storages so we can put them back after the TKE Workstation crypto adapter initialization.
  - 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 the **TKE File Management Utility**.
  - c. Logon the crypto adapter logon window appears. Select the Profile ID **Use Default Role** and logon to the TKE Workstation crypto adapter.
  - d. Copy the following files from the CNM Data Directory to the Migration Backup Data Directory: **desstore.dat**, **desstore.dat.NDX**, **pkastore.dat**, **pkastore.dat.NDX**. For more information on using the File Management Utility, see "TKE File Management Utility" on page 311.
  - e. Select File => Exit from the TKE File Management Utility.
2. Run TKE's IBM Crypto Adapter Initialization task.
  - a. In the right frame of the Trusted Key Entry Console, click on **TKE 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 use? (S/P)" prompt.
  - d. When complete, press **Enter** to exit.
3. Activate smart card support in CNM as follows:
  - 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 4.1.0**.
  - c. The crypto adapter logon window appears. Select **Default Logon**.
  - d. Enable smart card support. (Select: File => Enable Smart Card Readers). Smart Card support will be activated the next time you start CNM.
  - e. Exit and logoff CNM
4. **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, select **Trusted Key Entry**.
  - b. In the right frame of the Trusted Key Entry Console, click on **Smart Card Utility Program 7.0**.
  - c. The crypto adapter logon window appears. Select the Profile ID **Use Default Role** and log on to the TKE workstation crypto adapter.
  - d. 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 258.

**Note:** Cards initialized in TKE 7.0 cannot be used on previous versions of TKE. This should be considered when initializing smart cards if older TKE’s are going to be using the same set of smart cards.

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

See “Backup a CA smart card” on page 261.

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

See “Enroll a TKE cryptographic adapter” on page 265.

- g. Enroll remote workstation cryptographic adapter if applicable.

See “Enroll a TKE cryptographic adapter” on page 265.

- h. 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 263.

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

See “Personalize a TKE smart card” on page 264.

- j. Close the SCUP application.

**If the Master Key Parts for the TKE Workstation Master Key are known, or stored in files or on smart cards, do Steps 5 and 6 and then skip Step 7 or else if the Master Key Parts for the TKE Workstation Master Key are Unknown and NOT saved in files or on smart cards, skip Steps 5 and 6 and go directly to Step 7.**

- 5. Load Known Master Key Parts to the TKE workstation crypto adapter

To be able to use the migrated DES and PKA key storages, you must load the TKE workstation crypto adapter master key parts from your previous TKE workstation to the TKE V7.0 workstation.

- a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 4.1.0
- b. The crypto adapter logon window appears. Select **Default logon** and logon as the TEMPDEFAULT role.
- c. Load the known TKE workstation crypto adapter master key parts.  
See “Loading a new master key from clear key parts” on page 233 and “Loading master key parts from a TKE smart card” on page 237.
- d. Set the TKE workstation crypto adapter master key. (Select: Master Key => Set => Yes => OK).
- e. Exit and logoff CNM

- 6. Restore the saved TKE Workstation key storages

- 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 the **TKE File Management Utility**.
- c. The crypto adapter logon window appears. Select the Profile ID **Use Default Role** and logon to the TKE Workstation crypto adapter.
- d. Copy the following files from the Migration Backup Data Directory to the CNM Data Directory: **desstore.dat**, **desstore.dat.NDX**, **pkastore.dat**, **pkastore.dat.NDX** This will be overwriting the files that are currently in the



CNM Data Directory. For more information on using the File Management Utility, see “TKE File Management Utility” on page 311.

- e. Select File => Exit from the TKE File Management Utility.
7. Reinitialize 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 5), 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 7.0.
  - a. In the right frame of the Trusted Key Entry Console, click on **Cryptographic Node Management Utility 4.1.0**.
  - b. The crypto adapter logon window appears. Select **Default logon** and logon as TEMPDEFAULT role.
  - 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 and logoff CNM.
8. CNM initialization tasks
  - a. In the right frame of the Trusted Key Entry Console, click on Cryptographic Node Management Utility 4.1.0.
  - b. The crypto adapter logon window appears. Select **Default logon** and logon as the TEMPDEFAULT role.
  - c. Load any User Defined Roles to the TKE workstation crypto adapter.

**Note:** Due to new TKE 7.0 capability, 5 new “Required” ACPs will be added to each role automatically if they were not already included in the role.

See Open or Edit a disk stored role “Open or edit an existing role” on page 217 for additional details.

- d. 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 CD/DVD, USB Flash Memory Drive or CNM Data Directory) => Load => OK). Repeat for each role to be updated. When complete => Cancel.
  - If you have any user defined profiles that you want to continue to use to logon to the TKE workstation crypto adapter that are intended to be used to manage host crypto modules through the TKE application, you may need to add new ACPs to enable the new capabilities of TKE 7.0. Make sure the role tied to the user defined profile contains AT LEAST the ACPs in Table 11 on page 80. Add any missing ACPs to the role.
  - If you have any user defined profiles that you want to continue to use to logon to the TKE Workstation crypto adapter that are intended to be used for administration of the TKE workstation (managing CNM, for example) you may need to add new ACPs to enable the new capabilities of TKE 7.0. Make sure the role tied to the user defined profile contains AT LEAST the ACPs in Table 12 on page 81. Add any missing ACPs to the role.

- e. Generate a workstation cryptographic adapter logon key to a TKE smart card that will be used for logon to the TKE workstation cryptographic adapter. You will need to generate a TKE crypto 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 244.
- f. Define user profiles for the TKE smart cards that have a TKE workstation crypto adapter logon key. (Select: Access Control => Profiles => New => Smart Card => Insert Smart Card => fill in fields; map to SCTKEUSR, SCTKEADM, or user defined role => Save (If desired to the CD/DVD, CNM Data Directory => Enter File Name => Save => OK) => Load => OK)  
See "Define a User Profile" on page 222..

**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.

Empty group profiles SCTKEADM and SCTKEUSR are provided in the CNM Data Directory. If you want to require that multiple users logon to the TKE workstation crypto adapter before an application requiring crypto adapter logon 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 TKE workstation crypto adapter. If you also want to save the profile to the hard Drive, DVD-RAM or USB Flash Memory, 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 228.

For details on CNM smart card group logon, see "Smart Card Group Logon" on page 212.

For details on TKE group logon, see "Initializing TKE for smart cards" on page 77.

- g. 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\_70.rol => Open => Load => OK => Cancel)  
See "Open or edit a disk-stored role" on page 218.
  - h. Exit CNM.
9. Generate New Authority Signature Keys to TKE Smart Cards if needed. For each authority with an authority signature key saved to a binary file, logon TKE and generate a new authority signature key. Save the authority 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 z10 EC, z10 BC, and z196 Customers - TKE V7.0 Additional Tasks:
  - a. Create the IBM System z10 EC, z10 BC, and z196 Hosts if new host(s) available.
  - b. Create Groups for the IBM System z10 EC, z10 BC , and z196 host crypto modules.
  - 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.
11. Check the Host ACPs if ICSF level is upgraded. If you are upgrading your ICSF level, an authorized TKE authority must enable/disable access control points as appropriate. See Appendix B, “Access Control Points and Callable Services,” on page 281 as well as “Working with Domains Controls Settings” on page 173 for more details.

---

## Migrating Data from One Smart Card to Another

From time to time, it may be desirable to migrate data from one smart card to another. For example, you may want to migrate the data from one type of smart card to another type of smart card because the newer card has more capability or speed.

To migrate data from one CA smart card to another, make a backup of the CA smart card. Instructions for performing this task can be found in “Backup a CA smart card” on page 261.

You can copy keys or key parts from one TKE smart card to another using the Copy smart card contents function of the Utilities menu of the main TKE application, or using the Copy Smart Card function of the Smart Card menu of the Cryptographic Node Management Utility. The source and target smart cards must belong to the same zone.

---

## Migrate Data on DataKey Smart Cards to NXP JCOP 4.1 Smart Cards

TKE V6.0 was the last release where DataKey smart cards could be used. The only operations on TKE V7.0 that allow the use of DataKey smart cards are creating a backup CA smart card and copying keys and key parts between smart cards. DataKey smart cards can be used as the source card for these operations.

CA smart cards can be backed up using the Smart Card Utility Program.

To make a copy of a TKE smart card, take the following steps:

1. Using the Smart Card Utility Program, initialize and enroll a new TKE smart card in the same zone as the TKE smart card you want to copy.
2. Using the Smart Card Utility Program, personalize the new TKE smart card (set the card description and PIN).
3. Using the Cryptographic Node Management Utility, copy all keys from the original TKE smart card to the new TKE smart card.



## Chapter 4. TKE Setup and Customization

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

Table 5. TKE management system task checklist

TASK	RESPONSIBLE	WHERE	COMPLETED
1. Configure the host crypto modules	IBM CE or Client Operations Representative	Support Element	
2. Load host crypto module configuration data, 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. Permit each host crypto module for TKE commands	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 workstation crypto adapter	TKE Administrator	TKE workstation	
10. TKE Application Customization	TKE Administrator	TKE workstation	

For more information on tasks 1 and 2 see *System z Service Guide for Trusted Key Entry Workstations*.

For more information on tasks 3 and 4, see:

- *System z Service Guide for Trusted Key Entry Workstations*
- *PR/SM Planning Guide*
- “TKE Enablement” on page 7.
- Appendix C, “LPAR Considerations,” on page 291.

### TKE TCP/IP Setup

TKE uses TCP/IP for communication between the TKE workstation and the MVS operating system. You should already have TCP/IP installed and configured.

1. If you do not have a domain name server running, update the Hosts file with your IP address. TKE refers to the host by IP address, not by the host name. If a domain name server (DNS) is running, then this update is unnecessary as all hosts will be identified to the DNS.

```
HOST      : 9.117.59.140 :
```

Figure 10. Entry Example

2. Update your TCPIP profile to reserve a port for the TKE application.

```
PORT
50003 TCP CSFTTCP      ;ICSF TKE Server
```

Figure 11. Example of Reserving a Port

The example allows use of the port by the server named CSFTTCP. The port number must not start in column 1. TCP is the port type. CSFTTCP is the name of the started procedure. The 50003 is added to the port section and can be changed by the installation. The port number here has to be specified on the workstation when connecting to the host.

Any job with jobname CSFTTCP can connect to this port.

## TKE Host Transaction Program Setup

The TKE Host Transaction Program (TKE HTP) is the host-based part of Trusted Key Entry. It forms the interface between the TKE workstation and the host crypto modules.

The TKE HTP (server) needs to be started before a TKE workstation (client) can communicate with the host crypto modules. The TKE HTP consists of a started procedure (CSFTTCP) which passes some start-up parameters to a REXX clist (CSFTHTP3). The clist then calls a module (CSFTTKE) that does RACF authorization checking to make sure that no unauthorized clients get to the TKE HTP server.

In order to run the new TKE Host Transaction program, the CSFTTKE module must be added to the authorized command list in IKJTSOxx on the system where the TKE HTP server will be started.

Perform these steps to install the server:

1. Update the authorized commands list in the TSO commands and programs member, IKJTSOxx, in the SYS1.PARMLIB data set.

```
AUTHCMD NAMES(                /* AUTHORIZED COMMANDS */          +
COMMAND1                /*                */          +
COMMAND2                /*                */          +
COMMAND3                /*                */          +
.                        /*                */          +
.                        /*                */          +
.                        /*                */          +
CSFTTKE                /* AUTHORIZE TKE */          +
.                        /*                */          +
.                        /*                */          +
.                        /*                */          +
```

Figure 12. 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 13. 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 14. 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 15. 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=CSFTHTP3,
//          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 16. Sample Startup Procedure

## TKE Startup Parameters

**Note:** If upgrading from a legacy machine to a z10 EC, z10 BC, or z196 and upgrading to TKE 7.0, 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 z10 EC, z10 BC, or z196 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” on page 59).  
If a port number is not specified, a default port of 50003 will be used. However, if port 50003 is not reserved in your TCP/IP profile, another application may use it and the TKE HTP will fail.  
For example: PORT;1000

SYSTCPD is optional but, depending on your TCP/IP installation, may be needed.

You may choose between implicit and explicit allocation.

- Implicit - The name of the configuration data set is constructed at run time, based on rules implemented in the components of TCP/IP. Once a data set name is constructed, TCP/IP uses the dynamic allocation services of 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 17. 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 18. 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
```

---

## TKE Workstation Setup and Customization

This topic describes several tasks that are necessary preparation for operating your TKE workstation.

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 while it is connected directly to the LCD monitor. After initial boot up on the LCD monitor, the TKE can be connected to the KVM switching unit.

**IMPORTANT:** For reliable TKE operation, the customer 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.

Most of the workstation setup and customization tasks require you to be signed onto TKE in privileged mode with the ADMIN user name. When TKE is initially started, you are not signed onto TKE in privileged mode. The following steps are used to sign onto TKE in privileged mode.

- Close the Trusted Key Entry Console.
- From the Welcome to the Trusted Key Entry Console screen select *Privileged Mode Access*
- From the Trusted Key Entry Console Logon screen enter the user name ADMIN and the password PASSWORD
- Press the Logon button.

In the upper right hand corner, to the left of the word Help, the user name is displayed.



Figure 19. Login with ADMIN user name

When no user name is displayed, you are logged on with TKEUSER.

## Configuring TCP/IP

The TKE Administrator must configure the TKE workstation for TCP/IP. You must be logged on with the ADMIN user name for this task. TCP/IP is configured through the Customize Network Settings task.



## Customize Network Settings

In the left frame of the Trusted Key Entry Console, click on Service Management. In the right frame of the Trusted Key Entry Console, click on Customize Network Settings.

The Customize Network Settings window opens. Its Identification tab is displayed.

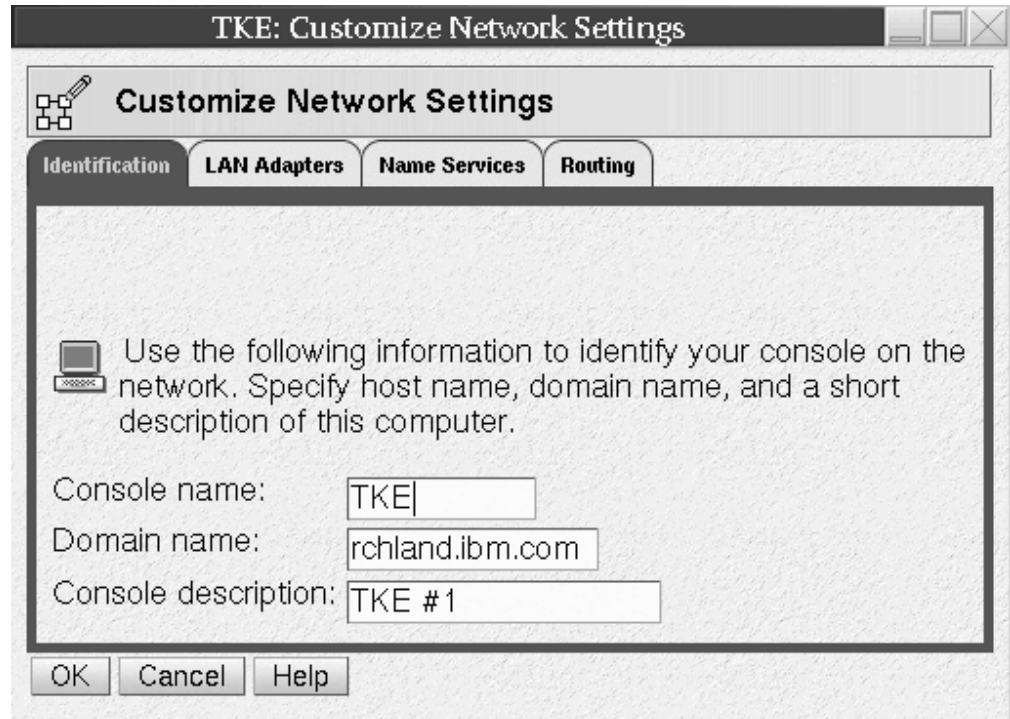


Figure 20. Customize Network Settings - Identification Tab

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.

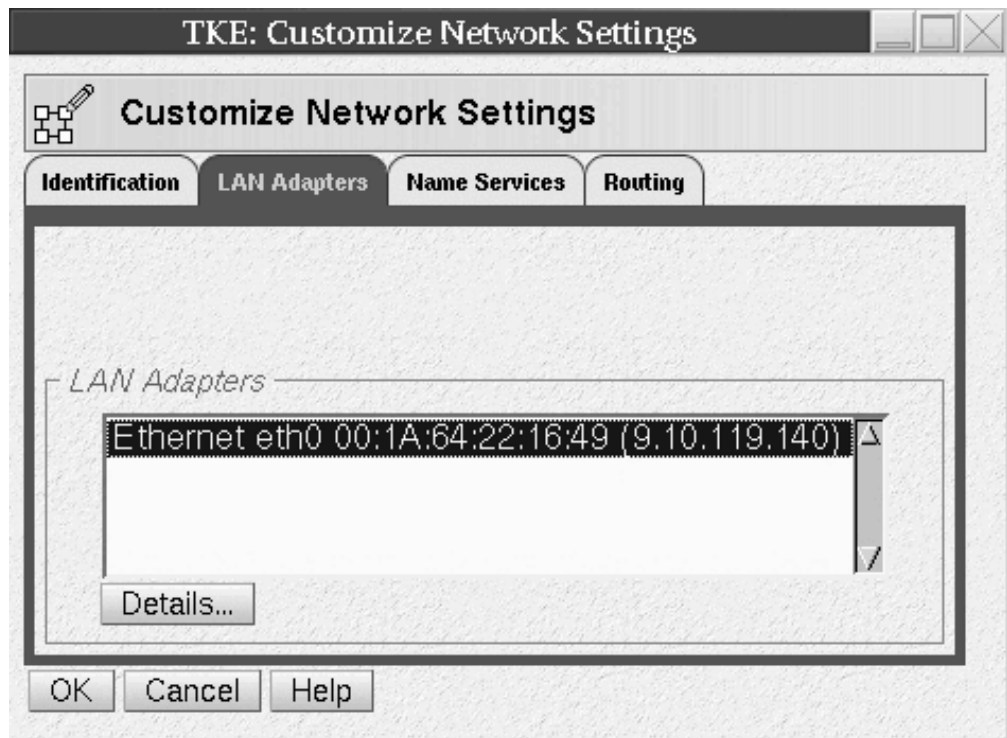


Figure 21. Customize Network Settings Lan Adapters Tab

With the Ethernet LAN adapter highlighted, click on Details.

The LAN Adapter Details window opens.

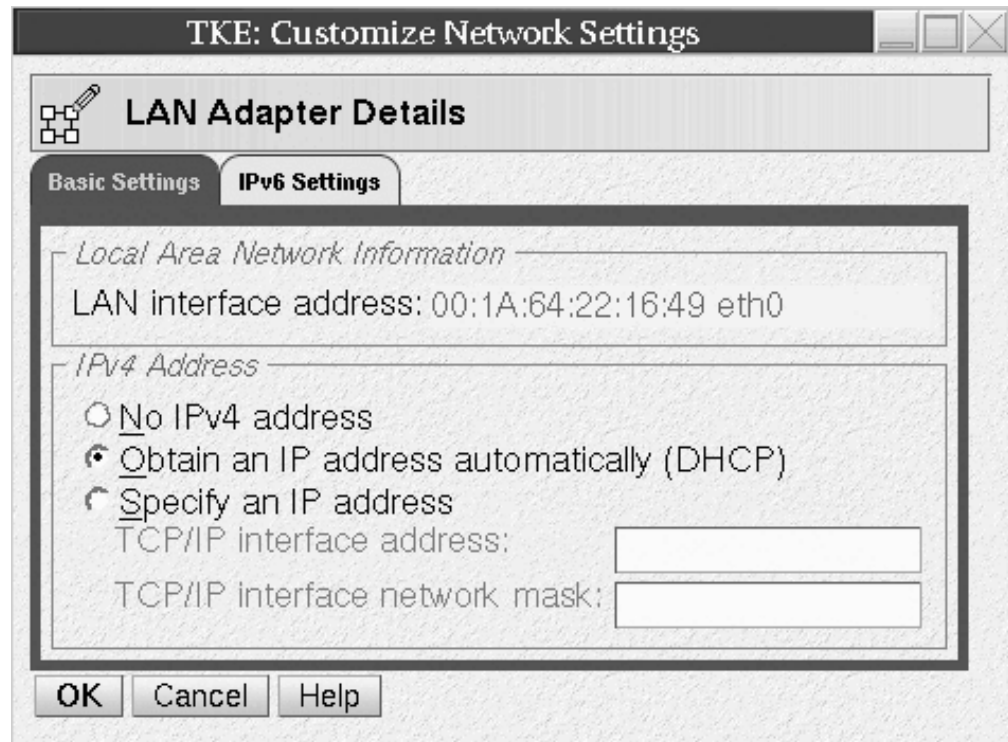


Figure 22. Local Area Network

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.

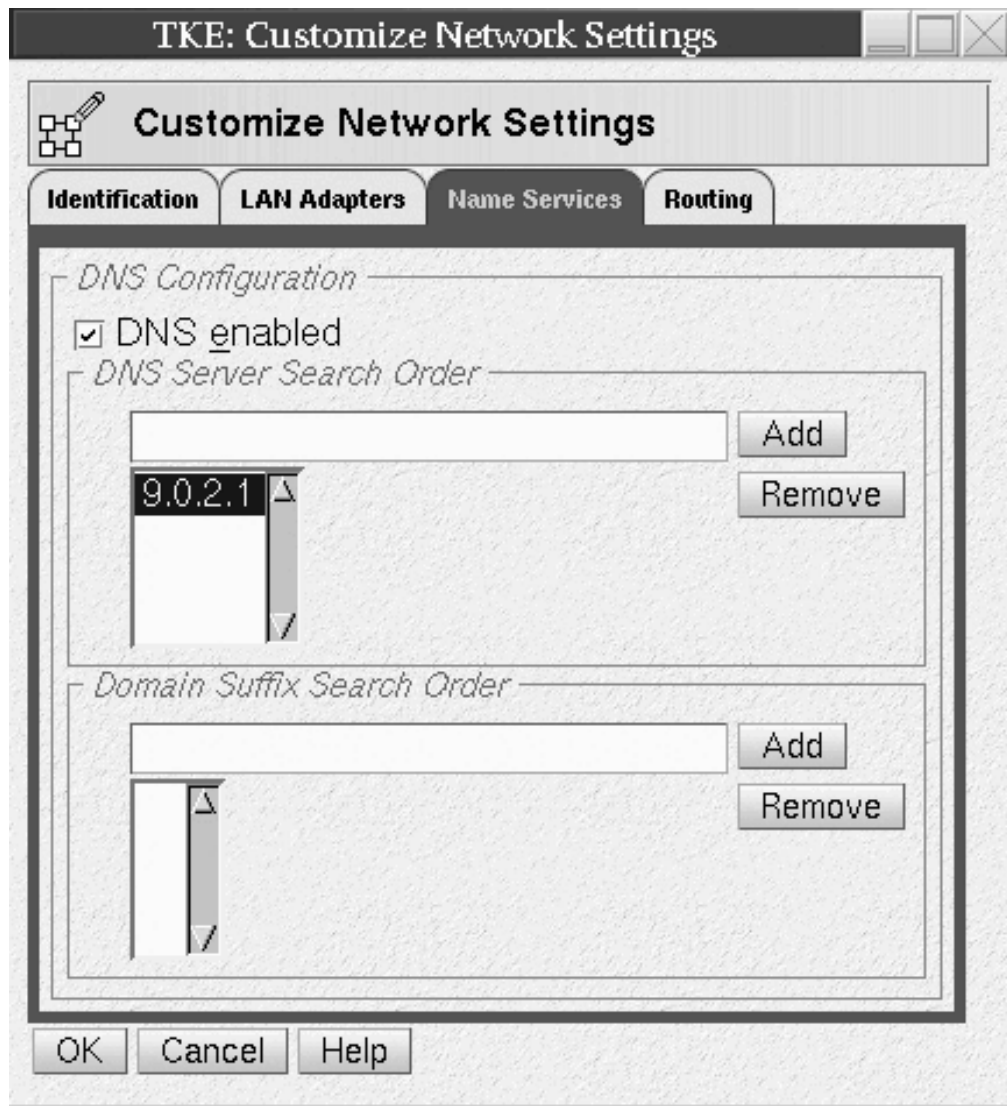


Figure 23. Customize Network Settings - Name Services Tab

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.

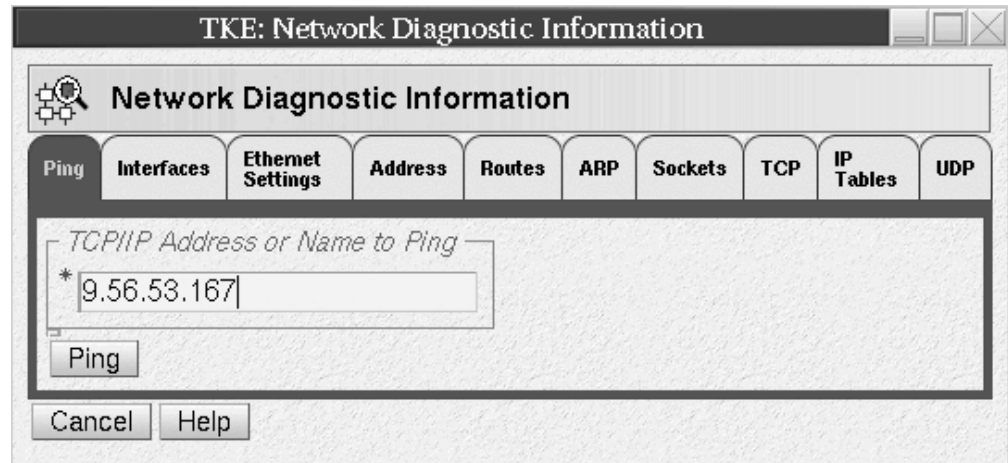


Figure 24. Network Diagnostic Information Task

## Initializing the TKE Workstation Crypto Adapter

The TKE workstation crypto adapter needs to be initialized before it can be used for cryptographic functions. You must be logged on with the ADMIN user name for this task.

You need to decide whether to use passphrase or smart card authentication. For simplicity, we recommend that you do not use a mix of authentication methods.

First, set the clock on your TKE workstation. See “Customize Console Date/Time.”

Next, initialize the TKE workstation crypto adapter using TKE's IBM Crypto Adapter Initialization and Cryptographic Node Management Utility 4.1.0.

- If you are initializing using passphrase, see “Initializing TKE for passphrase” on page 71.
- If you are initializing using smart cards, see “Initializing TKE for smart cards” on page 77.

### Customize Console Date/Time

To set the system clock on your workstation, open the Customize Console Date/Time task under Service Management. You must be logged on with the ADMIN user name for this task.

The Customize Console Data and Time window opens. Its *Customize Data and Time* tab is displayed.

### 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. Click **Customize** when finished.

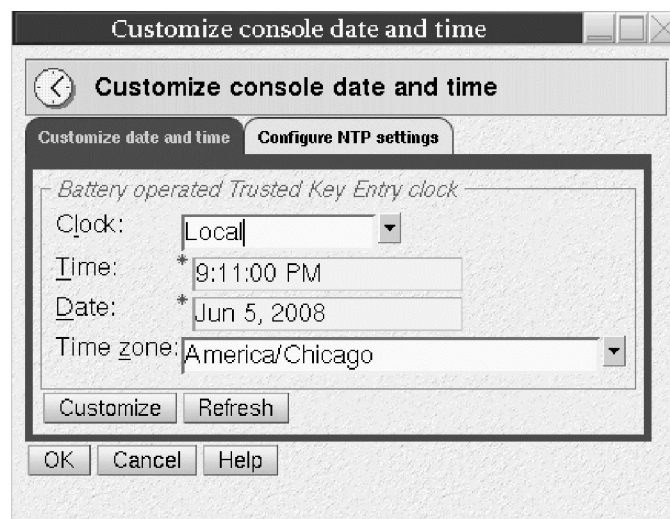


Figure 25. Customize Console Date and Time Window

## Setting the assigned time for your system - alternate procedure

To use NTP to set the workstation clock click on the Customize Console Date and Time window's *Configure NTP Settings* tab:



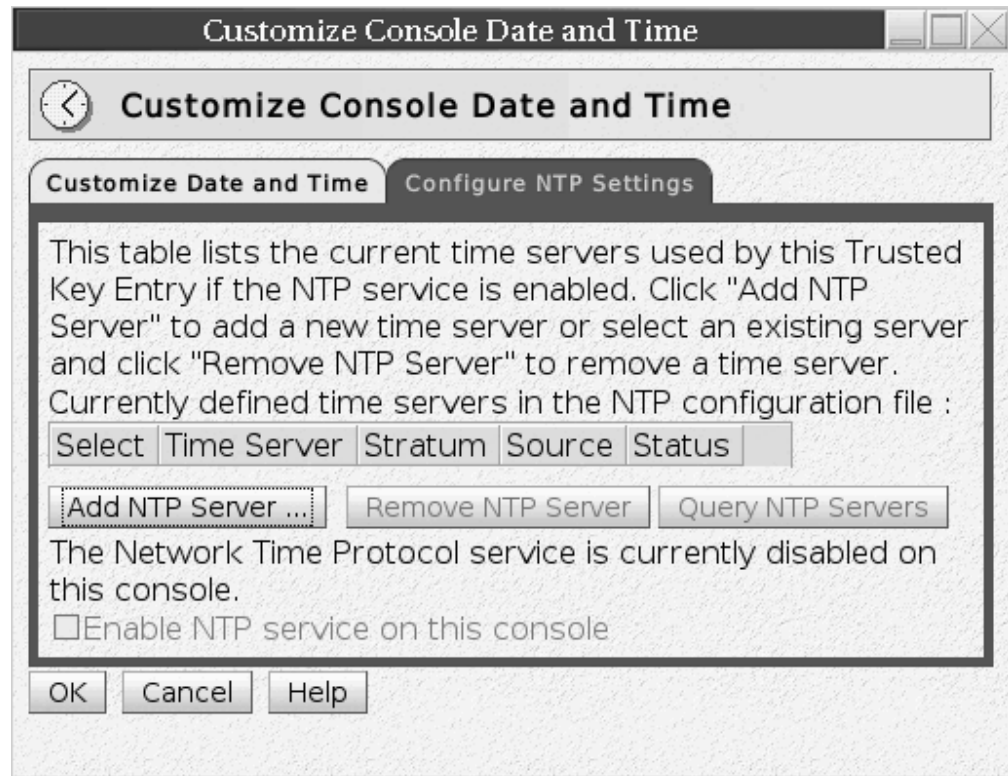


Figure 26. Configure NTP settings

To add an NTP server, click on the *Add NTP Server...* button.

The Add a Network Time Server dialog opens.



Figure 27. Add a Network Time Server

Enter the NTP server hostname, and click **OK**.

In order to enable the NTP service, select the checkbox *Enable NTP service on this console* and click **OK**.

### 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. You must be logged on with the ADMIN user name for this task.

A warning will remind you that this operation will initialize your TKE workstation crypto adapter and all modifications will be lost.

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]

Select **Y** if you would like to continue. You will see the following message.

Would you like to prepare your cryptographic coprocessor for Smart Card or Pass Phrase use? (S/P) [default=P]

The TKE workstation crypto adapter is initialized with the roles and profiles required for the passphrase environment. The time on the TKE workstation and the crypto adapter are synchronized. The crypto adapter master key is set and DES and PKA key storages are initialized.

Initialization output will be displayed. 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 4.1.0 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 TKE workstation crypto adapter.

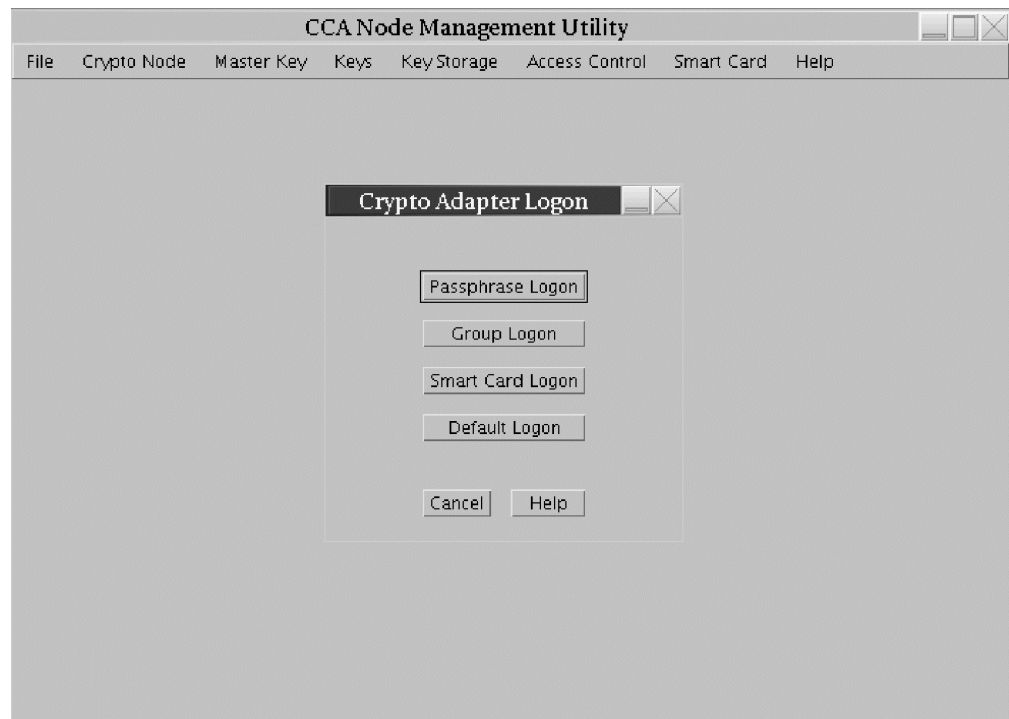


Figure 28. Cryptographic Node Management Utility

You must logon to the TKE workstation crypto adapter as the TKE administrator (TKEADM user name). To do this, click **Passphrase Logon...** from the Crypto Adapter Logon Screen.



**Note:** You will not be prompted for a logon if you previously logged on and did an exit without a logoff.

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 230 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 or USB flash memory drive.

**Warnings:**

1. 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 "TKE Media Manager" on page 313.
2. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

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 74. Refer to "Define a User Profile" on page 222 for instructions on defining a user profile. Backup your profiles to DVD-RAM or USB flash memory drive.

**Warnings:**

1. 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 "TKE Media Manager" on page 313.
2. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

**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 workstation crypto 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 222. You then need to define a group profile and assign the user profiles to the group profile (see "Define a Group Profile" on page 228).

**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 TKE workstation crypto adapter. 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 209. If using group logon, see “Group Logon” on page 210.

Logon to the TKE workstation crypto adapter as KEYMAN1. The master keys should be changed. Follow the directions in “Loading a new master key from clear key parts” on page 233 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 TKE workstation crypto adapter. Backup any key files to a DVD-RAM or USB flash memory drive.

**Warnings:**

1. 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 “TKE Media Manager” on page 313.
2. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

**Load Last Key Part:** If using passphrase logon, see “Passphrase Logon” on page 209. If using group logon, see “Group Logon” on page 210.

Next, logon to the TKE workstation crypto adapter 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 238 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 “TKE Media Manager” on page 313.

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 Parts	X'001C'
Compute Verification Pattern	X'001D'
Decipher	X'000F'
Delete Retained Key	X'0203'

Table 6. TKEUSER Role (continued)

Function	Access Control Point
Digital Signature Generate	X'0100'
Digital Signature Verify	X'0101'
Encipher	X'000E'
Export Card Device Certificate	X'02A9'
Generate Key	X'008E'
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'
OA Proxy Key Generate	X'0344'
OA Proxy Signature Return	X'0345'
Permit Regeneration Data From Retained Keys	X'027E'
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'
Symmetric Algorithm Decipher - secure AES keys	X'012B'
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'
Clear FCV	X'011A'
Compute Verification Pattern	X'001D'
Delete Device Retained Key	X'02A8'
Delete Retained Key	X'0203'
Delete Role	X'0118'

Table 7. TKEADM Role (continued)

Function	Access Control Point
Delete User Profile	X'0117'
Digital Signature Generate	X'0100'
Export Card Device Certificate	X'02A9'
Export CA Public Certificate	X'02AA'
Import Card Device Certificate	X'02A5'
Import CA Public Certificate	X'02A6'
Initialize Access Control	X'0112'
Load FCV	X'0119'
Load Roles and Profiles	X'0116'
One-Way Hash SHA-1	X'0107'
Permit Regeneration Data From Retained Keys	X'027E'
PKA Key Generate	X'0103'
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'
Symmetric Algorithm Decipher - secure AES keys	X'012B'
TKE USER	X'8002'

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'
Delete Retained Key	X'0203'
Digital Signature Generate	X'0100'
Generate Key	X'008E'
Load Roles and Profiles	X'0116'
Load first Master Key Part	X'0018'
Permit Regeneration Data From Retained Keys	X'027E'
PKA Key Generate	X'0103'
Symmetric Algorithm Decipher - secure AES keys	X'012B'

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 storages.

Table 9. KEYMAN2 Role

Function	Access Control Point
Combine Master Key Parts	X'0019'
Compute Verification Pattern	X'001D'
Delete Retained Key	X'0203'
Digital Signature Generate	X'0100'
Generate Key	X'008E'
Load Roles and Profiles	X'0116'
Permit Regeneration Data From Retained Keys	X'027E'
PKA Key Generate	X'0103'
PKA Key Token Change	X'0102'
Reencipher to Current Master Key	X'0090'
Set Master Key	X'001A'
Symmetric Algorithm Decipher - secure AES keys	X'012B'

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'
Delete Retained Key	X'0203'
Digital Signature Generate	X'0100'
Export Card Device Certificate	X'02A9'
Load Roles and Profiles	X'0116'
Permit Regeneration Data From Retained Keys	X'027E'
PKA Key Generate	X'0103'
Reinitialize Device	X'0111'
Symmetric Algorithm Decipher - secure AES keys	X'012B'

## Initializing TKE for smart cards

**Enable Smart Card Readers in CNM:** The user must first be logged on to the workstation as ADMIN. Click on **Trusted Key Entry** on the left panel, and on the right panel click **Cryptographic Node Management Utility 4.1.0**. Select **Default Logon** on the Crypto Adapter Logon popup. When the application is opened, click on the File dropdown, and click on the **Enable Smart Card Readers**. Close the application.

**Steps to initialize the TKE workstation crypto adapter for smart card support:**

1. To initialize the TKE workstation crypto adapter, click on Trusted Key Entry. Under Applications, click on TKE's IBM Crypto Adapter Initialization. You must be logged on with the ADMIN user name for this task.

A warning will remind you that this operation will initialize your TKE workstation crypto adapter and all modifications will be lost.

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]

Select **Y** if you would like to continue. You will see the following message.

Would you like to prepare your cryptographic coprocessor for Smart Card or Pass Phrase use? (S/P) [default=P]

Select **S** for Smart Card.

The TKE workstation crypto adapter is initialized with the roles 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.

Initialization output will be displayed. When complete, press Enter to exit the task.

2. You must logon to the TKE workstation crypto adapter at this time:  
Open the CNM Utility. You can find this task under Trusted Key Entry, Applications. Click **Cryptographic Node Management Utility 4.1.0** 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 TKE workstation crypto adapter.

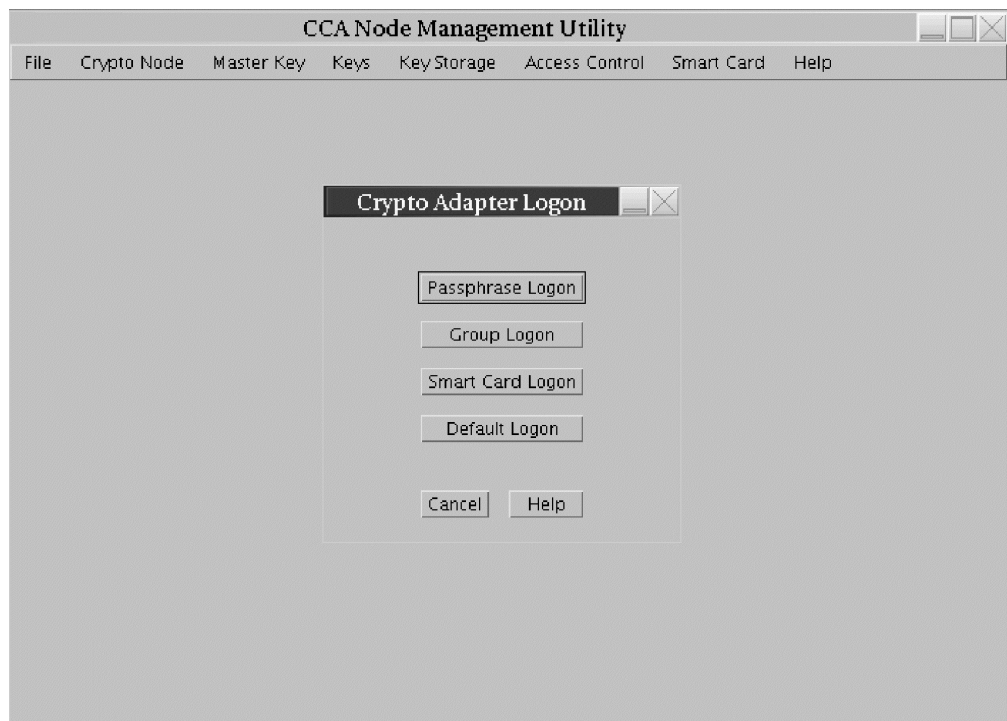


Figure 29. Cryptographic Node Management Utility

You must logon to the TKE workstation crypto adapter using the default logon. To do this, click **Default Logon** on the Crypto Adapter Logon Screen

3. Enable smart card readers in CNM. To do this, select **Enable Smart Card Readers** from the **File** menu.
4. SCUP initialization tasks (You must be logged onto the workstation as ADMIN. When opening the SCUP application, use the default logon and complete the tasks.)
  - a. Initialize and personalize a CA smart card.  
(see “Initialize and personalize the CA smart card” on page 258)
  - b. Backup CA smart card.  
(see “Backup a CA smart card” on page 261)
  - c. Enroll local TKE cryptographic adapter. Enroll remote TKE cryptographic adapter if applicable.  
(see “Enroll a TKE cryptographic adapter” on page 265)
  - d. Initialize and enroll TKE smart cards.  
(see “Initialize and enroll a TKE smart card” on page 263)
  - e. Personalize TKE smart cards.  
(see “Personalize a TKE smart card” on page 264)

Close the SCUP application.
5. CNM initialization tasks (You must be logged onto the workstation as ADMIN. When starting the CNM application, use the default logon and complete the tasks.)
  - a. Generate Crypto Adapter logon keys to TKE smart cards that will be used to logon to the TKE Workstation Crypto Adapter.  
(see “Generate TKE Crypto Adapter logon key” on page 244.)
  - b. Define user profiles for the TKE smart cards which have a Crypto Adapter logon key.  
(see “Define a User Profile” on page 222.)
  - 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 228.)
  - 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 218.
  - e. Logon to the TKE workstation crypto adapter using a TKE smart card profile or a smart card group profile.  
(see “Smart Card Logon” on page 210 or “Smart Card Group Logon” on page 212.)
  - f. Generate a TKE workstation crypto adapter first key part to a TKE smart card.  
(see “Generating master key parts to a TKE smart card” on page 235.)
  - g. Load the first key part to the new master key register.  
(see “Loading master key parts from a TKE smart card” on page 237.)
  - 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 238.)



- j. Set the master key.
- k. Reencipher DES/PKA key storage.  
(see “Reenciphering key storage” on page 241.)

**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 Parts	X'001C'
Compute Verification Pattern	X'001D'
Decipher	X'000F'
Delete Retained Key	X'0203'
Digital Signature Generate	X'0100'
Digital Signature Verify	X'0101'
Encipher	X'000E'
Export Card Device Certificate	X'02A9'
Generate Key	X'008E'
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'
OA Proxy Key Generate	X'0344'
OA Proxy Signature Return	X'0345'
Permit Regeneration Data From Retained Keys	X'027E'
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'
Symmetric Algorithm Decipher - secure AES keys	X'012B'
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'
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 Device Retained Key	X'02A8'
Delete Retained Key	X'0203'
Delete Role	X'0118'
Delete User Profile	X'0117'
Digital Signature Generate	X'0100'
Export Card Device Certificate	X'02A9'
Export CA Public Certificate	X'02AA'
Generate Key	X'008E'
Import Card Device Certificate	X'02A5'
Import CA Public Certificate	X'02A6'
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'
Permit Regeneration Data From Retained Keys	X'027E'
PKA Key Generate	X'0103'
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'

Table 12. SCTKEADM Role (continued)

Function	Access Control Point
Symmetric Algorithm Decipher - secure AES keys	X'012B'
TKE USER	X'8002'
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 workstation crypto adapter.

Table 13. DEFAULT Role

Function	Access Control Point
Compute Verification Pattern	X'001D'
Delete Retained Key	X'0203'
Digital Signature Generate	X'0100'
Export Card Device Certificate	X'02A9'
Load Roles and Profiles	X'0116'
Permit Regeneration Data From Retained Keys	X'027E'
PKA Key Generate	X'0103'
Reinitialize Device	X'0111'
Symmetric Algorithm Decipher - secure AES keys	X'012B'

## Customize the TKE Application

1. Open the TKE Application by clicking on Trusted Key Entry and then clicking on Trusted Key Entry 7.0.
2. Logon to the TKE workstation crypto adapter. See Workstation Logon: Passphrase or Smart Card on “Crypto Adapter Logon: Passphrase or Smart card” on page 85 for details.
3. Click on Preferences on the task bar.
4. Enable/Disable the Preferences as appropriate. See “TKE Customization” on page 121 for details.

## Configure 3270 Emulators

An MVS session is required on the host for several tasks executed on TKE 7.0 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**.

The Configure 3270 Emulators window is displayed.



Figure 30. Configure 3270 Emulators

1. Click on **New** to add a 3270 session.
2. The Add 3270 Emulator Session window is displayed.
3. Enter the Host Address you would like to connect to.
4. Select 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.

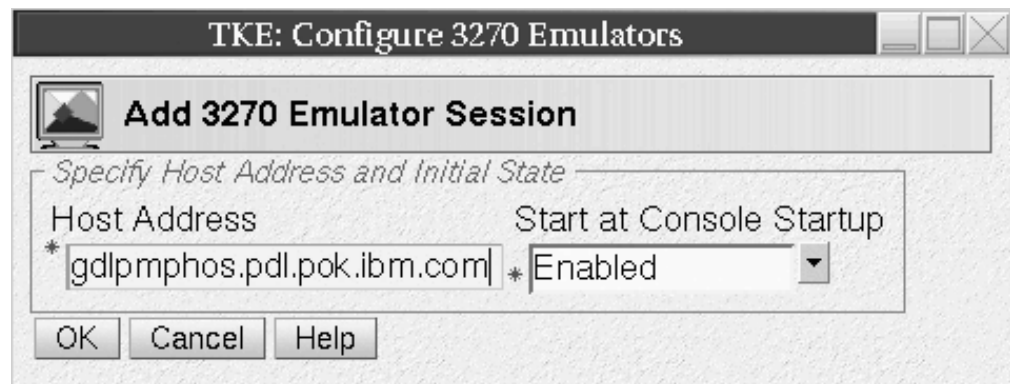


Figure 31. Add 3270 Emulator Session

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 32. 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**.

If you click on **Edit Keymap**, you can edit the keymap in the 3270 emulator session. You can customize the keyboard functions while in a 3270 session.

## Chapter 5. TKE Up and Running

The Trusted Key Entry console automatically loads with a set of commonly used tasks. You then logon with a predefined user name, depending on the type of task required.

### Crypto Adapter Logon: Passphrase or Smart card

If you have installed TKE V 7.0, 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 71
- Smart card - see “Initializing TKE for smart cards” on page 77

From the Framework tree on the left hand panel of the main TKE console screen, click on **Trusted key Entry**, then click on **Trusted Key Entry 7.0**.

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.

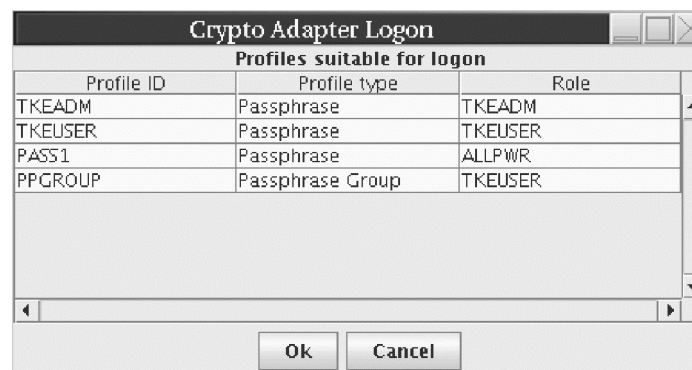


Figure 33. Crypto Adapter logon window with passphrase profiles

Steps for logging on are:

1. Select the Profile ID that you would like to use to log on to the TKE workstation crypto adapter.
2. Select **OK**

#### ***If you selected a single passphrase profile ID***

1. The Passphrase Logon window will be displayed.

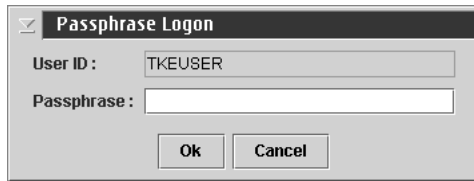


Figure 34. Enter passphrase for logon

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 35. Crypto Adapter group logon window with passphrase profiles

2. Select the member profile ID that you would like to use to log on to the TKE workstation crypto adapter.
3. Select **OK**  
The Passphrase Logon window is displayed.
4. Enter the passphrase for this profile ID and select **OK**.

**Note:** The passphrase is case sensitive.

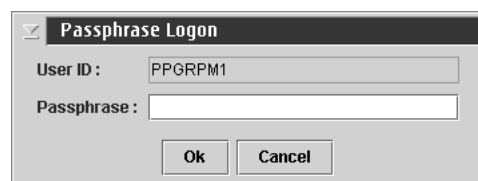


Figure 36. Enter passphrase for logon

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



Figure 37. Crypto Adapter Group logon window with passphrase profile ready

6. Repeat steps 2-4 until the number of group members required for logon is met

**Note:** If the group logon should fail, the *Group members ready for logon* is reset to zero and group logon must start over.

Once the single or group passphrase logon is successful, the TKE application will be opened for use.

You may use the predefined user profile, TKEUSER, for single passphrase logon or another user profile with an equivalent role. If you choose to use passphrase group logon, the TKE Administrator must create a passphrase group profile and add the single user passphrase profiles to the group profile. The passphrase group profile should be mapped to the TKEUSER role or an equivalent role. The single user profiles that will be added to the group profile should be mapped to the DEFAULT role. This is done to limit the services permitted to the single users outside of the group. For details on creating single and group passphrase profiles see Chapter 10, “Cryptographic Node Management Utility (CNM),” on page 209.

## 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 38. Crypto Adapter Logon Window with smart card profiles

Steps for logging on are:

1. Select the profile ID that you would like to use to log on to the TKE workstation crypto adapter.
2. Select **OK**.

**If you selected a single smart card profile ID**

1. The Smart Card Logon window will be displayed.
2. Insert the TKE smart card that contains the TKE workstation crypto adapter logon key for the selected profile ID and select **OK**

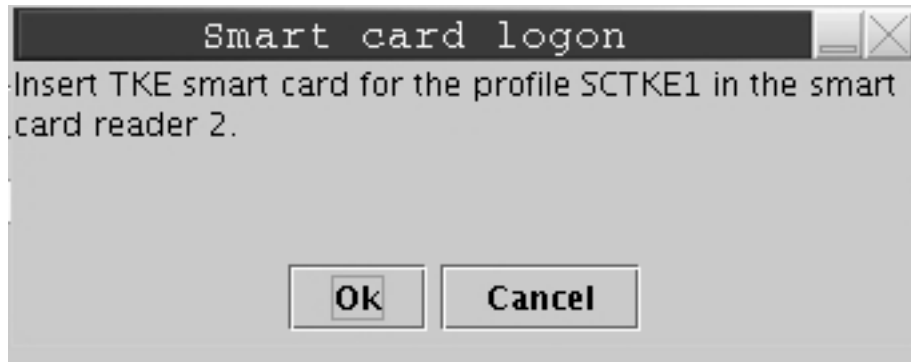


Figure 39. Insert the TKE smart card

3. A message box displays, instructing you to "Enter your PIN in the Smart Card Reader". Enter the PIN for the TKE smart card.

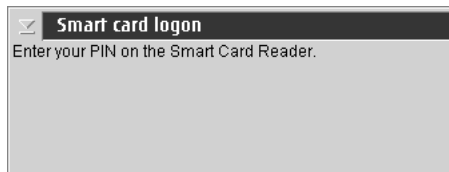


Figure 40. Enter smart card PIN

***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 41. Crypto Adapter Group logon window with smart card profiles

2. Select the member profile ID that you would like to use to log on to the TKE workstation crypto adapter.
3. Select **OK**  
The Smart card logon window is displayed.
4. Insert the TKE smart card that contains the TKE workstation crypto adapter logon key for the selected profile ID and select **OK**

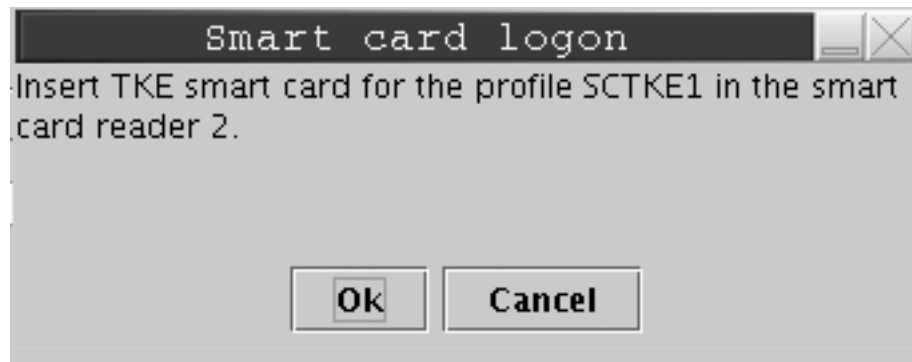


Figure 42. Insert the TKE smart card

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



Figure 43. Crypto Adapter Group logon window with smart card profile ready

6. Repeat steps 2-4 until the number of group members required for logon is met

**Note:** If the group logon should fail, the *Group members ready for logon* is reset to zero and group logon must start over.

Once the single or group smart card logon is successful, the TKE application will be opened for use.

You may use a group smart card profile assigned to the predefined role SCTKEUSR, or another user profile assigned to an equivalent role. If you choose to use single smart card logon, the TKE Administrator must create a single smart card user profile and map it to the SCTKEUSR role or an equivalent role. If a smart card group profile is used, the TKE Administrator must define single smart card user profiles to be added to the group. The single user profiles that will be added to the group profile should be mapped to the DEFAULT role. This is done to limit the services permitted to the single users outside of the group. For details on creating single and group smart card profiles see Chapter 10, "Cryptographic Node Management Utility (CNM)," on page 209.

With either passphrase or smart card logon, if you cancel the logon, the TKE application is not opened.

## Automated Crypto Module Recognition

For each host, the TKE workstation maintains a list of the installed crypto modules. The list contains all the information required to protect communication between the workstation and the host crypto modules.

Whenever the user of the workstation connects to a host, TKE queries the host to determine the installed cryptographic hardware. The resulting list is compared to the contents of the crypto module file.

The user is notified if any of the following events occur:

- A new crypto module has been installed

- A crypto module has been removed
- A crypto module has been replaced
- A crypto module had its authority signature key pair regenerated
- A crypto module has been moved from one slot to another

## 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 host crypto module.

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

On the Authenticate crypto module window:

- Press **Yes** if the coprocessor index and serial number on the host match the index and CMID on the window. The CMID value is saved on the TKE workstation for further communication with the host crypto module. The crypto module is marked as **Authenticated**.
- Press **No** if they do not match. The crypto module is marked as **Rejected by user**. You will not be able to work with the host crypto module but you are able to authenticate the module again. You select the crypto module and the CMID/type window is displayed for you to accept or reject the values.

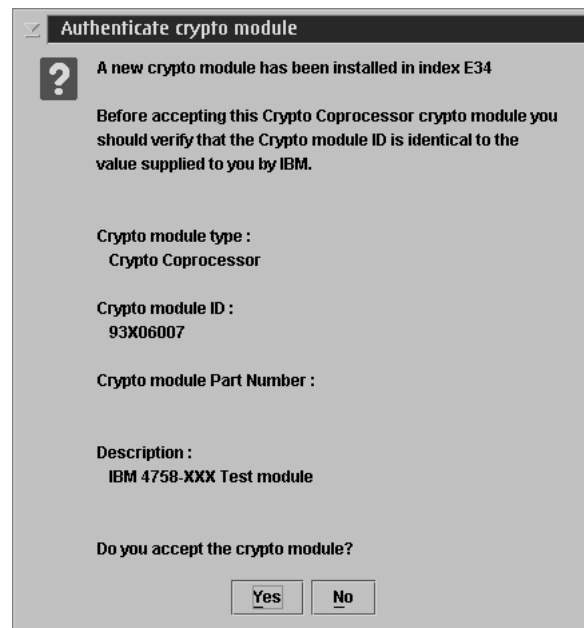


Figure 44. Authenticate Crypto Module

**Attention!** The crypto module type for the CEX2C and CEX3C on the TKE panels is “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 Customer Engineer (CE) may need to reload code in the host crypto module on the host for maintenance. If the code is reloaded, it may become necessary to reauthenticate the host crypto module during the first communication with it after the code reload. The reauthentication is necessary because the authority signature key has been regenerated.

---

## Initial Authorities

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

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 or USB flash memory drive 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 in “Workstation Files” and “Host Files” on page 93. 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. Two USB flash memory drives are shipped with your TKE workstation for backup purposes. Alternatively, a customer-supplied DVD-RAM may be used. See “Backup Critical Console Data” on page 323 and “TKE File Management Utility” on page 311 for more information.

## Workstation Files

Following is a list of the TKE application specific files. These files should be backed up whenever definitions are changed.

- 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.
- domaingroup.dat — contains definitions for domain groups.
- desstore.dat and desstore.dat.NDX — DES Key Storage used to hold IMP-PKA keys for encrypting RSA keys, IMPORTER keys, and EXPORTER keys.
- pkastore.dat and pkastore.dat.NDX — PKA Key Storage used to hold one authority signature key.
- kphcard.dat — contains information for the KPH smart cards known to the TKE workstation.
- zone.dat — contains information for the configuration migration zones known to the TKE workstation.

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

- Passphrase
  - default\_70.rol
  - tempdefault\_70.rol
  - tkeusr\_70.rol
  - tkeadm\_70.rol
  - keyman1\_70.rol
  - keyman2\_70.rol
  - tkeuser.pro
  - tkeadm.pro
  - keyman1.pro
  - keyman2.pro
- Smart card
  - default\_70.rol
  - tempdefault\_70.rol
  - sctkeusr\_70.rol
  - sctkeadm\_70.rol
  - sctkeusr.pro
  - sctkeadm.pro

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

## Host Files

One file (or dataset as it is referred to on z/OS) on the MVS Host system should be saved. The saved file is the name of the crypto module dataset and is defined in the Job Control Language (JCL) used to start the TKE Host Transaction program (see Chapter 4, “TKE Setup and Customization,” on page 59).

- Name of the crypto module dataset — this file is updated anytime the user makes changes in the TKE application windows and crypto module notebooks for the host crypto module. It contains host 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 files are documented in Chapter 4, “TKE Setup and Customization,” on page 59.



## Chapter 6. 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 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.

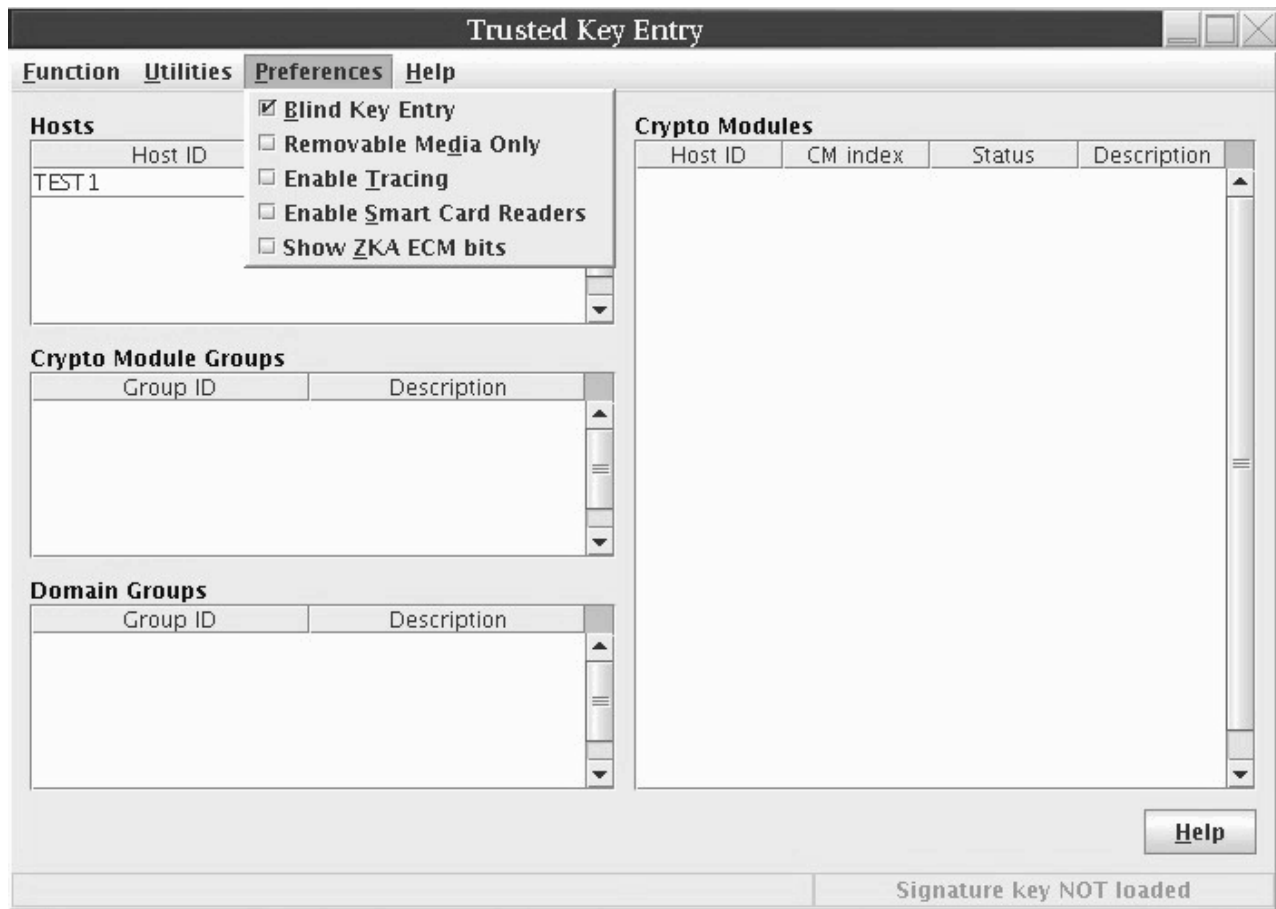


Figure 45. TKE Preferences

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 121.

**Note:** When the 'Enable Smart Card Readers' preference is enabled or disabled, the updated setting does not take effect until you restart the TKE application.

The main window has four containers labeled Hosts, Crypto Module Groups, Domain 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 Crypto Module Groups container or the Domain Groups container.

Note the message in the lower right corner that the signature key is not loaded. See “Load Signature Key” on page 113.

---

## Host Logon

To logon, double-click on the host entry. If working with a crypto module group or domain group, double click on the crypto module group or domain group. When you open a crypto module group or domain 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.

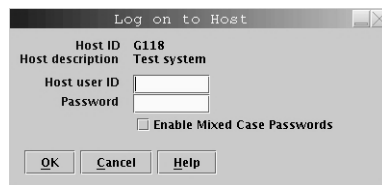


Figure 46. Host Logon Window

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 of the TKE Main Window lists the host IDs currently defined to the TKE 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. When you have logged in, 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 the **Create Host** menu item.

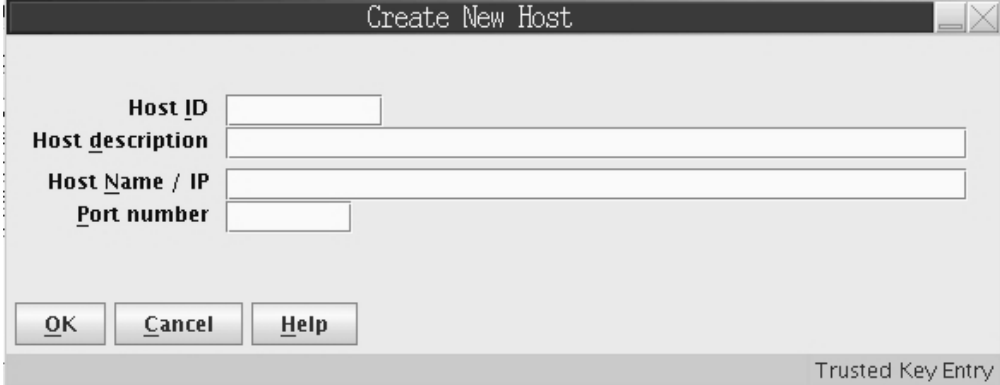


Figure 47. Create Host

The host definition contains the following information:

- *Host ID* — Mandatory free format text used for referencing the host within TKE.
- *Host description* — Free-format text for your own use
- *Host Name / IP* — Address in decimal-dot notation of the host where the TKE Host Transaction Program server is running. The field can contain a host name or a TCP/IP address in either TCP/IP V4 or TCP/IP V6 format.
- *Port number* — Application port number reserved in your host TCP/IP profile for the TKE Host Transaction Program server. See Chapter 4, “TKE Setup and Customization,” on page 59.

It is not necessary to define each logical partition to TKE. One partition will have its control domain contain its own domain as well as any other domain where you want to load keys. This domain must be unique and must have access to all host crypto modules that it is to control.

For additional details on LPAR setup, refer to Appendix C, “LPAR Considerations,” on page 291.

## 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 the **Change Host** menu item.

You can change the host description, IP address and port number. However, you cannot change the host ID. If you want to change the host ID, you must delete the host definition. You then create a new host ID.

## Deleting Host Entries

To delete a host definition, highlight the host you want to delete from the hosts container and right mouse click. A pop-up menu is displayed. Select the **Delete Host** menu item. A confirmation message is displayed. Select **Yes** to confirm the delete request. Select **No** to cancel the delete.

---

## Working with Crypto Modules

The crypto module container of the TKE Main Window displays the crypto modules that are available for use with the host or group you have selected. The container lists the 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 48 illustrates 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 Signature Key” on page 113.

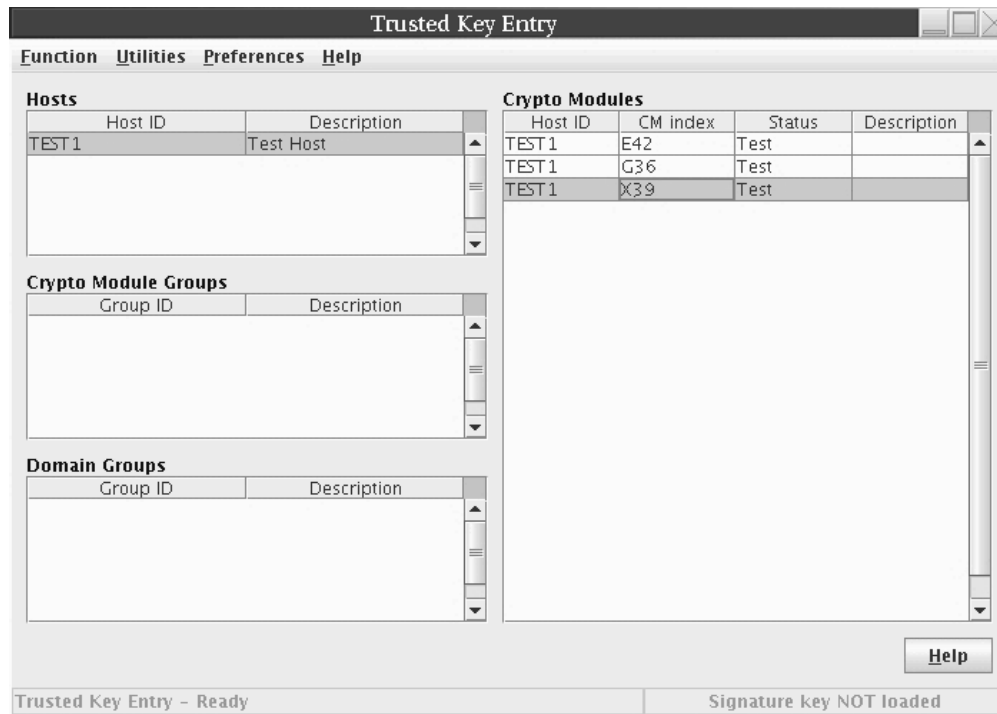


Figure 48. Main Window

As discussed in “Automated Crypto Module Recognition” on page 90, 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 Crypto Module Groups

You manage crypto module groups in the TKE main window. You can add, change or delete crypto module group definitions from the Crypto Module Groups container.

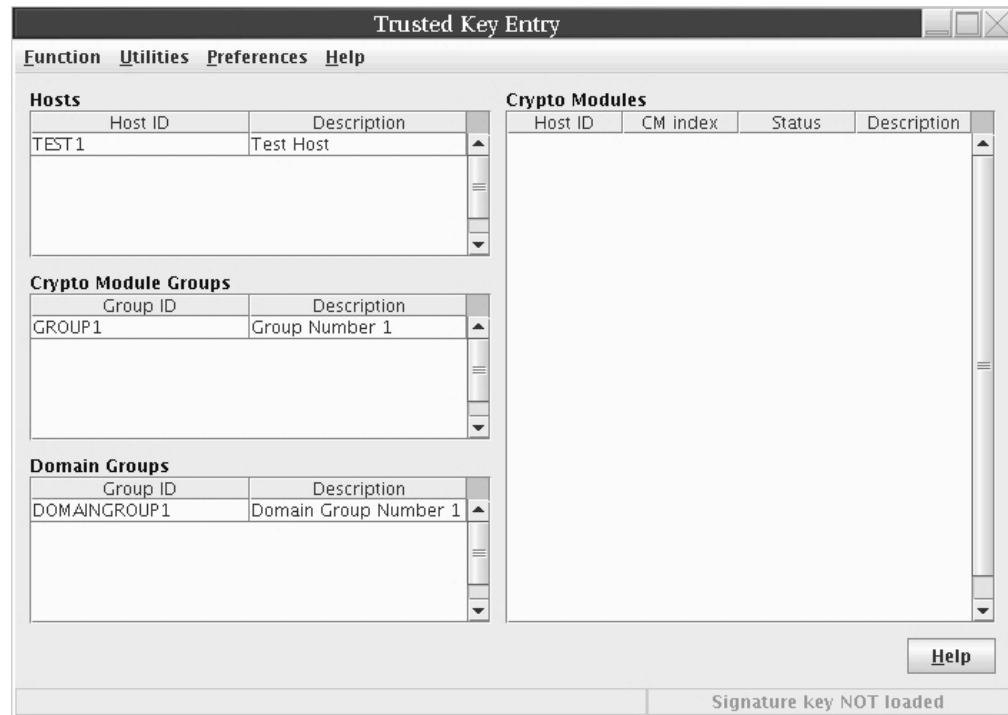


Figure 49. Main Window - working with crypto module groups

The crypto module group concept allows you to perform operations on a set of crypto modules as you would on a single crypto module. A crypto module group can include crypto modules from different hosts.

It is highly recommended that you create crypto module groups for easier management of your host crypto modules.

TKE 6.0 and later allows you to create AES keys if you have either a CEX2C that is AES capable or a CEX3C. To perform AES functions on a crypto module group, the master module must be a crypto module that is AES capable. You can mix AES and non-AES cards together, but the master module must be an AES capable module if the crypto module group is intended to perform AES actions.

TKE 7.0 allows you to manage ECC keys if you have a CEX3C that is ECC capable. To perform ECC functions on a crypto module group, the master module must be a crypto module that is ECC capable. You can mix ECC and non-ECC cards together, but the master module must be an ECC capable module if the crypto module group is intended to perform ECC actions.

In general, you work with the crypto module 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 crypto module group are the values of the master crypto module. You select the master crypto module when you create the crypto module group.

It is important that the crypto modules within a crypto module group are in the same state. This is achieved by always working on the crypto modules through the crypto module group interface. When doing access control administration or loading master keys, you should always work with crypto module groups to ensure that the values are the same across all crypto modules.

If a crypto module group is selected when loading operational key parts to key part registers, only the master crypto module will be loaded, even if the crypto module group contains other crypto modules.

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

When you work with a crypto module group, you do not use the host container. To open, you double-click or right-click on one of the groups defined in the crypto module groups container. You will be prompted to log on to the hosts associated with the crypto module members of the crypto module group.

When you open the crypto modules of a crypto module group, a Crypto Module Notebook is displayed.

## Creating a Crypto Module Group

To create a new crypto module group:

1. Right-click the mouse button in the Crypto Module Groups container.  
A popup menu displays.
2. Select the **Create Group** menu item from the popup menu.  
The Create New Group window opens.

The screenshot shows the 'Create New Group' dialog box. It features a title bar with the text 'Create New Group'. Inside the dialog, there are two text input fields: 'Group ID' and 'Group Description'. Below these fields is a 'Host' dropdown menu. To the right of the 'Host' dropdown is a table titled 'Crypto Modules In Group' with three columns: 'Host ID', 'CM index', and 'Master Module'. To the left of this table is another table titled 'Crypto Modules Available On Host' with two columns: 'CM index' and 'Description'. Between these two tables are two buttons: 'Add >>' and '<< Remove'. At the bottom of the dialog are three buttons: 'Close', 'Cancel', and 'Help'. The text 'Trusted Key Entry' is located in the bottom right corner of the dialog.

Figure 50. Create New Group

3. Enter your information in the following fields:
  - a. *Group ID* - Name of the crypto module group (mandatory)
  - b. *Description* - Optional free text description
  - c. Select the crypto modules to be included in the crypto module group:

- 1) In the Host drop down list, select the host containing the crypto modules you want to include in the crypto module group.  
You will be prompted to log on 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 crypto module group.
  - 3) Press **Add**, and the crypto modules selected now appear in the container: Crypto Modules in Group
  - 4) Repeat the prior three steps as required.
- d. 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 crypto module group. Unless you change it, the first crypto module added to the crypto module group becomes the master module.
- TKE 6.0 and later allows you to create AES keys if you have a CEX2C that is AES capable or a CEX3C. To perform AES functions on a crypto module group, the master module must be a crypto module that is AES capable. You can mix AES and non-AES cards together, but the master module must be an AES capable module if the crypto module group is intended to perform AES actions.
- TKE 7.0 allows you to manage ECC keys if you have a CEX3C that is ECC capable. To perform ECC functions on a crypto module group, the master module must be a crypto module that is ECC capable. You can mix ECC and non-ECC cards together, but the master module must be an ECC capable module if the crypto module group is intended to perform ECC actions.
- e. When finished, press **Close**.

## Changing a Crypto Module Group

To change a crypto module group:

1. Highlight the crypto module group you want to work with in the Crypto Module Groups container and then right-click the mouse button.  
A popup menu displays.
2. Select the **Change Group** menu item from the popup menu.  
The Change Group window opens.

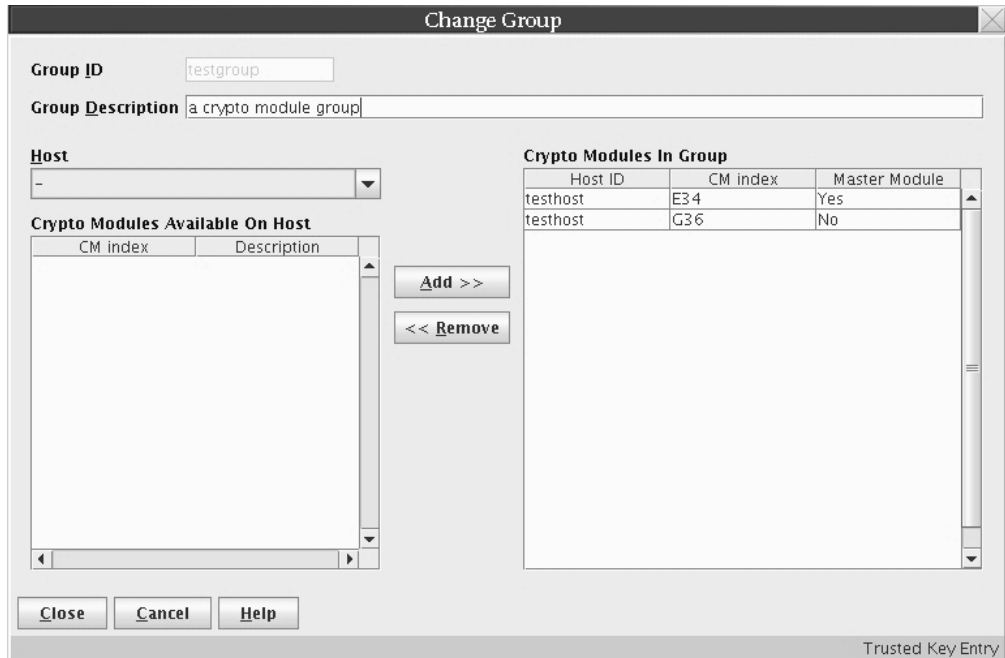


Figure 51. Change Group

3. To change the description, edit the following field:
  - *Description* - Optional free text description
4. To add more crypto modules to the crypto module group, do the following:
  - a. In the Host drop down list, select the host that has the crypto modules you want to add to the crypto module 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 crypto module group.
  - c. Press **Add**, and the crypto modules selected now appear in the “Crypto Modules in Group” container.
  - d. Repeat steps 1-3 as required.
5. To remove crypto modules from the crypto module group, select the modules in the Crypto Modules in Group container and press **Remove**. If you remove the master module, you are prompted to set another master module.
6. When finished, press **Close**.

### Changing the Master Crypto Module

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

To change the master crypto module for a crypto module group:

1. Highlight the crypto module you want to set as the master module and right mouse click.  
A popup menu displays.
2. Select the **Set as Master Module** menu item from the popup menu.  
The master module is changed.

TKE 6.0 and later allows you to create AES keys if you have a CEX2C that is AES capable or a CEX3C. To perform AES functions on a crypto module group, the master module must be a crypto module that is AES capable. You can mix AES and non-AES cards together, but the master module must be an AES capable module if the crypto module group is intended to perform AES actions.

TKE 7.0 allows you to manage ECC keys if you have a CEX3C that is ECC capable. To perform ECC functions on a crypto module group, the master module must be a crypto module that is ECC capable. You can mix ECC and non-ECC cards together, but the master module must be an ECC capable module if the crypto module group is intended to perform ECC actions.

## Comparing Crypto Module Groups

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

To compare the crypto modules, do the following:

1. Highlight a specific crypto module group in the Crypto Module Groups container from the main window.
2. Right click on the highlighted entry to display a popup menu, and select **Open Group** from the menu.

This displays the list of crypto modules in the Crypto Modules container.

3. Right click within the Crypto Modules container to display a popup menu, and select **Open Crypto Module Group** from the menu.

This opens the crypto module group notebook.

4. Select **Compare Group** from the **Function** pulldown menu.

TKE reads and compares information from all the crypto modules in the crypto module 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.

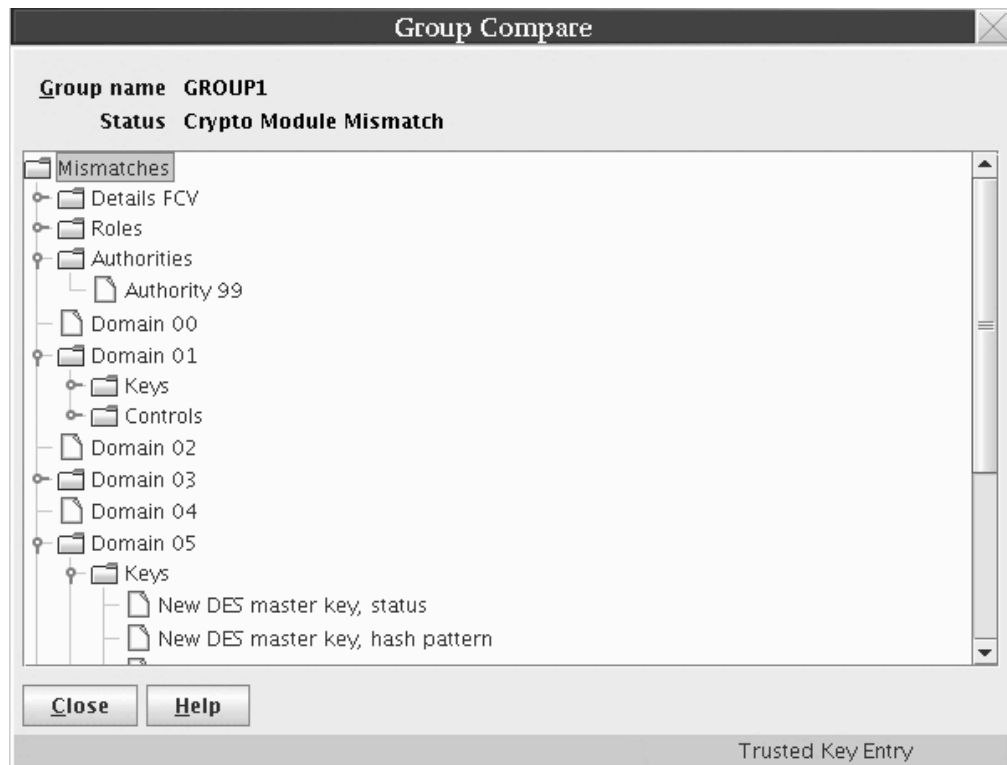


Figure 52. Group Compare

The Group Compare window displays the results:

- *Group Name* — Name of the crypto module 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 crypto module group with the actual values for that property is displayed.

## TKE Functions Supporting Crypto Module Groups

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

- Create, change, and delete authority
- Create, change, and delete role
- Zeroize domain
- Domain Controls changes
- Enable/disable crypto modules
- Domain keys:
  - Load key part to new master key register
  - Clear key register
  - Set ASYM master key
  - Load RSA key to PKDS
  - Load RSA key to dataset
  - Load operational key part to key part register (executed only on the master crypto module of the group)



- View operational key part registers (executed only on the master crypto module of the group).
- Clear operational key part registers (executed only on the master crypto module of the group)
- Co-sign pending commands
- Change signature index for notebook
- Release crypto modules

## Working with Domain Groups

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

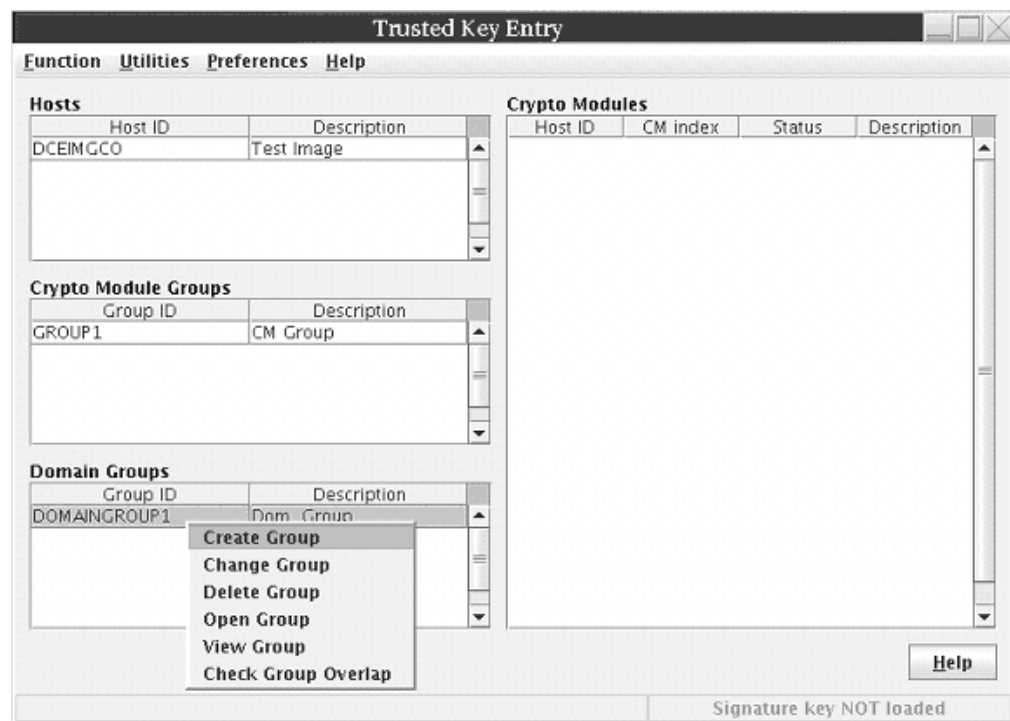


Figure 53. Main Window - working with domain groups

The domain group concept allows you to perform operations on a set of crypto module domains as you would on a single crypto module domain. A domain group can include crypto modules from many hosts.

TKE 6.0 and later allows you to work with AES keys if you have either a CEX2C that is AES capable, or a CEX3C. To perform AES functions on a domain group, the master domain must be set on a crypto module that is AES capable. You can mix AES and non-AES cards together, but the master domain must be set on an AES-capable module.

TKE 7.0 allows you to manage ECC keys if you have a CEX3C that is ECC capable. To perform ECC functions on a domain group, the master domain must be set on a crypto module that is ECC capable. You can mix ECC and non-ECC cards together, but the master domain must be set on an ECC capable module.

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

For most operations, it is important that the crypto module domains within a domain group are in the same state (for example, identical roles). You maintain this by always working on the crypto modules through the domain group interface, and not operating on the crypto modules individually.

If a domain group is selected when loading operational key parts to key part registers, only the master domain will be loaded, even if the domain group contains other crypto module domains.

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

When you work with a domain group, either double-click or click with the right mouse button on one of the domain groups defined in the Domain Groups container. You will be prompted to log on to the hosts associated with the crypto module members of the domain group.

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

## Creating a Domain Group

To create a new domain group:

1. Right-click the mouse button in the Domain Groups container.  
A popup menu displays.
2. Select the **Create Group** menu item from the popup menu.  
The "Create New Group" window opens.

**Note:** The crypto module types supported are CEX2C and CEX3C.

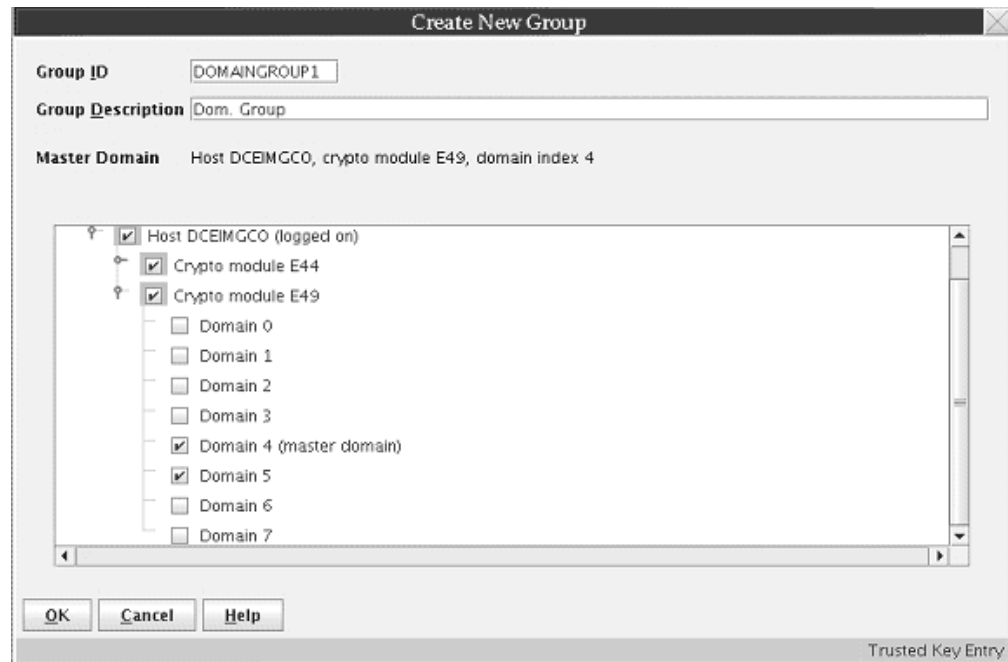


Figure 54. Create Domain Group

3. Enter your information in the following fields:
  - a. *Group ID* - Name of the domain group (mandatory)
  - b. *Description* - Optional free text description
  - c. Select the crypto module domains to be in the domain group. In the Host tree structure, select the domains from each host you want to include in the domain group by selecting the checkbox associated with the domain. You will be prompted to log on to the selected host(s) if you are not currently logged on.

**Note:** Only domains defined as control domains on the crypto adapter will be available for inclusion in the domain group.

- d. Select the crypto module domain to be the Master Domain by right-clicking on the domain and selecting **Make this the Master Domain**. The Master Domain information field of the Create New Group window changes to represent the Master Domain information.

TKE 6.0 and later allows you to work with AES keys if you have a CEX2C that is AES capable, or a CEX3C. To perform AES functions on a domain group, the master domain must be associated with a crypto module that is AES capable. You can mix AES and non-AES cards together, but the master domain must be set on an AES capable module if the domain group is intended to perform AES actions.

TKE 7.0 allows you to manage ECC keys if you have a CEX3C that is ECC capable. To perform ECC functions on a domain group, the master domain must be associated with a crypto module that is ECC capable. You can mix ECC and non-ECC cards together, but the master domain must be set on an ECC capable module if the domain group is intended to perform ECC actions.

- e. When finished, press **OK**.

## Changing a Domain Group

To change a domain group click with the right mouse button in the Domain Groups container in the TKE main window and select the Change Group menu item.

The Change Group window is displayed.

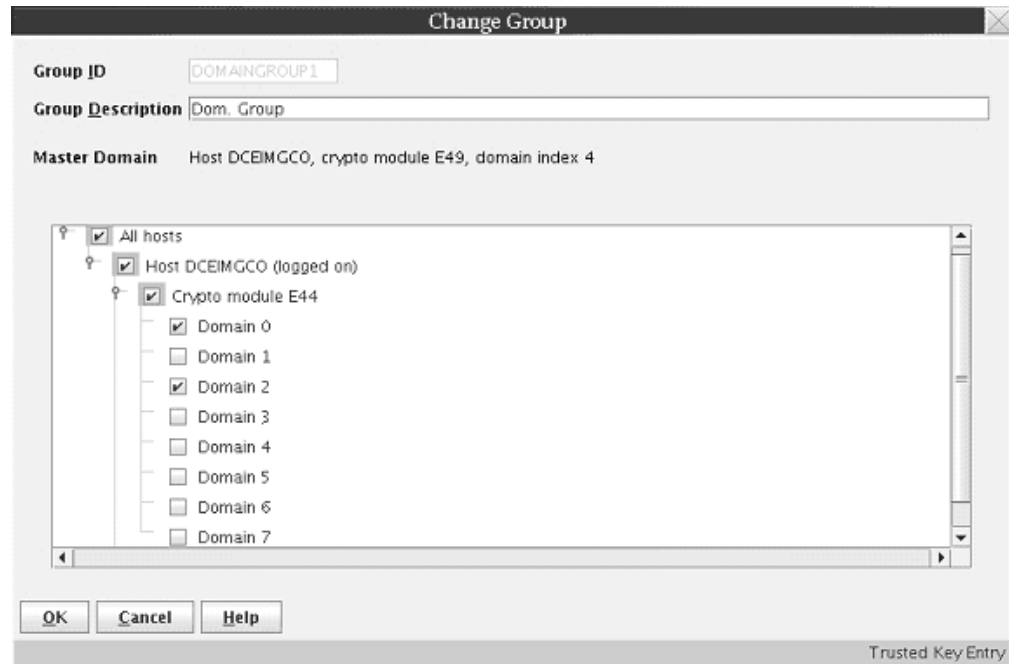


Figure 55. Change Domain Group

To change the description, edit the Group Description field:

To modify which crypto module domains are in the domain group, check the boxes corresponding to the domains to be included in the domain group. At least one domain must be checked.

To refresh the list of crypto modules associated with a host, do the following:

1. Highlight the host with the left mouse button.
2. Click the right mouse button to display a pop-up selection menu.
3. Select **Refresh crypto module list**.

To select which domain is the master domain, do the following:

1. Highlight a checked domain with the left mouse button.
2. Click the right mouse button to display a pop-up selection menu.
3. Select **Make this the master domain** menu item from the popup menu.

One domain must be selected as the master domain.

When finished, press **OK**.

## Viewing a Domain Group

To view a domain group, either right click in the “Domain Groups” container in the TKE main window and select the **View Group** action or open a domain group and

press the **View Group** button on the Domain -> General tab.

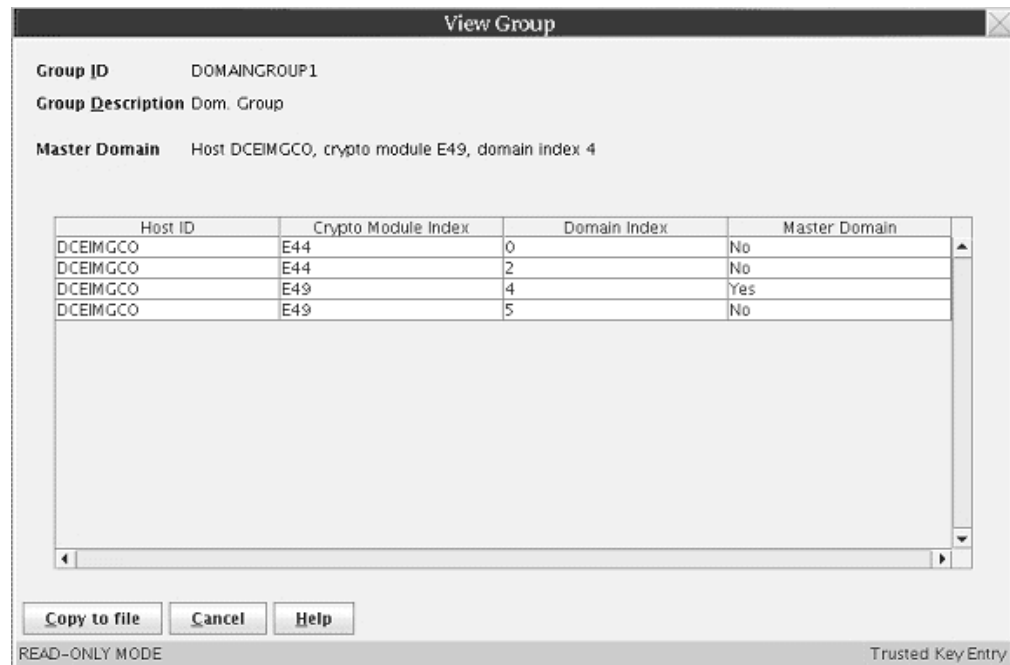


Figure 56. View Domain Group

The “View Group” window is opened. The following information is displayed:

- *Group ID* – The group identifier
- *Group Description* – Optional free text description
- *Master Domain* – The master domain for this domain group. All displayed values for this group are retrieved from this domain.
- *Domain table window* – A window containing a table that lists the crypto module domains in the domain group. There are four columns in the table: Host ID, Crypto Module Index, Domain Index and Master Domain.

You can copy the domain group information to a file by selecting **Copy to file** and specifying the file name and location to be saved. Otherwise, when finished, press **Cancel**.

## Checking Domain Group Overlap

To check if domain groups defined on the TKE workstation contain crypto module domains that are found in more than one domain group, click with the right mouse button in the “Domain Groups” container in the TKE main window and select the “Check Group Overlap” action. The Domain Group Overlap window is opened.

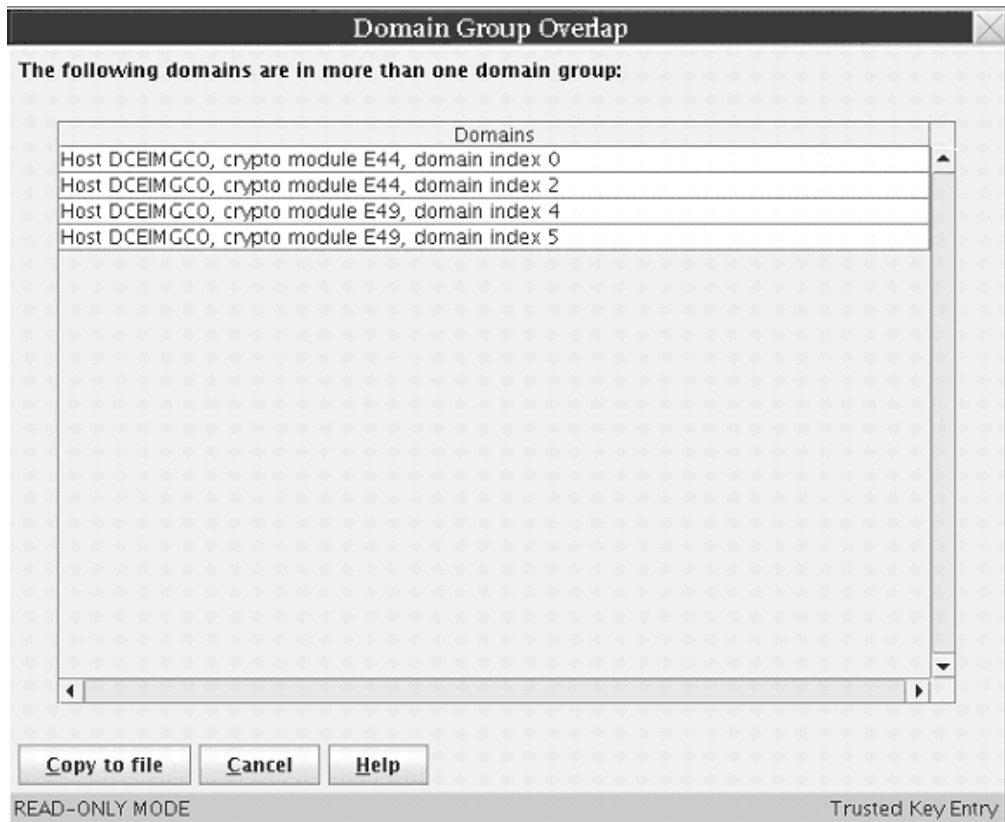


Figure 57. Check Domain Group Overlap

This window displays a list of domains that are specified in more than one domain group defined on the TKE workstation. Double clicking with the left mouse button on one of the domains displays an Overlap Details window that lists the names of the domain groups that contain the selected domain.

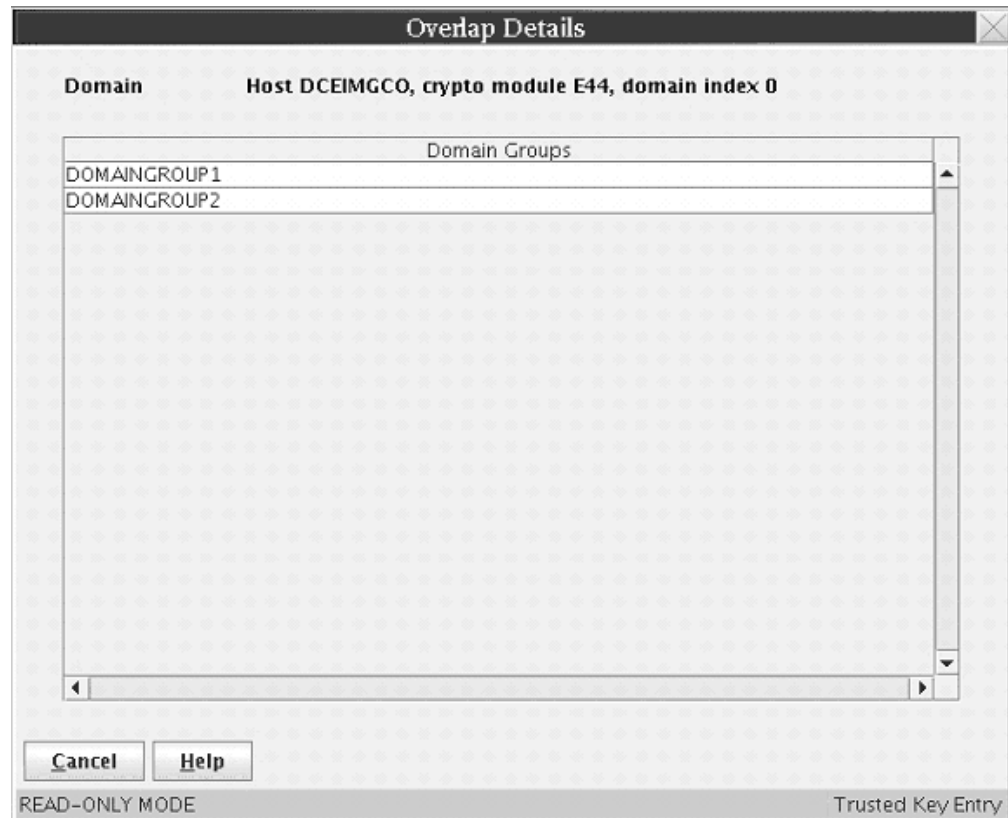


Figure 58. Domain Group Overlap Details

You can copy the domain group overlap information to a file by selecting **Copy to file** and specifying the file name and location to be saved. Otherwise, when finished, press **Cancel**.

## Comparing Groups

Comparing domain groups is not done from the dropdown menu on the main window. The comparison can be done when the domain group notebook is open. It does not compare domain groups, but instead compares the crypto modules within a domain group. To compare the crypto modules, highlight a domain group in the Domain Groups container. You must click with the right mouse button the entry to display the Open Group option, and select the Open Group option. Then the list of crypto modules in the domain group is displayed in the Crypto Modules container. Next, you click with the right mouse button the list of crypto modules to display the Open Domain Group option and select the Open Domain Group option. The crypto module group notebook opens. Click on **Function** and select **Compare Group**.

TKE reads and compares information from all the crypto modules in the domain 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 59. Compare Group

The Domain Group Compare window displays the following results:

- *Group Name* – Name of the group that has been compared
- *Status* – Overall result of the compare operation
- *Mismatches* – A list of properties that do not match.

If you select a property, a list of all crypto modules in the group with the actual values for that property is displayed.

## TKE Functions Supporting Domain Groups

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

- Create, change, and delete authority
- Create, change, and delete role
- Zeroize domains in the domain group
- Domain Controls Changes
- Enable/disable crypto module
- Domain keys:
  - Load key part to new master key register
  - Clear key register
  - Set ASYM master key
  - Load RSA key to PKDS
  - Load RSA key to dataset
  - Load operational key part to key part register (Master domain only)
  - View operational key part registers (Master domain only)



- Clear operational key part registers (Master domain only)
- Co-sign pending commands

---

## Function Menu

These selections are available from the **Function** pull-down menu in the TKE main window:

- **Load signature key...**
- **Display signature key information...**
- **Define transport key policy...**
- **Exit**
- **Exit and logoff**

## Load Signature Key

This function is used to load the authority signature key. This authority 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.

The CEX2C does not support authority signature keys greater than 1024-bits. CEX3C supports 1024-bit, 2048-bit, and 4096-bit authority signature keys.

To create an authority signature key, see “Generating Authority Signature Keys” on page 132.

A Select Source dialog box is displayed for you to select the source of the authority signature key. Select the appropriate radio button, and press the **Continue** command button.



Figure 60. Select Authority Signature Key Source

**Note:** In order to see a smart card as one of the authority signature key sources, you must have previously selected Enable smart card readers through the TKE main window Preferences menu.

- If you specify **Key storage** or **Default key** as the authority signature key source, the Specify authority index dialog is displayed. Specify the authority index to be used, and press the **Continue** command button.

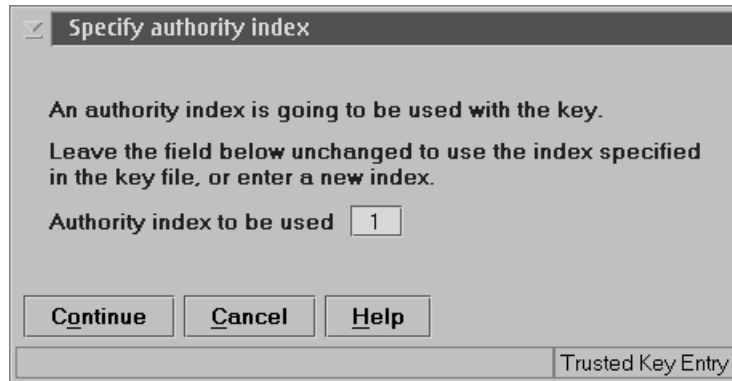


Figure 61. Specify Authority Index

- If you specify **Binary file** as the authority signature key source, the Load Signature Key window is displayed. In this window, you must either select a file from the container or enter a file name. Additionally, you must enter a password. This assumes the authority signature key was previously generated and saved to a binary file.

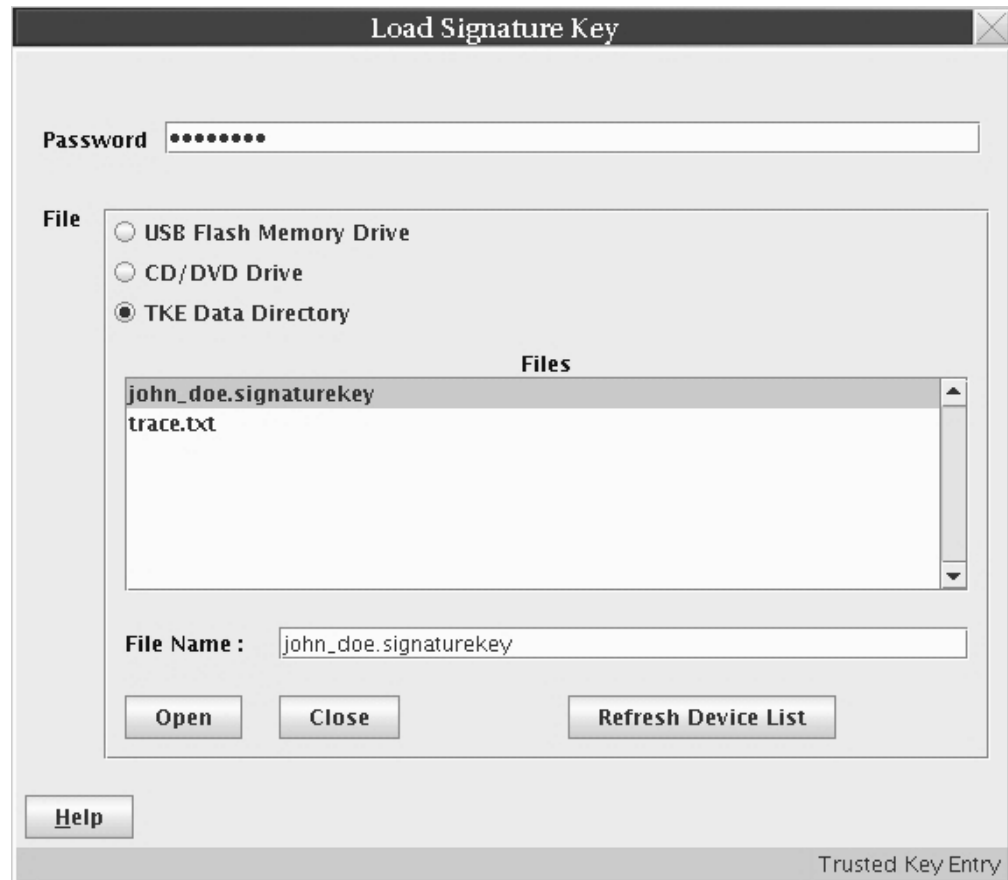


Figure 62. Load Signature Key

You will then be prompted to specify the authority index.

- If you select **Smart card in reader 1** or **Smart card in reader 1**, you will be prompted to insert your TKE smart card into the smart card reader. You will then you will be prompted to enter the PIN on the PIN pad.

You will then be prompted to specify the authority index.

## Display signature key information

Selecting **Display signature key information** displays a panel showing the current signature index and the key identifier for the current authority signature key.

## Define Transport Key Policy

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

From the TKE main window, selecting **Function → Define Transport Key Policy...** displays the Select Transport Key Policy window. This window lets you choose the transport key policy to follow.

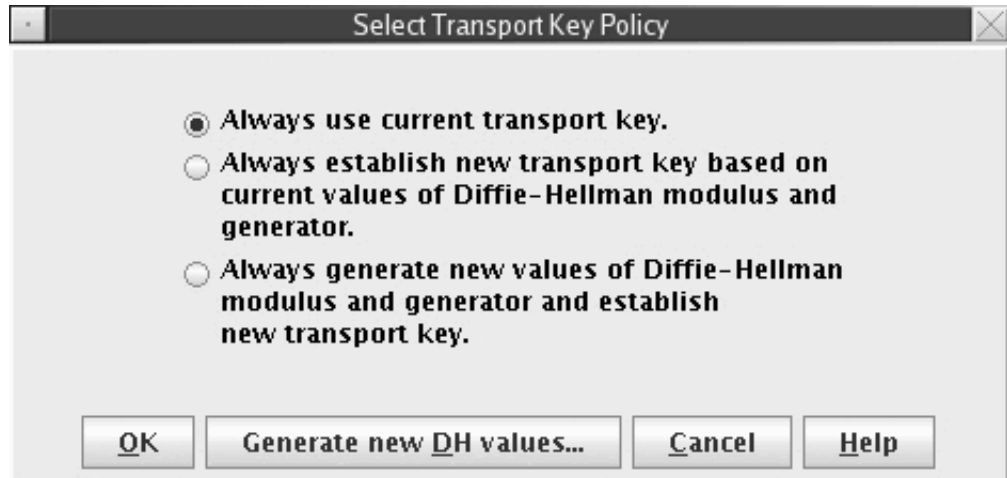


Figure 63. Select Transport Key Policy

Using the Select Transport Key Policy window, you can select one of the following:

- **Always use current transport key.**

This is the default. 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).

- **Always establish new transport key based on current values of Diffie-Hellman modulus and generator.**

If 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 if reusing the Diffie-Hellman modulus and generator values.

- **Always generate new values of Diffie-Hellman modulus and generator and establish new transport key.**

The last selection in the Transport Key Policy dialog box allows you 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 window but does not log the current user off the TKE workstation crypto adapter. The TKE application can be restarted without logging in to the TKE workstation crypto adapter.

## Exit and logoff

Selecting **Exit and logoff** closes the TKE application window and logs the current user off the TKE workstation crypto adapter. A user login is required to restart the TKE application.

# Utilities Menu

These selections are available from the **Utilities** pull-down menu in the TKE main window:

- **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. The **Manage smart card contents...** and **Copy smart card contents...** selections are available only if you have selected **Enable Smart Card Readers** under the **Preferences** menu.

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.

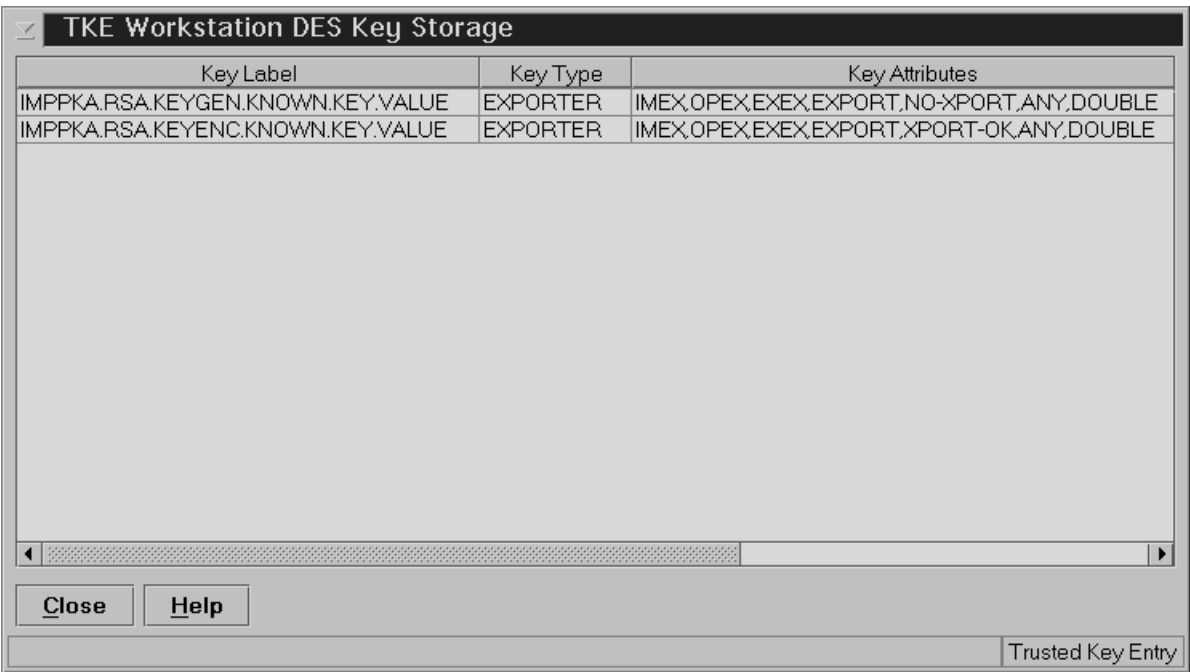


Figure 64. TKE Workstation DES Key Storage Window

The TKE Workstation DES Key Storage window displays the following information:

- 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 workstation crypto adapter is used for purposes other than TKE.
- Key Attributes

Following is a list of some of the key words used by the TKE crypto adapter card for defining the control vector.

- KEY-PART - The initial key part has been loaded but the last key part has not been loaded.
- NO-XPORT - The key cannot be exported. IMP-PKAs used to protect generated RSA keys have this attribute.
- XPORT-OK - The key is exportable. IMP-PKAs used to protect entered RSA keys have this attribute.
- Control vector - The CCA control vector.
- Created date and time
- Updated date and time

### Deleting an Entry

When you 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 authority signature key. This can be a 1024-bit, 2048-bit, or 4096-bit signature key.

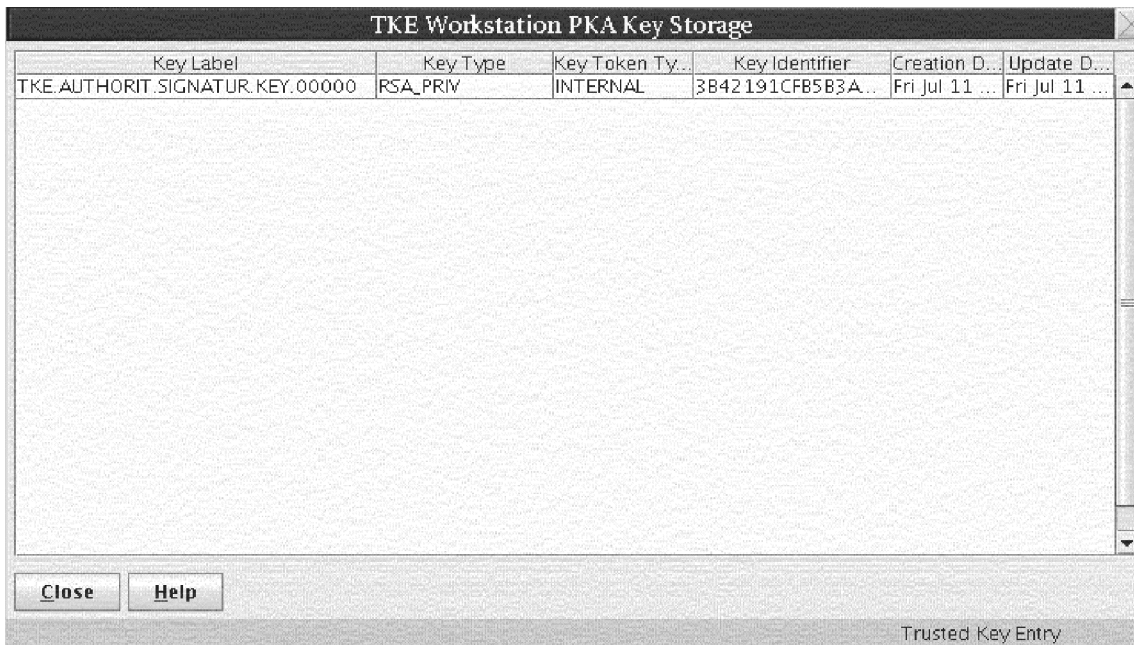


Figure 65. TKE Workstation PKA Key Storage Window

The TKE Workstation PKA Key Storage window displays the following information:

- Key label
- Key type

The type of key is one of the following:

- RSA-PRIV - A token holding the private and public key part of a PKA key pair. This is the key type for an authority signature key.
- RSA-PUB - A token holding the public part of a PKA key pair.

- RSA-OPT - A token holding the private and public part of a PKA key part in optimized form.
- Key Token Type
 

The type of token is one of the following:

  - Internal - The key token is internal and the key value is enciphered under the TKE crypto adapter master key.
  - External - The key token is external and the key value is either enciphered by a key-encrypting key or unenciphered.
  - No\_Key - The key token is empty.
- Key Identifier - Identifies the RSA key in PKA key storage. The key identifier is the SHA-256 hash of the DER-encoded public modulus and public exponent of the RSA key pair.
- Created date and time
- Updated date and time

### Deleting an Entry

When you 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.

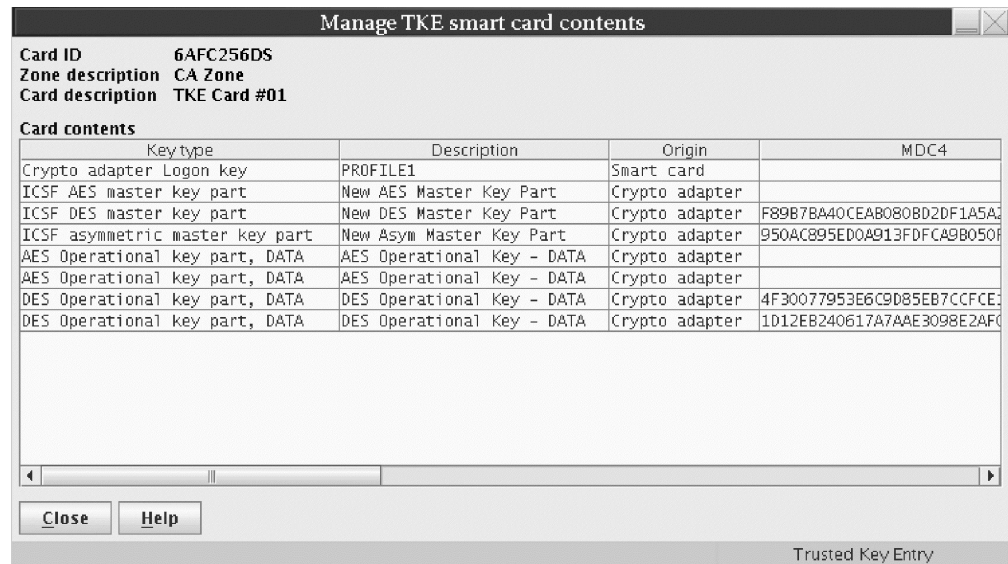


Figure 66. TKE smart card contents

The Manage TKE smart card contents window displays the following information for a TKE smart card:

#### Card ID

Identification of TKE smart card



### Zone description

Description of the zone in which the TKE smart card is enrolled

### 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, AES-VP, 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 6-digit PIN.

**Note:** TKE smart cards created before TKE 7.0 use 4-digit PINs.

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

### Notes:

1. 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 4.1.0 or the Smart Card Utility Program 7.0 under Trusted Key Entry Applications on the Framework. See "Cryptographic Node Management Batch Initialization 4.1.0" on page 293 or Chapter 11, "Smart Card Utility Program (SCUP)," on page 253.
2. ECC key parts cannot be copied to lower level release cards.

To copy a smart card:

1. Select **Copy smart card contents...** from the **Utilities** menu.  
A message box displays prompting you to "Insert source TKE smart card in smart card reader 1".
2. Insert the source TKE smart card in smart card reader 1 and press **OK**.  
A message box displays prompting you to "Insert target TKE smart card in smart card reader 2".

3. Insert the target TKE smart card in smart card reader 2 and press **OK**.  
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.

The Copy smart card contents window lists the following information for a TKE smart card:



**Card ID**

Identification of TKE smart card

**Zone description**

Description of the zone in which the TKE smart card is enrolled

**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, AES-VP, Control Vector (for operational keys only), and Length.

- Highlight the keys that you want to copy. By holding down the control button on the keyboard, you can select specific entries on the list with your mouse. By holding down the shift button on the keyboard, you can select a specific range of entries on the list with your mouse. 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 119) or use a different TKE smart card.

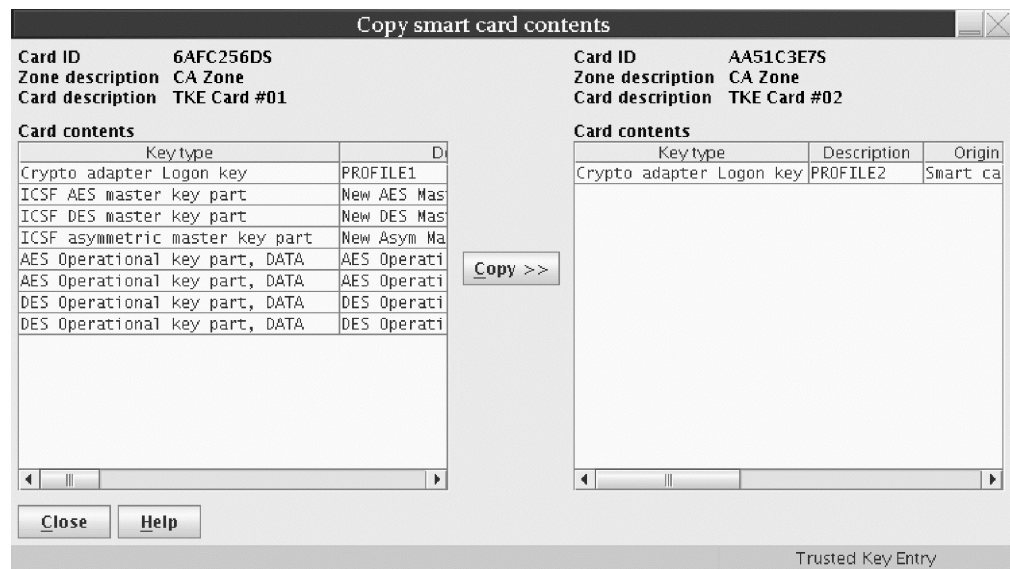


Figure 67. Select keys to copy

- 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 panel is refreshed.

## TKE Customization

After installation of the TKE workstation, the following 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.

### **Removable Media Only**

Limits file read and write operations to removable media only.

When this box is selected, any TKE application files that are being accessed through a floppy disk are read-only. On the other hand, files being accessed from either DVD-RAM or a USB flash memory drive can be either read-only or writable. For DVD-RAM, when you mount the DVD drive through the TKE Media Manager, you specify whether you want to activate it as read-only or writable. For a USB flash memory drive, the drive is automatically mounted and is both readable and writable

When unchecked, the TKE data directory on the TKE local hard drive can also be used for file read / write operations.

### **Enable Tracing**

Activates the trace facility in TKE. The output can be used to help debug problems with TKE. Do not check this menu item unless 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.

## Chapter 7. Crypto Module Notebook

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

The Crypto Module 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 for groups of modules and domain groups. The contents of some of the pages will vary depending on whether you have selected a single crypto module, a group of crypto modules, or a domain group.

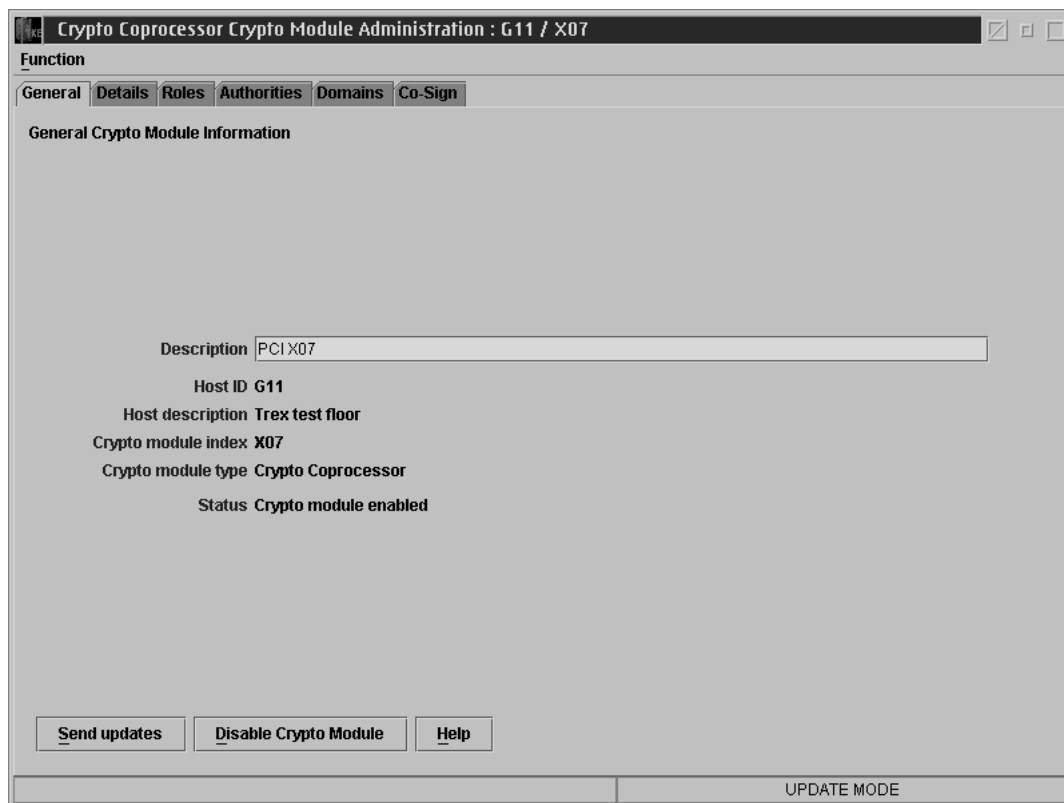


Figure 68. Crypto Coprocessor Crypto Module Administration Notebook - General Page

**Note:** Many screen captures 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.

### Crypto Module Notebook General Tab

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. The index value is 00 through 63. There is no crypto module index for a crypto module group or a domain group.

- **Crypto Module Type**

- **Status**

A crypto module is either enabled or disabled. When a supported crypto module (CEX2C or CEX3C) is enabled, it is available for processing. You can change the status of the module by pressing the **Enable Crypto Module / Disable Crypto Module** button. **Enable Crypto Module** is a dual-signature command and another authority may need to co-sign. **Disable Crypto Module** is a single signature command.

Disabling a crypto module disables all the cryptographic functions for a single crypto module, a group of crypto modules, or a domain group. This disables the crypto module for the entire system, not just the LPAR that issued the disable.

If you press the **Disable Crypto Module** button, a series of windows opens. You are asked if you are sure you want to disable the module, and are then notified if the command executes successfully. If the authority signature key has not been loaded, you will be asked, through a series of windows, to load an authority signature key. Once the module is disabled, the **Disable Crypto Module** button becomes the **Enable Crypto Module** button.

## Intrusion Latch

Under normal operation, a cryptographic card's intrusion latch is tripped when the card is removed. This causes all installation data, master keys, retained keys, roles and authorities to be zeroized in the card when it is reinstalled. Any new roles and authorities are deleted and the defaults are recreated. The setting for TKE Enablement is also returned to the default value of *Denied* when the intrusion latch is tripped.

A situation may arise where a cryptographic card needs to be removed. For example, you may need to remove a card for service. If you do have to remove a card, and you do not want the installation data to be cleared, perform the following procedure to disable the card. This procedure will require you to switch between the TKE application, the ICSF Coprocessor Management panel, and the Support Element.

1. Open an Emulator Session on the TKE workstation and log on to your TSO user ID on the Host System where the card 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 card will be removed. Open the crypto module notebook for the CEX2C or CEX3C. Click on the **Disable Crypto Module** button.
5. After the crypto module has been disabled within TKE, hit ENTER on the ICSF Coprocessor Management panel. The status should change to DISABLED.

**Note:** You do not need to deactivate a disabled card before configuring it OFFLINE.

6. **Configure Off** the card from the Support Element.

7. After the card has been taken Offline, hit ENTER on the Coprocessor Management panel. The status should change to OFFLINE.
8. Remove the card. Perform whatever operation needs to be done. Replace the card.
9. **Configure On** the card from the Support Element.
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 the **Enable Crypto Module** button.
12. After the card 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 card is enabled it should return to ACTIVE.

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

---

## 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 of 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.

In **PENDING COMMAND MODE**, a command is waiting to be co-signed. A multi-signature command issued by an authority, but not yet executed, is called a pending command. You must perform the co-sign. You cannot issue other commands in this mode. For information about co-signing a pending command, refer to "Crypto Module Notebook Co-Sign Tab" on page 174.

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 or domain group.

---

## Crypto Module Notebook Function Menu

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

- **Refresh Notebook** - The content of the notebook is refreshed by reading information from the host. Be aware that performing a refresh may change the mode of the notebook.
- **Change Signature Index** - The authority signature index for the currently loaded authority signature key can be changed. An authority may use the same authority 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 authority 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.

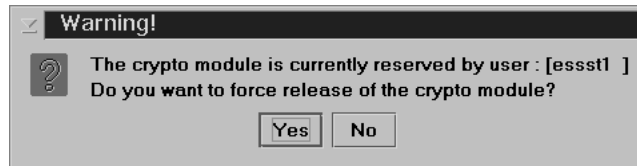


Figure 69. Window to Release Crypto Module

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

**Warning:** 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 or a domain group. For more information, see “Comparing Crypto Module Groups” on page 103.
- **Close** - This selection closes the Crypto Module Notebook.

---

## Tabular Pages

For the host cryptographic modules, the tabular pages available are:

- **Details:** see “Crypto Module Notebook Details Tab.”
- **Roles:** see “Crypto Module Notebook Roles Tab” on page 127.
- **Authorities:** see “Crypto Module Notebook Authorities Tab” on page 131.
- **Domains:** see “Domains Keys Page” on page 140.
- **Co-sign:** see “Crypto Module Notebook Co-Sign Tab” on page 174.

As discussed previously, the notebook opens to the General tab.

---

## Crypto Module Notebook Details Tab

The Details page has two pages for crypto modules. No changes to the information are allowed from these pages. The pages and their contents are:

- **Crypto module:**
  - **Crypto Module ID** - Unique identifier burnt into the crypto module during the manufacturing process.
  - **Public Modulus** - The public modulus of the RSA key pair associated with the crypto module. The public portion of the RSA key pair is used to verify signed replies from the crypto module.
  - **Key Identifier** - Identifies the RSA key pair associated with the crypto module. The key identifier is the SHA-256 hash of the DER-encoded public modulus and public exponent of the RSA key pair.
  - **Signature Sequence Number** - Each signed reply from the crypto module contains a unique sequence number; the current value is displayed.

- **Hash pattern of transport key** - MDC-4 value of the current Diffie-Hellman generated DES and PKA transport key for this crypto module
- **FCV (referred to as Crypto Services on the Details page):**
  - Base CCA services availability
  - CDMF availability
  - 56-bit DES availability
  - Triple DES availability
  - 128-bit AES availability
  - 192-bit AES availability
  - 256-bit AES availability
  - SET services
  - Maximum length of RSA keys used to encipher DES keys
  - Maximum elliptic curve field size in bits for key management

The settings in the Crypto Module Details tab are loaded during crypto module initialization.

---

## Crypto Module Notebook Roles Tab

The supported 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. Having a predefined authority with both the Issue and Co-sign access control points enabled allows you to create the necessary roles and profiles for the crypto modules using just one authority, rather than requiring an extra authority to co-sign.

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

## Multi-Signature Commands

Multi-signature commands for the supported crypto 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 tab when changing the crypto module state.



- **Access Control** - This command is issued from:
  - *Create New/Change Role windows* - when creating or changing a role
  - *Role Tab* - when deleting a role
  - *Create New/Change Authority windows* - when creating or changing an authority
  - *Authorities Tab* - 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

The following commands require only one signature:

- *Disable crypto card*
- *Set asymmetric master key*
- *Load first key part* - DES-MK, AES-MK, ASYM-MK, and ECC-MK
- *Combine middle key parts* - DES-MK, AES-MK, ASYM-MK, and ECC-MK
- *Combine final key part* - DES-MK, AES-MK, ASYM-MK, and ECC-MK
- *Clear new master key register* - DES-MK, AES-MK, ASYM-MK, and ECC-MK
- *Clear old master key register* - DES-MK, AES-MK, ASYM-MK, and ECC-MK
- *Load first key part* - DES Operational Keys
- *Load additional key part* - DES Operational Keys
- *Complete key* - DES Operational Keys
- *Clear operational key register* - DES Operational Keys
- *Load first key part* - AES Operational Keys
- *Load additional key part* - AES Operational Keys
- *Complete key* - AES Operational Keys
- *Clear operational key register* - AES Operational Keys
- *Change default key wrapping* - wrap internal keys using enhanced method
- *Change default key wrapping* - wrap internal keys using original method
- *Change default key wrapping* - wrap external keys using enhanced method
- *Change default key wrapping* - wrap external keys using original method

## Creating or Changing a Role

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



**Create New Role**

**Role ID**

**Description**

- ☐ Role Access Control Points
  - ☐ Crypto Module Enable
  - ☐ Access Control
  - ☐ AES Master Key
  - ☐ ECC Master Key
  - ☐ DES Master Key
  - ☐ Asymmetric Master Key
  - ☐ Domain Zeroize
  - ☐ Domain Controls
  - ☐ AES Operational Key
  - ☐ DES Operational Key
  - ☐ Change Default Key Wrapping
  - ☐ Configuration Migration
  - ☐ Domain Access

**Send updates** **Cancel** **Help**

Trusted Key Entry

Figure 70. Create New Role Page

If you select **Create** or **Change** off the pop-up menu, a window opens displaying the following fields and elements:

- **Role ID** — Enter the Role ID. If you are creating a new role you must fill in a name for that role. If you are changing a role, you cannot change this field.
- **Description** — Optional free text description.
- **Tree structure and check boxes** — Navigate the tree structure and mark the boxes you require for the role. Choices must be made in these categories:
  - **Crypto Module Enable**  
Choose whether the role can disable the crypto card, issue the enable crypto card command, or co-sign the enable crypto card command.
  - **Access Control**

Choose whether the role can issue the access control command or co-sign the access control command (needed for creating roles and profiles).

– **AES Master Key**

Choose whether the role can load the first key part, combine middle key parts, combine final key part, clear new AES master key registers, or clear old AES master key registers.

– **ECC Master Key**

Choose whether the role can load the first key part, combine middle key parts, combine final key part, clear new ECC master key registers, or clear old ECC master key registers.

– **DES Master Key**

Choose whether the role can load the first key part, combine middle key parts, combine final key part, clear new DES master key registers, or clear old DES master key registers.

– **Asymmetric Master Key**

Choose whether the role can load the first key part, combine middle key parts, combine final key part, clear new asymmetric master key registers, clear old asymmetric master key registers, or set the asymmetric master key.

– **Domain Zeroize**

Choose whether the role can issue a zeroize domain command or co-sign a zeroize domain command.

– **Domain Controls**

Choose whether 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)).

– **AES Operational Key**

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

– **DES Operational Key**

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

– **Change Default Key Wrapping**

Choose the default key wrapping changes allowed by the role.

– **Configuration Migration**

Choose if the role is allowed to perform configuration migration operations.

– **Domain Access**

Choose the domains this role can access.

Check boxes for operations that are not supported on the crypto module do not appear. Operations on AES master keys and AES operational keys are only supported on CEX2C crypto modules (with Nov. 2008 or later licensed internal code) or on CEX3C crypto modules (with FMID HCR7770 or later of ICSF). Operations on ECC master keys and default key wrapping are only supported on CEX3C crypto modules (with FMID HCR7780 or later of ICSF and CCA level 4.1.0 or later).

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 all authorities associated with a role before you delete the role.

---

## Crypto Module Notebook Authorities Tab

An authority is a person who is able to issue signed commands to the crypto module. For each of the currently defined authorities, this container lists the name, index and other authority information.

When you right-click in the Authorities container, you can:

- **Create Authority:** Upload the public part of the authority signature key and the authority information for the selected crypto module or group of crypto modules.
- **Change Authority:** Display and edit the authority-related information for the selected crypto module or group of crypto modules.
- **Delete Authority:** Delete the authority-related information for the selected crypto module or group of crypto modules.
- **Generate Signature Key:** Generate a signature key for an authority and save it on a selected medium together with authority-related information (name, telephone number et cetera).

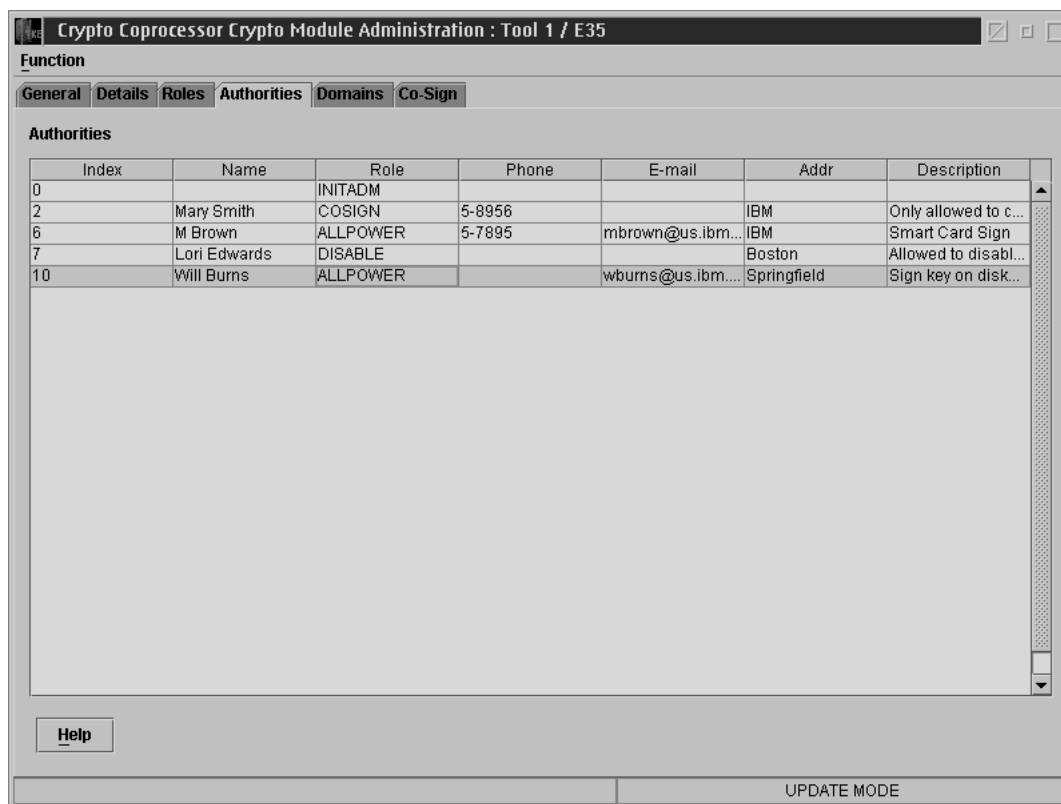


Figure 71. Authorities Page

## Generating Authority Signature Keys

You generate and save an authority signature key by right-clicking in the Authorities container and selecting the *Generate Signature Key* action.

The Generate Signature Key window is displayed.

Follow this procedure:

1. Enter **Authority index**. This is a mandatory field with the index of the authority. Valid range is 00 through 99. The authority index will be saved with the key and is called the Default Authority index. The Default Authority index for a saved authority signature key can be overridden when the authority signature key is loaded.
2. Enter **Name**, **Phone**, **E-mail**, **Address** and **Description** to identify the authority. These are optional free text fields. The information that you enter here is saved with the key. It will be filled in automatically when the key is selected for creating a new authority. Press **Continue**.



Figure 72. Filled In generate signature key window

3. A Select Target dialog box is displayed, enabling you to select the target destination for the generated key. Authority signature keys can be saved to a **binary file**, **key storage**, or **TKE smart card**. Make your selection and press **Continue**.
4. Select the length of the authority signature key you want to generate. The length choices will vary depending on the signature key source. If the signature key source is a smart card, you can generate 1024-bit or 2048-bit authority signature keys. If the signature key source is a binary file or key storage, you can generate 1024-bit, 2048-bit, or 4096-bit authority signature keys.
5. If the keys are to be saved as a **binary file**, 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.

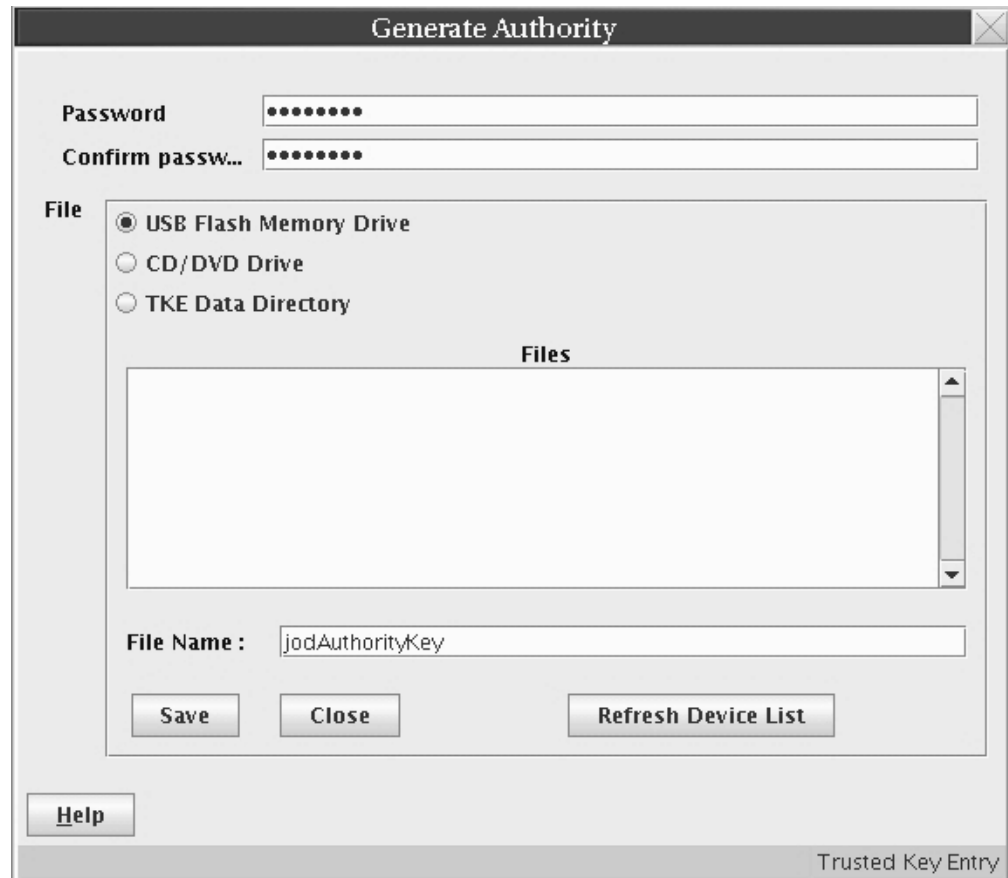


Figure 73. Save authority signature key

#### Warnings:

- a. 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 “TKE Media Manager” on page 313.
- b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.
6. If the keys are to be saved to a **TKE smart card**, a message box displays, prompting you to "Insert TKE smart card in smart card reader 2."
  - a. Insert the TKE smart card into Smart Card Reader 2. Press **OK**.
  - b. When the authority signature key is saved to a TKE smart card, it is protected by the PIN of the TKE smart card. A message box will prompt you to “Enter a 6 digit PIN on smart card reader 2 PIN pad”. Enter the PIN as prompted.

**Note:** If the TKE smart card was created on a version of the TKE Workstation prior to version 7.0, the PIN of the TKE smart card will be 4 digits instead of 6 digits.

The authority signature key is generated on the TKE smart card and a successful message is displayed.

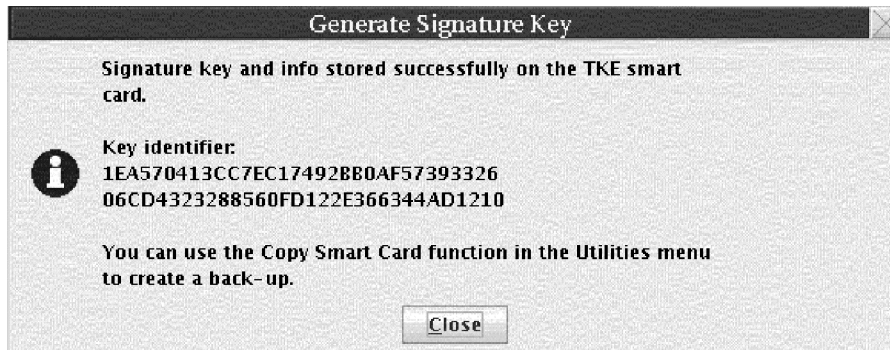


Figure 74. Generate signature key

When saving an authority signature key on a TKE smart card, you are not given the option to save it again. You should use the copy smart card contents utility to save the signature key again. See “Copy smart cards” on page 120.

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

7. If the keys are to be saved in **Key Storage**, note that only one authority signature key can be stored in PKA key storage.



Figure 75. Key saved status message

## Create Authority

This selection allows you to create an authority at the host and select its authority signature key. Before you can create a new authority, you need to generate an authority signature key (see “Generating Authority Signature Keys” on page 132).

To create an authority, click with the right mouse button in the container on the Authorities page. A popup menu displays. From this menu, select the **Create Authority** menu item.

The Select Source window opens, enabling you to specify the authority signature key source. Make your selection and press the **Continue** command button.

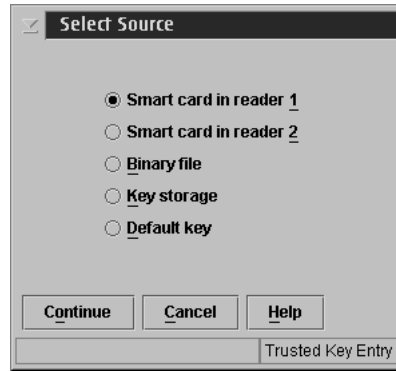


Figure 76. Select source of authority signature key

- If you select **Key storage**, the key and accompanying information from key storage appears in the Create New Authority window.
- If you select **Smart card in reader 1** or **Smart card in reader 2**, you are prompted to insert the TKE smart card into the appropriate reader. Insert the smart card into the reader, and press **OK**.

A message box will prompt you to enter the TKE smart card PIN. Enter the PIN as prompted.

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

Figure 77. Create new authority

- If you select **Binary file**, the Load Signature Key window is displayed. You are prompted for the signature key file to load and password before the Create New Authority window appears.

#### Warnings:

1. 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 “TKE Media Manager” on page 313.

2. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

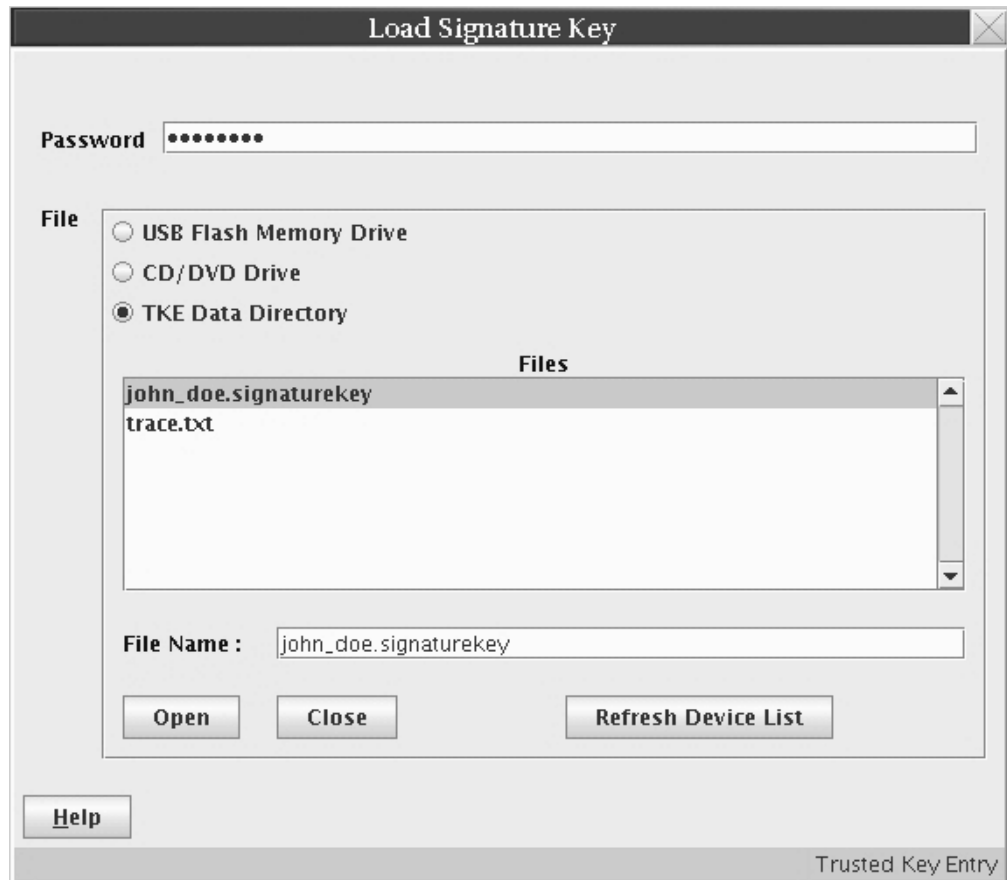


Figure 78. Load Signature Key from binary file

- 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 79. Create New Authority with Role Container

The Create New Authority window is opened with the following 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 authority signature key is going to be used on several crypto modules, it simplifies matters to use the same authority index for all crypto modules.

- **Name** - Name of the authority. Optional free text entry field.
- **Phone** - 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 authority signature key.
- **Key Length** - Length of the authority signature key.
- **Key Identifier** - Identifier for the authority signature key associated with the authority. The key identifier is the SHA-256 hash of the DER-encoded public modulus and public exponent of the authority signature key.

You can edit all of the entry fields.

In the **Role** container there is a drop-down list. Select one of the previously defined roles. The authority is mapped to the access rights of that role. This is available only when creating or changing a crypto module authority.

Press **Send updates**. This is a dual signature command. If you do not have both sign and co-sign authority, you 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

This selection opens the Change Authority window, allowing you to change authority information, change the role, and replace the authority signature key.

Figure 80. Change Authority

When an authority is selected, you will be able to update the Name, Phone, E-mail, Address and Description fields. You can change the Role definition by clicking on the pull-down menu and selecting a different role. You can change the authority signature key by clicking on **Get Signature Key**.

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

**Send updates** uploads the information displayed at the window to the crypto module. The authority information (name, phone, e-mail and address) is updated in the crypto module dataset specified in the TKE host transaction program started procedure on the host.

## Delete Authority

The supported crypto modules operate with a variable number of TKE authorities (TKEAUTxx profiles). TKE allows a user to delete an authority from a crypto module. TKE performs a consistency check of the resulting TKE roles and profiles to ensure that access to the crypto module is not lost when the profile is deleted.

## Crypto Module Notebook Domains Tab

The Domains tab defines the domains that can have AES, ECC, DES and asymmetric master keys and operational keys loaded and changed, as well as providing domains controls.

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

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

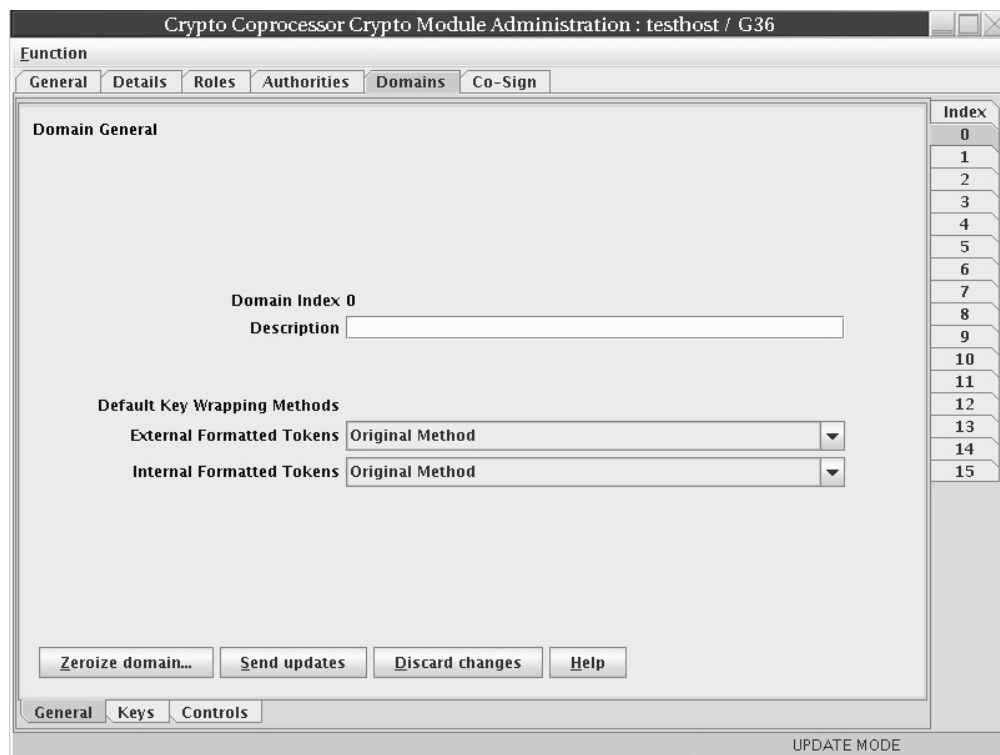


Figure 81. Domains General Page

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.

To change the default key wrapping methods used for the domain, select the desired methods for external and internal formatted tokens and press **Send updates**.

### Zeroize Domain

Zeroizing a domain erases its configuration data and clears all cryptographic keys and registers for the current domain.

Selecting **Zeroize domain...** results in the display of an action (warning) message. By accepting the message, the domain is zeroized. That is, all registers and keys related to this domain are set to zero or set to not valid.

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

When a domain is zeroized, the domain's controls are reset to their initial state.

**Note:** Unlike the Global Zeroize issued from the Support Element, zeroize domain does not affect the enablement of TKE Commands on the supported crypto modules (CEX2C and CEX3C). Refer to "TKE Enablement" on page 7.

## Domains Keys Page

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 AES (on supported crypto modules), DES, and Asymmetric key registers.

If you have implemented smart card support, make sure that the TKE workstation crypto adapter and the TKE smart cards are in the same zone. To display the zone of a TKE smart card, exit from TKE and use either the Cryptographic Node Management Utility 4.1.0 or the Smart Card Utility Program 7.0 under Trusted Key Entry Applications. See “Display smart card details” on page 245 or Chapter 11, “Smart Card Utility Program (SCUP),” on page 253.

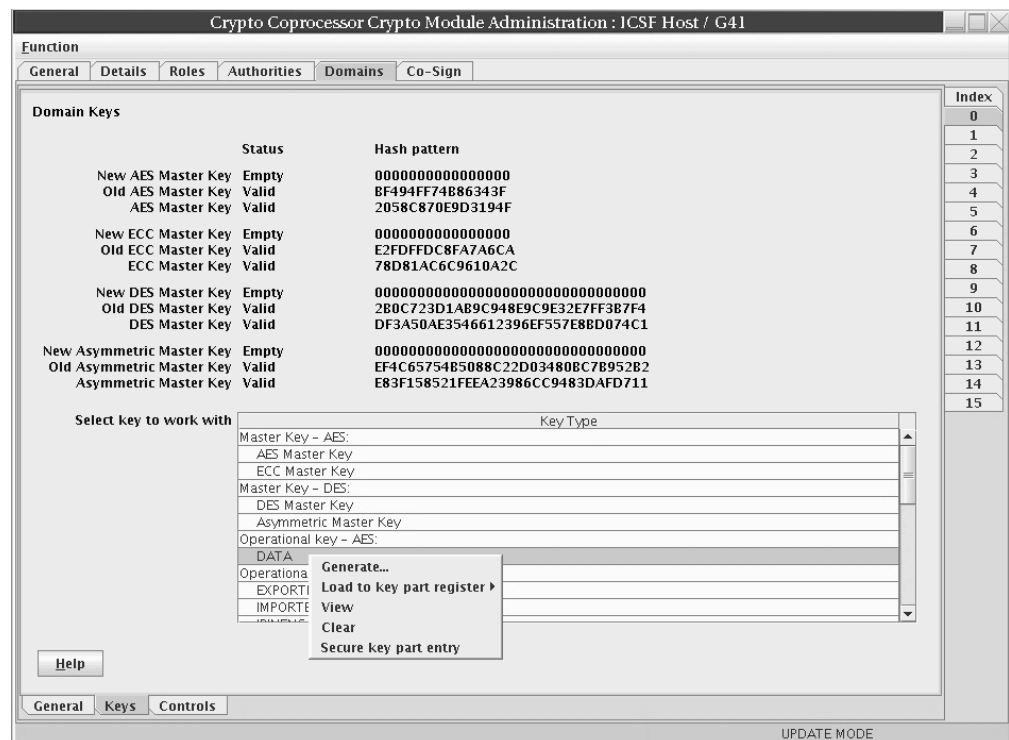


Figure 82. Domains Keys Page

The lower part of the Domains Keys page allows you to select the key type with which you wish to work. Select the key type you will be working with from the Key Type container. Each key type supports various actions. Not all actions are available for all key types. Table 14 on page 141 illustrates the possibilities for the supported crypto modules.

Table 14. Key types and actions for the supported crypto modules

Key Type	Popup	Sub-popup	Action Description
DES, ECC, or AES MK	Generate new		Generate a key part and save to a file or TKE smart card
	Load new	First Intermediate Last	Load a key part directly to the relevant new master key register.  Load First requires the register to be empty. Load Intermediate and Last require the register to be part full.
	Clear	New master key register  Old master key register	Clear (reset) the new or old master key register
	Secure key part entry		Enter known key part values to a TKE smart card; see Appendix A, "Secure Key Part Entry," on page 275.
Asymmetric MK	Generate new		Generate a key part and save to a file or TKE smart card
	Load new	First Intermediate Last	Load a key part directly to the relevant new master key register.  Load First requires the register to be empty. Load Intermediate and Last require the register to be part full.
	Set		Sets the new asymmetric master key. 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.
	Clear	New master key register  Old master key register	Clear (reset) the new or old asymmetric master key register
	Secure key part entry		Enter known key part values to a TKE smart card; see Appendix A, "Secure Key Part Entry," on page 275.
DES or AES Operational Keys	Generate		Generate a key part and save to a file or TKE smart card
	Load to Key Storage	First Intermediate Last	Load a key part to the workstation DES key storage.  This function is only performed for DES 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		View key part register information
	Clear		Clear (reset) the operational key part register
	Secure key part entry		Enter known key part values to a TKE smart card; see Appendix A, "Secure Key Part Entry," on page 275.

Table 14. Key types and actions for the supported crypto modules (continued)

Key Type	Popup	Sub-popup	Action Description
RSA Keys	Generate...		Generate an RSA Key and encrypt it under an IMP-PKA key.
	Encipher		Encipher an unencrypted RSA key under an IMP-PKA key
	Load to PKDS...		Load an RSA key to the PKDS active in the logical partition where the Host Transaction Program is started
	Load to dataset		Load an RSA key to a host data set

## Master Keys - AES, ECC, DES, or Asymmetric

**Generate new:** The generate action for a new AES, DES, or Asymmetric Master Key type will generate a master key part that can be stored in a file or on a smart card. Note, that this action does not load the key part to the host.

When you select **Generate new**, a Select Target window opens, enabling you to specify the target.



Figure 83. 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.

**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 4.1.0 or the Smart Card Utility Program 7.0 under Trusted Key Entry Applications. See “Display smart card details” on page 245 or “Display smart card information” on page 255.

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

**Saving to a TKE Smart Card:** If you are saving to a TKE smart card, a message box prompts you to insert the smart card into the smart card reader.



Figure 84. 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.

A dialog is displayed prompting you for a key part description.



Figure 85. Enter key part description

Enter a description for the key part, and press the **Continue** command button.

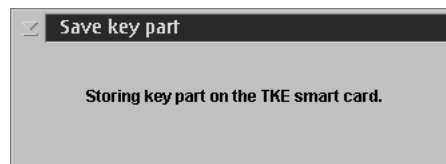


Figure 86. Save key part

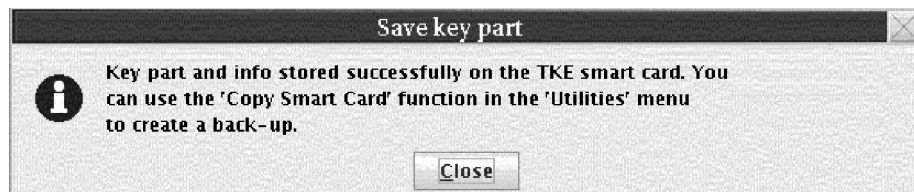


Figure 87. Save key part success message

**Load new:** The load action from the New AES, DES, ECC, or Asymmetric Master Key type loads a key part to the new master key register. The key part can be obtained from a smart card, a file, or the keyboard. At least two key parts (First and Last) must be loaded. In addition, you can enter more than one intermediate key part.

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

- First
- Intermediate
- Last

*Input from TKE Smart Card:* Follow these steps:



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

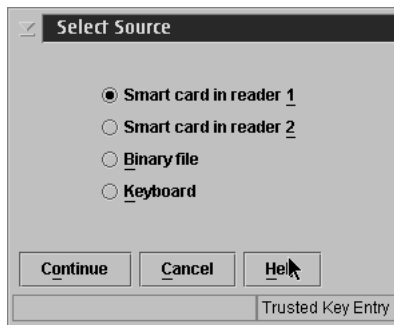


Figure 88. Select key source - smart card

Make your selection and 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 4.1.0 or the Smart Card Utility Program 7.0 under Trusted Key Entry Applications. See “Display smart card details” on page 245 or “Display smart card information” on page 255.

3. The smart card contents are read and displayed in the Select key part from TKE smart card window:

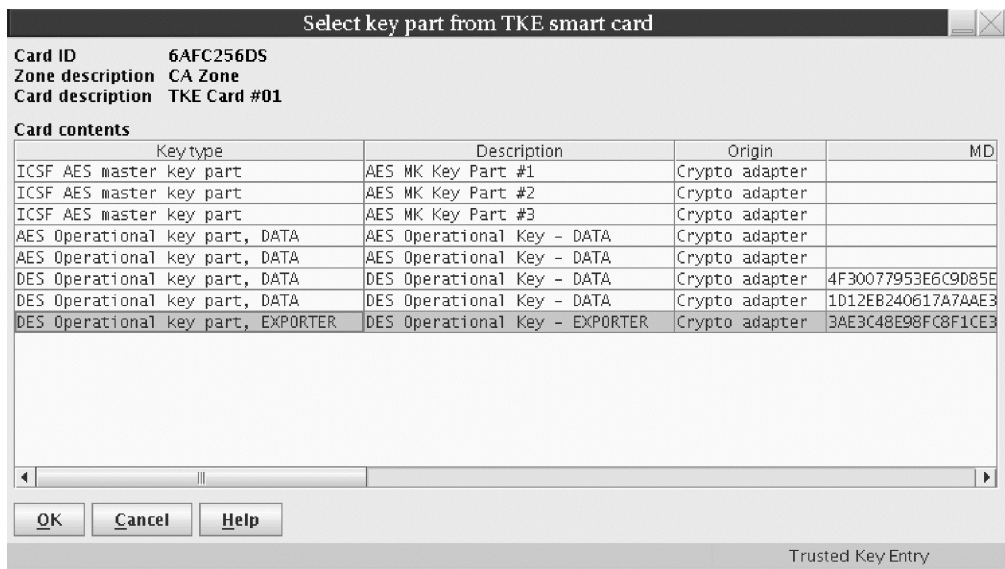


Figure 89. Select key part from TKE smart card

4. Highlight the key part to load.
5. Click **OK**.
6. Enter the PIN on the smart card reader PIN pad when prompted.
7. For a DES or Asymmetric Master Key, the MDC-4 is calculated and displayed, providing the user with the opportunity to visually verify the MDC-4 value. For a



DES Master Key, the Encipher Zero VP (ENC-ZERO) is also displayed. For an AES or ECC Master Key, the AES-VP is calculated and displayed, providing the user with the opportunity to visually verify the AES-VP value.

8. Press **Load key**.
9. You will get a message that the command was executed successfully.

*Input from Keyboard:*

A dialog box is displayed for selecting the input source. Select "Keyboard" and press the **Continue** command button.



Figure 90. Select 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, a 24-byte key or a 32-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 by representing the values as asterisks.

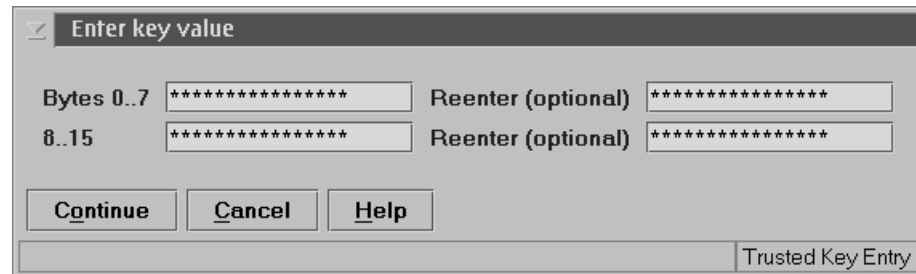


Figure 91. Enter Key Value - Blind Key Entry

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 121.

If Blind Key Entry is not being used, the key values are not masked, and there is no optional confirmation field.

Enter the key values and press the **Continue** command button.

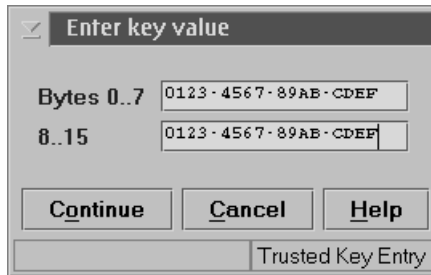


Figure 92. Enter Key Value

- For the DES and Asymmetric Master Keys, when the user presses **Continue**, the MDC-4 (and Encipher Zero for DES Master Key) 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 he or she would like to save the key part. If the user selects **Yes** to save the key part, a file chooser window is opened for the user to specify the file location (CD/DVD drive, USB flash memory drive, or TKE Data Directory) and file name for saving the key part. Then the key part is loaded. If the user selects **No**, the key part is not saved and the key part is loaded.



Figure 93. Key Part Information Window

Press **Load key**.

- For an AES or ECC Master Key, when the user presses **Continue**, the AES-VP is calculated and displayed, providing the user with the opportunity to visually verify the AES-VP value. When Load key is pressed, the user is asked if he or she would like to save the key part. If yes, a file chooser window is opened for the user to specify the file location (CD/DVD drive, USB flash memory 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 94. Key Part Information Window

Press **Load key**.

### Input from Binary File:

A dialog box is displayed for selecting the input source. Select "Binary file" and press the **Continue** command button.

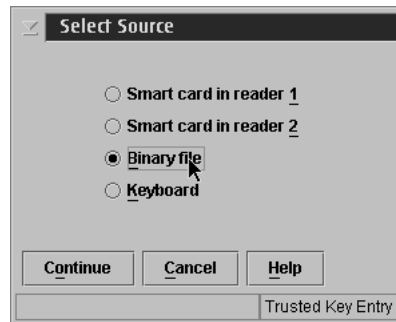


Figure 95. Select key source - binary file

The Specify key file window is displayed.

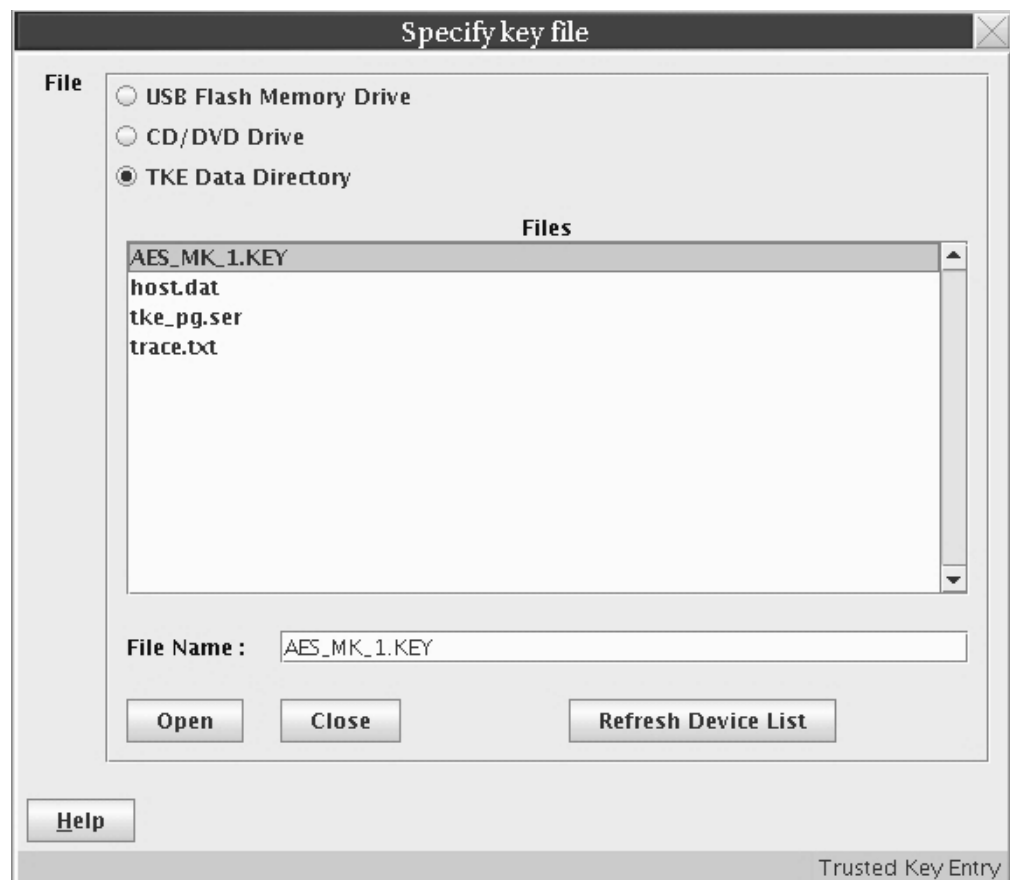


Figure 96. Specify Key File

Using the Specify key file window, specify the file location (Floppy, CD/DVD Drive, USB flash memory drive, or TKE Data Directory) and file name. Select **Open**.

The Key part information window is displayed.

- For a DES or Asymmetric Master Key, the MDC-4 is calculated and displayed, providing the user with the opportunity to visually verify the value.
- For a DES Master Key, when loading from a binary file, the Encipher Zero hash is calculated and displayed. This provides the user with the opportunity to visually verify the value.
- For an AES Master Key, the AES-VP is calculated and displayed, providing the user with the opportunity to visually verify the AES-VP value.

**Warnings:**

1. 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 “TKE Media Manager” on page 313.
2. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.



Figure 97. Key Part Information Window

Once you have verified the information in the Key part information dialog, press the **Load key** command button.

**Clear:** If you would like to clear either the new master key register or the old master key register, you can select either **Clear → New master key register** or **Clear → Old master key register**.

A warning is displayed, prompting you to verify that you want to clear the key register.



Figure 98. Clear new or old master key register validation message

If you press **Yes**, but an authority signature key has not been loaded, you will be prompted to load an authority signature key.

If you press **Yes** and the command executes successfully, a message box is displayed informing you of this.



Figure 99. Clear new or old new master key successful message

### Set (ASYM-MK only)

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.

## Operational Keys

Beginning with TKE V4.1, operational keys can be loaded on a host crypto module. Operational key part registers allow operational keys to be loaded and accumulated on a host crypto module before storing them in the host key store.

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

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 201) or using an option on KGUP JCL (see *z/OS Cryptographic Services ICSF Administrator's Guide*).

Each of the supported crypto modules can have a maximum of 100 key part registers distributed across all domains. A key part register can be in one of the following 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. There is no maximum number of key parts that can be entered.

Available tasks for Operational key part registers are as follows:

- Load to key part register
- View

- Clear

Tasks for Load to key part register are as follows:

- 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 is controlled by access control points in the role definition. The access control points are as follows:

- Load First Key Part
- Load Additional Key Part
- Complete Key
- Clear Operational Key Part Register

**Note:** There are separate access control points for DES and AES keys.

The host crypto module supports all ICSF operational key types. A USER DEFINED key type is also available, and allows the user to specify his or her own control vector for DES keys. 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**

The generate action for an operational key type generates a key part of that type and stores it in a file or on a smart card. Note that this action does not load the key part to the host.

When Generate is selected for a predefined 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.

The dialog box is titled "Generate Operational Key". It features a "Key type" field set to "EXPORTER". To the right, a "Key length" group box contains three radio buttons: 8, 16 (which is selected), and 24. Below this, a "Description" text box contains the text "DES Operational Key - EXPORTER". Underneath the description, there are two input fields for the "Control vector": the first is labeled "Bytes 0..7" and contains "00417D0003410000"; the second is labeled "8..15" and contains "00417D0003210000". At the bottom of the dialog are three buttons: "Continue", "Cancel", and "Help".

Figure 100. Generate Operational Key - predefined EXPORTER 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.

The dialog box is titled "Generate Operational Key". It features a "Key type" field set to "USER DEFINED". To the right, a "Key length" group box contains three radio buttons: 8 (which is selected), 16, and 24. Below this, a "Description" text box contains the text "DES Operational Key - USER DEFINED". Underneath the description, there are two empty input fields for the "Control vector": the first is labeled "Bytes 0..7" and the second is labeled "8..15". At the bottom of the dialog are three buttons: "Continue", "Cancel", and "Help".

Figure 101. Generate Operational Key - USER DEFINED

In both cases, after selecting **Continue** on the Generate window, the Select Target dialog displays, presenting you with a choice of targets: Binary File, Print File or Smart Card.

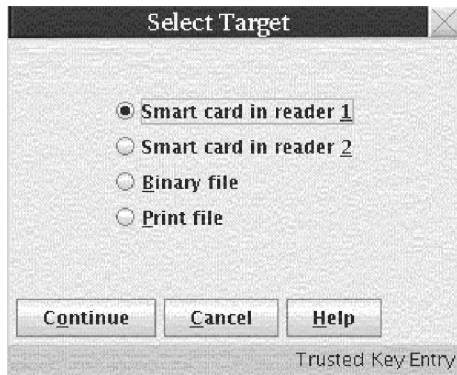


Figure 102. Select Target

### Save key to Binary File or Print File

For either the binary file or print file option, the Save key part window is displayed. Specify where the key is to be saved, and press the **Save** command button.

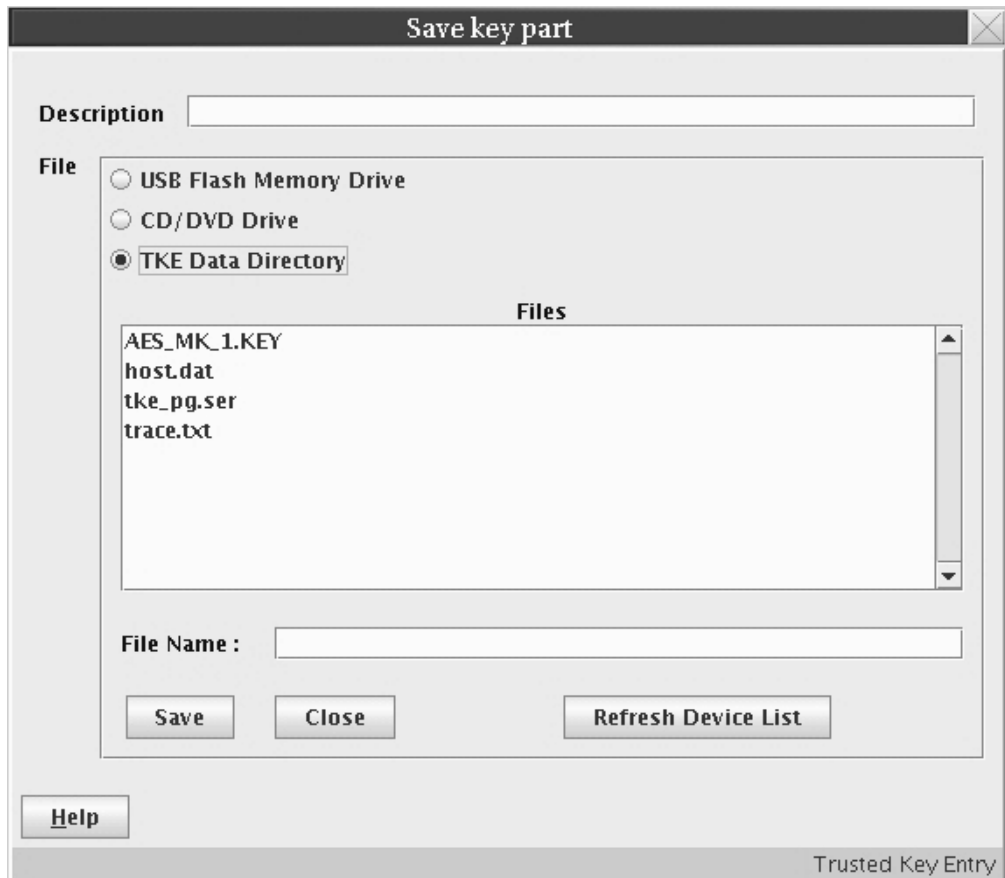


Figure 103. Save key part

After the key is saved, the user can save the same key value again in another location on the Save key again window.



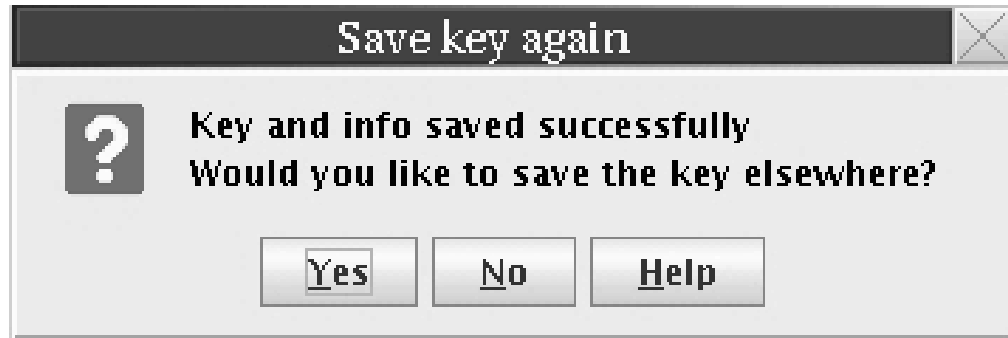


Figure 104. Save key again

#### Warnings:

1. 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 “TKE Media Manager” on page 313.
2. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

#### 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 4.1.0 or the Smart Card Utility Program 7.0 under Trusted Key Entry Applications. See “Display smart card details” on page 245, “Display smart card information” on page 255 or “View current zone” on page 274.

Steps for saving a key to a TKE smart card are as follows:

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 120.

#### Load to Key Part Register First

The Load to key part register action for an operational key type loads a key part to a key part register on the host crypto module. If the register already contains a value, it is XOR'd with the existing value. The key part can be obtained from a smart card, a file, or the keyboard. At least two key parts must be loaded (first, and add part), and then a complete action must be performed on the key register.

When you select Load to Key Part Register First, the Select Source window is displayed, prompting you to select the source for the key part.

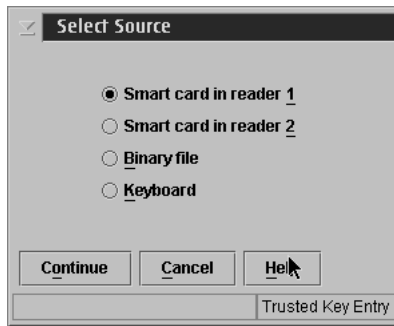


Figure 105. Select Source

If binary file is selected, the **Specify key file window** displays. Specify the file to be used for the key load, and press the **Open** command button.

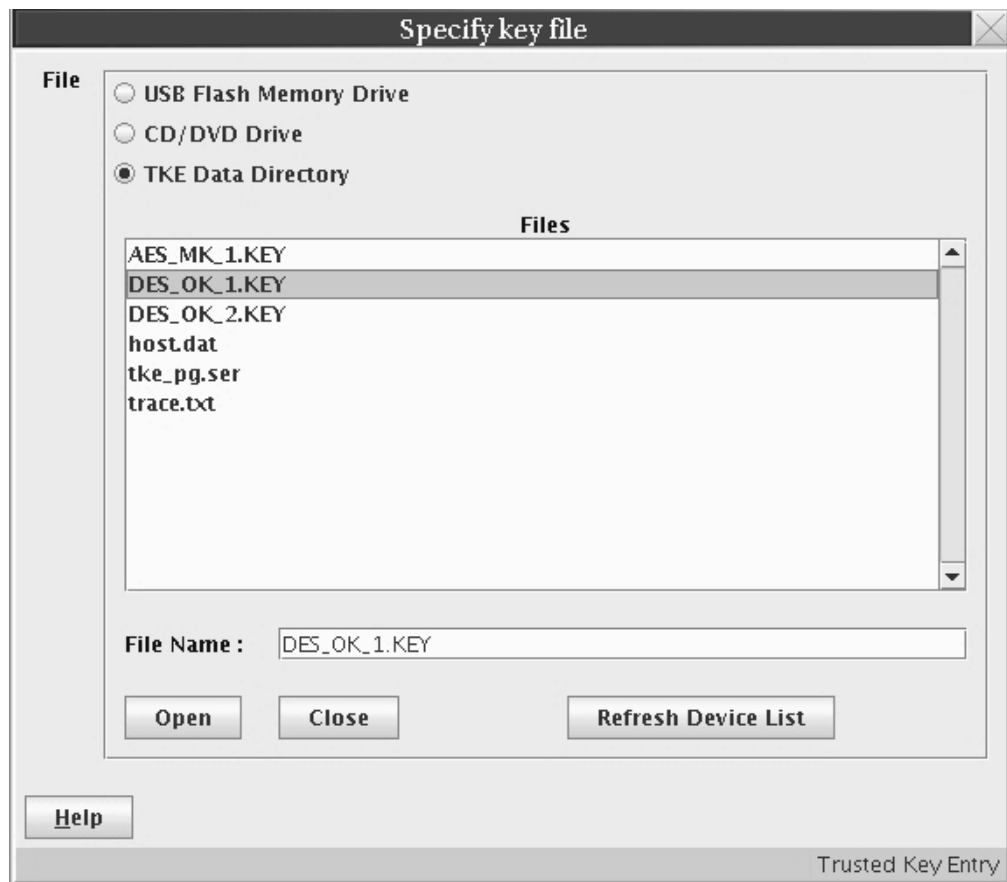


Figure 106. Specify key file for binary file source

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 originally selected by the user.

### Warnings:

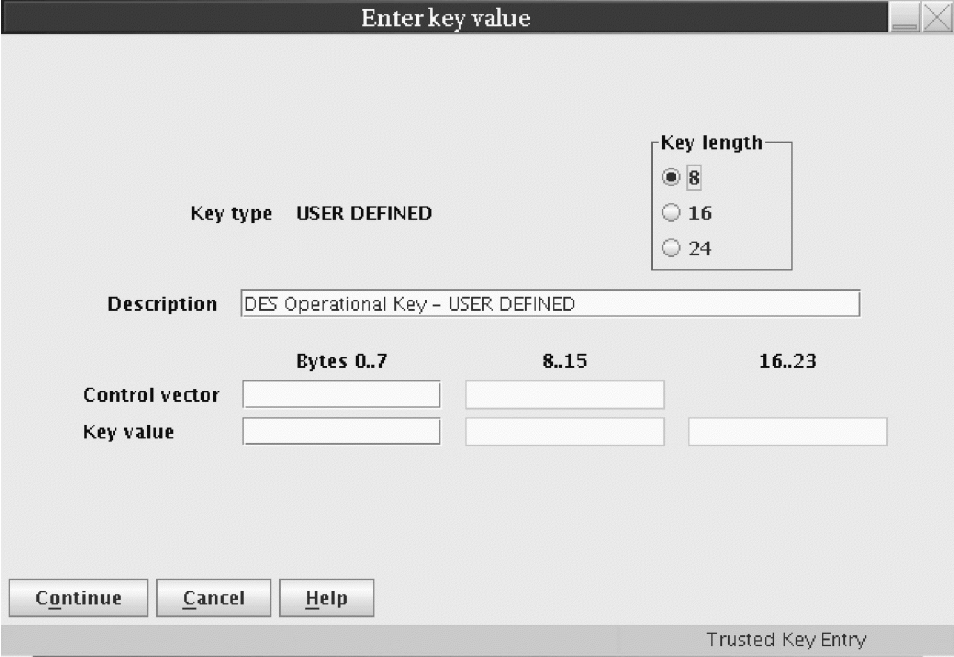
1. If the file is loaded from a floppy or CD/DVD, you must deactivate the floppy or CD/DVD drive before removing the diskette or disc. If the diskette is removed prior to deactivating the drive data could be lost or corrupted. For details on deactivating media see “TKE Media Manager” on page 313.
2. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

If keyboard is selected, the **Enter key value** window is displayed. When the key type is a predefined 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 predefined 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 are calculated and displayed for the DES key part or the AES-VP is calculated and displayed for the AES key part, providing the user with the opportunity to visually verify the values. When Load key is pressed, the user is asked if he or she 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, a USB flash memory 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.

The screenshot shows a window titled "Enter key value" with a close button in the top right corner. Inside the window, the "Key type" is set to "EXPORTER". To the right, a "Key length" group box contains three radio buttons: "8", "16" (which is selected), and "24". Below this, the "Description" field contains the text "DES Operational Key - EXPORTER". Underneath the description, there are three columns of input fields labeled "Bytes 0..7", "8..15", and "16..23". The "Control vector" row has two input fields: the first contains "00417D0003410000" and the second contains "00417D0003210000". The "Key value" row has three empty input fields corresponding to the three byte ranges. At the bottom left are three buttons: "Continue", "Cancel", and "Help". At the bottom right, the text "Trusted Key Entry" is displayed.

Figure 107. Enter key value - keyboard source for predefined EXPORTER 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*.



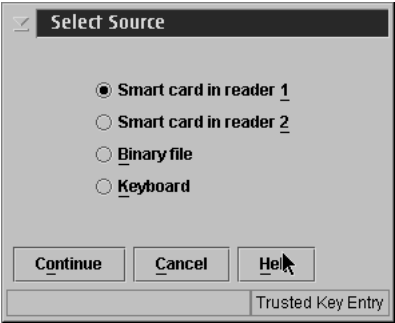
The "Enter key value" dialog box has a title bar with the text "Enter key value" and standard window controls. The main area contains the following elements:

- Key type:** A label followed by the text "USER DEFINED".
- Key length:** A group box containing three radio buttons labeled "8", "16", and "24". The "8" radio button is selected.
- Description:** A text input field containing the text "DES Operational Key - USER DEFINED".
- Control vector:** A row of three text input fields. The first field is labeled "Bytes 0..7", the second "8..15", and the third "16..23".
- Key value:** A row of three text input fields, each aligned under the corresponding "Control vector" field.
- Buttons:** At the bottom left are three buttons: "Continue", "Cancel", and "Help".
- Footer:** At the bottom right, the text "Trusted Key Entry" is displayed.

Figure 108. Enter key value - keyboard source for USER DEFINED key type

If TKE smart card is selected:

1. The user is prompted to insert a TKE card into the appropriate reader and select **OK**.



The "Select Source" dialog box has a title bar with a checkmark icon and the text "Select Source". The main area contains the following elements:

- Radio buttons:** Four radio buttons are listed: "Smart card in reader 1" (selected), "Smart card in reader 2", "Binary file", and "Keyboard".
- Buttons:** At the bottom left are three buttons: "Continue", "Cancel", and "Help".
- Footer:** At the bottom right, the text "Trusted Key Entry" is displayed.

Figure 109. Select Source

2. In the Select key part from TKE smart card window, highlight the key part, right click, and either choose **Select** or 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 originally selected by the user.

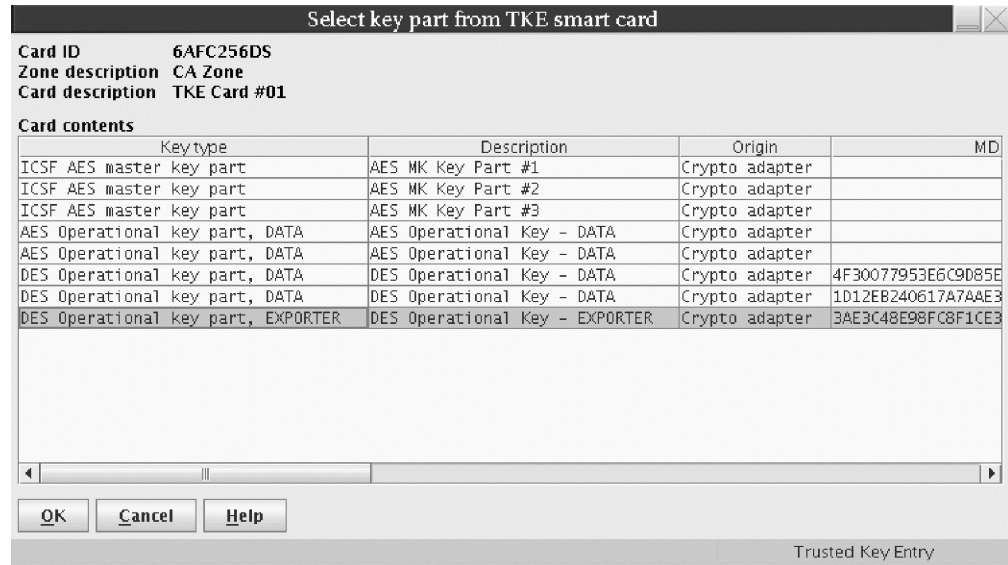


Figure 110. Select key part from TKE smart card

### 3. Enter the PIN on the PIN pad.

After the binary file or TKE smart card is read or the DES operational 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.)

For an AES operational key, the AES-VP is calculated and displayed along with the description, key type, and control vector on the Key part information window.

The user must enter a key label for the key part register. 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.



Figure 111. Key part information - first DES 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.



Figure 112. DES key part register information

After **OK** is selected on the Key part register information window, a message is displayed indicating that the load was processed successfully.

**Load to Key Part Register - Add Part:** A **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 predefined 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.



Figure 113. 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 Figure 114, which displays 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 of whether or not the user turned it on when the control vector was defined.

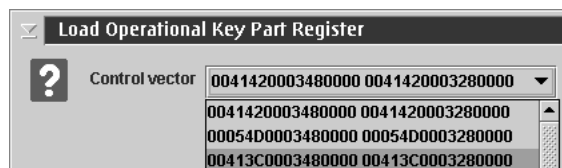


Figure 114. Drop down of control vectors - add part, keyboard source for **USER DEFINED**

After the control vector is selected, the **Key part information** 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.



The 'Key part information' dialog box displays the following fields:

- Description:** DES Operational Key - EXPORTER
- ENC-ZERO:** A47B562B
- MDC-4:** 1336847235E7DA4847CB6596CB2CF002
- Key type:** DES Operational Key - EXPORTER
- Control vector:** 00417D0003410000 00417D0003210000
- Key label:** A drop-down menu showing 'EXPORTER.KEY'.
- Key label's SHA1:** B14CDF25012C52836F405138608EB215F6024F5F

Buttons at the bottom: Load key, Cancel, Help. A status bar at the bottom right reads 'Trusted Key Entry'.

Figure 115. DES Key part information - add part

The key label field is now a drop-down menu for all the labels for all the key registers that have the same control vector, same key length, and are not in a Complete state. The user selects the appropriate key register 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.



The 'Key part register information' dialog box displays the following fields:

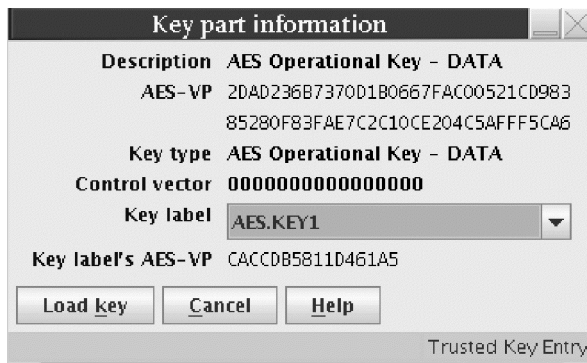
- Key type:** DES Operational Key - EXPORTER
- SHA1:** D94DCB7AF7BF72795D36F77A8254BCF8A79115BF
- Control vector:** 00417D0003410000 00417D0003210000
- Key label:** EXPORTER.KEY

Buttons at the bottom: OK, Help.

Figure 116. DES Key part register information - add part with SHA-1 for combined key

When the Add Part is successfully processed, a message is displayed indicating the command was successfully executed.

Equivalent panels for AES keys are shown below:



**Key part information**

**Description** AES Operational Key - DATA

**AES-VP** 2DAD236B7370D1B0667FAC00521CD983  
85280F83FAE7C2C10CE204C5AFF5CA6

**Key type** AES Operational Key - DATA

**Control vector** 0000000000000000

**Key label** AES.KEY1

**Key label's AES-VP** CACCD85811D461A5

Trusted Key Entry

Figure 117. AES key part information - add part



**Key part register information**

**Key type** AES Operational Key - DATA

**AES-VP** 764DD8FFFA3A86AD

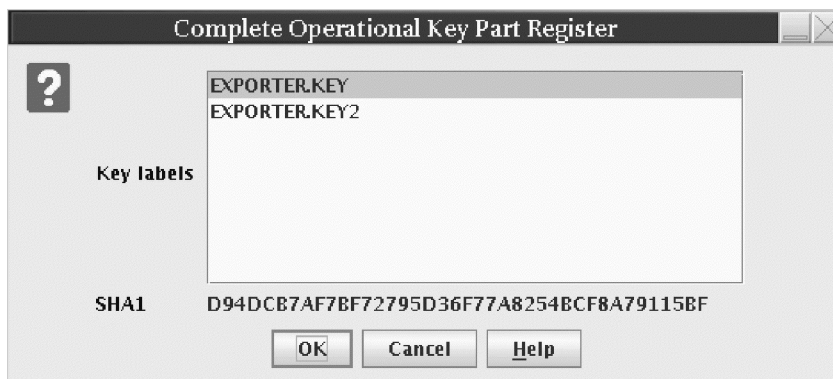
**Control vector** 0000000000000000

**Key label** AES.KEY

Figure 118. AES key part register information

## 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 predefined operational key, the **Complete Operational Key Part Register** window is displayed. Only labels of key part registers 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, then all key part registers of the key type selected will be displayed regardless of key length.



**Complete Operational Key Part Register**

**Key labels**

EXPORTER.KEY  
EXPORTER.KEY2

**SHA1** D94DCB7AF7BF72795D36F77A8254BCF8A79115BF

Figure 119. Complete DES Operational Key Part Register - predefined EXPORTER key type

To select one key label, highlight the label using the left mouse button. To select more than one key label, highlight the label using the left mouse button, then hold down the Control key and highlight additional key labels using the button. To select a range of key labels, highlight the first key label using the left mouse button, then hold down the Shift key and highlight the last key label. All key labels 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 for a DES key, 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 containing DES keys that are in the intermediate state.

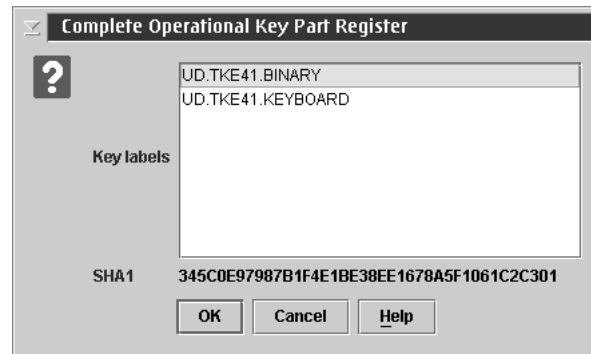


Figure 120. Complete DES Operational Key Part Register - USER DEFINED key type

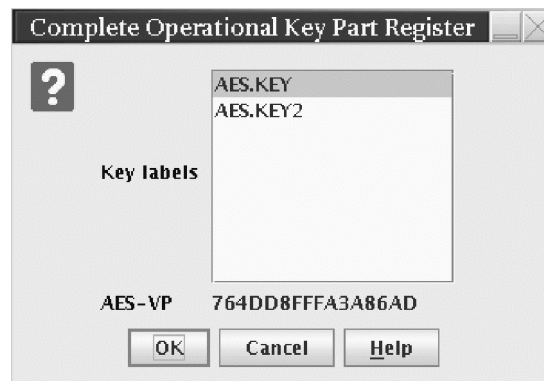


Figure 121. Complete AES Operational Key Part Register - predefined DATA key type

When only one key label is selected for an AES key, the AES-VP of the accumulated key in the key part register is displayed. If more than one key label is selected then the AES-VP field on the window contains a '-'.

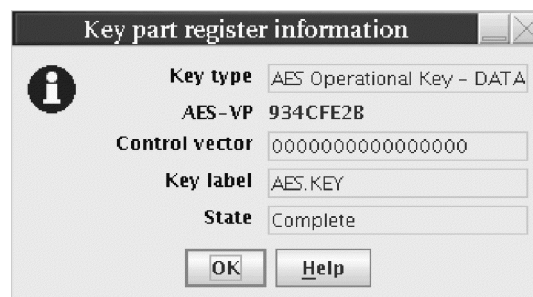


Figure 122. AES Key part register information - predefined DATA key type in Complete state

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 completed DES keys and the AES-VP is shown for completed AES keys.



Figure 123. DES Key part register information - predefined EXPORTER key type in Complete state

After all the key labels that were selected are processed, a message 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 predefined 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.

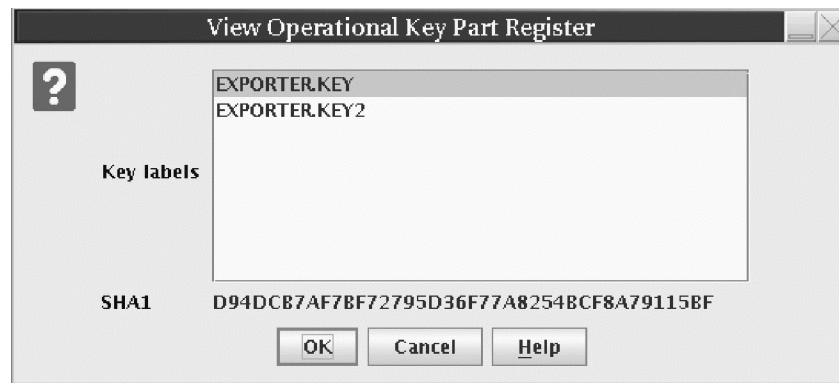


Figure 124. View DES Operational Key Part Register - EXPORTER, one key label selected

To select one key label, highlight the label using the left mouse button. To select more than one key label, highlight the label using the left mouse button, then hold down the Control key and highlight additional key labels using the button. To select a range of key labels, highlight the first key label using the left mouse button, then hold down the Shift key and highlight the last key label. All key labels 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 verification pattern of the accumulated key in the key part register is displayed (SHA-1 for DES keys, AES-VP for AES keys). If more than one key label is selected then the verification pattern field on the window contains a '-'.

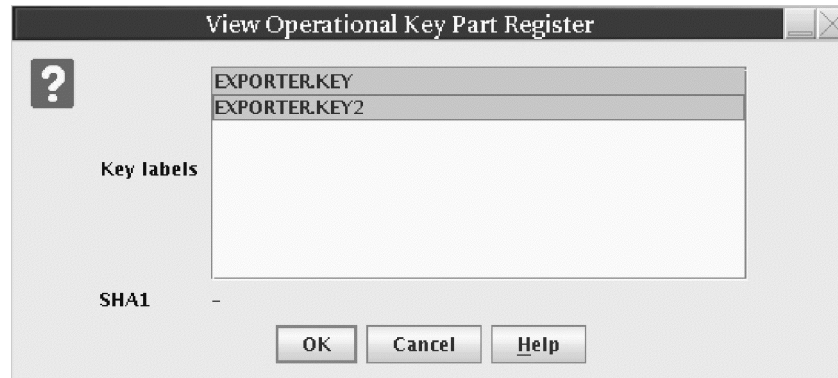


Figure 125. View DES Operational Key Part Register - EXPORTER, all key labels selected

When View is selected for a USER DEFINED key type, the **View Operational Key Part Register** window is displayed with all the domain's key part registers containing DES keys.

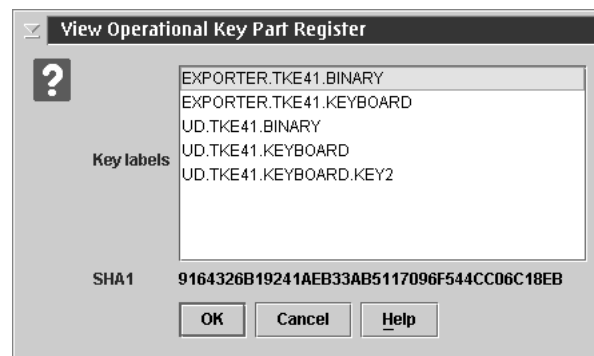


Figure 126. View DES Operational Key Part Register - USER DEFINED

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 (CV) will be turned on. This is true for predefined and USER DEFINED key types.



Figure 127. View DES 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 for DES keys, and the AES-VP value of the completed key is displayed for AES keys. The control vector for the completed key will have the key part bit

turned off.

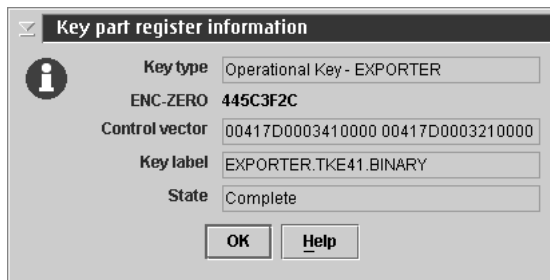


Figure 128. View DES key part register information - complete key

After all the key labels that were selected are processed, a message is displayed indicating that the command was executed successfully.



Figure 129. 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 he or she wants to clear the key part registers.

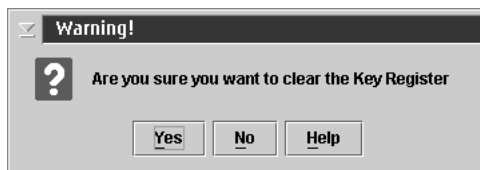


Figure 130. Warning! message for clear operational key part register

When clear is selected for a predefined 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, then all key part registers of the key type selected will be displayed regardless of key length.

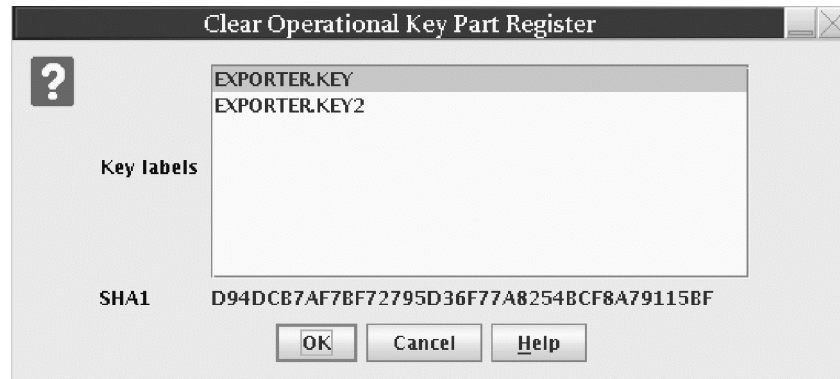


Figure 131. Clear Operational Key Part Register - EXPORTER key type, one key label selected

To select one key label, highlight the label with the left mouse button. To select more than one key label, highlight the label with the left mouse button, then hold down the Control key and highlight additional key labels with the button. To select a range of key labels, highlight the first key label with the left mouse button, then hold down the Shift key and highlight the last key label. All key labels 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 verification pattern of the accumulated key in the key part register is displayed (SHA-1 for DES keys, AES-VP for AES keys). If more than one key label is selected then the verification pattern field on the window contains a '-'.

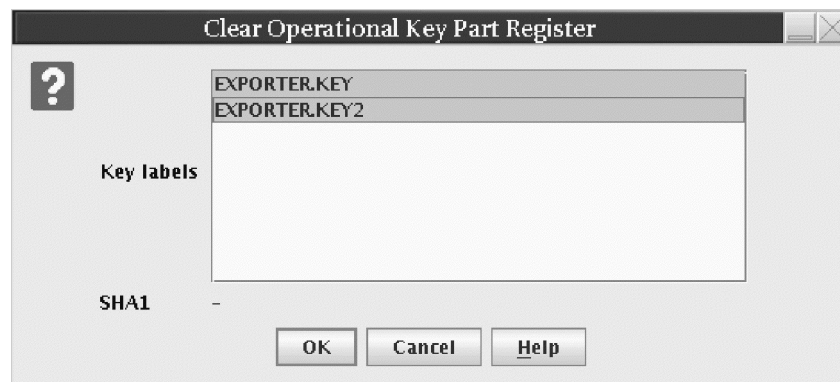


Figure 132. Clear DES Operational Key Part Register - EXPORTER key type, all key labels selected

When **Clear** is selected for a USER DEFINED key type, the **Clear Operational Key Part Register** is displayed with all the domain's key part registers containing DES keys.



Figure 133. Clear DES Operational Key Part Register - USER DEFINED, one key label selected

When you press the **OK** command button on the Clear Operational Key Part Register window, the selected key labels are processed, and a message is displayed indicating that the command was executed successfully.



Figure 134. Clear Key Register successful message

## Load to Key Storage

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. Having selected **Load to Key Storage**, the user chooses one of the following key parts to load to the workstation key storage:

- First...
- Intermediate...
- Last...

The contents of the container depend upon the user's selection.

If the user selected First, the container shows all keys in the workstation key storage usable as IMP-PKA key encrypting keys. The user can utilize these as skeletons for composing the new key label.

If the user selected Intermediate or Last, the container shows all keys in the workstation key storage that have been installed with the first key part. It also shows any optional intermediate key parts that have been installed. The user must select one of these as the key label.

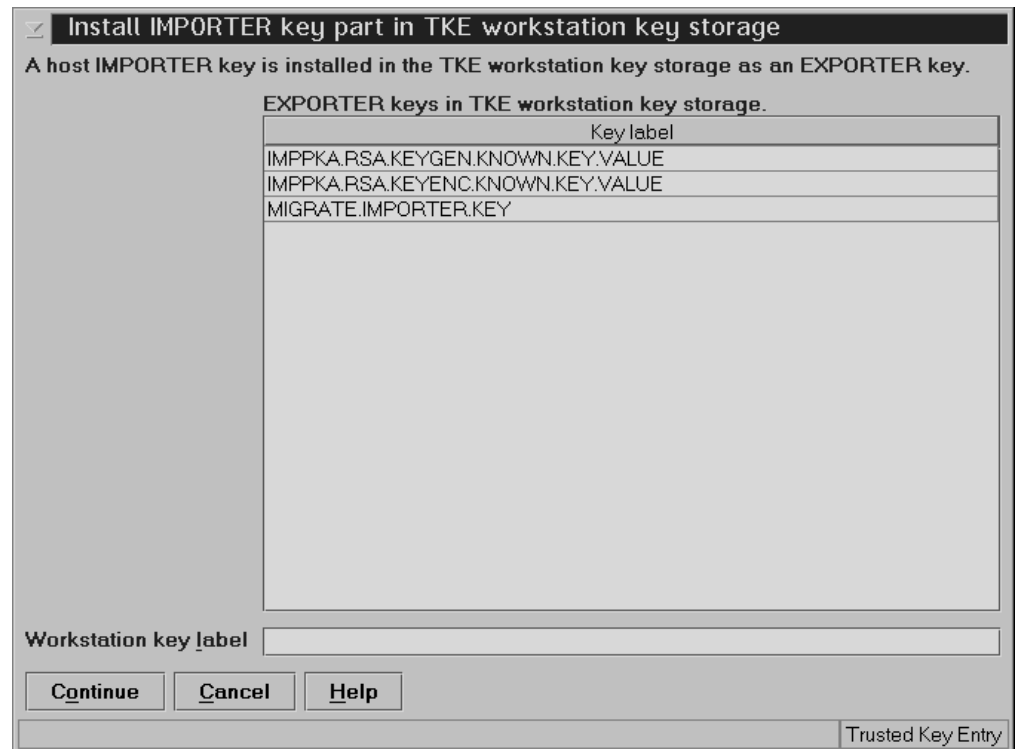


Figure 135. Install Importer Key Part in Key Storage

For IMP-PKA keys, you must specify additional information. A window is displayed for the user to specify the workstation key label and whether this IMP-PKA key will be used for protecting either an RSA key to be generated at the workstation or a clear RSA key to be enciphered at the workstation.

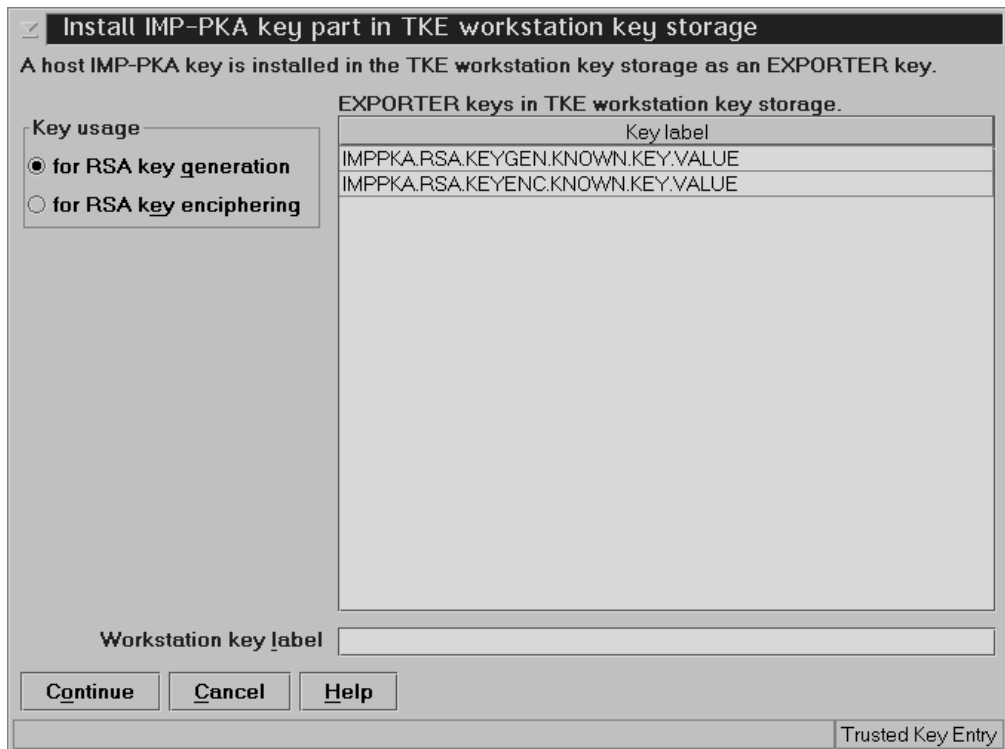


Figure 136. Install IMP-PKA Key Part in Key Storage

**Note:** For the RSA key to be loaded into the PKDS, the same IMP-PKA key value must be stored in the CKDS. See “Load to Key Part Register First” on page 153.

### Secure Key Part Entry

To save known key part values to a TKE Smart Card use secure key part entry. Refer to Appendix A, “Secure Key Part Entry,” on page 275 for details on using this function.

## RSA Keys

### Generate RSA Key

**Note:** On z10 EC, z10 BC, and z196, 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 137. Generate RSA Key

In the Generate RSA key window, specify the following information:

- **RSA key usage control** — Specifies whether or not the RSA key can be used for key management purposes (encryption of DES keys). All RSA keys can be used for signature generation and verification.
- **Key length** — Length of the modulus of the RSA key in bits. All values from 512 to 1024 are valid.
- **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. The key-encrypting keys are sometimes referred to as workstation EXPORTER keys. 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 drive, USB flash memory drive, or TKE Data Directory) and file name for saving the generated RSA key.

#### Warnings:

1. 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 “TKE Media Manager” on page 313.
2. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

### Encipher RSA Key

This selection allows an RSA key to be read from a clear key file, encrypted with a previously generated IMP-PKA key encrypting key, and saved in a file. The format of the clear key file is described in Appendix E, “Clear RSA Key Format,” on page 301.

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** VM16P1.IMPPKA.RSA.KEYENC.KNOWN.KEY.VALUE

**Encipher** **Cancel** **Help**

☐ Trusted Key Entry

Figure 138. Encipher RSA Key

In the Encipher RSA key window, specify the following information:

- **RSA key usage control** — Specifies whether the RSA key can be used for key management purposes (encryption of DES keys). All RSA keys can be used for signature generation and verification.

- **PKDS key label** — Label to be given the imported RSA key at the host. The information provided in this field can be changed when you load the RSA key to the host.
- **Private key name** — Text string that is included in the RSA key token and cryptographically related to the key. The private key name can be used for access control for the key. The information you entered in the PKDS key label field is copied to this field and can be edited.
- **Description** — Optional free text that is saved with the RSA key and displayed when you retrieve the key.
- **Workstation 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. These key-encrypting keys are previously generated IMP-PKA keys that are currently in the TKE workstation key storage. 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, USB flash memory drive, or TKE Data Directory) and file name for saving the encrypted RSA key.

#### Warnings:

1. 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 “TKE Media Manager” on page 313.
2. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

### Load RSA Key to PKDS

This selection allows the user to load an RSA key to the host and install it in the PKDS. Using this function, it is only possible to load the RSA key to the PKDS in the TKE Host LPAR. For loading RSA keys to TKE target LPARs, see “Load RSA Key to Host Dataset” on page 172.

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 139. Load RSA Key to PKDS

In the Load RSA key to PKDS window, specify the following information:

- **PKDS key label** — Label to be given the imported RSA key at the host. Change this field as needed.
- **Private key name** — Text string that is included in the RSA key token and cryptographically related to the key. The private key name can be used for access control for the key. The information you entered in the PKDS key label field is copied to this field and can be edited.
- **Description** — Optional free text that was saved with the RSA key.
- **Workstation 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

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 207.

The steps are the same as for loading an RSA key to PKDS (see “Load RSA Key to PKDS” on page 171), 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 140. 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.

- 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**

**Note:** When managing domain controls through a TKE 7.0 workstation, services displayed on the Domain Controls panel may not be available on the host crypto module. Enabling services on this panel that are not supported by the host crypto module will NOT make this service available.

### Working with Domains Controls Settings

You are able to administer access control points to ISPF Services, API Cryptographic Services and User Defined Extensions (UDX) from this page.

There are expandable folders for the Domain Cryptographic services. Some services cannot be disabled because they are “required”. This is indicated on the panel. You can enable or disable services within the following folders:

- ISPF Services
- API Cryptographic Services
- UDXs (appears only if you have created UDXs on your system)

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.

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.

For new TKE 7.0 users, all access control points enabled in the Default Role will be enabled on the supported host crypto modules (CEX2C and CEX3C). If migrating

from TKE V4.0 or later to TKE 7.0 on a z10 EC, z10 BC, or z196, 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. (For UDXs with access control points, enablement requires a TKE workstation.)

**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 DES, AES, ECC, and Asymmetric Master Keys on supported host crypto modules through the ICSF panel interface.

If you are using a TKE workstation for the first time, your settings under ISPF Services will indicate that all services are enabled.

**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 B, “Access Control Points and Callable Services,” on page 281 for the correlation between the access control point and the ICSF callable service.

**UDXs:** The UDX folder appears only if there are User Defined Extensions on your system. The UDXs folder lists your extensions and allows you to enable or disable them.

---

## Crypto Module Notebook Co-Sign Tab

For co-signing a pending command in a host crypto module, open the notebook for that crypto module and select the Co-sign page. This page displays the following information on the command to co-sign:

- **Pending command** – Name of the pending command
- **Pending command reference** – Unique hexadecimal number returned to the issuer of the command
- **Loading Authority** – Issuer of the command
- **Pending command details container** – Important parts of the pending command
- **Signature requirements container** – Current status for the fulfillment of the signature requirements

For host crypto module, 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**.

Pressing the **Co-sign** button initiates the signing of the pending command. It opens windows where you can choose the source of the authority signature key and then choose the authority index associated with that key. The possible authority signature key sources are as follows:

- **Current key** - Uses the currently loaded signature key
- **Smart card** - Reads an authority signature key from a TKE smart card
- **Binary file** - Reads an authority signature key from a hard disk or diskette
- **Key storage** - Reads an authority signature key from PKA key storage
- **Default key** - Uses the default authority signature key hardcoded into TKE

Press **Delete** if you want to delete the pending command.

---

## Chapter 8. Auditing

TKE 7.0 implements logging of security relevant operations that occur on the TKE workstation. TKE provides auditors with a trail of activities on the TKE workstation that are not currently tracked. Security actions performed on the TKE workstation are recorded in a security log and tied to a user identity. TKE security audit records are in addition to the SMF records that are already cut on the host system that are triggered by requests from TKE.

To perform auditing tasks or configure auditing settings on the TKE workstation, you must log on with the AUDITOR user name. When logged on to the TKE Workstation as AUDITOR, you are able to:

- Use the TKE Audit Configuration Utility to turn TKE auditing on and off.
- Use Service Management functions to:
  - View the security log
  - Archive the security logs
  - Format security logs to DVD-RAM
- Use the TKE Audit Record Upload Configuration Utility to configure audit record upload to a System z host, where the audit records will be saved in the z/OS System Management Facilities (SMF) dataset.

ICSF also uses SMF record type 82 to record certain ICSF events. ICSF writes to subtype 16 whenever a TKE workstation either issues a command request to, or receives a reply response from, a Crypto Express2 Coprocessor or Crypto Express3 Coprocessor. In addition to the subtype 16 records, you can use the TKE Audit Record Upload Configuration Utility to send Trusted Key Entry workstation security audit records to a System z host. These security audit records are stored in the SMF dataset as a type 82 subtype 29 record.

---

### TKE Audit Configuration Utility

To configure auditing, log on with the AUDITOR user name, select **Trusted Key Entry** and then select the **Audit Configuration Utility**.

The TKE Audit Configuration Utility is displayed.

By default, all available auditing is enabled.



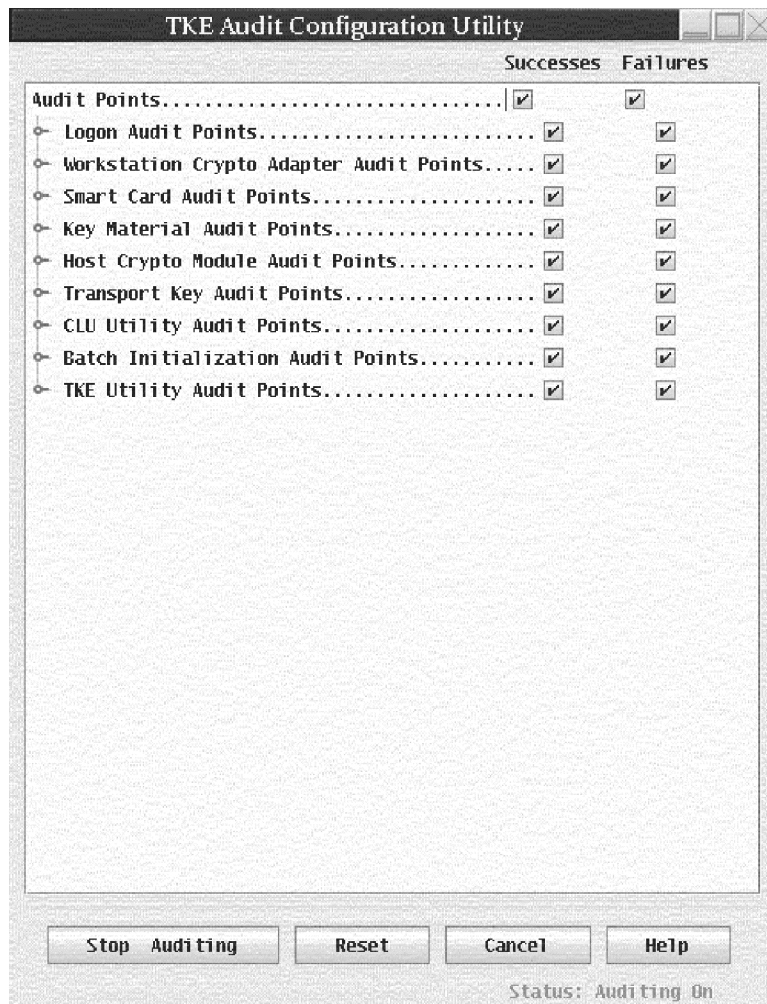


Figure 141. Default settings for auditing

You can customize the auditing utility to your desired preference. To turn off auditing, click on **Stop Auditing** to change the status to **Auditing Off**.



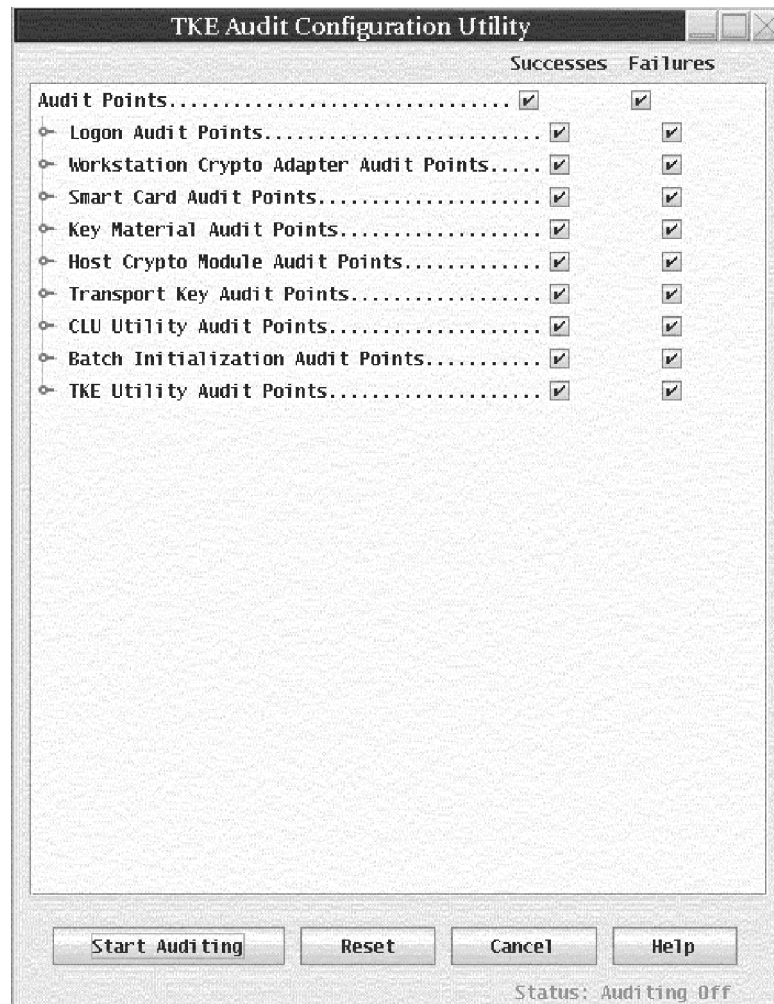


Figure 142. Auditing is off

If you wish to enable and disable specific audit records (both successes and failures) you can expand each audit point to see the individual audit records associated with the group by clicking on the symbol to the left of the audit point.

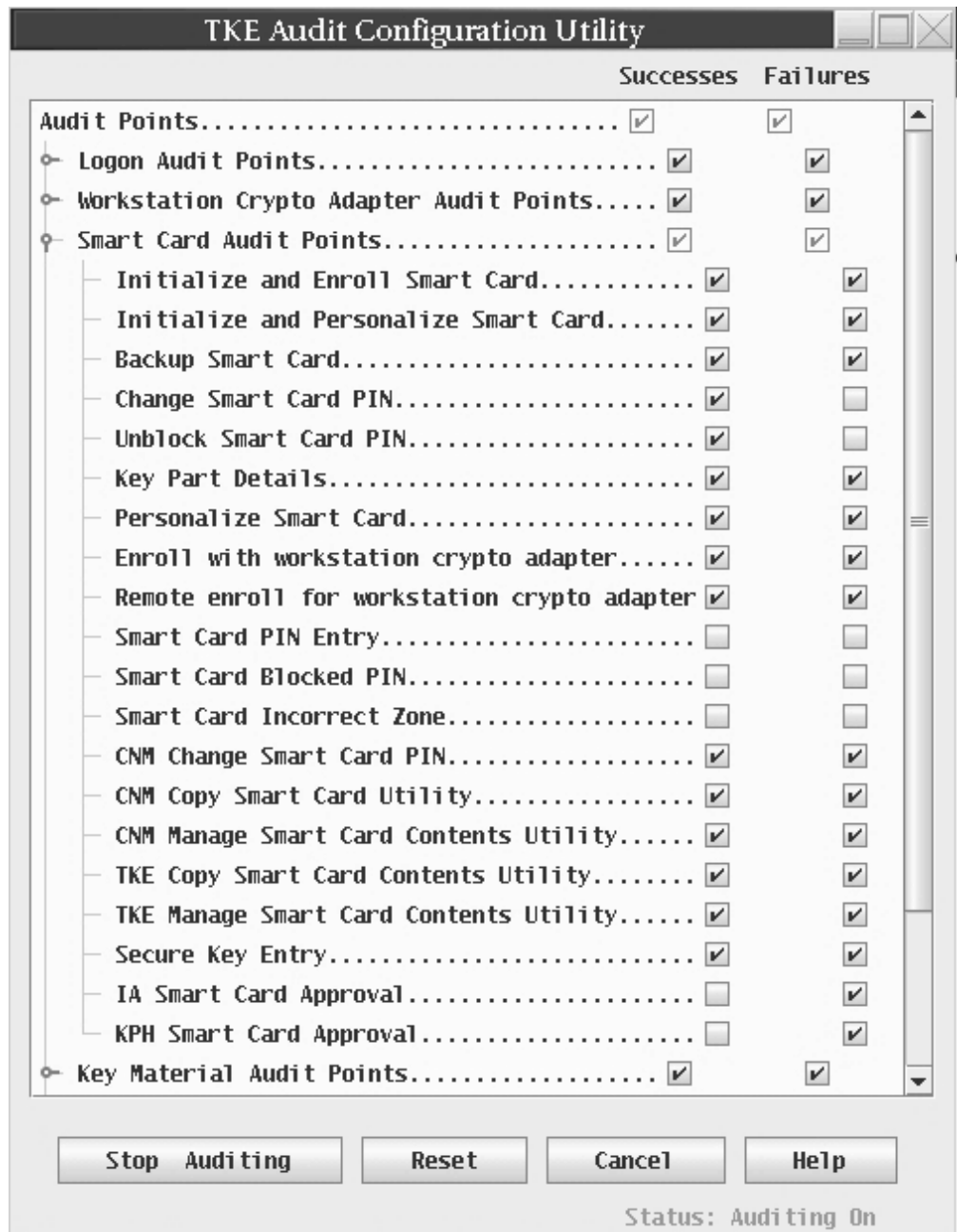


Figure 143. Example of expanded auditing points

When you expand an audit point, you can configure the individual audit records as desired.

If you wish to enable or disable all success or failure audit points, you can click on the successes or failures checkbox on the line corresponding to the audit points group.

---

## Service Management Auditing Functions

You can use Service Management functions to perform the following auditing tasks:

- View the security log
- Archive the security logs
- Format security logs to DVD-RAM

### View Security Logs

The security logs can be viewed on the TKE, but only when you are logged in with the AUDITOR user name. The security log has a max size allowed of 30MB.

When the security log reaches 75% full, a hardware message alerts the user on the TKE console. The View Security Logs task determines if the message displays. By default, the message displays.

When the security log reaches 100% capacity, the oldest third of the audit records are deleted.

In order to avoid deleting records you can either archive the security logs (see “Archive Security Logs” on page 181) or format the security logs to a DVD-RAM (see “Format Security Logs to DVD-RAM” on page 182).

In order to view the security logs, log in as the AUDITOR user, select **Service Management** and select **View Security Logs**.

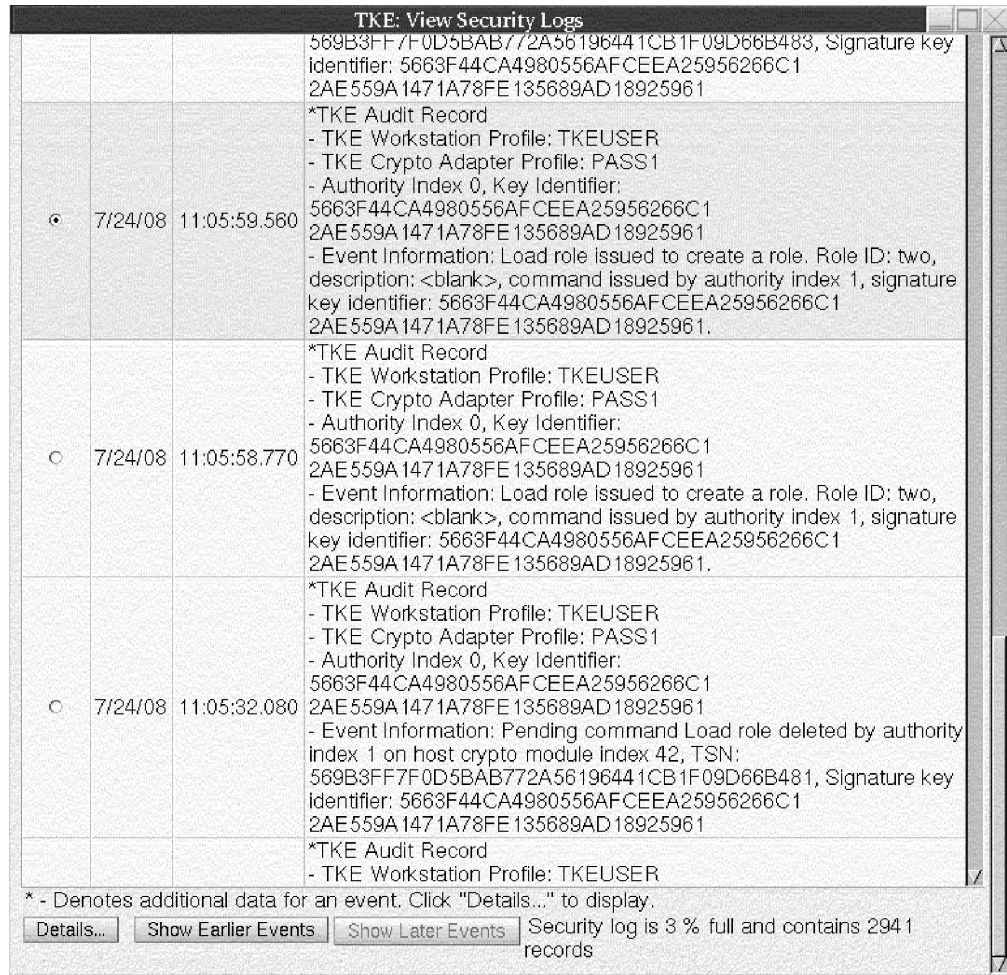


Figure 144. Viewing the security logs

This log displays 1000 records per page. The 1000 record pages can be navigated by clicking on **Show Earlier Events** and **Show Later Events**.

If the audit record contains an asterisk (\*) next to the line saying 'TKE Audit Record', this means that there are further details available to view. You can view the details by selecting the radio button corresponding to the desired audit record and clicking **Details...**





Figure 145. Viewing additional details of the security logs

## Archive Security Logs

If you wish to archive the security logs you must be logged onto the TKE console with the AUDITOR user name. Archiving the security logs saves the security log's event data in another file on the DVD-RAM or USB flash memory drive, and then erases enough events from the security log to reduce its size to 20% of its maximum capacity.

In order to Archive the Security log, log in as the AUDITOR user and select **Service Management**. From the service management window select **Archive Security Logs**.

**Note:** You must either have a DVD-RAM or USB flash memory drive that is formatted with no volume label or a volume label of ACTSECLG. In order to do this, use the Format Media utility (see "Format Media" on page 331).



Figure 146. Archiving the security logs

With a valid DVD-RAM or USB flash memory drive inserted, click **Archive**.

While the security log is being archived, an "Archiving Security Log..." message box displays. After the archiving is completed, a message box displays indicating that the archive operation has completed.

## Format Security Logs to DVD-RAM

Formatting the security logs to DVD-RAM copies the security log in ASCII format to DVD-RAM. If you wish to format the security logs to DVD-RAM you must be logged onto the TKE console with the AUDITOR user name. Select **Service Management** and from the service management window select **Format Security Logs to DVD-RAM**.

A dialog box prompts you to insert a DVD-RAM.

**Note:** You must either have a DVD-RAM that is formatted with no volume label or a volume label of ACTSECLG. In order to do this, use the Format Media utility (see "Format Media" on page 331).



Figure 147. Formatting the security logs

With a valid DVD-RAM inserted in the drive, click **OK**.

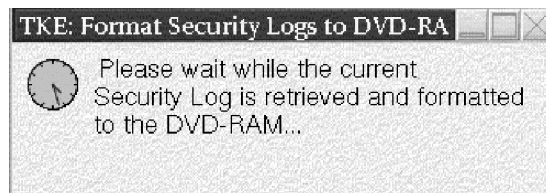


Figure 148. Formatting the security logs message

An information box will display when the security log has been successfully formatted to DVD-RAM.



Figure 149. Formatting the security logs complete message

## TKE Audit Record Upload Configuration Utility

ICSF uses SMF record type 82 to record certain ICSF events. ICSF writes to subtype 16 whenever a TKE workstation either issues a command request to, or receives a reply response from, a Crypto Express2 Coprocessor or Crypto Express3 Coprocessor. In addition to the subtype 16 records, you can use the TKE Audit Record Upload Configuration Utility to send Trusted Key Entry workstation security audit records to a System z host, where they will be saved in the z/OS System Management Facilities (SMF) dataset. Each TKE security audit record is stored in the SMF dataset as a type 82 subtype 29 record.

**Note:** The audit upload process does not remove any data from the TKE Workstation. Copies of security audit records are sent to the host system and all data is retained by the TKE Workstation.

## Starting TKE Audit Record Upload Configuration Utility

To use the TKE Audit Record Upload Configuration Utility, you must first sign on to the Trusted Key Entry console in privileged mode with the AUDITOR user ID. To do this:

1. Close the Trusted Key Entry Console.
2. From the Welcome to the Trusted Key Entry Console screen select *Privileged Mode Access*.
3. From the Trusted Key Entry Console Logon screen, enter the user name ADMIN and the password. (The default password is PASSWORD, but this can be changed by the user. See “Change Password” on page 325.)
4. Press the **Logon** command button.

To start the TKE Audit Record Upload Configuration Utility, go to the Trusted Key Entry Console Workplace window and select *TKE Audit Record Upload Utility*.

The TKE Audit Record Upload Configuration Utility window is displayed.

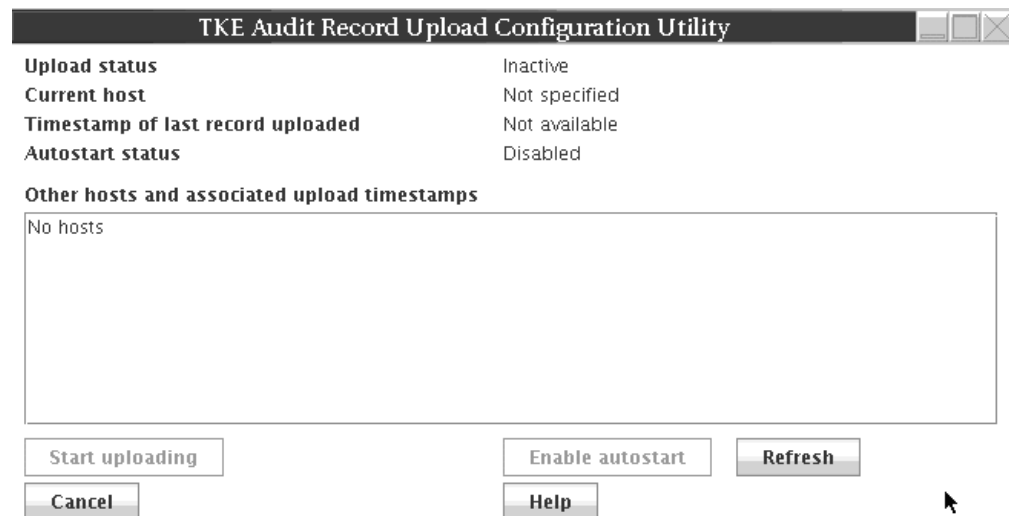


Figure 150. TKE Audit Record Upload Configuration Utility

Using the TKE Audit Record Upload Configuration Utility, you can:

- Specify the host machine to which the audit records will be sent. See “Configure TKE for Audit Data Upload” on page 184 for more information.

- Upload audit records to the target host. See “Uploading Audit Records” on page 185 for more information.
- Enable automatic audit record upload. When enabled, audit records will be uploaded every time the workstation is rebooted. See “Enabling and Disabling Automatic Audit Record Upload” on page 186 for more information.

## Configure TKE for Audit Data Upload

To upload audit data to a host system, you need to add the target host to the TKE Audit Record Upload Utility's host list, and make the target host the current host. To do this:

1. Add the target host to the TKE Audit Record Upload Utility's host list. To do this:
  - a. In the TKE Audit Record Upload Configuration Utility window, right click to display a popup menu, and select the **Add Host** menu item.  
The Specify Host Information dialog is displayed.

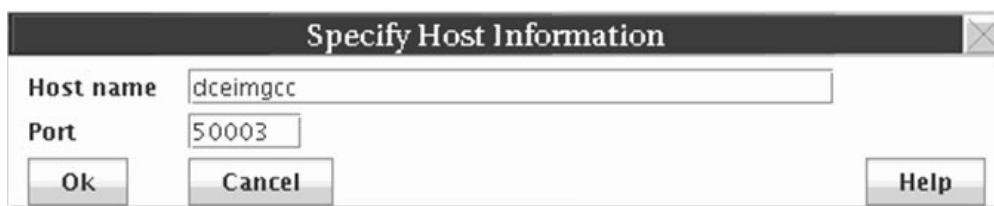


Figure 151. Specify Host Information dialog

- b. In the Specify Host Information dialog's Host name field, enter the host name.
- c. In the Specify Host Information dialog's Port field, enter the port number assigned to the TKE Host Transaction Program.
- d. Click the **Ok** command button.

The Specify Host Information dialog closes and the host name is added to the TKE Audit Record Upload Configuration Utility's host list. The host name will appear in the *Other hosts and associated timestamps* area of the window.

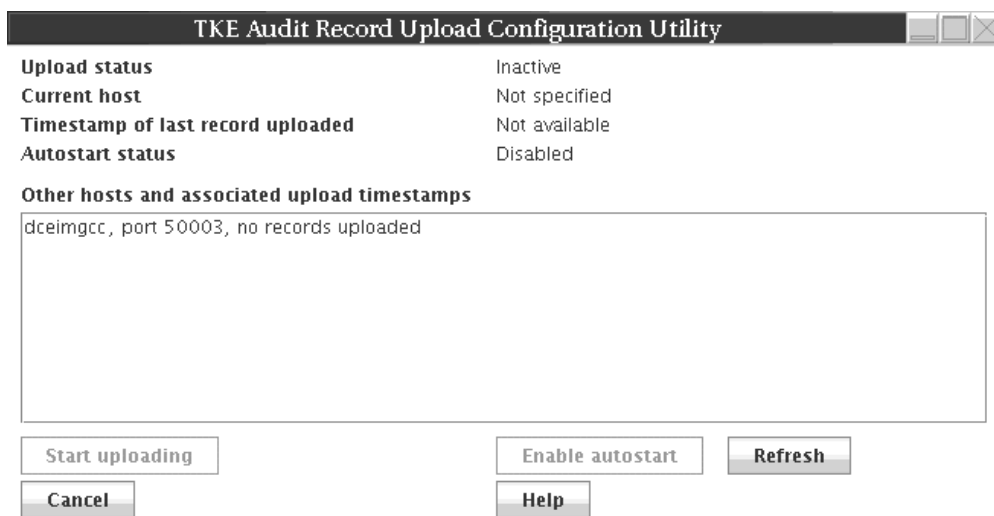


Figure 152. Other hosts and associated timestamps



2. Make the target host the current host. To complete this step, you must have a user ID and password for the target host.
  - a. In the TKE Audit Record Upload Utility window's *Other hosts and associated timestamps* area, click on the target host name to highlight it.
  - b. In the TKE Audit Record Upload Utility window's *Other hosts and associated timestamps* area, right click on the target host name to display a popup menu, and select the **Specify current host** menu item.The Specify Host Login Information dialog is displayed.



Figure 153. Specify Host Login Information

- c. In the Specify Host Login Information dialog, enter the user ID and password, and click the **Ok** command button.The target host is made the current host. The host name will appear in the Current Host field of the TKE Audit Record Upload Configuration Utility

Once the TKE Audit Record Upload Utility to specify the target host, you can:

- Upload audit records to the target host. See "Uploading Audit Records" for more information.
- Enable automatic audit record upload. When enabled, audit records will be uploaded every time the workstation is rebooted. See "Enabling and Disabling Automatic Audit Record Upload" on page 186 for more information.

## Uploading Audit Records

Once you have used the TKE Audit Record Upload Configuration Utility to specify the target host (as described in "Configure TKE for Audit Data Upload" on page 184), you can upload audit records to the target host. If you have not already signed into the host system during this session, the Specify Host Logon Information dialog will prompt you for a user ID and password before the audit records will be uploaded. To complete this task, you must have a user ID and password for the target host.

In the TKE Audit Record Upload Utility window, click the **Start uploading** command button.

**Note:** If you have not already signed into the host system, the Specify Host Logon Information dialog will prompt you for a user ID and password.

The TKE Audit Record Upload Configuration Utility will begin uploading the audit records to the target host. The TKE Audit Record Upload Configuration Utility window's Upload status field will indicate the status of the upload operation.

- Pressing the **Refresh** command button will refresh the TKE Audit Record Upload Utility window. In particular, the Timestamp of last record uploaded field will be updated.
- Pressing the **Stop uploading** command button will stop the audit record upload.

You can also enable automatic audit record upload. When enabled, audit records will be uploaded every time the workstation is rebooted. See “Enabling and Disabling Automatic Audit Record Upload” for more information.

## Enabling and Disabling Automatic Audit Record Upload

Once you have used the TKE Audit Record Upload Configuration Utility to specify the target host (as described in “Configure TKE for Audit Data Upload” on page 184), you can enable automatic audit record upload. This is called autostart mode. In autostart mode, audit records will be uploaded every time the workstation is rebooted. If you have not already signed into the host system during this session, the Specify Host Logon Information dialog will prompt you for a user ID and password before autostart mode will be enabled. To complete this task, you must have a user ID and password for the target host.

In the TKE Audit Record Upload Utility window, click the **Enable autostart** command button.

**Note:** If you have not already signed into the host system, the Specify Host Logon Information dialog will prompt you for a user ID and password.

The TKE Audit Record Upload Configuration Utility will enable autostart mode, and will upload audit records every time the workstation is rebooted. The TKE Audit Record Upload Configuration Utility window's Autostart status field will indicate that autostart is enabled.

To disable automatic audit record upload, click the **Disable autostart** command button.

---

## Chapter 9. Managing Keys

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 z10 system with a CEX2C or CEX3C and the Nov. 2008 or later licensed internal code (LIC), secure AES keys are supported. On the z196 with the Sept. 2010 or later LIC, secure ECC keys are supported.

**ICSF is required to complete some operations initiated from TKE. These operations include setting the AES, ECC, or DES master keys, loading operational keys into the CKDS, and loading RSA keys from a host data set to the PKDS.**

**Note: ICSF is also required for initializing/refreshing the CKDS, 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 188)
- Changing the DES-MK or AES-MK periodically (page 190)
- Reentering the master keys (page 194)
- Adding Additional Coprocessors (page 196)
- Changing the ASYM-MK master keys (page 196)
- Loading Operational Keys to the CKDS (page 201)
- Refreshing the CKDS (page 204)
- Install RSA Keys (page 207)

---

### 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” on page 140.

**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-MK or AES-MK, 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 DES-MK or AES-MK 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 DES-MK or AES-MK. After the master key has been set, you can generate or enter any keys you need to perform cryptographic functions.

To define a DES-MK or AES-MK, you must load the key parts to the DES or AES 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 z10 EC or z10 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 204.

## Initialize the CKDS

At this point, the new DES and/or AES master key register on each host crypto module in this domain is full.

You must now initialize the CKDS (which also activates the DES or AES master key).

From the ICSF Primary Menu on TSO:

1. Select Option 2, MASTER KEY MGMT, as shown in Figure 154 on page 189.

```
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 MGMT  | - 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. 2008. 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 154. ICSF Selecting the Master Key Option on the Primary Menu Panel

2. The Master Key Management panel appears. Select Option 1, INIT/REFRESH/UPDATE CKDS, as shown in Figure 155.

```
CSFMKM10 ----- ICSF - Master Key Management -----
OPTION ==> 1
```

Enter the number of the desired option above.

- |   |                          |  |
|---|--------------------------|--|
| 1 | INIT/REFRESH/UPDATE CKDS | - Initialize a Cryptographic Key Data Set or activate an updated Cryptographic Key Data Set                            |
| 2 | SET MK                   | - Set a master key (AES, DES, ECC)   |
| 3 | REENCIPHER CKDS          | - Reencipher the CKDS prior to changing a symmetric master key   |
| 4 | CHANGE SYM MK            | - Change a symmetric master key and activate the reenciphered CKDS   |
| 5 | INIT/REFRESH/UPDATE PKDS | - Initialize a Public Key Data Set or activate an updated Public Key Data Set or update the Public Key Data Set header |
| 6 | REENCIPHER PKDS          | - Reencipher the PKDS  |
| 7 | CHANGE ASYM PKDS         | - Change an asymmetric master key and activate the reenciphered PKDS   |

Figure 155. 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 156. 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 or AES 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 DES-MK or AES-MK (first, middle, last)
2. Re-encipher CKDS
3. Change master key

The step-by-step procedure for changing the DES or AES master key, reenciphering the CKDS, and activating the new 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 or AES 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(s).

When the DES or AES master key is changed, the current active DES or AES master key is moved to the auxiliary master key register and the new DES or AES 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 DES or AES 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 DES or AES master key register on all supported host crypto cards must be full before you change the master key.

1. Select option 2, MASTER KEY MGMT, 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 MGMT  | - 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 157. 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 158 on page 192, and press ENTER.



```

CSFMKM10 ----- ICSF - Master Key Management -----
OPTION ==> 3

Enter the number of the desired option above.

 1 INIT/REFRESH/UPDATE CKDS - Initialize a Cryptographic Key Data Set or
                             activate an updated Cryptographic Key Data Set
 2 SET MK                    - Set a master key (AES, DES, ECC)
 3 REENCIPHER CKDS           - Reencipher the CKDS prior to changing a symmetric
                             master key
 4 CHANGE SYM MK             - Change a symmetric master key and activate the
                             reenciphered CKDS
 5 INIT/REFRESH/UPDATE PKDS  - Initialize a Public Key Data Set or
                             activate an updated Public Key Data Set or
                             update the Public Key Data Set header
 6 REENCIPHER PKDS           - Reencipher the PKDS
 7 CHANGE ASYM PKDS          - Change an asymmetric master key and activate the
                             reenciphered PKDS

```

Figure 158. Selecting the Reencipher CKDS Option on the ICSF Master Key Management Panel

3. The Reencipher CKDS panel appears. See Figure 159.

```

CSFCMK10 ----- ICSF - Reencipher CKDS -----
COMMAND ==>

To reencipher all CKDS entries from encryption under the current 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 159. 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 160.

```
CSFMKM10 ----- ICSF - Master Key Management -----
OPTION ==> 4

Enter the number of the desired option above.

 1 INIT/REFRESH/UPDATE CKDS - Initialize a Cryptographic Key Data Set or
                             activate an updated Cryptographic Key Data Set
 2 SET MK                    - Set a master key (AES, DES, ECC)
 3 REENCIPHER CKDS          - Reencipher the CKDS prior to changing a symmetric
                             master key
 4 CHANGE SYM MK            - Change a symmetric master key and activate the
                             reenciphered CKDS
 5 INIT/REFRESH/UPDATE PKDS - Initialize a Public Key Data Set or
                             activate an updated Public Key Data Set or
                             update the Public Key Data Set header
 6 REENCIPHER PKDS          - Reencipher the PKDS
 7 CHANGE ASYM PKDS         - Change an asymmetric master key and activate the
                             reenciphered PKDS
```

Figure 160. 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 161.

```
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 161. 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 159 on page 192, 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 host crypto module (CEX2C or CEX3C) clears the master key registers so that the master key values are not disclosed:

- If the card 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 card 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 domains

This command can zeroize 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 crypto modules set for TKE Enablement.

If you are running on z10 servers, you can zeroize the data specific to a domain: master keys, retained keys and operational key part registers

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 DES or AES 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, a tamper situation causes all installation data; master keys, retained keys, operational key part registers, roles and authorities on the crypto card 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 new” on page 143.

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 DES or AES 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 MGMT  | - 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 162. ICSF Selecting the Master Key Option on the Primary Menu Panel

4. To set the DES or AES master key, choose option 2 on the panel and press ENTER.

```
CSFMKM10 ----- ICSF - Master Key Management -----  
OPTION ==> 2
```

Enter the number of the desired option above.

- |   |                          |  |
|---|--------------------------|--|
| 1 | INIT/REFRESH/UPDATE CKDS | - Initialize a Cryptographic Key Data Set or activate an updated Cryptographic Key Data Set                            |
| 2 | SET MK                   | - Set a master key (AES, DES, ECC)   |
| 3 | RENCIPHER CKDS           | - Reencipher the CKDS prior to changing a symmetric master key   |
| 4 | CHANGE SYM MK            | - Change a symmetric master key and activate the reenciphered CKDS   |
| 5 | INIT/REFRESH/UPDATE PKDS | - Initialize a Public Key Data Set or activate an updated Public Key Data Set or update the Public Key Data Set header |
| 6 | RENCIPHER PKDS           | - Reencipher the PKDS  |
| 7 | CHANGE ASYM PKDS         | - Change an asymmetric master key and activate the reenciphered PKDS   |

Figure 163. 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 and/or the AES 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 DES or AES master key, if you choose to, for security reasons. Continue with “Changing Master Keys” on page 190.

---

## Adding Host Crypto Modules After ICSF Initialization

There may come a time when you wish to add additional host crypto modules to your system. After the new crypto modules have been installed and configured by the appropriate hardware personnel, make them known to the TKE workstation by following the appropriate procedure.

**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 crypto module to match the crypto modules currently on the host). Load the authority signature keys to match the other crypto modules.
4. Load a new signature for an authority that can load master keys. If one authority does not have the ability to load all the master key parts for each master key, you may need to load additional authority signature keys.
5. Load the master keys.

**Note:** The keys should be the same keys that you loaded to the other crypto modules. If you are adding more than one crypto module, load the keys in all crypto modules before setting the master key.

6. Set the asymmetric master key from TKE.
7. Set the DES or AES master key on the crypto module from ICSF (see “Setting the Master Key” on page 195) when everything is the same (roles, authorities, controls, master keys).
8. If desired, add the new crypto module to the group by doing a group change.

---

## Asymmetric-keys Master Key Parts

When you enter the asymmetric 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 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 197.

To enter an asymmetric 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 DES or AES master key or asymmetric master key, the host crypto module 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 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 164.

```
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 164. Selecting the Administrative Control Option on the ICSF Primary Menu Panel

2. The Administrative Control Function panel appears. See Figure 165 on page 198.

```

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 165. 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 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 166.

```

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 166. Selecting the Administrative Control Option on the ICSF Primary Menu Panel

2. The Administrative Control Function panel appears. See Figure 167 on page 199.



```

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 167. 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 Master Keys

If you realize that you have made a mistake entering key parts to the asymmetric 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” on page 140 and “Operational Keys” on page 149). Select the asymmetric master key and then select **Clear**.

### Notes:

1. Once the asymmetric 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 Refreshing 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 master keys. See “Load RSA Key to PKDS” on page 171 and “Installing RSA Keys in the PKDS from a Data Set” on page 207 for details.

## Reenciphering and Refreshing the PKDS

For security reasons, your installation should periodically change the asymmetric master key and reencipher the private keys.

To reencipher the PKDS after the ASYM-MK has been changed, go to the Master Key Management panel and select option 6.

```

CSFMKM10 ----- ICSF - Master Key Management -----
OPTION ==> 6

Enter the number of the desired option above.

 1 INIT/REFRESH/UPDATE CKDS - Initialize a Cryptographic Key Data Set or
                             activate an updated Cryptographic Key Data Set
 2 SET MK                    - Set a master key (AES, DES, ECC)
 3 REENCIPHER CKDS          - Reencipher the CKDS prior to changing a symmetric
                             master key
 4 CHANGE SYM MK            - Change a symmetric master key and activate the
                             reenciphered CKDS
 5 INIT/REFRESH/UPDATE PKDS - Initialize a Public Key Data Set or
                             activate an updated Public Key Data Set or
                             update the Public Key Data Set header
 6 REENCIPHER PKDS          - Reencipher the PKDS
 7 CHANGE ASYM PKDS         - Change an asymmetric master key and activate the
                             reenciphered PKDS

```

Figure 168. 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 RSA master key
and/or current ECC master keys to encryption under the current RSA master key
and/or new ECC 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 169. Reencipher PKDS

Press enter to reencipher the PKDS. Once successful, you will then want to refresh the PKDS. Return to the Master Key Management panel and select option 5.

```

CSFMKM10 ----- ICSF - Master Key Management -----
OPTION ==> 7

Enter the number of the desired option above.

 1 INIT/REFRESH/UPDATE CKDS - Initialize a Cryptographic Key Data Set or
                             activate an updated Cryptographic Key Data Set
 2 SET MK                    - Set a master key (AES, DES, ECC)
 3 REENCIPHER CKDS          - Reencipher the CKDS prior to changing a symmetric
                             master key
 4 CHANGE SYM MK            - Change a symmetric master key and activate the
                             reenciphered CKDS
 5 INIT/REFRESH/UPDATE PKDS - Initialize a Public Key Data Set or
                             activate an updated Public Key Data Set or
                             update the Public Key Data Set header
 6 REENCIPHER PKDS          - Reencipher the PKDS
 7 CHANGE ASYM PKDS         - Change an asymmetric master key and activate the
                             reenciphered PKDS

```

Figure 170. Selecting the Refresh 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 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 171. Refresh PKDS

After you press ENTER, the PKDS becomes active.

## Loading Operational Keys to the CKDS

You can load operational key parts into key part registers on host crypto modules. To load these keys into the CKDS you need to use the ICSF Operational Key Load panel or KGUP. For KGUP details, refer to *z/OS Cryptographic Services ICSF Administrator's Guide*.

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 crypto module 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 MGMT  - 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. ICSF Primary Menu Panel

2. The Coprocessor Management panel appears. Put a 'K' by the coprocessor 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 173. Coprocessor Management Panel

3. The Operational Key Load panel appears. The coprocessor previously selected and the active CKDS are displayed at the top of the panel.

```

CSFCMP50 ----- ICSF Operational Key Load -----
COMMAND ==>

Coprocessor selected for new key: X04
CKDS name: 'CSFLPAR1.SYSPLEX.CKDS'

Enter the key label

Key label
==> FRED.S.MAC.KEY

Control Vector ==> YES      YES or NO

```

Figure 174. 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 153.
- 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 Operational Key Load panel appears alerting you that CKDS RECORD EXISTS. If you want to replace the existing key with the new key you are trying to load, press ENTER.

```
CSFCMP51 ----- ICSF 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 175. Operational Key Load Panel

When the key has been successfully loaded the ENC-ZERO value (DES Operational Keys) or the AES-VP value (AES Operational Keys) of the key and the control vector are displayed for the user.

```
CSFCMP50 ----- ICSF Operational Key Load ----- KEY LOAD COMPLETE
COMMAND ==>

Coproprocessor 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 176. Operational Key Load Panel - ENC-ZERO and CV values displayed

```

CSFCMP50 ----- ICSF 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.AES.KEY

Control Vector ==> YES          YES or NO

AES-VP:
Control vector: 0000000000000000

```

Figure 177. Operational Key Load Panel - AES control vector 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/UPDATE CKDS to access the Initialize a CKDS panel, which is shown in Figure 178.

```

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 178. 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 the record authentication is enabled. 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.

---

## Updating the CKDS with the AES master key

On systems that support the AES master key, you can add the AES master key to any existing CKDS. It is also possible to add the DES master key to a CKDS that was initialized with only the AES master key.

These are the steps to update the CKDS:

1. Load the new AES master key by using the master key entry panels or by using TKE. The AES master key must be loaded on all active coprocessors.
2. From the Primary Menu, select option 2, MASTER KEY MGMT:

```
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 MGMT      - 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

5694-A01 (C) Copyright IBM Corp. 1990, 2008. 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 179. Selecting the Master Key option on the primary menu panel*

3. Select option 1, INIT/REFERSH/UPDATE CKDS.



```

CSFMKM10 ----- ICSF - Master Key Management -----
OPTION ==> 1

Enter the number of the desired option above.

 1 INIT/REFRESH/UPDATE CKDS - Initialize a Cryptographic Key Data Set or
                             activate an updated Cryptographic Key Data Set
 2 SET MK                    - Set a master key (AES, DES, ECC)
 3 REENCIPHER CKDS          - Reencipher the CKDS prior to changing a symmetric
                             master key
 4 CHANGE SYM MK            - Change a symmetric master key and activate the
                             reenciphered CKDS
 5 INIT/REFRESH/UPDATE PKDS - Initialize a Public Key Data Set or
                             activate an updated Public Key Data Set or
                             update the Public Key Data Set header
 6 REENCIPHER PKDS          - Reencipher the PKDS
 7 CHANGE ASYM PKDS         - Change an asymmetric master key and activate the
                             reenciphered PKDS

```

Figure 180. ICSF Master Key Management Panel

4. The Initialize a CKDS panel appears. In the CKDS field, enter the name of an existing, initialized CKDS.

```

CSFCKD20 ----- ICSF - Initialize a CKDS -----
COMMAND ==>

Enter the number of the desired option.

 1 Initialize an empty CKDS
   Record authentication required? (Y/N) ==>
 2 REFRESH - Activate an updated CKDS
 3 Update an existing CKDS

Enter the name of the CKDS below.

CKDS ==> 'FIRST.EMPTY.CKDS'

```

Figure 181. ICSF Initialize a CKDS Panel if AES master keys are supported

5. Choose option 3, Update an existing CKDS and press **ENTER**. ICSF will check the status of the new master key registers and the master key verification pattern of the master key is written to the CKDS header record. Note that all the CKDS' that you wish to update should be processed prior to going to step 6.
6. In the CKDS field, enter the name of the updated CKDS that will be the active CKDS.
7. Select option 2, REFRESH and press **ENTER**. The in-storage copy of the CKDS will be updated with your updated CKDS.

```

CSFCKD20 ----- ICSF - Initialize a CKDS -----
COMMAND ==>

Enter the number of the desired option.

1 Initialize an empty CKDS
   Record authentication required? (Y/N) ==>
2 REFRESH - Activate an updated CKDS
3 Update an existing CKDS

Enter the name of the CKDS below.

CKDS ==> 'FIRST.EMPTY.CKDS'

```

Figure 182. ICSF Initialize a CKDS Panel

8. Return to the Master Key Management panel by pressing **END**. Choose option 2, SET MK and press **ENTER**. ICSF sets the AES master key and your system can be used to encrypt AES key operations.

## 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 201), 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 MGMT - 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 183. 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 184. 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 185. 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 10. 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 enabled to support Smart Cards. See “Initializing TKE for smart cards” on page 77.

To start CNM, go to Trusted Key Entry, Applications, and click on Cryptographic Node Management Utility 4.1.0.



Figure 186. CNM main window

---

### Passphrase Logon

When logging on to the Cryptographic Node Management Utility (CNM), you will be prompted to enter a user ID and passphrase. They are both case sensitive. The user ID and passphrase could be one of the predefined ones shipped with the TKE (such as user ID TKEADM), or one that has been defined at your installation.



Figure 187. Passphrase logon prompt

## Smart Card Logon

When you click on the CNM utility's Smart Card Logon button, you will be prompted 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.

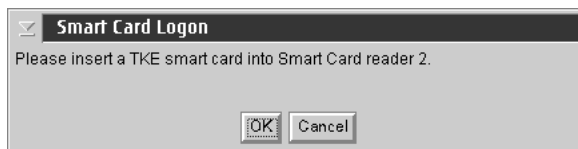


Figure 188. TKE smart card prompt

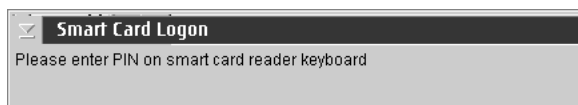


Figure 189. PIN prompt

## Group Logon

Group logon allows multiple users to cosign a logon to the TKE cryptographic adapter. When you click on the CNM utility's Group Logon button, a dialog will prompt you to enter a group profile name for Group ID. Profile names are case sensitive.



Figure 190. 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.

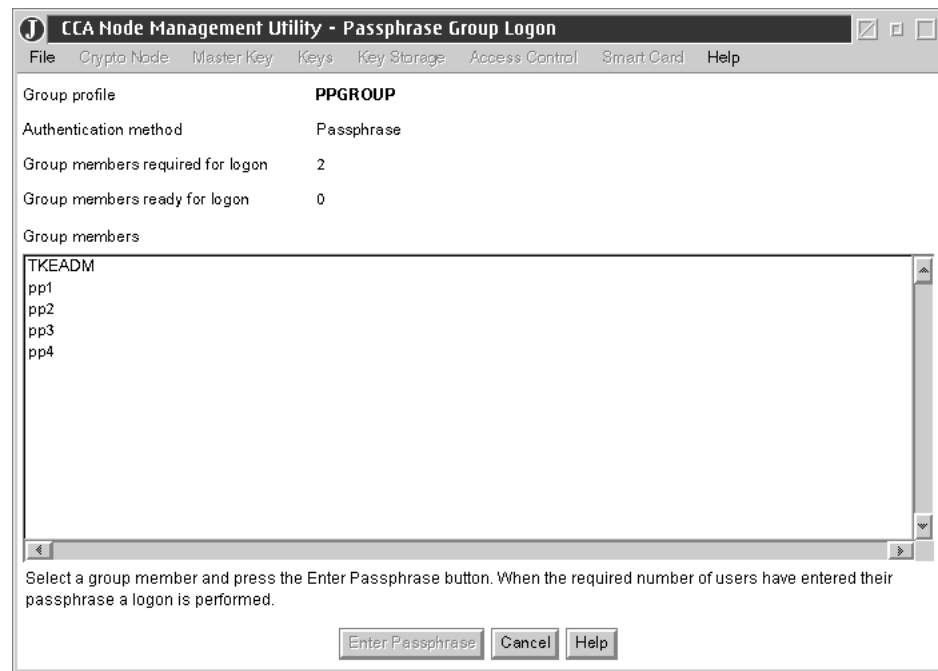


Figure 191. Group logon prompt

In this window, the group profile name is displayed and 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 or her 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 or her passphrase.

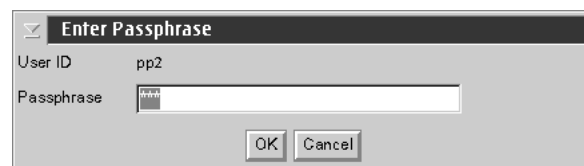


Figure 192. Passphrase group logon - enter passphrase prompt

The list is updated indicating that the user is *ready for logon*. The *Group members ready for logon* field is incremented.

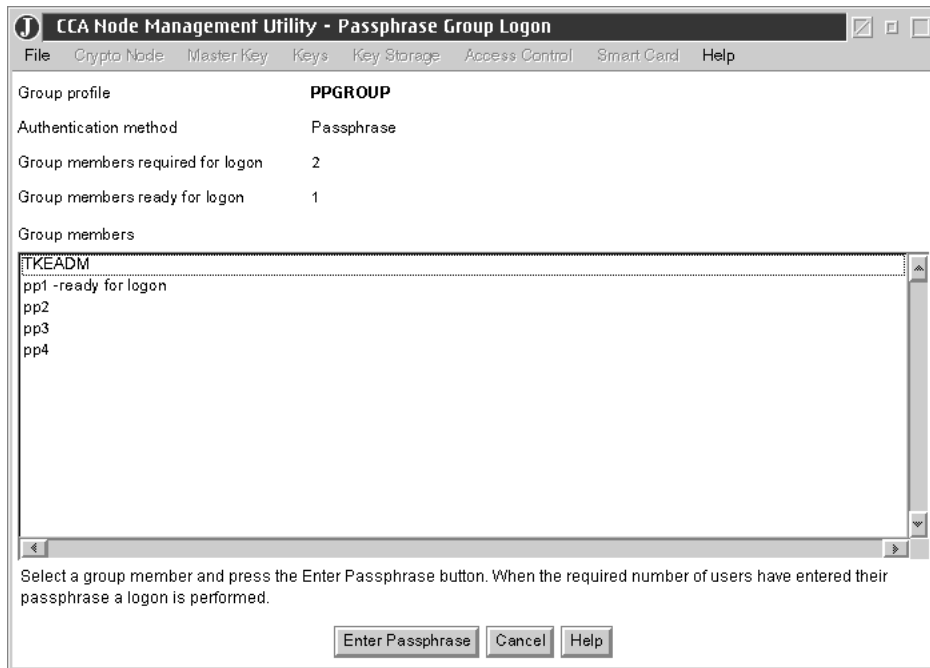


Figure 193. Passphrase group logon - member is ready for logon

When *Group members ready for logon* equals *Group members required for logon*, the logon is performed.

If the group logon is successful, a *Group Logon Completed* message is displayed.



Figure 194. 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.

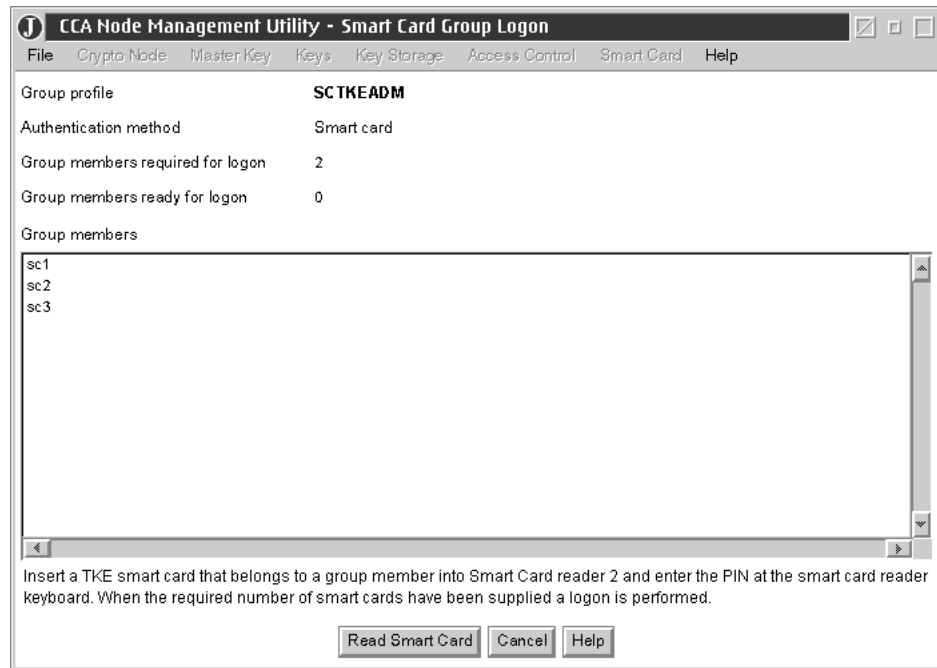


Figure 195. Smart card group logon window

In this window, the group profile name is displayed and 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 or her TKE smart card into smart card reader 2 and enter his or her 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 or her 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.

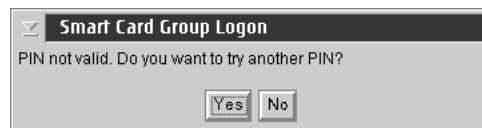


Figure 196. Smart card group logon — retry PIN prompt



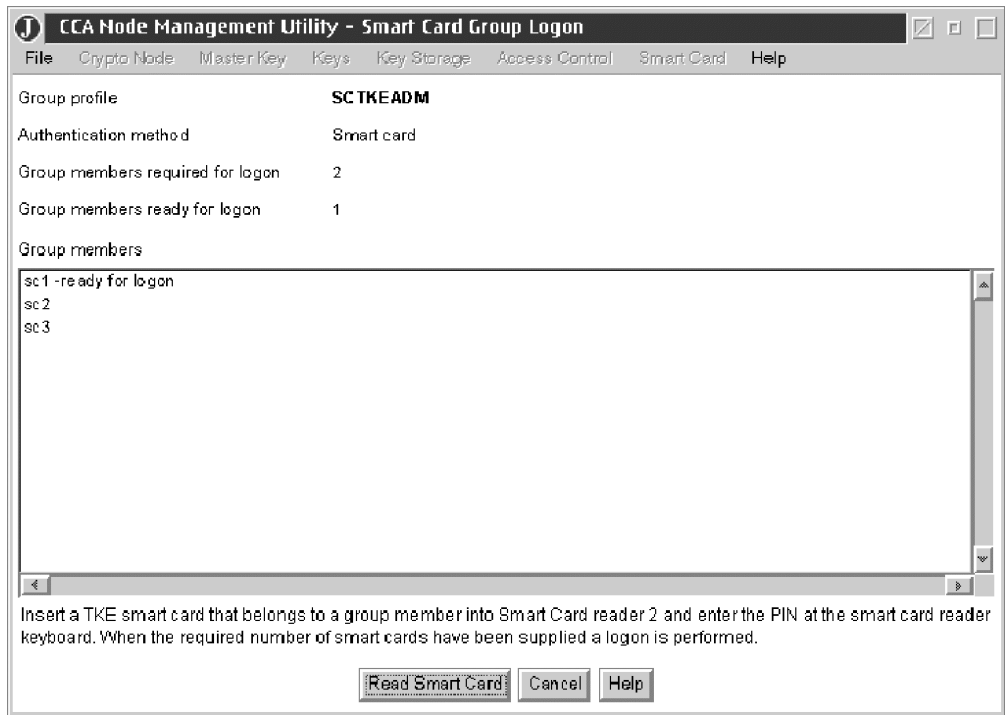


Figure 197. Smart card group logon window - member is ready for logon

**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 265.)

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 198. 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.

## File Menu

From the **File** pull-down, you can choose any of the following:

- CNI Editor
- Enable Smart Card Readers
- Exit
- Exit and Logoff

## Exit

Exit the CNM 4.1.0 application.

## Exit and Logoff

To logoff from the TKE cryptographic adapter, and exit from CNM, select **Exit and Logoff** from the **File** pull-down menu.

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 logon.

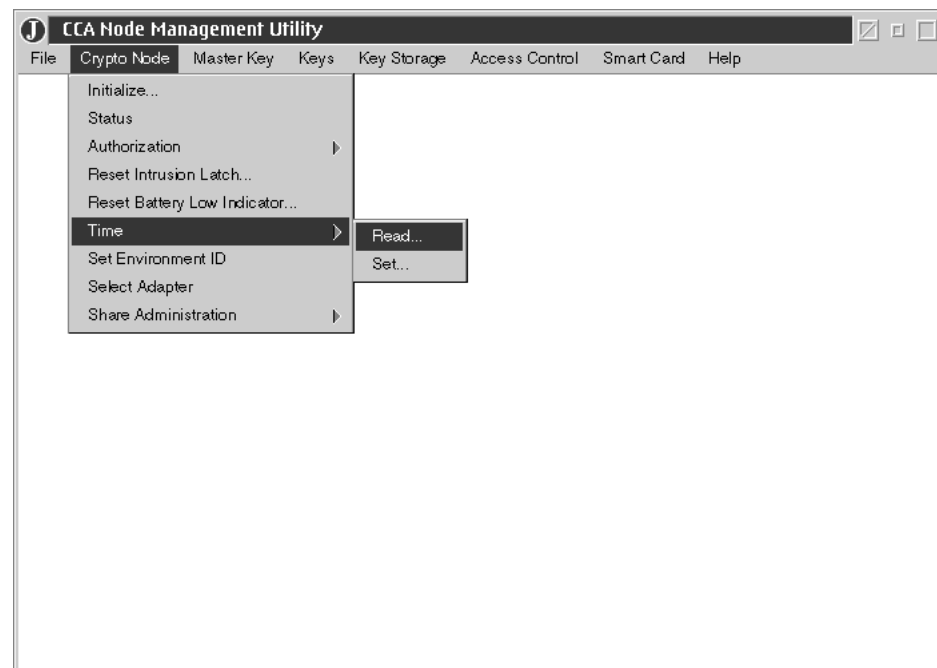


Figure 199. CNM main window — Crypto Node Time sub-menu

### 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 200. 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 dialog is displayed.



Figure 201. Sync time with host window

3. Respond **Yes** in the confirmation dialog to synchronize the clock-calendar with the host.
4. Finish the task by selecting **OK**.

---

## Access Control Menu

The access control 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 crypto adapter logon key contained on a TKE smart card and protected by the smart card PIN that identifies the user.

A TKE administrator can manage roles and profiles from the CNM utility Access Control pull-down menu.



Figure 202. 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:

- DEFAULT
- TKEUSER
- TKEADM
- KEYMAN1
- KEYMAN2

For smart card:

- DEFAULT
- 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 do the following:

- Open or edit a disk-stored role
- Edit a role loaded in the TKE crypto adapter

## Open or edit a disk-stored role

Follow the steps listed below for opening and editing a disk-stored role. In addition, when you need to reload the DEFAULT or the TEMPDEFAULT role, the steps listed for opening and editing a disk-stored role should also be followed. 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, do the following:

1. From the **Access Control** pull-down menu, select **Roles**; a list of currently defined roles is displayed:



Figure 203. Role Management panel - list of roles loaded to the TKE crypto adapter for Smart Card

2. Press the **Open** command button at the bottom of the window. The **Specify file to open** window displays.

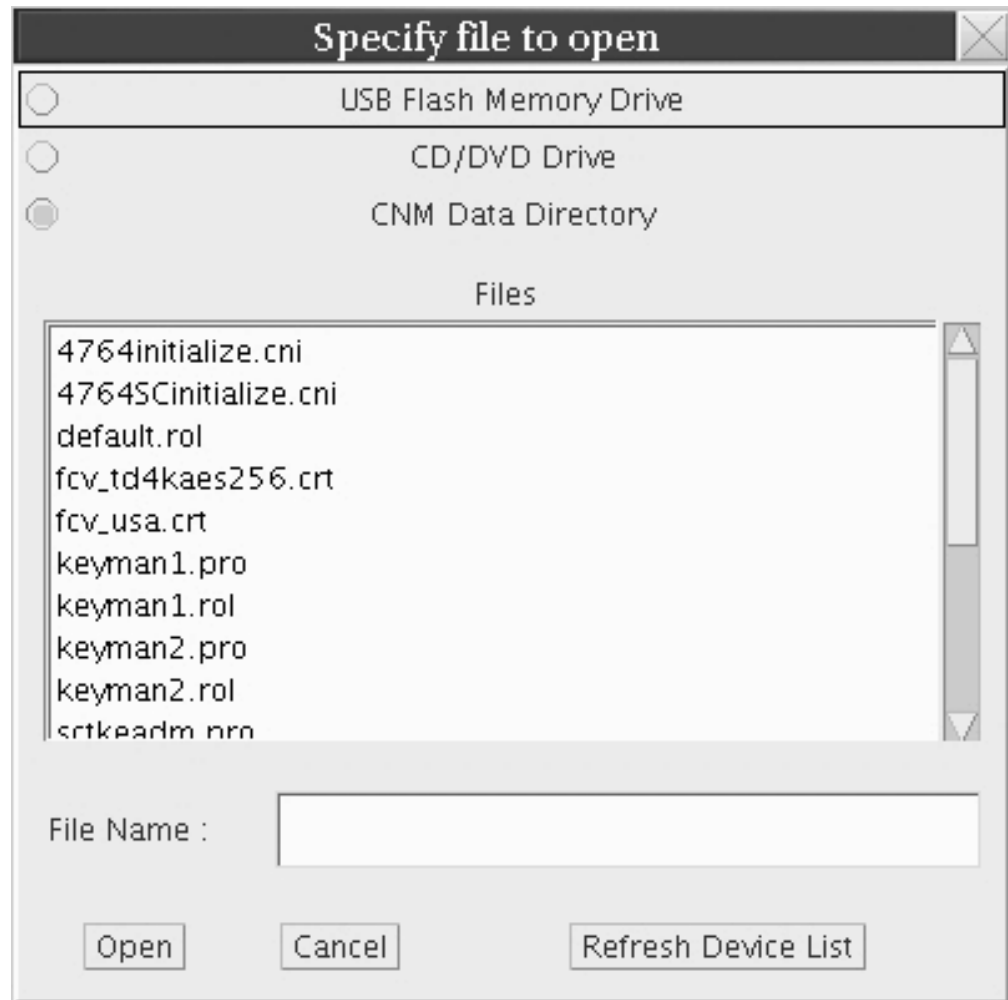


Figure 204. Open a disk-stored role - choose a file

**Note:** All predefined roles and profiles will be in the CNM Data Directory.

3. In the **Specify file to open** window, select a file and click the **Open** command button. The data is displayed in the Role Definition panel.

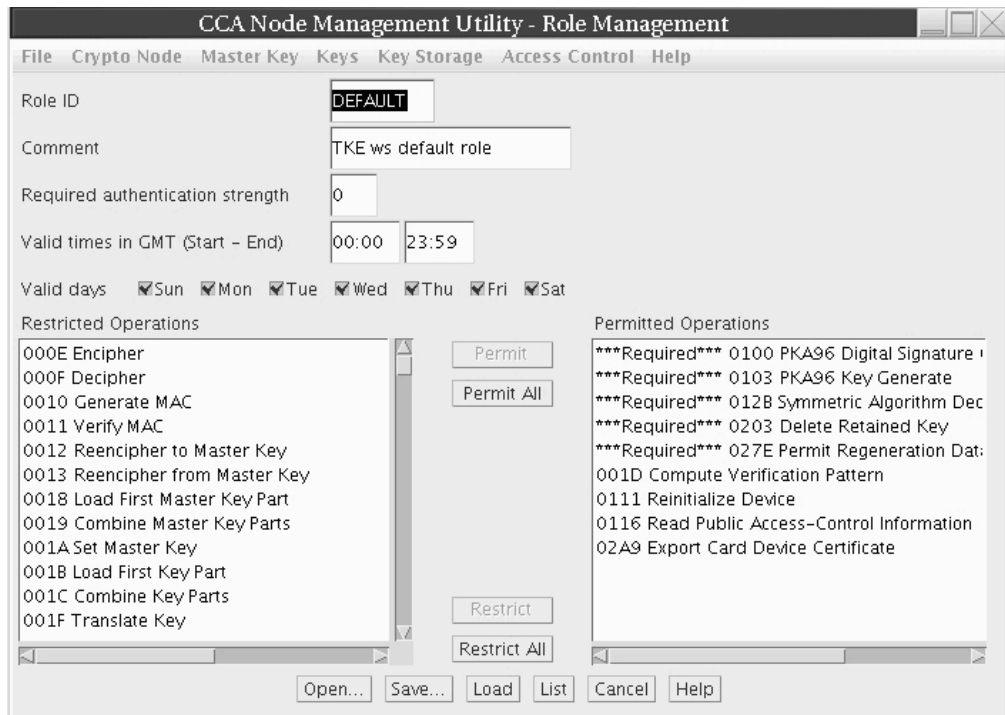


Figure 205. Role Definition panel - role is displayed

4. Select **Load** to save the new role to the TKE cryptographic adapter.  
Certain Access Control Points are required for all roles. These will automatically be listed in the Permitted Operations area of the CNM utility and will be added to the role.
5. A "Role successfully loaded" message displays.

### Edit a role loaded in the TKE crypto adapter

To edit a role loaded in the TKE cryptographic adapter, do the following:

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.

**Warning:** 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 7.0, you may need to add access control points to your roles. See Chapter 3, "Migration," on page 23.

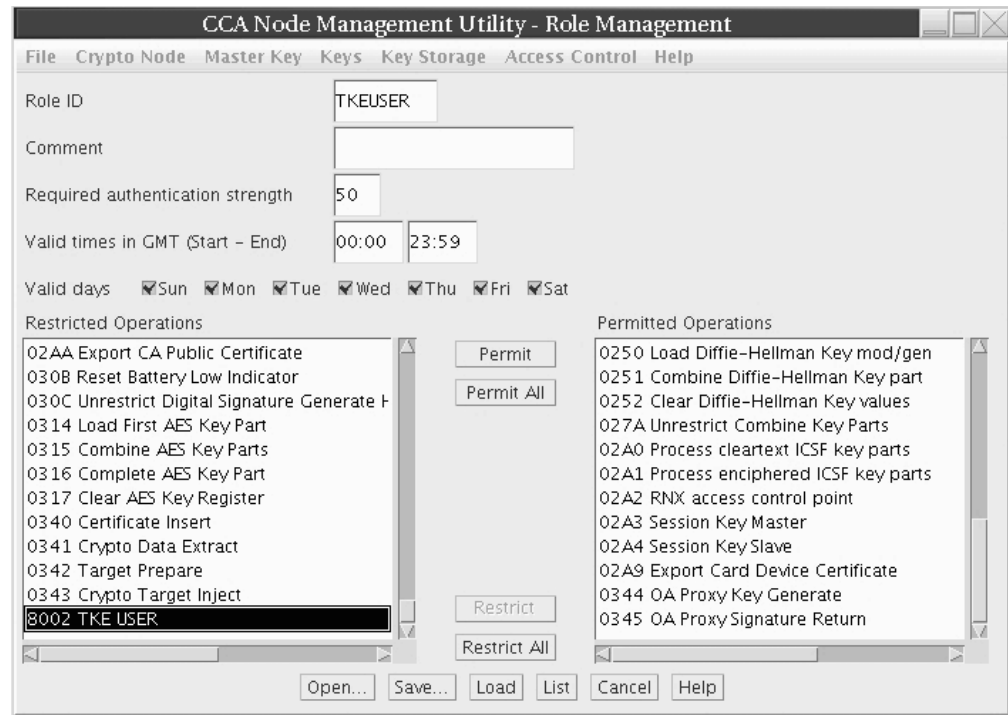


Figure 206. Edit a role - highlight access point to permit

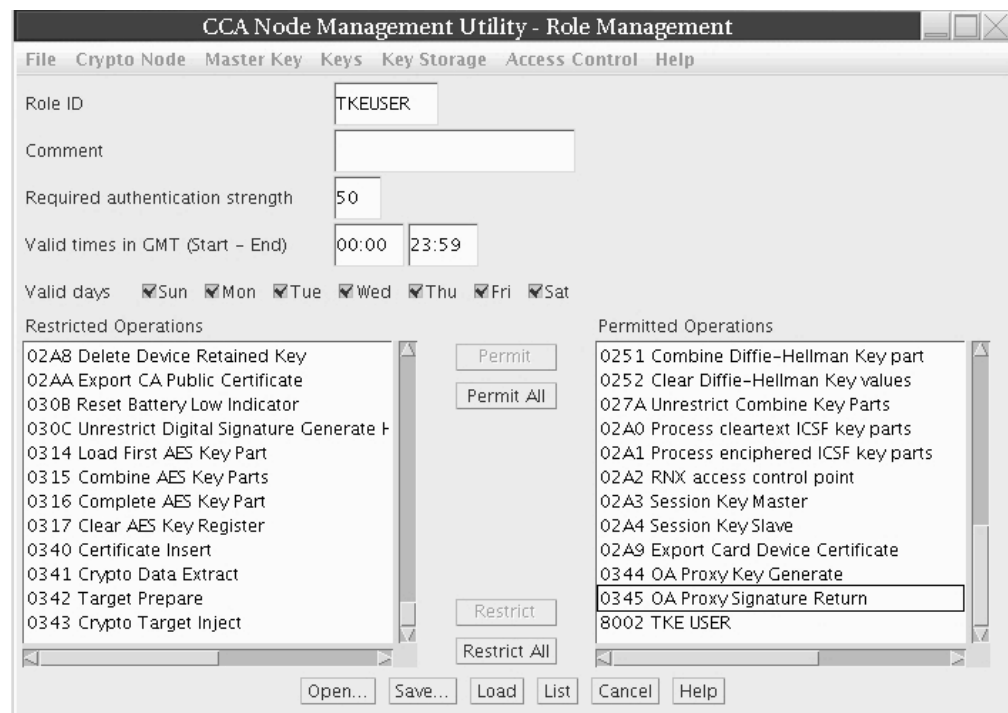


Figure 207. Edit a role - access point is moved to Permitted Operations column

5. Select **Save** to save the role to disk; you will be prompted for a file name. You may save the file to either the CNM data directory, a CD/DVD, or a USB flash memory drive.



Certain Access Control Points are required for all roles. These will automatically be listed in the Permitted Operations area of the CNM utility and will be added to the role.

Select **Load** to load the role into the TKE cryptographic adapter.

**Warnings:**

- a. 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 “TKE Media Manager” on page 313.
- b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

## Define a User Profile

A user profile identifies a specific user to the TKE cryptographic adapter. To define a user profile, do the following.

1. From the **Access Control** pull-down menu, select **Profiles**. A list of existing profiles is displayed.



Figure 208. Profile management panel — profile list

### Passphrase profiles

TKE supplies the following predefined profiles:

- |                |  |
|----------------|--|
| <b>TKEUSER</b> | Associated with role TKEUSER. Use this profile for logging onto the TKE application and performing TKE functions.              |
| <b>TKEADM</b>  | 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

- 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 dialog is displayed, enabling you to select the profile type – either **Passphrase**, **Smart card** or **Group**. Select the type of profile you want to define, and press **Continue**.

Depending on your choice, see the following topics:

- “Define a Passphrase Profile”
- “Define a Smart Card Profile” on page 225
- “Define a Group Profile” on page 228

### Define a Passphrase Profile

1. If Passphrase is selected as the profile type when defining a user profile, a panel is displayed with fields for defining a passphrase profile.

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 content area includes 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 209. Profile Management panel — Passphrase profile

2. Fill in the fields on the panel as described below:

- 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. The passphrase must:

- be at least 8 characters, and cannot be more than 64 characters
- contain at least two letters and at least two numbers
- must not contain the user ID

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 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.

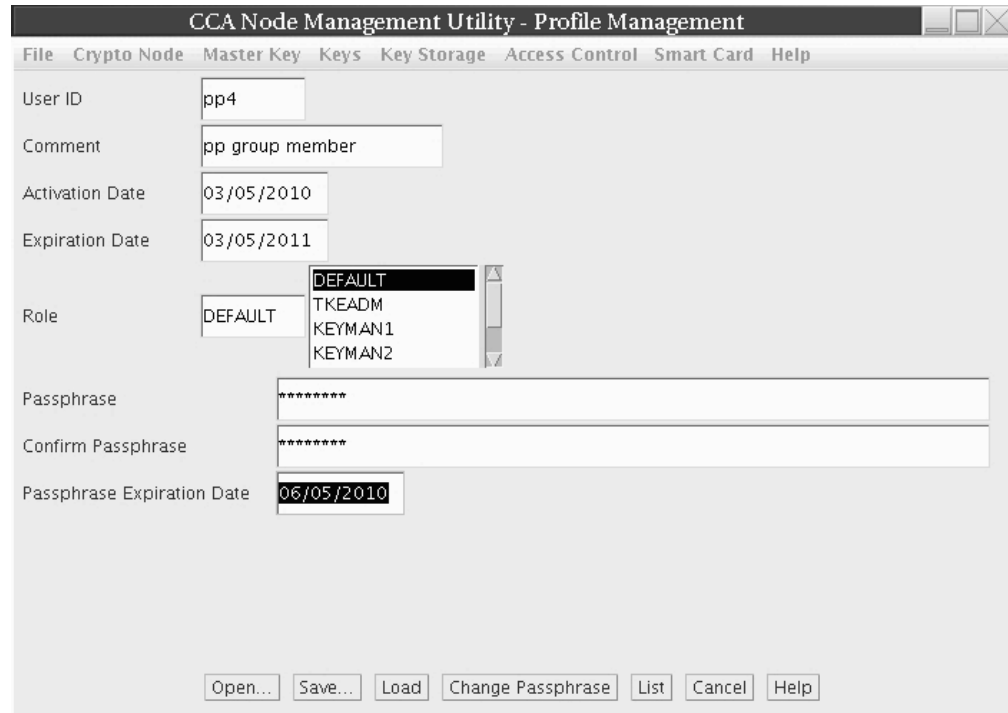


Figure 210. Profile Management panel — Passphrase profile fields filled in

3. Select **Save** to save the profile to disk.

**Warnings:**

- a. 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 “TKE Media Manager” on page 313.
- b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

4. Select **Load** to load the profile into the TKE crypto adapter.

Other actions and tasks available from this panel are as follows:

- 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, a dialog will prompt you to insert a TKE smart card into smart card reader 2. Insert the TKE smart card and press the OK command button.



Figure 211. Smart card profile — TKE smart card prompt

2. The TKE smart card is read, and the information is displayed in a smart card profile panel of the CNM utility window.

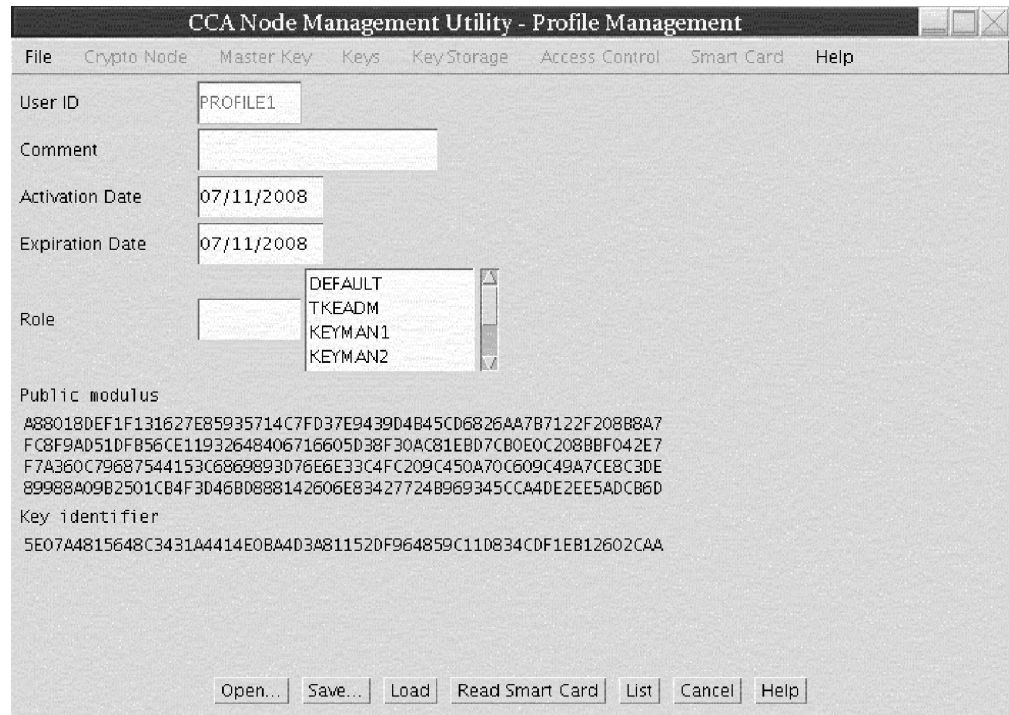


Figure 212. Profile management panel — smart card profile

3. Fill in the fields on the panel as follows:

<b>User ID</b>	The name of the profile. This field is read from the TKE Crypto Adapter logon key and cannot be changed. The User ID is set when the Crypto Adapter logon key is generated. (See Generate Crypto Adapter logon key).
<b>Comment</b>	An optional character string. A maximum of 20 characters may be specified.
<b>Activation Date</b>	Determines the first date when the user can logon. This field defaults to the current date. Change this date as appropriate.
<b>Expiration Date</b>	Determines the last date when the user can logon. This field defaults to the current date. Change this date as appropriate.
<b>Role</b>	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 logon key read from the TKE smart card. This field cannot be changed. See “Generate TKE Crypto Adapter logon key” on page 244.

**Key Identifier** This is the SHA-256 hash of the DER-encoded public modulus and public exponent of the TKE crypto adapter logon key read from the TKE smart card. This field cannot be changed.

Figure 213. Profile Management panel – smart card profile fields filled in

4. Select **Save** to save the profile to disk.

#### Warnings:

- a. 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 “TKE Media Manager” on page 313.
- b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

5. Select **Load** to load the profile into the TKE crypto adapter.

Other actions and tasks available from this panel are as follows:

- 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 Crypto Adapter logon key of 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, a panel is displayed for defining a group profile.

Figure 214. Profile Management panel — Passphrase Group profile

2. Fill in the fields on the panel as follows:

**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.

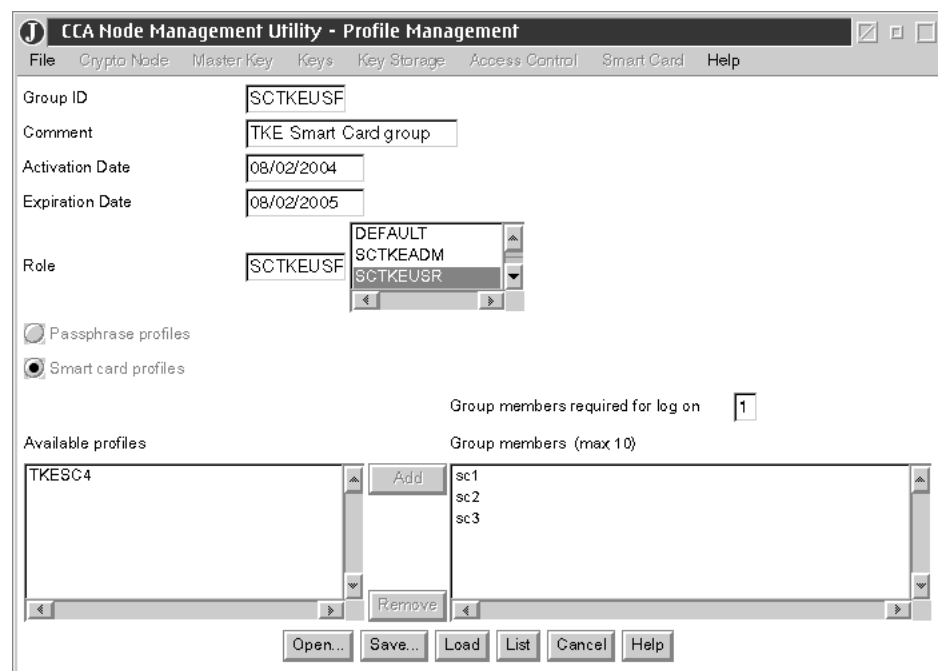


Figure 215. Profile Management panel — Smart Card Group profile filled in

3. Select **Save** to save the profile to disk.

### Warnings:

- a. 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 "TKE Media Manager" on page 313.
  - b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.
4. Select **Load** to load the profile into the TKE crypto adapter.

Other actions and tasks available from the panel are as follows:



- 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 do any of the following:

- 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, do the following:

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 or USB flash memory drive.

#### Warnings:

- a. 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 “TKE Media Manager” on page 313.
- b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

### Edit a User Profile loaded in the TKE Crypto Adapter

To edit a user profile loaded in the TKE crypto adapter, do the following:

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 DVD-RAM or USB flash memory drive.

#### Warnings:

- a. 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 “TKE Media Manager” on page 313.
- b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a

| message related to the operation that is using the drive. If you do remove a  
| drive before the operation is complete, hardware messages may be  
| generated on the TKE workstation.

### **Delete a User Profile loaded in the TKE Crypto Adapter**

To delete a user profile loaded in the TKE crypto adapter, do the following:

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, do the following:

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**

From the **Master Key** pull-down menu of the CNM main window, you can choose one of the following:

- Auto Set...
- Create Random Master Key...
- Clear New...
- Clear Parts
- Smart Card Parts
- Set...
- Verify

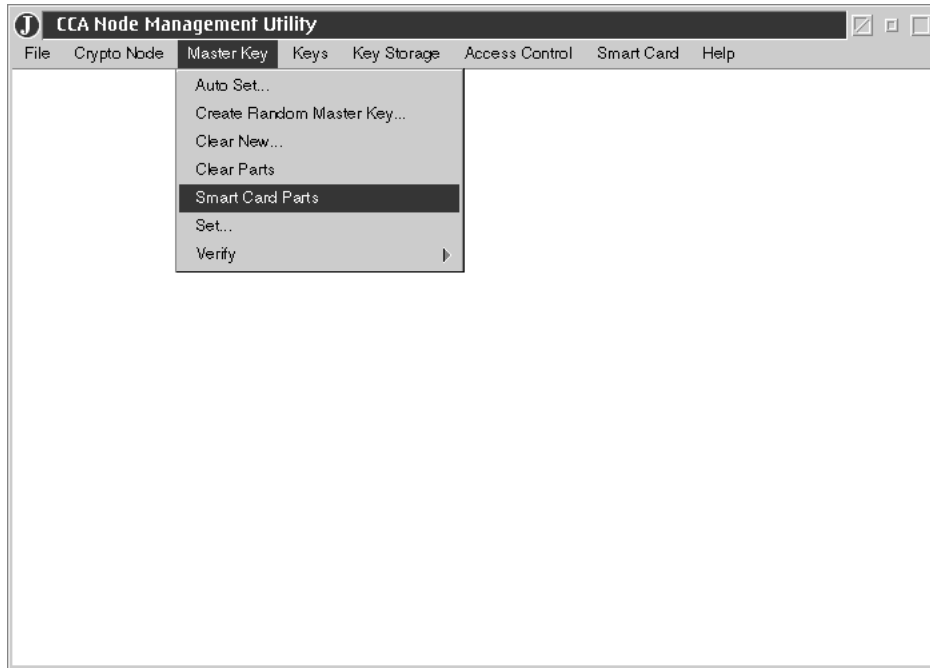


Figure 216. CNM main window — Master Key pull-down menu

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:

- **Current Master Key Register.** The active master key is stored in the current master key register.
- **Old Master Key Register.** The previous master key is stored in the old master key register.
- **New Master Key Register.** The new master key register is an interim location used to combine master key parts to form a new master key

## 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 as follows:

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 217. Clear New Master Key Register — confirm clearing

2. An information box informs you that the new master key register is cleared. Select OK to finish.



Figure 218. Clear New Master Key Register — register cleared

## Loading a new master key from clear key parts

To load new master key parts 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 load the new master key. The first and last key parts are required. Middle key parts are optional; you can load multiple middle key parts.

1. From the Master Key pull-down menu, select Clear Parts; the Load Master Key panel is displayed.

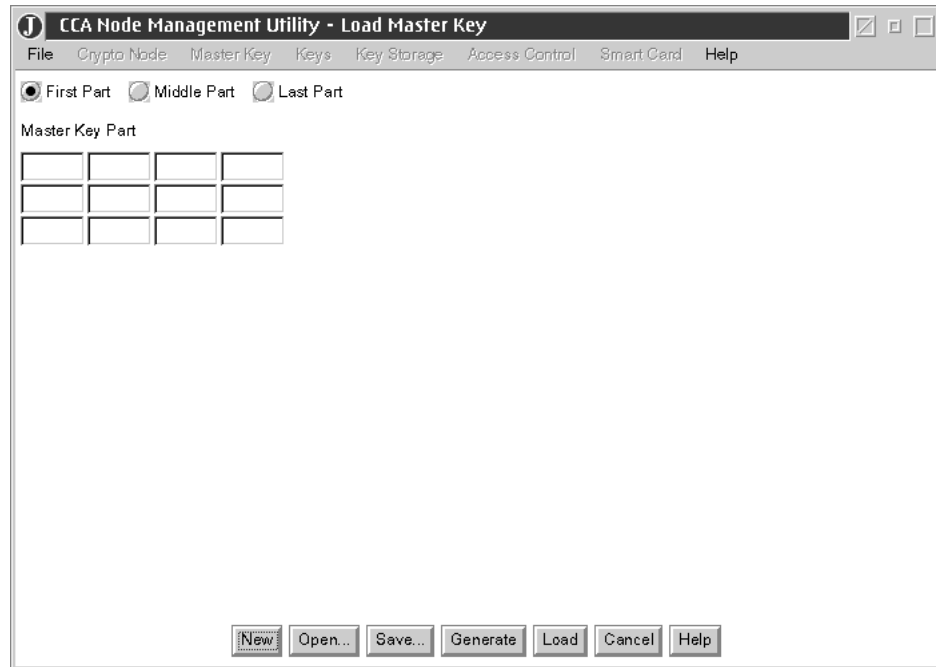


Figure 219. Load Master Key from Clear Parts

2. Select the radio button corresponding to the key part you are loading (First Part, Middle Part or Last Part).
3. Enter the clear key part by doing one of the following:
  - Select **New** to clear data entered in error.
  - Select **Open...** to retrieve key parts saved to disk.
  - Select **Generate** to have the TKE crypto adapter randomly generate a key part.
  - Manually enter a key value into the "Master Key Part" fields. Each field accepts four hexadecimal digits.

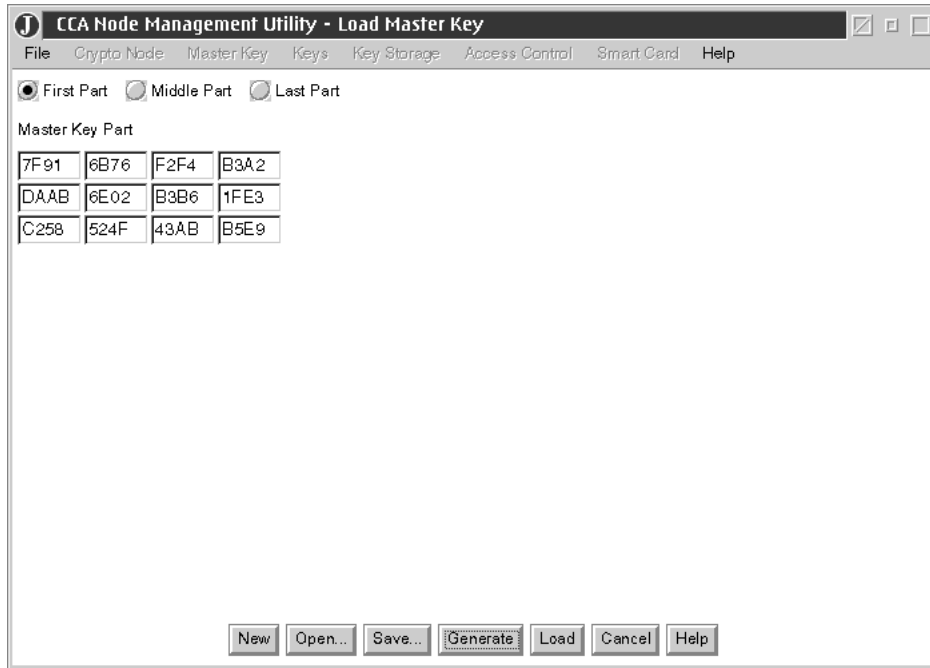


Figure 220. Load Master Key from Clear Parts — key part randomly generated

4. Select **Load** to load the key part into the new master key register, and select **Save...** to save the key part to disk.

**Warnings:**

- a. 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 “TKE Media Manager” on page 313.
- b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.



Figure 221. Load Master Key from Clear Parts — key part successfully loaded

**Note:** Key parts saved to disk are not enciphered.

5. Repeat the preceding steps to load the remaining key parts into the new master key register.
6. From the **Master Key** pull-down menu, select **Set...** This will do the following:
  - a. Transfer the key in the current master key register to the old master key register and delete the former old master key.
  - b. Transfer the key in the new master key register to the current master key register.

After setting a new master key, reencrypt the keys currently in key storage. (Refer to “Reencrypting key storage” on page 241.)

We recommend a dual control security policy. With a dual control security policy, 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 as follows:

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.

**Note:** 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 245 or SCUP “Display smart card information” on page 255. To determine the zone of a TKE cryptographic adapter, use SCUP “View current zone” on page 274. To use SCUP, you must first exit from CNM.

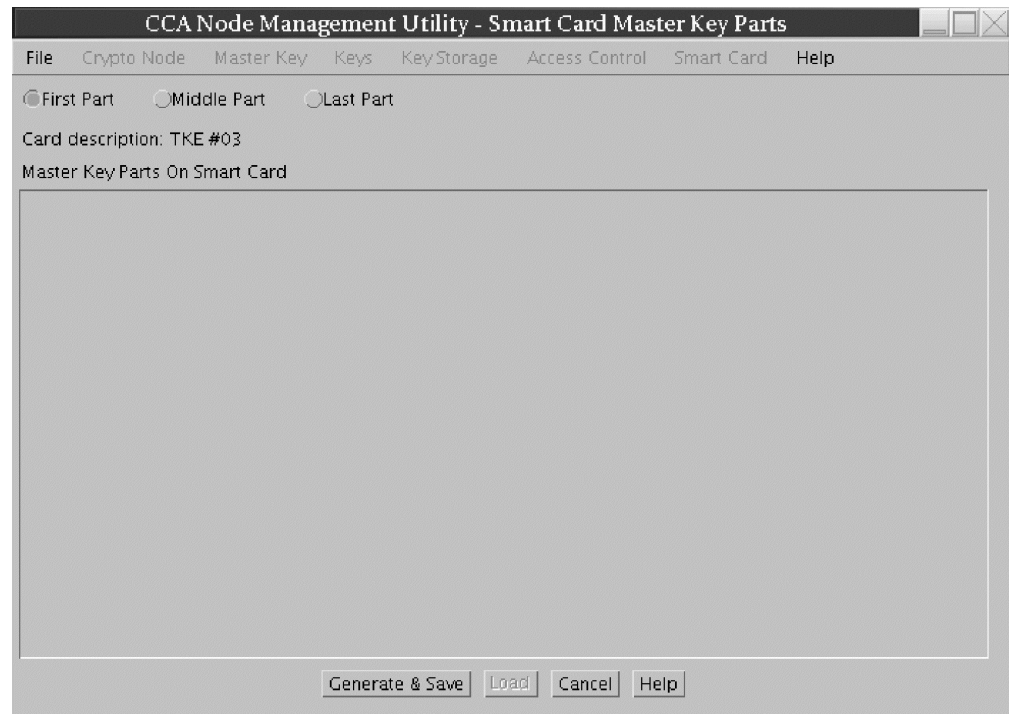


Figure 222. Smart Card Master Key Parts panel

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.

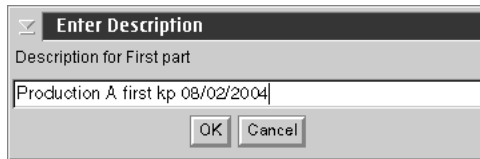


Figure 223. Smart Card Master Key Parts panel — key part description prompt

4. You will be prompted for the PIN of the TKE smart card inserted in Smart Card Reader 2.

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.

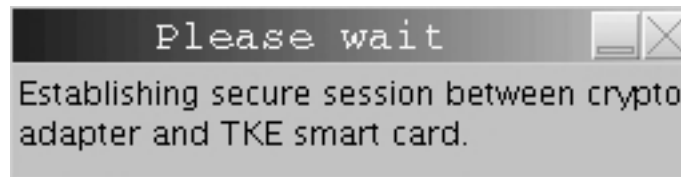


Figure 224. Establishing a secure session between TKE crypto adapter and TKE smart card

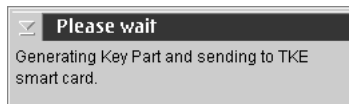


Figure 225. Generating key part to TKE smart card

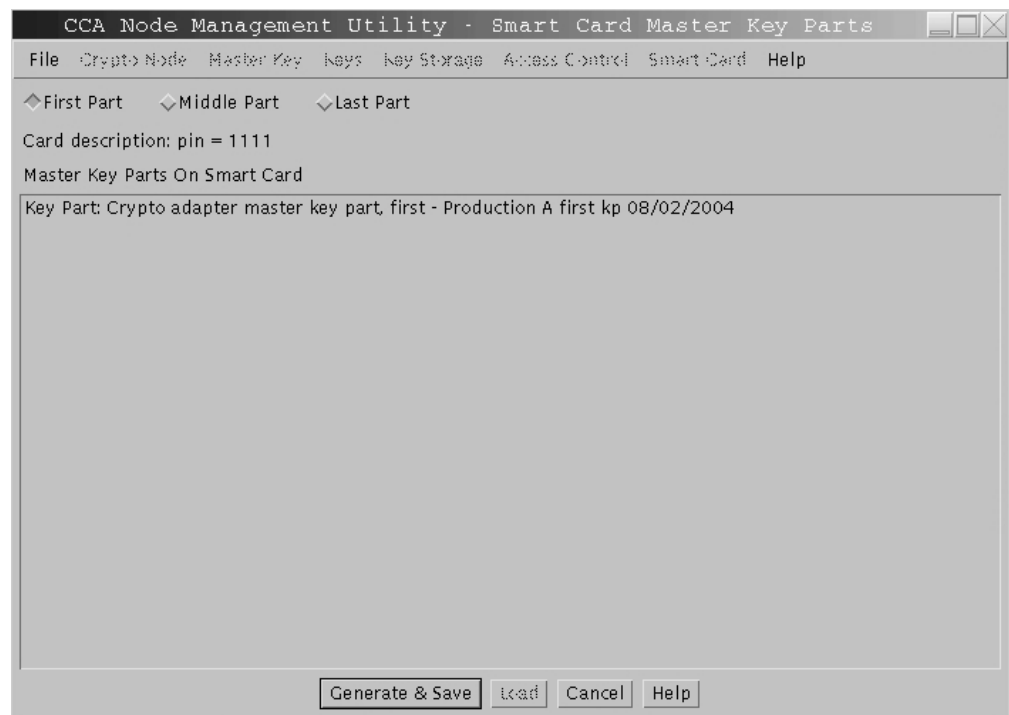


Figure 226. Smart Card Master Key Parts panel — key part generated to TKE smart card

**Note:** The key parts in the list are prefixed as follows:

- Key Part: Crypto Adapter master key part, first - <optional description follows>
- Key Part: Crypto Adapter master key part, middle - <optional description follows>
- Key Part: Crypto Adapter master key part, last - <optional description follows>

A First and Last key part is required. Middle key parts are optional. We recommend a dual control security policy. With a dual control security policy, the first and last key parts are generated to different 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 as follows:

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.

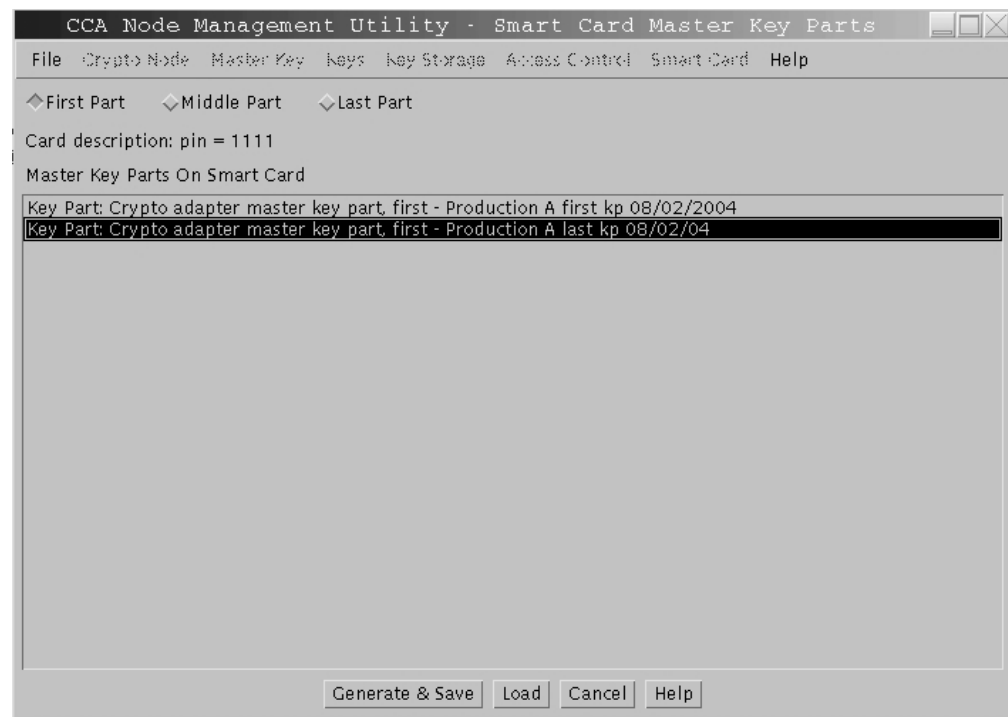


Figure 227. Master Key Part Smart Card panel — loading a Crypto Adapter key part from TKE smart card



3. A secure session is established between the Crypto Adapter and the TKE smart card. A pop-up message will display, indicating that the key part was successfully loaded.

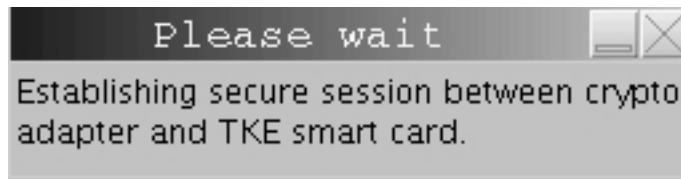


Figure 228. Establishing a secure session between Crypto Adapter and TKE smart card

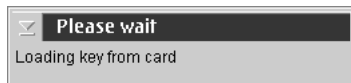


Figure 229. Loading key part from TKE smart card



Figure 230. Master key part successfully loaded

4. Repeat steps 1 on page 237 through 3 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. Specifically, a first key part must be loaded first (Key Part: Crypto Adapter master key part, first) and the last key part (Key Part: Crypto Adapter master key part, last) must be loaded last.

5. From the **Master Key** pull-down menu, select **Set...** This will do the following:
  - Transfer the key in the current master key register to the old master key register and delete the former old master key.
  - Transfer the key in the new master key register to the current master key register.
6. After setting a new master key, reencipher the keys currently in key storage. See “Reenciphering key storage” on page 241.

## 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, do the following:

1. From the **Master Key** pull-down menu, select **Verify**. A sub-menu is displayed.

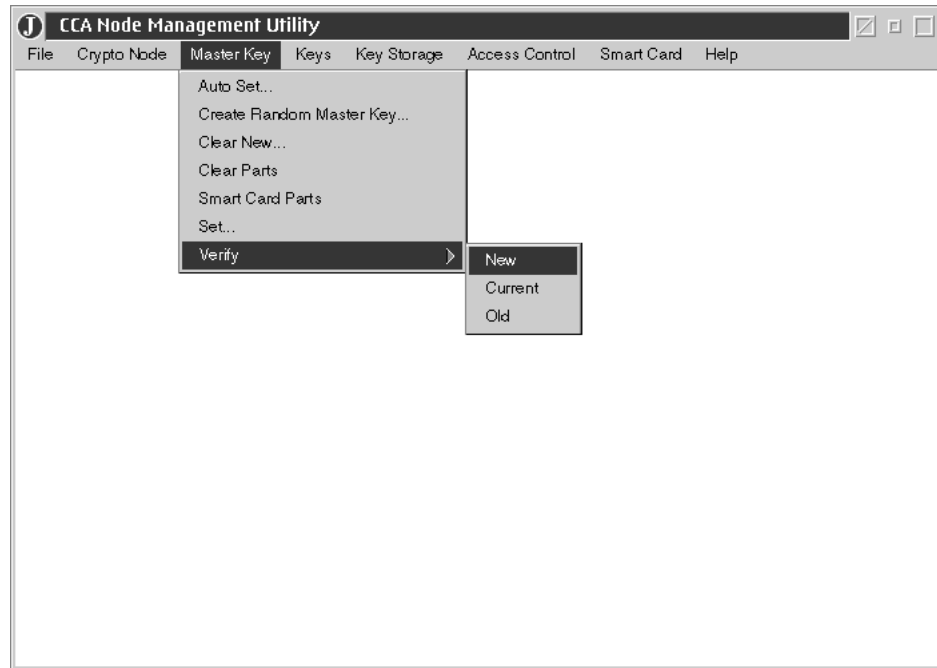


Figure 231. Master Key Verify sub-menu

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.

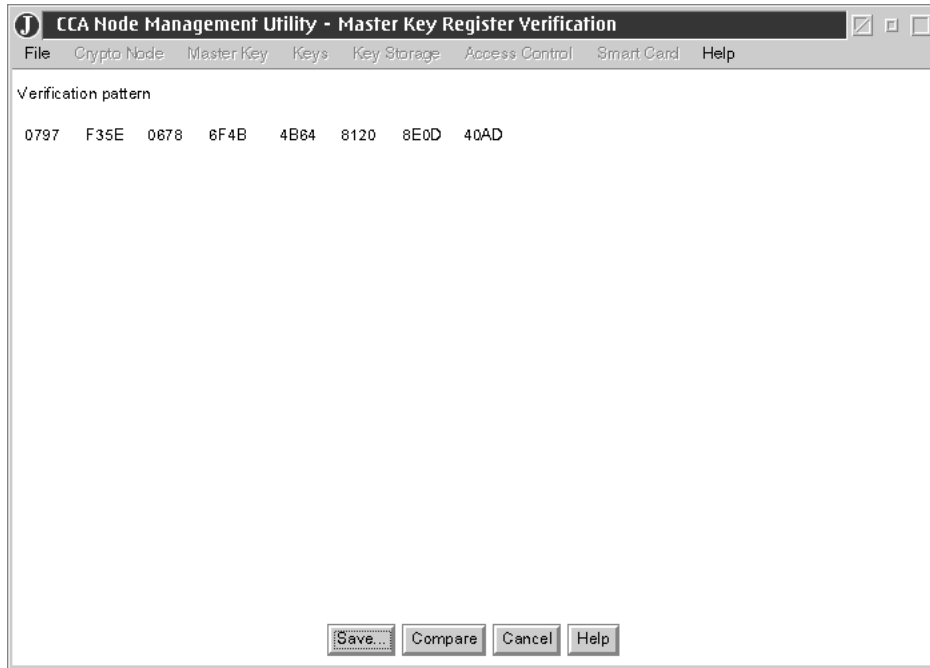


Figure 232. Master Key Register Verification panel - verification pattern is displayed

4. Select **Save** to Save the VP to a file. A file chooser will be displayed for the user to specify both a file name, and where to save the file (CD/DVD drive, USB flash memory drive, or CNM Data Directory).

**Warnings:**

- a. 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 “TKE Media Manager” on page 313.
  - b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.
5. Select **Compare** to compare the VP to a VP previously saved to disk. A file chooser will be displayed for the user to specify the location and filename of the saved VP.



Figure 233. Master Key Register VP compare successful

## Key Storage Menu

The Key Storage pull-down menu of the CNM main window contains menu items to manage or initialize DES key storage or RKA key storage.



Figure 234. CNM main window — Key Storage pull-down menu

## Reenciphering key storage

Key storage is a repository of keys that you access by key label. DES keys 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, thereby becoming the current master key, the keys must be reenciphered to the current master key.

To reencipher the keys in storage, do the following:

1. From the **Key Storage** pull-down menu, select **DES Key Storage** or **PKA Key Storage**. A sub-menu is displayed.
2. 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.

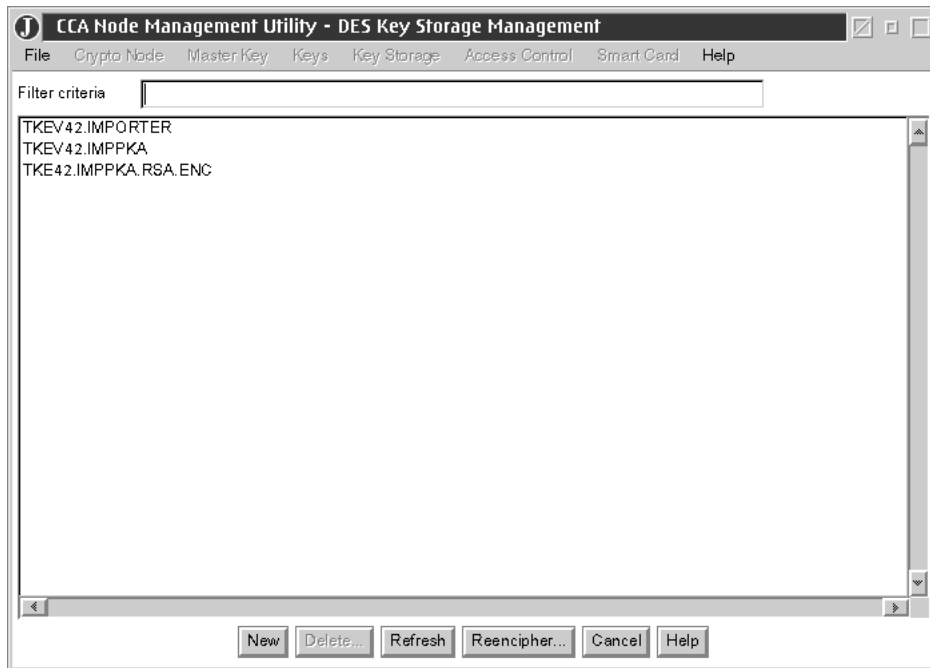


Figure 235. Key Storage Management Panel – key labels list

3. Select **Reencipher...**; the keys are reenciphered using the key in the current master key register.

## Smart card Menu

The Smart Card pull-down menu of the CNM main window contains the following menu items.

- Change PIN
- Generate Crypto Adapter Logon Key
- Display Smart Card Details
- Manage Smart Card contents
- Copy Smart Card



Figure 236. CNM main menu — Smart Card pull-down 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.

To change the PIN, perform the following steps:

1. From the **Smart Card** pull-down menu, select **Change PIN**. An informational window will prompt you to insert your TKE smart card into Smart Card Reader
2. Insert your TKE smart card and press **OK** to continue.



Figure 237. 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 238. 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 239. 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.

To generate a Crypto Adapter logon key, do the following:

1. From the Smart Card pull-down menu, select Generate Crypto Adapter Logon Key. You will be prompted for a TKE smart card. Insert the TKE smart card into smart card reader 2.

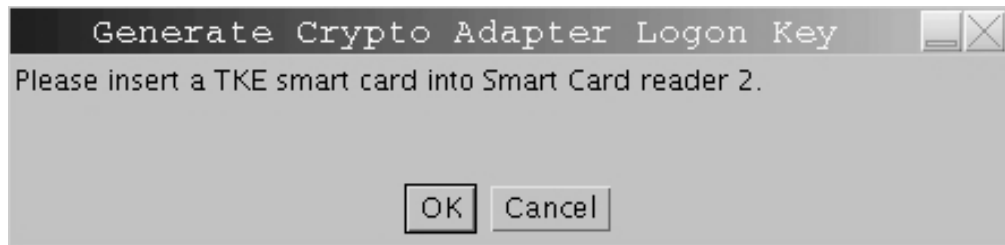


Figure 240. Generate Crypto Adapter Logon Key — insert TKE smart card

2. You will be prompted for a PIN. Enter the PIN on the smart card reader 2 PIN pad.

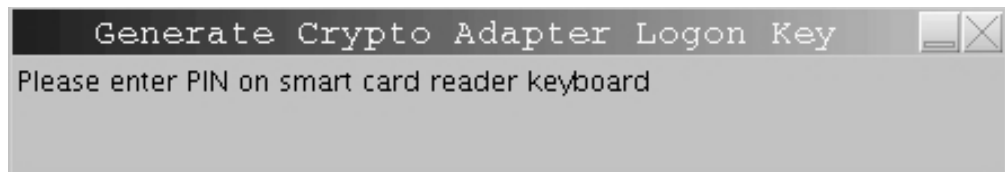


Figure 241. Generate Crypto Adapter Logon Key — PIN prompt

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 242. Generate Crypto Adapter Logon Key — User ID prompt

4. The Crypto Adapter logon key is generated.



Figure 243. Generate Crypto Adapter Logon Key — key generated

## Display smart card details

Use this function to display public information about a TKE smart card.

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.

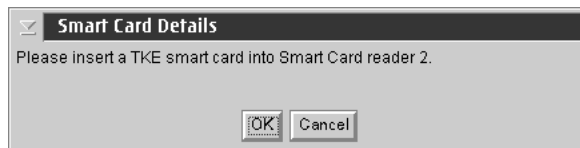


Figure 244. Display Smart Card Details — insert TKE smart card prompt

The TKE smart card is read and the public information is displayed.



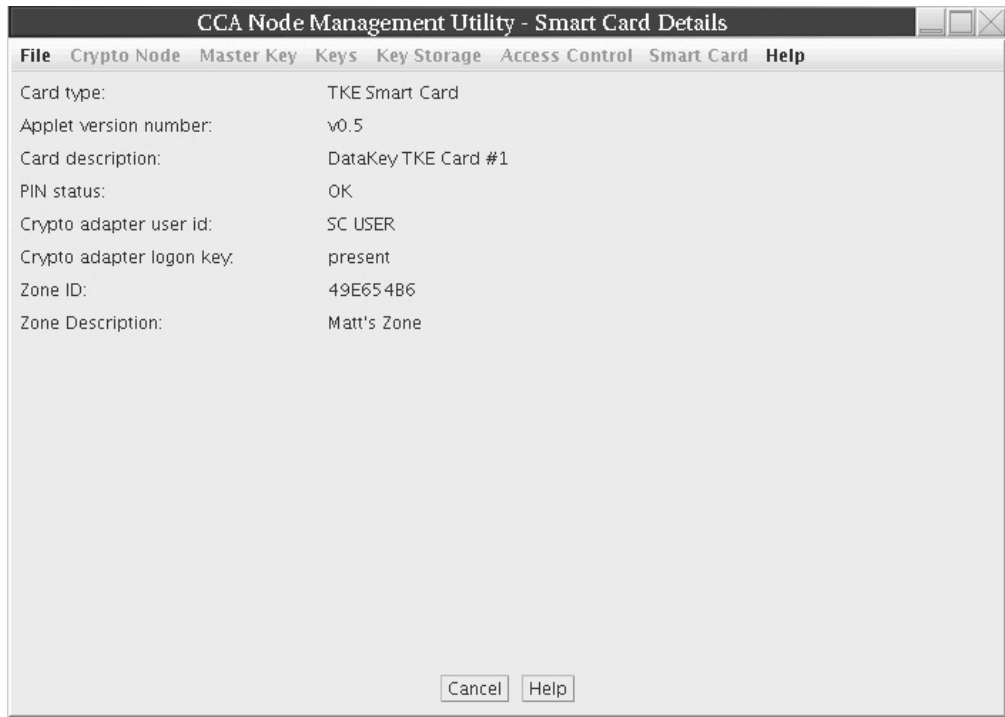


Figure 245. Display Smart Card Details — public information displayed

The following 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. The smart card description was entered when the smart card was personalized

**PIN status**

The PIN status can be OK/blocked/not set. The PIN is set when TKE smart card is personalized

**Crypto Adapter User ID**

User ID entered when a Crypto Adapter logon key is generated. The User ID may be blank if the TKE smart card does not have a Crypto Adapter logon key

**Crypto Adapter Logon Key**

Status can be present/not present

**Zone ID**

Set when the 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 log on to the TKE crypto adapter to use the

Manage Smart Card Contents function. To display the smart card contents using the Manage Smart Card Contents function, do the following:

1. From the **Smart Card** pull-down menu, select **Manage Smart Card contents**. You will be prompted for a TKE smart card. Insert the source TKE smart card into Smart Card Reader 2.

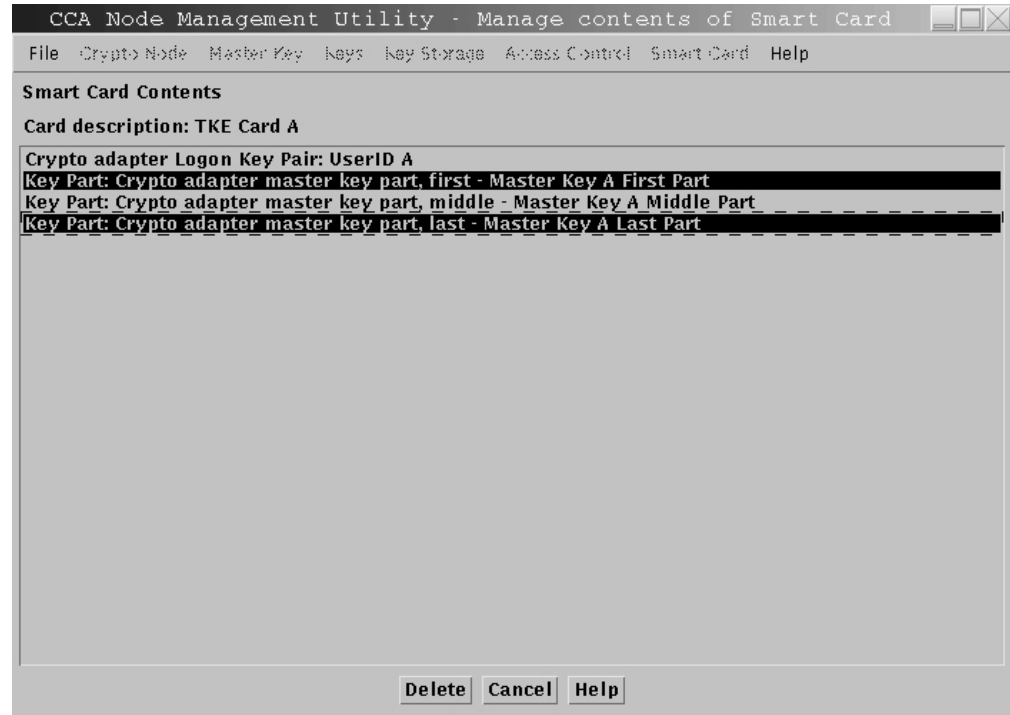


Figure 246. Manage Smart Card contents — contents of TKE smart card are displayed

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.

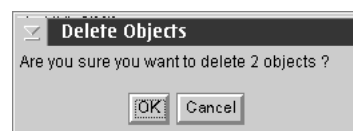


Figure 247. Manage Smart Card contents — confirm delete prompt

5. The objects are deleted and the list is refreshed.

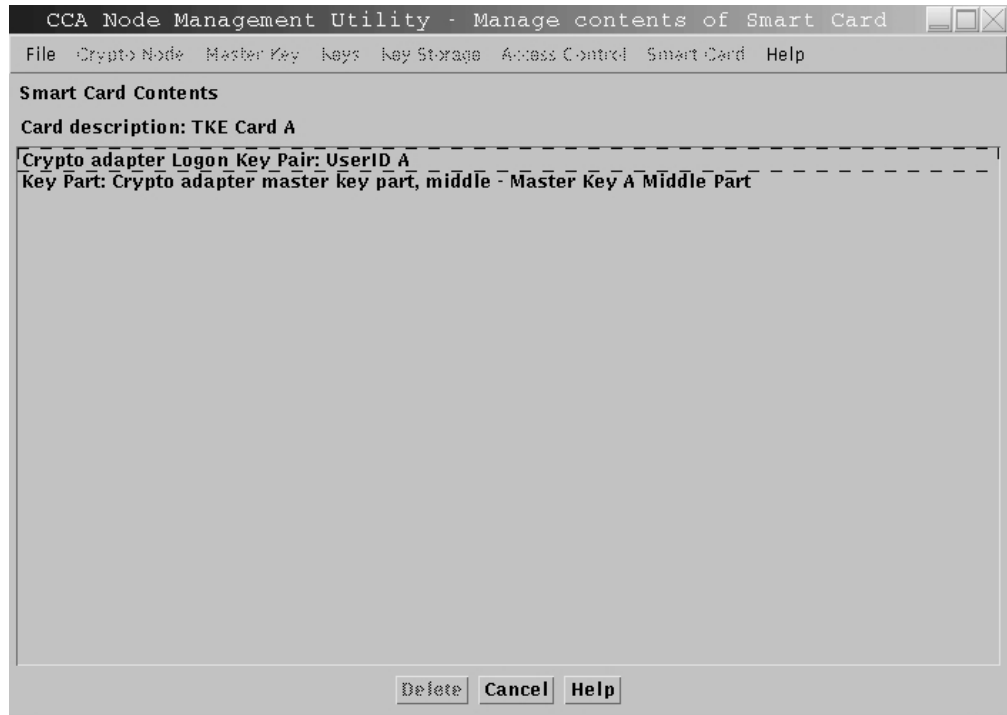


Figure 248. Manage Smart Card contents

**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 authority signature key, you will not be able to sign a TKE command until the administrator generates a new authority signature key and uploads it to the host.

## Copy Smart Card

Use this function to copy a key or key part(s) from one TKE smart card to another. The two TKE smart cards must belong to the same zone. Specifically, 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.

### Notes:

1. AES key parts cannot be copied to a TKE smart card that does not have the TKE applet version 0.4 or later. ECC key parts cannot be copied to a TKE smart card that does not have the TKE applet version 0.6 or later.
2. 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 246) or use a different TKE smart card.
3. TKE Version 6.0 was the final release that supported DataKey smart cards. Copying a DataKey smart card is the only action still supported. You can only copy data from a DataKey smart card. You cannot copy to a DataKey smart card.

To copy smart card contents, do the following:

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 249. 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 out.



Figure 250. Copy Smart Card — insert target TKE smart card

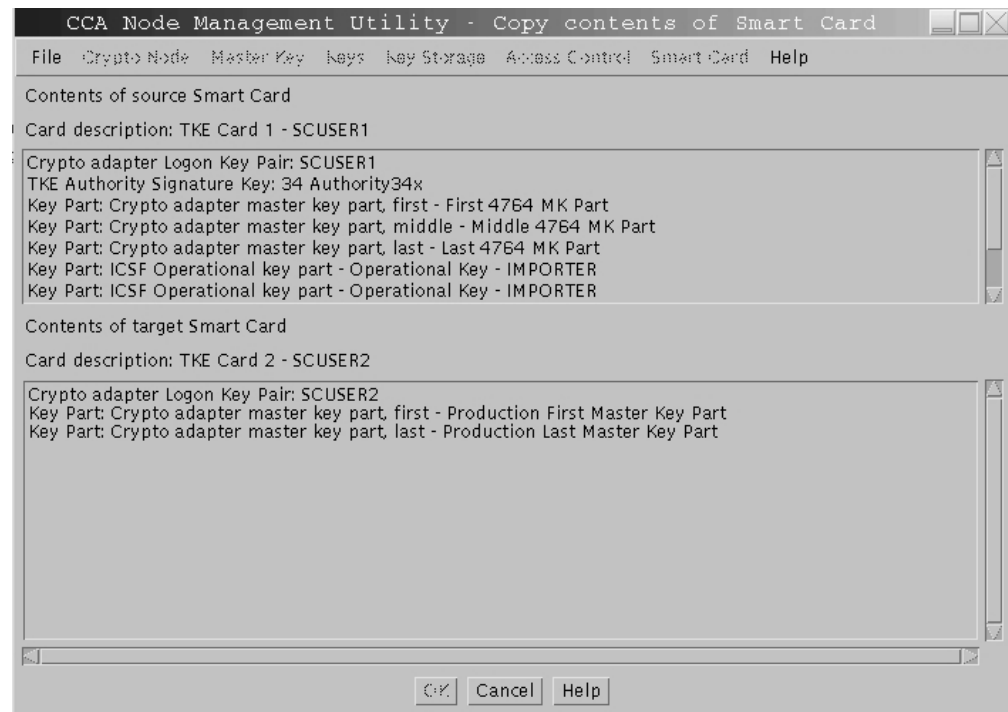


Figure 251. Copy Smart Card — TKE smart card key parts are displayed

3. Highlight the objects in the source container to copy to the target container. Press **OK** to continue.

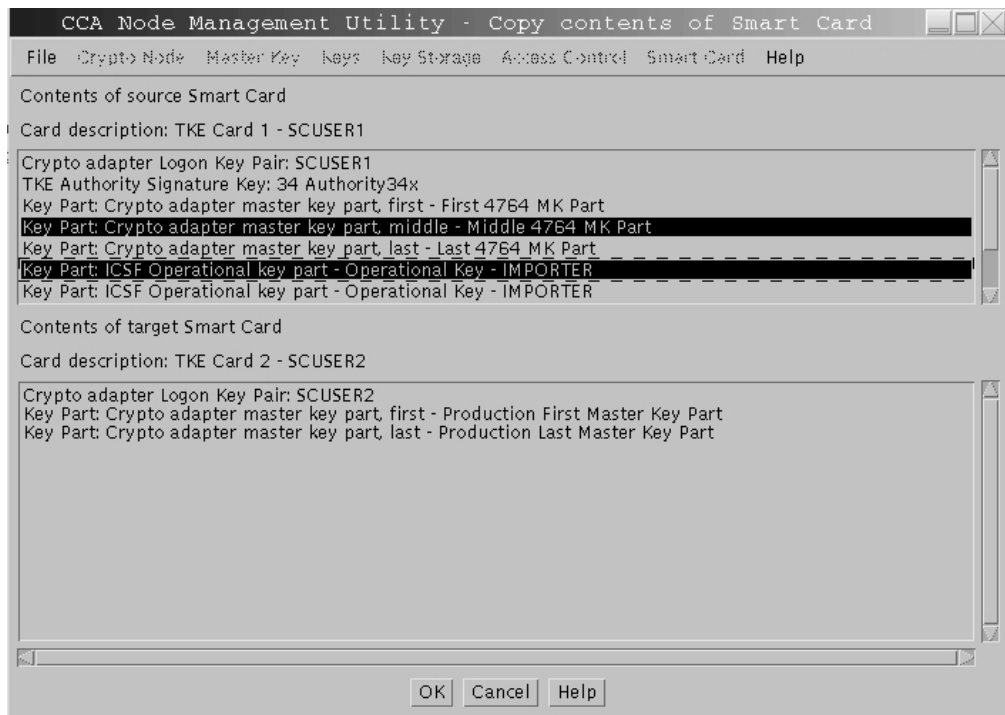


Figure 252. Copy Smart Card — highlight source objects to copy to target

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.

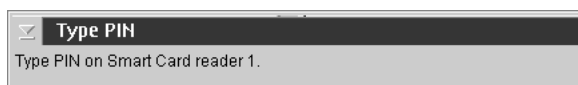


Figure 253. Copy Smart Card — source TKE smart card PIN prompt

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.

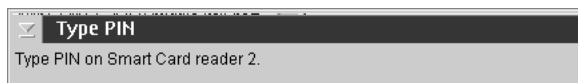


Figure 254. Copy Smart Card — target TKE smart card PIN prompt



Figure 255. Establishing a secure session between source and target TKE smart cards

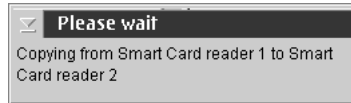


Figure 256. Objects are copied to the target TKE smart card

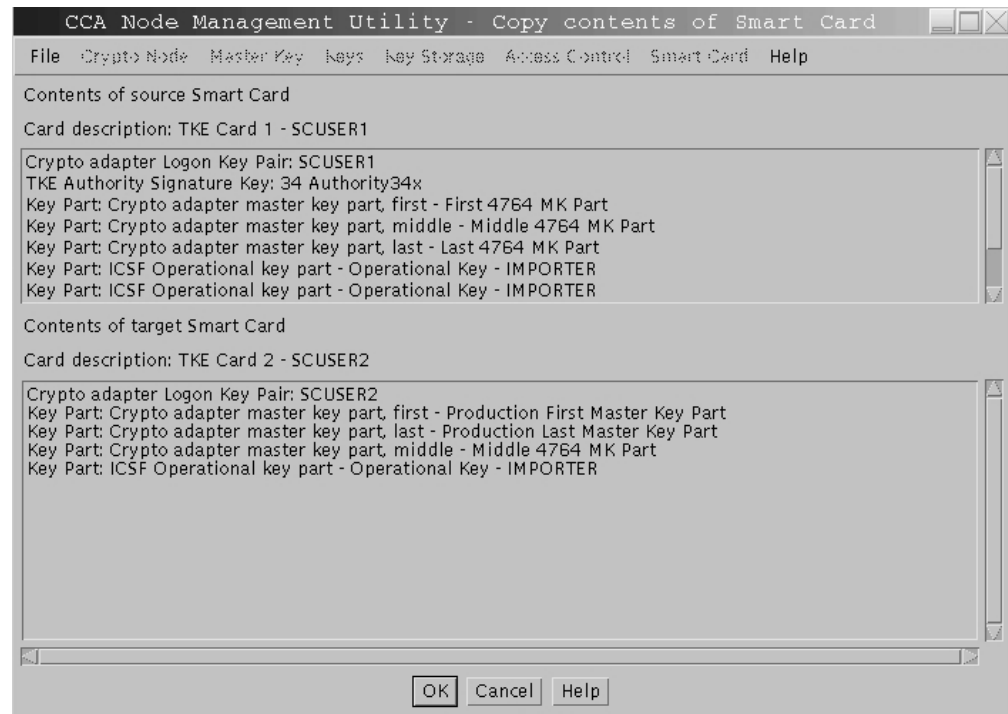


Figure 257. Copy Smart Card — objects are copied to the target container

A TKE smart card can hold a maximum of 10 key parts, in addition to a crypto 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. Log off the crypto module and log on using a profile associated with a role that allows this function.

**Message:** “Your user profile has expired”

**Return Code:** 8

**Reason Code:** 92

**Explanation:** The TKE administrator must reset the expiration date on the user profile.

**Message:** "Your authentication data (for example, passphrase) has expired."

**Return Code:** 8

**Reason Code:** 94

**Explanation:** The TKE administrator must change the passphrase and reset the passphrase expiration date on the user profile. Then, select **Replace** to load the profile into the workstation coprocessor.

**Message:** "The user profile does not exist"

**Return Code:** 8

**Reason Code:** 773

**Explanation:** Make sure you typed in the user ID correctly. The user ID is case sensitive.

**Message:** "The group logon failed because authentication of one or more group members failed."

**Return Code:** 8

**Reason Code:** 2084

**Explanation:** One or more user profiles in the group failed authentication (for example, passphrase expired or profile expired) causing the group logon to fail. The group logon window will indicate which user failed and the reason for the logon failure. Correct the user profile or attempt group logon again and select a different member in the group members list for logon.

**Message:** "The profile is included in one or more groups"

**Return Code:** 8

**Reason Code:** 2085

**Explanation:** You attempted to delete a user profile that is currently a member of a group profile. You must remove the user profile from the group member list before deleting the profile.

**Message:** "The group role does not exist."

**Return Code:** 8

**Reason Code:** 2086

**Explanation:** You attempted group logon using a group profile that is associated with a role that does not exist. The TKE administrator must define the role and load it to the TKE crypto adapter before the group profile may be used.

**Message:** "Your group profile has not yet reached its activation date"

**Return Code :** 8

**Reason Code:** 2087

**Explanation:** The group profile has an activation date that is later than the current date. The TKE administrator must change the activation date before the group profile may be used or wait until the activation date arrives.

**Message:** "Your group profile has expired."

**Return Code:** 8

**Reason Code:** 2088

**Explanation:** The group profile has surpassed its expiration date. The TKE administrator must change the expiration date before the group profile may be used.

---

## Chapter 11. Smart Card Utility Program (SCUP)

The TKE Smart Card Utility Program (SCUP) supports the smart card system with the following functions:

- “Display smart card information” on page 255
- “Display smart card key identifiers” on page 256
- “Initialize and personalize the CA smart card” on page 258
- “Backup a CA smart card” on page 261
- “Change PIN of a CA smart card” on page 262
- “Initialize and enroll a TKE smart card” on page 263
- “Personalize a TKE smart card” on page 264
- “Change PIN of a TKE smart card” on page 265
- “Unblock PIN on a TKE smart card” on page 265
- “Enroll a TKE cryptographic adapter” on page 265
- “View current zone” on page 274

---

### General Information

When entering PINs, the PIN prompt appears on both the TKE workstation screen as well as on the smart card reader. When certain tasks will take over one minute for SCUP to execute, information messages are returned. Be patient so that you do not have to restart the task.

The utility is capable of overwriting your smart cards. You will be prompted to reply **OK** before the card is overwritten.

To start SCUP, click on **Trusted Key Entry** in the main workstation screen. This will display various workstation functions.

**Note:** You can use the Smart Card Utility Program if you are logged on at the console as ADMIN or TKEUSER. In addition, you must be logged onto the crypto adapter with a profile defined when you configured the TKE workstation from CNM. You are prompted to logon to the crypto adapter if you are not currently logged on.

Click on **Applications**. Under Applications, click on **Smart Card Utility Program 7.0**. The Smart Card Utility Program screen appears.



**TKE Smart Card Utility Program Version 7.0**

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:	Zone key length:
TKE Authority key:	
Crypto Adapter Logon key:	

**Key parts:**

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	AES-VP	Control vector	Length

**Smart card reader 2**

Card type:	Zone enroll status:
Card ID:	Zone ID:
Card description:	Zone description:
PIN status:	Zone key length:
TKE Authority key:	
Crypto Adapter Logon key:	

**Key parts:**

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	AES-VP	Control vector	Length

Main Menu

Figure 258. 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” on page 255.
- “Display smart card key identifiers” on page 256
- Exit
- Exit and logoff

Tasks associated with the drop down menu for **CA Smart Card** are:

- “Initialize and personalize the CA smart card” on page 258.
- “Backup a CA smart card” on page 261.
- “Change PIN of a CA smart card” on page 262.

Tasks associated with the drop down menu for **TKE Smart Card** are:

- “Initialize and enroll a TKE smart card” on page 263.
- “Personalize a TKE smart card” on page 264.
- “Unblock PIN on a TKE smart card” on page 265.
- “Change PIN of a TKE smart card” on page 265..

Tasks associated with the drop down menu for **Crypto Adapter** are:

- “Enroll a TKE cryptographic adapter” on page 265.
- “View current zone” on page 274.

## File Menu Functions

### Display smart card information

After you have created a smart card, you are advised to check the results. If you are copying keys from one TKE smart card to another, you may also want to verify that all of the keys were correctly copied to the other TKE smart card.

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.

The screenshot shows the 'TKE Smart Card Utility Program Version 7.0' window. It has a menu bar with 'File', 'CA Smart Card', 'TKE Smart Card', 'Crypto Adapter', and 'Help'. The main area is divided into two sections for 'Smart card reader 1' and 'Smart card reader 2'. Each section displays card details and a table of key parts.

**Smart card reader 1**

Card type:	TKE Smart Card v0.5	Zone enroll status:	Enrolled
Card ID:	6CE499E7S	Zone ID:	4B2803A6
Card description:		Zone description:	v0.4CA zone
PIN status:	OK	Zone key length:	1024
TKE Authority key:	Not present		
Crypto Adapter Logon key:	Not present		

Key parts:

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	AES-VP	Control vector	Length

**Smart card reader 2**

Card type:	CA Smart Card v0.4	Zone enroll status:	Enrolled
Card ID:	5A49C8CFS	Zone ID:	4B2803A6
Card description:	v0.4 CA card	Zone description:	v0.4CA zone
PIN status:	OK	Zone key length:	1024
TKE Authority key:			
Crypto Adapter Logon key:			

Key parts:

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	AES-VP	Control vector	Length

Main Menu

Figure 259. Display of CA smart card and TKE smart card

The panel provides the following 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.
- **Zone key length:** The length of the zone certificate public modulus in bits.
- **Key type:** operational key parts, TKE crypto adapter master key parts, or ICSF master key parts
- **Description:** description of key part (optional)
- **Origin:** Crypto Adapter or PIN-PAD
- **MDC-4:** MDC-4 hash value of the key part
- **SHA-1:** SHA-1 hash value of the key part
- **ENC-ZERO:** ENC-ZERO hash value of the key part
- **AES-VP:** AES verification pattern of the key part
- **Control vector:** CCA control vector of operational key parts or blank for master key parts
- **Length:** 8, 16, 24 or 32 bytes

## Display smart card key identifiers

This function displays the key identifiers and key lengths for the TKE Authority Key and Crypto Adapter Logon Key on a TKE smart card. Some information from the Display smart card information panel is repeated to provide context.

1. Insert smart card(s) to be displayed in smart card reader 1 or 2. From the *File* menu, select *Display smart card key identifiers* option.



Figure 260. Display of smart card key identifiers

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.
- **TKE Authority Key Identifier:** For TKE cards only, identifies the TKE authority key. The key identifier is the SHA-256 hash of the DER-encoded public modulus and public exponent of the RSA key pair.
- **TKE Authority key length:** The length of the RSA authority signature key, if present, in bits.
- **Crypto Adapter Logon Key:** For TKE smart cards only, the value can be Present or Not Present.
- **Crypto Adapter Logon Key Identifier:** For TKE cards only, identifies the crypto adapter logon key. The key identifier is the SHA-256 hash of the DER-encoded public modulus and public exponent of the RSA key pair.
- **Crypto Adapter Logon key length:** The length of the RSA key (in bits) on the smart card used to log on to the local crypto adapter.
- **Zone enroll status:** The Zone enroll status is the status of the card. It is either Enrolled or Not enrolled.
- **Zone ID:** When a CA 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.

- **Zone key length:** The length of the zone certificate public modulus in bits.

---

## CA Smart Card Menu Functions

### Initialize and personalize the CA smart card

A zone is created when a CA smart card is initialized and personalized.

**Note:** In general, a CA smart card initialized on TKE 7.0 cannot be used on a TKE workstation at a lower release. Refer to “Smart Card Compatibility Issues” on page 15 for more information on compatibility of smart cards across different releases.

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.

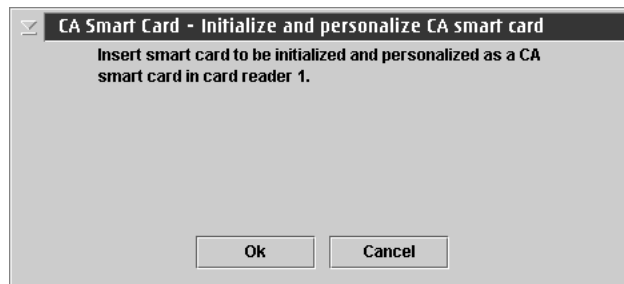


Figure 261. First step for initialization and personalization of the CA smart card

3. A dialog box displays, prompting you to select the zone key length. The zone key length can be either 1024 bit or 2048 bit.

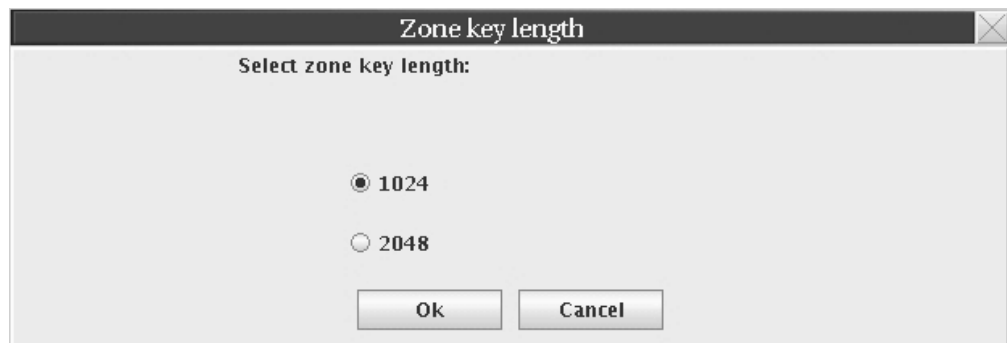


Figure 262. Zone key length window

4. If the smart card is not empty, a message is displayed indicating that the smart card is not empty and all data will be overwritten. If this is acceptable click **OK**.

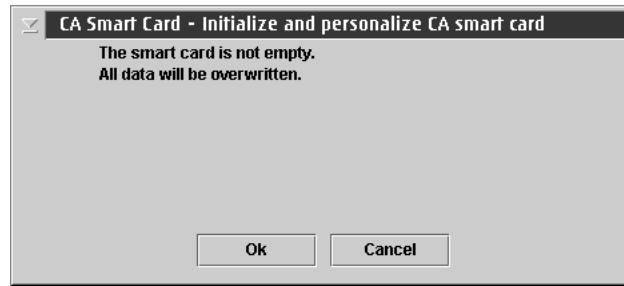


Figure 263. Message if card is not empty

5. The smart card will now be initialized.

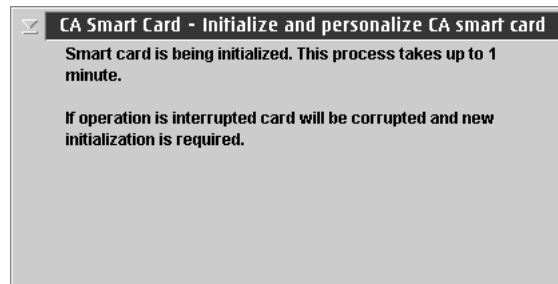


Figure 264. Initialization message for CA smart card

6. At the next prompt, enter a 6-digit PIN number twice. This is the first CA smart card PIN.

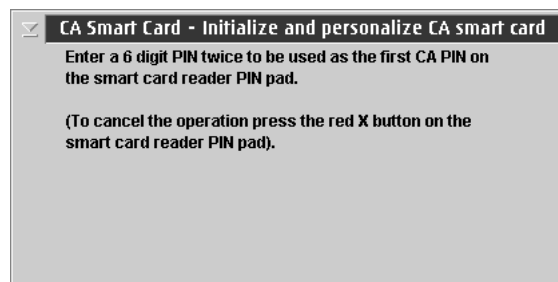


Figure 265. Enter first PIN for CA smart card

7. At the next prompt, enter a 6-digit PIN number twice. This is the second CA smart card PIN. For dual control it is recommended that different administrators enter the first and second CA smart card PIN and the PINs should not be the same.

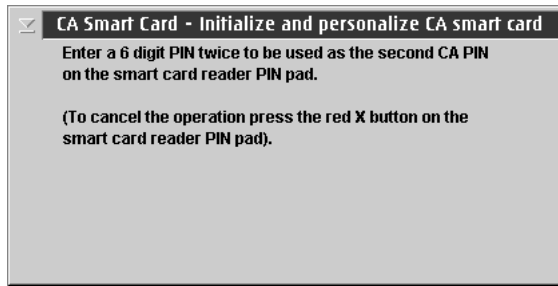


Figure 266. Enter second PIN twice for CA smart card

8. A dialog displays, prompting you to enter a zone description. Although a zone description is optional, it is recommended that you specify one.

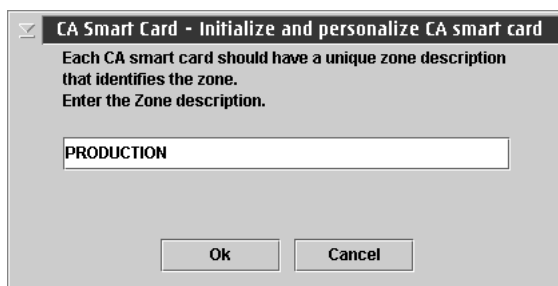


Figure 267. Enter zone description for CA smart card

9. A dialog displays, prompting you to enter a CA smart card description. Although a smart card description is optional, it is recommended that you specify one. After the description is entered the CA Smart Card will be built.

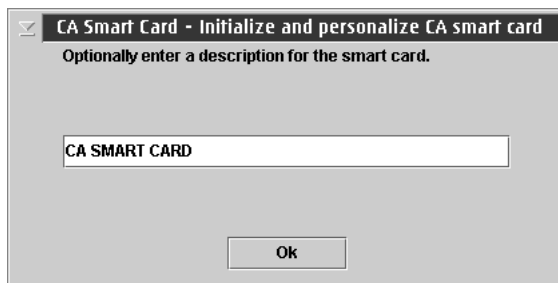


Figure 268. Enter card description for CA smart card

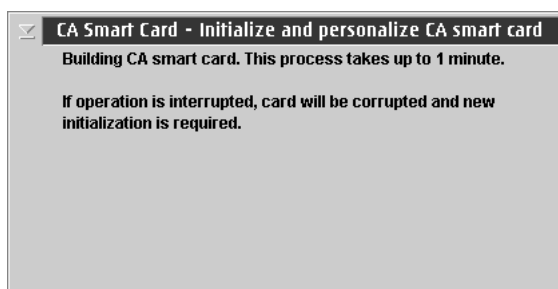


Figure 269. Building a CA smart card

10. 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.

**Note:** Although DataKey smart cards are no longer supported in TKE 7.0 and later, you can still back up DataKey smart card information to an NXP smart card.

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.

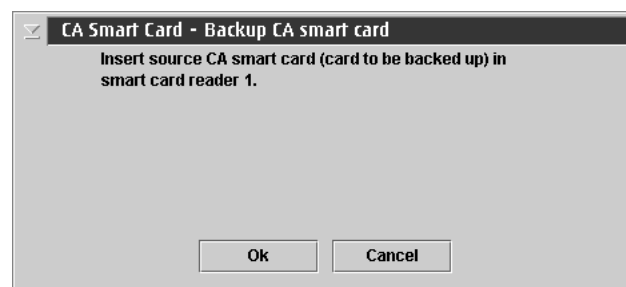


Figure 270. Begin creation of backup CA smart card

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.

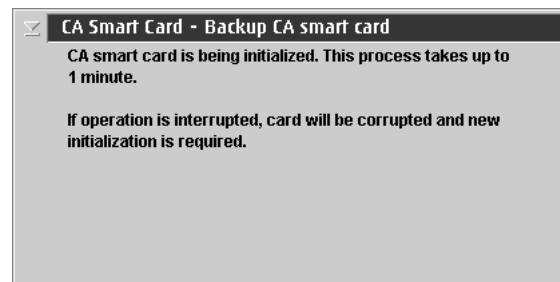


Figure 271. Initialization of backup CA smart card



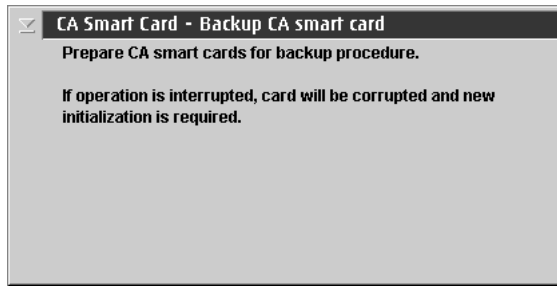


Figure 272. Continue creation of backup CA smart card

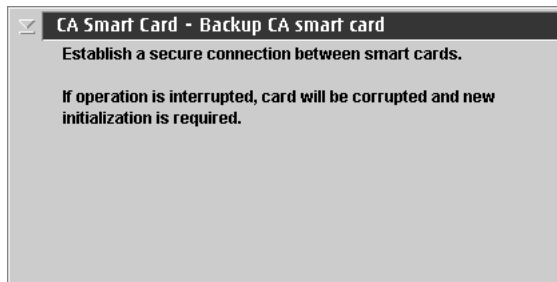


Figure 273. Establish secure connection for backup CA smart card

8. At the prompts, enter the first and second CA PINs of the original CA smart card on the smart card reader 2.

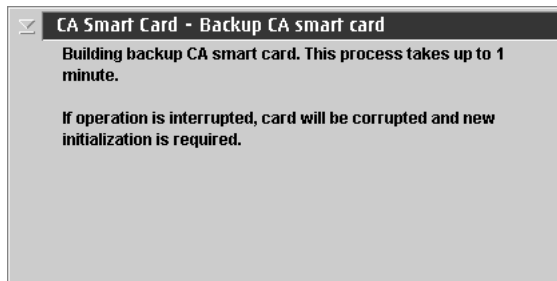


Figure 274. Building backup CA smart card

9. You will get a message that a CA Smart Card was successfully copied.

## 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. A dialog displays, prompting you to select either first CA PIN or second CA PIN.

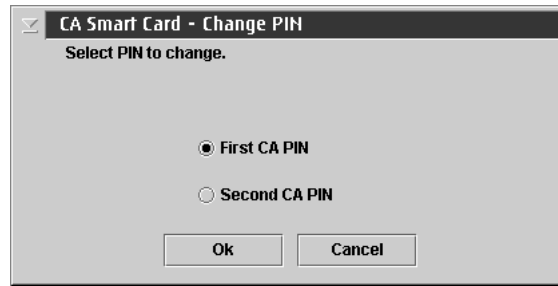


Figure 275. Select first CA PIN

4. Enter the current 6-digit PIN once.
5. Enter the new PIN twice — when prompted.
6. You will get a message that the PIN was successfully changed.

---

## TKE Smart Card Menu Functions

The purpose of a TKE smart card is to hold key material. Before the TKE smart card can hold key material, however, it must be initialized and personalized. The TKE Smart Card menu contains options for initializing and personalizing a TKE smart card. Menu options are also available to unblock and change the smart card's PIN.

### Initialize and enroll a TKE smart card

In general, smart cards initialized with TKE 7.0 cannot be used on older versions of TKE. Refer to “Smart Card Compatibility Issues” on page 15 for more information.

**Note:** You must be logged onto the console as TKEUSER or ADMIN to 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 in smart card reader 2 a smart card to be initialized as a TKE smart card.

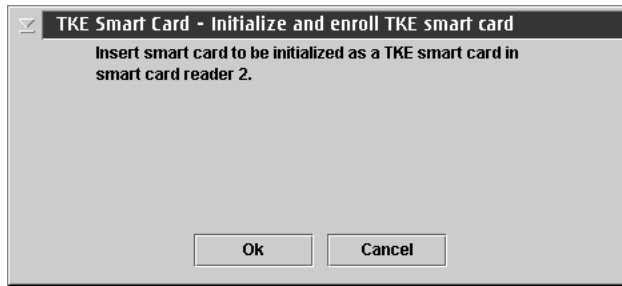


Figure 276. Initialize and enroll TKE smart card

6. If the card is not empty, you will be asked to overwrite all of the data on the smart card.
7. You will see screens indicating that the smart card is being initialized and then the TKE smart card is being built.

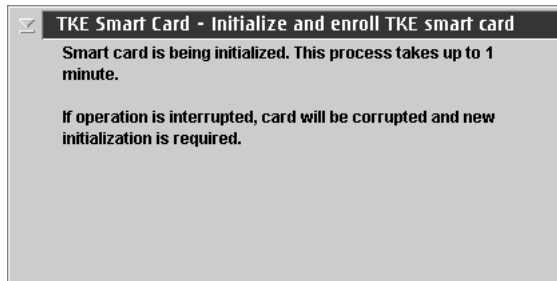


Figure 277. Initializing TKE smart card

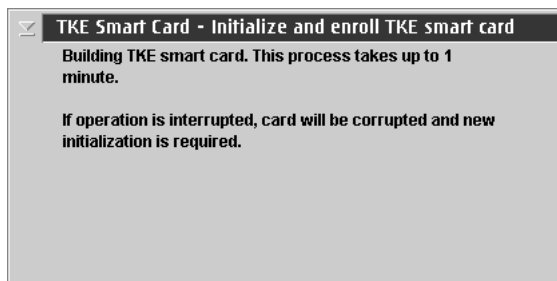


Figure 278. Building TKE smart card

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, select the *Personalize TKE smart card* option.
2. You will be prompted to insert an initialized TKE smart card in smart card reader 2.

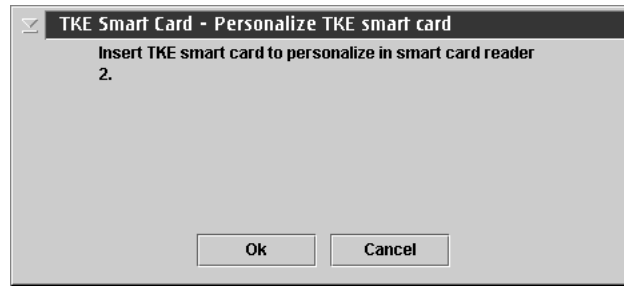


Figure 279. Personalizing TKE smart card

3. A window will open, prompting you to enter a 6-digit PIN twice on the PIN pad of smart card reader 2. Enter the 6-digit PIN when prompted.
4. At the prompt, enter a 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 a TKE smart card PIN is entered incorrectly 3 times, the card becomes blocked and will be unusable until it is unblocked. When you unblock the PIN, the PIN does not change. You still need to enter the correct PIN and will have 3 more attempts to enter the PIN correctly.

To unblock the PIN on a TKE smart card, follow these steps:

1. From the *TKE Smart Card* drop down menu, select *Unblock TKE smart card* option.
2. Insert the CA smart card in smart card reader 1 when prompted.
3. Enter the first CA PIN on the PIN pad of smart card reader 1.
4. Enter the second CA PIN on the PIN pad of smart card reader 1.
5. At the prompt, insert the TKE smart card to be unblocked in smart card reader 2.
6. You will get a message that the TKE smart card was successfully unblocked.

## Change PIN of a 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 PIN once. For TKE Version 7.0 or later, this is a 6-digit PIN. For versions of TKE prior to 7.0, this is a 4-digit PIN.
4. At the prompt, enter the new PIN twice.
5. You will get a message that the PIN was successfully changed.

---

## Crypto Adapter Menu Functions

### Enroll a TKE cryptographic adapter

A TKE workstation with a cryptographic adapter can be enrolled locally or remotely.

**Note:** Enrolling of the cryptographic adapter 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. If it is not, a message window will indicate that the IBM crypto adapter is not enrolled in a zone.



Figure 280. View current zone for a TKE cryptographic adapter

Local TKE workstations that have access to the CA Card may be enrolled locally. If you have offsite TKE workstations without access to the CA card, you may use the remote enroll application to enroll these workstations in the same zone.

If the enroll does not occur as part of the initialization, the current DEFAULT role will not have the necessary ACPs to perform the enroll. You can log on with a profile using SCTKEADM or equivalent authority, or you can reload the TEMPDEFAULT role (see “Open or edit a disk-stored role” on page 218). If the TEMPDEFAULT role is used, then, once the enroll is complete, it is critical that the TEMPDEFAULT role be returned to the normal DEFAULT role. The TEMPDEFAULT role cannot be allowed to stay loaded as this role has ACPs for all functions.

## Local Crypto Adapter Enrollment

1. From the Crypto Adapter drop down menu, select Enroll Crypto Adapter option.
2. Select *local* when prompted for enrollment type.



Figure 281. 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.

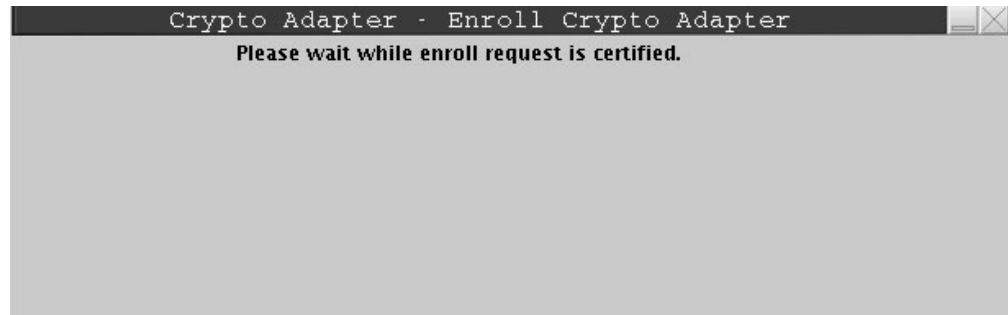


Figure 282. Certifying request for local Crypto Adapter enrollment



Figure 283. 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 284. View current zone after Crypto Adapter enrollment

## Remote/Secondary Crypto Adapter 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 the following message: "This program generates an enrollment request for the IBM Cryptographic card installed in this workstation Continue?? (Yes/no)"
4. Choose the zone key length request to be generated. If target zone has a CA zone key length of 1024 bits choose "Yes". If the target zone has a CA zone

key length of 2048 bits choose "No".

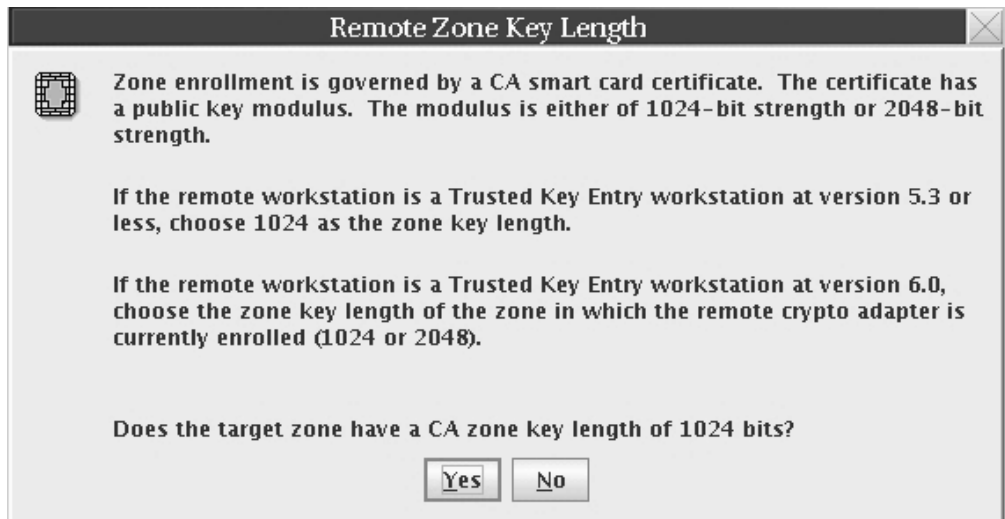


Figure 285. Remote Zone Key Length

If "No" was selected, a dialog displays, asking "Does the target zone have a CA zone key length of 2048 bits?"

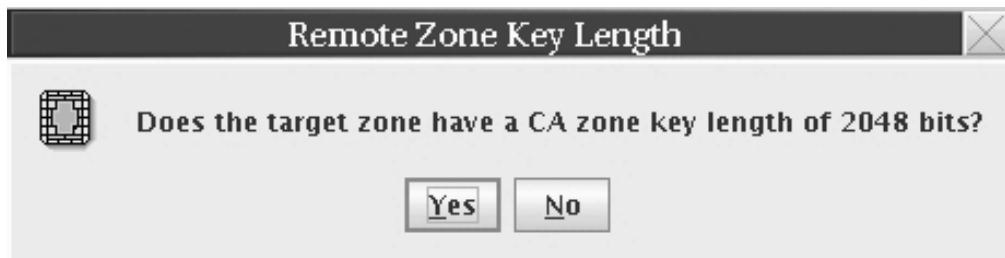


Figure 286. Remote Zone Key Length is 2048

Choose "Yes" to generate the 2048 bit request or "No" to end the Begin Remote Enroll application.

5. 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.

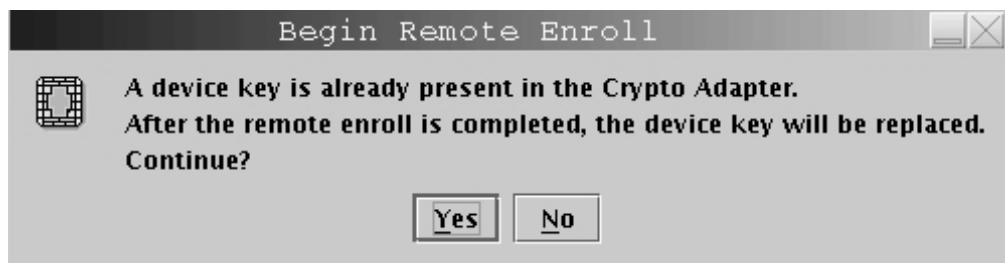


Figure 287. Crypto Adapter Enrolled

6. The restricted file chooser will open and prompt you for a file name and destination. Store the file.

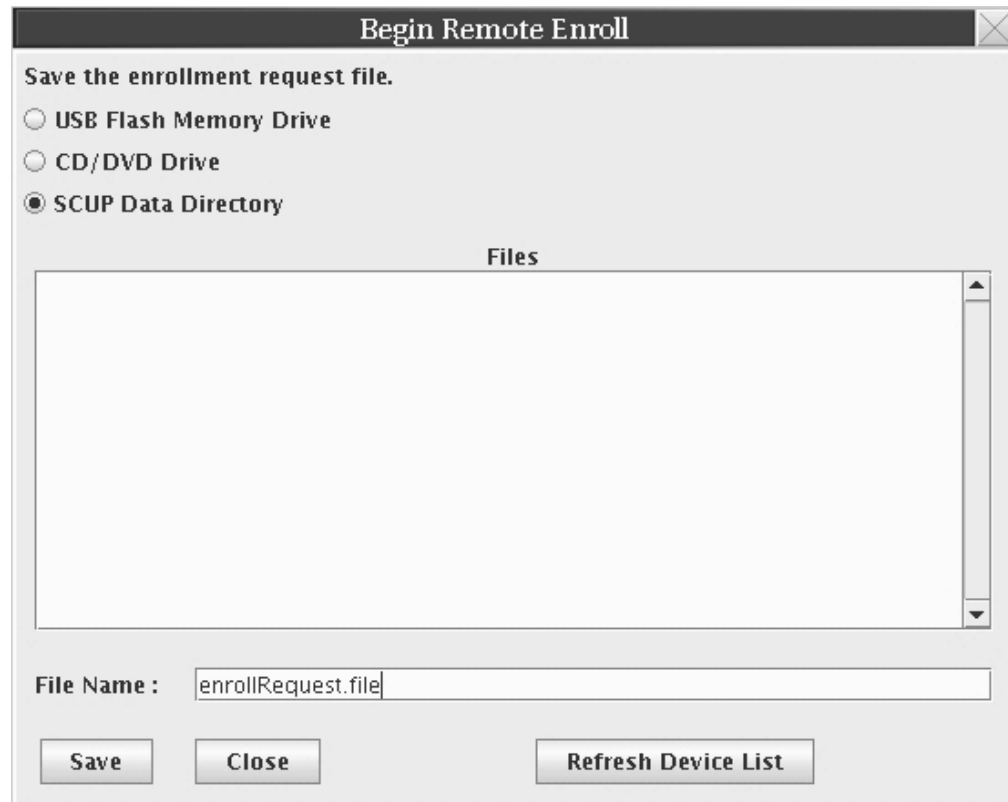


Figure 288. Save Enrollment Request



Figure 289. Enrollment Request Stored

**Warnings:**

- a. 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 “TKE Media Manager” on page 313.
- b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

7. 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.



8. On the local workstation, from the *Crypto Adapter* drop down menu, select *Enroll Crypto Adapter* option in SCUP.
9. Select *remote* when prompted for enrollment type.



Figure 290. Select remote zone



Figure 291. Remote zone enrollment instructions

10. At the prompt, insert the CA smart card in smart card reader 1.
11. At the prompt, enter the first CA PIN on the PIN pad of smart card reader 1.
12. At the prompt, enter the second CA PIN on the PIN pad of smart card reader 1.
13. At the prompt, select the enrollment request file (created above in step 6 on page 269).

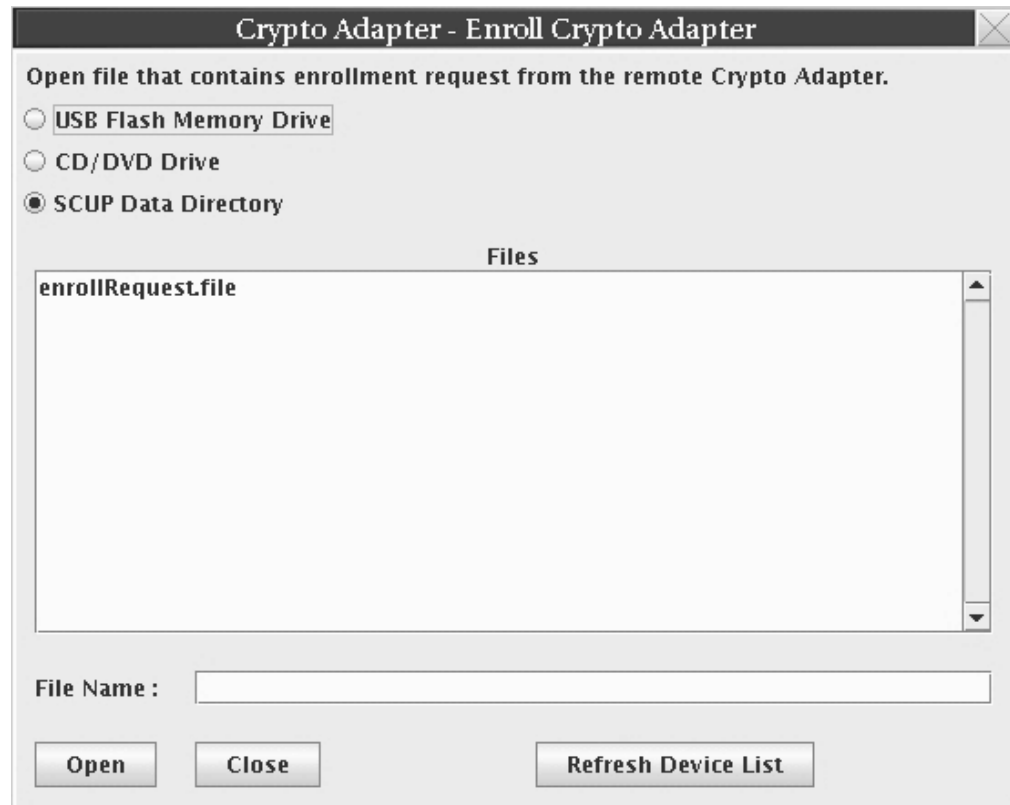


Figure 292. Open enrollment request file

14. The Crypto Adapter serial number is displayed. Confirm this enrollment by clicking **OK** if the serial number is correct or **Cancel** if it is incorrect.

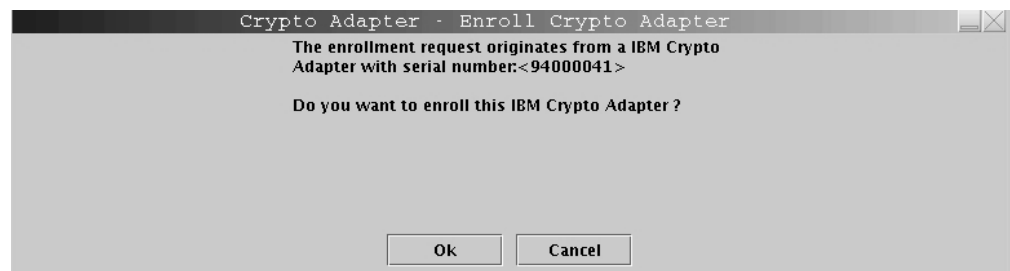


Figure 293. Verification of enrollment request

15. An enrollment certificate is created for the remote cryptographic adapter.
16. 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 294. Save the enrollment certificate



Figure 295. Continue with remote enrollment

**Warnings:**

- a. 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 "TKE Media Manager" on page 313.
- b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

17. 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.

18. On the remote workstation, click on Trusted Key Entry, Applications.
19. Click on Complete Zone Remote Enroll Process for an IBM Crypto Adapter.
20. Respond YES to the following message: "This program installs an enrollment accept in the IBM Cryptographic card installed in this workstation. Continue? (Yes/no)"
21. If the TKE crypto adapter is already enrolled, you are asked to confirm the enrollment and then asked to continue.
22. You are prompted for the file that contains the enrollment certificate (from step 16) by the restricted file chooser.

**Warnings:**

- a. 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 "TKE Media Manager" on page 313.
- b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

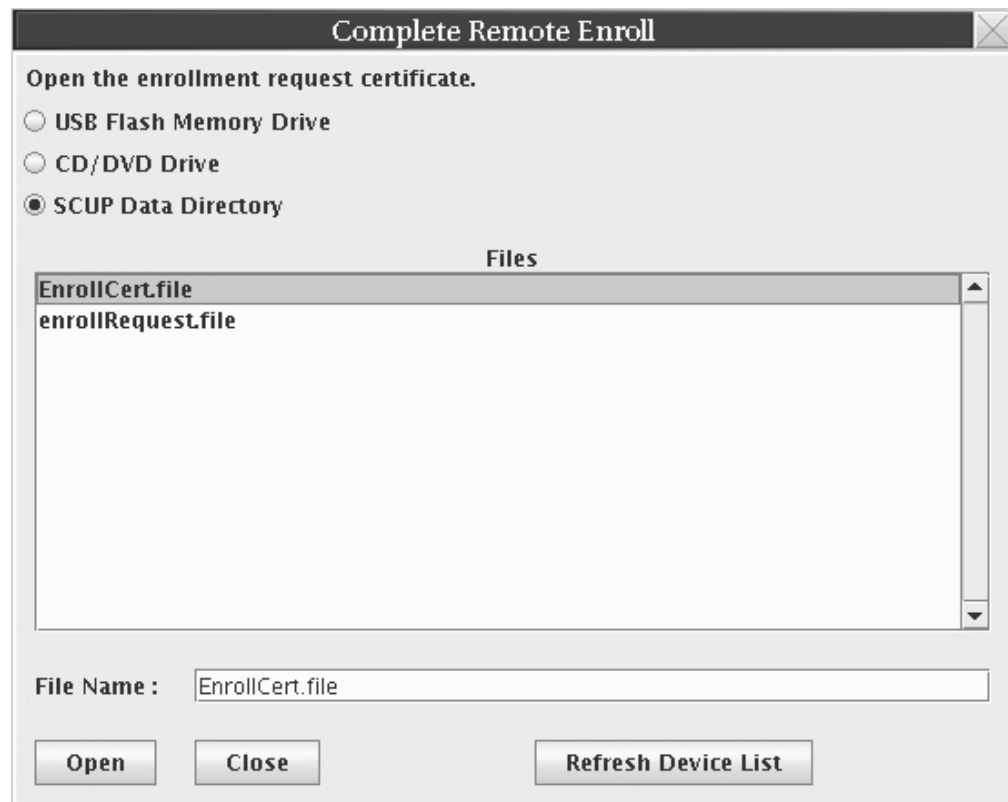


Figure 296. File Chooser Enroll Certificate

23. You will get a message that the remote Crypto Adapter has been installed in the zone (giving the zone description and ID).

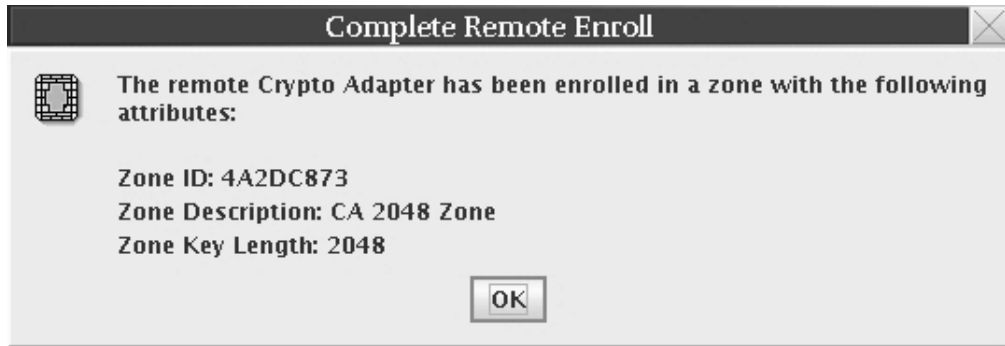


Figure 297. Remote Enroll Success

## View current zone

Use the View current zone 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 298. View current zone after Crypto Adapter enrollment

A window is returned with the Zone ID, Zone Key Length, and the Zone description (if you had previously entered a zone ID description).

## Appendix A. Secure Key Part Entry

This topic describes how you can enter a known key part value onto a TKE smart card. A known key part will have been saved on paper or in a binary file.

Secure Key Part Entry allows migration of existing key parts to TKE 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 278.

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, the user should use the TKE to securely copy the key part to another smartcard that is enrolled in the same zone for a backup. The user can then load the key part into key storage or onto the host.

### Steps for secure key part entry

Secure Key Part Entry begins from the Crypto Module Notebook Domains tab's Key tab by right-clicking the desired key type for entry. Right-clicking the desired key type reveals a menu with an entry for secure key part.

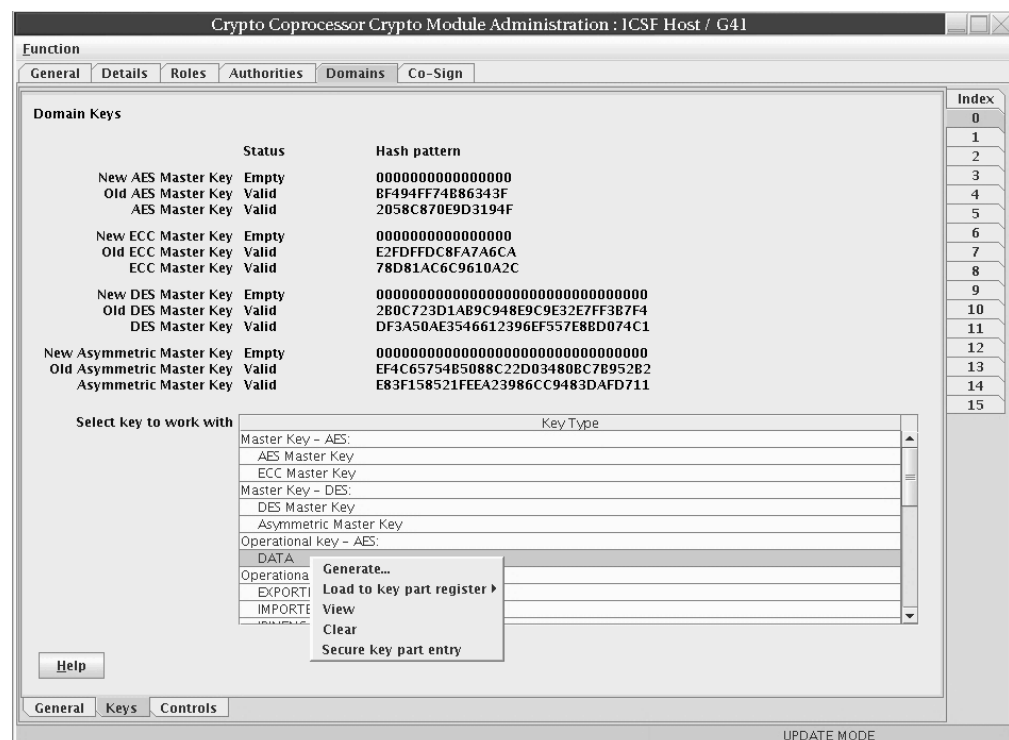


Figure 299. Choosing secure key part entry from the domains keys panel

This menu entry will be available for all supported crypto module types.

#### 1. Select **Secure key part entry**.

For master keys on all host crypto modules, a panel for entering a key part description displays.

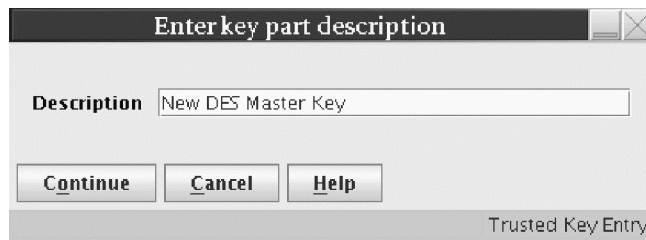


Figure 300. Enter description panel for secure key part entry

For operational keys, the Secure Key Part Entry panel displays.

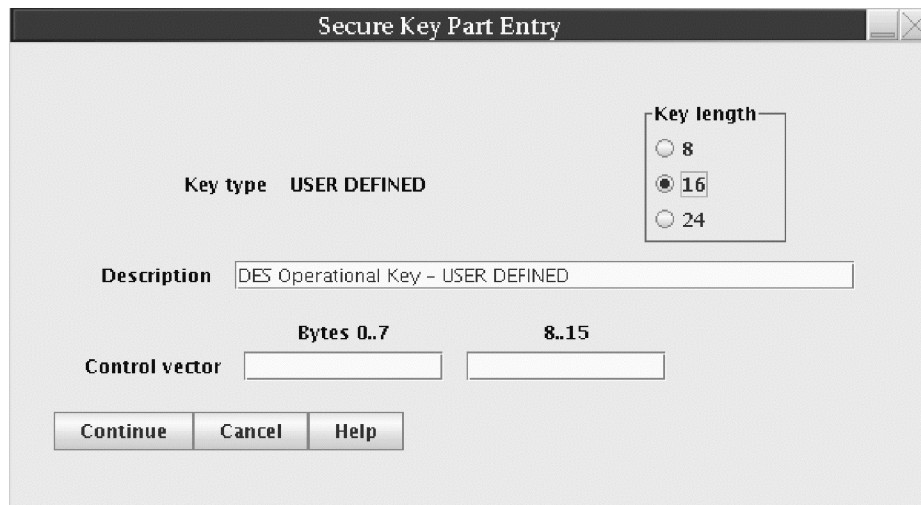


Figure 301. USER DEFINED operational key for secure key part entry

For a USER DEFINED operational key, the user is allowed to update the description, the key length, and the control vector.

For a predefined operational key, only the description may be updated, unless the predefined key type supports multiple key lengths. In that case, the key length field can also be updated. For a predefined 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.

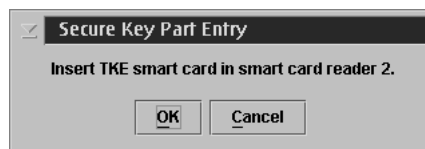


Figure 302. Secure key part entry — enter TKE smart card into reader

3. Enter the PIN on the smart card reader PIN pad when prompted.

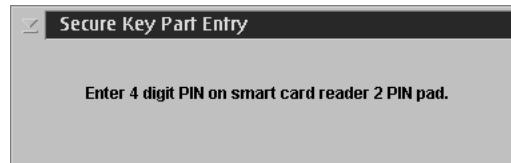


Figure 303. Secure key part entry — enter PIN

A dialog displays information about the TKE smart card.

4. If the TKE smart card information is correct, press **Yes** to continue.

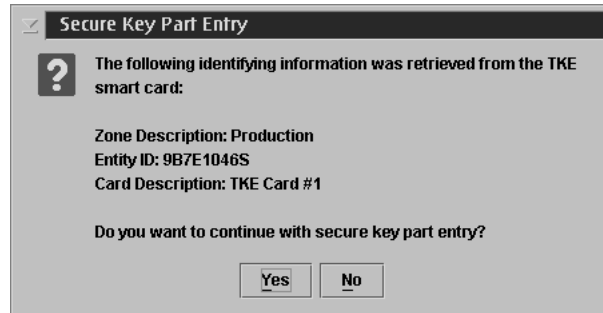


Figure 304. Secure key part entry card identification

The Secure Key Part Entry dialog displays.

5. Enter the known key part digits, which will have been saved on paper or in a binary file. See “Entering a key part on the smart card reader” on page 278.

**Note:** 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 4.1.0 or the Smart Card Utility Program 7.0 under Trusted Key Entry Applications. See “Display smart card information” on page 255 or “Display smart card key identifiers” on page 256.

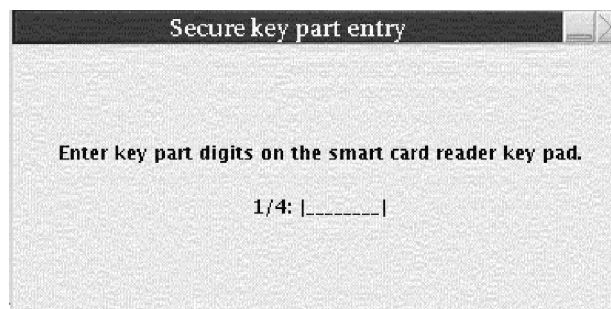


Figure 305. Secure key part entry — enter PIN

The dialog shows the progress of each hexadecimal digit entered with an asterisk (\*).

6. After the key part value has been successfully entered on the PIN pad, a 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 DES key part was entered correctly. The AES-VP value is shown to the user for verification that the AES or ECC key part was entered correctly. If the



key part entered was for an operational key, the control vector (CV) would also be displayed. Press OK to continue

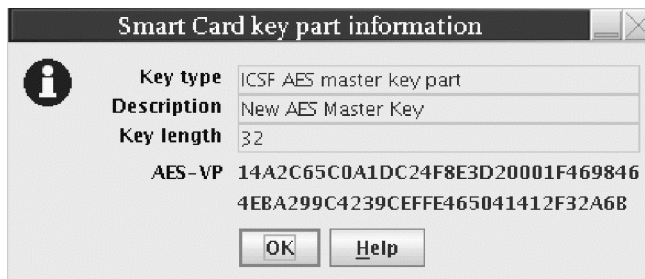


Smart Card key part information

**i** Key type ICSF DES master key part  
Description New DES Master Key  
Key length 16  
ENC-ZERO B635E389  
MDC-4 143C167FB323E77156EFDAA1372A3E45  
SHA1 BDA32C5F74683B3925DCEA5C6454E6B30F517034

OK Help

Figure 306. Secure key part entry — DES key part information for a master key



Smart Card key part information

**i** Key type ICSF AES master key part  
Description New AES Master Key  
Key length 32  
AES-VP 14A2C65C0A1DC24F8E3D20001F469846  
4EBA299C4239CEFFE465041412F32A6B

OK Help

Figure 307. Secure key part entry — AES key part information for a master key



Smart Card key part information

**i** Key type DES Operational key part, EXPORTER  
Description DES Operational Key - EXPORTER  
Key length 16  
Control vector 00417D0003410000 00417D0003210000  
ENC-ZERO C704A6A9  
MDC-4 DDE8EC6226034C8A377072122FB32DCA  
SHA1 7F7959D607F95CA4FFFD4CBCE4294C54BA5CAB2

OK Help

Figure 308. Secure key part entry — DES key part information for operational key

7. A message is displayed if the command executed successfully.



Secure Key Part Entry

**i** Command was executed successfully

Close

Figure 309. 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 15).

Except for RSA keys, all other key types for all crypto module types can be entered securely on the smart card reader PIN pad. These key parts can then be used to load master or operational key registers on the host.

Secure key part entry on the smart card reader PIN pad works as follows:

- A key part is separated into blocks. The key length in bytes (2 hexadecimal characters per byte) is divided by 4 and gives you the number of blocks.
- A block on the smart card reader PIN pad consists of 8 hexadecimal digits.
- Once a hexadecimal digit has been entered, the value cannot be changed.
- After entering the two digit decimal equivalent, the smart card reader records a hexadecimal digit, updating the smart card reader display with an '\*' in the section depicting the number of hexadecimal digits that have been recorded in the current block.
- After all the hexadecimal digits in a block have been entered, a running counter of the number of blocks completed on the screen is updated and the current block display is reset.
- Once a block is updated with a hexadecimal digit, the values cannot be changed.
- On the OmniKey reader, there is blank space for entering the two decimal digits. A single lock image is depicted on the right.
- The current decimal digit input can be changed. If an invalid two decimal digit input is entered, a change must occur. The Backspace key (yellow button labeled with a <-) on the smart card reader PIN pad can be used to undo entered decimal digits. The <- button lets the user change the first decimal of the hex digit. Example: if you entered 0\_ you can use the <-button to reenter the 0. The abort key (red button labeled with an X) on the smart card reader PIN pad can be used to reset the current decimal digit. It can also be used to cancel the secure key entry process.

### EXAMPLE

Key part type: 8-byte DES data operational key

Key part hexadecimal digits: AB CD EF 12 34 56 78 90

Number of blocks: 2

Number of hexadecimal digits per block: 8

Initial Block Counter Value: 1/2

Two decimal digit conversion of key part hexadecimal digits:

1011 1213 1415 0102 0304 0506 0708 0900

Table 15. 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

*Table 15. Decimal to Hexadecimal Conversion Table (continued)*

7	07
8	08
9	09
A	10
B	11
C	12
D	13
E	14
F	15

---

## Appendix B. 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, Crypto Express2 Coprocessor, or Crypto Express3 Coprocessor.

Access to services that are executed on the PCIXCC, CEX2C, or CEX3C is through Access Control Points in the DEFAULT Role. To execute callable services on the PCI X Cryptographic Coprocessor/Crypto Express2 Coprocessor, 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 new TKE V5.x users. If you are migrating from TKE V4.0, V4.1, or V4.2 to TKE V5.0 and have a PCIXCC/CEX2C/CEX3C, all your current access control points will remain the same and any new access control points for ICSF will not be enabled.

**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.

Access control points added in ICSF FMID HCR7780:

- ANSI X9.8 PIN - Enforce PIN block restrictions
- ANSI X9.8 PIN - Allow modification of PAN
- ANSI X9.8 PIN - Allow only ANSI PIN blocks
- Clear New ECC Master Key
- Load First ECC Master Key Part
- Combine ECC Master Key Parts
- Set ECC Master Key
- Generate ECC keys in the clear
- Symmetric token wrapping - internal enhanced method
- Symmetric token wrapping - internal original method
- Symmetric token wrapping - external enhanced method
- Symmetric token wrapping - external original method
- Diversified Key Generate - Allow wrapping override keywords
- Symmetric Key Generate - Allow wrapping override keywords
- Key Part Import - Allow wrapping override keywords
- Multiple Clear Key Import - Allow wrapping override keywords
- Multiple Secure Key Import - Allow wrapping override keywords
- Symmetric Key Import - Allow wrapping override keywords
- CKDS Conversion2 - Allow use of REFORMAT
- CKDS Conversion2 - Allow wrapping override keywords
- CKDS Conversion2 - Convert from enhanced to original
- PCF CKDS Conversion - Allow wrapping override keywords
- Key Translate2
- Key Translate2 - Allow wrapping override keywords

- Key Translate2 - Allow use of REFORMAT
- HMAC Generate – SHA-1
- HMAC Generate – SHA-224
- HMAC Generate – SHA-256
- HMAC Generate – SHA-384
- HMAC Generate – SHA-512
- Restrict Key Attribute – Export Control
- Key Generate2 – OP,EX,IM
- Key Generate2 – OPOP,OPIM,OPEX, etc
- Symmetric Key Token Change2
- Symmetric Key Token Change2 – RTCMK
- Secure Key Import2 - HMAC, OP
- Symmetric Key Import2 – HMAC,PKOAEP2
- Symmetric Key Export – HMAC,PKOAEP2
- HMAC Verify – SHA-1
- HMAC Verify – SHA-224
- HMAC Verify – SHA-256
- HMAC Verify – SHA-384
- HMAC Verify – SHA-512
- Key Part Import2 – Load first key part, require 3 key parts
- Key Part Import2 – Load first key part, require 2 key parts
- Key Part Import2 - Load first key part, require 1 key parts
- Key Part Import2 - Add second of 3 or more key parts
- Key Part Import2 - Add last required key part
- Key Part Import2 - Add optional key part
- Key Part Import2 – Complete key
- Key Test and Key Test2

Access control points added in ICSF FMID HCR7770 are:

- PKA Key Token Change RTNMK
- PKA Key Translate - from CCA RSA to SC Visa Format
- PKA Key Translate - from CCA RSA to SC ME Format
- PKA Key Translate - from CCA RSA to SC CRT Format
- PKA Key Translate - from source EXP KEK to target EXP KEK
- PKA Key Translate - from source IMP KEK to target EXP KEK
- PKA Key Translate - from source IMP KEK to target IMP KEK
- Symmetric Key Encipher/Decipher - Encrypted DES keys
- Symmetric Key Encipher/Decipher - Encrypted AES keys

In addition, access control point PKA Key Token Change was renamed to PKA Key Token Change RTCMK

Access Control Points for HCR7751 are:

- Clear New AES Master Key Register (ISPF ACP)
- Load First AES Master Key Part (ISPF ACP)
- Combine AES Master Key Parts (ISPF ACP)
- Set AES Master Key (ISPF ACP)

- Multiple Clear Key Import/Multiple Secure Key Import - AES
- Symmetric Algorithm Encipher - Secure AES
- Symmetric Algorithm Decipher - Secure AES
- Symmetric Key Generate - AES, PKCSOEP, PKCS- 1.2
- Symmetric Key Generate - AES, ZERO-PAD
- Symmetric Key Import - AES, PKCSOEP, PKCS-1.2
- Symmetric Key Import - AES, ZERO-PAD
- Symmetric Key Export - AES, PKCSOEP, PKCS-1.2
- Symmetric Key Export - AES, ZERO-PAD

These access control points require the November, 2008 or later licensed internal code (LIC).

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
- PTR Enhanced PIN Security

Callable services affected by PTR enhanced PIN security:

- Clear PIN Encrypt - PTR Enhanced PIN Security
- Clear Pin Generate Alternate - PTR Enhanced PIN Security
- Encrypted PIN Generate - PTR Enhanced PIN Security
- Encrypted PIN Translate - PTR Enhanced PIN Security
- Encrypted PIN Verify - PTR Enhanced PIN Security
- PIN Change/Unblock - PTR Enhanced PIN Security

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/CEX3C.

For the relationship between access control points and callable services, see Table 16.

If an access control point is disabled, the corresponding ICSF callable service or utility will fail during execution with an access denied error.

*Table 16. Callable service access control points*

Access Control Point	Callable Service/Utility
Allow ECC Clear Key Generation	CSNDPKG and CSNFPKG
ANSI X9.8 PIN - Enforce PIN block restrictions	CSNBCPA / CSNECPA, CSNBPTR / CSNEPTR, and CSNBSPN / CSNESP
ANSI X9.8 PIN - Allow modification of PAN	CSNBPTR / CSNEPTR
ANSI X9.8 PIN - Allow only ANSI PIN blocks	CSNBPTR / CSNEPTR
CKDS Conversion2 - Allow use of REFORMAT	CSFCNV2
CKDS Conversion2 - Allow wrapping override keywords	CSFCNV2
CKDS Conversion2 - Convert from enhanced to original	CSFCNV2
Clear Key Import / Multiple Clear Key Import - DES	CSNBCKI or CSNBCKM
Clear Key Import / Multiple Clear Key Import - AES	CSNBCKI , CSNBCKM or CSNBCKM
Clear PIN Encrypt	CSNBCPE
Clear PIN Generate - 3624	CSNBPGN
Clear PIN Generate - GBP	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
CVV Generate	CSNBCSG
CVV Verify	CSNBCSV
DATAM Key Management Control	CSNBKGN, CSNBKIM, CSNBKEX and CSNBKDG
Data Key Export	CSNBKX
Data Key Export - Unrestricted	CSNBKX
Data Key Import	CSNBKIM
Data Key Import - Unrestricted	CSNBKIM
Decipher - DES	CSNBDEC

Table 16. Callable service access control points (continued)

Digital Signature Generate	CSNDDSG
DSG ZERO-PAD restriction lifted	CSNDDSG
Digital Signature Verify	CSNDDSV
Diversified Key Generate - Allow wrapping override keywords	CSNBDKG and CSNEDKG
Diversified Key Generate - CLR8-ENC	CSNBDKG
Diversified Key Generate - SESS-XOR	CSNBDKG
Diversified Key Generate - TDES-ENC	CSNBDKG
Diversified Key Generate - TDES-DEC	CSNBDKG
Diversified Key Generate - TDES-XOR	CSNBDKG
Diversified Key Generate - TDESEMV2/TDESEMV4	CSNBDKG
Diversified Key Generate - single length or same halves	CSNBDKG
DKYGENKY - DALL	CSNBDKG
Encipher - DES	CSNBENC
Encrypted PIN Generate - 3624	CSNBEPG
Encrypted PIN Generate - GBP	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
HMAC Generate – SHA-1	CSNBHMG or CSNBHMG1 and CSNEHMG or CSNEHMG1
HMAC Generate – SHA-224	CSNBHMG or CSNBHMG1 and CSNEHMG or CSNEHMG1
HMAC Generate – SHA-256	CSNBHMG or CSNBHMG1 and CSNEHMG or CSNEHMG1
HMAC Generate – SHA-384	CSNBHMG or CSNBHMG1 and CSNEHMG or CSNEHMG1
HMAC Generate – SHA-512	CSNBHMG or CSNBHMG1 and CSNEHMG or CSNEHMG1
HMAC Verify – SHA-1	CSNBHMG or CSNBHMG1 and CSNEHMG or CSNEHMG1
HMAC Verify – SHA-224	CSNBHMG or CSNBHMG1 and CSNEHMG or CSNEHMG1
HMAC Verify – SHA-256	CSNBHMG or CSNBHMG1 and CSNEHMG or CSNEHMG1
HMAC Verify – SHA-384	CSNBHMG or CSNBHMG1 and CSNEHMG or CSNEHMG1
HMAC Verify – SHA-512	CSNBHMG or CSNBHMG1 and CSNEHMG or CSNEHMG1



Table 16. Callable service access control points (continued)

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 Generate2 – OP,EX,IM	CSNBKGN2 and CSNEKGN2
Key Generate2 – OPOP,OPIM,OPEX etc	CSNBKGN2 and CSNEKGN2
Key Import	CSNBKIM
Key Import - Unrestricted	CSNBKIM
Key Part Import2 – Load first key part, require 3 key parts	CSNBKPI2 and CSNEKPI2
Key Part Import2 – Load first key part, require 2 key parts	CSNBKPI2 and CSNEKPI2
Key Part Import2 - Load first key part, require 1 key parts	CSNBKPI2 and CSNEKPI2
Key Part Import2 - Add second of 3 or more key parts	CSNBKPI2 and CSNEKPI2
Key Part Import2 - Add last required key part	CSNBKPI2 and CSNEKPI2
Key Part Import2 - Add optional key part	CSNBKPI2 and CSNEKPI2
Key Part Import2 – Complete key	CSNBKPI2 and CSNEKPI2
Key Part Import - ADD-PART	CSNBKPI
Key Part Import - Allow wrapping override keywords	CSNBKPI
Key Part Import - COMPLETE	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 Test and Key Test2	CSNBKYT, CSNEKYT, CSNBKYT2, and CSNEKYT2
Key Translate	CSNBKTR
Key Translate2	CSNBKTR2 and CSNEKTR2
Key Translate2 - Allow wrapping override keywords	CSNBKTR2 and CSNEKTR2
Key Translate2 - Allow use of REFORMAT	CSNBKTR2 and CSNEKTR2
MAC Generate	CSNBMGN
MAC Verify	CSNBMVR
Multiple Clear Key Import - Allow wrapping override keywords	CSNBCKM and CSNECKM
Multiple Secure Key Import - Allow wrapping override keywords	CSNBSKM and CSNESKM
NOCV KEK usage for export-related functions	CSNBKEX, CSNBSKM, and CSNBKGN
NOCV KEK usage for import-related functions	CSNBKIM, CSNBSKI, CSNBSKM, and CSNBKGN

Table 16. Callable service access control points (continued)

PCF CKDS Conversion - Allow wrapping override keywords	CSFCONV
PCF CKDS Conversion Program	CSFCONV
PIN Change/Unblock - change EMV PIN with OPINENC	CSNBPCU
PIN Change/Unblock - change EMV PIN with IPINENC	CSNBPCU
PIN Change/Unblock - PTR Enhanced PIN Security	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
PKA Key Generate - Permit Regeneration Data Retain	CSNDPKG
PKA Key Import	CSNDPKI
PKA Key Import - Import an External Trusted Key Block to internal form	CSNDPKI
PKA Key Token Change RTCMK	CSNDKTC
PKA Key Token Change RTNMK	CSNDKTC
PKA Key Translate - from CCA RSA to SC Visa Format	CSNDPKT
PKA Key Translate - from CCA RSA to SC ME Format	CSNDPKT
PKA Key Translate - from CCA RSA to SC CRT Format	CSNDPKT
PKA Key Translate - from source EXP KEK to target EXP KEK	CSNDPKT
PKA Key Translate - from source IMP KEK to target EXP KEK	CSNDPKT
PKA Key Translate - from source IMP KEK to target IMP KEK	CSNDPKT
Prohibit Export	CSNBPEX
Prohibit Export Extended	CSNBPEXX
PTR Enhanced PIN Security	CSNBCPE, CSNBCPA, CSNBEPG, CSNBPTR, CSNBPVR, and CSNBPCU
Remote Key Export - Generate or export a key for use by a non-CCA node	CSNDRKX and CSNFRKX
Restrict Key Attribute – Export Control	CSNBRKA and CSNERKA
Retained Key Delete	CSNDRKD
Retained Key List	CSNDRKL
Secure Key Import - IM	CSNBSKI or CSNBSKM
Secure Key Import - OP	CSNBSKI or CSNBSKM

Table 16. Callable service access control points (continued)

Secure Key Import2 - HMAC, OP	CSNBSKI2 and CSNESKI2
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 Algorithm Decipher - Secure AES	CSNBSAD or CSNBSAD1
Symmetric Algorithm Encipher - Secure AES	CSNBSAE or CSNBSAE1
Symmetric Key Export - AES, PKCS-1.2	CSNDSYX and CSNFSYX
Symmetric Key Export - DES, PKCS-1.2	CSNDSYX and CSNFSYX
Symmetric Key Export - AES, ZERO-PAD	CSNDSYX and CSNFSYX
Symmetric Key Export - DES, ZERO-PAD	CSNDSYX and CSNFSYX
Symmetric Key Export – HMAC,PKOAEP2	CSNDSYX and CSNFSYX
Symmetric Key Encipher/Decipher - Encrypted DES keys	CSNBSYD or CSNBSYE
Symmetric Key Encipher/Decipher - Encrypted AES keys	CSNBSYD or CSNBSYE
Symmetric Key Generate - Allow wrapping override keywords	CSNDSYG and CSNFSYG
Symmetric Key Generate - DES, PKA92	CSNDSYG and CSNFSYG
Symmetric Key Generate - AES, PKCS-1.2	CSNDSYG and CSNFSYG
Symmetric Key Generate - DES, PKCS-1.2	CSNDSYG and CSNFSYG
Symmetric Key Generate - AES, ZERO-PAD	CSNDSYG and CSNFSYG
Symmetric Key Generate - DES, ZERO-PAD	CSNDSYG and CSNFSYG
Symmetric Key Import - Allow wrapping override keywords	CSNDSYI and CSNFSYI
Symmetric Key Import - DES, PKA92 KEK	CSNDSYI and CSNFSYI
Symmetric Key Import - AES, PKCS-1.2	CSNDSYI and CSNFSYI
Symmetric Key Import - DES, PKCS-1.2	CSNDSYI and CSNFSYI
Symmetric Key Import - AES, ZERO-PAD	CSNDSYI and CSNFSYI
Symmetric Key Import - DES, ZERO-PAD	CSNDSYI and CSNFSYI
Symmetric Key Import2 – HMAC,PKOAEP2	CSNDSYI2 and CSNFSYI2
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 Trusted Key Block in Inactive Form	CSNDTBC
UKPT - PIN Verify, PIN Translate	CSNBPVR and CSNBPTR

**Notes:**

1. The Access Control Points available depend on the coprocessor you are using.
2. 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.
3. 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.
4. Diversified Key Generate - single length or same halves requires either Diversified Key Generate - TDES-ENC or Diversified Key Generate - TDES-DEC be enabled.
5. In order to use ATM Remote Key Loading, TKE users will have to enable the access control points for these functions:
  - Trusted Block Create - Activate an Inactive Trusted Key Block
  - Trusted Block Create - Create Trusted Key Block in Inactive Form
  - PKA Key Import - Import an External Trusted Key Block to internal form
  - Remote Key Export - Generate or export a key for use by a non-CCA node



---

## Appendix C. LPAR Considerations

---

### Setup for CEX2C/CEX3C Systems

Host image profiles for logical partitions must be correctly configured in order to use the TKE workstation to manage keys and perform other operations. The host support element is used to set and change the configuration.

When customizing an image profile using the support element, four fields are specified:

- **Usage domain index** – The domain associated with the logical partition.
- **Control domain index** – The set of domains that can be managed from this logical partition. It must include the usage domain index value for this logical partition. A logical partition used as the TKE host includes the usage domain index values for all logical partitions the TKE workstation may manage.
- **PCI Cryptographic Candidate List** – The set of cryptographic coprocessors that the logical partition may access.
- **PCI Cryptographic Online List** – The set of cryptographic coprocessors that will be brought online when the logical partition is activated.

If a logical partition sends a command to a domain that is not in its control domain index, ICSF returns an error (return code 12, reason code 2015).

There is no specific field to identify a logical partition as a TKE host when you are customizing image profiles. You must decide which logical partition will be the TKE host and set up the control domain index and PCI Cryptographic Candidate List appropriately. The control domain index for this partition must include the usage domain index values for all logical partitions that the TKE workstation will control, and the PCI Cryptographic Candidate List for this partition must include all entries in the PCI Cryptographic Candidate Lists for the logical partitions that the TKE workstation will control. The control domain index must also include the usage domain index value for the TKE host partition itself.

Multiple logical partitions may specify the same usage domain index, provided there are no common entries on their PCI Cryptographic Candidate Lists. (Logical partitions may not share the same domain on the same cryptographic coprocessor, but can use the same domain index value on different cryptographic coprocessors.) In order to control these partitions, however, the TKE host partition must have a unique usage domain index, since its PCI Cryptographic Candidate List must include all coprocessors of the logical partitions being controlled.

The example in Figure 310 on page 292 has 3 LPARs and 4 CEX2Cs: 00, 01, 02, 03. There is no domain sharing. In this case, all the CEX2Cs can be specified in the Candidate List for each LPAR.

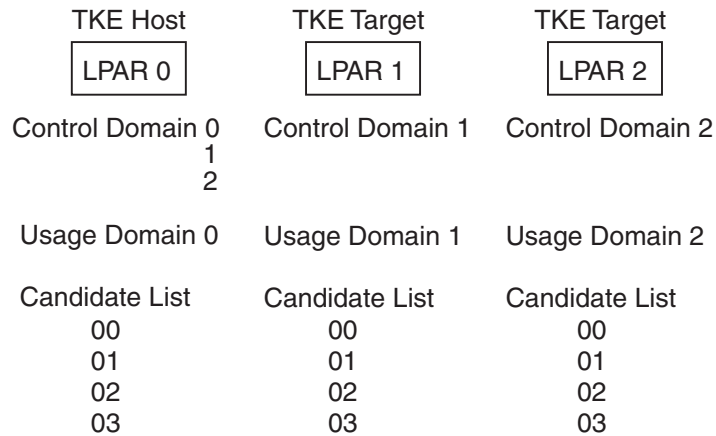


Figure 310. An Example of TKE Host and TKE Target LPARs without Domain Sharing

The example in Figure 311 has 4 LPARs, 2 sharing the same domain and 4 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 CEX2Cs.

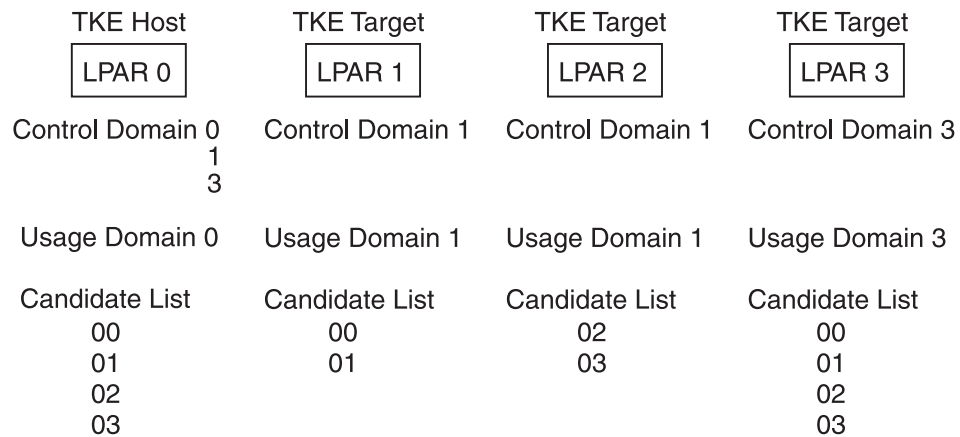


Figure 311. An Example of TKE Host and TKE Target LPARs with Domain Sharing

If the same domain is specified by more than one LPAR and the Candidate List has any of the same CEX2Cs, the first LPAR that is activated will IPL without error but the other LPARs with the same domain will fail activation.

## Appendix D. Trusted Key Entry - Workstation Cryptographic Adapter Initialization

### Cryptographic Node Management Batch Initialization 4.1.0

The Cryptographic Node Management Batch Initialization 4.1.0 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 4.1.0. Open the Cryptographic Node Management Utility 4.1.0. Click on **File** and select **CNI Editor**.

All scripts must be run from the floppy, DVD-RAM, USB flash memory drive, or CNM Data Directory. User-created scripts can be used to further initialize the TKE workstation crypto adapter after passphrase or smart card initialization has been done. For details on initializing the TKE workstation crypto adapter for passphrase or smart card use, see “Initializing TKE for passphrase” on page 71 and “Initializing TKE for smart cards” on page 77.

To execute a user-defined CNI script, click on **Trusted Key Entry**, and then **Cryptographic Node Management Batch Initialization 4.1.0**. You must be logged onto the console as ADMIN to access this task. The Select CNI file to Run window is displayed. Select the location (CD/DVD drive, floppy drive, USB flash memory drive, or CNM data directory) and the file name of the CNI to execute. Click on **Open**.

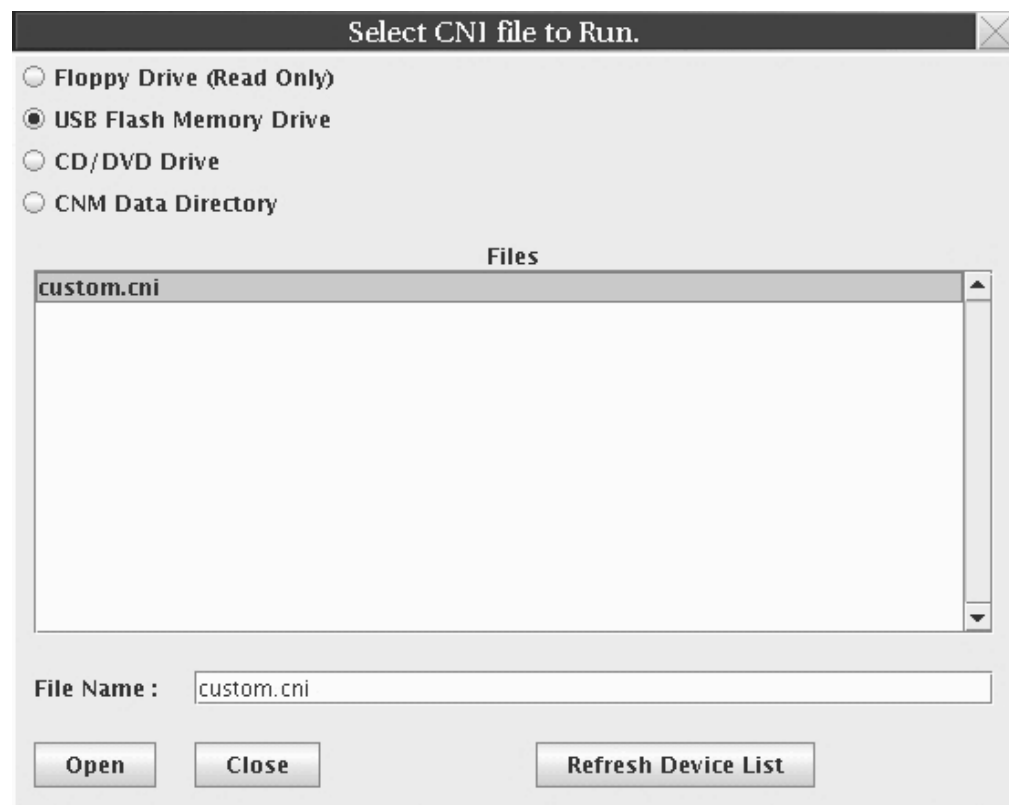


Figure 312. Cryptographic Node Management Batch Initialization 4.1.0 Task Window



The output window shows the operations performed. Select **OK** to exit this task.

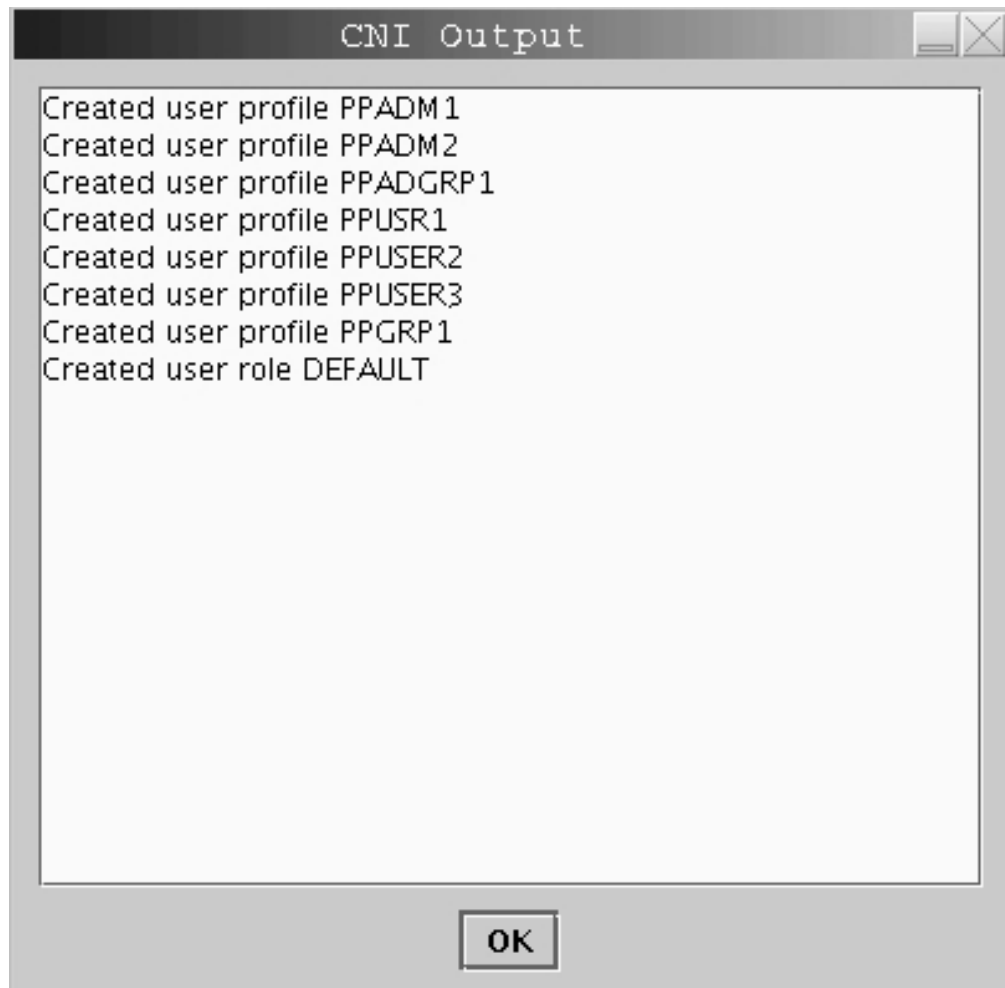


Figure 313. Cryptographic Node Management Batch Initialization Task Output Window

---

## CCA CLU 4.1.0

- | The CCA CLU 4.1.0 task is used for loading and checking code on the TKE workstation crypto adapter.
- | If you are running with TKE 7.0, you must perform CLU actions after your system has been rebooted and before attempting to use any other utility or application that communicates with the TKE workstation crypto adapter.  
  
**Note:** CLU should only be executed when directed by IBM support. CLU functions can take several minutes to execute.
- | To invoke the CLU Utility, click on **Trusted Key Entry**, then select **CCA CLU 4.1.0**. You must be logged on as ADMIN to access this task.

## CLU Processing

When CLU is invoked, the Non-Factory Mode is displayed. You can select any combination of CLU command check boxes.

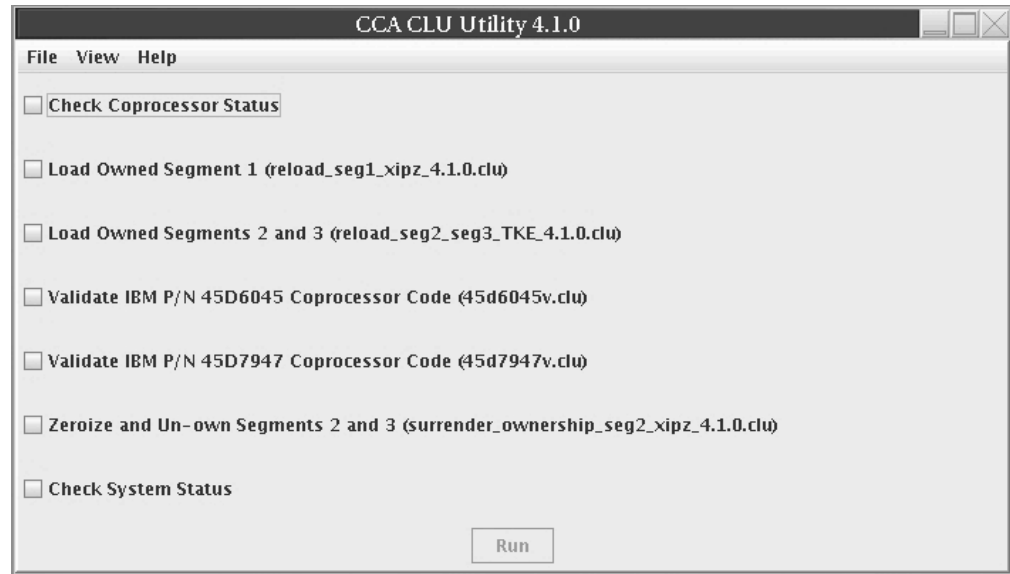


Figure 314. CLU Command Check Boxes

When RUN is pressed, the commands will execute in the order they appear on the application window.

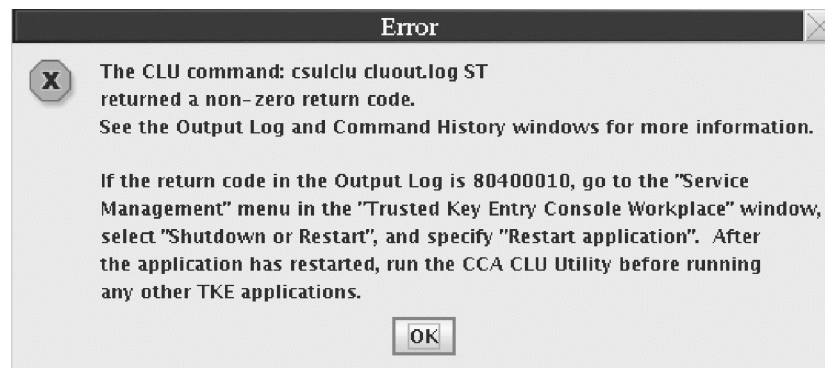


Figure 315. CLU Error

If a command fails, the commands checked after the failing command will not execute and will remain checked.

After pressing **Run**, 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.

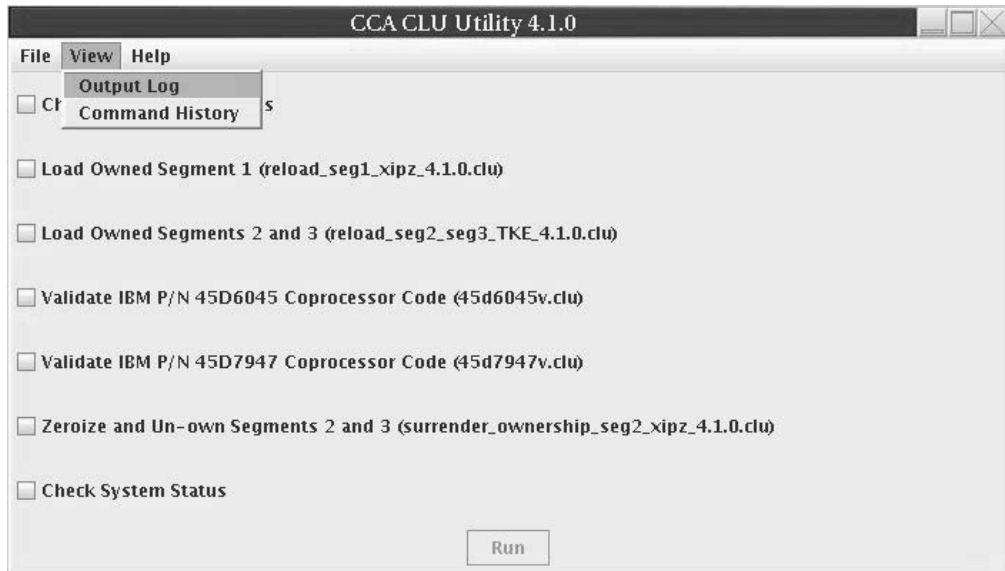


Figure 316. CLU View Menu

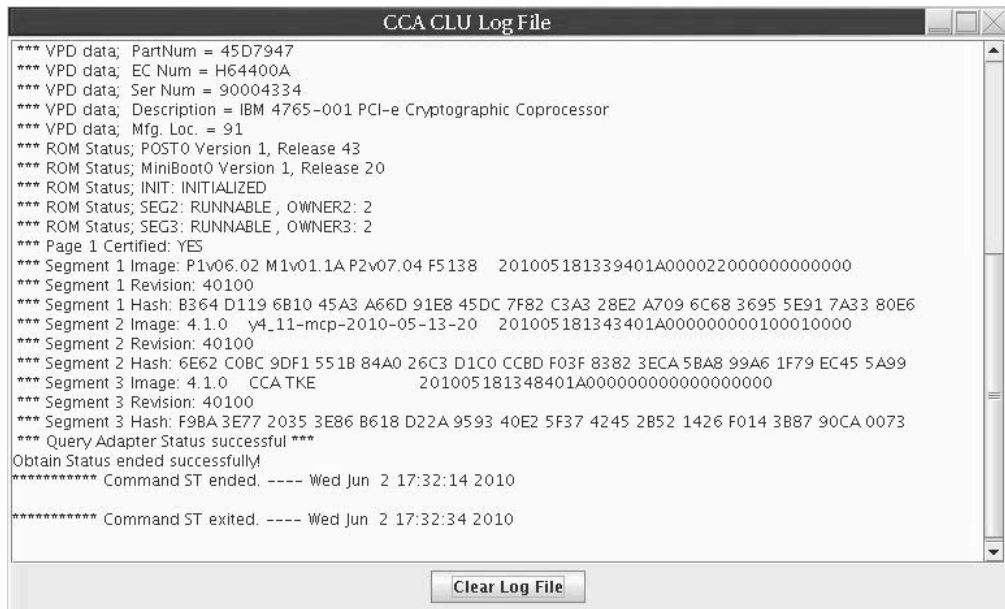


Figure 317. Output Log file

The CLU output log file is available to the user in the CNM Data Directory.

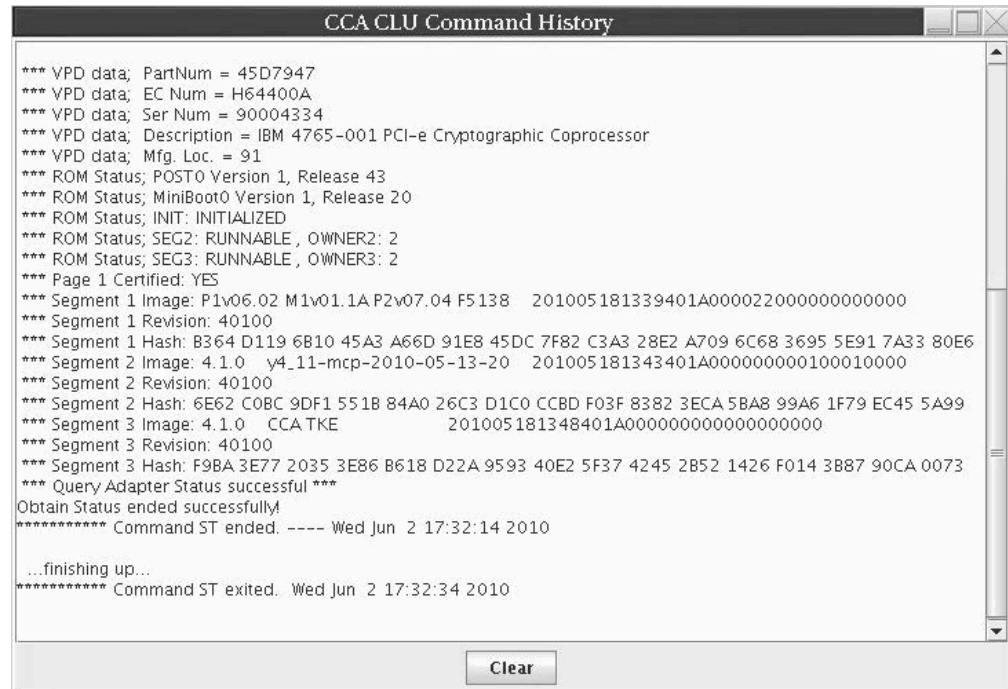


Figure 318. CLU Command History

If all CLU commands complete without error, a message indicating that all CLU commands completed successfully will be displayed.

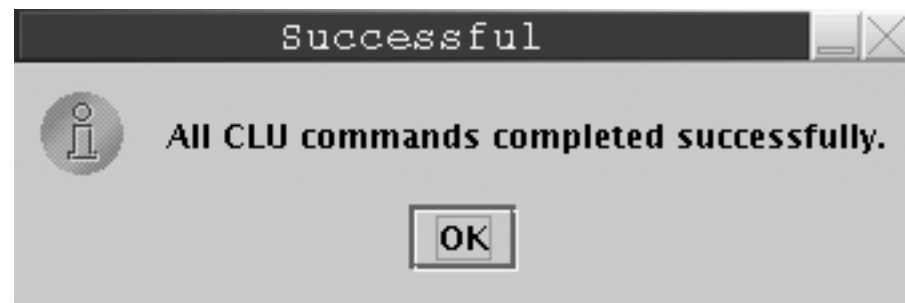


Figure 319. Successful Completion of CLU Commands

## Checking Coprocessor Status

Before loading code you should check the coprocessor status. To use the CLU utility check status command (ST), you must select the "Check Coprocessor Status" check box and then press **Run**.

View the results in the Output Log or Command History.

## Loading Coprocessor Code

IBM 4765-001 P/N 45D6045 and 45D7947 crypto adapters are supported.

1. Change segment 1:
  - a. If the segment 1 image name indicates ... Factory ...Set the application to Factory Mode (File -> Factory Mode). The Factory Mode CLU window will be displayed.

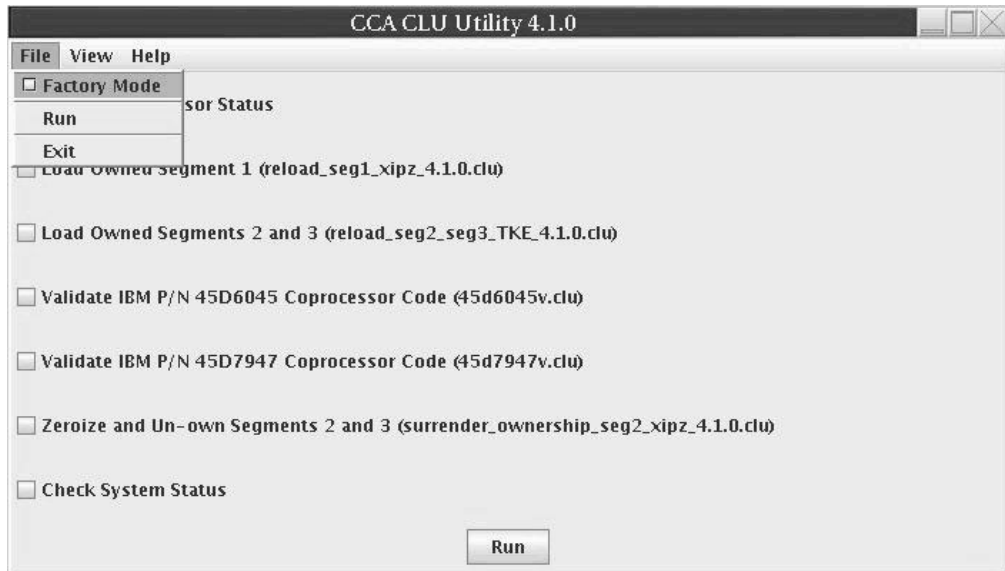


Figure 320. CLU File Menu

Reload segment 1 with the CCA segment 1 file

(reload\_seg1\_xipz\_factory\_4.1.0.clu) Select the "Load Factory Segment 1 (reload\_seg1\_xipz\_factory\_4.1.0.clu)" check box and then press **Run**.

- b. If the segment 1 image name indicates ...CCA ..., and the revision level is below 4.1.0, reload segment 1 with the CCA segment 1 file (reload\_seg1\_xipz\_4.1.0.clu) by selecting the "Load Owned Segment 1 (reload\_seg1\_xipz\_4.1.0.clu)" check box and then pressing **Run**.

**Note:** This choice is only available when the application is not in Factory Mode (File -> Factory Mode).

2. Change segments 2 and 3:

- a. If segment 2 ROM status indicates Unowned... Set the application to Factory Mode (File->Factory Mode). Select the 'Load IBM Factory Segments 2 and 3 (establish\_ownership\_then\_emergency\_reload\_seg2\_seg3\_TKE\_4.1.0.clu)' check box and press **Run**.
- b. If segment 2 and 3 ROM status both indicate owner 02... Select the 'Load Owned Segments 2 and 3 (reload\_seg2\_seg3\_TKE\_4.1.0.clu)' check box and press **Run**.

**Note:** This choice is only available when the application is not in Factory Mode (File -> Factory Mode).

3. When you have successfully completed this process, a check of the coprocessor status or validate of the coprocessor code will indicate that the segments contain:

Segment 1 Image: P1v05.77 M1v01.17

Segment 2 Image: 4.1.0 y4\_11-mcp-2010-02-12-14

Segment 3 Image: 4.1.0 CCA TKE

View the results in the Output Log or Command History.

## Validating Coprocessor Code

If you want to validate the code loaded on the crypto adapter use the CLU utility validate command (VA). Select the appropriate check box for your TKE workstation crypto adapter and press **Run**.

```
| IBM 4765 Model 01 P/N 45D6045
| Validate IBM P/N 45D6045 Coprocessor Code (45d6045v.clu)
```

View the results in the Output Log or Command History.

## Checking System Status

If you want to check the system status of your TKE workstation crypto adapter, use the CLU utility check system status command (SS). Select the **Check System Status** check box and then press **Run**.

View the results in the Output Log or Command History.

## Resetting Coprocessor

If you need to reset the TKE workstation crypto adapter use the CLU utility reset coprocessor command (RS). You must enter Factory mode by clicking **Factory Mode** under the File menu. Then select the **Reset Coprocessor** check box and press **Run**.

View the results in the Output Log or Command History.

## Removing Coprocessor CCA Code and Zeroizing CCA

To Zeroize the CCA node and remove the CCA Coprocessor Code from segments 2 and 3, select the "Zeroize and Unown Segments 2 and 3 (surrender\_ownership\_seg2\_xipz\_4.1.0.clu)" check box and then press **Run**. This should result in the segment 2 and 3 ROM Status indicated Unowned.

View the results in the Output Log or Command History.

## Help Menu

The CLU Utility has a help page. To view the help, select **Contents** from the **Help** menu.



## Appendix E. 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 F. Trusted Key Entry Applications and Utilities

The TKE console supports a variety of tasks, applications, and utilities.

The set of tasks, applications, and utilities available depends on the console user name specified when the console is initially started. The default console user name is TKEUSER. Other console user names are AUDITOR, ADMIN, and SERVICE.

See “Trusted Key Entry Console” on page 8 for more information.

Table 17. Tasks, applications and utilities accessible by console user name

Navigation	Task	TKEUSER	ADMIN	AUDITOR	SERVICE
<b>Trusted Key Entry</b>					
	Begin Zone Remote Enroll Process for an IBM Crypto Adapter	X	X		
	CCA CLU 4.1.0		X		
	Complete Zone Remote Enroll Process for an IBM Crypto Adapter	X	X		
	Cryptographic Node Management Batch Initialization 4.1.0		X		
	Cryptographic Node Management Utility 4.1.0	X	X		
	Smart Card Utility Program 7.0	X	X		
	TKE's IBM Crypto Adapter Initialization		X		
	Trusted Key Entry 7.0	X	X		
	Edit TKE Files	X	X		
	Migrate Previous TKE Version to TKE 7.0		X		
	TKE File Management Utility	X	X	X	X
	TKE Media Manager	X	X	X	X
	TKE Workstation Code Information	X	X		
	TKE Audit Configuration Utility			X	
	Migrate IBM Host Crypto Module Public Configuration Data	X	X		
	Configuration Migration Tasks	X	X		
	TKE Audit Record Upload Utility			X	
<b>Service Management</b>					
	Lock Console	X	X	X	X
	Shutdown or Restart	X	X	X	X
	Hardware Messages	X	X	X	X
	Network Diagnostic Information	X	X	X	X
	Users and Tasks	X	X	X	X
	View Console Information	X	X	X	X
	View Console Service History				X
	View Licenses	X	X	X	X
	Format Media	X	X	X	X

Table 17. Tasks, applications and utilities accessible by console user name (continued)

Navigation	Task	TKEUSER	ADMIN	AUDITOR	SERVICE
	Backup Critical Console Data		X		X
	Offload Virtual RETAIN Data to DVD-RAM				X
	Rebuild Vital Product Data				X
	Save Upgrade Data		X		X
	Transmit Console Service Data				X
	Manage Print Screen Files	X	X	X	X
	View Console Events	X	X	X	X
	View Console Tasks Performed			X	X
	View Security Logs			X	
	Archive Security Logs			X	
	Format Security Log to DVD-RAM			X	
	Analyze Console Internal Code				X
	Authorize Internal Code Changes				X
	Change Console Internal Code				X
	Change Password		X	X	X
	Configure 3270 Emulators	X	X	X	X
	Customize Console Date/Time		X		X
	Customize Network Settings		X		X
	Customize Scheduled Operations		X		X

## Trusted Key Entry Applications and Utilities

- “Begin Zone Remote Enroll Process” on page 305
- “CCA CLU 4.1.0” on page 305
- “Complete Zone Remote Enroll Process” on page 305
- “Cryptographic Node Management Batch Initialization 4.1.0” on page 305
- “Cryptographic Node Management Utility 4.1.0” on page 305
- “Edit TKE Files” on page 305
- “Migrate Previous TKE Version to TKE 7.0” on page 309
- “Smart Card Utility Program 7.0” on page 311
- “TKE Audit Configuration Utility” on page 311
- “TKE Audit Record Upload Configuration Utility” on page 311
- “TKE File Management Utility” on page 311
- “TKE Media Manager” on page 313
- “TKE Workstation Code Information” on page 315
- “Migrate IBM Host Crypto Module Public Configuration Data” on page 316
- “Configuration Migration Tasks” on page 317
- Trusted Key Entry 7.0
- TKE IBM Crypto Adapter Initialization

## Begin Zone Remote Enroll Process

This task is for an IBM Crypto Adapter. It is for use on the Remote TKE to begin the zone enrollment process.

See “Remote/Secondary Crypto Adapter Enrollment” on page 267.

## CCA CLU 4.1.0

This task is for loading code onto the TKE V7.0 Workstation Crypto Adapter.

See “CCA CLU 4.1.0” on page 294.

## Complete Zone Remote Enroll Process

This task is for an IBM Crypto Adapter. It is for use on the Remote TKE to complete the zone enrollment process.

See “Remote/Secondary Crypto Adapter Enrollment” on page 267

## Cryptographic Node Management Batch Initialization 4.1.0

This task is for using a batch interface to execute a user-created CNI file. A user-created CNI file can be used to initialize a TKE crypto adapter differently than the TKE IBM Crypto Adapter Initialization task. To create the user CNI, use the Cryptographic Node Management Utility 4.1.0, CNI Editor function.

See “Cryptographic Node Management Batch Initialization 4.1.0” on page 293

## Cryptographic Node Management Utility 4.1.0

This task is for managing the TKE workstation crypto adapter (create and manage Roles and Profiles, manage workstation master keys, et cetera).

See Chapter 10, “Cryptographic Node Management Utility (CNM),” on page 209.

## Edit TKE Files

The Edit TKE Files task provides a way to edit/browse files on diskette, CD/DVD, USB flash memory drive, 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

Files in the Configuration Data Directory can not be accessed by the Edit TKE Files task and should be reviewed using the review functions in the configuration migration applications.

To open the Edit TKE Files task, click on **Trusted Key Entry** and then click on **Edit TKE Files**.

You must be logged on to the TKE workstation crypto adapter for this task. If you are not currently logged onto the adapter, a logon window is displayed. You will need to select a profile to logon to the adapter. If you are already logged onto the adapter, no logon window will be displayed (the current logon will be used).

In the Open Text Editor window, select a file from the displayed list or manually enter a file name. If you manually enter a file name that does not exist, a new file by that name will be created in the location specified.

**Note:** Files on a CD or floppy can only be browsed. Writing to a CD or floppy is not supported.

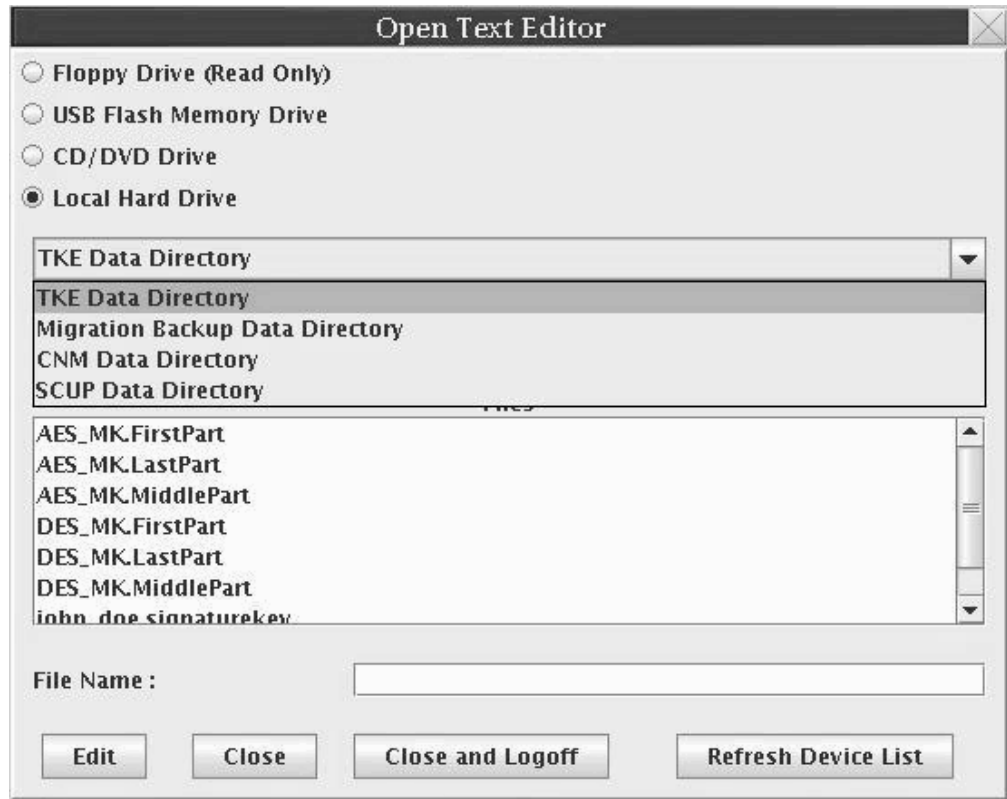


Figure 321. Edit TKE Files Task Window

You can edit the file within the edit text box and use File -> Save menu item to save the file.

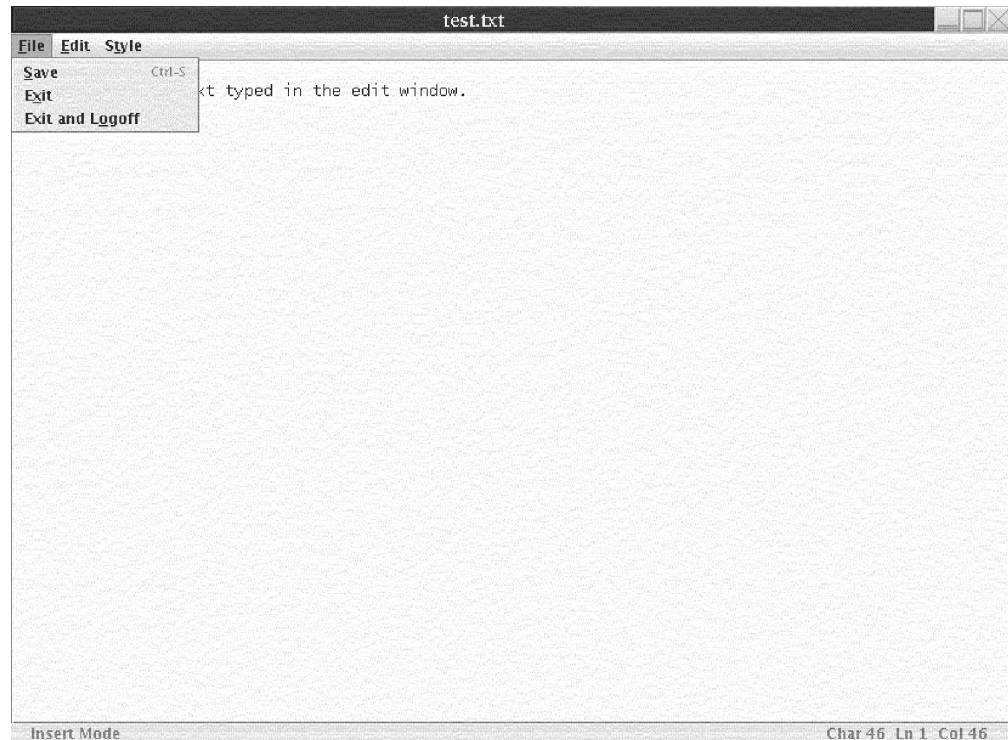


Figure 322. Editor - File menu items

#### Warnings:

1. 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 “TKE Media Manager” on page 313.
2. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

The editor provides options for Undo, Cut, Copy, Paste, along with Line Selection and Search/Replace.

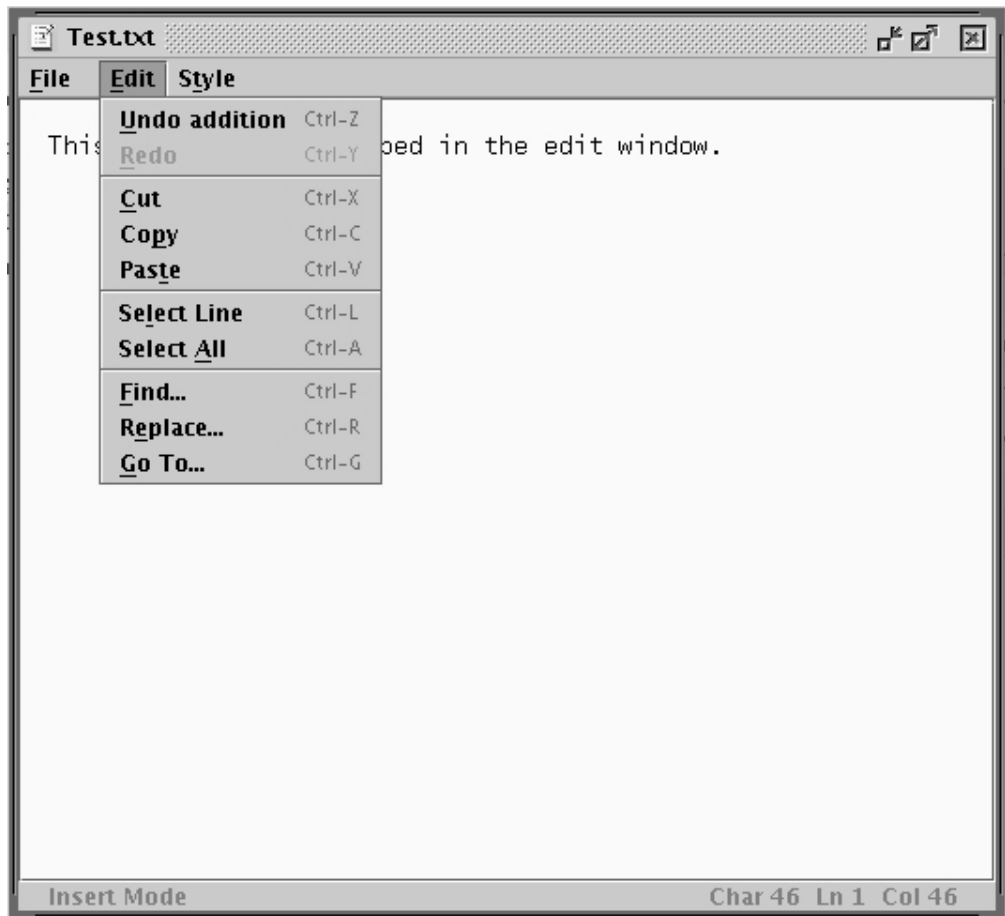


Figure 323. Editor - Edit menu items

In addition, there are options for Fonts, line wrap, and background.

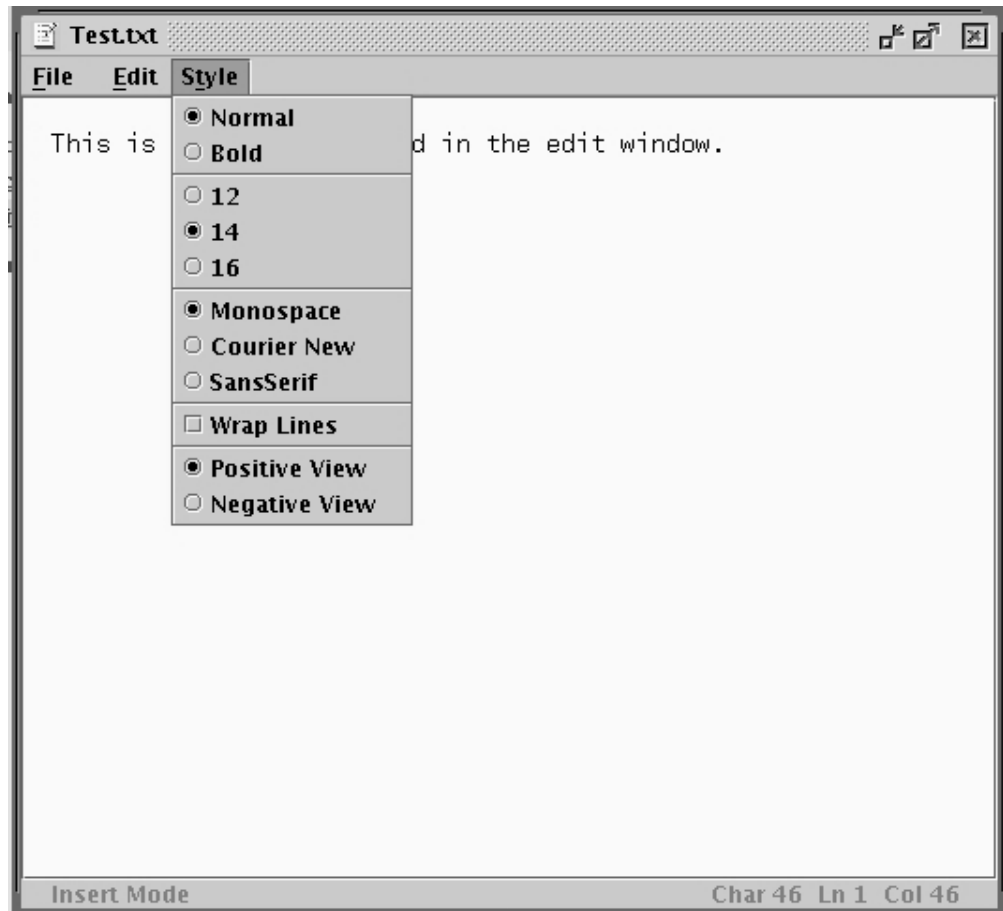


Figure 324. Editor - Style Menu Items

## Migrate Previous TKE Version to TKE 7.0

You must be signed onto the TKE Workstation Console in privileged mode using the ADMIN user name for this task. When TKE is initially started, you are not signed on to TKE in privileged mode. The following steps are used to sign on to TKE in privileged mode.

- Close the Trusted Key Entry Console.
- From the Welcome to the Trusted Key Entry Console screen select *Privileged Mode Access*
- From the Trusted Key Entry Console Logon screen enter the user name ADMIN and the password. (Default password is PASSWORD, but this can be changed by the user. See “Change Password” on page 325.)
- Press **Logon**.

This task is executed only when you have an existing TKE 3.0 through TKE 4.2 workstation and are migrating to TKE Version 7.0. 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 crypto adapter stored on the hard drive and you want them migrated, manually copy the files to the TKE Backup diskette.



**Notes:**

1. Authority signature keys, Master key parts, and Operational key parts cannot be migrated with this task.
2. 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 to TKE 7.0.

You will be requested to insert the TKE Backup diskette from the workstation you are migrating from. Click **OK**.

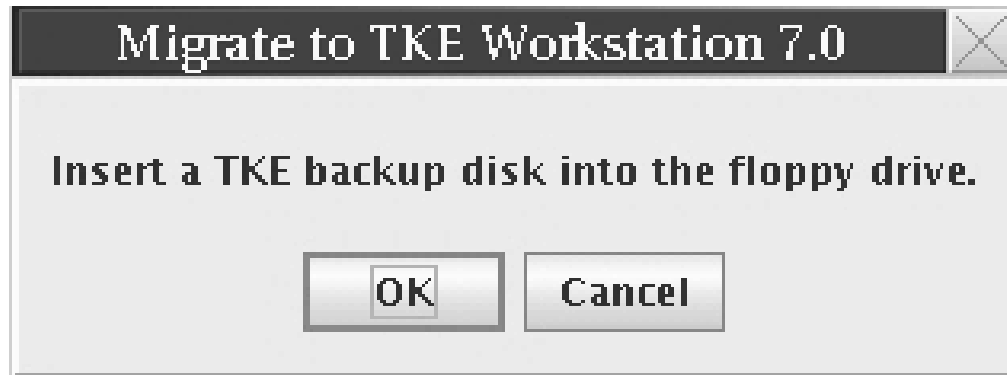


Figure 325. Migrate to TKE Workstation 7.0 - Backup floppy prompt

Files migrated will be displayed in the Migrate to TKE Workstation 7.0 window.

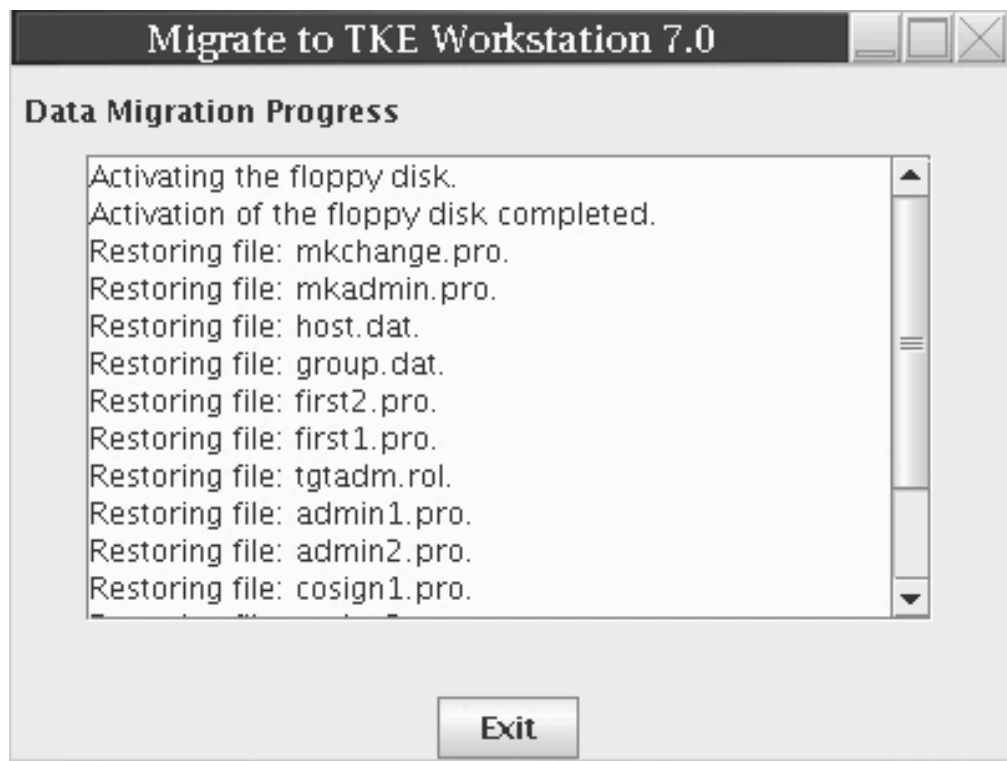


Figure 326. Migrate to TKE Workstation 7.0 - Data migration progress window

The task is complete when **Exit** is no longer greyed out.

## Smart Card Utility Program 7.0

This task is used for initializing smart cards, enrolling smart cards in a zone, and enrolling TKE workstations in a zone.

See Chapter 11, “Smart Card Utility Program (SCUP),” on page 253.

## TKE Audit Configuration Utility

This utility starts and stops auditing of security-relevant events on the TKE workstation, and controls what events will create audit records. You must log on with a console user name of AUDITOR to use this utility.

See “TKE Audit Configuration Utility” on page 175 for more information

## TKE Audit Record Upload Configuration Utility

This utility enables you to send TKE workstation security audit records to a System z host, where they will be saved in the z/OS System Management Facilities (SMF) dataset. Each TKE security audit record is stored in the SMF dataset as a type 82 subtype 29 record. This allows you to place TKE security audit records from 1 or more TKE Workstations into a single SMF data set on a target host. From the host, a security officer can use SMF features to analyze and archive the TKE security audit data.

See “TKE Audit Record Upload Configuration Utility” on page 183 for more information

## TKE File Management Utility

The TKE File Management Utility task allows you to manage files on diskette, CD/DVD, USB flash memory drive, 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 the **TKE File Management Utility**.

You must be logged on to the TKE workstation crypto adapter for this task. If you are not currently logged on to the adapter, a logon window is displayed. You will need to select a profile to log on to the adapter. If you are already logged onto the adapter, no logon window will be displayed (the current logon will be used).

When the TKE File Management Utility is opened the user is presented with the following task window.

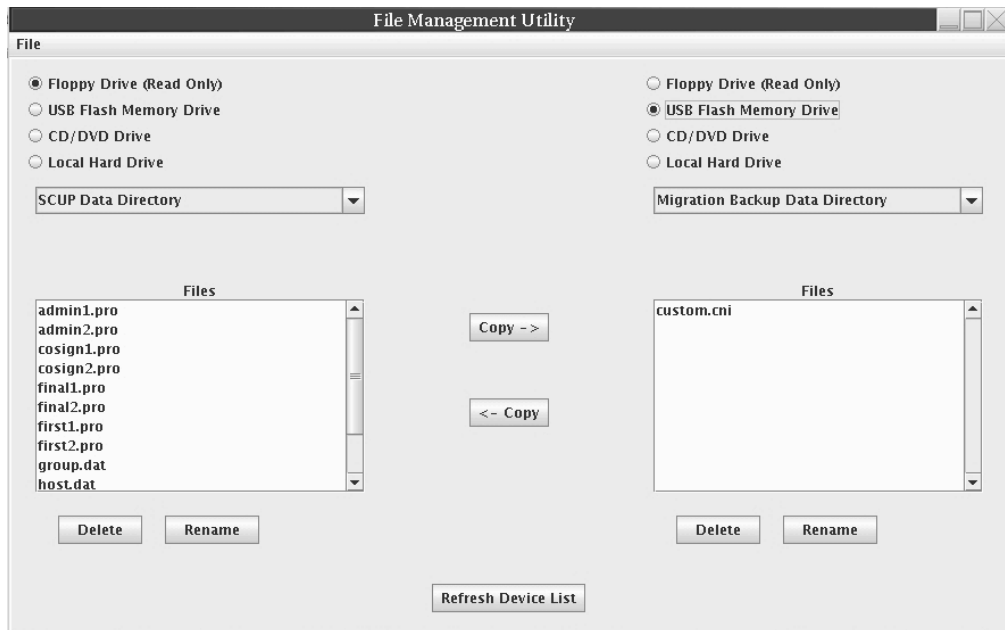


Figure 327. TKE File Management Utility Task Window

In the File Management Utility window, selecting the hard drive for either **Source** or **Target** will allow you to select from one of five data directories:

- TKE Data Directory
- Migration Backup Data Directory
- CNM Data Directory
- SCUP Data Directory
- Configuration Data Directory

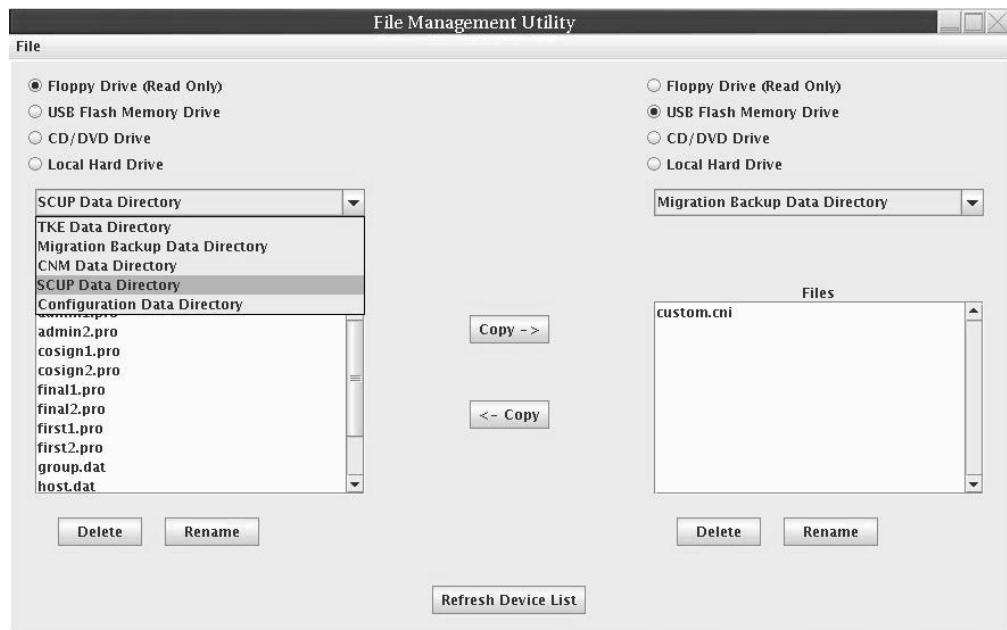


Figure 328. TKE File Management - Directory options

From the displayed list you can select a single file, numerous files, blocks of files, or the entire display.

- For a single file, just click on the desired file.
- To select more than one file click on the first file, hold down the Ctrl key and click on each additional file.
- To select a block of files, click on the first file, hold down the Shift key and click on the last file. All files between the two selected files will be selected.
- To select all the files, hold down the Ctrl key and type an 'a'.

Clicking on **Delete** will display a confirmation window.

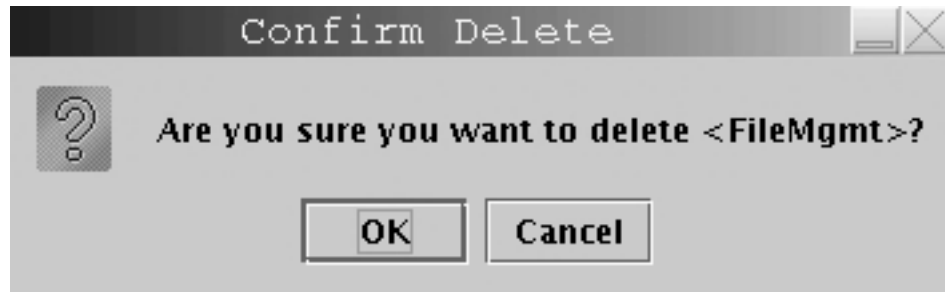


Figure 329. Delete Confirmation Window

Clicking on **Rename** will present a window for inputting a filename.

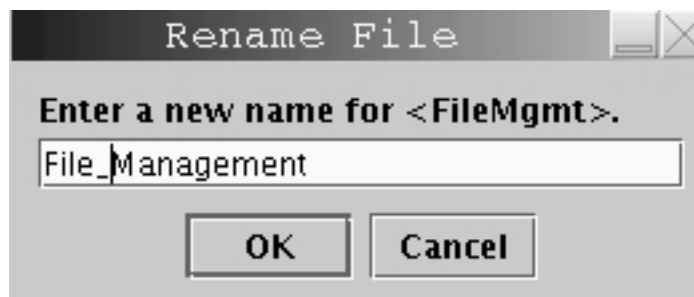


Figure 330. Window for Inputting a Filename

#### Warnings:

1. 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.
2. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

## TKE Media Manager

The TKE Version 7.0 workstation allows the use of these media devices:

- Floppy Disk (read-only)
- Compact Disc (read-only)
- DVD-RAM Disc
- USB flash memory drive

TKE 7.0 is shipped with two USB flash memory drives. One USB drive should be used for saving and backing up TKE related files in the TKE data directories, and the other USB drive should be used for backing up critical console data only.

To invoke this task, click on Trusted Key Entry and then click on TKE Media Manager.

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 **Cancel** to exit the TKE Media Manager.

**Note:** To execute the Migrate Previous TKE Version to TKE 7.0, the floppy drive must **NOT** be activated. If it is, the migrate will fail.

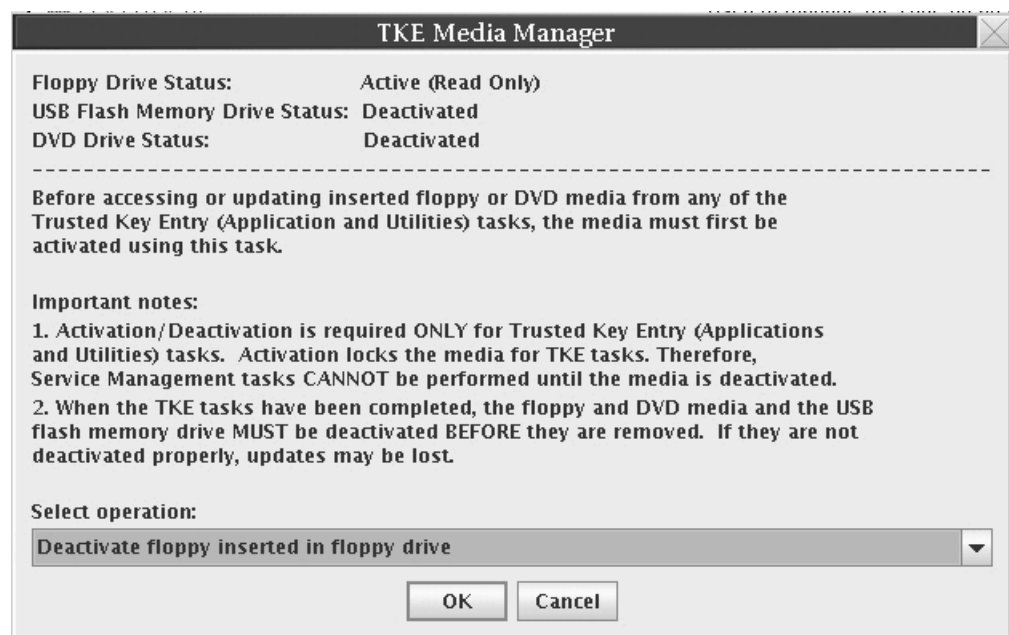


Figure 331. TKE Media Manager

**Important Notes:**

1. Activation / Deactivation are required only for Trusted Key Entry (Applications and Utilities) tasks. Activation locks the media for TKE tasks. Therefore, Service Management Tasks cannot be performed until the media is deactivated.
2. 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.
3. 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.
4. 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.

5. 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.

6. Trusted Key Entry (Applications and Utilities) tasks will recognize a USB flash memory drive and allow you to use the drive (if applicable for the task) only if the IBM supported drive:

- is plugged into a USB port on the TKE
- is 1GB or larger in size
- has been formatted with the Trusted Key Entry data label (TKEDATA)

Otherwise, Trusted Key Entry (Applications and Utilities) tasks will not recognize the drive and you will not be able to use it. Service Management Tasks behave differently and require different labels.

7. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages may be generated on the TKE workstation.

## 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 the TKE workstation crypto adapter.

To invoke this task, click on **Trusted Key Entry** and then click on **TKE Workstation Code Information**.

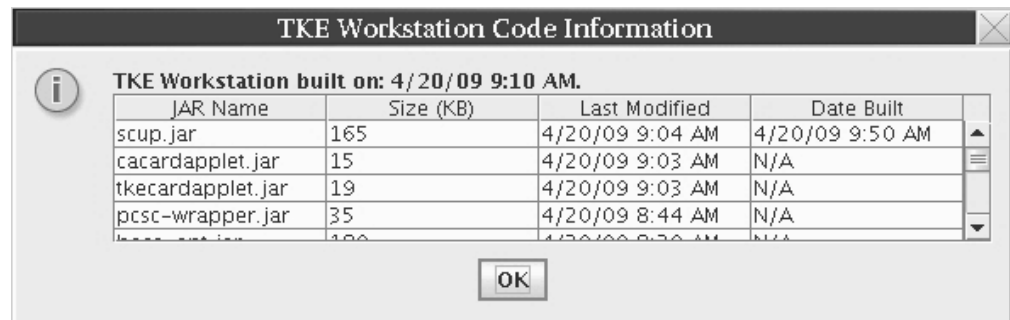


Figure 332. TKE Workstation Code Information window

## Configuration Migration

The TKE workstation provides tools to securely capture host crypto module configuration data to a file, and then reapply this data to another host crypto module or crypto module group. The data that can be securely captured includes roles, authorities, domain control settings, and master keys. These tools simplify the task of installing new or replacement host crypto modules, and can be used for backup and disaster recovery as well.

Two tools are provided: one that migrates only public configuration data (roles, authorities, domain control settings) and one that migrates all configuration data, including secret data, such as master key values. The protocol for migrating secret data is more complex than the protocol for migrating only public data, and requires the participation of several smart card holders.

To migrate only public configuration data, select the **Migrate IBM Host Crypto Module Public Configuration Data** application on the Trusted Key Entry menu. To migrate all configuration data, select the **Configuration Migration Tasks** application on the Trusted Key Entry menu.

### **Migrate IBM Host Crypto Module Public Configuration Data**

This utility allows you to save host crypto module configuration data (such as roles, authorities, and domain control settings) to a file on the TKE workstation, and to load a host crypto module with configuration data that was previously saved to a file. The utility simplifies the task of restoring the configuration when a host crypto module is replaced.

Only public configuration data is saved and loaded using the utility. Private data, such as the value of master key registers, is not accessed.

The utility supports the following four tasks:

- Collecting configuration data from a host crypto module and saving it in a file.
- Applying previously saved configuration data to a host crypto module.
- Collecting configuration data from one host crypto module and applying it to a different host crypto module in one operation.
- Reviewing previously saved configuration information in a file.

The source and target can be either a single host crypto module, or a crypto module group. When the source is a crypto module group, the master module of the group is located and used as the source of the saved configuration data. When the target is a crypto module group, all members of the group are updated with the configuration data read from a file.

To apply configuration data to a target host crypto module, you must load an authority signature key that allows roles and authorities, such as an authority signature key for an authority using the predefined INITADM role, to be created on the target. When applying configuration data to a crypto module group, the current authority signature key is checked before each member of the group is updated. If it does not have the required authority, you can load a different authority signature key.

The apply task creates and uses a temporary role and authority, which it removes when finished. In some cases, the temporary role cannot be removed. Because a temporary authority is used, 99 authorities are the most that can be migrated by the utility. If 100 authorities are defined in the source configuration, the authority at index 99 must be created on the target manually. A warning is displayed for these special cases.

Target crypto modules must support all cryptographic services of the source configuration. If you do not, the migration will not be allowed. The cryptographic services are displayed in the Details tab of the crypto module notebook and in the Details tab of the review task for the configuration migration utility. Similarly, target crypto modules must support all enabled domain controls in the source configuration. If they do not, the migration will not be allowed. If the source configuration includes a User Defined Extension with enabled domain controls, the User Defined Extension must be installed on all target crypto modules before the apply task is run. Target crypto modules must support 2048-bit authority signature keys, if these are present in the source configuration.

In the apply task, existing roles, authorities, and domain control settings on target crypto modules are removed and replaced with the configuration data from the file. Domains optionally can be zeroized before applying configuration data. This clears the master key registers. Only control domains can be zeroized. See Appendix C, “LPAR Considerations,” on page 291 for more information on control domains.

Files used by the configuration migration utility are created in, and read from, the Configuration Data Directory. The TKE File Management Utility can copy, rename, and delete files in this directory.

**Note:** The apply task reserves target host crypto modules for update. If a target host crypto module is already reserved for update by another application, the apply task will fail with an error message. The other application must be closed before the apply task can be run. In abnormal situations, it may be necessary to take the following steps to force release of the target host crypto module:

1. Start the main TKE application.
2. Open a crypto module notebook for the reserved host crypto module.
3. Select **Release Crypto Module** from the **Function** pull-down menu of the crypto module notebook. This forcibly releases the host crypto module.
4. Close the crypto module notebook to release the host crypto module.

## Configuration Migration Tasks

This application provides access to utilities used to securely migrate configuration data, including secret data such as master key values, from one crypto module to another. When you select this application, the Configuration Migration Tasks panel is displayed.

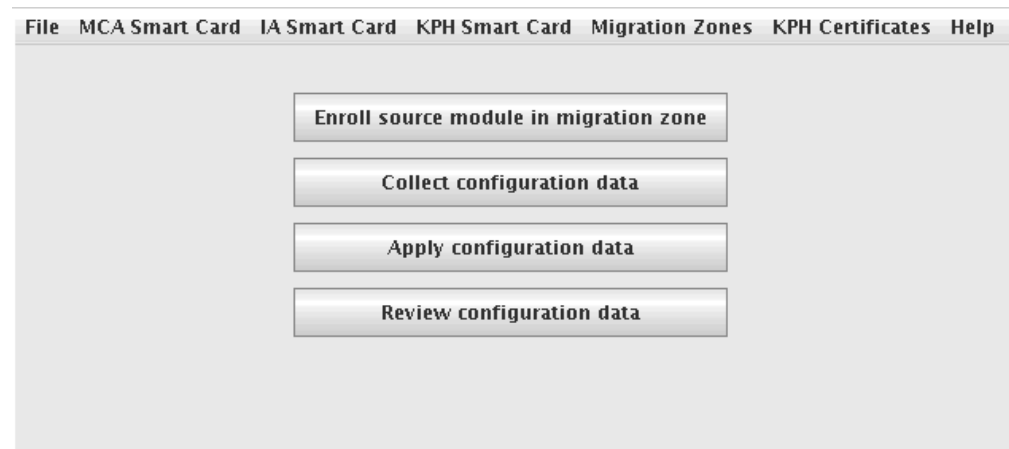


Figure 333. Configuration Migration Tasks panel

When migrating configuration data that includes master keys, the data in transit must be just as secure as if it were still resident inside a host crypto module. To accomplish this, the configuration data is encrypted using a 256-byte AES transport key, which is split into as many as 10 parts.

Three smart card types support configuration migration that includes master keys: Migration Certificate Authority (MCA) smart cards, Injection Authority (IA) smart cards, and Key Part Holder (KPH) smart cards.



The MCA smart card defines the migration zone. A migration zone is a set of smart cards that can work together to accomplish a migration task. When the migration zone is created, two policies are set indicating the number of smart cards needed for the tasks. The "M-of-N" policy indicates the number of parts the transport key is split into (N), and the number of parts needed to reconstruct the transport key (M). The maximum value for N is 10, and M must be less than or equal to N. The "K" policy indicates the number of IA smart cards required to apply configuration data to a target host crypto module. The maximum value for K is 10.

The MCA smart card is used to create IA and KPH smart cards. These smart cards become part of that migration zone, and can be used only in that migration zone. An unlimited number of migration zones can be created, but each migration zone has its own MCA smart card (and backup MCA smart cards) and set of IA and KPH smart cards.

The IA smart card authorizes application of configuration data to a target host crypto module or crypto module group.

The KPH smart card authorizes reconstruction of the transport key.

Before configuration data can be collected from a source host crypto module, the source host crypto module must be enrolled in the migration zone using the **Enroll source module in migration zone** task.

During the **Collect configuration data** task, the source host crypto module generates a transport key and splits it into "N" parts. (The key splitting algorithm allows the key to be recovered with only "M" of the original "N" parts. It does not matter which "M" parts are provided.) Each key part is encrypted using the public key from one of the "N" KPH smart cards. The source host crypto module captures the configuration data and encrypts it using the transport key. The encrypted configuration data and "N" encrypted key parts are returned.

During the **Apply configuration data** task, the target crypto module generates and returns a target decryption public key. It also returns an Outbound Authentication (OA) signature over the target decryption public key and the target host crypto module OA certificate chain.

"K" IA smart cards approve the target crypto module and target decryption public key, with help from the OA proxy (see "OA proxy" on page 321).

"M" KPH smart cards approve reconstructing the transport key, with help from the OA proxy (see "OA proxy" on page 321). KPH smart cards receive the transport key part that was encrypted with their public key, decrypt it using their private key, re-encrypt it using the target decryption public key, and return the result.

The target crypto module receives the encrypted configuration data and the "M" re-wrapped key parts. It decrypts the re-wrapped key parts using its private key, reconstructs the transport key, and decrypts and applies the configuration data.

When the target is a host crypto module group, the processing is done on each member of the target group.

#### **MCA Smart Card pull-down menu**

This menu allows you to display the contents of an MCA smart card, initialize and personalize an MCA smart card, backup an MCA smart card, or change the PIN on an MCA smart card.

### **IA Smart Card pull-down menu**

This menu allows you to display the contents of an IA smart card, initialize and enroll an IA smart card in a migration zone, personalize an IA smart card (set the PIN and description), unblock an IA smart card, or change the PIN on an IA smart card.

### **KPH Smart Card pull-down menu**

This menu allows you to display the contents of a KPH smart card, initialize and enroll a KPH smart card in a migration zone, personalize a KPH smart card (set the PIN and description), unblock a KPH smart card, or change the PIN on a KPH smart card.

### **Migration Zones pull-down menu**

The **Work with migration zones** function on this menu displays the list of migration zones known to the TKE workstation, and allows you to add or delete entries.

To minimize the number of times an MCA smart card must be inserted in a card reader during migration tasks, the TKE workstation maintains a list of known migration zones. The list is updated automatically when a new MCA smart card is created. If you need to add or remove migration zones from this list, you can use this function. To add a migration zone to the list, you need to insert the MCA smart card for the zone in the smart card reader and enter the PINs.

### **KPH Certificates pull-down menu**

The **Work with KPH certificates** function on this menu displays the list of KPH smart cards known to the TKE workstation, and allows you to add or delete entries.

To minimize the number of times KPH smart cards need to be inserted in a card reader during migration tasks, the TKE workstation maintains a list of known KPH certificates. The list is updated automatically when a new KPH smart card is created. If you need to add or remove a KPH certificate from this list, you can use this function. To add a KPH certificate to the list, you need to insert the KPH smart card in the smart card reader.

### **Enroll source module in migration zone**

This button starts a wizard that takes you through the steps to enroll a source host crypto module in a migration zone. The source crypto module must be enrolled in a migration zone before configuration data can be collected from it.

You need to know what migration zone you will use before running this wizard. If you need to define a new migration zone, you can use the **MCA Smart Card** pull-down menu to create a new MCA smart card. If you define a new migration zone, you also need to create IA and KPH smart cards to use in the zone.

To run this wizard, you need to load a signature key that permits the Certificate Insert operation on the source crypto module. If the signature key has insufficient authority, you will be given the opportunity to load a different signature key.

### **Collect configuration data**

This button starts a wizard that takes you through the steps to collect configuration data from a source host crypto module and save it in a file. Before running this wizard, you need to enroll the source host crypto module in the migration zone.

You need to know what migration zone and what KPH smart cards you will use before running this wizard. Only KPH smart cards for the selected migration zone can be used.

In this wizard you will indicate the set of domains you want to collect configuration data from. Configuration data for only those domains will be saved in the configuration data file. During the apply task, configuration data for domains not saved in the configuration data file will be set to the default value.

To run this wizard, you need to load a signature key that permits the Crypto Data Extract operation on the source host crypto module. If the signature key has insufficient authority, you will be given the opportunity to load a different signature key.

### **Apply configuration data**

This button starts a wizard that takes you through the steps to apply configuration data to a target host crypto module or target host crypto module group.

The wizard asks you to insert IA smart cards in the smart card reader and enter the PIN. The "K" policy for the migration zone specifies the required number of IA smart cards.

The wizard asks you to insert KPH smart cards in the smart card reader and enter the PIN. "M" of the "M-of-N" policy for the migration zone is the required number of KPH smart cards.

To run this wizard, you need to load a signature key that permits the Target Prepare and Crypto Target Inject operations on the target host crypto module or target host crypto module group. If the signature key has insufficient authority, you will be given the opportunity to load a different signature key. The default role and authority created when a host crypto module is initialized allow you to run these operations.

### **Review Configuration Data**

This button starts a wizard that allows you to select a configuration data file and display its non-secret contents.

The configuration data file contains both encrypted and unencrypted data. The unencrypted data includes information such as the serial number and code level of the source crypto module, the date and time the configuration data was collected, the migration zone and KPH certificates used, and what domains were collected. It includes a list of the roles and authorities collected, the domain controls for collected domains, and key register status and key hashes for collected domains.

### **Instructions For Migrating Key Material**

If you want to migrate configuration data including master key values, do the following:

1. Decide what migration zone you will use. If you will not use an existing migration zone, create an MCA smart card that defines the new zone. You will need to define the M-of-N and K policies. "N" is the number of parts the transport key is split into and must be between 1 and 10. "M" is the number of key parts required to reconstruct the transport key and must be between 1 and "N". "K" is the number of Injection Authorities required to approve applying configuration data on the target host crypto module and must be between 1 and 10. Creating a backup is recommended whenever you create a new MCA smart card.

2. Use the **Migration Zones** pull-down menu to check that the migration zone you want to use is listed. If not, add it.
3. If you are using a new migration zone, create IA and KPH smart cards. You must create at least "K" IA smart cards and "N" KPH smart cards for the migration zone, but you can create more.
4. Decide what KPH smart cards you will use. Use the **KPH Certificates** pull-down menu to check that the KPH smart cards you want to use are listed. If not, add them.
5. Run the **Enroll source module in migration zone** wizard to enroll the source host crypto module in the migration zone.
6. Run the **Collect configuration data** wizard to collect configuration data on the source host crypto module. The wizard will ask you to enter the media type and a file name for storing the encrypted configuration data.
7. Run the **Apply configuration data** wizard to apply configuration data on the target host crypto module. As the wizard runs, the IA and KPH smart card holders will be asked to insert their smart cards in a smart card reader and enter their PINs.

### OA proxy

When migrating configuration data from one host crypto module to another, the Injection Authority (IA) and Key Part Holder (KPH) smart cards verify outputs from the source and target host crypto modules. These outputs are signed by the host crypto modules' private keys, as part of a process called Outbound Authentication. In addition to the OA signature, the source and target host crypto modules provide their OA certificate chain, which terminates in an IBM root certificate.

Some IBM host crypto modules use key sizes for their OA signatures and certificate chains that are larger than what is supported by currently available smart cards. To handle these host crypto modules, the TKE workstation crypto adapter acts as an OA proxy for the smart cards. The TKE workstation crypto adapter verifies the OA signature and certificate chain and signs the output data using a specially-generated OA proxy signing key.

Each migration zone on the workstation needs to create an OA proxy certificate for this OA proxy signing key. The OA proxy certificate is created automatically when Migration Certificate Authority (MCA) smart cards are created, and when the migration zone is added or updated using the **Migration Zones** pull-down menu on the **Configuration Migration Tasks** panel.

If the TKE workstation crypto adapter is replaced or re-initialized, these OA proxy certificates are no longer valid. The migration zones listed under the **Migration Zones** pull-down menu will be removed automatically and must be re-registered using the MCA smart cards. Users who wish to change the OA proxy signing key can do so by manually deleting all migration zones found using the **Migration Zones** pull-down menu and then re-adding them.

---

## Service Management Tasks

The Service Management category contains tasks and utilities to service, manage, configure and maintain the TKE console. The tasks vary with the user name used to log on.

The following tasks are displayed if you are logged in as **Service**:

- "Analyze Console Internal Code" on page 322

- “Authorize Internal Code Changes” on page 323
- “Change Console Internal Code” on page 324
- “Offload Virtual RETAIN Data to Removable Media” on page 337
- “Transmit Console Service Data” on page 340
- “View Console Service History” on page 347
- “Rebuild Vital Product Data” on page 336

The following tasks are displayed if you are logged in as **Auditor**:

- “Archive Security Logs”
- “Log Offload Support for Customer Audit” on page 334
- “View Security Logs” on page 351

The following tasks are displayed for multiple user names:

- “Backup Critical Console Data” on page 323
- “Change Password” on page 325
- “Configure 3270 Emulators” on page 82
- “Customize Console Date/Time” on page 69
- “Customize Network Settings” on page 65
- “Customize Scheduled Operations” on page 326
- “Format Media” on page 331
- “Hardware Messages” on page 334
- “Lock console” on page 335
- “Manage Print Screen Files” on page 336
- “Network Diagnostic Information” on page 336
- “Save Upgrade Data” on page 338
- “Shutdown or Restart” on page 339
- “Users and Tasks” on page 343
- “View Console Events” on page 344
- “View Console Information” on page 345
- “View Console Tasks Performed” on page 349
- “View Licenses” on page 350

## Analyze Console Internal Code

This task is used to work with temporary internal code fixes or to debug problems if errors occur during a code fix install. This task should only be invoked by your IBM Customer Engineer or when directed by IBM Product Engineering. You must log on with a console user name of SERVICE to use this task.

For details, refer to *System z Service Guide for Trusted Key Entry Workstations*, GC28-6901.

## Archive Security Logs

This task saves the TKE console's default security log to a DVD-RAM or USB flash memory drive, then erases up to 80 percent of the oldest entries to make room for additional audit records. You must log on with a console user name of AUDITOR to use this task.

See “Archive Security Logs” on page 181 for more information.

## Authorize Internal Code Changes

This task is used to verify or change the setting that allows using this TKE workstation to perform installation and activation of internal code changes and other subsequent operations. This task should only be invoked by your IBM Customer Engineer or when directed by IBM Product Engineering. You must log on with a console name of SERVICE to use this task.

For details, refer to *System z Service Guide for Trusted Key Entry Workstations*, GC28-6901.

## 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 console data operation copies critical files from the Trusted Key Entry workstation to the Backup DVD-RAM or USB flash memory drive.

To invoke this task, log on as either ADMIN or SERVICE, click on Service Management and then click on Backup Critical Console Data.

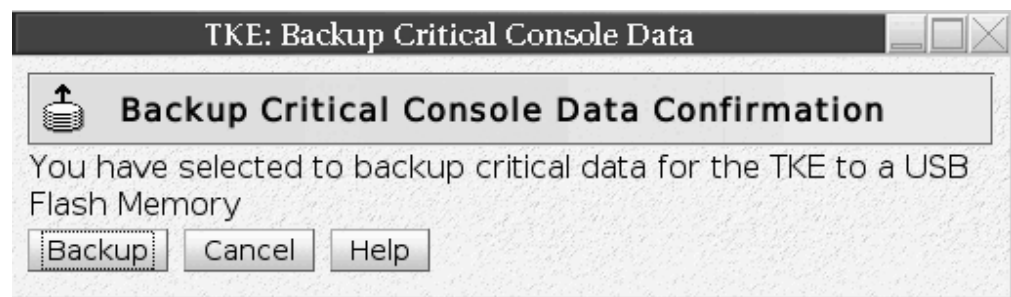


Figure 334. Backup Critical Console Data Window

The DVD-RAM or USB flash memory drive for the Backup Critical Console Data task must be formatted with a volume identification of ACTBKP, using the Format Media task.

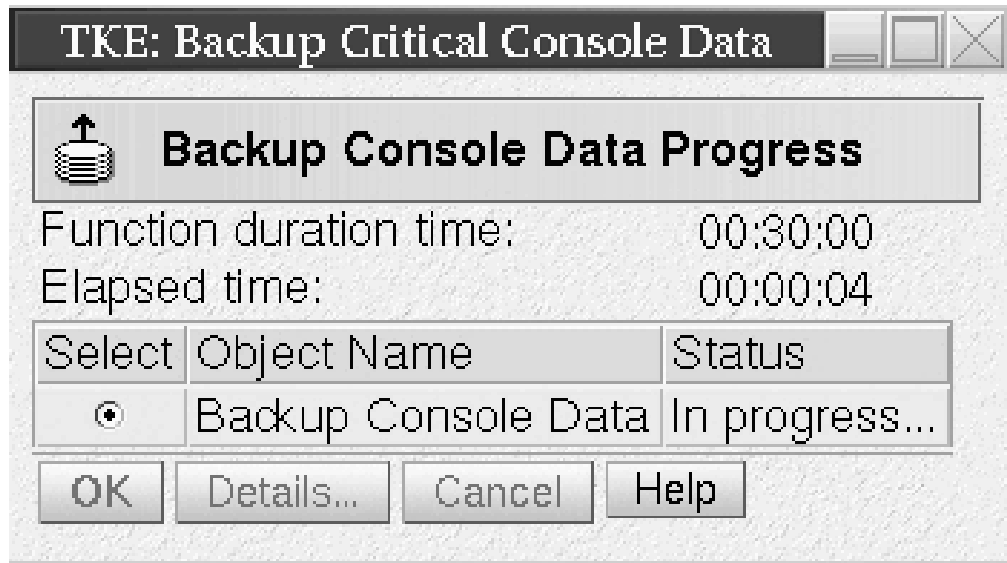


Figure 335. Backup Console Data Progress window - in progress

When the operation is complete the Status field of the Backup Critical Console Data window will be updated to indicate Success.

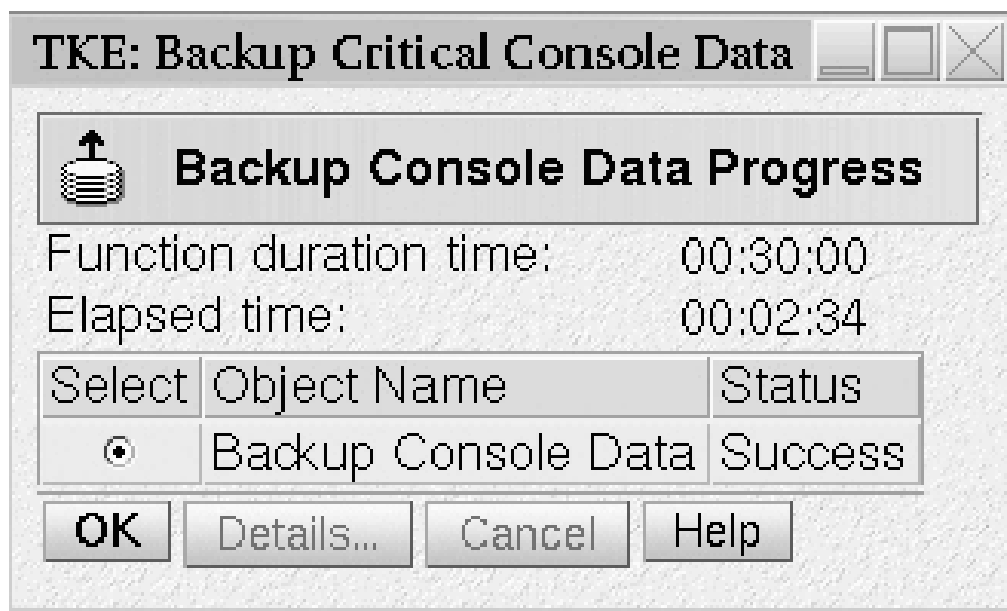


Figure 336. Backup Console Data Progress window - Success

## Change Console Internal Code

This task is used to work with internal code changes for the TKE workstation. Code changes can be retrieved, installed and activated, removed, and accepted. **This task should only be invoked by your IBM Customer Engineer or when directed by IBM Product Engineering.** You must log on with a console name of SERVICE to use this task.

For details, refer to *System z Service Guide for Trusted Key Entry Workstations*, GC28-6901.



## Change Password

The Trusted Key Entry workstation is shipped with predefined console user names and default passwords. The Change Password task appears in the Service Management tree when you are logged on as any of the following Privileged Mode Access user IDs.

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

After logging on the first time with one of these console user names, the user should change the password by selecting **Service Management** and **Change Password**.

A Change Password dialog displays.

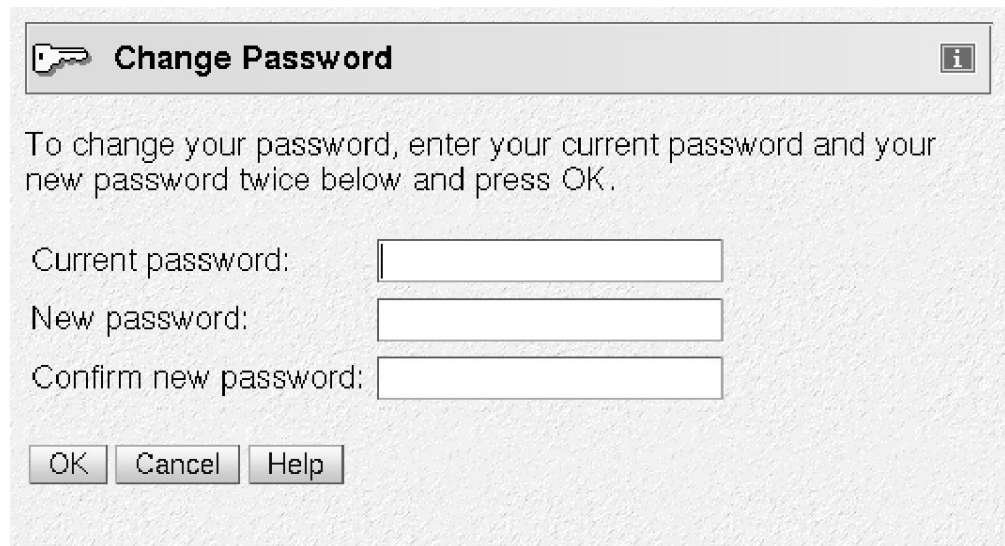
A screenshot of a 'Change Password' dialog box. The title bar contains a key icon, the text 'Change Password', and an information icon. The main text area says: 'To change your password, enter your current password and your new password twice below and press OK.' Below this are three input fields: 'Current password:', 'New password:', and 'Confirm new password:'. At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.

Figure 337. 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 if 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:** When the TKE workstation is migrated to a new version, the password values are preserved. They do not revert to the default values.

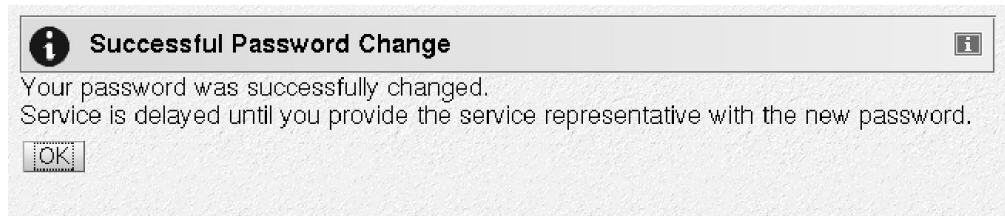
A screenshot of a 'Successful Password Change' dialog box. The title bar contains an information icon, the text 'Successful Password Change', and another information icon. The main text area says: 'Your password was successfully changed. Service is delayed until you provide the service representative with the new password.' At the bottom is a single button labeled 'OK'.

Figure 338. Change Password - Success



## Password Requirements

Password requirements for the user's password are as follows:

- Password must be between 4 and 8 characters.
- The password may be alphanumeric but may not contain any special characters.

No other restrictions, such as password history rules or repeating characters, apply.

## Customize Scheduled Operations

Use this task to customize a schedule for backing up critical hard disk information to DVD-RAM or USB flash memory drive. You must log on with a console user name of SERVICE or ADMIN to use this task.

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-RAM or USB flash memory drive used for the Backup Critical hard disk information must be formatted as ACTBKP. See "Format Media" on page 331 for details.



Figure 339. Customize Scheduled Operations Task Window

The Backup DVD-RAM or USB flash memory drive 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-RAM or USB flash memory drive.

Included on the Backup DVD-RAM or USB flash memory drive 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.

The Customize Scheduled Operations window displays.

Click Options on the menu bar to select:

- |                     |   |
|---------------------|---|
| <b>New</b>          | to create a new scheduled operation                               |
| <b>Delete</b>       | to remove a scheduled operation                                   |
| <b>Refresh</b>      | to update the current list of scheduled operations                |
| <b>Select All</b>   | to choose all scheduled operations currently displayed            |
| <b>Deselect All</b> | to deselect all scheduled operations that were currently selected |
| <b>Exit</b>         | to exit this task   |

When **New** is selected from the Options menu, the Add a Scheduled Operation screen is displayed.

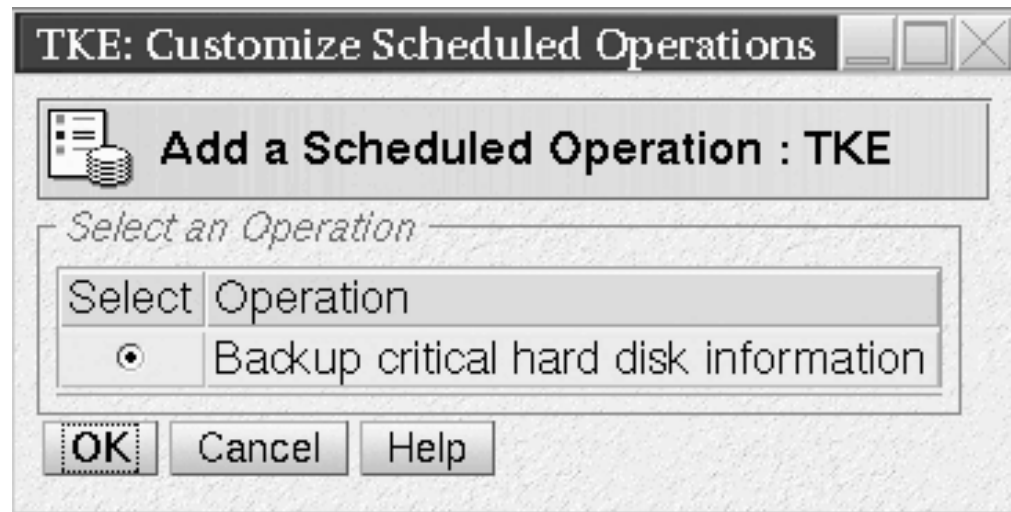


Figure 340. Customize Scheduled Operations - Add a Scheduled Operation window

Clicking on **OK** displays a screen in which the Time, Date, and Repetition of the operation can be specified.

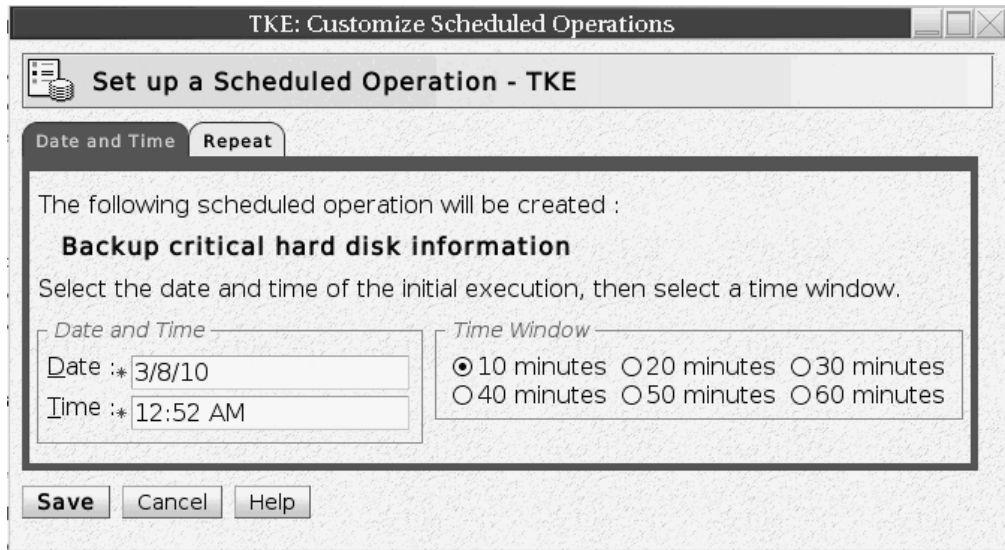


Figure 341. Customize Scheduled Operations - Set Date and Time window

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 and Time, and have 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.

**TKE: Customize Scheduled Operations**

**Set up a Scheduled Operation - TKE**

**Date and Time Repeat**

The following scheduled operation will be created :

**Backup critical hard disk information**

*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 1 to 26 weeks  
Repetitions : 1 1 to 100  
☐ Repeat indefinitely

**Save Cancel Help**

Figure 342. Customize Scheduled Operations - Set Repetition of operation

After all the information is selected, press **Save** 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
<input type="checkbox"/>	pokpd16	Jun 22, 2005	9:42:47 AM	Backup critical hard disk information	1

Figure 343. Completion Window for Adding Scheduled Operation

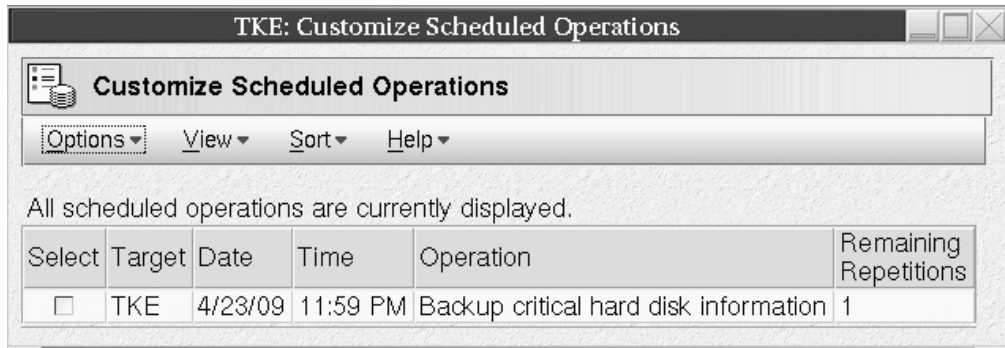


Figure 344. Customize Schedule Operations

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

Used to display schedule information for the selected scheduled operation. For TKE, Object and Operation are not relevant.

#### New Time Range

Used to specify a definite time range (days, weeks, months, or displayed scheduled operations) for the selected operation.

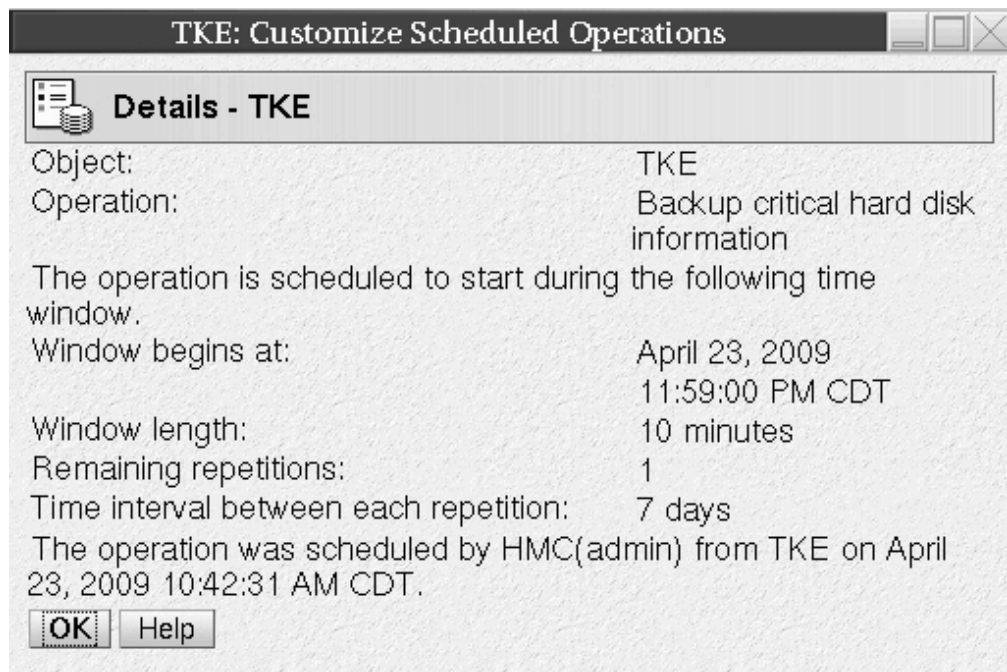


Figure 345. Details View of Scheduled Operation



Figure 346. New Time Range window for Scheduled Operation

## Format Media

The Format Media task is used to format DVD-RAMs, USB flash memory drives, and diskettes only.

**Warning:** Prior to formatting any media, ensure that the applicable floppy, DVD-RAM drive, or USB flash memory drive is deactivated in the TKE Media Manager. If the media is not deactivated, the format will fail.

1. To invoke this task, click on **Service Management** and then click on **Format Media**.

The Format Media dialog is displayed.



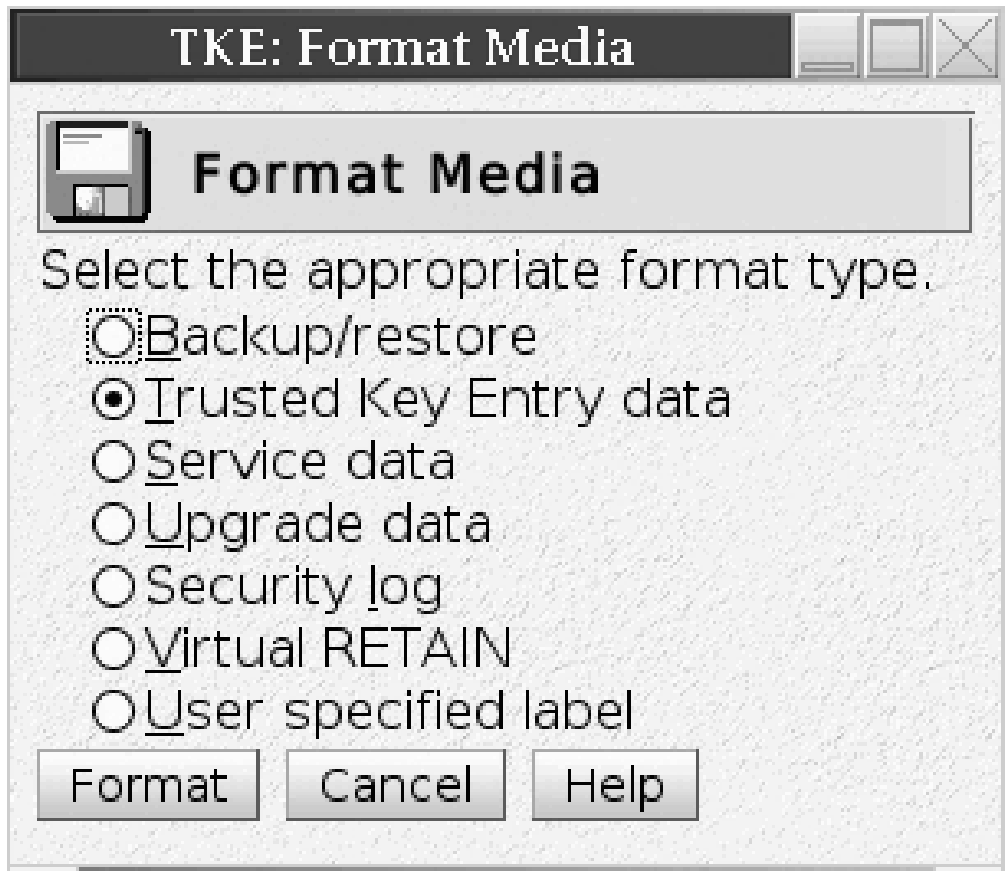


Figure 347. Format Media Dialog

2. In the Format Media dialog, select the appropriate format type from the list. The format type you select will determine how the media is formatted and what label is written on it.

Table 18. Allowable labels when formatting DVD-RAM or USB flash memory drive

Format	Label	Description:
Backup/restore	ACTBKP	This formatted media is used in the Backup Critical Console Data task and the Customize Scheduled Operations task. To choose this format type, select Backup/restore.
Trusted Key Entry data	TKEDATA	This formatted media is used in the TKE applications and tasks. TKE data can be related to TKE, SCUP, CNM, or user defined. To choose this format type, select Trusted Key Entry data
Service data	SRVDAT	This formatted media is used in the Transmit Console Service Data task. To choose this format type, select Service data.

Table 18. Allowable labels when formatting DVD-RAM or USB flash memory drive (continued)

Format	Label	Description:
Upgrade data	ACTUPG	This formatted media is used in the Save Upgrade Data task. To choose this format type, select Upgrade data.
Security log	ACTSECLG	This formatted media is used in the Archive Security Logs or the Log Offload Support for Customer Audit tasks. To choose this format type, select Security log.
Virtual RETAIN	VIRTRET	This formatted media is used in the Offload Virtual RETAIN Data to DVD-RAM task. To choose this format type, select Virtual RETAIN.
User specified label.		

- In the Format Media dialog, click the **Format** command button. If you selected "User specified label", a dialog will prompt you for a label name. Type in the name, and click the **Format** command button.  
The Select Media Device dialog is displayed.



Figure 348. Select Media Device

- In the Select Media Device dialog, select the radio button for the desired device, and click the **OK** command button.  
A confirmation dialog displays a warning that the format media action will remove all data on the removable media selected.
- If you wish to continue the format media action, click the confirmation dialog's **Yes** command button.  
An informational window will display when the Format Media action has completed.



## Log Offload Support for Customer Audit

This task copies the TKE console's default security log to an ASCII format file on a DVD-RAM or USB flash memory drive. The default security log on the TKE console is not changed. You must logon with a console user name of AUDITOR to use this task. See "Format Security Logs to DVD-RAM" on page 182 for more information.

## Hardware Messages

This task displays messages about hardware activity on the Trusted Key Entry workstation.

When the green 'Status OK' icon (lower left corner of the TKE Console), changes to the blue 'Status Messages' icon it indicates that a Hardware Message is pending. The message can be viewed by clicking on the Status icon or by invoking this task.

To invoke the Hardware Messages task, click on Service Management and then click on Hardware Messages.

Messages are listed from the oldest to the newest message, with the oldest message displayed at the top of the list.

### Date

Displays the date the message was sent.

### Time

Displays the time the message was sent.

### Message Text

Displays the message.

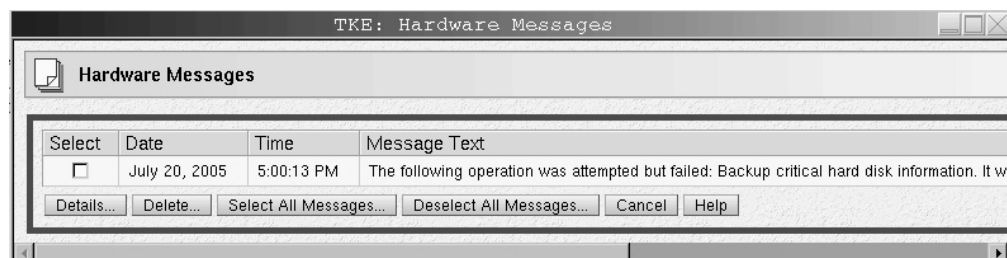


Figure 349. Hardware Messages window

Hardware messages notify you of events that involve or affect the TKE workstation hardware or internal code.

To promptly view, act on, or delete messages:

1. Select a message, then click Details to display details.

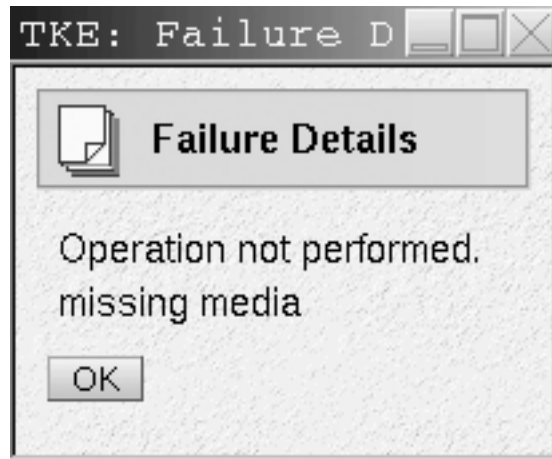


Figure 350. Hardware Messages - Details Window

2. If messages details are available and intervention is required, perform the action recommended in the details.
3. To delete the selected message, click Delete.

A message is displayed until an action causes it to be deleted.

Some messages are deleted automatically after the message or its details are displayed, if available. These messages generally provide information only, and are deleted automatically because no further action is required.

Messages that require further action provide message details that include a recommended action. The message and its details remain available until it is deleted manually. This allows reviewing the message details to assist intervention. But the message must be deleted when its information is no longer required.

Deleting messages provides greater assurance that new messages will be displayed as they are received.

## Lock console

This task is used to allow customers to lock the TKE console. The Lock Console task appears in the Service Management tree when you are logged in as ADMIN, SERVICE, AUDITOR, or TKEUSER.

To invoke this task, click on Service Management and then click on Lock Console.

This task prompts the user for a password in order to lock the TKE console. Passwords can be up to any 12 characters except a space, backspace (\), \*, and -. If any of these characters are entered you will receive an error message.

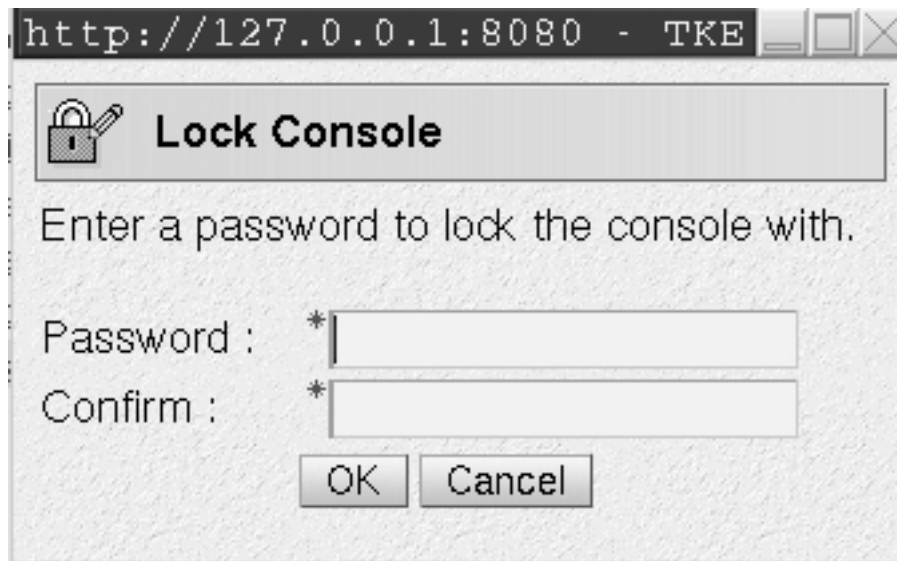


Figure 351. Prompt for Password

The user must enter a password and confirm it.

Once you have entered a password value, confirmed it, and selected **OK**, a screen saver will lock the TKE Console. To unlock the console, move the mouse or touch the keyboard and you will be prompted for the password.

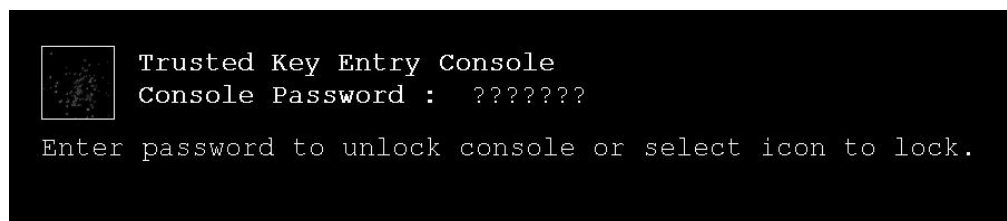


Figure 352. Prompt to Unlock Console

At the Console Password prompt, each keystroke appears as a question mark on the password prompt. If the correct password is entered, the user returns to the TKE console. If an incorrect password is entered, an error message will be displayed informing the user.

## Manage Print Screen Files

The Manage Print Screen Files task can be used to print individual windows on the TKE console to a file or to print the entire screen. Print screen files can be viewed, copied to floppy, DVD/RAM, or USB flash memory drive and deleted using this task.

## Network Diagnostic Information

The Network Diagnostic Information task displays network information such as TCP/IP addresses and Ethernet settings. It can test network connections by sending an echo request (ping) to a remote host.

## Rebuild Vital Product Data

This task is used to rebuild the Vital Product Data for the TKE machine.

**Note:** This task will only be displayed when logged on with the SERVICE user name.

## Offload Virtual RETAIN Data to Removable Media

**Note:** This task will only be displayed when logged on as the SERVICE id.

This task is used to select, by problem number, specific virtual RETAIN data to offload to DVD-RAM or a USB flash memory drive.

To invoke this task, click on Service Management and then click on Offload Virtual RETAIN Data to removable media.

**Note:** The removable media must be formatted with volume identification label VIRTRET, using the Format Media task.

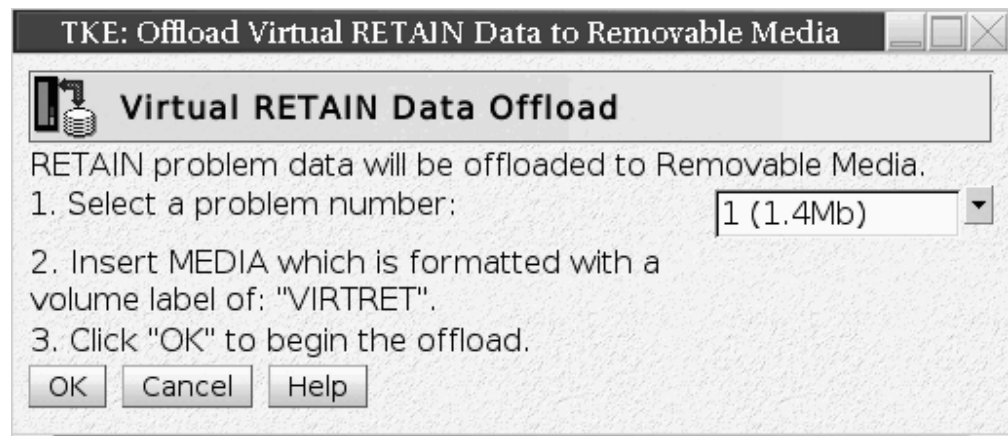


Figure 353. Virtual RETAIN Data Offload Window

In the Virtual RETAIN Data Offload window, select the Problem Number and click OK. The selected virtual RETAIN data is off-loaded to the removable media.

When the virtual RETAIN data is offloaded successfully, a message is displayed indicating the offload was successful.

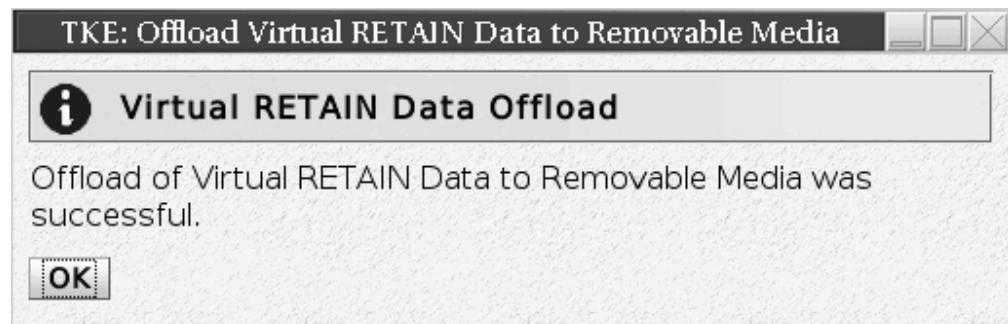


Figure 354. Successful Offload of Data

If you insert removable media that has not been formatted or that has the wrong label, an error message is displayed.

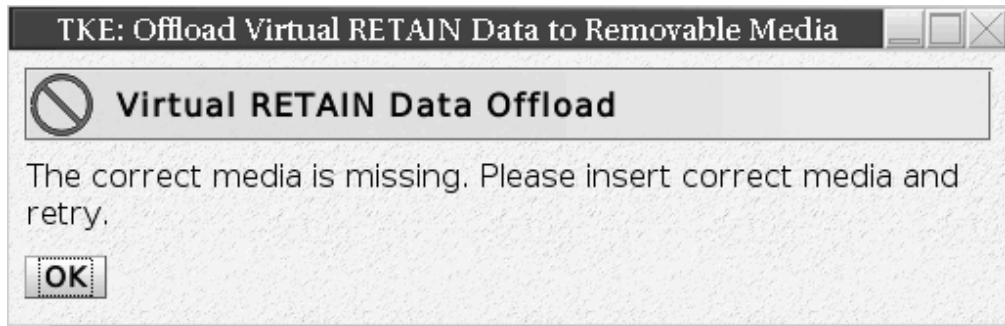


Figure 355. Virtual RETAIN Data Offload Incorrect Media Error

## 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. You must log on with a console user name of ADMIN or SERVICE to use this task.

All data pertinent to the TKE workstation (for example, TKE related data directories, emulator sessions, and TCP/IP information) will be saved. Upgrading the Trusted Key Entry workstation requires saving its upgrade data before installing new EC or MES code, then restoring the upgrade data afterwards.

To invoke this task, click on Service Management and then click on Save Upgrade Data.

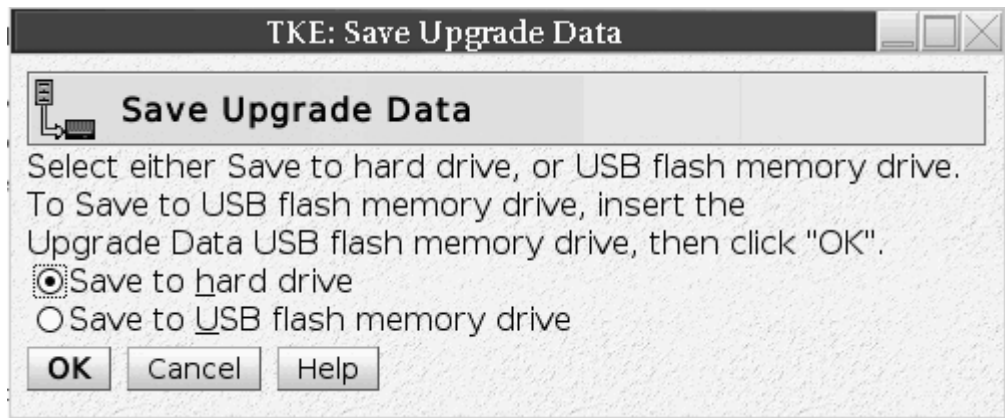


Figure 356. Save Upgrade Window

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 or USB flash memory drive for this task must be formatted with a volume identification label of ACTUPG, using the Format Media task.

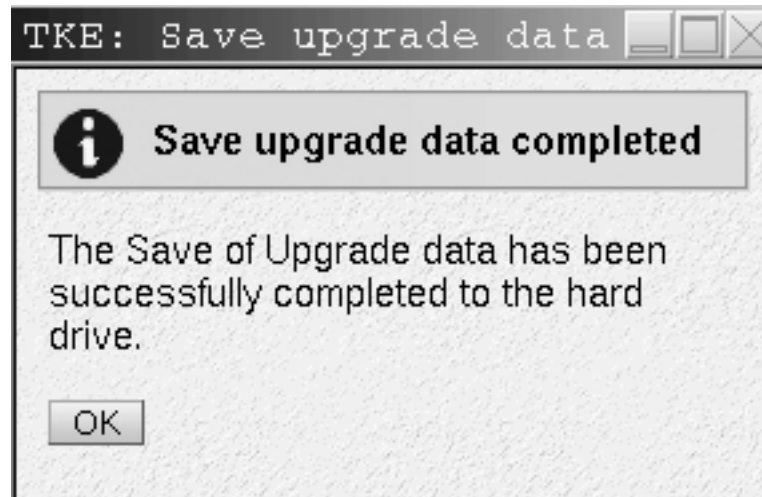


Figure 357. Save Upgrade Success Window

**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.

The Shutdown or Restart dialog displays.

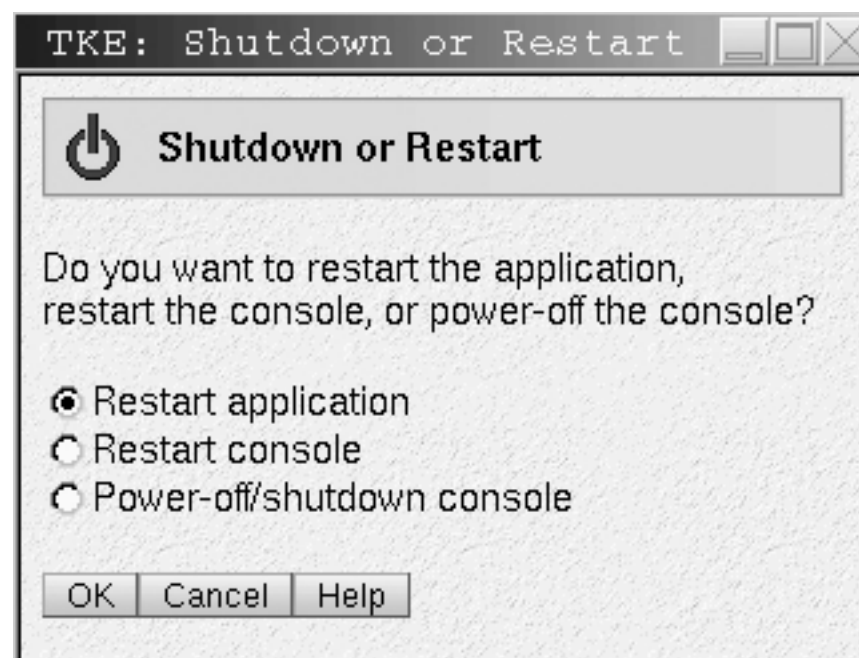


Figure 358. Shutdown or Restart Task Window

Select one of the following options from the dialog and press **OK**.



### Restart Application

To close the Trusted Key Entry workstation and restart the application, select Restart application.

### Restart Console

To close the Trusted Key Entry workstation, perform a system power-on reset, and restart the console, select Restart console.

### Power Off/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. Press **Yes** to continue.

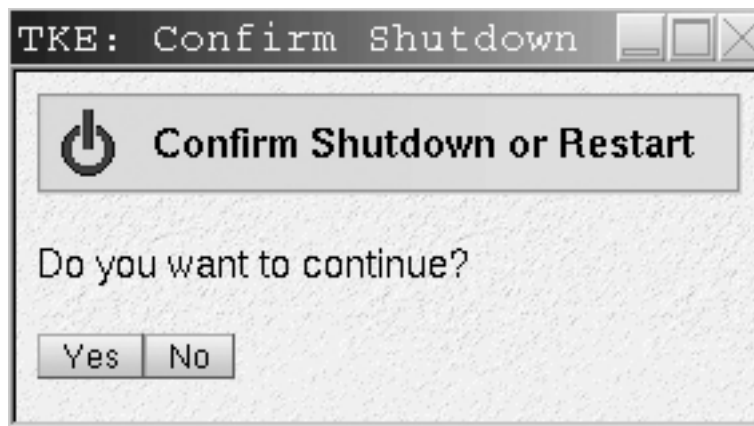


Figure 359. Confirmation Window

## Transmit Console Service Data

This task is used to select the types of service data and the method to send the data to aid in the problem determination. You must log on with a console user name of SERVICE to use this task.

To invoke this task, click on Service Management and then click on Transmit Console Service Data.

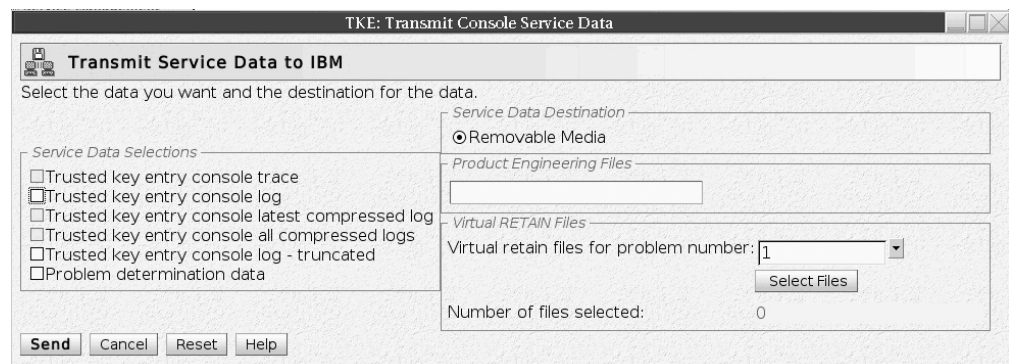


Figure 360. Transmit Console Service Data

Service data is a set of program and event traces and storage dumps. The data in the traces and the contents of storage assists in servicing the system.

Use the Transmit Console Service Data window only when directed by your service representative or 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**

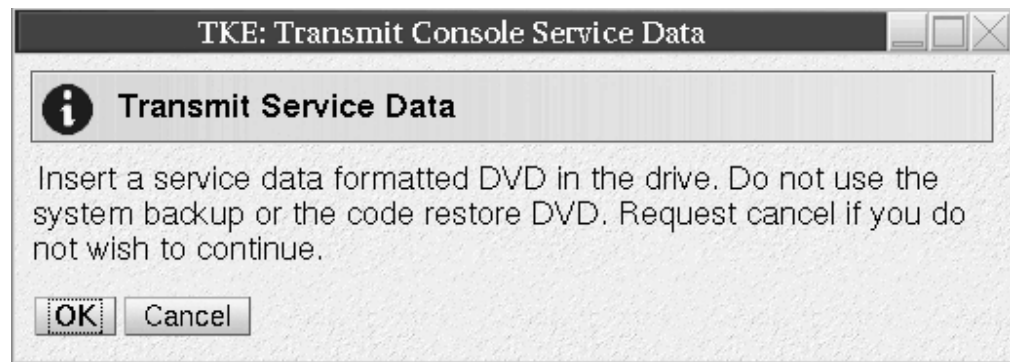
Use this topic to specify how your service data is sent to IBM.

#### **Virtual RETAIN Files**

Use this topic to copy to diskette, DVD-RAM, or USB flash memory drive selected virtual RETAIN files for the specified problem number.

**Note:** You can select and copy virtual RETAIN files to diskette, DVD-RAM, or USB flash memory drive for only a single problem number at a time.

**Note:** When using a DVD-RAM or USB flash memory drive for service data it must first be formatted specifically for Service Data. See “Format Media” on page 331 for details.



*Figure 361. Transmit Console Service Data Task Window for DVD-RAM*

Successful completion will present the following window.



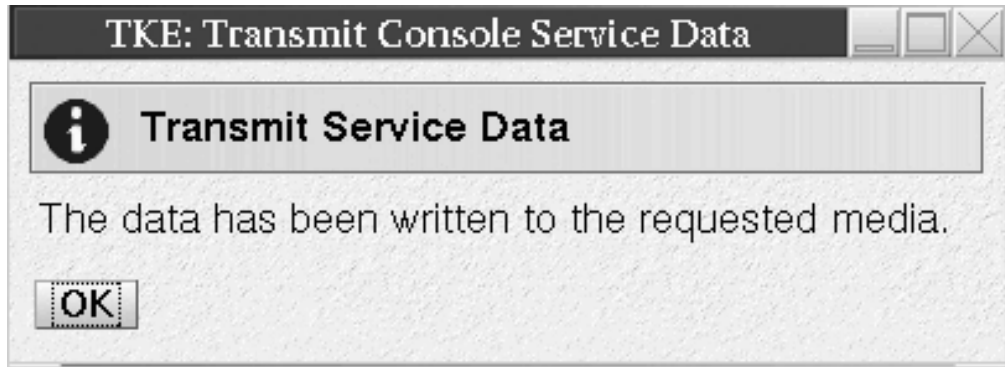


Figure 362. Transmit Console Service Data - Successful completion

For Virtual RETAIN Files, enter the problem number in the Virtual RETAIN Files for Problem Number field and click on Select Files.

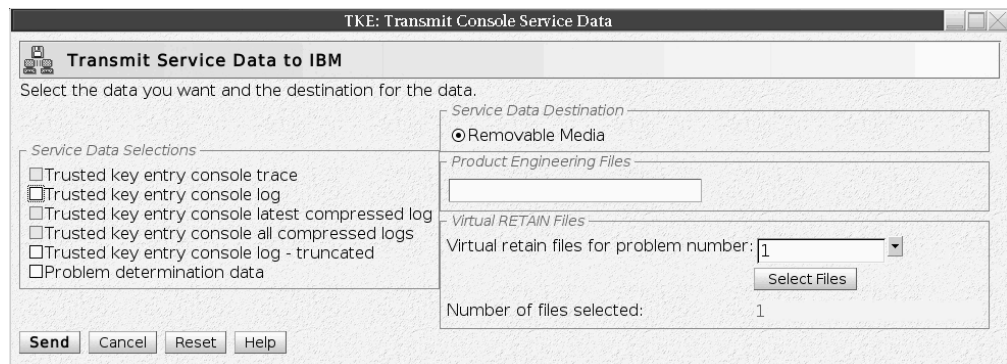


Figure 363. Update Problem Number for Virtual RETAIN File

Select the applicable Virtual RETAIN Files and click OK.

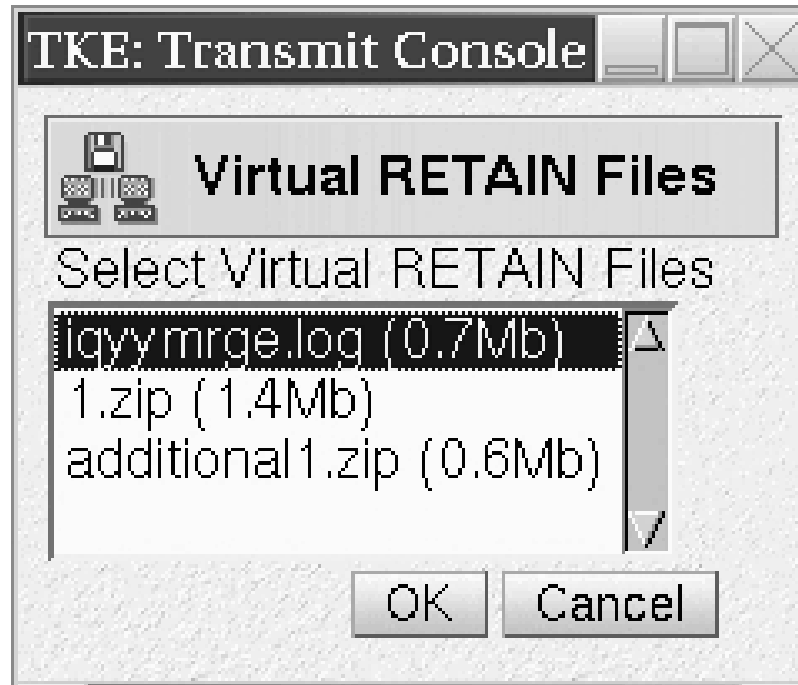


Figure 364. Select the Virtual RETAIN Files

Select the Service Data Destination, Diskette, DVD-RAM, or USB flash memory drive 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.

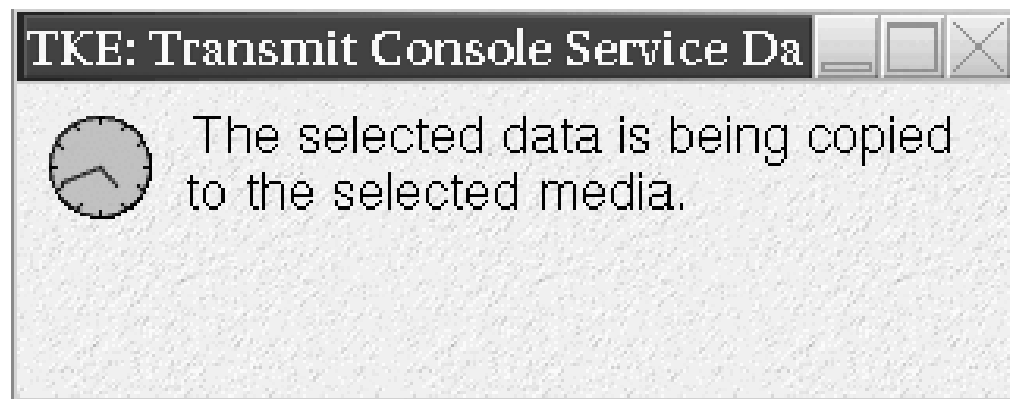


Figure 365. Copying Data to Selected Media

An information window will display when the data has been written to the required media.

## Users and Tasks

The Users and Tasks task window displays the users and running tasks on the TKE Workstation and allows you to Switch to a currently running task or Terminate a task that perhaps 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 4.1.0 task. If you attempt to terminate CLU from this task you will be presented with a window stating 'You cannot terminate the CCA CLU Utility from the Login Details and Task menu. If you need to terminate CLU you must use the Exit option of the CLU Utility.'

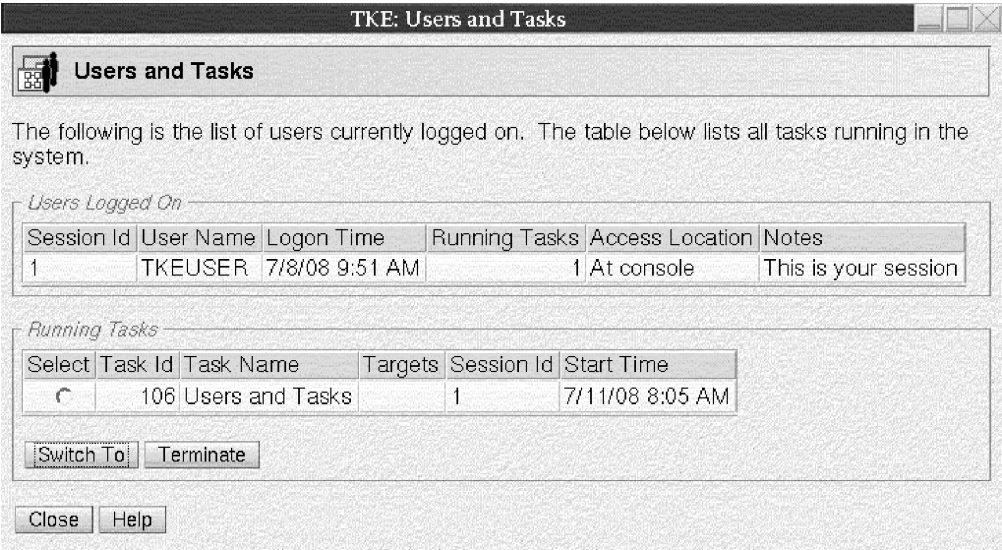


Figure 366. Users and Tasks Window

## View Console Events

This task displays console events logged by the Trusted Key Entry workstation.

To invoke this task, click on Service Management and then click View Console Events.

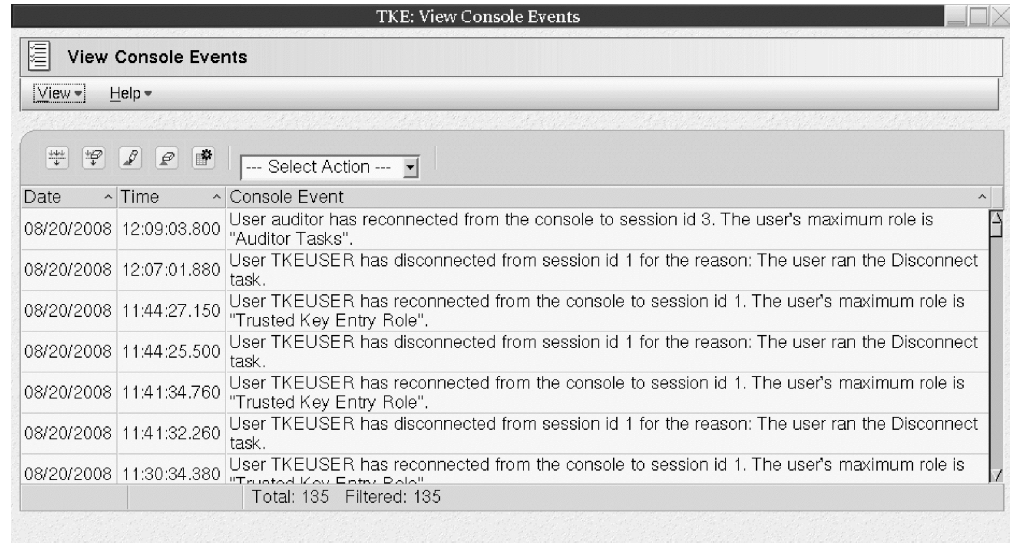


Figure 367. View Console Events Window

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 as follows:

- 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 for problem determination.

To invoke this task, click on Service Management and then click on View Console Information.

The View Console Information window is displayed.

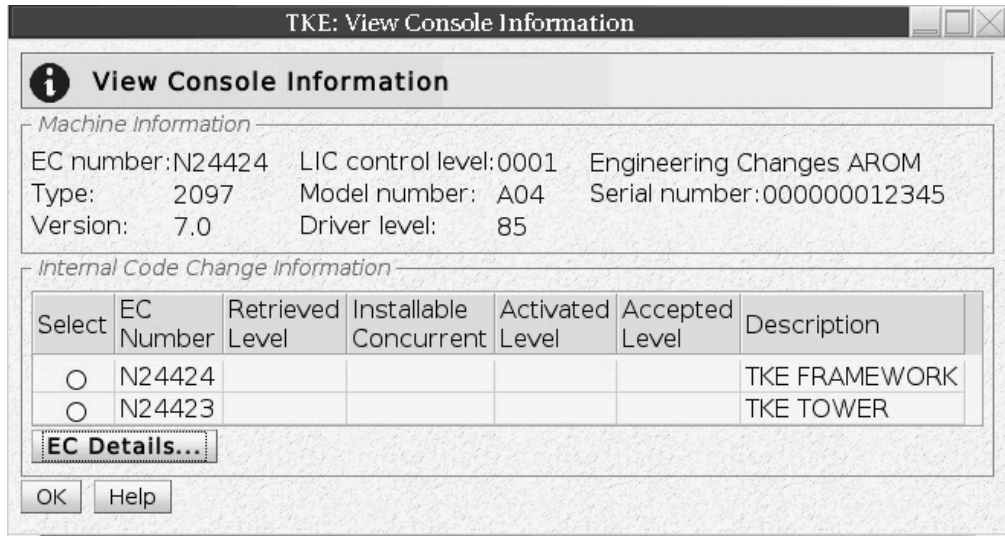


Figure 368. View Console Information Window

For additional information about an internal code change, select an EC number, then click **EC Details**.

The Internal Code Change Details window is displayed.

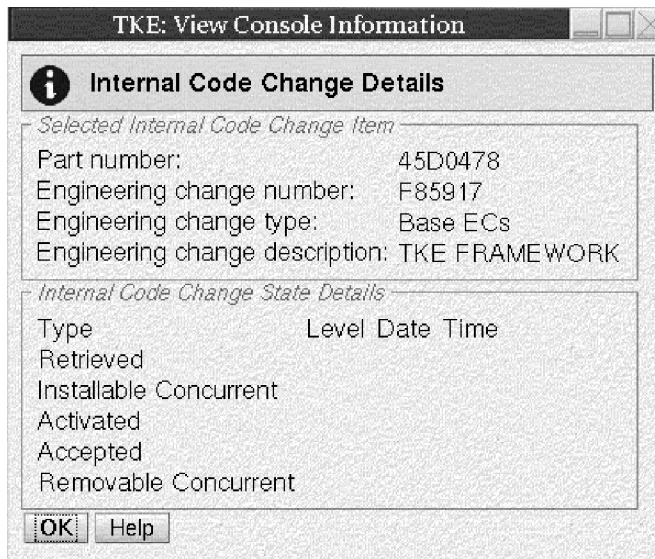


Figure 369. Internal Code Change Details Window

The View Console Information window contains the following information.

#### EC Number

Displays the engineering change (EC) number of the internal code change.

#### Retrieved Level

Displays the internal code change level that was most recently copied to the console, making it available for installation.

#### Installable Concurrent

Displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change



levels retrieved for this console, from the current installed level up to and including the installable concurrent level, without disrupting the operations of this console.

#### **Activated Level**

Displays the internal code change level that was most recently activated as a working part of the licensed internal code of the console.

#### **Accepted Level**

Displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the console.

#### **Removable Concurrent**

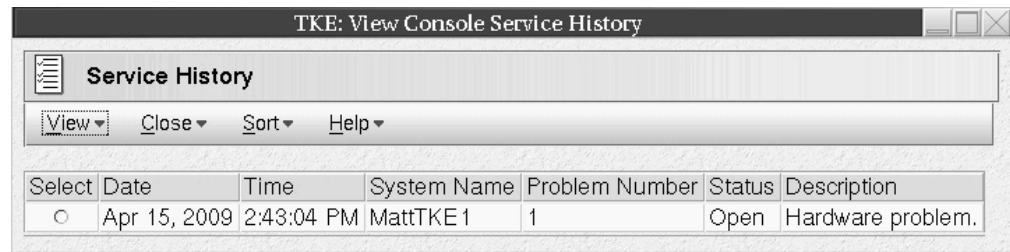
Displays the lowest installed internal code change level that can be removed such that the remaining installed change level can be activated concurrently. That is, you can remove all change levels installed for this console, from the current installed level down to and including the removable concurrent level, without disrupting the operations of this console.

## **View Console Service History**

The View Console Service History is used to review or close problems that are discovered by Problem Analysis. A problem is opened when Problem Analysis determines service is required to correct a problem.

To invoke this task, click on Service Management and then click on View Console Service History.

The View Console Service History window is displayed.




*Figure 370. 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.

http://127.0.0.1:8080 - TKE: Service Histor

 **Service History**

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

Figure 371. Problem Summary

- The **Problem Analysis Panel** shows System Name, Date and Time, Problem Description, Corrective Actions that a user can take and impact of repair.

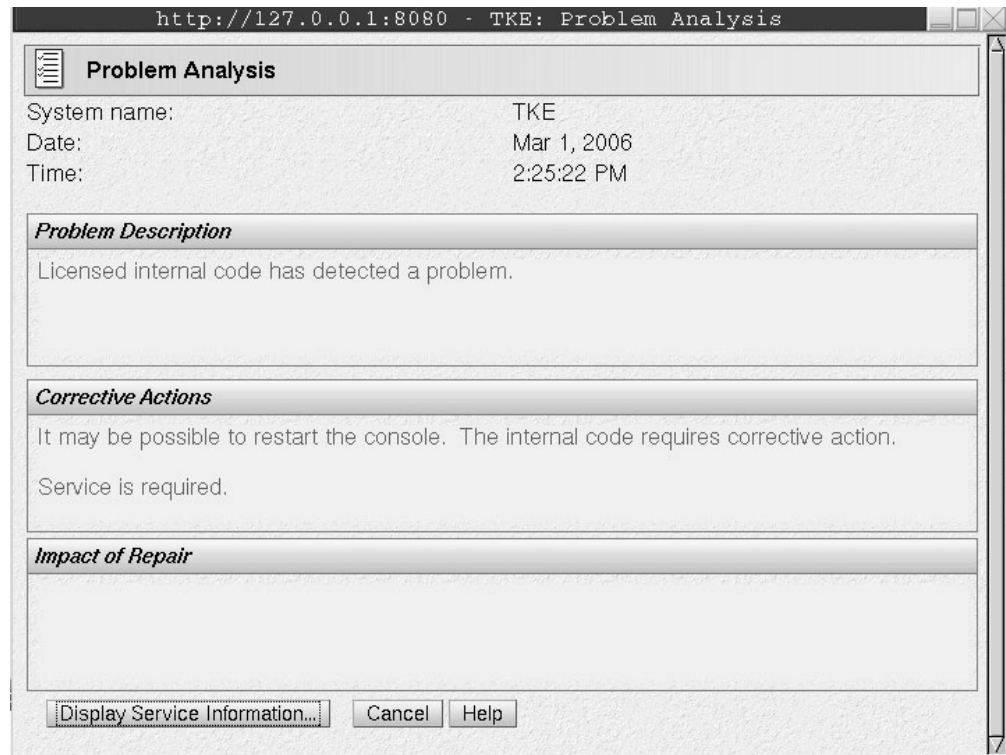


Figure 372. Problem Analysis

- **Cancel** exits this task and returns to the Trusted Key Entry Console.

Clicking **Close** on the menu bar brings up two options:

- **Selected Problem** changes the status of the selected problem to Closed.
- **All Problems** changes the status of all open problems to Closed.

## View Console Tasks Performed

The View Console Tasks Performed task window shows a summary of the console tasks performed with the date and time associated with each task. The most recent tasks invoked are appended to the bottom of the list. This information is useful in determining past activity performed on the TKE Workstation for auditing or problem determination.

To invoke this task, click on Service Management and then click on View Console Tasks Performed. The View Console Tasks Performed window is displayed.

You must scroll the display to the right until you see the inner right hand scroll bar for moving the display up and down.



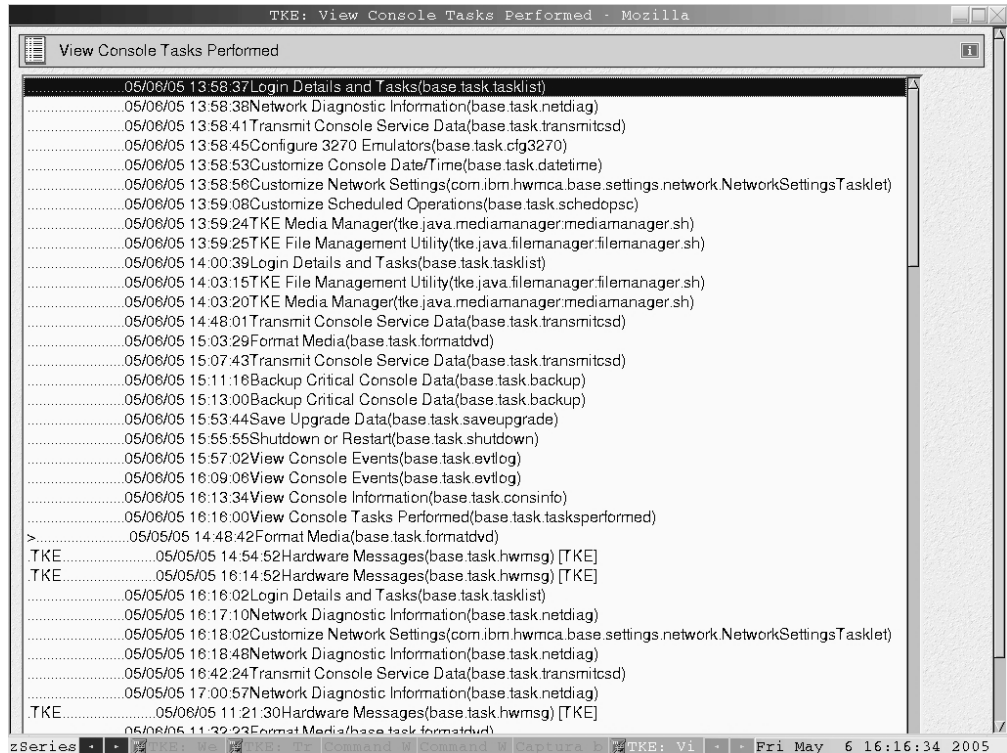


Figure 373. View Console Tasks Performed window

## 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
- Mozilla Firefox Browser License
- Opera Browser License
- International License Agreement for Non-Warranted Programs
- Additional License Information
- Apache Tomcat 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 through this task, the first TKE related task that you invoke will display the license information. This will only be done once.

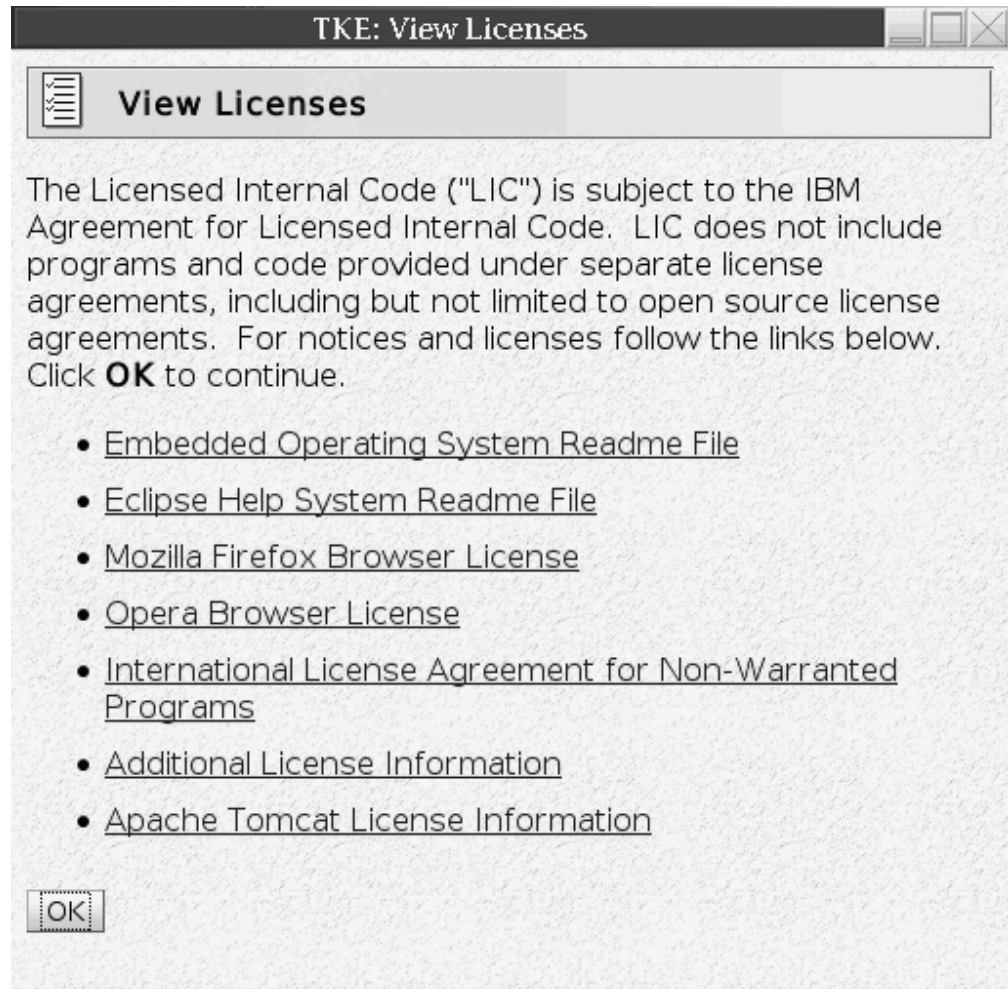


Figure 374. View Licenses window

## View Security Logs

This task displays the TKE console's default security log. The security log is a record of the security-relevant events that have occurred on or have been initiated by the TKE workstation. You must logon with a console user name of AUDITOR to use this task.

See "View Security Logs" on page 179 for more information.



---

## Appendix G. TKE Best Practices

---

### Checklist for Loading a TKE Machine - Passphrase

#### Expectations

- You are working on a CEX2C or CEX3C card
- TKE is enabled on the card(s) on the Host machine
- LPARs are established
- TKE LIC 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
  - One for production
  - One for backup
- 2 Central electronic complex (CEC) cards being shared
  - One Test LPARs (Domain 0)
  - Three Production LPARs (Domain 1, 2, 3)

TKE can load the master key in groups as defined by either crypto module group or domain group setup

- 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.

The following 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 CEX2C and CEX3C crypto modules on the host machine.

One way to control access to the crypto modules 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
- COSIGN
  - Access control co-sign
  - Enable crypto card co-sign

- Zeroize domain co-sign
- Domain control change co-sign
- MKFIRST
  - AES, DES, ECC, or ASYM load first master key part
  - Clear new master key register
  - Clear old master key register
- MKMIDDLE
  - AES, DES, ECC, or ASYM combine middle master key parts
- MKLAST
  - AES, DES, ECC, or ASYM combine final master key part
  - Set asymmetric master key
- FIRSTCLEAR
  - Load first operational key part
  - Clear operational key register
- ADDCOMP
  - Load additional operational key part
  - Complete key
- TKE 1

**Note:** The Service Management tasks available to you will vary depending on the console user name you used to log on. Refer to “Service Management Tasks” on page 321 for more information.

1. Customize Network Settings
2. Customize 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 roles - OPTIONAL
  - b. Create user defined profiles - OPTIONAL
  - c. Create groups and add users - OPTIONAL

**Note:** Group members should already be defined.

- d. Change the passphrases for all of the predefined profiles - TKEADM, TKEUSER, KEYMAN1, and KEYMAN2
7. Log on to 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
  - Removable media only

- c. Create a Host
- d. Create crypto module groups or domain 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)

**Note:** If planning on interacting with a CEX2C, be aware that it supports only 1024-bit authority keys. If interacting with a CEX3C, 1024-bit, 2048-bit, and 4096-bit authority keys are supported.

- 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-RAM or USB flash memory drive.
- 10. Customize Scheduled Operations to schedule the backup critical console data task

---

## Checklist for Loading a TKE Machine - Smart Card

### Expectations

- You are working on a CEX2C or CEX3C crypto module
- TKE is enabled on the Host machine you are using
- LPARs are established (set up and predefined)
- TKE LIC 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
- Smart card readers are attached

### Setup

- 2 TKEs both running the same level of software
  - One for production
  - One for backup
- 2 CECs cards being shared
  - One Test LPARs (Domain 0)
  - Three Production LPARs (Domain 1, 2, 3)

TKE can load the master key in groups as defined by either crypto module group or domain group setup.

- 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, listed below, that are needed to use the TKE and CNM applications. Profiles are created by first generating a Crypto Adapter Logon key and then creating a profile using the Crypto Adapter Logon key.

- SCTKEUSR - 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 CEX2C and CEX3C crypto modules on the host machine.

One way to control access to the host crypto modules is with a minimum of seven 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
- COSIGN
  - Access control co-sign
  - Enable crypto card co-sign
  - Zeroize domain co-sign
  - Domain control change co-sign
- MKFIRST
  - AES, DES, ECC, or ASYM load first master key part
  - Clear new master key register
  - Clear old master key register
- MKMIDDLE
  - AES, DES, ECC, or ASYM combine middle master key parts
- MKLAST
  - AES, DES, ECC, or ASYM combine final master key part
  - Set asymmetric master key
- FIRSTCLEAR
  - Load first operational key part
  - Clear operational key register
- ADDCOMP
  - Load additional operational key part
  - Complete key
- The steps to set up the TKE workstation for smart card use are as follows. Be aware that the Service Management tasks available to you will vary depending on the console user name you used to log on. Refer to “Service Management Tasks” on page 321 for more information.
  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

**Note:** Smart cards created, initialized, or backed up using TKE 7.0 are not usable on earlier releases of TKE.

- 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:** Choose the "Default Logon". The temp default role will be used, and has full access to do everything on the crypto adapter.

- a. Enter known 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 TKE workstation crypto adapter 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
    - Removable media only
  - c. Create a Host
  - d. Create crypto module groups or domain groups - OPTIONAL
  - e. Logon to host with VM id



- f. Create role(s)
- g. Generate authority key(s) and save them to a TKE smart card

**Note:** You can save 1024-bit or 2048-bit authority keys on the smart card. Be aware, however, that 2048-bit keys are supported only on the CEX3C.

- 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 H. Accessibility

Publications for this product are offered in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when using PDF files, you may view the information through the z/OS Internet Library Web site or the z/OS Information Center. If you continue to experience problems, send an e-mail to [mhvrdfs@us.ibm.com](mailto:mhvrdfs@us.ibm.com) or write to:

IBM Corporation  
Attention: MHVRCFS Reader Comments  
Department H6MA, Building 707  
2455 South Road  
Poughkeepsie, NY 12601-5400  
U.S.A.

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 or Library Server versions of z/OS books in the Internet library at:

<http://www.ibm.com/systems/z/os/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

IBM®, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.



---

# Index

## Numerics

4764 cryptographic adapter  
  enroll local 265  
  enroll remote 267  
  local enrollment 265  
  remote enrollment 267  
  view zone 274

## A

access control 6, 72  
access control menu  
  CNM 216  
access control points  
  DEFAULT 77  
  KEYMAN1 76  
  KEYMAN2 76  
  SCTKEUSR 80  
  TKEADM 75, 81  
  TKEUSER 74  
accessibility 359  
adding cryptographic coprocessor 196  
Administrative Control Functions panel 198, 199  
API cryptographic services 174  
auditing 175  
authorities 4, 131  
  changing 137  
  creating 134  
  deleting 138  
authorities page 131  
authority administration  
  generating signature keys 132  
authority default signature key 5  
authority signature key 4  
  load 113  
authority signature keys  
  generating 132  
automated recognition  
  crypto module 90

## B

backup  
  CA smart card 261  
  host files 93  
  workstation files 92  
bibliography xxi  
blind key entry 145  
books, ICSF xxi

## C

CA smart card 18  
  backup 261  
  change PIN 262  
  display 255  
  initialize 258

CA smart card (*continued*)  
  personalize 258  
cancel TKE server 63  
CEX2C/CEX3C  
  access control 6  
  API cryptographic services 174  
  API cryptographic/SPF services 174  
  clear 164  
  description 1  
  disabling 124  
  domain keys page 149  
  encipher RSA key 170  
  generate operational key parts 150  
  generate RSA key 168  
  generating keys 142  
  load 143  
  load RSA key to host dataset 172  
  load RSA key to PKDS 171  
  load to key part register - add part 158  
  load to key part register - complete 160  
  load to key part register - first 153  
  load to key storage 166  
  multi-signature commands 127  
  operational keys 149  
  roles 127  
  set ASYM-MK 149  
  single signature commands 128  
  UDXs 174  
Change Master Key panel 193  
change PIN  
  CNM 243  
change signature index 125  
changing entries  
  authorities 137  
  host 97  
changing master keys 190  
  using panels 191  
CKDS (cryptographic key data set)  
  initializing 188  
  panel option 188, 206, 207  
  reenciphering 192  
  refreshing 204  
clear 164  
clearing new master key register  
  CNM 232  
clock  
  setting 69  
clock-calendar  
  read 215  
  synchronize 216  
CMID 3  
cni list  
  smart card 77  
cnm  
  errors 251  
CNM  
  access control menu 216  
  change PIN 243



## CNM (continued)

- clearing new master key register 232
- crypto node menu 215
- define a role 217
- define group profile 228
- define passphrase profile 223
- define smart card profile 225
- define user profile 222
- delete user profile loaded in the 4764 231
- description 209
- display smart card details 245
- edit a disk-stored role 218
- edit a role loaded in the 4764 220
- edit disk-stored user profile 230
- edit existing user profile 230
- edit icon 77
- edit user profile loaded in the 4764 230
- file menu 214
- generate 4764 logon key 244
- generating master key parts to a TKE smart card 235
- group logon 210
- key storage menu 241
- loading a new master key from key parts 233
- loading master key parts from a TKE smart card 237
- manage smart card contents 246
- master key menu 231
- passphrase group logon 211
- passphrase logon 209
- read clock-calendar 215
- reenciphering key storage 241
- reset user profile failure count 231
- smart card group logon 212
- smart card logon 210
- smart card menu 242
- starting 209
- synchronize clock-calendar 216
- verifying master key parts 238
- co-sign page
  - description 174
- commands
  - multi-signature 5
- configuration migration
  - all data 317
  - public data 316
- configuring
  - TCP/IP 64
- Coprocessor Management panel 202
- creating entries
  - authorities 134
  - crypto module groups 100
- Crypto Express2 Coprocessor 3
  - description 1
- Crypto Express3 Coprocessor
  - description 1
- crypto module
  - authenticating 91
  - automated recognition 90
  - groups 98
  - master 102

## crypto module (continued)

- signature key 5
  - using 98
- crypto module ID 3, 91
- crypto module notebook
  - authorities page 131
  - change signature index 125
  - co-sign page 174
  - compare group 125
  - description 123
  - details page 126
  - domains controls 173
  - domains page 138
  - functions 125
  - general page 123
  - modes 125
  - refresh notebook 125
  - release crypto module 125
  - roles 127
  - tabular pages 126
- crypto module public modulus 91
- crypto module, releasing 317
- crypto node menu
  - CNM 215
- cryptographic coprocessor
  - adding 196

## D

- default signature key 5, 92
- define a role
  - CNM 217
- define groupe profile
  - CNM 228
- define passphrase profile
  - CNM 223
- define smart card profile
  - CNM 225
- define user profile
  - CNM 222
- delete user profile loaded in the 4764
  - CNM 231
- deleting entries
  - authorities 138
  - DES key storage 118
  - host 97
  - PKA key storage 119
- DES key storage 117
  - deleting an entry 118
- DES Operational Key Load panel 202
- disability 359
- disabling crypto module 124
- disabling PKA callable services 196
- disabling PKA services 197
- display
  - CA smart card information 255
- display smart card details
  - CNM 245
- domain controls 6
- domain keys page
  - encipher RSA key 170

- domain keys page *(continued)*
  - load RSA key to host dataset 172
  - load RSA key to PKDS 171
- domains
  - domains general page 139
- domains controls page
  - description 173
- domains general page
  - zeroize domain 139
- domains keys page
  - clear 148
  - generate 142
  - generate RSA key 168
  - load 143
  - load to key storage 166
  - set 149
- domains keys page (CEX2C) 140
- domains page 138

## E

- edit an existing role
  - CNM 217
- edit disk-stored user profile
  - CNM 230
- edit existing user profile
  - CNM 230
- edit user profile loaded in the 4764
  - CNM 230
- emulator session
  - configuring 82
- enabling PKA services 198
- encipher RSA key 170
- enrolling an entity
  - description 19
- entering a key part
  - smart card reader 278

## F

- file menu
  - CNM 214
- files
  - backing up 92

## G

- general page 123
- generate 4764 logon key
  - CNM 244
- generate RSA key 168
- generating
  - authority signature keys 132
  - master key parts 142
  - operational key parts 150
- generating master key parts to a TKE smart card
  - CNM 235
- group logon
  - CNM 210
- groups
  - changing crypto module 101

- groups *(continued)*
  - comparing crypto module 103
  - creating crypto module 100
  - supporting functions 104
  - using crypto module 98

## H

- host
  - changing 97
  - creating 97
  - deleting 97
  - logon 96
- host crypto module
  - description 3
  - RSA key 4
- host files
  - backing up 93
- host transaction program
  - installation 60

## I

- initial authorities 92
- initialize a CKDS panel 190, 204
- Initialize a CKDS panel 206, 207
- initializing
  - CKDS 188
  - symmetric keys master key 188
  - TKE 4764 cryptographic adapter 69
- integrity 4
- intrusion latch 124
- ISPF services 174

## K

- key part
  - description 196
- key storage menu
  - CNM 241
- key-exchange protocol 6
- keyboard 359
  - input from keyboard 145

## L

- load new 143
  - input from binary file 147
  - input from keyboard 145
  - input from TKE smart card 143
- load RSA key to host dataset 172
- load RSA key to PKDS 171
- load to key part register - add part 158
- load to key part register - complete 160
- load to key part register - first 153
- load to key storage (CEX2C) 166
- loading a new master key from key parts
  - CNM 233
- loading master key parts from a TKE smart card
  - CNM 237

LPAR considerations 6, 97

## M

- main window 95
  - function menu 113
  - load authority signature key 113
  - utilities 117
- manage smart card contents
  - CNM 246
- master crypto module
  - changing 102
  - setting 101
- master key
  - initializing 188
  - setting 195
- master key management panel 189, 192, 193, 195
- Master key management panel 206
- Master Key Management panel 200, 201
- master key menu
  - CNM 231
- master key parts 187
- master keys
  - changing 190
  - re-entering 194
- migration
  - of configuration data 316
- mode
  - locked read-only 125
  - pending command 125
  - read-only 125
  - update 125
- modifying entries
  - groups 101
- multi-signature commands 5
  - description 5
- multiple hosts 7
- multiple workstations 7
- multiple zones 19

## N

Notices 361

## O

- Operational Key Load panel 203, 204
- operational key parts
  - generate 150

## P

- panels
  - CSF@PRIM — Primary Menu 189, 191, 195, 197, 198, 202, 205, 207
  - CSFACF00 — Administrative Control
    - Functions 198, 199
  - CSFCKD00 — Initialize a CKDS 190, 204
  - CSFCKD20 — Initialize a CKDS 206, 207
  - CSFCMK10 — Reencipher CKDS 192

panels (*continued*)

- CSFCMK11 — Reencipher PKDS 200
- CSFCMK20 — Change Master Key 193
- CSFCMK21 — Refresh PKDS 201
- CSFCMP50 — DES Operational Key Load 202
- CSFCMP50 — Operational Key Load 203, 204
- CSFCMP51 — Operational Key Load 203
- CSFGCMP0 — Coprocessor Management 202
- CSFMKM10 — Initialize a CKDS 206
- CSFMKM10 — Master Key Management 189, 192, 193, 195, 200, 201
- CSFOPK00 — TKE Processing Selection 207

passphrase

- access control administration 72
- access control points 74
- DEFAULT role 77
- initialize 71
- KEYMAN1 role 76
- KEYMAN2 role 76
- load first key part 74
- load last key part 74
- TKEADM role 75
- TKEUSER role 74

passphrase group logon

- CNM 211

passphrase logon

- CNM 209

PKA callable services

- disabling before entering PKA master keys 196

PKA key storage 118

- deleting an entry 119

PKDS

- activating 199
- reenciphering 199

PR/SM considerations 194

primary menu panel 189, 197, 202, 207

Primary Menu panel 191, 195, 198, 205

publications

- ICSF xxi
- related xx

## R

- re-entering master keys 194
- reencipher CKDS panel 192
- Reencipher PKDS panel 200
- reenciphering key storage
  - CNM 241
- refresh notebook 125
- refresh PKDS panel 201
- refreshing the CKDS
  - using panels 204
- release crypto module 125, 317
- remote cryptographic adapter
  - enroll 267
- reset user profile failure count
  - CNM 231
- resetting PKA master keys 199
- role
  - edit 218, 220

- roles
  - access control points (passphrase) 74
  - access control points (smart card) 80
  - changing 128
  - creating 128
  - deleting 131
  - description 127
- RSA key 3
  - encipher 170
  - generate 168
  - host crypto module 4
  - installing in the PKDS 207
  - load to host dataset 172
  - load to PKDS 171
- S**
- SCUP
  - backup the CA smart card 261
  - change PIN of a CA smart card 262
  - change PIN of a TKE smart card 265
  - description 253
  - display smart card 255
  - enroll a 4764 cryptographic adapter 265
  - initialize and enroll a TKE smart card 263
  - initialize and personalize the CA smart card 258
  - personalize a TKE smart card 264
  - unblock PIN on a TKE smart card 265
  - view zone 274
- secure key part entry
  - description 275
  - entering a key part 278
  - steps 275
- security policy
  - defining 7
- setting master key 195
- shortcut keys 359
- smart card
  - access control points 80
  - cni list 77
  - edit CNM icon 77
  - initialize 77
  - SCTKEUSR role 80
  - TKEADM role 81
- smart card group logon
  - CNM 212
- smart card logon
  - CNM 210
- smart card menu
  - CNM 242
- smart card reader
  - secure key part entry 278
  - using 15
- smart card support
  - authentication 18
  - CA smart card 18
  - description 17
  - enrolling an entity 19
  - multiple zones 19
  - preparation and planning 14
  - requirements 13

- smart card support *(continued)*
  - setting up 21
  - terminology 13
  - TKE smart card 20
  - using the smart card reader 15
  - zone creation 18
  - zone description 18
  - zone identifier 19
- start TKE server 63
- symmetric keys master key
  - initializing 188

## T

- TCP/IP
  - configure 64
  - setup 59
- TKE
  - host transaction program 60
  - smart card support 13
- TKE enablement 7
- TKE processing selection panel 207
- TKE smart card
  - change PIN 265
  - description 20, 21
  - initialize and enroll 263
  - personalize 264
  - unblock PIN 265
- TKE workstation crypto adapter
  - initialize 69
- transport key policy
  - defining 115
- trusted key entry
  - access control 6
  - activating the host 96
  - authorities 4
  - authority default signature key 5
  - authority signature key 4
  - concepts 3
  - Crypto Express2 Coprocessor 3
  - crypto module signature key 5
  - exiting 116
  - integrity 4
  - interaction with ICSF 187
  - introducing 2
  - key-exchange protocol 6
  - LPAR 6
  - main window 95
  - multi-signature commands 5
  - operational considerations 6
  - optional pc hardware 2
  - pc hardware 1
  - pc software 2
  - smart card hardware 2
  - system hardware 1
  - terms 3
  - workstation logon 85
- TSS HIKM
  - using 24

## U

UDXs 174

utilities

- copying smart card contents 120
- managing DES keys 117
- managing PKA keys 118
- managing smart card contents 119

## V

verification pattern

- description 197

verifying master key parts

- CNM 238

## W

workstation

- logon 85

workstation files

- backing up 92

workstation logon

- passphrase 85
- smart card 85

## Z

zeroize domain 139

zone creation 18

zone description 18

zone identifier 19

---

## Readers' Comments — We'd Like to Hear from You

z/OS

Cryptographic Services

ICSF

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

**Publication No. SA23-2211-06**

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 email to: [mhvrdfs@us.ibm.com](mailto:mhvrdfs@us.ibm.com)

If you would like a response from IBM, please fill in the following information:

\_\_\_\_\_  
Name

\_\_\_\_\_  
Address

\_\_\_\_\_  
Company or Organization

\_\_\_\_\_  
Phone No.

\_\_\_\_\_  
Email address



Cut or Fold  
Along Line

Fold and Tape

Please do not staple

Fold and Tape



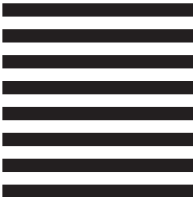
NO POSTAGE  
NECESSARY  
IF MAILED IN THE  
UNITED STATES

**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

SA23-2211-06

