z/OS
Cryptographic Services
ICSF

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

SA23-2211-07

Note!

Before using this information and the product it supports, be sure to read the general information under “Notices” on page 381.

Eighth Edition

This is a major revision of SA23-2211-06.

This edition applies to Version 1 Release 13 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.

Contents

Figures

Tables

About this information

This information introduces Version 7.1 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 7.1 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, “TKE migration overview,” provides details on migrating from previous versions of TKE to TKE 7.1.

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

Chapter 5, “TKE Up and Running,” 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,” explans 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, “LPAR Considerations,” discusses host setup considerations for managing CEX2Cs and CEX3Cs across multiple logical partitions.

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

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

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

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

Appendix G, “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. These books include:

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

How to send your comments to IBM

We appreciate your input on this publication. Feel free to comment on the clarity, accuracy, and completeness of the information or give us any other feedback that you might have.

Use one of the following methods to send us your comments:

1. Send an email to mhvrcfs@us.ibm.com
2. Visit the Contact z/OS web page at http://www.ibm.com/systems/z/os/zos/webqs.html
3. Mail the comments to the following address:

   IBM Corporation
   Attention: MHVRCFS Reader Comments
   Department H6MA, Building 707
   2455 South Road
   Poughkeepsie, NY 12601-5400
   U.S.A.
4. Fax the comments to us as follows:

   From the United States and Canada: 1+845+432-9405
   From all other countries: Your international access code +1+845+432-9405

Include the following information:

- Your name and address
- Your email address
- Your telephone or fax number
- The publication title and order number:

  z/OS Cryptographic Services ICSF Trusted Key Entry Workstation User's Guide
  SA23-2211-07
- The topic and page number related to your comment
- The text of your comment.

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 submit.

If you have a technical problem

Do not use the feedback methods listed above. Instead, do one of the following:

- Contact your IBM service representative
- Call IBM technical support
- Visit the IBM zSeries support web page at http://www.ibm.com/systems/z/support/

Summary of Changes

Changes made in z/OS Version 1 Release 13

This book contains information previously presented in *z/OS Cryptographic Services ICSF TKE PCIX Workstation User's Guide*, SA23-2211-06, which supports z/OS Version 1 Release 12.

New information:

- Revised information on how to migrate your customer unique data from one version of TKE to another. This information is provided in Chapter 3, “TKE migration overview,” on page 41.
- New access control points (ACPs), and a new utility for adding ACPs to existing roles on your TKE’s local crypto adapter. See “Adding new ACPs to existing roles using the Migrate Roles Utility” on page 95 for more information.
- Added support for decimalization tables. Decimalization tables map hexadecimal digits to decimal digits and are used in certain host crypto module operations that process Personal Identification Numbers (PINs). A new page for loading, activating, and deleting tables has been added to the Crypto Module Notebook Domains Tab. See “Dec Tables Page” on page 201 for more information.

Changes made in 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 336 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 214.
- 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.

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 41 smart cards. Copying a DataKey smart card is the only action still supported. See “Copy Smart Card” on page 280

- 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.

Changes made in 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 utility for saving and restoring crypto adapter configuration data described in “Migrate IBM Host Crypto Module Public Configuration Data” on page 336.
- 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.

Chapter 1. Overview

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

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

Trusted Key Entry (TKE) is an optional 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 7.1 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 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.

Also available with a TKE 7.1 workstation are:

- Feature 0885: 2 OmniKey smart card readers and 20 NXP JCOP 41 smart cards
- Feature 0884: 10 NXP JCOP 41 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 Time Sharing Option/Extended (TSO/E) session on the TKE workstation or another workstation located nearby. The ICSF panels are used to load operational keys from key part registers, set the master key, and initialize or reencipher the CKDS

(Cryptographic Keys Data Set). The TSO/E session is also required to disable and enable PKA services so that the Public Key Algorithm (PKA) master keys can be reset and changed and the PKDS (PKA Cryptographic Key Data Set) can be initialized, reenciphered and refreshed.

Supported Host Cryptographic Card Features

The host cryptographic cards supported with TKE 7.1 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 an entity that 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 its signature key. If an authority has a different index on each host crypto module, it will have to change its index as it works with different crypto modules.

In addition to the ease of use from crypto module to crypto module, if you intend to create 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 following 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

  Note: If you are running HCR7790 or later, you will no longer be able to set the asymmetric master key from the TKE. The set must be done from ICSF.
- 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 System z, you must have at least one CEX2C or 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 Processor Resource/Systems Manager (PR/SM) logical partitions, provided unique domains are assigned to each LPAR.

When you run in LPAR mode, each logical partition can have its own master keys, CKDS 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 B, “LPAR Considerations,” on page 313.

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

A support element is a dedicated workstation used for monitoring and operating IBM System z hardware. TKE commands must be permitted on the Support Element before any commands issued by the TKE workstation can be executed. Default setting for TKE commands is **Denied**.

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.'
```

An authorized user can permit TKE commands on the Support Element, using the IBM Support Element Console Application. For more information, refer to the *Support Element Operations Guide* for your specific IBM System z hardware. You can download the *Support Element Operations Guide* from IBM Resource Link (http://www.ibm.com/servers/resourcelink).

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.

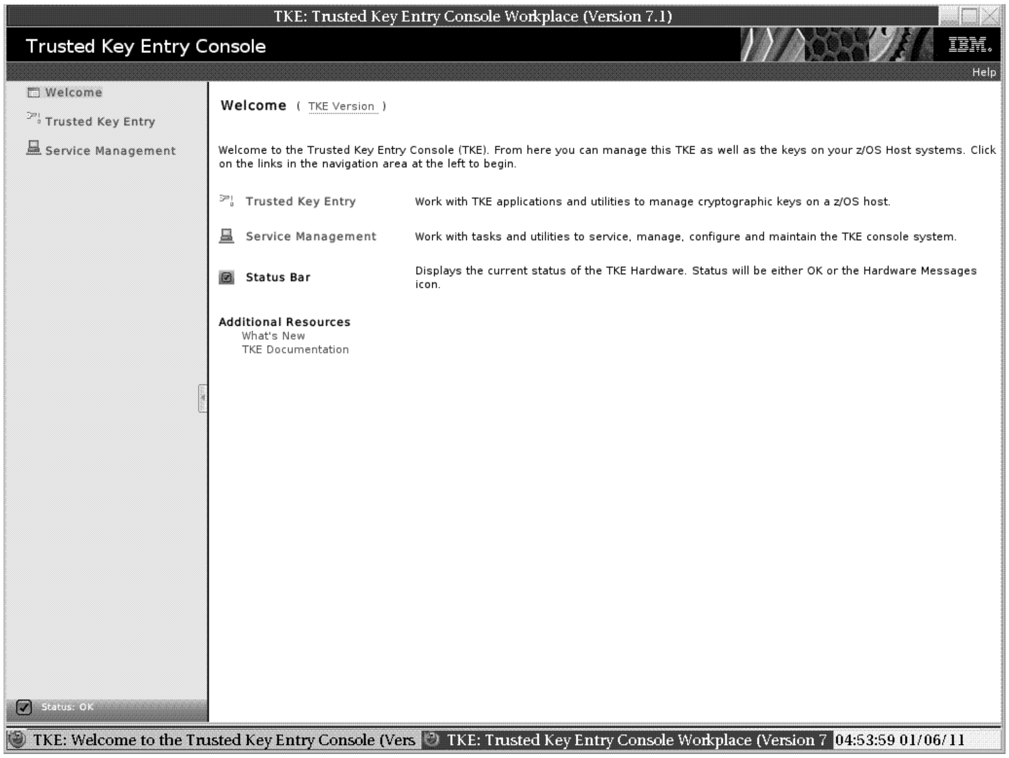
Most tasks require an additional logon to the TKE Workstation Crypto Adapter. You log on with your workstation crypto adapter profile. The profile is defined for your workstation when TKE is configured and customized. See “Define a User Profile” on page 254 for more information.

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 E, “Trusted Key Entry Applications and Utilities,” on page 325 describes the applications and utilities available to each console user name.

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



TKE: Trusted Key Entry Console Workplace (Version 7.1)

Trusted Key Entry Console

Welcome (TKE Version)

Welcome to the Trusted Key Entry Console (TKE). From here you can manage this TKE as well as the keys on your z/OS Host systems. Click on the links in the navigation area at the left to begin.

Trusted Key Entry	Work with TKE applications and utilities to manage cryptographic keys on a z/OS host.
Service Management	Work with tasks and utilities to service, manage, configure and maintain the TKE console system.
Status Bar	Displays the current status of the TKE Hardware. Status will be either OK or the Hardware Messages icon.

Additional Resources
What's New
TKE Documentation

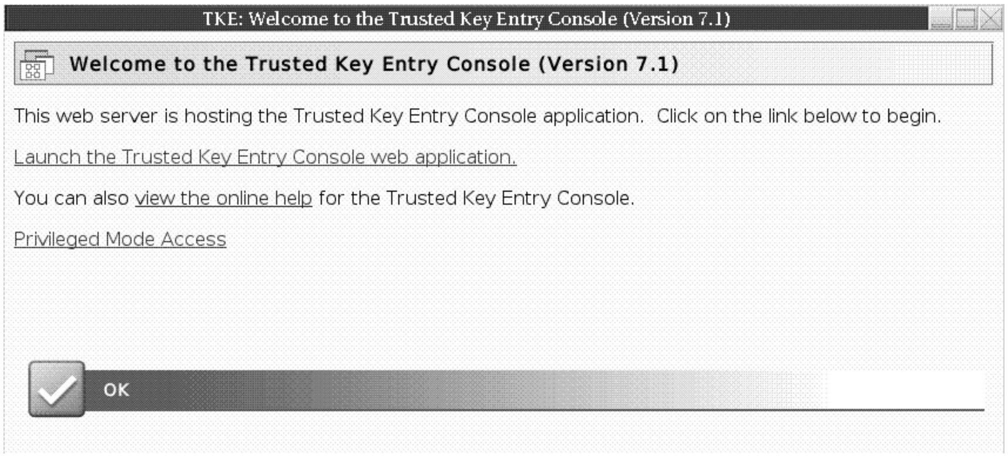
Status: OK
TKE: Welcome to the Trusted Key Entry Console (Vers
TKE: Trusted Key Entry Console Workplace (Version 7
04:53:59 01/06/11

Figure 1. TKE Console - initial panel

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

- Clicking 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.



TKE: Welcome to the Trusted Key Entry Console (Version 7.1)

Welcome to the Trusted Key Entry Console (Version 7.1)

This web server is hosting the Trusted Key Entry Console application. Click on the link below to begin.

Launch the Trusted Key Entry Console web application.

You can also view the online help for the Trusted Key Entry Console.

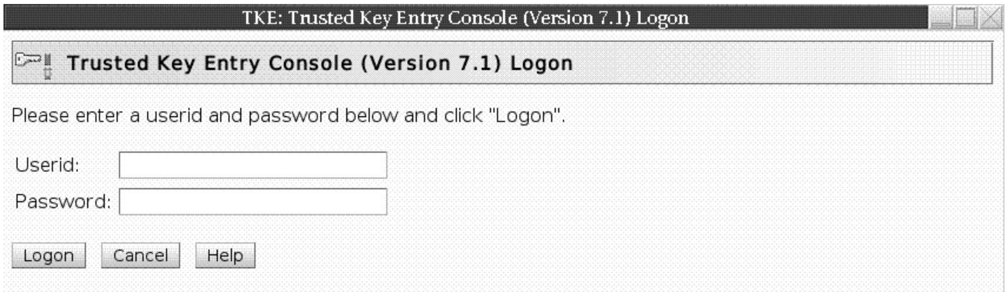
Privileged Mode Access

Figure 2. 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.



TKE: Trusted Key Entry Console (Version 7.1) Logon

Trusted Key Entry Console (Version 7.1) Logon

Please enter a userid and password below and click "Logon".

Userid:

Password:

Figure 3. Log on with other console user names

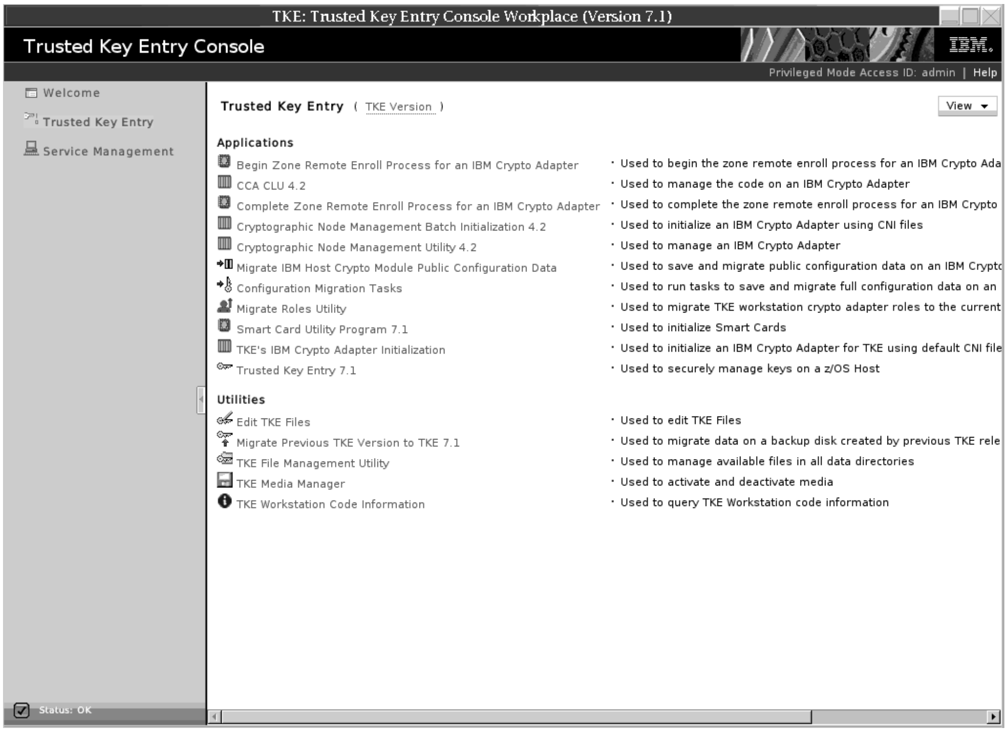
Fill in the user name field with one of the following:

- 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.


TKE: Trusted Key Entry Console Workplace (Version 7.1)
Trusted Key Entry Console
IBM.
Privileged Mode Access ID: admin | Help
Welcome
Trusted Key Entry
Service Management
Trusted Key Entry (TKE Version)
View
Status: OK

Applications

Begin Zone Remote Enroll Process for an IBM Crypto Adapter	Used to begin the zone remote enroll process for an IBM Crypto Ada
CCA CLU 4.2	Used to manage the code on an IBM Crypto Adapter
Complete Zone Remote Enroll Process for an IBM Crypto Adapter	Used to complete the zone remote enroll process for an IBM Crypto
Cryptographic Node Management Batch Initialization 4.2	Used to initialize an IBM Crypto Adapter using CNI files
Cryptographic Node Management Utility 4.2	Used to manage an IBM Crypto Adapter
Migrate IBM Host Crypto Module Public Configuration Data	Used to save and migrate public configuration data on an IBM Crypto
Configuration Migration Tasks	Used to run tasks to save and migrate full configuration data on an
Migrate Roles Utility	Used to migrate TKE workstation crypto adapter roles to the current
Smart Card Utility Program 7.1	Used to initialize Smart Cards
TKE's IBM Crypto Adapter Initialization	Used to initialize an IBM Crypto Adapter for TKE using default CNI file
Trusted Key Entry 7.1	Used to securely manage keys on a z/OS Host

Utilities

Edit TKE Files	Used to edit TKE Files
Migrate Previous TKE Version to TKE 7.1	Used to migrate data on a backup disk created by previous TKE rele
TKE File Management Utility	Used to manage available files in all data directories
TKE Media Manager	Used to activate and deactivate media
TKE Workstation Code Information	Used to query TKE Workstation code information

Figure 4. Trusted Key Entry for ADMIN - catagorized

After logging in the first time, it is recommended that you change the password with the Change Password task. See "Change Password" on page 345.

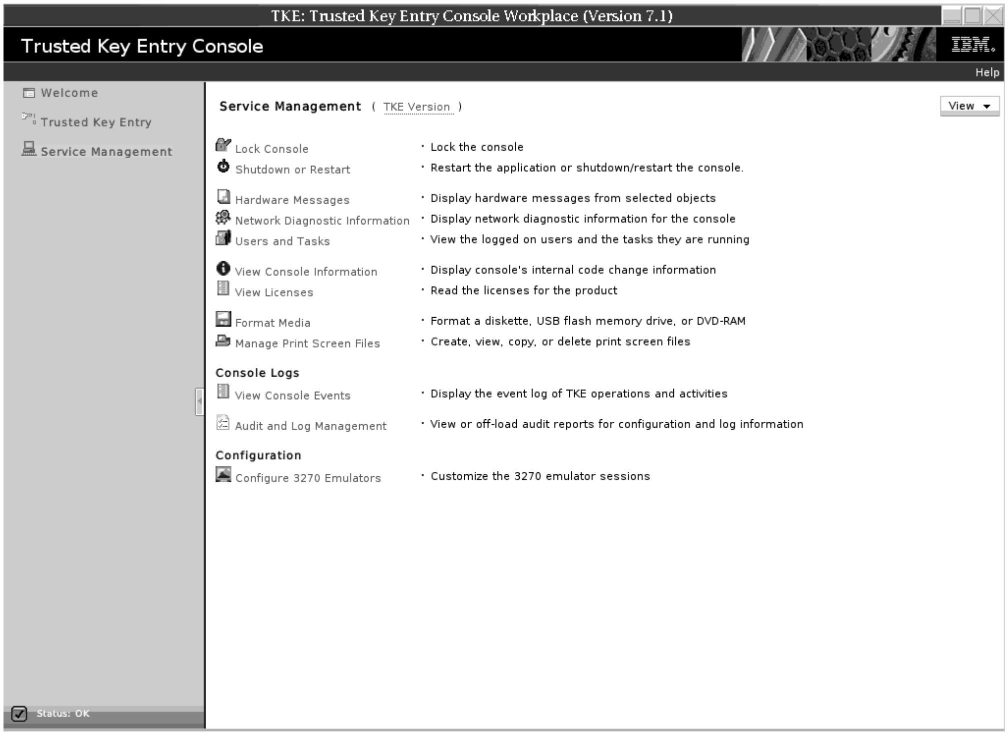
Trusted Key Entry Console Navigation

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.


TKE: Trusted Key Entry Console Workplace (Version 7.1)
Trusted Key Entry Console
IBM.
Help
Welcome
Trusted Key Entry
Service Management
View
Status: OK

Service Management (TKE Version)

- Lock Console · Lock the console
- Shutdown or Restart · Restart the application or shutdown/restart the console.
- Hardware Messages · Display hardware messages from selected objects
- Network Diagnostic Information · Display network diagnostic information for the console
- Users and Tasks · View the logged on users and the tasks they are running
- View Console Information · Display console's internal code change information
- View Licenses · Read the licenses for the product
- Format Media · Format a diskette, USB flash memory drive, or DVD-RAM
- Manage Print Screen Files · Create, view, copy, or delete print screen files

Console Logs

- View Console Events · Display the event log of TKE operations and activities
- Audit and Log Management · View or off-load audit reports for configuration and log information

Configuration

- Configure 3270 Emulators · Customize the 3270 emulator sessions

Figure 5. Service Management – No Privileged Mode Access

TKE Local Crypto Adapter Roles and Profiles

This information describes how the Roles and Profiles on the TKE's local crypto adapter are used to control access to the TKE applications and the cryptographic services on the TKE's Local Crypto adapter.

Roles and profiles are placed on a TKE's local crypto adapter when you:

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

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

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

There is always a current role in effect.

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

Authority Checking on the TKE

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

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

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

Types of Profiles

A TKE local crypto adapter supports 3 types of profiles:

- **Passphrase Profiles:** A profile that requires the user to provide the correct passphrase during the authentication process.
- **Smart Card Profiles:** A profile that requires the user to have the correct TKE Crypto Adapter Logon Key on their smart card during the authentication process. In addition, the user must know the PIN number of the smart card that has the logon key.
- **Group Profiles:** A profile designed to require a specific number of people to sign on to their individual profle's before the logon process for the group profile is complete. The following characteristics apply to group profiles:
  - A group profile has a set of 1 to 10 members.
  - A group member is an individual passphrase or smart card profile that must exist when the group profile is created.
  - All the members of a group profile must be the same type: Passphrase or smart card profiles.
  - A group profile contains an attribute that defines how many people must sign on before the group logon is complete. The number is a value between 1 and the total number of members of the group.
  - A group profile has a role. Normally the group's role is more powerful than the roles given to each individual group member.

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

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

For instructions on creating or changing roles and profiles, refer to Chapter 10, "Cryptographic Node Management Utility (CNM)," on page 241.

Initializing a TKE Local Crypto Adapter

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

Initial Adapter Conditions

Before you can start using your TKE, the local crypto adapter must have the:

- Correct CCA level of code
- Function Control Vector Loaded

Initial Adapter Conditions on New TKE Workstations: Every TKE comes with a cryptographic adapter. The following steps were performed before the adapter was shipped with the TKE:

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

Table 1. CAA code loaded for specific releases of TKE

TKE Release	CCA Release
TKE 5.3	CCA 3.4
TKE 6.0	CCA 3.5
TKE 7.0	CCA 4.1
TKE 7.1	CCA 4.2

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

  Note: During the process of loading the CCA code and the FCV, the card was initialized for use with passphrase profiles. The IBM-supplied roles and profiles may still be on the adapter.

Initial Adapter Conditions on Upgraded TKE workstations: When you upgrade an existing TKE workstation to a new level of TKE, the upgrade process states:

- You must go into the CCA CLU utility and load the new CCA code onto your TKE's crypto adapter.
- You might have to load a new Function Control Vector onto your TKE's crypto adapter. The Installation Instructions for your upgrade will tell you if this is required.

Verify Current Crypto Adapter Settings: You can check the state of the TKE's local crypto adapter at any time using the following utilities.

- You can determine the CCA level by running the **Check Coprocessor Status** command from the CCA CLU utility.
- You can determine if the FCV is loaded by pressing the "export control" button on the **Crypto Node -> Status** screen in the Cryptographic Node Management (CNM) Utility.
- You can determine if there are any roles on the adapter by looking at the **Access Control –Roles** screen in the CNM utility.
- You can determine if there are any roles on the adapter by looking at the **Access Control –Profiles** screen in the CNM utility.

IBM-supplied Roles and Profiles on TKE Crypto Adapters:

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

Recommendation: Use smart cards profiles whenever possible. They provide the highest level of security.

Once you have decided what type of profiles you will use, you need to initialize the TKE's local crypto adapter for use with those kinds of profiles. The initialization is done through the TKE's IBM Crypto Adapter Initialization application. When you start this application, you will be asked:

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

We recommend you:

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

Initializing for Use with Smart Card Profiles: When you initialize a TKE crypto adapter for use with Smart Card profiles, the following IBM-supplied roles and profiles will be created:

- IBM-supplied Roles:

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

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

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

- IBM-supplied Profiles:

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

Initializing for Use with Passphrase Profiles: When you initialize a TKE crypto adapter for use with passphrase profiles, the following IBM-supplied roles and profiles will be created:

- IBM-supplied Roles:

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

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

  TKEUSER
  Intended for use with IBM-supplied and customer defined passphrase profiles. The role is designed to provide the authority to manage host cryptographic adapters.

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

  KEYMAN2
  Intended for use with the IBM-supplied passphrase profile KEYMAN2. The role is designed to provide users authority to load any middle and

last master key parts to the TKE crypto adapter new master key register, set the master key and reencipher key storage.

- IBM-supplied Profiles:

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

  TKEUSER
  Intended for a person with the responsibility of managing host cryptographic adapters.

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

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

Roles and Profiles Definition Files

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

- TKE's local crypto adapter is initialized
- Migration is being done
- Recovery is being done

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

Table 2. Definition files and their corresponding role or profile

Role or Profile Definition File Exists	Corresponding Role or Profile Exists On TKE Adapter	File Attributes Equal Adapter's Attributes
Yes	Yes	Yes
Yes	Yes	No
Yes	No	N/A
No	Yes	N/A

Role Definition Files

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

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

All IBM-supplied Roles have corresponding IBM-supplied Role definition files. When you create a role, you can also create a corresponding role definition file for the role.

IBM-supplied Role Definition Files

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

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

Passphrase Roles: When a TKE local crypto adapter is initialized for use with Passphrase profiles, 5 roles are created. The following table shows the names of the IBM-supplied role definition files that are used to create the roles.

Table 3. IBM-supplied role definition files for Passphrase roles

	Roles				
TKE Release	**DEFAULT**	**KEYMAN1**	**KEYMAN2**	**TKEADM**	**TKEUSER**
TKE 5.0	default.rol	keyman1.rol	keyman2.rol	tkeadm50.rol	tkeuser42.rol
TKE 5.1	default.rol	keyman1.rol	keyman2.rol	tkeadm50.rol	tkeuser42.rol
TKE 5.2	default.rol	keyman1.rol	keyman2.rol	tkeadm50.rol	tkeuser42.rol
TKE 5.3	default.rol	keyman1.rol	keyman2.rol	tkeadm50.rol	tkeuser42.rol
TKE 6.0	default.rol	keyman1.rol	keyman2.rol	tkeadm50.rol	tkeuser42.rol
TKE 7.0	default_70.rol	keyman1_70.rol	keyman2_70.rol	tkeadm_70.rol	tkeuser_70.rol
TKE 7.1	default_71.rol	keyman1_71.rol	keyman2_71.rol	tkeadm_71.rol	tkeuser_71.rol

Smart Card Roles: When a TKE local crypto adapter is initialized for use with Smart Card profiles, 3 roles are created. The following table shows the names of the IBM-supplied role definition files that are used to create the roles.

Table 4. IBM-supplied role definition files for Smart Card roles

	Roles		
TKE Release	**DEFAULT**	**SCTKEADM**	**KEYMAN2**
TKE 5.0	tempdefault.rol	sctkeadm50.rol	sctkeusr.rol
TKE 5.1	tempdefault.rol	sctkeadm50.rol	sctkeusr.rol
TKE 5.2	tempdefault.rol	sctkeadm50.rol	sctkeusr.rol
TKE 5.3	tempdefault.rol	sctkeadm50.rol	sctkeusr.rol
TKE 6.0	tempdefault.rol	sctkeadm50.rol	sctkeusr.rol
TKE 7.0	tempdefault_70.rol	sctkeadm_70.rol	sctkeusr_70.rol
TKE 7.1	tempdefault_71.rol	sctkeadm_71.rol	sctkeusr_71.rol

Customer Defined Role Definition Files

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

We recommend you:

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

For Instructions on creating or changing role definition files, refer to Chapter 10, "Cryptographic Node Management Utility (CNM)," on page 241.

Profile Definition Files

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

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

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

IBM-supplied Profile Definition Files

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

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

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

Table 5. IBM-supplied Profile Definition files for Passphrase Profiles

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

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

Customer Defined Profile Definition Files

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

We recommend you:

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

For instructions on creating or changing profile definition files, refer to Chapter 10, "Cryptographic Node Management Utility (CNM)," on page 241.

IBM-supplied Role Access Control Points (ACP)

The primary purpose of any role is to define the capabilities of a user with the role. Each role has a list of permitted operations: Also called Access Control Points (ACPs), which define the capabilities of the user.

ACP Considerations for User Defined Roles

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

Recommendation: If you are going to create roles, use one of the following IBM-Supplied roles as the basis for your new role.

TKE local Crypto Adapter initialized for passphrase profile use:

- TKEUSER
- TKEADM

TKE local crypto adapter initialized for smart card profile use:

- SCTKEUSER
- SCTKEADM

ACPs Assigned to IBM-supplied Roles

The following tables show the ACPs assigned to each of the IBM-supplied roles.

The following three roles are created when a TKE adapter is initialized for use with smart cards profiles:

- SCTKEADM
- SCTKEUSR
- DEFAULT

Table 6. ACPs Assigned to the SCTKEADM role

SCTKEADM					
ACP		**ACPs Enabled In release**			
Current Description	**Numeric Value**	**TKE 5.0 to TKE 5.2**	**TKE 5.3, TKE 6.0**	**TKE 7.0**	**TKE 7.1**
Required 0100 PKA96 Digital Signature Generate	X'0100'			x	x
Required 0103 PKA96 Key Generate	X'0103'		x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x

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

SCTKEADM					
ACP		ACPs Enabled In release			
Current Description	Numeric Value	TKE 5.0 to TKE 5.2	TKE 5.3, TKE 6.0	TKE 7.0	TKE 7.1
Required 0203 Delete Retained Key	X'012B'			x	x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'0203'		x	x	x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'			x	x
Load First Master Key Part	X'0018'	x	x	x	x
Combine Master Key Parts	X'0019'	x	x	x	x
Set Master Key	X'001A'	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x
Clear New Master Key Register	X'0032'	x	x	x	x
Generate Key	X'008E'	x	x	x	x
Reencipher to Current Master Key	X'0090'	x	x	x	x
PKA96 Key Token Change	X'0102'	x	x	x	x
One-Way Hash, SHA-1	X'0107'	x	x	x	x
Reset Intrusion Latch	X'010F'	x	x	x	x
Set Clock	X'0110'	x	x	x	x
Reinitialize Device	X'0111'	x	x	x	x
Initialize Access-Control System	X'0112'	x	x	x	x
Change User Profile Expiration Date	X'0113'	x	x	x	x
Change User Profile Authentication Data	X'0114'	x	x	x	x
Reset User Profile Logon-Attempt-Failure Count	X'0115'	x	x	x	x
Delete User Profile	X'0117'	x	x	x	x
Delete Role	X'0118'	x	x	x	x
Load Function-Control Vector	X'0119'	x	x	x	x
Clear Function-Control Vector	X'011A'	x	x	x	x
Unrestrict Combine Key Parts	X'027A'	x	x	x	x
RNX access control point	X'02A2'	x	x	x	x
Session Key Master	X'02A3'	x	x	x	x
Session Key Slave	X'02A4'	x	x	x	x
Import Card Device Certificate	X'02A5'		x	x	x
Import CA Public Certificate	X'02A6'		x	x	x
Master Key Extended	X'02A7'	x	x	x	x
Delete Device Retained Key	X'02A8'		x	x	x
Export Card Device Certificate	X'02A9'		x	x	x
Export CA Public Certificate	X'02AA'		x	x	x
Reset Battery Low Indicator	X'030B'	x	x	x	x
Open Begin Zone Remote Enroll Process	X'1000'				x
Open Complete Zone Remote Enroll Process	X'1001'				x
Open Cryptographic Node Management Utility	X'1002'				x
Open Smart Card Utility Program	X'1005'				x
Open Edit TKE Files	X'100D'				x
Open TKE File Management Utility	X'100E'				x
TKE USER	X'8002'		x	x	

Table 7. ACPs Assigned to the SCTKEUSR role

SCTKEUSR				
ACP		**ACPs Enabled In release**		
Current Description	**Numeric Value**	**TKE 5.0 to TKE 6.0**	**TKE 7.0**	**TKE 7.1**
Required 0100 PKA96 Digital Signature Generate	X'0100'	x	x	x
Required 0103 PKA96 Key Generate	X'0103'	x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x
Required 0203 Delete Retained Key	X'012B'		x	x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'0203'			x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'			x
Encipher	X'000E'	x	x	x
Decipher	X'000F'	x	x	x
Reencipher to Master Key	X'0012'	x	x	x
Reencipher from Master Key	X'0013'	x	x	x
Load First Key Part	X'001B'	x	x	x
Combine Key Parts	X'001C'	x	x	x
Compute Verification Pattern	X'001D'	x	x	x
Generate Key Set	X'008C'	x	x	x
Generate Key	X'008E'	x	x	x
PKA96 Digital Signature Verify	X'0101'	x	x	x
PKA96 Key Import	X'0104'	x	x	x
PKA Clone Key Generate	X'0204'	x	x	x
PKA Clear Key Generate	X'0205'	x	x	x
Load Diffie-Hellman Key mod/gen	X'0250'	x	x	x
Combine Diffie-Hellman Key part	X'0251'	x	x	x
Clear Diffie-Hellman Key values	X'0252'	x	x	x
Unrestrict Combine Key Parts	X'027A'	x	x	x
Process cleartext ICSF key parts	X'02A0'	x	x	x
Process enciphered ICSF key parts	X'02A1'	x	x	x
RNX access control point	X'02A2'	x	x	x
Session Key Master	X'02A3'	x	x	x
Session Key Slave	X'02A4'	x	x	x
Export Card Device Certificate	X'02A9'	x	x	x
OA Proxy Key Generate	X'0344'		x	x
OA Proxy Signature Return	X'0345'		x	x
Open Migrate IBM Host Crypto Module Public Configuration Data	X'1003'			x
Open Configuration Migration Tasks	X'1004'			x
Open Trusted Key Entry	X'1006'			x
Create Domain Group	X'1007'			x
Change Domain Group	X'1008'			x
Delete Domain Group	X'1009'			x
Create Crypto Module Group	X'100A'			x
Change Crypto Module Group	X'100B'			x
Delete Crypto Module Group	X'100C'			x

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

SCTKEUSR				
ACP		**ACPs Enabled In release**		
Current Description	**Numeric Value**	**TKE 5.0 to TKE 6.0**	**TKE 7.0**	**TKE 7.1**
Open Edit TKE Files	X'100D'			x
Open TKE File Management Utility	X'100E'			x
TKE USER	X'8002'	x	x	

Table 8. ACPs Assigned to the DEFAULT role when initialized for use with smart card profiles

DEFAULT Role When Initialized for Use with Smart Card Profiles			
ACP		**ACPs Enabled In release**	
Current Description	**Numeric Value**	**TKE 5.0 to TKE 6.0**	**TKE 7.0 and above**
Required 0100 PKA96 Digital Signature Generate	X'0100'	x	x
Required 0103 PKA96 Key Generate	X'0103'	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x
Required 0203 Delete Retained Key	X'012B'		x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'0203'	x	x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'		x
Encipher	X'000E'	x	x
Decipher	X'000F'	x	x
Generate MAC	X'0010'	x	x
Verify MAC	X'0011'	x	x
Reencipher to Master Key	X'0012'	x	x
Reencipher from Master Key	X'0013'	x	x
Load First Master Key Part	X'0018'	x	x
Combine Master Key Parts	X'0019'	x	x
Set Master Key	X'001A'	x	x
Load First Key Part	X'001B'	x	x
Combine Key Parts	X'001C'	x	x
Compute Verification Pattern	X'001D'	x	x
Translate Key	X'001F'	x	x
Generate Random Master Key	X'0020'	x	x
Clear New Master Key Register	X'0032'	x	x
Clear Old Master Key Register	X'0033'	x	x
Generate Diversified Key (CLR8-ENC)	X'0040'	x	x
Generate Diversified Key (TDES-ENC)	X'0041'	x	x
Generate Diversified Key (TDES-DEC)	X'0042'	x	x
Generate Diversified Key (SESS-XOR)	X'0043'	x	x
Enable DKG Single Length Keys and Equal Halves for TDES-ENC, TDES-DEC	X'0044'	x	x
Load First Asymmetric Master Key Part	X'0053'	x	x
Combine PKA Master Key Parts	X'0054'	x	x
Set Asymmetric Master Key	X'0057'	x	x
Clear New Asymmetric Master Key Buffer	X'0060'	x	x

Table 8. ACPs Assigned to the DEFAULT role when initialized for use with smart card profiles (continued)

DEFAULT Role When Initialized for Use with Smart Card Profiles			
ACP		**ACPs Enabled In release**	
Current Description	**Numeric Value**	**TKE 5.0 to TKE 6.0**	**TKE 7.0 and above**
Clear Old Asymmetric Master Key Buffer	X'0061'	x	x
Generate MDC	X'008A'	x	x
Generate Key Set	X'008C'	x	x
Generate Key	X'008E'	x	x
Reencipher to Current Master Key	X'0090'	x	x
Generate Clear 3624 PIN	X'00A0'	x	x
Generate Clear 3624 PIN Offset	X'00A4'	x	x
Verify Encrypted 3624 PIN	X'00AB'	x	x
Verify Encrypted German Bank Pool PIN	X'00AC'	x	x
Verify Encrypted VISA PVV	X'00AD'	x	x
Verify Encrypted InterBank PIN	X'00AE'	x	x
Format and Encrypt PIN	X'00AF'	x	x
Generate Formatted and Encrypted 3624 PIN	X'00B0'	x	x
Generate Formatted and Encrypted German Bank Pool PIN	X'00B1'	x	x
Generate Formatted and Encrypted InterBank PIN	X'00B2'	x	x
Translate PIN with No Format-Control to No Format-Control	X'00B3'	x	x
Reformat PIN with No Format-Control to No Format-Control	X'00B7'	x	x
Generate Clear VISA PVV Alternate	X'00BB'	x	x
Encipher Under Master Key	X'00C3'	x	x
Lower Export Authority	X'00CD'	x	x
Translate Control Vector	X'00D6'	x	x
Generate Key Set Extended	X'00D7'	x	x
Encipher/Decipher Cryptovariable	X'00DA'	x	x
Replicate Key	X'00DB'	x	x
Generate CVV	X'00DF'	x	x
Verify CVV	X'00E0'	x	x
Unique Key Per Transaction, ANSI X9.24	X'00E1'	x	x
PKA96 Digital Signature Verify	X'0101'	x	x
PKA96 Key Token Change	X'0102'	x	x
PKA96 Key Import	X'0104'	x	x
Symmetric Key Export PKCS-1.2/OAEP	X'0105'	x	x
Symmetric Key Import PKCS-1.2/OAEP	X'0106'	x	x
One-Way Hash, SHA-1	X'0107'	x	x
Data Key Import	X'0109'	x	x
Data Key Export	X'010A'	x	x
Compose SET Block	X'010B'	x	x
Decompose SET Block	X'010C'	x	x
PKA92 Symmetric Key Generate	X'010D'	x	x
NL-EPP-5 Symmetric Key Generate	X'010E'	x	x
Reset Intrusion Latch	X'010F'	x	x
Set Clock	X'0110'	x	x

Table 8. ACPs Assigned to the DEFAULT role when initialized for use with smart card profiles (continued)

DEFAULT Role When Initialized for Use with Smart Card Profiles			
ACP		**ACPs Enabled In release**	
Current Description	**Numeric Value**	**TKE 5.0 to TKE 6.0**	**TKE 7.0 and above**
Reinitialize Device	X'0111'	x	x
Initialize Access-Control System	X'0112'	x	x
Change User Profile Expiration Date	X'0113'	x	x
Change User Profile Authentication Data	X'0114'	x	x
Reset User Profile Logon-Attempt-Failure Count	X'0115'	x	x
Delete User Profile	X'0117'	x	x
Delete Role	X'0118'	x	x
Load Function-Control Vector	X'0119'	x	x
Clear Function-Control Vector	X'011A'	x	x
Force User Logoff	X'011B'	x	x
Set EID	X'011C'	x	x
Initialize Master Key Cloning	X'011D'	x	x
RSA Encipher Clear Key	X'011E'	x	x
RSA Decipher Clear Key	X'011F'	x	x
Generate Random Asymmetric Master Key	X'0120'	x	x
SET PIN Encrypt with IPINENC	X'0121'	x	x
SET PIN Encrypt with OPINENC	X'0122'	x	x
PKA Register Public Key Hash	X'0200'	x	x
PKA Public Key Register with Cloning	X'0201'	x	x
PKA Public Key Register	X'0202'	x	x
PKA Clone Key Generate	X'0204'	x	x
PKA Clear Key Generate	X'0205'	x	x
Clone-info (share) Obtain 1	X'0211'	x	x
Clone-info (share) Obtain 2	X'0212'	x	x
Clone-info (share) Obtain 3	X'0213'	x	x
Clone-info (share) Obtain 4	X'0214'	x	x
Clone-info (share) Obtain 5	X'0215'	x	x
Clone-info (share) Obtain 6	X'0216'	x	x
Clone-info (share) Obtain 7	X'0217'	x	x
Clone-info (share) Obtain 8	X'0218'	x	x
Clone-info (share) Obtain 9	X'0219'	x	x
Clone-info (share) Obtain 10	X'021A'	x	x
Clone-info (share) Obtain 11	X'021B'	x	x
Clone-info (share) Obtain 12	X'021C'	x	x
Clone-info (share) Obtain 13	X'021D'	x	x
Clone-info (share) Obtain 14	X'021E'	x	x
Clone-info (share) Obtain 15	X'021F'	x	x
Clone-info (share) Install 1	X'0221'	x	x
Clone-info (share) Install 2	X'0222'	x	x
Clone-info (share) Install 3	X'0223'	x	x
Clone-info (share) Install 4	X'0224'	x	x

Table 8. ACPs Assigned to the DEFAULT role when initialized for use with smart card profiles (continued)

DEFAULT Role When Initialized for Use with Smart Card Profiles			
ACP		**ACPs Enabled In release**	
Current Description	**Numeric Value**	**TKE 5.0 to TKE 6.0**	**TKE 7.0 and above**
Clone-info (share) Install 5	X'0225'	x	x
Clone-info (share) Install 6	X'0226'	x	x
Clone-info (share) Install 7	X'0227'	x	x
Clone-info (share) Install 8	X'0228'	x	x
Clone-info (share) Install 9	X'0229'	x	x
Clone-info (share) Install 10	X'022A'	x	x
Clone-info (share) Install 11	X'022B'	x	x
Clone-info (share) Install 12	X'022C'	x	x
Clone-info (share) Install 13	X'022D'	x	x
Clone-info (share) Install 14	X'022E'	x	x
Clone-info (share) Install 15	X'022F'	x	x
List Retained Key	X'0230'	x	x
Generate Clear NL-PIN-1 Offset	X'0231'	x	x
Verify Encrypted NL-PIN-1	X'0232'	x	x
PKA92 Symmetric Key Import	X'0235'	x	x
PKA92 Symmetric Key Import with PIN keys	X'0236'	x	x
ZERO-PAD Symmetric Key Generate	X'023C'	x	x
ZERO-PAD Symmetric Key Import	X'023D'	x	x
ZERO-PAD Symmetric Key Export	X'023E'	x	x
Symmetric Key Generate PKCS-1.2/OAEP	X'023F'	x	x
Load Diffie-Hellman Key mod/gen	X'0250'	x	x
Combine Diffie-Hellman Key part	X'0251'	x	x
Clear Diffie-Hellman Key values	X'0252'	x	x
Unrestrict Reencipher from Master Key	X'0276'	x	x
Unrestrict Data Key Export	X'0277'	x	x
Add Key Part	X'0278'	x	x
Complete Key Part	X'0279'	x	x
Unrestrict Combine Key Parts	X'027A'	x	x
Unrestrict Reencipher to Master Key	X'027B'	x	x
Unrestrict Data Key Import	X'027C'	x	x
Generate Diversified Key (DALL with DKYGENKY Key Type)	X'0290'	x	x
Generate CSC-5, 4 and 3 Values	X'0291'	x	x
Verify CSC-3 Values	X'0292'	x	x
Verify CSC-4 Values	X'0293'	x	x
Verify CSC-5 Values	X'0294'	x	x
Process cleartext ICSF key parts	X'02A0'	x	x
Process enciphered ICSF key parts	X'02A1'	x	x
RNX access control point	X'02A2'	x	x
Session Key Master	X'02A3'	x	x
Session Key Slave	X'02A4'	x	x
Import Card Device Certificate	X'02A5'	x	x

Table 8. ACPs Assigned to the DEFAULT role when initialized for use with smart card profiles (continued)

DEFAULT Role When Initialized for Use with Smart Card Profiles			
ACP		ACPs Enabled In release	
Current Description	Numeric Value	TKE 5.0 to TKE 6.0	TKE 7.0 and above
Import CA Public Certificate	X'02A6'	x	x
Master Key Extended	X'02A7'	x	x
Delete Device Retained Key	X'02A8'	x	x
Export Card Device Certificate	X'02A9'	x	x
Export CA Public Certificate	X'02AA'	x	x
Reset Battery Low Indicator	X'030B'	x	x

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

- TKEADM
- TKEUSER
- KEYMAN1
- KEYMAN2
- DEFAULT

Table 9. ACPs Assigned to the TKEADM role

TKEADM					
ACP		ACPs Enabled In release			
Current Description	Numeric Value	TKE 5.0 to TKE 5.2	TKE 5.3, TKE 6.0	TKE 7.0	TKE 7.1
Required 0100 PKA96 Digital Signature Generate	X'0100'			x	x
Required 0103 PKA96 Key Generate	X'0103'		x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x
Required 0203 Delete Retained Key	X'012B'			x	x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'0203'		x	x	x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'			x	x
Compute Verification Pattern	X'001D'	x	x	x	x
One-Way Hash, SHA-1	X'0107'	x	x	x	x
Reset Intrusion Latch	X'010F'	x	x	x	x
Set Clock	X'0110'	x	x	x	x
Reinitialize Device	X'0111'	x	x	x	x
Initialize Access-Control System	X'0112'	x	x	x	x
Change User Profile Expiration Date	X'0113'	x	x	x	x
Change User Profile Authentication Data	X'0114'	x	x	x	x
Reset User Profile Logon-Attempt-Failure Count	X'0115'	x	x	x	x
Delete User Profile	X'0117'	x	x	x	x
Delete Role	X'0118'	x	x	x	x
Load Function-Control Vector	X'0119'	x	x	x	x
Clear Function-Control Vector	X'011A'	x	x	x	x
Import Card Device Certificate	X'02A5'		x	x	x

Table 9. ACPs Assigned to the TKEADM role (continued)

TKEADM					
ACP		**ACPs Enabled In release**			
Current Description	**Numeric Value**	**TKE 5.0 to TKE 5.2**	**TKE 5.3, TKE 6.0**	**TKE 7.0**	**TKE 7.1**
Import CA Public Certificate	X'02A6'		x	x	x
Delete Device Retained Key	X'02A8'		x	x	x
Export Card Device Certificate	X'02A9'		x	x	x
Export CA Public Certificate	X'02AA'		x	x	x
Reset Battery Low Indicator	X'030B'	x	x	x	x
Open Begin Zone Remote Enroll Process	X'1000'				x
Open Complete Zone Remote Enroll Process	X'1001'				x
Open Cryptographic Node Management Utility	X'1002'				x
Open Smart Card Utility Program	X'1005'				x
Open Edit TKE Files	X'100D'				x
Open TKE File Management Utility	X'100E'				x
TKE USER	X'8002'		x	x	

Table 10. ACPs Assigned to the TKEUSER role

TKEUSER				
ACP		**ACPs Enabled In release**		
Current Description	**Numeric Value**	**TKE 5.0 to TKE 6.0**	**TKE 7.0**	**TKE 7.1**
Required 0100 PKA96 Digital Signature Generate	X'0100'	x	x	x
Required 0103 PKA96 Key Generate	X'0103'	x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x
Required 0203 Delete Retained Key	X'012B'		x	x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'0203'			x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'			x
Encipher	X'000E'	x	x	x
Decipher	X'000F'	x	x	x
Reencipher to Master Key	X'0012'	x	x	x
Reencipher from Master Key	X'0013'	x	x	x
Load First Key Part	X'001B'	x	x	x
Combine Key Parts	X'001C'	x	x	x
Compute Verification Pattern	X'001D'	x	x	x
Generate Key Set	X'008C'	x	x	x
Generate Key	X'008E'	x	x	x
PKA96 Digital Signature Verify	X'0101'	x	x	x
PKA96 Key Import	X'0104'	x	x	x
PKA Clone Key Generate	X'0204'	x	x	x
PKA Clear Key Generate	X'0205'	x	x	x
Load Diffie-Hellman Key mod/gen	X'0250'	x	x	x
Combine Diffie-Hellman Key part	X'0251'	x	x	x
Clear Diffie-Hellman Key values	X'0252'	x	x	x

Table 10. ACPs Assigned to the TKEUSER role (continued)

TKEUSER				
ACP		**ACPs Enabled In release**		
Current Description	**Numeric Value**	**TKE 5.0 to TKE 6.0**	**TKE 7.0**	**TKE 7.1**
Unrestrict Combine Key Parts	X'027A'	x	x	x
Process cleartext ICSF key parts	X'02A0'	x	x	x
Process enciphered ICSF key parts	X'02A1'	x	x	x
RNX access control point	X'02A2'	x	x	x
Session Key Master	X'02A3'	x	x	x
Session Key Slave	X'02A4'	x	x	x
Export Card Device Certificate	X'02A9'	x	x	x
OA Proxy Key Generate	X'0344'		x	x
OA Proxy Signature Return	X'0345'		x	x
Open Migrate IBM Host Crypto Module Public Configuration Data	X'1003'			x
Open Configuration Migration Tasks	X'1004'			x
Open Trusted Key Entry	X'1006'			x
Create Domain Group	X'1007'			x
Change Domain Group	X'1008'			x
Delete Domain Group	X'1009'			x
Create Crypto Module Group	X'100A'			x
Change Crypto Module Group	X'100B'			x
Delete Crypto Module Group	X'100C'			x
Open Edit TKE Files	X'100D'			x
Open TKE File Management Utility	X'100E'			x
TKE USER	X'8002'	x	x	

Table 11. ACPs Assigned to the KEYMAN1 role

KEYMAN1				
ACP		**ACPs Enabled In release**		
Current Description	**Numeric Value**	**TKE 5.0 to TKE 6.0**	**TKE 7.0**	**TKE 7.1**
Required 0100 PKA96 Digital Signature Generate	X'0100'		x	x
Required 0103 PKA96 Key Generate	X'0103'		x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x
Required 0203 Delete Retained Key	X'012B'		x	x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'0203'		x	x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'		x	x
Load First Master Key Part	X'0018'	x	x	x
Compute Verification Pattern	X'001D'	x	x	x
Clear New Master Key Register	X'0032'	x	x	x
Generate Key	X'008E'		x	x
Open Cryptographic Node Management Utility	X'1002'			x

Table 12. ACPs Assigned to the KEYMAN2 role

KEYMAN2				
ACP		**ACPs Enabled In release**		
Current Description	**Numeric Value**	**TKE 5.0 to TKE 6.0**	**TKE 7.0**	**TKE 7.1**
Required 0100 PKA96 Digital Signature Generate	X'0100'		x	x
Required 0103 PKA96 Key Generate	X'0103'		x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x
Required 0203 Delete Retained Key	X'012B'		x	x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'0203'		x	x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'		x	x
Combine Master Key Parts	X'0019'	x	x	x
Set Master Key	X'001A'	x	x	x
Compute Verification Pattern	X'001D'	x	x	x
Generate Key	X'008E'	x	x	x
Reencipher to Current Master Key	X'0090'	x	x	x
PKA96 Key Token Change	X'0102'	x	x	x
Open Cryptographic Node Management Utility	X'1002'			x

Table 13. ACPs Assigned to the DEFAULT role when initialized for use with passphrase profiles

DEFAULT Role When Initialized for Use with Passphrase Profiles			
ACP		**ACPs Enabled In release**	
Current Description	**Numeric Value**	**TKE 5.0 to TKE 6.0**	**TKE 7.0 and above**
Required 0100 PKA96 Digital Signature Generate	X'0100'		x
Required 0103 PKA96 Key Generate	X'0103'		x
Required 0116 Read Public Access-Control Information	X'0116'	x	x
Required 0203 Delete Retained Key	X'012B'		x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'0203'		x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'		x
Compute Verification Pattern	X'001D'	x	x
Reinitialize Device	X'0111'	x	x
Export Card Device Certificate	X'02AD'	x	x

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 7.1, 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 7.1, the 4.2 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 241.

CNI
Cryptographic Node Batch Initialization utility. The CNI Editor is a utility within CNM that is used to create CNI scripts to automate some of the functions of CNM. CNI scripts can be used for additional setup of the TKE 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 285.

Zone
A security concept ensuring that only members of the same zone can exchange key parts. A zone is established by a CA smart card. See “Zone creation” on page 36.

Entity
A member of a zone. Entities can be a CA smart card, one or more TKE smart cards, and one or more TKE workstation 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 50 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

TKE 7.1 requires Omnikey smart card readers.

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 a microprocessor chip symbol displays. If a USB plug symbol displays, you have not inserted the smart card correctly

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

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

The other buttons on the PIN pad are not operational.

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 14. Applet version by TKE release

	CA Smart Card	TKE Smart Card
TKE 5.2 or before	applet version = 0.3	applet version = 0.3

Table 14. Applet version by TKE release (continued)

	CA Smart Card	TKE Smart Card
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
TKE 7.1	applet version = 0.4	applet version = 0.7

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 7.1 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 15. 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	Use on TKE 7.1
Created on TKE 5.2 or before	Yes	Yes	Yes	No	No
Created on TKE 5.3	No	Yes	Yes	Yes[1]	Yes[1]
Created on TKE 6.0, 1024-bit zone key	No	Yes	Yes	Yes[1]	Yes[1]
Created on TKE 6.0, 2048-bit zone key	No	No	Yes	Yes	Yes
Created on TKE 7.0	No	No	No	Yes	Yes
Created on TKE 7.1	No	No	No	Yes	Yes

[1] You must use NXP JCOP 41 smart cards in this release of TKE. Datakey smart cards are not supported in TKE 7.0 or later.

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 to generate and retain an authority signature key or a crypto adapter logon key, to copy keys and key parts from one smart card to another, to log on to the TKE workstation crypto adapter, or to create a profile for the TKE workstation crypto adapter. The TKE smart card must be enrolled in the zone where it is used, although this is not required to use the authority signature key or crypto adapter logon key on the smart card. The authority signature key and the crypto adapter logon key are not subject to zone constraints.

Table 16. 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**	**Use on TKE 7.1**
Created on TKE 5.2 or before	Yes	Yes	Yes	No	No
Created on TKE 5.3	No	Yes	Yes	Yes[2]	Yes[2]
Created on TKE 6.0, 1024-bit zone key	No	Yes[1]	Yes	Yes[2]	Yes[2]
Created on TKE 6.0, 2048-bit zone key	No	No	Yes	Yes	Yes
Created on TKE 7.0	No	No	No	Yes	Yes
Created on TKE 7.1	No	No	No	Yes	Yes

[1] This smart card could contain:

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

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

[2] You must use NXP JCOP 41 or NXP JCOP 31 smart cards in this release of TKE. Datakey smart cards are not supported in TKE 7.0 or later.

NXP Smart Cards Required

On TKE 7.1, NXP JCOP 41 or NXP JCOP 31 smart cards must be used for all operations on the TKE workstation. DataKey smart cards not supported.

In TKE 7.0 or later, you can copy data from a Datakey smart card onto an NXP JCOP 41 smart card. The procedure you use depends on whether the Datakey smart card was initialized as a CA smart card or a TKE smart card.

If you have a Datakey CA smart card, you can use the Smart Card Utility program to make a backup of the CA card.

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

These are members of a zone:

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

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.

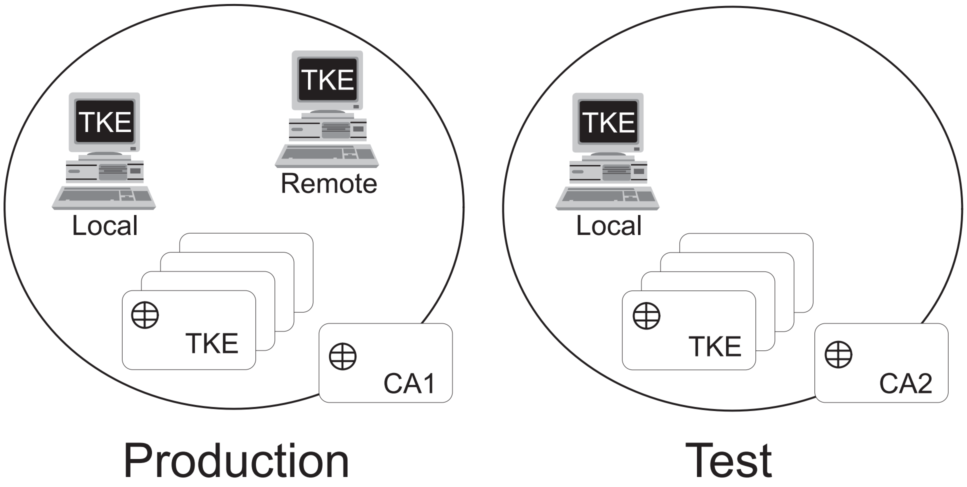


Figure 6. Multiple zones

Figure 6 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 50 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 and later are 2048-bits long. TKE crypto adapter logon keys generated on earlier versions of the TKE workstation may be 1024-bits long.
- One authority signature key. When generating an authority signature key and saving it to a smart card, you 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 or later) is protected by a 6-digit PIN. Smart cards initialized on earlier versions of TKE are protected by a 4-digit PIN. Enter this PIN when prompted to access the TKE smart card. If the PIN of a TKE smart card is entered incorrectly 3 times, the TKE smart card will be blocked. It is possible to unblock a TKE smart card using SCUP and a CA smart card in the same zone. The unblocking process resets the PIN failure counter on the TKE smart card. It does not reset or change the PIN value.

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

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

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 21 on page 69. The tasks defined here replace task 9: *Customize the TKE workstation crypto adapter*.
2. You must be logged in as ADMIN for this task.

Table 17. Smart card task checklist

TASK	RESPONSIBLE	WHERE	COMPLETED
1. Attach the smart card readers	IBM CE	TKE workstation	

Table 17. Smart card task checklist (continued)

2. Initialize the TKE workstation crypto adapter for smart card use; see “Initializing TKE for smart cards” on page 87.	TKE Administrator	TKE workstation	
3. Create CA smart card (zone); see “Initialize and personalize the CA smart card” on page 290.	TKE Administrator	TKE workstation	
4. Backup the CA smart card; see “Backup a CA smart card” on page 293.	TKE Administrator	TKE workstation	
5. Initialize and enroll TKE smart cards into the zone; see “Initialize and enroll a TKE smart card” on page 295.	TKE Administrator	TKE workstation	
6. Personalize TKE smart cards; see “Personalize a TKE smart card” on page 296.	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 297.	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 241.	TKE Administrator	TKE workstation	

Chapter 3. TKE migration overview

This information describes how to migrate your customer unique data from one version of TKE to another. It is important that you understand your situation. In some cases you can move your current workstation to a new level of TKE. For example, a TKE workstation with TKE 5.3 can be upgraded to TKE 6.0 without changing the workstation. In other situations, you may have a new TKE workstation because you need an additional TKE workstation, you want a faster TKE workstation, or you are moving to a new release of TKE which requires a new workstation.

Regardless of the situation, the migration requirements are easy to understand. For existing TKE workstations that are upgraded to new release levels of TKE, you want to preserve the customer unique data and make it available after the upgrade process is complete. When moving to a new TKE workstation, you want to collect the customer unique data from a source TKE workstation and make it available on the new TKE workstation.

Customer unique data includes the following:

- Network and Time settings for workstation
- Data found in the following TKE directories (Some directories first appear in specific releases of TKE):
  - TKE Data Directory
  - Migration Backup Data Directory
  - CNM Data Directory
  - SCUP Data Directory
  - Configuration Data Directory
- Roles and Profiles on the TKE local Crypto Adapter

The steps necessary for migrating customer unique data are dependent on:

- The release level of the source TKE and the release level of the target TKE
- Whether the data is preserved on an existing TKE workstation or moved to a new TKE workstation.

The following sections describe the migration impacts based on the source and target TKE release level and whether a new TKE workstation is involved.

- "Migrating an existing TKE workstation to a new level of TKE"
- "Migrating TKE Version 5.x, 6.0, 7.0 to a new TKE workstation at equal or newer level" on page 42

Migrating an existing TKE workstation to a new level of TKE

Existing TKE workstations can only be upgraded as follows:

- TKE workstations that use the 4764 as their Local Crypto Adapter can only be upgraded to a maximum level of TKE 6.0.
- TKE workstations that use the 4765 as their Local Crypto Adapter require a minimum level of TKE 7.0.

When migrating an existing TKE workstation to a new level of TKE, TKE firmware is updated on an existing TKE workstation. The firmware upgrade is done by an IBM Customer Engineer (CE). The following steps highlight some of the important steps taken by the IBM CE during the upgrade process.

1. Prior to starting the firmware upgrade, the CE performed a Save Upgrade Data operation. The data could have been saved to the local hard drive or to removable media that was properly formatted.
2. The CE performed the TKE Firmware upgrade. During the process, the Save Upgrade Data was used to restore the customer unique data.
3. Following the TKE Firmware upgrade, the CE used the “CCA CLU” utility to upgrade the firmware on the TKE’s local crypto adapter. Only the firmware on the adapter was updated. Any roles, profiles, TKE zone enrollment, migration zone certificates, and key part holder certificates will still be on the adapter after the adapter’s upgrade.
4. In some cases, the TKE's local crypto adapter must have a new Function Control Vector (FCV) loaded onto the adapter. The CE will load the new FCV when MES instructions list this requirement.

Required actions after IBM CE completes TKE firmware upgrade

The role of a TKE’s Local Crypto Adapter profile determines what actions a TKE user can perform. Roles contain a list of permitted operations, also known as Access Control Points (ACPs), that a profile with the role is authorized to use. When new ACPs are added between TKE releases, the new ACPs must be manually added to:

- IBM-supplied roles.
- Customer defined roles where necessary.

Note: The tables in “Access Control Points for Roles” on page 83 list the new ACPs for each of the IBM-Supplied Roles.

Recommendation: When you add an ACP to a role that also has a role definition file, you should also update the role definition file.

After making any necessary changes to roles and role definition files, the migration is complete.

Migrating TKE Version 5.x, 6.0, 7.0 to a new TKE workstation at equal or newer level

In this case, you have a new TKE workstation with a new local crypto adapter. The goal is the same as any other migration: to copy customer unique data from the source TKE to the target TKE. Customer unique data includes data on the TKE hard drive, TKE settings, and data and settings from the TKE’s local crypto adapter.

Note: Customer unique data on the TKE local crypto adapter includes roles, profiles, TKE zone enrollment, certificates used for the host adapter migration utility, and some adapter settings. No information can be collected from a TKE’s local crypto adapter. However, you can use role and profile definition files to migrate roles and profiles to a new TKE’s local crypto adapter.

The basic steps for this migration are:

On the source TKE:

1. Prepare the role and profile definition files for each TKE local crypto adapter role and profile that will be installed on the target TKE local crypto adapter. Role and profile definition files are the only way to capture the data needed to load

an existing role or profile on a new TKE local Crypto Adapter. This step is described in “Source TKE action: Create or prepare role and profile definition files.”

2. Collect the TKE’s customer unique data and system settings by running the Save Upgrade Data utility. The role and profile definition files are included in the output from the Save Upgrade Data operation. This step is described in “Source TKE action: Perform Save Upgrade Data” on page 46.

On the target TKE:

1. Perform a “frame roll” install. This install does not reinstall the workstation code. The frame roll install is a technique for restoring the information gathered by the “save upgrade data” utility onto the target TKE. This step is described in “Target TKE action: Perform a frame roll install” on page 48.
2. Load the roles and profiles from the source TKE crypto adapter onto the target TKE crypto adapter. There are two methods for loading the roles and profiles onto the target TKE crypto adapter. Both methods are described in “Target TKE action: Load roles and profiles into the TKE’s local crypto adapter” on page 51.
   - Manually load the roles and profiles through the Cryptographic Node Management (CNM) Utility.
   - Create a CCA Node Initialization (CNI) script and use it as input to the Cryptographic Note Management Batch utility.
3. Manually load any remaining customer unique data or settings onto the target TKE local crypto adapter. For example, you may need to enroll the TKE in a zone or install Migration Zone or Key Part Holder certificates.

Source TKE action: Create or prepare role and profile definition files

TKE local crypto adapter roles and profiles reside on the TKE's crypto adapter. Optionally, you can create a definition file for each role and profile that exists on your TKE's adapter. These files are kept on the TKE’s local hard drive. These files can be used to load roles or profiles onto a TKE local crypto adapter during an initialization, recovery, upgrade, or migration operation. The only way to migrate a TKE local crypto adapter role or profile is to:

- Create the role or profile definition file on the source TKE for the item to be taken to the new TKE.
- Transport the role or profile definition file to the new TKE. In this case, transport is done by doing a Save Upgrade Data on a source TKE and using that data during an upgrade on a target TKE.
- Perform the role or profile load operations, using the definition file, on the new TKE.

Before describing the process for preparing the role and profile definition files for the migration, you should be aware of the following:

- The TKE comes with definition files for all of the IBM-supplied roles and profiles. These definition files are used to create the IBM-supplied roles and profiles when the TKE’s IBM Crypto Adapter Initialization application is run.
- When a customer unique role or profile is created, there is no requirement to create the associated definition file. Therefore you may have roles or profiles on the TKE local crypto adapter which do not currently have a definition file.
- When you load a role or profile onto a TKE local crypto adapter, its definition file is not changed. Conversely, if you save a role or profile definition file, the profile

on the TKE local crypto adapter is not changed. Therefore, the role or profile on the TKE local crypto adapter can have attributes that do not match what is in its definition file.

- The Save Upgrade Data operation collects all the role and profile definitions files on the TKE, including the IBM-supplied role and profile definition files.

For this migration, it is necessary to create current definition files of the roles and profiles to be copied to the target TKE. For more information, see:

- “Selecting the roles and profiles to copy to the target TKE”
- “Steps to create role and profile definition files” on page 45

Selecting the roles and profiles to copy to the target TKE

You must explicitly decide which TKE local crypto adapter roles and profiles you want to copy to the target TKE’s local crypto adapter. Because there are differences between TKE releases, serious consideration must be given to which roles and profiles are selected.

Selecting roles to copy to the target TKE: When you do a Save Upgrade Data on the source TKE, every role definition file on the TKE is included in the upgrade data.

- To include a role in a migration, there must be a role definition file for it when the Save Upgrade Data operation is done.
- To exclude a role from a migration, there must not be a role definition file for it when the Save Upgrade Data operation is done.

Customer Unique Roles: Look at each of the customer unique roles you have on your TKE local crypto adapter and decide if you want that same role on your target TKE. The only roles you should exclude are those you consider obsolete.

IBM-Supplied Roles: The TKE is shipped with role definition files for every IBM-supplied role that can be created on a TKE. Every IBM-Supplied role definition file on the TKE is included in the data collected by the Save Upgrade Data operation. You must know the names of the IBM-supplied role definition files on both the source and target TKE workstation. When a source TKE workstation file has the same name as the target TKE workstation file name, the file is overwritten when the upgrade data is applied to the target TKE workstation.

Passphrase Roles: When a TKE local crypto adapter is initialized for use with Passphrase profiles, 5 roles are created. The following table shows the names of the IBM-Supplied role definition files that are used to create the roles.

Table 18. IBM-Supplied role definition files (Passphrase roles)

TKE Release	Roles				
	DEFAULT	**KEYMAN1**	**KEYMAN2**	**TKEADM**	**TKEUSER**
TKE 5.0 to TKE 6.0	default.rol	keyman1.rol	keyman2.rol	tkeadm50.rol	tkeuser42.rol
TKE 7.0	default_70.rol	keyman1_70.rol	keyman2_70.rol	tkeadm_70.rol	tkeuser_70.rol
TKE 7.1	default_71.rol	keyman1_71.rol	keyman2_71.rol	tkeadm_71.rol	tkeuser_71.rol

Smart Card Roles: When a TKE local crypto adapter is initialized for use with smart card profiles, 3 roles are created. The following table shows the names of the IBM-Supplied role definition files that are used to create the roles.

Table 19. IBM-Supplied role definition files (smart card roles)

TKE Release	Roles		
	DEFAULT	SCTKEADM	KEYMAN2
TKE 5.0 to TKE 6.0	tempdefault.rol	sctkeadm50.rol	sctkeusr.rol
TKE 7.0	tempdefault_70.rol	sctkeadm_70.rol	sctkeusr_70.rol
TKE 7.1	tempdefault_71.rol	sctkeadm_71.rol	sctkeusr_71.rol

Selecting profiles to copy to the target TKE: When you do a Save Upgrade Data on the source TKE, every profile definition file on the TKE is included in the upgrade data.

- To include a profile in a migration, there must be a profile definition file for it when the Save Upgrade Data operation is done.
- To exclude a profile from a migration, there must not be a profile definition file for it when the Save Upgrade Data operation is done.

Customer Unique Profiles: Look at each of the customer unique profiles you have on your TKE local crypto adapter and decide if you want that same profile on your target TKE. The only profiles you should exclude are those you consider obsolete.

IBM-Supplied profiles: The TKE is shipped with profile definition files for every IBM-supplied profile that can be created on a TKE. The names of the IBM-Supplied profile definition files and the attributes in the files do not change between TKE releases. Every IBM-Supplied profile definition file on the TKE is included in the data collected by the Save Upgrade Data operation. When a source TKE workstation file has the same name as the target TKE workstation file name, the file is overwritten when the upgrade data is applied to the target TKE workstation. Therefore, when save upgrade data is applied to a target TKE workstation, the IBM-supplied profile definition files are overwritten.

Note: To preserve the ability to restore IBM-Supplied profiles to their default settings, including the default passwords, do not update IBM-Supplied profile definition files.

Passphrase Profiles: When a TKE local crypto adapter is initialized for use with Passphrase profiles, 4 profiles are created using their IBM-Supplied profiles definition files. The following table shows the profiles and the definition files used to create them.

Table 20. IBM-Supplied role definition files (Passphrase profiles)

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

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

Steps to create role and profile definition files

Definition files are managed through the Cryptographic Node management Utility (CNM).

- For instructions on creating or updating a role definition file, see “Edit a role loaded in the TKE crypto adapter” on page 252.
- For instructions on creating or updating a profile definition file, see “Edit a User Profile loaded in the TKE Crypto Adapter” on page 262.

Source TKE action: Perform Save Upgrade Data

Use the Save Upgrade Data utility to collect the customer unique data from the source TKE. The following steps describe how to perform the save.

Note: Beginning in TKE 7.0, the target workstation requires the Save Upgrade Date to be on a USB Flash Memory drive. Only TKE 5.3 and greater allow you to place the Save Upgrade Data directly onto a USB Flash memory drive. If the source system is TKE 5.0 through 5.2, you must upgrade your TKE to 5.3 or later so you can get Save Upgrade Data to place its results on a USB Flash Memory Drive.

1. Sign on to the TKE with the Privileged Access Mode ID of ADMIN.
2. From the left pane on the Trusted Key Entry Console, select Service Management.

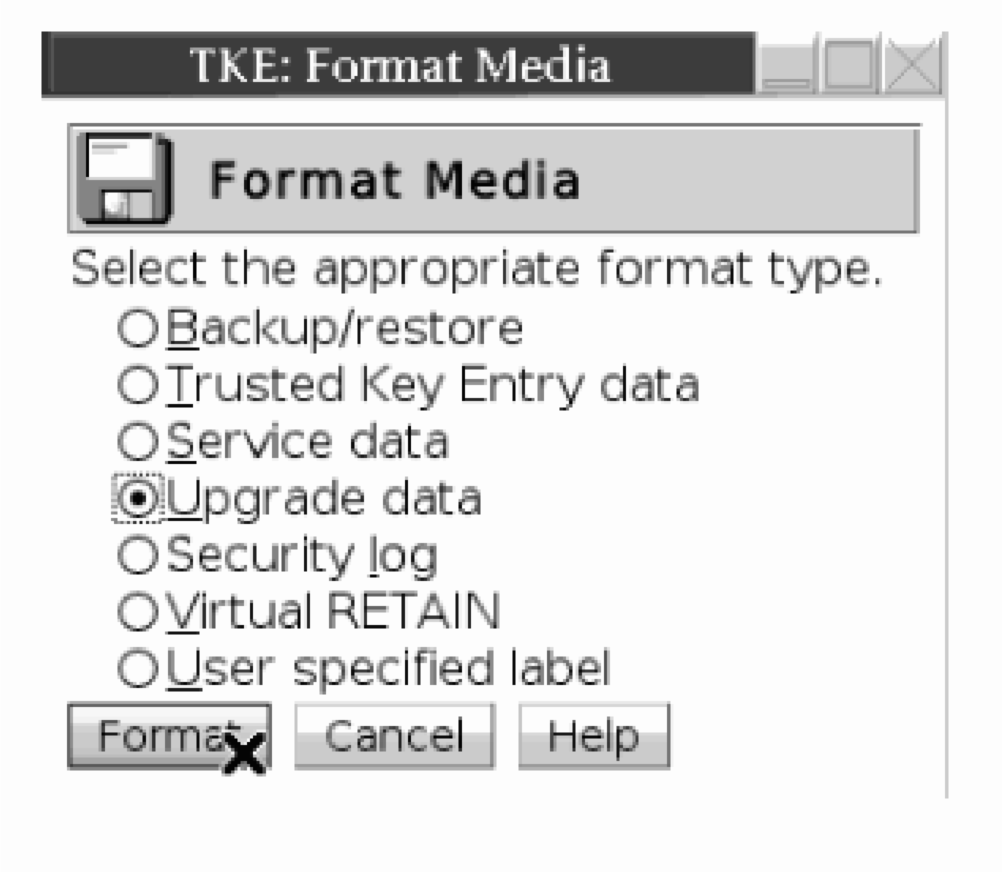
Format the removable media:

Place your removable media into the TKE.

- When the target TKE level is 6.0 or less, use a DVD-RAM
- When the target TKE level is 7.0 or greater, use a USB Flash memory drive

Note: Only TKE 5.3 and greater allow you to place the Save Upgrade Data directly onto a USB Flash memory drive. If the source system is TKE 5.0 through 5.2, you must upgrade your TKE to 5.3 or later so you can get Save Upgrade Data to place its results on a USB Flash Memory Drive.

1. From the right pane on the Trusted Key Entry Console, open the Format Media application.
2. Select the Upgrade Data radio button and press the Format button.



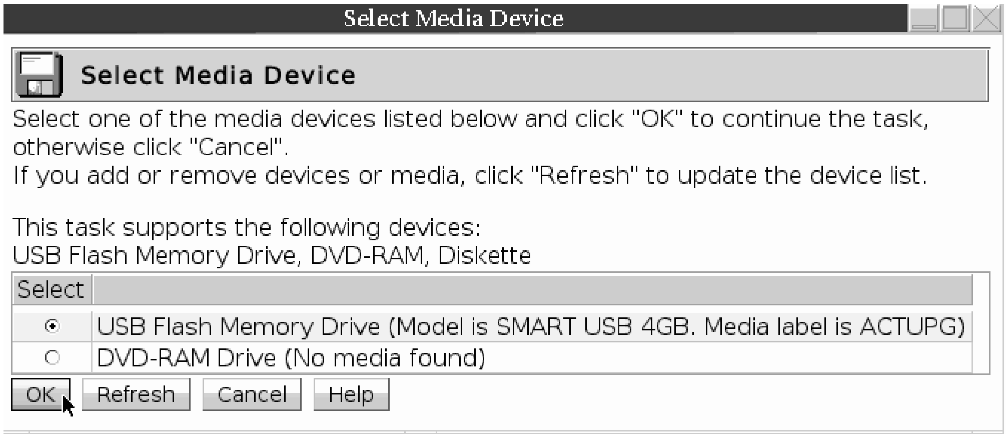
Select the appropriate format type.

○ Backup/restore
○ Trusted Key Entry data
○ Service data
● Upgrade data
○ Security log
○ Virtual RETAIN
○ User specified label

Figure 7. Select Upgrade data and press the Format button

3. Select the appropriate removable media radio button, and press the OK button.

   Note: If the media label is already ACTUPG, you do not need to format the drive. The drive is ready to use and you may press Cancel to exit this task. You can also reformat the drive if you press the OK button.



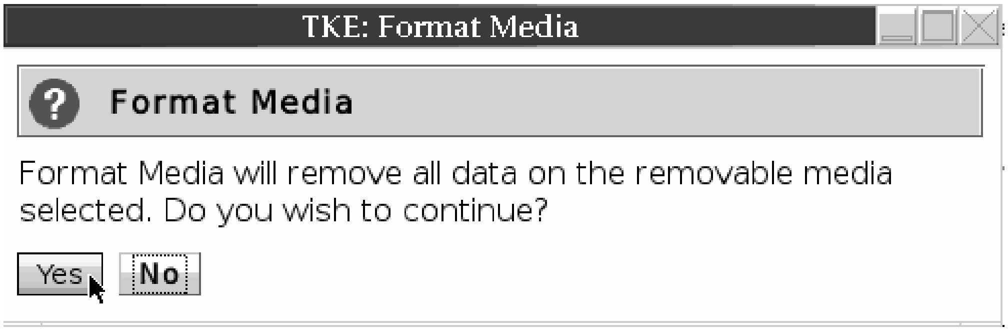
Select one of the media devices listed below and click "OK" to continue the task, otherwise click "Cancel".
If you add or remove devices or media, click "Refresh" to update the device list.

This task supports the following devices:
USB Flash Memory Drive, DVD-RAM, Diskette

Select	
●	USB Flash Memory Drive (Model is SMART USB 4GB. Media label is ACTUPG)
○	DVD-RAM Drive (No media found)

Figure 8. Select the appropriate removable media and press the OK button.

4. Press the Yes button if you receive a confirmation window.



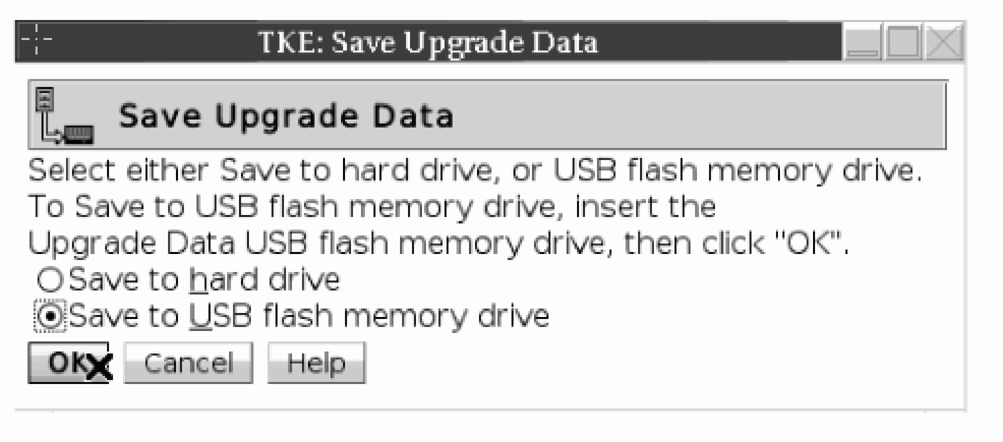
Format Media will remove all data on the removable media selected. Do you wish to continue?

Figure 9. Confirmation window

5. When you receive the successful completion message, press the OK button. The format media step is complete.

Perform the Save Upgrade Data operation:

1. From the right pane on the Trusted Key Entry Console, open the “Save Upgrade Data” application.
2. Save the data to the appropriate removable media device and press the OK button. This example uses a USB flash memory drive:
   - When the target TKE level is 6.0 or less, use a DVD-RAM
   - When the target TKE level is 7.0 or greater, use a USB Flash memory drive



Select either Save to hard drive, or USB flash memory drive. To Save to USB flash memory drive, insert the Upgrade Data USB flash memory drive, then click "OK".

○ Save to hard drive

● Save to USB flash memory drive

Figure 10. Save upgrade data

3. When the completion message appears, press the OK button.

The customer unique data has been collected; the source TKE actions are now complete.

Target TKE action: Perform a frame roll install

The purpose of a frame roll install is to restore information gathered by a Save Upgrade Data operation onto a TKE that already has a desired level of TKE code on it. Prior to the Frame Roll install, you should run the “TKE’s IBM Crypto Adapter Initialization” utility to load the IBM-supplied roles and profiles onto the target TKE’s local crypto adapter.

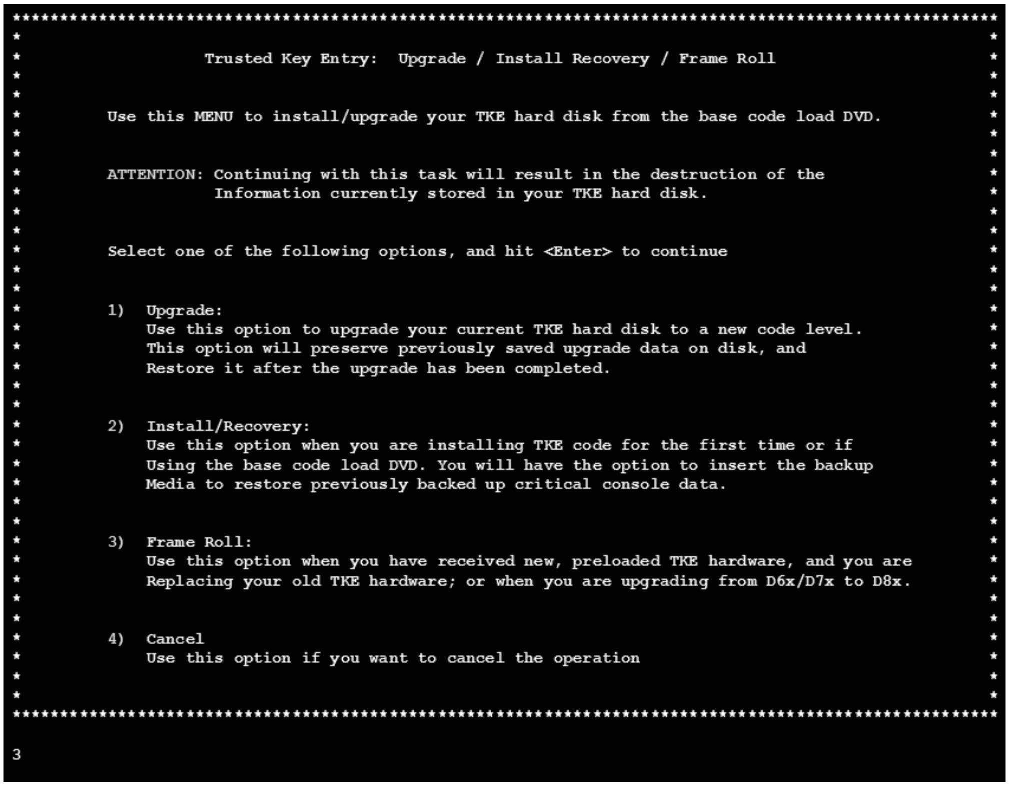
You must have the following items available for the frame roll install:

- The Save Upgrade Data from the source TKE. This data must be on an appropriate removable media device for the target TKE.
  - When the target TKE level is 6.0 or less, use a DVD-RAM.
  - When the target TKE level is 7.0 or greater, use a USB Flash memory drive.
- The TKE installation DVD for the target TKE.

To perform a frame roll install:

1. For TKE 7.0 or greater, place the USB Flash Memory drive that contains the Save Upgrade Data into any available USB port on the target TKE.
2. Place the TKE Installation DVD into the DVD drive of the target TKE.
3. Reboot the TKE with the installation DVD in the DVD drive.
4. When the installation options are presented, type the number 3 to select the frame roll install and press the Enter key:

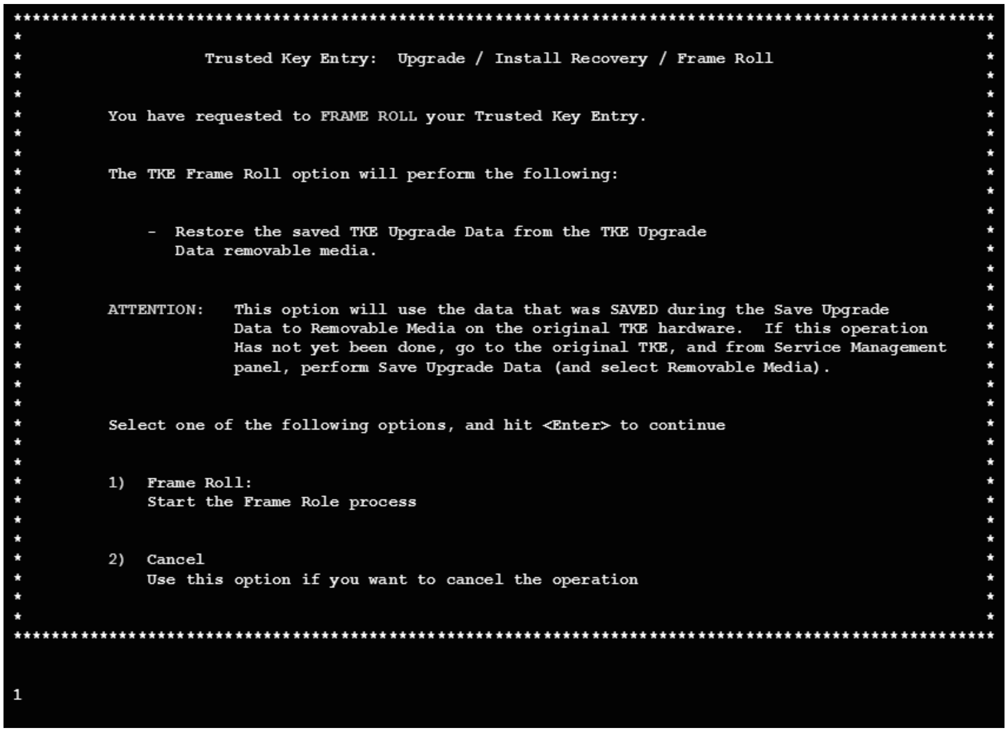
   Note: The exact text on the screen varies between different levels of TKE.



```
****************************************************************************************************
*                                                                                                  *
*                   Trusted Key Entry:  Upgrade / Install Recovery / Frame Roll                    *
*                                                                                                  *
*                                                                                                  *
*         Use this MENU to install/upgrade your TKE hard disk from the base code load DVD.         *
*                                                                                                  *
*                                                                                                  *
*         ATTENTION: Continuing with this task will result in the destruction of the               *
*                    Information currently stored in your TKE hard disk.                           *
*                                                                                                  *
*                                                                                                  *
*         Select one of the following options, and hit <Enter> to continue                         *
*                                                                                                  *
*                                                                                                  *
*         1)  Upgrade:                                                                             *
*             Use this option to upgrade your current TKE hard disk to a new code level.           *
*             This option will preserve previously saved upgrade data on disk, and                 *
*             Restore it after the upgrade has been completed.                                     *
*                                                                                                  *
*                                                                                                  *
*         2)  Install/Recovery:                                                                    *
*             Use this option when you are installing TKE code for the first time or if            *
*             Using the base code load DVD. You will have the option to insert the backup          *
*             Media to restore previously backed up critical console data.                         *
*                                                                                                  *
*                                                                                                  *
*         3)  Frame Roll:                                                                          *
*             Use this option when you have received new, preloaded TKE hardware, and you are      *
*             Replacing your old TKE hardware; or when you are upgrading from D6x/D7x to D8x.      *
*                                                                                                  *
*                                                                                                  *
*         4)  Cancel                                                                               *
*             Use this option if you want to cancel the operation                                  *
*                                                                                                  *
*                                                                                                  *
****************************************************************************************************

3
```

Figure 11. Select the Frame Roll option

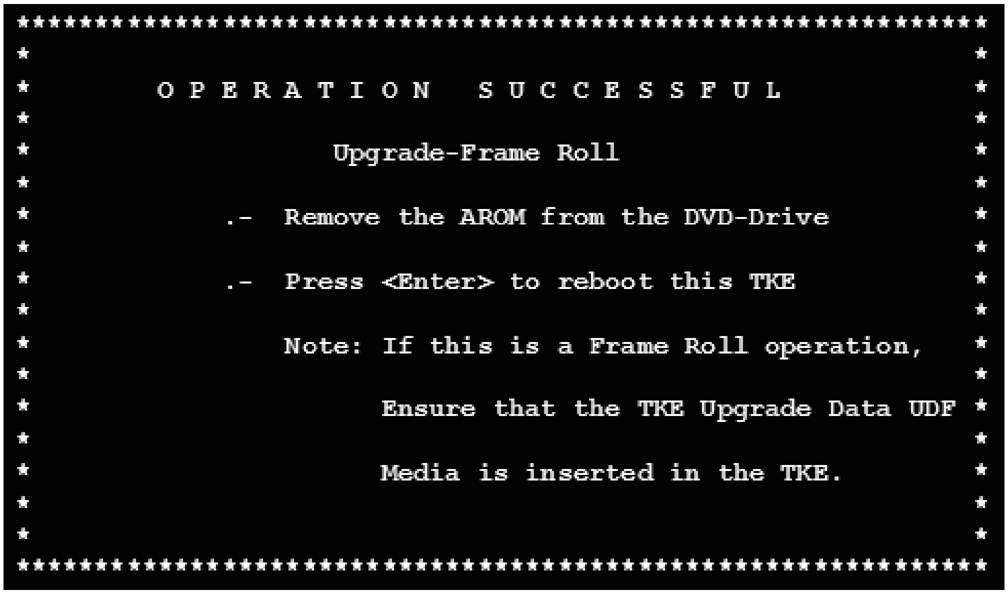
5. When the confirmation screen appears, type the number 1 to start the process and press the Enter key:



```
******************************************************************************************************
*                                                                                                    *
*                   Trusted Key Entry:  Upgrade / Install Recovery / Frame Roll                      *
*                                                                                                    *
*                                                                                                    *
*         You have requested to FRAME ROLL your Trusted Key Entry.                                   *
*                                                                                                    *
*                                                                                                    *
*         The TKE Frame Roll option will perform the following:                                      *
*                                                                                                    *
*                                                                                                    *
*             -  Restore the saved TKE Upgrade Data from the TKE Upgrade                             *
*                Data removable media.                                                               *
*                                                                                                    *
*                                                                                                    *
*         ATTENTION:   This option will use the data that was SAVED during the Save Upgrade          *
*                      Data to Removable Media on the original TKE hardware.  If this operation      *
*                      Has not yet been done, go to the original TKE, and from Service Management    *
*                      panel, perform Save Upgrade Data (and select Removable Media).                *
*                                                                                                    *
*                                                                                                    *
*         Select one of the following options, and hit <Enter> to continue                          *
*                                                                                                    *
*                                                                                                    *
*         1)  Frame Roll:                                                                            *
*             Start the Frame Role process                                                           *
*                                                                                                    *
*                                                                                                    *
*         2)  Cancel                                                                                 *
*             Use this option if you want to cancel the operation                                    *
*                                                                                                    *
*                                                                                                    *
******************************************************************************************************


1
```

Figure 12. Start the Frame Roll process

6. When the message requesting you to remove the DVD from the drive appears:
   a. Remove the DVD
   b. If target TKE is V 6.0 or less, place DVD-RAM with save upgrade data into the DVD drive
   c. Press the Enter key



```
*************************************************************
*                                                           *
*        O P E R A T I O N   S U C C E S S F U L            *
*                                                           *
*                   Upgrade-Frame Roll                      *
*                                                           *
*            .-  Remove the AROM from the DVD-Drive         *
*                                                           *
*            .-  Press <Enter> to reboot this TKE           *
*                                                           *
*                Note: If this is a Frame Roll operation,   *
*                                                           *
*                      Ensure that the TKE Upgrade Data UDF *
*                                                           *
*                      Media is inserted in the TKE.        *
*                                                           *
*                                                           *
*************************************************************
```

Figure 13. Operation successful message

7. After several minutes, which will include multiple automatic restarts, your TKE will finish its install process. When the process is complete:

- The Trusted Key Entry Console Welcome screen will be displayed.
- Your customer unique data is now on the target TKE. However, additional steps are needed to configure your TKE's local crypto adapter.

Target TKE action: Load roles and profiles into the TKE's local crypto adapter

The save upgrade data that was restored onto the target TKE contains the role and profile definition files that will be used to load the roles and profiles onto the target TKE's local crypto adapter.

There are two methods that can be used to do the loads:

- Manually load each role and profile onto the TKE's local crypto adapter through the Cryptographic Node Management (CNM) Utility. See "Manually load roles and profiles into the TKE's local crypto adapter" for more information.
- Create a CCA Node Initialization (CNI) file and use it as input to the Cryptographic Node Management (CNM) Batch Initialization utility to load the roles and profiles onto the target TKE local crypto adapter. See "Load roles and profiles using the Cryptographic Node Management (CNM) Batch Initialization application" on page 59 for more information.

Manually load roles and profiles into the TKE's local crypto adapter

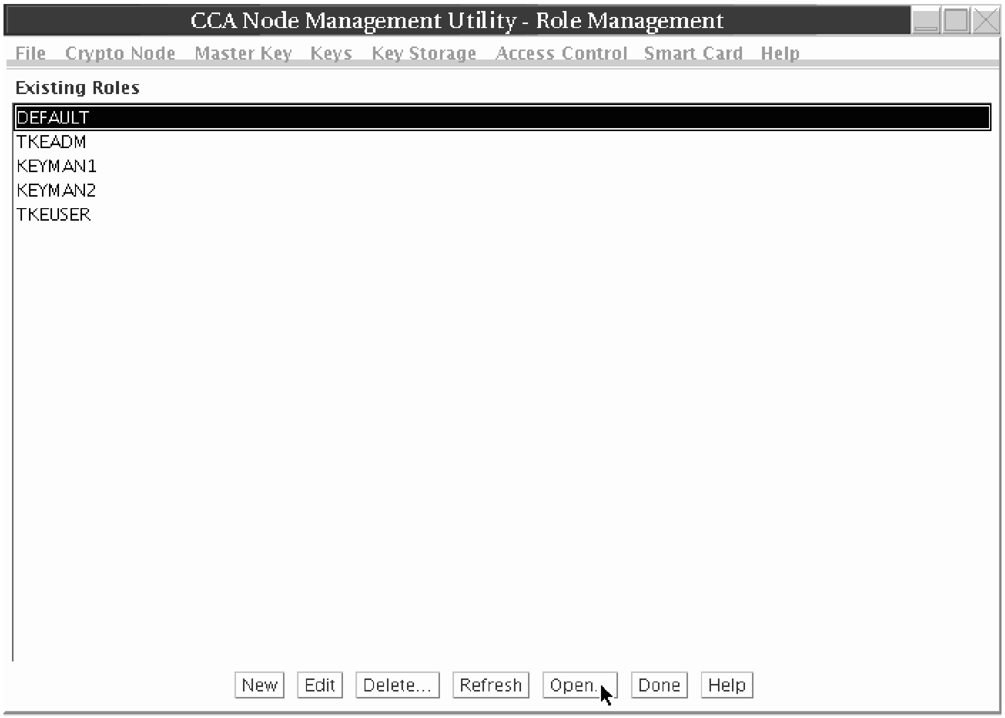
We recommend you load all roles onto the TKE's local crypto adapter before you attempt to load any profiles. If a profile's role does not exist, the profile will not have authority to anything.

Loading roles: Roles are loaded onto the TKE's local crypto adapter through the Cryptographic Node Management (CNM) Utility. The following steps describe how you load a role through this utility.

1. From the left pane on the Trusted Key Entry Console, select Trusted Key Entry.
2. From the right pane on the Trusted Key Entry Console, open the CNM Utility.

   Note: You will be required to log on to the application.
   - If you use passphrase profiles, sign on with TKEADM or a user with equivalent authority.
   - If you use smart card profiles, sign on with a profile that has SCTKEADM authority.
   - If you initialized your TKE's local crypto adapter to use smart card profiles and you don't have any smart card profile's loaded yet, you must:
     a. Sign on to the TKE console in Privileged Mode Access with the ADMIN user ID.
     b. Sign on to the CNM Utility with the "User default role" user ID.
3. Navigate to the list of roles currently on this TKE's local crypto adapter. From the CCA Node Management Utility window, select **Access Control -> Roles**.

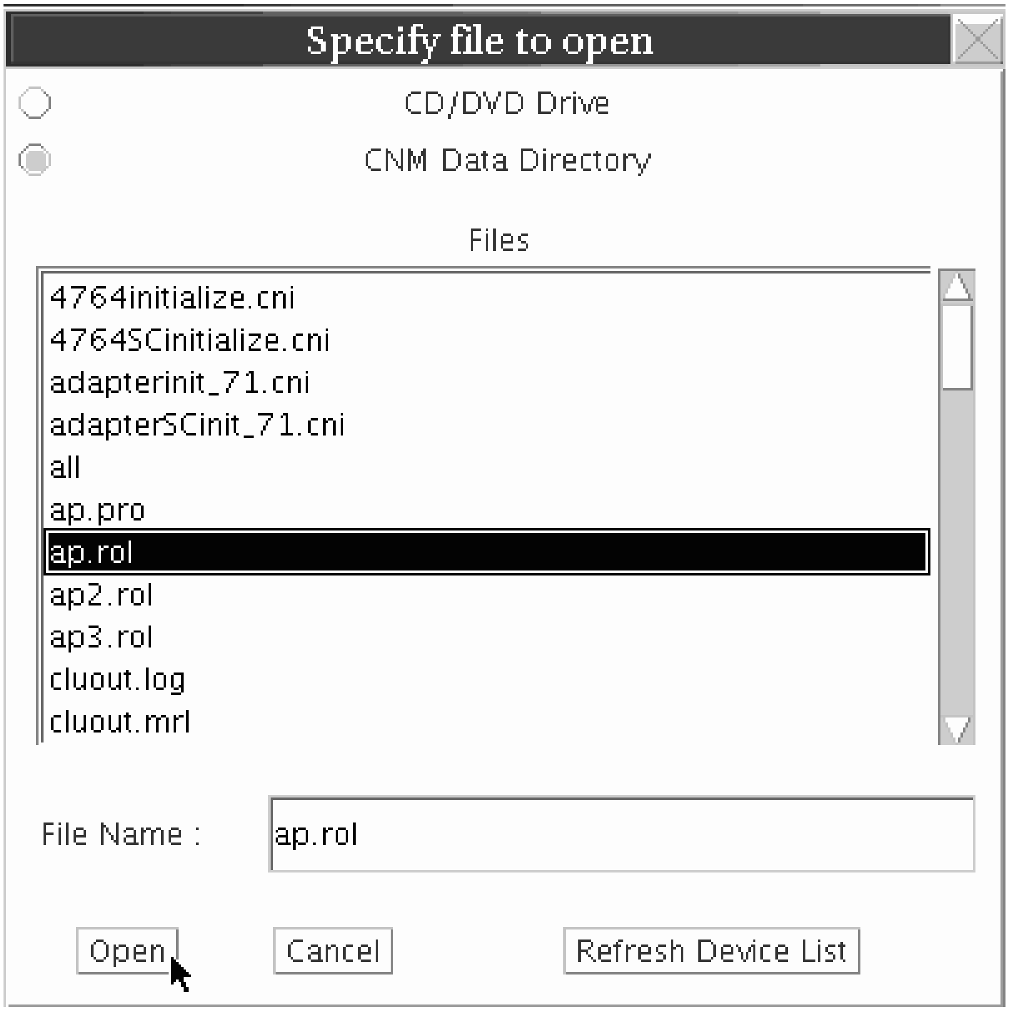
   The list of existing roles is displayed.
4. Repeat the following steps for every role you want to load onto the target TKE local crypto adapter:
   a. From the list window, press the **Open** button. This will allow you to select one of the role definition files you migrated from the source TKE.


CCA Node Management Utility - Role Management
File Crypto Node Master Key Keys Key Storage Access Control Smart Card Help
Existing Roles
New
Edit
Delete...
Refresh
Open...
Done
Help

DEFAULT
TKEADM
KEYMAN1
KEYMAN2
TKEUSER

Figure 14. Press the Open button

b. From the Files list, highlight the role definition file you want to work with and press the **Open** button.



○ CD/DVD Drive

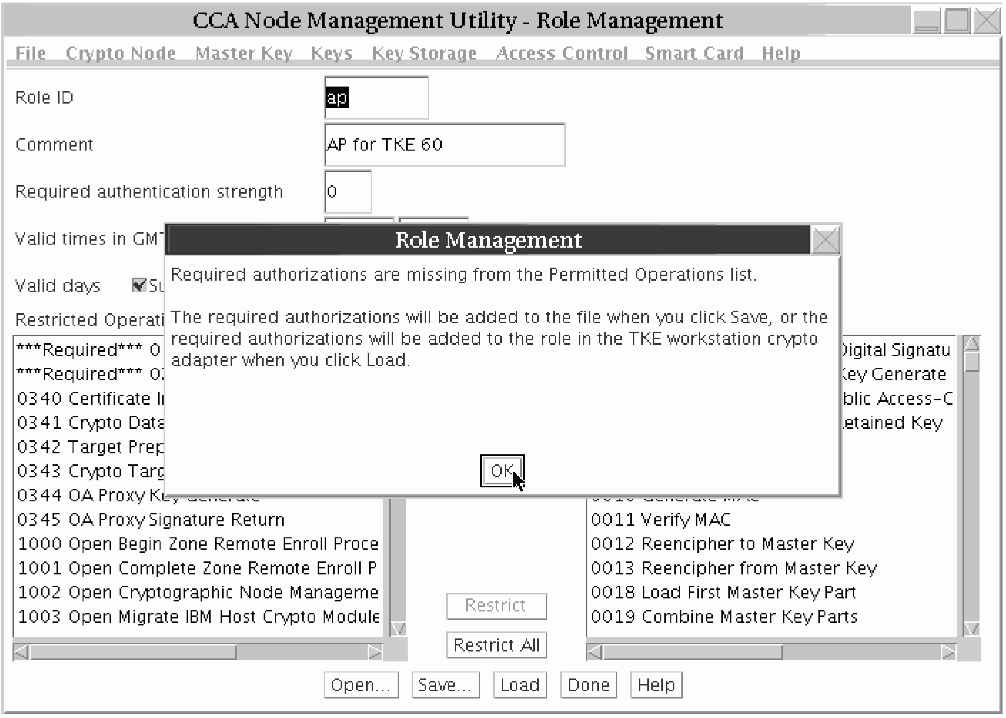
● CNM Data Directory

4764initialize.cni
4764SCinitialize.cni
adapterinit_71.cni
adapterSCinit_71.cni
all
ap.pro
ap.rol
ap2.rol
ap3.rol
cluout.log
cluout.mrl

File Name : ap.rol

Figure 15. Open the role definition file

c. While the file is being opened, the code may detect that your role's definition is missing some required authorizations. If this condition is detected, a message is displayed telling you how the TKE will correct the role definition file or role for you. Press the **OK** button after you have read the message.



Role ID ap

Comment AP for TKE 60

Required authentication strength 0

Valid times in GM

Valid days ☑Su

Restricted Operati

Required 0
Required 0
0340 Certificate I
0341 Crypto Data
0342 Target Prep
0343 Crypto Targ
0344 OA Proxy K
0345 OA Proxy Signature Return
1000 Open Begin Zone Remote Enroll Proce
1001 Open Complete Zone Remote Enroll P
1002 Open Cryptographic Node Manageme
1003 Open Migrate IBM Host Crypto Module

Digital Signatu
Key Generate
blic Access-C
etained Key
0011 Verify MAC
0012 Reencipher to Master Key
0013 Reencipher from Master Key
0018 Load First Master Key Part
0019 Combine Master Key Parts

Role Management

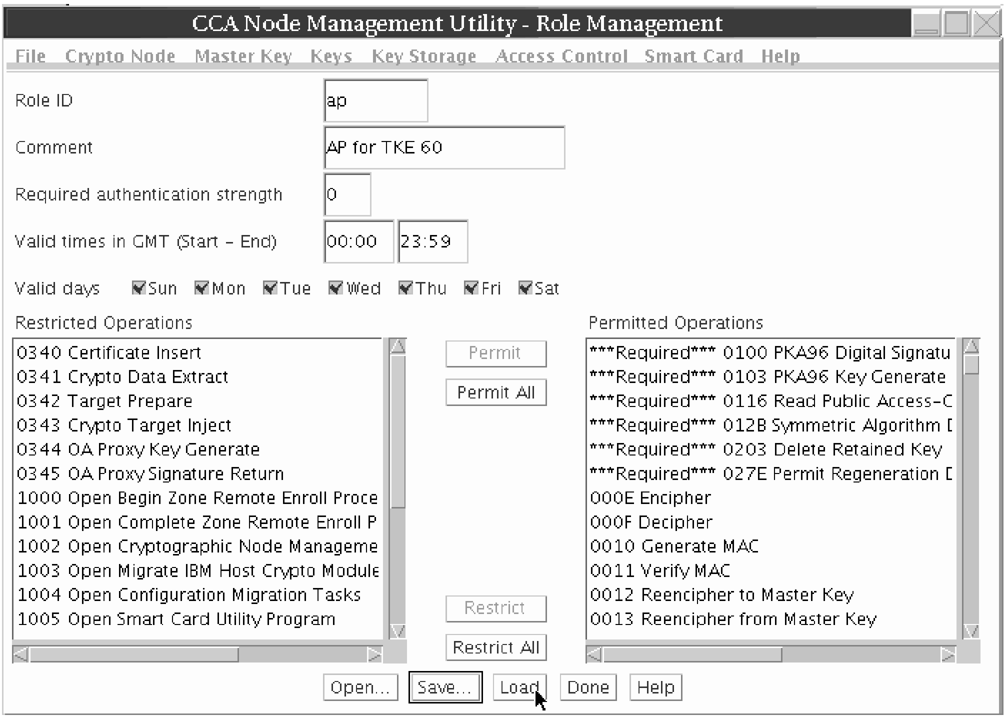
Required authorizations are missing from the Permitted Operations list.

The required authorizations will be added to the file when you click Save, or the required authorizations will be added to the role in the TKE workstation crypto adapter when you click Load.

Figure 16. Required authorizations are missing

d. To install this role on your TKE's local crypto adapter, press the **Load** button.

Note: If your role definition file is missing required authorizations and you want to update the role definition file, we recommend you press the **Save** button before you press the **Load** button. The save operation will leave you on the Edit screen after the role definition file has been fixed. If you press the **Load** button without pressing the **Save** button first, the profile on the TKE's local crypto adapter will include all the required operations. However, you will have to reopen the role definition file to fix it.


CCA Node Management Utility - Role Management
File Crypto Node Master Key Keys Key Storage Access Control Smart Card Help
Permit
Permit All
Restrict
Restrict All
Open...
Save...
Load
Done
Help

Role ID: ap

Comment: AP for TKE 60

Required authentication strength: 0

Valid times in GMT (Start – End): 00:00 23:59

Valid days ☑Sun ☑Mon ☑Tue ☑Wed ☑Thu ☑Fri ☑Sat

Restricted Operations

```
0340 Certificate Insert
0341 Crypto Data Extract
0342 Target Prepare
0343 Crypto Target Inject
0344 OA Proxy Key Generate
0345 OA Proxy Signature Return
1000 Open Begin Zone Remote Enroll Proce
1001 Open Complete Zone Remote Enroll P
1002 Open Cryptographic Node Manageme
1003 Open Migrate IBM Host Crypto Module
1004 Open Configuration Migration Tasks
1005 Open Smart Card Utility Program
```

Permitted Operations

```
***Required*** 0100 PKA96 Digital Signatu
***Required*** 0103 PKA96 Key Generate
***Required*** 0116 Read Public Access-C
***Required*** 012B Symmetric Algorithm D
***Required*** 0203 Delete Retained Key
***Required*** 027E Permit Regeneration D
000E Encipher
000F Decipher
0010 Generate MAC
0011 Verify MAC
0012 Reencipher to Master Key
0013 Reencipher from Master Key
```

Figure 17. Press Load to install the role

e. A message window displays, indicating that the role was successfully created. Press **OK** to close this message window.

f. The role has been created and you have returned to the list of roles on the TKE local crypto adapter. Repeat the create role steps until all of the roles you need have been loaded onto the TKE's local Crypto Adapter. When you are finished, exit this screen.

Loading profiles: Profiles are loaded onto the TKE's local crypto adapter through the CNM Utility. The following steps describe how you load a profile through this utility:

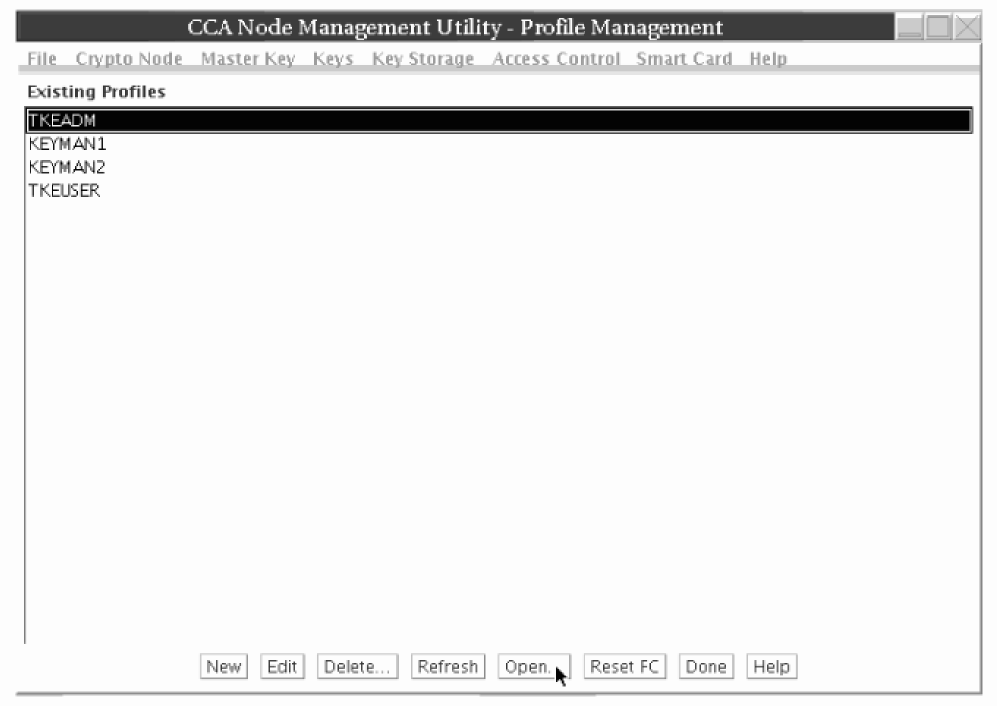
1. From the left pane on the Trusted Key Entry Console, select Trusted Key Entry.
2. From the right pane on the Trusted Key Entry Console, open the CNM Utility.

   Note: You will be required to log on to the application.
   - If you use passphrase profiles, sign on with TKEADM or a user with equivalent authority.
   - If you use smart card profiles, sign on with a profile that has SCTKEADM authority.
   - If you initialized your TKE's local crypto adapter to use smart card profiles and you do not have any smart card profiles loaded yet, you must:
     a. Sign on to the TKE console in Privileged Mode Access with the ADMIN user ID.
     b. Sign on to the CNM utility with the “User default role” user ID.
3. Navigate to the list of profiles currently on this TKE's local crypto adapter. From the CCA Node Management Utility window, select **Access Control -> Profiles**:

   The list of existing profiles is displayed.

4. Repeat the following steps for every profile you want to load onto the target TKE local crypto adapter:

   a. From the list window, press the **Open** button. This will allow you to select one of the profile definition files you brought over from the source TKE.

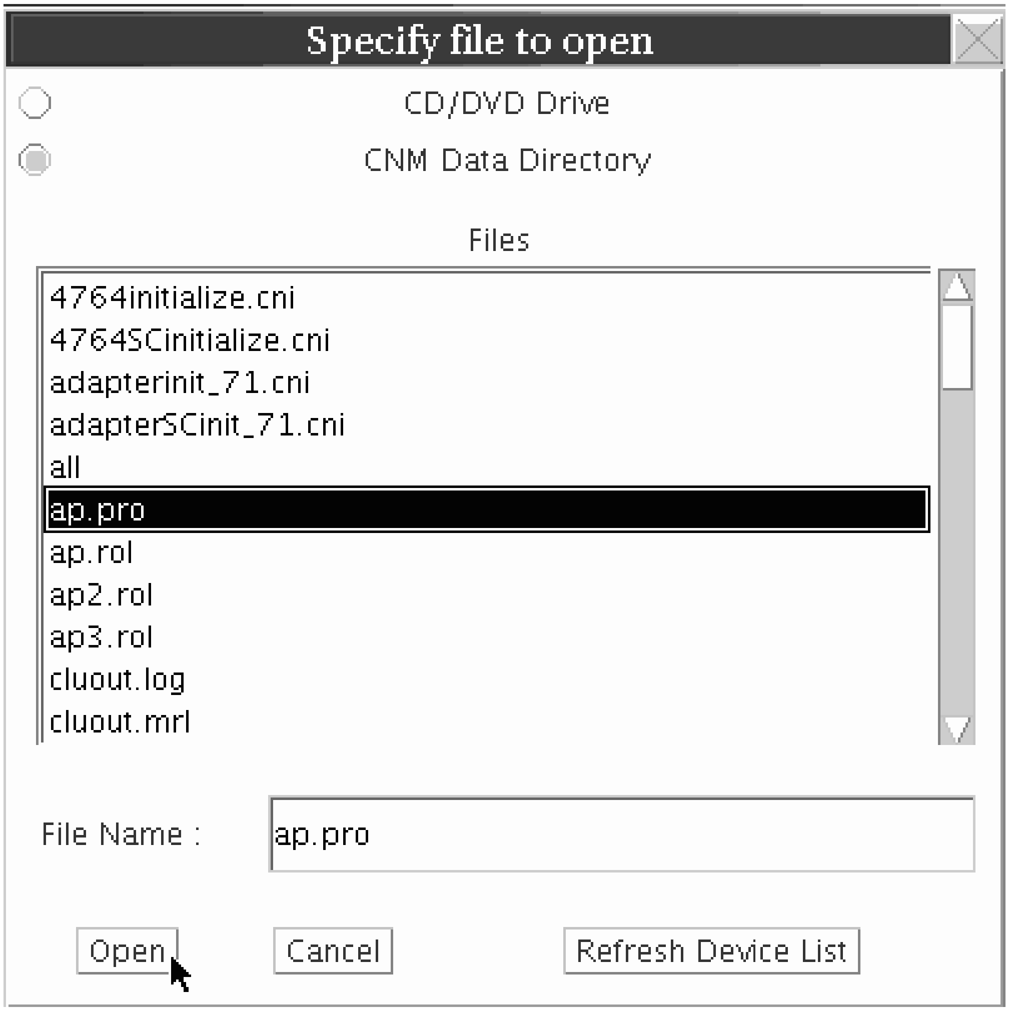


Existing Profiles

TKEADM
KEYMAN1
KEYMAN2
TKEUSER

Figure 18. Press the Open button

   b. From the Files list, highlight the profile definition file you want to work with and press the **Open** button.



Specify file to open

○ CD/DVD Drive

● CNM Data Directory

Files

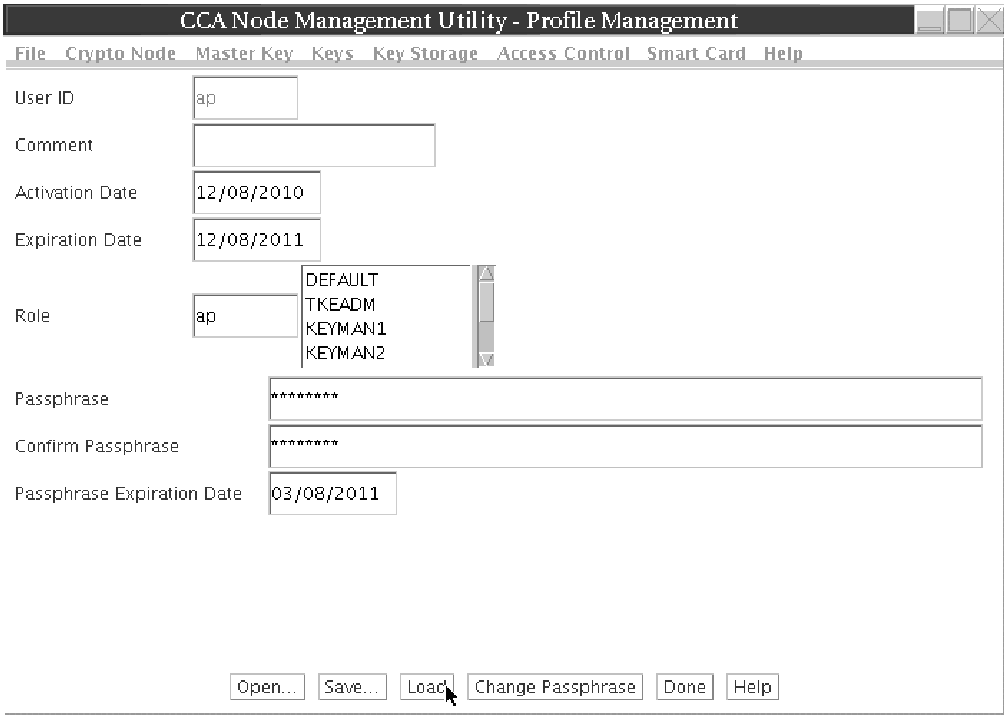
- 4764initialize.cni
- 4764SCinitialize.cni
- adapterinit_71.cni
- adapterSCinit_71.cni
- all
- ap.pro
- ap.rol
- ap2.rol
- ap3.rol
- cluout.log
- cluout.mrl

File Name : ap.pro

Figure 19. Open the profile definition file

c. If loading a:

- Passphrase profile, a Passphrase is required before the profile can be either loaded or saved. The passphrase you enter does not have to match the current definition file's passphrase. From the Edit screen, enter the same value for both Passphrase fields and press the **Load** button.


CCA Node Management Utility - Profile Management
File Crypto Node Master Key Keys Key Storage Access Control Smart Card Help
DEFAULT
TKEADM
KEYMAN1
KEYMAN2
Open...
Save...
Load
Change Passphrase
Done
Help

User ID: ap

Comment:

Activation Date: 12/08/2010

Expiration Date: 12/08/2011

Role: ap

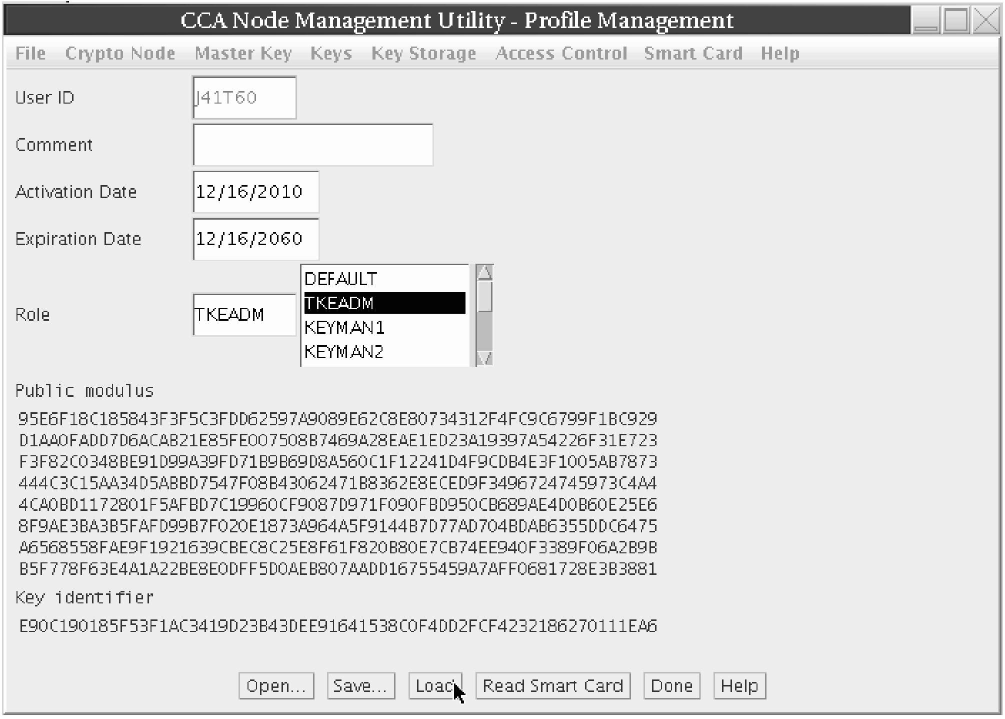
Passphrase: *********

Confirm Passphrase: *********

Passphrase Expiration Date: 03/08/2011

Figure 20. Load a passphrase profile

- Smart card or group profile: From the Edit screen, press the **Load** button.


CCA Node Management Utility - Profile Management
File Crypto Node Master Key Keys Key Storage Access Control Smart Card Help
DEFAULT
TKEADM
KEYMAN1
KEYMAN2
Open...
Save...
Load
Read Smart Card
Done
Help

User ID: J41T60

Comment:

Activation Date: 12/16/2010

Expiration Date: 12/16/2060

Role: TKEADM

```
Public modulus
95E6F18C185843F3F5C3FDD62597A9089E62C8E80734312F4FC9C6799F1BC929
D1AA0FADD7D6ACAB21E85FE007508B7469A28EAE1ED23A19397A54226F31E723
F3F82C0348BE91D99A39FD71B9B69D8A560C1F12241D4F9CDB4E3F1005AB7873
444C3C15AA34D5ABBD7547F08B43062471B8362E8ECED9F3496724745973C4A4
4CA0BD1172801F5AFBD7C19960CF9087D971F090FBD950CB689AE4D0B60E25E6
8F9AE3BA3B5FAFD99B7F020E1873A964A5F9144B7D77AD704BDAB6355DDC6475
A6568558FAE9F1921639CBEC8C25E8F61F820B80E7CB74EE940F3389F06A2B9B
B5F778F63E4A1A22BE8E0DFF5D0AEB807AADD16755459A7AFF0681728E3B3881
Key identifier
E90C190185F53F1AC3419D23B43DEE91641538C0F4DD2FCF4232186270111EA6
```

Figure 21. Load a smart card or group profile

d. A message window displays, indicating that the profile was successfully created. Press OK to close this message window.

e. The profile has been created and you have returned to the list of profiles on the TKE local crypto adapter. Repeat the create profile steps until all of the profiles you need have been created. When you are finished, exit this screen.

Load roles and profiles using the Cryptographic Node Management (CNM) Batch Initialization application

The Cryptographic Node Management (CNM) Batch Initialization application of the TKE is used to run a series of commands on the TKE's local crypto adapter. The CNM Batch Initialization feature can be used to load a set of roles and profiles onto a TKE's local crypto adapter from a set of role and profile definition files.

In the migration scenario, a set of role and profile definition files was collected from a source TKE using the Save Upgrade Data feature of TKE. The same set of role and profile definition files was placed on a target TKE when the upgrade data was used during a frame roll install. This section will describe how to use the batch initialization feature to load the set of roles and profiles onto the target TKE's local crypto adapter using the role and profile definition files that were applied to the target system.

Cryptographic Node Management (CNM) Batch Initialization basics: When you run the batch utility, you must provide the name of a CCA Node Initialization (CNI) file. The CNI file contains the list of commands that are run on the TKE's local cryptographic adapter. The batch utility reads the file and executes each command in the order it appears in the file.

Note: IBM-supplied roles and profiles are loaded onto a TKE's local crypto adapter when the TKE's IBM Crypto Adapter Initialization application is run. The application uses the CNI batch utility to load the roles and profiles. This invocation of the CNI batch utility uses an IBM-supplied CNI file and a set of IBM-supplied role and profile definition files to initialize the TKE's local crypto adapter.

Migration task overview: To use the CNI batch utility to load roles and profiles onto a TKE's local crypto adapter, you must do two things:

1. Create a CNI file with list of load role and profile commands to run
2. Invoke the CNM batch initialization utility

Create a CCA Node Initialization (CNI) file: CNI files are created or changed though the CNI editor found in Cryptographic Node Management (CNM) Utility. The following steps describe how to create the CNI file.

1. From the left pane on the Trusted Key Entry Console, select Trusted Key Entry.
2. From the right pane on the Trusted Key Entry Console, open the Cryptographic Node Management Utility

   Note: You will be required to log on to the application.
   - If you use passphrase profiles, you must sign on with TKEADM or a user with equivalent authority.
   - If you use smart card profiles, you must sign on with a profile that has SCTKEADM authority.
   - If you initialized your TKE's local crypto adapter to use smart card profiles and you do not have any smart card profiles loaded yet, you must:

   a. Sign on to the TKE console in Privileged Mode Access with the ADMIN user ID.
   b. Sign on to the CNM utility with the “User default role” user ID.

3. Navigate to the CNI Editor. From the CCA Node Management Utility window, select **File -> CNI Editor**

   The CNI Edit screen is displayed.

   There are only two types of commands you need to put in your CNI file.

   - Load user role
   - Load user profile

   CNI Batch Utility behaviors:

   - In any TKE release, if a load role is attempted and the role exists, the role is replaced.
   - In any TKE release, if a load profile is attempted and the profile exists, the batch utility will flag this as an error and will not attempt any more commands from the CNI file.

   CNI Command Order:

   a. Add all of the create role commands.
   b. Add all of the create profile commands for the individual user profiles.
   c. Add all of the create profile commands for the group profiles.

4. Repeat the following steps for every role you want to load onto your TKE’s local Crypto Adapter:

   a. From the CNI Edit screen, highlight “Load user role” and press the **Add** button.

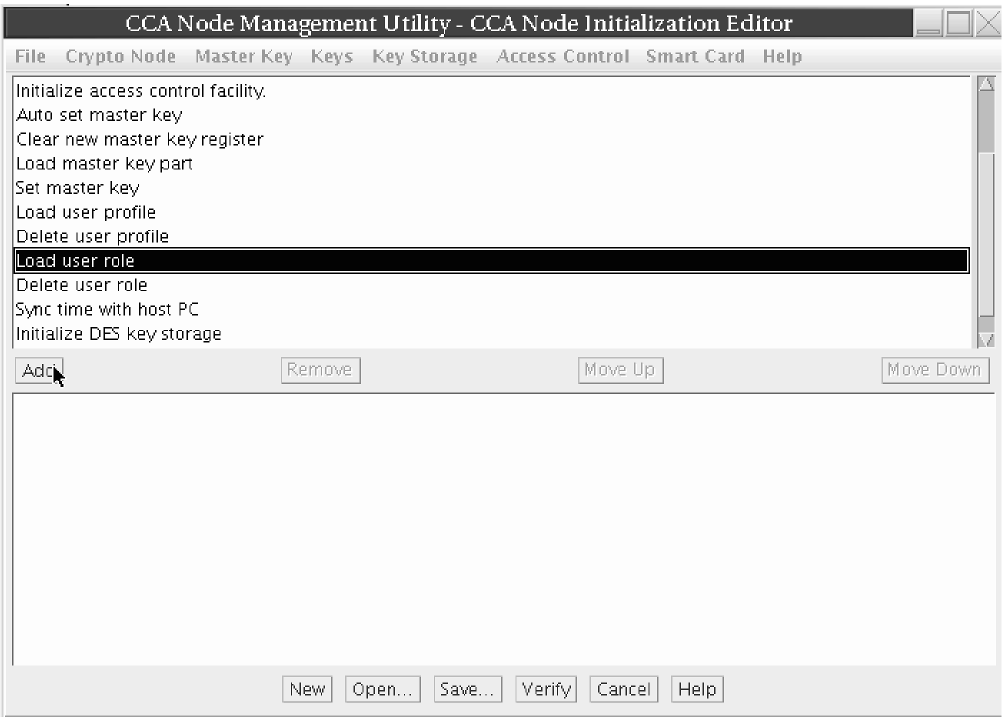
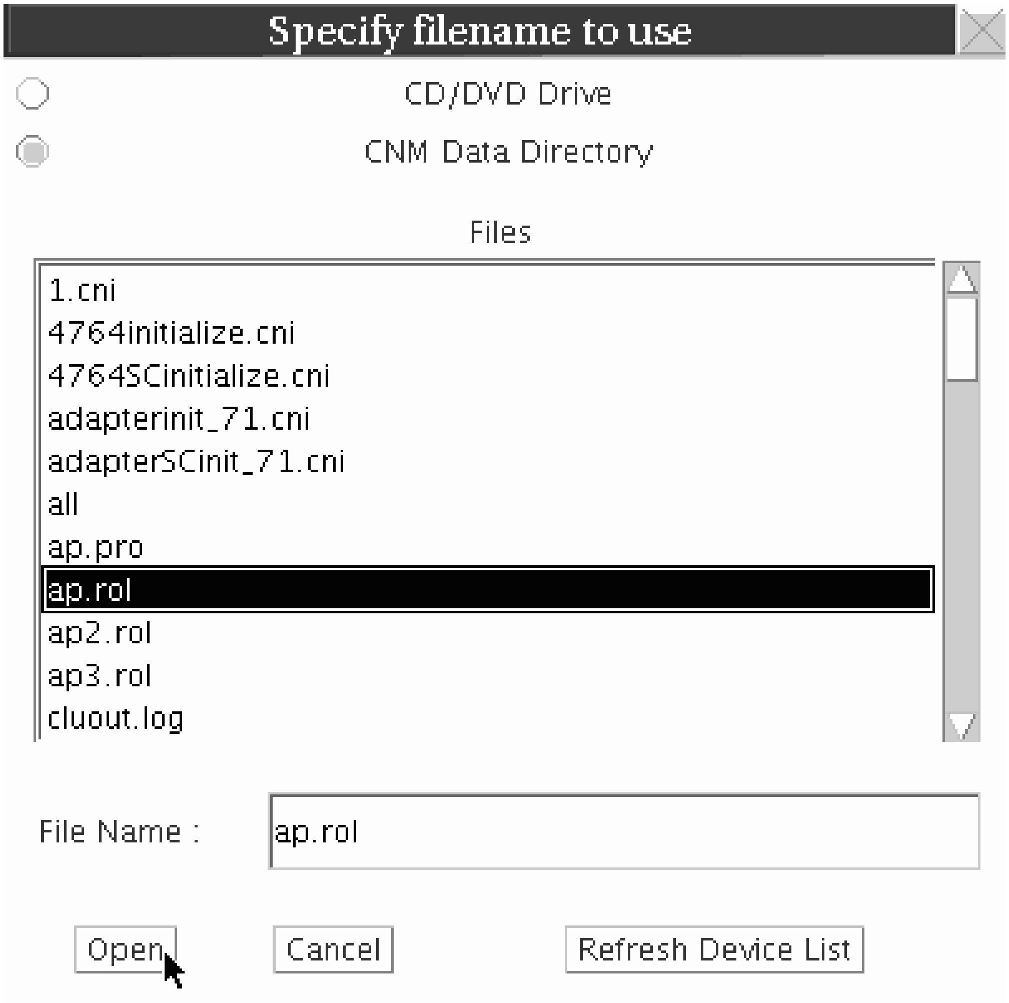


Figure 22. Select Load user role and press the Add button

   b. Select the role definition file for the role to be loaded and press the **Open** button.



○ CD/DVD Drive

● CNM Data Directory

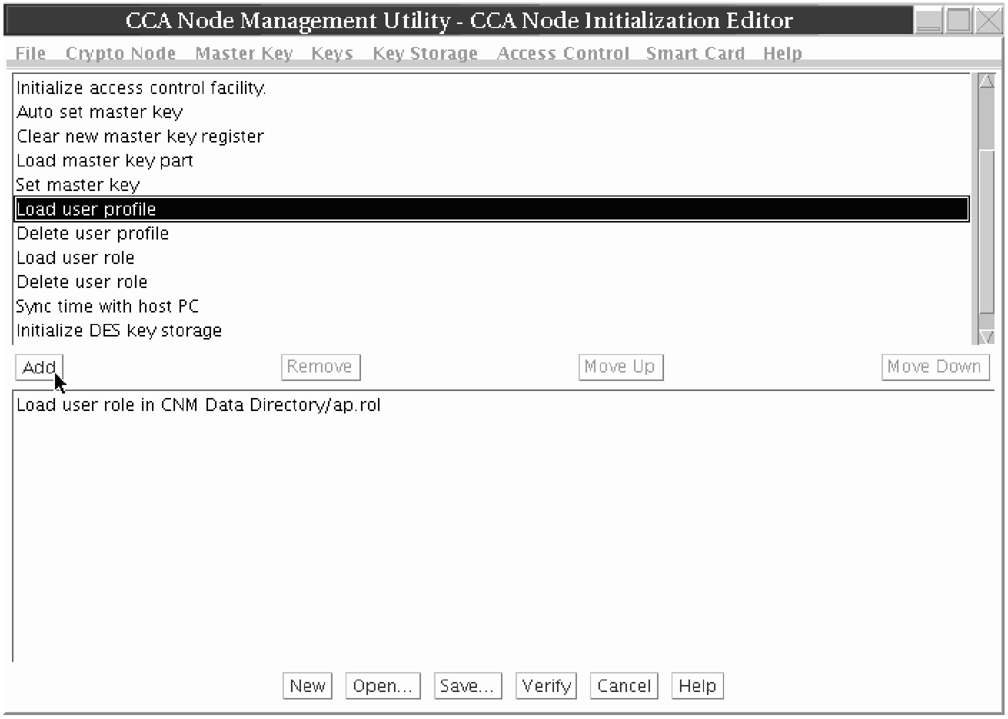
File Name : ap.rol

Figure 23. Open the role definition file

   c. You have returned to the Edit screen. Repeat the add load user role process until all the load user role commands have been added to the list.

5. Repeat the following steps for every profile you want to load onto your TKE's local Crypto Adapter:

   a. Highlight "Load user profile" and press the Add button.

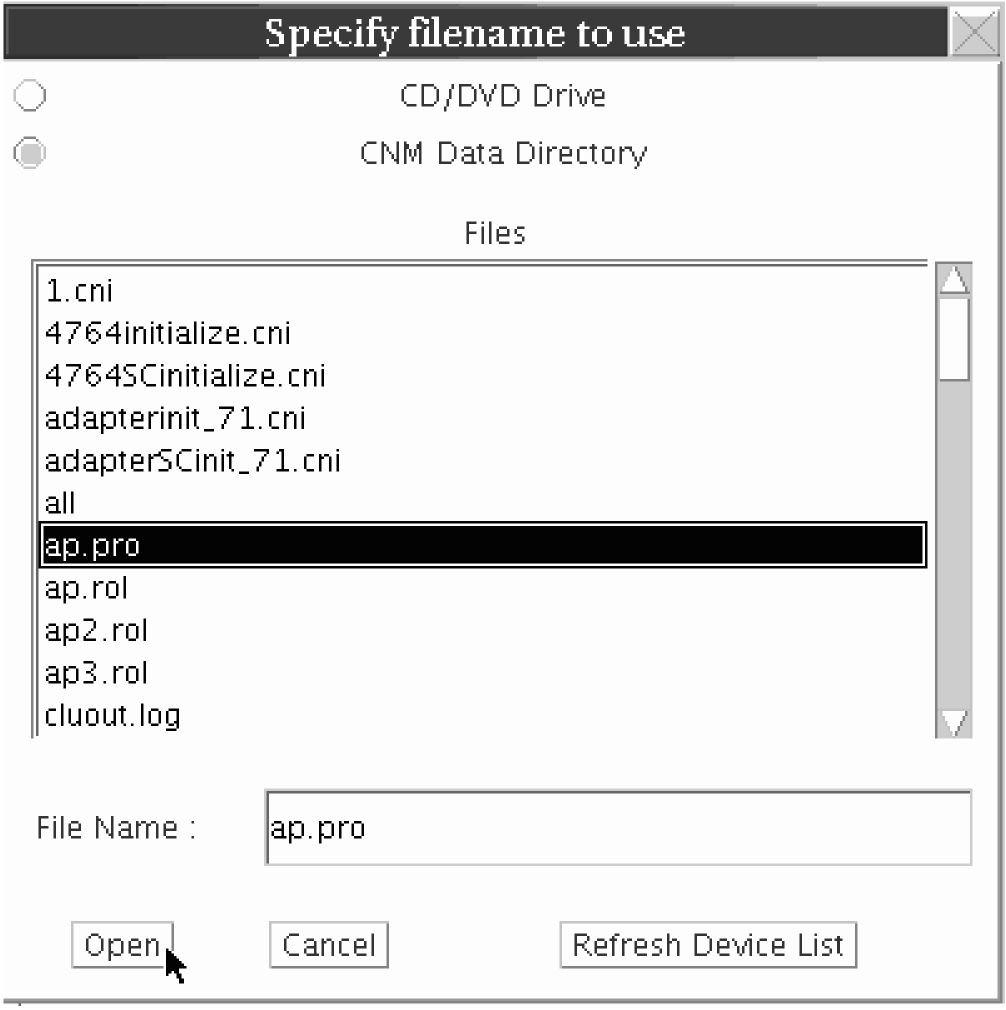


Initialize access control facility.
Auto set master key
Clear new master key register
Load master key part
Set master key
Load user profile
Delete user profile
Load user role
Delete user role
Sync time with host PC
Initialize DES key storage

Load user role in CNM Data Directory/ap.rol

Figure 24. Select Load user profile and press the Add button

b. Select the profile definition file for the profile to be loaded and press the Open button.



○ CD/DVD Drive

● CNM Data Directory

Files:

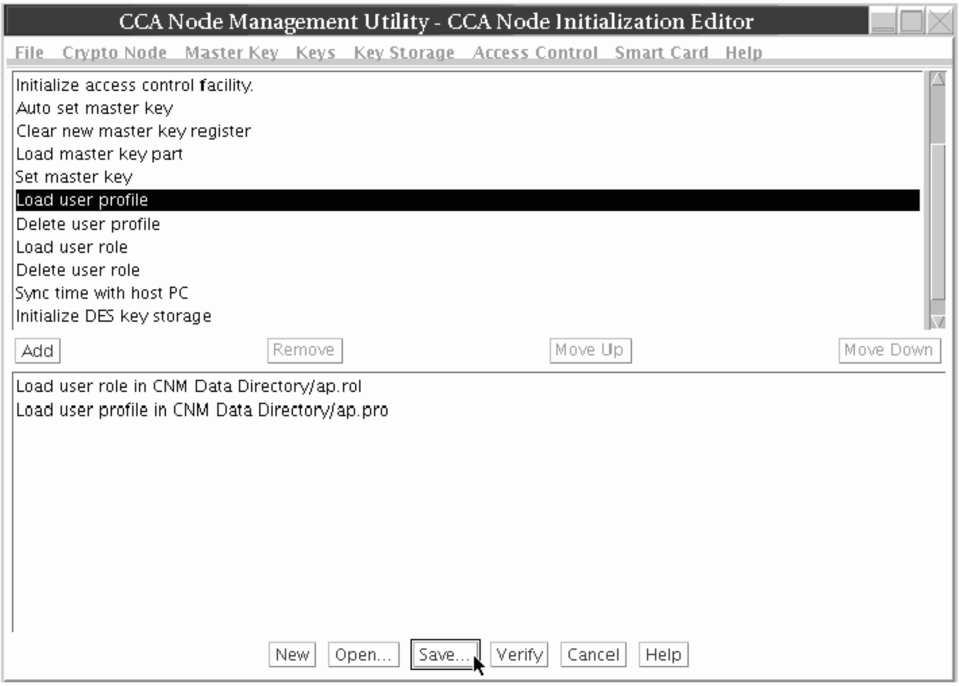
```
1.cni
4764initialize.cni
4764SCinitialize.cni
adapterinit_71.cni
adapterSCinit_71.cni
all
ap.pro
ap.rol
ap2.rol
ap3.rol
cluout.log
```

File Name : ap.pro

Figure 25. Open the profile definition file

c. You have returned to the Edit screen. Repeat the add load user profile process until all the load user profile commands have been added to the list.

6. On the CNI Editor Screen, press the **Save** button.

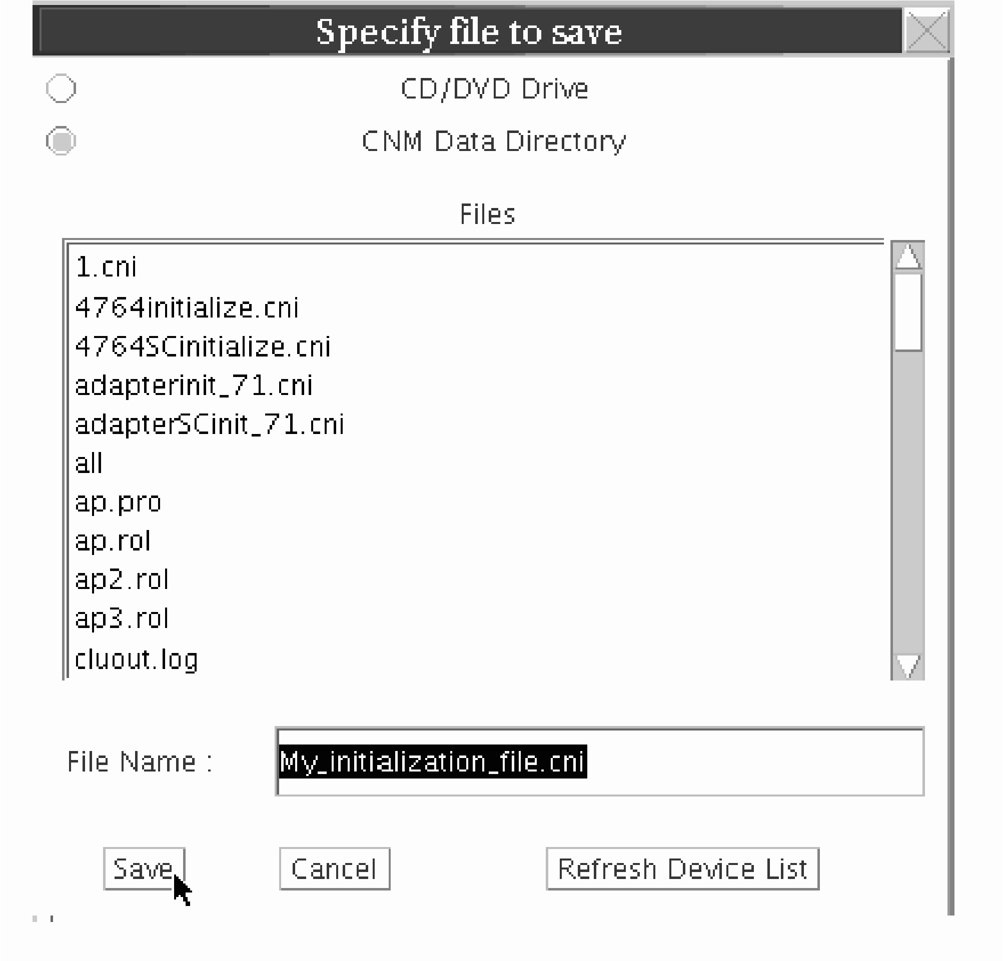


Initialize access control facility.
Auto set master key
Clear new master key register
Load master key part
Set master key
Load user profile
Delete user profile
Load user role
Delete user role
Sync time with host PC
Initialize DES key storage

Load user role in CNM Data Directory/ap.rol
Load user profile in CNM Data Directory/ap.pro

Figure 26. Press the Save button

7. Specify the name of the CNI file in the File Name field. You can type in a new or existing file name or select an existing file from the Files list. After the File Name field is filled in, press the **Save** button to create or replace your CNI file.



Specify file to save

○ CD/DVD Drive

● CNM Data Directory

Files

1.cni
4764initialize.cni
4764SCinitialize.cni
adapterinit_71.cni
adapterSCinit_71.cni
all
ap.pro
ap.rol
ap2.rol
ap3.rol
cluout.log

File Name : My_initialization_file.cni

Figure 27. Specify a CNI file name and press the Save button

8. A message window displays, indicating that the file was saved. Press **OK** to close this message window.
9. Your CNI file is now complete. Press the **Cancel** button to exit the CNI editor.
10. Exit the CNM Utility.

Invoke the CNM Batch Initialization application: The Cryptographic Node Management (CNM) Batch Initialization utility is a separate TKE application. The following steps describe how to use the batch utility to run the commands listed in your CNI file.

The CNM Batch Initialization application is only available when you have signed onto the TKE with the Privileged Mode Access ID of ADMIN.

1. From the left pane on the Trusted Key Entry Console, select Trusted Key Entry.
2. From the right pane on the Trusted Key Entry Console, open the Cryptographic Node Management Batch Initialization application.

   Note: You will not be prompted for a TKE workstation crypto adapter logon when you start the application. However, you must have enough authority to load roles and profiles onto the TKE's Local Crypto Adapter.

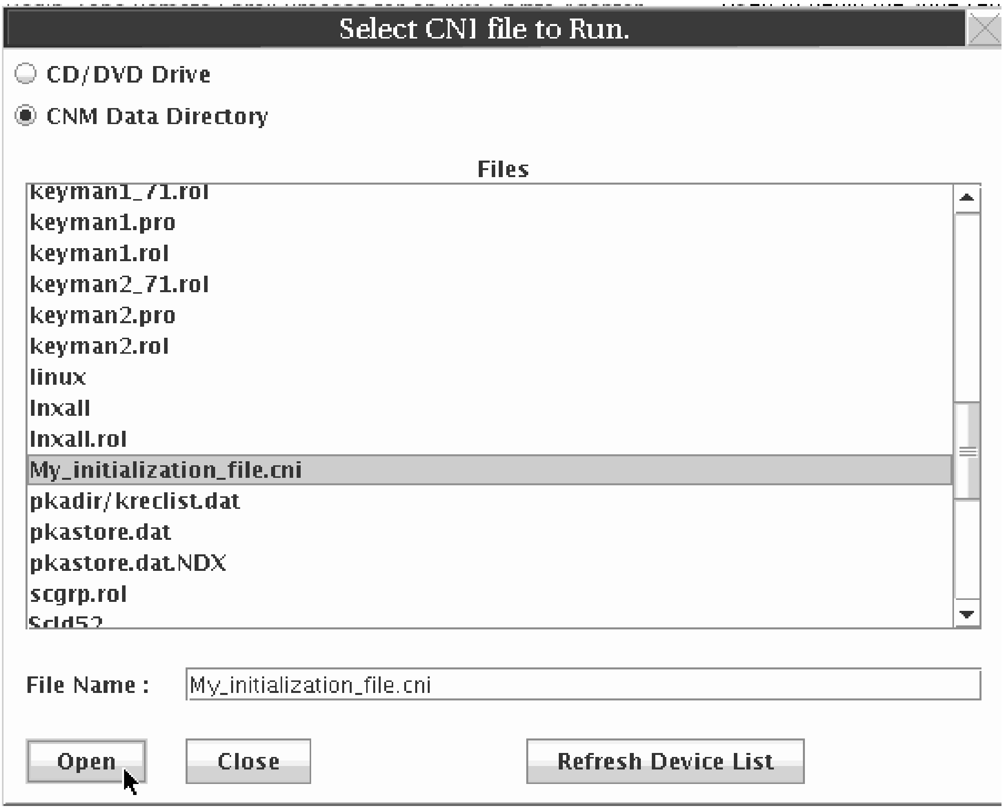
   - If you are not explicitly signed onto the TKE workstation crypto adapter, then the DEFAULT role is in effect.

- If you are explicitly signed onto the TKE workstation crypto adapter, then the role of the profile is in effect.

In either case, the role must have enough authority to perform the LOAD commands. As long as you have not changed the attributes of IBM-supplied roles and profiles, you will be allowed to do the LOAD commands when you are:

- Not explicitly signed on and the DEFAULT role is in effect.
- Explicitly signed on with a passphrase profile that has the TKEADM role.
- Explicitly signed on with a smart card profile that has the SCTKEADM role.

3. From the initial CNM Batch Initialization screen, enter the name of the CNI file to run, and press **Open**.



Select CNI file to Run.

○ CD/DVD Drive

● CNM Data Directory

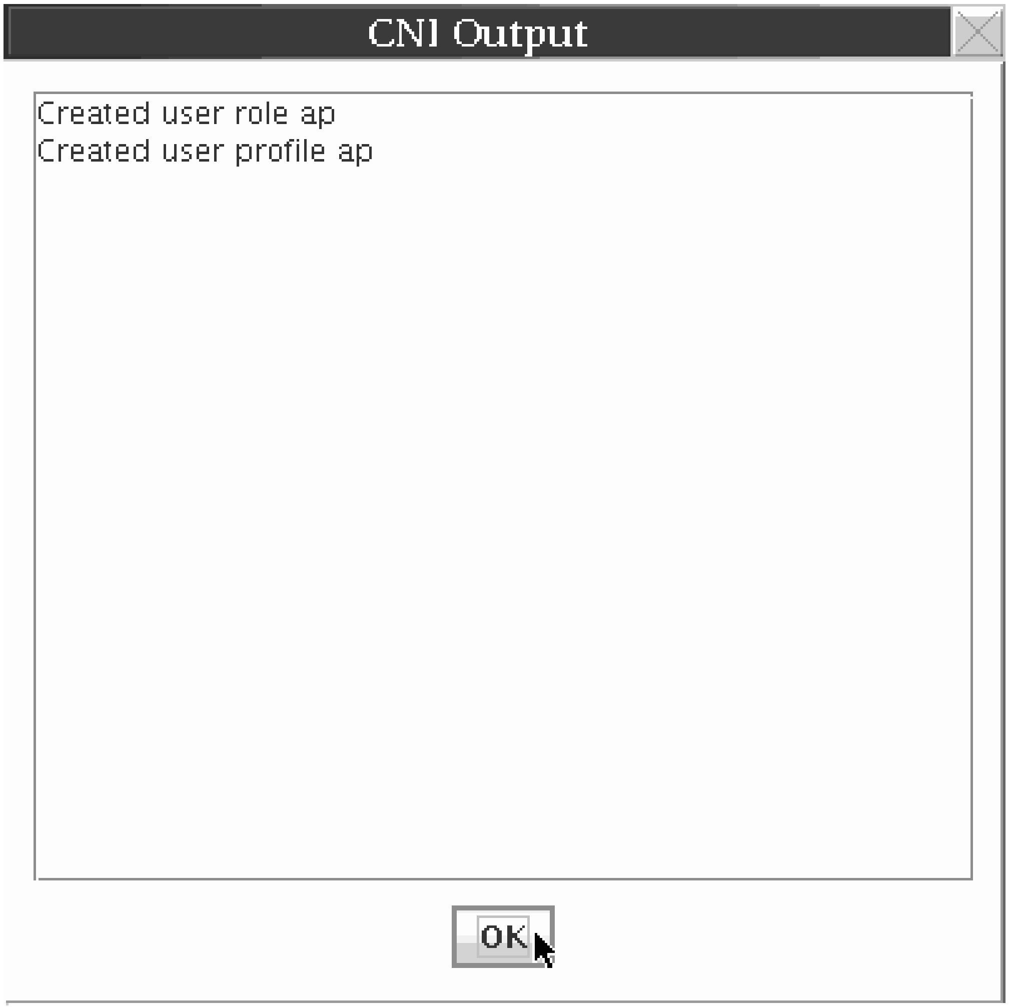
Files

keyman1_71.rol
keyman1.pro
keyman1.rol
keyman2_71.rol
keyman2.pro
keyman2.rol
linux
lnxall
lnxall.rol
My_initialization_file.cni
pkadir/kreclist.dat
pkastore.dat
pkastore.dat.NDX
scgrp.rol
Scld52

File Name : My_initialization_file.cni

Figure 28. Enter a CNI file name, and press Open

4. Press the **OK** button on the CNI Output screen.



```
Created user role ap
Created user profile ap
```

Figure 29. CNI Output

The migration of your roles and profiles is complete.

Chapter 4. TKE Setup and Customization

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

Table 21. 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 8.
- Appendix B, “LPAR Considerations,” on page 313.

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 30. Entry Example

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

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

Figure 31. Example of Reserving a Port

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

Any job with jobname CSFTTCP can connect to this port.

TKE Host Transaction Program Setup

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

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

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

Perform these steps to install the server:

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

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

Figure 32. 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 33. 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 34. 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 35. 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..SCSFCLI0(&MEMBER)'' ''&CPARM'' EXEC'
//STEPLIB   DD DSN=EZA.SEZALINK,DISP=SHR
//SYSABEND  DD SYSOUT=*
//SYSPRINT  DD SYSOUT=*
//SYSEXEC   DD DSN=&LEVEL..SCSFCLI0,DISP=SHR
//SYSPROC   DD DSN=&LEVEL..SCSFCLI0,DISP=SHR
//SYSTSPRT  DD SYSOUT=*
//SYSTSIN   DD DUMMY
//TKEPARMS  DD DSN=&LEVEL..SAMPLIB(CSFTPRM),DISP=SHR
//*
//* customize the DSN to be the TCP/IP data set on your system
//*
//*SYSTCPD   DD DSN=TCPIP.SEZAINST(TCPDATA),DISP=SHR
//         PEND CSFTTCP
//* -----------------------------------------------------------------
```

Figure 36. 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 or later, 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 69).

    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 37. Start the TKE server

Note: If you encounter problems during the start of CSFTTCP, the documented Errortype and Reason Codes are located within the REXX clist CSFTHTP3.

Cancel the TKE server

To cancel the TKE server:

```
S CSFTCTCP
```

Figure 38. 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.

| You can determine if you are signed on to the TKE in privileged mode by looking at
| the upper right-hand corner of the TKE console. When you are signed on in
| privileged mode, the ID is listed in the area.

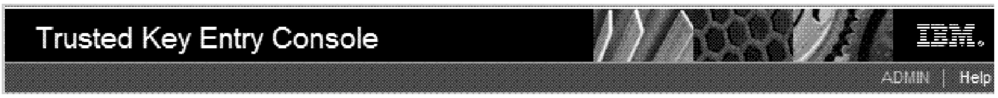


Figure 39. Login with ADMIN user name

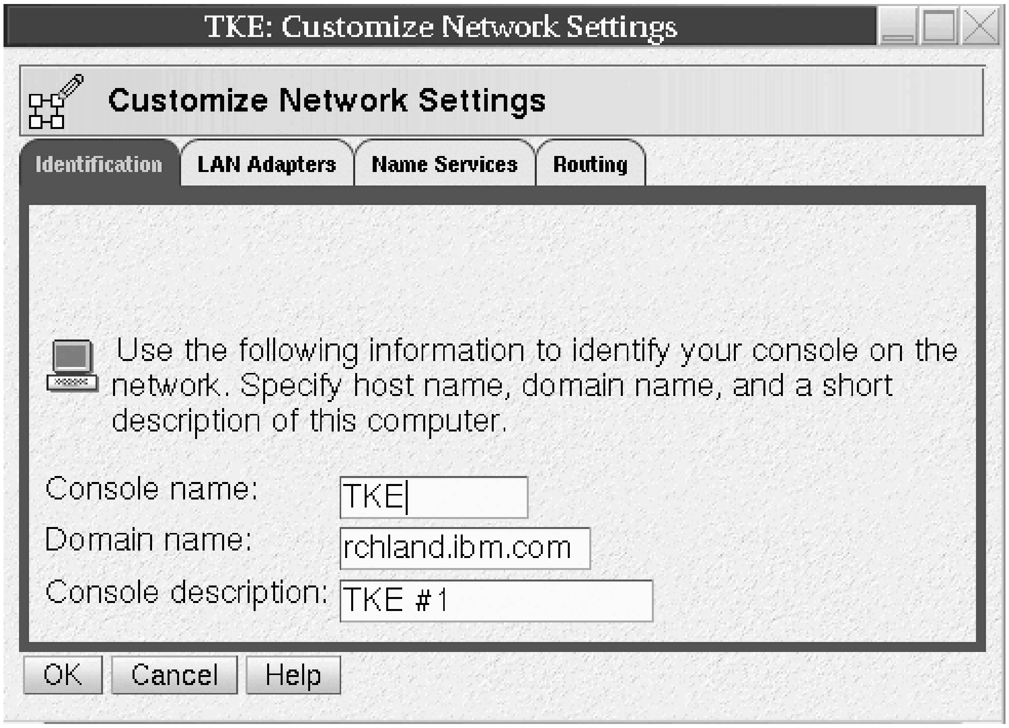
Configuring TCP/IP

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.



Use the following information to identify your console on the network. Specify host name, domain name, and a short description of this computer.

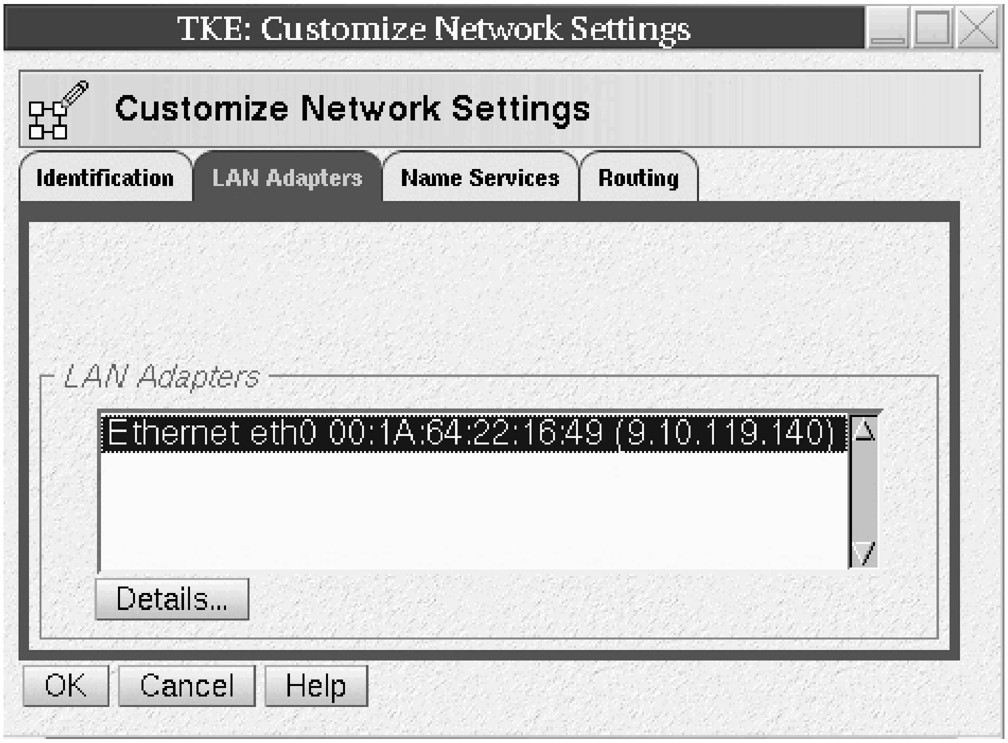
Console name: TKE

Domain name: rchland.ibm.com

Console description: TKE #1

Figure 40. 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.

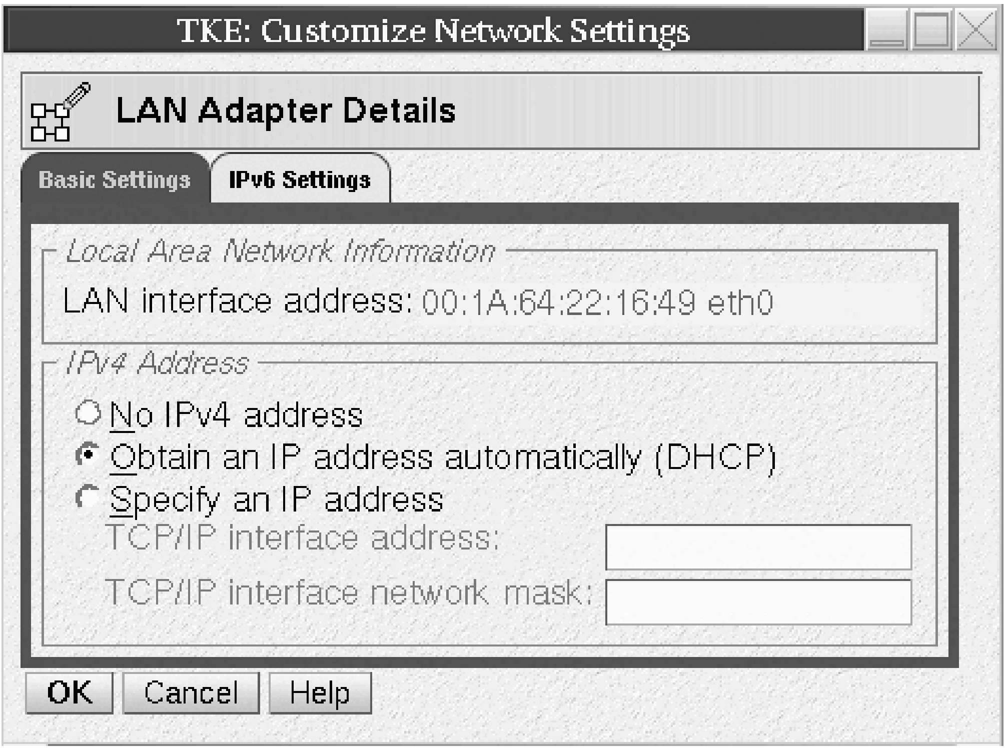


Ethernet eth0 00:1A:64:22:16:49 (9.10.119.140)

Figure 41. Customize Network Settings Lan Adapters Tab

With the Ethernet LAN adapter highlighted, click on Details.

The LAN Adapter Details window opens.



TKE: Customize Network Settings

LAN Adapter Details

Local Area Network Information

LAN interface address: 00:1A:64:22:16:49 eth0

IPv4 Address

○ No IPv4 address

● Obtain an IP address automatically (DHCP)

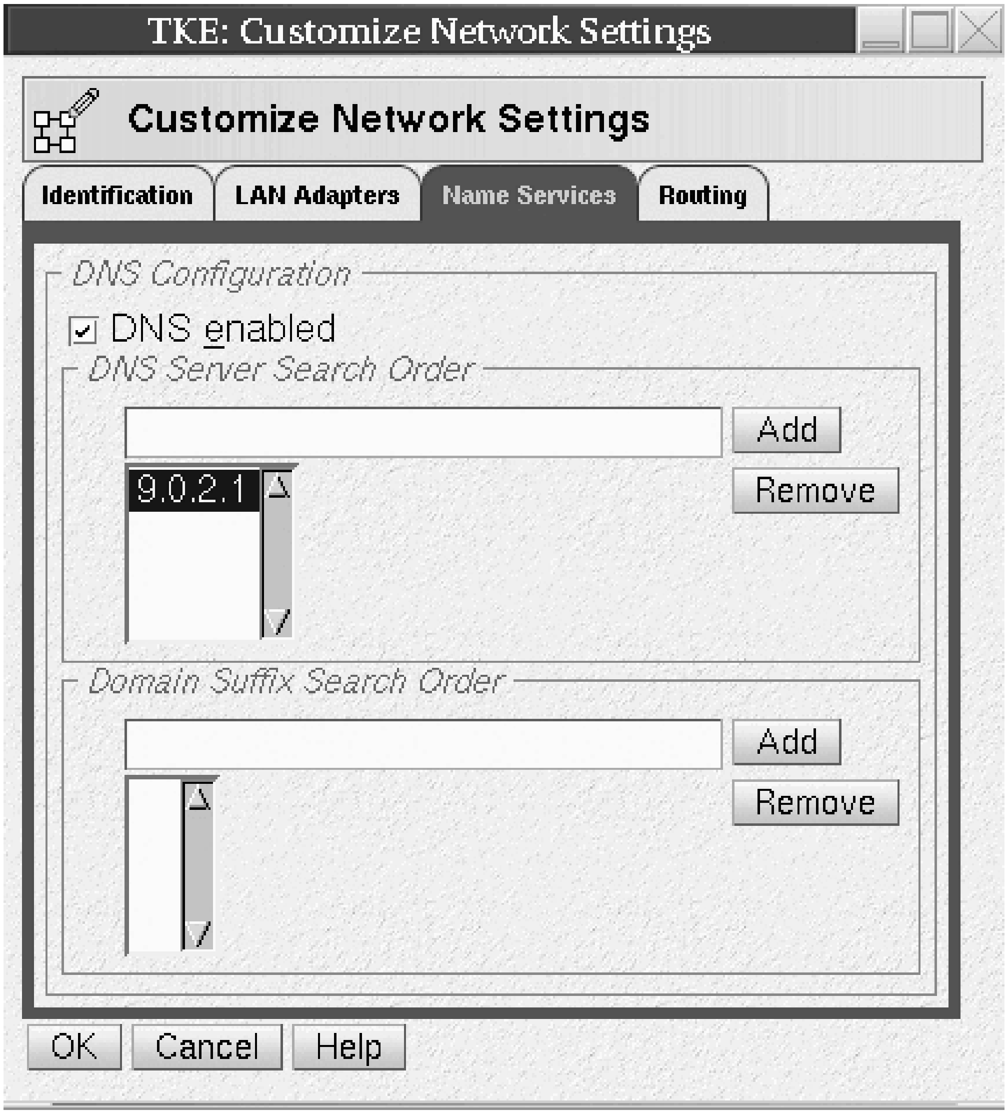
○ Specify an IP address

TCP/IP interface address:

TCP/IP interface network mask:

Figure 42. 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.



☑ DNS enabled

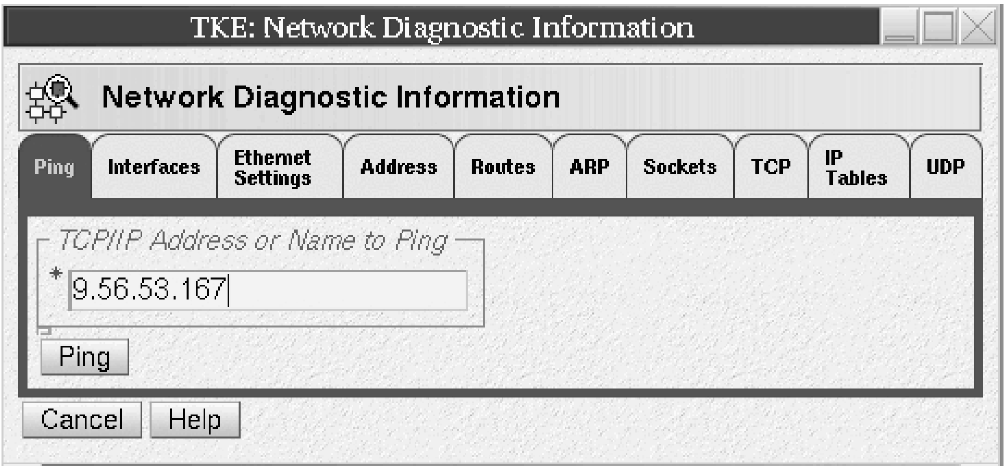
DNS Server Search Order: 9.0.2.1

Figure 43. 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.



TCP/IP Address or Name to Ping

* 9.56.53.167

Figure 44. 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.

- If you are initializing using passphrase, see “Initializing TKE for passphrase” on page 81.
- If you are initializing using smart cards, see “Initializing TKE for smart cards” on page 87.

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,

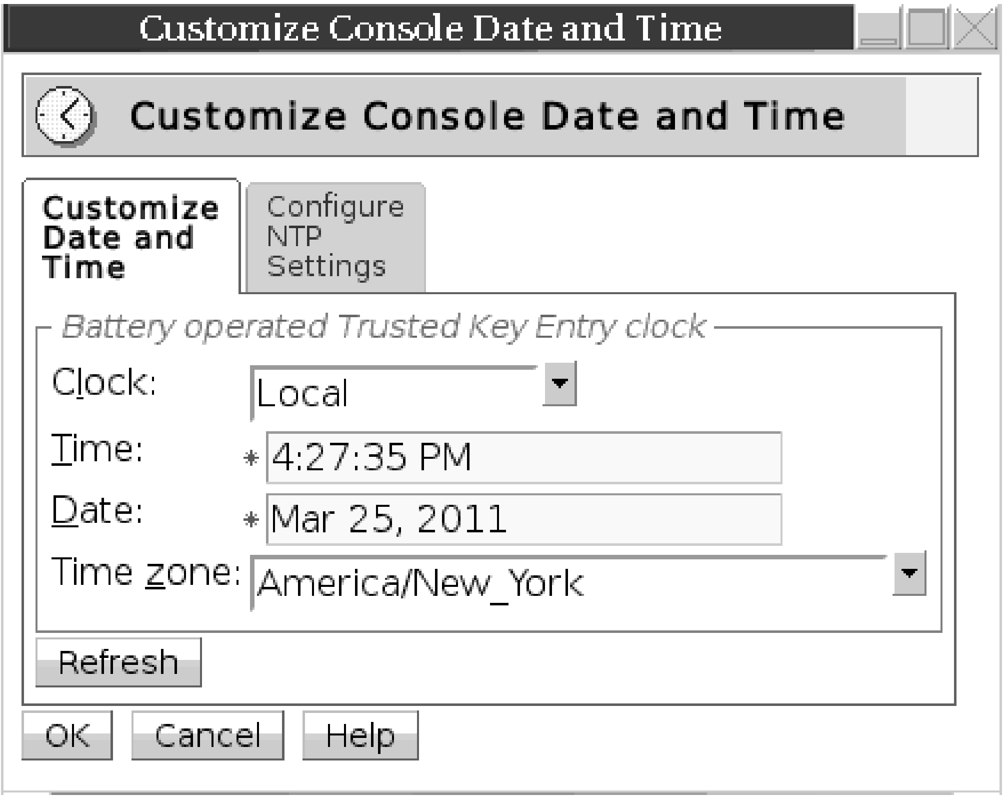
```
09:35:00 AM
```

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 **OK** when finished.



Customize Console Date and Time

Customize Console Date and Time

Battery operated Trusted Key Entry clock

Clock: Local

Time: * 4:27:35 PM

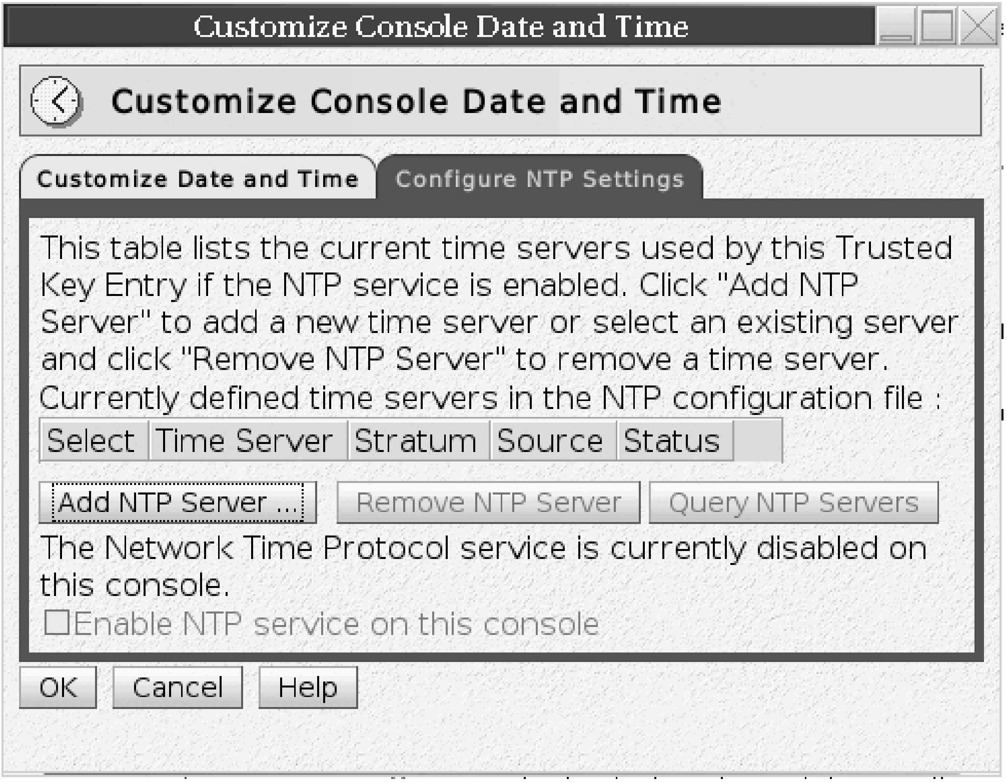
Date: * Mar 25, 2011

Time zone: America/New_York

Figure 45. 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:



This table lists the current time servers used by this Trusted Key Entry if the NTP service is enabled. Click "Add NTP Server" to add a new time server or select an existing server and click "Remove NTP Server" to remove a time server.

Currently defined time servers in the NTP configuration file :

Select	Time Server	Stratum	Source	Status

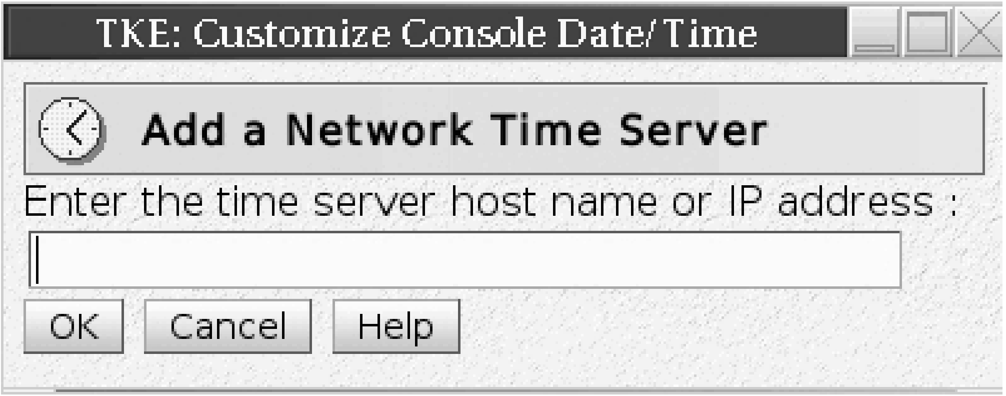
The Network Time Protocol service is currently disabled on this console.

□Enable NTP service on this console

Figure 46. Configure NTP settings

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

The Add a Network Time Server dialog opens.



Enter the time server host name or IP address :

Figure 47. 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.

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 to a random value, 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 to open the task.

When the utility is started, you must logon to the TKE workstation crypto adapter. Logon as the TKEADM user using its default password TKEADM. After you have logged on, the CNM utility provides a graphical user interface for administering access control and managing CCA master keys on the TKE workstation crypto adapter.

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

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 262 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. When using 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 334.
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, or create one or more group logons. The access control points for each of the predefined roles are listed in “Access Control Points for Roles” on page 83. Refer to “Define a User Profile” on page 254 for instructions on defining a user profile. Backup your profiles to DVD-RAM or USB flash memory drive.

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 254. You then need to define a group profile and assign the user profiles to the group profile (see “Define a Group Profile” on page 260).

Note: The group role overrides the role assigned to the individual profiles. When defining profiles, we recommend that the DEFAULT role be mapped to each of the user profiles to limit the functions that the user can perform outside of the group. The group profile should be mapped to role TKEADM or TKEUSER.

The TKEADM user ID can now logoff the TKE workstation crypto adapter. Click on **File** and then choose **Logoff** from the drop down menu.

Loading a New Master Key: When the TKE workstation crypto adapter is initialized, a new random master key value is loaded. If you want to, you can load a new master key value from clear key parts. To do this, follow steps described in “Loading a new master key from clear key parts” on page 265. After loading a new master key, you need to set the master key and reencipher DES and PKA key storage. “Reenciphering key storage” on page 274 describes how to reencipher key storage.

To clear the new master key register and load the first master key part, you must logon the TKE workstation crypto adapter using a profile with the KEYMAN1 role. To combine master key parts, set the master key, and reencipher key storage, you must logon the TKE workstation crypto adapter using a profile with the KEYMAN2 role.

Access Control Points for Roles: When a TKE workstation crypto adapter is initialized for use with passphrase profiles, 5 IBM-supplied roles are created. They are:

- TKEUSER
- TKEADM
- KEYMAN1
- KEYMAN2
- DEFAULT

The following tables show you the ACPs given to each of the IBM-supplied roles.

Profiles using the TKEUSER Role are for TKE authorities.

Table 22. TKEUSER Role

Function	Access Control Point
PKA96 Digital Signature Generate	X'0100'
PKA96 Key Generate	X'0103'
Read Public Access-Control Information	X'0116'
Symmetric Algorithm Decipher - secure AES keys	X'012B'
Delete Retained Key	X'0203'
Permit Regeneration Data For Retained Keys	X'027E'
Encipher	X'000E'
Decipher	X'000F'

Table 22. TKEUSER Role (continued)

Function	Access Control Point
Reencipher to Master Key	X'0012'
Reencipher from Master Key	X'0013'
Load First Key Part	X'001B'
Combine Key Parts	X'001C'
Compute Verification Pattern	X'001D'
Generate Key Set	X'008C'
Generate Key	X'008E'
PKA96 Digital Signature Verify	X'0101'
PKA96 Key Import	X'0104'
PKA Clone Key Generate	X'0204'
PKA Clear Key Generate	X'0205'
Load Diffie-Hellman Key mod/gen	X'0250'
Combine Diffie-Hellman Key part	X'0251'
Clear Diffie-Hellman Key values	X'0252'
Unrestrict Combine Key Parts	X'027A'
Process cleartext ICSF key parts	X'02A0'
Process enciphered ICSF key parts	X'02A1'
RNX access control point	X'02A2'
Session Key Master	X'02A3'
Session Key Slave	X'02A4'
Export Card Device Certificate	X'02A9'
OA Proxy Key Generate	X'0344'
OA Proxy Signature Return	X'0345'
Open Migrate IBM Host Crypto Module Public Configuration Data	X'1003'
Open Configuration Migration Tasks	X'1004'
Open Smart Card Utility Program	X'1005'
Open Trusted Key Entry	X'1006'
Create Domain Group	X'1007'
Change Domain Group	X'1008'
Delete Domain Group	X'1009'
Create Crypto Module Group	X'100A'
Change Crypto Module Group	X'100B'
Delete Crypto Module Group	X'100C'
Open Edit TKE Files	X'100D'
Open TKE File Management Utility	X'100E'

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 23. TKEADM Role

Function	Access Control Point
PKA96 Digital Signature Generate	X'0100'
PKA96 Key Generate	X'0103'
Read Public Access-Control Information	X'0116'
Symmetric Algorithm Decipher - secure AES keys	X'012B'
Delete Retained Key	X'0203'
Permit Regeneration Data For Retained Keys	X'027E'
Compute Verification Pattern	X'001D'
One-Way Hash, SHA-1	X'0107'
Reset Intrusion Latch	X'010F'
Set Clock	X'0110'
Reinitialize Device	X'0111'
Initialize Access-Control System	X'0112'
Change User Profile Expiration Date	X'0113'
Change User Profile Authentication Data	X'0114'
Reset User Profile Logon-Attempt-Failure Count	X'0115'
Delete User Profile	X'0117'
Delete Role	X'0118'
Load Function-Control Vector	X'0119'
Clear Function-Control Vector	X'011A'
Import Card Device Certificate	X'02A5'
Import CA Public Certificate	X'02A6'
Delete Device Retained Key	X'02A8'
Export Card Device Certificate	X'02A9'
Export CA Public Certificate	X'02AA'
Reset Battery Low Indicator	X'030B'
Open Begin Zone Remote Enroll Process	X'1000'
Open Complete Zone Remote Enroll Process	X'1001'
Open Cryptographic Node Management Utility	X'1002'
Open Smart Card Utility Program	X'1005'
Open Edit TKE Files	X'100D'
Open TKE File Management Utility	X'100E'

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 24. KEYMAN1 Role

Function	Access Control Point
PKA96 Digital Signature Generate	X'0100'
PKA96 Key Generate	X'0103'

Table 24. KEYMAN1 Role (continued)

Function	Access Control Point
Read Public Access-Control Information	X'0116'
Symmetric Algorithm Decipher - secure AES keys	X'012B'
Delete Retained Key	X'0203'
Permit Regeneration Data For Retained Keys	X'027E'
Load First Master Key Part	X'0018'
Compute Verification Pattern	X'001D'
Clear New Master Key Register	X'0032'
Generate Key	X'008E'
Open Cryptographic Node Management Utility	X'1002'

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 25. KEYMAN2 Role

Function	Access Control Point
PKA96 Digital Signature Generate	X'0100'
PKA96 Key Generate	X'0103'
Read Public Access-Control Information	X'0116'
Symmetric Algorithm Decipher - secure AES keys	X'012B'
Delete Retained Key	X'0203'
Permit Regeneration Data For Retained Keys	X'027E'
Combine Master Key Parts	X'0019'
Set Master Key	X'001A'
Compute Verification Pattern	X'001D'
Generate Key	X'008E'
Reencipher to Current Master Key	X'0090'
PKA96 Key Token Change	X'0102'
Open Cryptographic Node Management Utility	X'1002'

The DEFAULT role allows any user to view public role and profile information. It also allows re-initialization of the TKE crypto adapter.

Table 26. DEFAULT Role

Function	Access Control Point
PKA96 Digital Signature Generate	X'0100'
PKA96 Key Generate	X'0103'
Read Public Access-Control Information	X'0116'

Table 26. DEFAULT Role (continued)

Function	Access Control Point
Symmetric Algorithm Decipher - secure AES keys	X'012B'
Delete Retained Key	X'0203'
Permit Regeneration Data For Retained Keys	X'027E'
Compute Verification Pattern	X'001D'
Reinitialize Device	X'0111'
Export Card Device Certificate	X'02A9'

Initializing TKE for smart cards

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 to a random value, and DES and PKA key storages are initialized.

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

   Note: Beginning in TKE 7.1, when you initialize a TKE workstation crypto adapter for use with smart card profiles, the "Enable Smart Card Readers" attribute is automatically turned on.

2. 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 290)

   b. Backup CA smart card.

      (see “Backup a CA smart card” on page 293)

   c. Enroll local TKE cryptographic adapter. Enroll remote TKE cryptographic adapter if applicable.

      (see “Enroll a TKE cryptographic adapter” on page 297)

   d. Initialize and enroll TKE smart cards.

      (see “Initialize and enroll a TKE smart card” on page 295)

   e. Personalize TKE smart cards.

    (see “Personalize a TKE smart card” on page 296)

  Close the SCUP application.

3. 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.)
   1. 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 276.)
   2. Define user profiles for the TKE smart cards which have a Crypto Adapter logon key.

      (see “Define a User Profile” on page 254.)
   3. Define a group profile (optional). Empty group profiles SCTKEADM and SCTKEUSR are provided. A group may contain 1 to 10 members.

      (see “Define a Group Profile” on page 260.)
   4. When the TKE workstation crypto adapter is initialized, a new random master key value is loaded. If you want to, you can load a new master key value from clear key parts, or create random master key parts, store them on smart cards, and load a new master key value from the key parts on smart cards. To do this, follow the steps described in “Master Key Menu” on page 263. After loading a new master key, you need to set the master key and reencipher DES and PKA key storage. “Reenciphering key storage” on page 274 describes how to reencipher key storage.
   5. Reset the DEFAULT role. When a TKE workstation crypto adapter is initialized for use with smart card profiles, an extremely powerful DEFAULT role is created. After you have created your smart card profiles, you should reload the DEFAULT role using the IBM-supplied role definition file default_71.rol file. To reload the DEFAULT role, follow instructions in “Open or edit a disk-stored role” on page 250 using the default_71.rol file.

Access Control Points for Roles: When a TKE workstation crypto adapter is initialized for use with smart card profiles, 3 IBM-supplied roles are created. They are:
- SCTKEUSR
- SCTKEADM
- DEFAULT

The following tables show you the ACPs given to each of the IBM-supplied roles.

Profiles using the SCTKEUSR Role are for TKE authorities.

Table 27. SCTKEUSR Role

Function	Access Control Point
PKA96 Digital Signature Generate	X'0100'
PKA96 Key Generate	X'0103'
Read Public Access-Control Information	X'0116'
Symmetric Algorithm Decipher - secure AES keys	X'012B'
Delete Retained Key	X'0203'
Permit Regeneration Data For Retained Keys	X'027E'
Encipher	X'000E'

Table 27. SCTKEUSR Role (continued)

Function	Access Control Point
Decipher	X'000F'
Reencipher to Master Key	X'0012'
Reencipher from Master Key	X'0013'
Load First Key Part	X'001B'
Combine Key Parts	X'001C'
Compute Verification Pattern	X'001D'
Generate Key Set	X'008C'
Generate Key	X'008E'
PKA96 Digital Signature Verify	X'0101'
PKA96 Key Import	X'0104'
PKA Clone Key Generate	X'0204'
PKA Clear Key Generate	X'0205'
Load Diffie-Hellman Key mod/gen	X'0250'
Combine Diffie-Hellman Key part	X'0251'
Clear Diffie-Hellman Key values	X'0252'
Unrestrict Combine Key Parts	X'027A'
Process cleartext ICSF key parts	X'02A0'
Process enciphered ICSF key parts	X'02A1'
RNX access control point	X'02A2'
Session Key Master	X'02A3'
Session Key Slave	X'02A4'
Export Card Device Certificate	X'02A9'
OA Proxy Key Generate	X'0344'
OA Proxy Signature Return	X'0345'
Open Migrate IBM Host Crypto Module Public Configuration Data	X'1003'
Open Configuration Migration Tasks	X'1004'
Open Smart Card Utility Program	X'1005'
Open Trusted Key Entry	X'1006'
Create Domain Group	X'1007'
Change Domain Group	X'1008'
Delete Domain Group	X'1009'
Create Crypto Module Group	X'100A'
Change Crypto Module Group	X'100B'
Delete Crypto Module Group	X'100C'
Open Edit TKE Files	X'100D'
Open TKE File Management Utility	X'100E'

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 28. SCTKEADM Role

Function	Access Control Point
PKA96 Digital Signature Generate	X'0100'
PKA96 Key Generate	X'0103'
Read Public Access-Control Information	X'0116'
Symmetric Algorithm Decipher - secure AES keys	X'012B'
Delete Retained Key	X'0203'
Permit Regeneration Data For Retained Keys	X'027E'
Load First Master Key Part	X'0018'
Combine Master Key Parts	X'0019'
Set Master Key	X'001A'
Compute Verification Pattern	X'001D'
Clear New Master Key Register	X'0032'
Generate Key	X'008E'
Reencipher to Current Master Key	X'0090'
PKA96 Key Token Change	X'0102'
One-Way Hash, SHA-1	X'0107'
Reset Intrusion Latch	X'010F'
Set Clock	X'0110'
Reinitialize Device	X'0111'
Initialize Access-Control System	X'0112'
Change User Profile Expiration Date	X'0113'
Change User Profile Authentication Data	X'0114'
Reset User Profile Logon-Attempt-Failure Count	X'0115'
Delete User Profile	X'0117'
Delete Role	X'0118'
Load Function-Control Vector	X'0119'
Clear Function-Control Vector	X'011A'
Unrestrict Combine Key Parts	X'027A'
RNX access control point	X'02A2'
Session Key Master	X'02A3'
Session Key Slave	X'02A4'
Import Card Device Certificate	X'02A5'
Import CA Public Certificate	X'02A6'
Master Key Extended	X'02A7'
Delete Device Retained Key	X'02A8'
Export Card Device Certificate	X'02A9'
Export CA Public Certificate	X'02AA'
Reset Battery Low Indicator	X'030B'
Open Begin Zone Remote Enroll Process	X'1000'

Table 28. SCTKEADM Role (continued)

Function	Access Control Point
Open Complete Zone Remote Enroll Process	X'1001'
Open Cryptographic Node Management Utility	X'1002'
Open Smart Card Utility Program	X'1005'
Open Edit TKE Files	X'100D'
Open TKE File Management Utility	X'100E'

The DEFAULT role created when a TKE workstation crypto adapter is initialized for use with smart card profiles is designed to provide enough authority to perform the initial administration of the TKE's crypto adapter.

Warning: This is an extremely powerful role. Once the initial administration is done, you should replace the DEFAULT role with the less powerful DEFAULT role that is created when a TKE workstation crypto adapter is initialized for use with passphrase profiles. To reload the DEFAULT role, follow instructions in “Open or edit a disk-stored role” on page 250 using the default_71.rol file.

Table 29. DEFAULT Role

Function	Access Control Point
PKA96 Digital Signature Generate	X'0100'
PKA96 Key Generate	X'0103'
Read Public Access-Control Information	X'0116'
Symmetric Algorithm Decipher - secure AES keys	X'012B'
Delete Retained Key	X''0203'
Permit Regeneration Data For Retained Keys	X'027E'
Encipher	X'000E'
Decipher	X'000F'
Generate MAC	X'0010'
Verify MAC	X'0011'
Reencipher to Master Key	X'0012'
Reencipher from Master Key	X'0013'
Load First Master Key Part	X'0018'
Combine Master Key Parts	X'0019'
Set Master Key	X'001A'
Load First Key Part	X'001B'
Combine Key Parts	X'001C'
Compute Verification Pattern	X'001D'
Translate Key	X'001F'
Generate Random Master Key	X'0020'
Clear New Master Key Register	X'0032'
Clear Old Master Key Register	X'0033'

Table 29. DEFAULT Role (continued)

Function	Access Control Point
Generate Diversified Key (CLR8-ENC)	X'0040'
Generate Diversified Key (TDES-ENC)	X'0041'
Generate Diversified Key (TDES-DEC)	X'0042'
Generate Diversified Key (SESS-XOR)	X'0043'
Enable DKG Single Length Keys and Equal Halves for TDES-ENC, TDES-DEC	X'0044'
Load First Asymmetric Master Key Part	X'0053'
Combine PKA Master Key Parts	X'0054'
Set Asymmetric Master Key	X'0057'
Clear New Asymmetric Master Key Buffer	X'0060'
Clear Old Asymmetric Master Key Buffer	X'0061'
Generate MDC	X'008A'
Generate Key Set	X'008C'
Generate Key	X'008E'
Reencipher to Current Master Key	X'0090'
Generate Clear 3624 PIN	X'00A0'
Generate Clear 3624 PIN Offset	X'00A4'
Verify Encrypted 3624 PIN	X'00AB'
Verify Encrypted German Bank Pool PIN	X'00AC'
Verify Encrypted VISA PVV	X'00AD'
Verify Encrypted InterBank PIN	X'00AE'
Format and Encrypt PIN	X'00AF'
Generate Formatted and Encrypted 3624 PIN	X'00B0'
Generate Formatted and Encrypted German Bank Pool PIN	X'00B1'
Generate Formatted and Encrypted InterBank PIN	X'00B2'
Translate PIN with No Format-Control to No Format-Control	X'00B3'
Reformat PIN with No Format-Control to No Format-Control	X''00B7'
Generate Clear VISA PVV Alternate	X'00BB'
Encipher Under Master Key	X'00C3'
Lower Export Authority	X'00CD'
Translate Control Vector	X'00D6'
Generate Key Set Extended	X'00D7'
Encipher/Decipher Cryptovariable	X'00DA'
Replicate Key	X'00DB'
Generate CVV	X'00DF'
Verify CVV	X'00E0'
Unique Key Per Transaction, ANSI X9.24	X''00E1'

Table 29. DEFAULT Role (continued)

Function	**Access Control Point**
PKA96 Digital Signature Verify	X'0101'
PKA96 Key Token Change	X'0102'
PKA96 Key Import	X'0104'
Symmetric Key Export PKCS-1.2/OAEP	X'0105'
Symmetric Key Import PKCS-1.2/OAEP	X'0106'
One-Way Hash, SHA-1	X'0107'
Data Key Import	X'0109'
Data Key Export	X'010A'
Compose SET Block	X'010B'
Decompose SET Block	X'010C'
PKA92 Symmetric Key Generate	X'010D''
NL-EPP-5 Symmetric Key Generate	X'010E'
Reset Intrusion Latch	X'010F'
Set Clock	X'0110'
Reinitialize Device	X'0111'
Initialize Access-Control System	X'1112'
Change User Profile Expiration Date	X'0113'
Change User Profile Authentication Data	X'0114'
Reset User Profile Logon-Attempt-Failure Count	X'0115'
Delete User Profile	X'0117'
Delete Role	X'0118'
Load Function-Control Vector	X'0119'
Clear Function-Control Vector	X'011A'
Force User Logoff	X'011B'
Set EID	X'011C'
Initialize Master Key Cloning	X'011D'
RSA Encipher Clear Key	X'011E'
RSA Decipher Clear Key	X'011F'
Generate Random Asymmetric Master Key	X'0120'
SET PIN Encrypt with IPINENC	X'0121'
SET PIN Encrypt with OPINENC	X'0122'
PKA Register Public Key Hash	X'0200'
PKA Public Key Register with Cloning	X'0201'
PKA Public Key Register	X'0202'
PKA Clone Key Generate	X'0204'
PKA Clear Key Generate	X'0205'
Clone-info (share) Obtain 1	X'0211'
Clone-info (share) Obtain 2	X'0212'
Clone-info (share) Obtain 3	X'0213'

Table 29. DEFAULT Role (continued)

Function	Access Control Point
Clone-info (share) Obtain 4	X'0214'
Clone-info (share) Obtain 5	X'0215'
Clone-info (share) Obtain 6	X'0216'
Clone-info (share) Obtain 7	X'0217'
Clone-info (share) Obtain 8	X'0218'
Clone-info (share) Obtain 9	X'0219'
Clone-info (share) Obtain 10	X'021A'
Clone-info (share) Obtain 11	X'021B'
Clone-info (share) Obtain 12	X'021C'
Clone-info (share) Obtain 13	X'021D'
Clone-info (share) Obtain 14	X'021E'
Clone-info (share) Obtain 15	X'021F'
Clone-info (share) Install 1	X'0221'
Clone-info (share) Install 2	X'0222'
Clone-info (share) Install 3	X'0223'
Clone-info (share) Install 4	X'0224'
Clone-info (share) Install 5	X'0225'
Clone-info (share) Install 6	X'0226'
Clone-info (share) Install 7	X'0227'
Clone-info (share) Install 8	X'0228'
Clone-info (share) Install 9	X'0229'
Clone-info (share) Install 10	X'022A'
Clone-info (share) Install 11	X'022B'
Clone-info (share) Install 12	X'022C'
Clone-info (share) Install 13	X'022D'
Clone-info (share) Install 14	X'022E'
Clone-info (share) Install 15	X'022F'
List Retained Key	X'0230'
Generate Clear NL-PIN-1 Offset	X'0231'
Verify Encrypted NL-PIN-1	X'0232'
PKA92 Symmetric Key Import	X'0235'
PKA92 Symmetric Key Import with PIN keys	X'0236'
ZERO-PAD Symmetric Key Generate	X'023C'
ZERO-PAD Symmetric Key Import	X'023D'
ZERO-PAD Symmetric Key Export	X'023E'
Symmetric Key Generate PKCS-1.2/OAEP	X'023F'
Load Diffie-Hellman Key mod/gen	X'0250'
Combine Diffie-Hellman Key part	X'0251'
Clear Diffie-Hellman Key values	X'0252'
Unrestrict Reencipher from Master Key	X'0276'

Table 29. DEFAULT Role (continued)

Function	Access Control Point
Unrestrict Data Key Export	X'0277'
Add Key Part	X'0278'
Complete Key Part	X'0279'
Unrestrict Combine Key Parts	X'027A'
Unrestrict Reencipher to Master Key	X'027B'
Unrestrict Data Key Import	X'027C'
Generate Diversified Key (DALL with DKYGENKY Key Type)	X'0290'
Generate CSC-5, 4 and 3 Values	X'0291'
Verify CSC-3 Values	X'0292'
Verify CSC-4 Values	X'0293'
Verify CSC-5 Values	X'0294'
Process cleartext ICSF key parts	X'02A0'
Process enciphered ICSF key parts	X'02A1'
RNX access control point	X'02A2'
Session Key Master	X'02A3'
Session Key Slave	X'02A4'
Import Card Device Certificate	X'02A5'
Import CA Public Certificate	X'02A6'
Master Key Extended	X'02A7'
Delete Device Retained Key	X'02A8'
Export Card Device Certificate	X'02A9'
Export CA Public Certificate	X'02AA'
Reset Battery Low Indicator	X'030B'

Customize the TKE Application

1. Open the TKE Application by clicking on Trusted Key Entry and then clicking on Trusted Key Entry 7.1.
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 101 for details.
3. Click on Preferences on the task bar.
4. Enable/Disable the Preferences as appropriate. See “TKE Customization” on page 138 for details.

Adding new ACPs to existing roles using the Migrate Roles Utility

Sometimes between TKE releases, new Access Control Points (ACPs) are made available to the roles on the TKE workstation crypto adapter. New ACPs are never automatically added to existing roles during the migration process. For this reason, it may be necessary to add ACPs to existing roles after migrating to a new TKE release. Beginning in TKE 7.1, TKE includes the Migrate Roles Utility to simplify the process of adding new ACPs to existing roles on the TKE workstation crypto adapter.

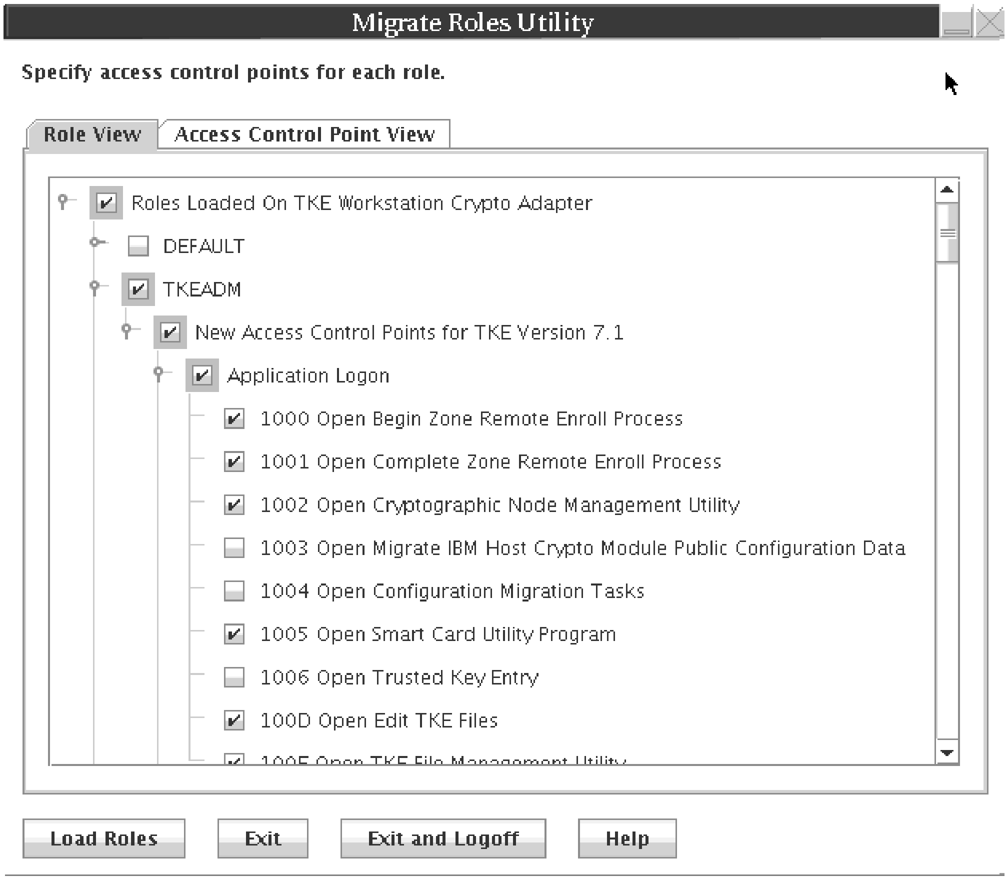
Note: In TKE 7.1, fifteen individual ACPs were added to control access to TKE applications and some functions within TKE applications. If you have migrated roles from an earlier version of TKE to TKE 7.1 or later, review the information in "TKE 7.1 Role Migration Considerations" on page 97.

The Migrate Role Utility is a graphical user interface that allows you to quickly add new ACPs to existing roles. Starting with TKE 7.1, the utility lists the new ACPs that were added in each release. Using a tree structure interface, you can quickly select the ACPs you want to add to your roles. When you have made your selection, you simply send the command to make the updates.

To start the Migrate Roles Utility, you must be signed onto the TKE with the Privileged Mode Access ID of ADMIN.

1. In the left frame of the Trusted Key Entry Console, click on **Trusted Key Entry**.
2. In the right frame of the Trusted Key Entry Console, under the Applications list, click on **Migrate Roles Utility**.

   The Migrate Roles Utility is started.



Specify access control points for each role.

- ☑ Roles Loaded On TKE Workstation Crypto Adapter
  - □ DEFAULT
  - ☑ TKEADM
    - ☑ New Access Control Points for TKE Version 7.1
      - ☑ Application Logon
        - ☑ 1000 Open Begin Zone Remote Enroll Process
        - ☑ 1001 Open Complete Zone Remote Enroll Process
        - ☑ 1002 Open Cryptographic Node Management Utility
        - □ 1003 Open Migrate IBM Host Crypto Module Public Configuration Data
        - □ 1004 Open Configuration Migration Tasks
        - ☑ 1005 Open Smart Card Utility Program
        - □ 1006 Open Trusted Key Entry
        - ☑ 100D Open Edit TKE Files
        - ☑ 100E Open TKE File Management Utility

Figure 48. Migrate Roles Utility

The Migrate Roles Utility window has two tabs that provide two different views of the ACPs that can be added. In the:

- **Role View**, each individual Role has every new ACP listed under it. Check boxes under each role are provided to activate or deactivate individual ACPs for that role.

- **Access Control Point View**, each individual ACP has every role listed under it. Check boxes under each ACP are provided to activate or deactivate the ACP for individual roles.

To add new ACPs to existing roles:

1. Click on the **Role View** or **Access Control Point View** tab depending on your desired view of the new ACPs.
2. Use the check boxes provided to select which ACPs you want to add to which roles.
3. Press the **Load Rules** command button to add the selected ACPs to the selected roles.

   When load operation completes, a message box displays a "Role loaded successfully" message. Press the **Close** button on this message box. The process is complete.

TKE 7.1 Role Migration Considerations

Beginning in TKE 7.1, fifteen individual ACPs were added to control access to TKE applications and some functions within TKE applications. The new TKE 7.1 ACPs were logically put into three groups. The following list shows the ACP groups and their ACP values. The items are listed in the order they appear in the Role View of the Migrate Roles Utility.

Application Logon ACPs

- 1000: Open Begin Zone Remote Enroll Process
- 1001: Open Complete Zone Remote Enroll Process
- 1002: Open Cryptographic Node Management Utility
- 1003: Open Migrate IBM Host Crypto Module Public Configuration Data
- 1004: Open Configuration Migration Tasks
- 1005: Open Smart Card Utility Program
- 1006: Open Trusted Key Entry
- 100D: Open Edit TKE Files
- 100E: Open TKE File Management Utility

Crypto Module Group ACPs

- 100A: Create Crypto Module Group
- 100B: Change Crypto Module Group
- 100C: Delete Crypto Module Group

Domain Group ACPs

- 1007: Create Domain Group
- 1008: Change Domain Group
- 1009: Delete Domain Group

New ACPs are never automatically added to existing roles on a TKE workstation crypto adapter. You must take explicit actions to add the new ACPs to existing roles when:

- The role was created on a TKE workstation before the workstation was upgraded to TKE 7.1 or later.
- The role was created on TKE 7.1 or later from a role definition file that was created on a pre-TKE 7.1 system.

TKE 7.1 Role Migration Considerations for IBM-Supplied Roles

If your IBM-supplied roles were created before your system was upgraded to TKE 7.1 or later, you will need to add ACPs to your IBM-supplied roles. To do this, you must determine which IBM supplied roles you have on your TKE workstation. If you initialized your TKE workstation for use with smart card profiles, you will need to update the following roles:

- SCTKEUSR
- SCTKEADM

If you initialized your TKE workstation for use with passphrase profiles, you will need to update the following roles:

- TKEUSER
- TKEADM
- KEYMAN1
- KEYMAN2

Once you have determined which roles you need to update, go into the Crypto Node Management Utility and reload the IBM-supplied roles from the IBM-supplied role definition files for this release. For instructions on loading IBM-supplied roles from IBM-supplied role definition files, refer to “Open or edit a disk-stored role” on page 250.

TKE 7.1 Role Migration Considerations for Customer Defined Roles

If your customer defined roles were created before your system was upgraded to TKE 7.1 or later, or your roles were created from role definition files that were created on a TKE that was pre-TKE 7.1, you will need to add ACPs to your customer defined roles. To do this, you must determine which ACPs you want to add to your customer defined roles. Once you have made your choices, use the Migrate Roles Utility (described in “Adding new ACPs to existing roles using the Migrate Roles Utility” on page 95) to manually add the ACPs to each of the customer defined roles.

The TKE has two pairs of general purpose roles; TKEUSER/SCTKEUSR and TKEADM/SCTKEADM. The TKEUSER and SCTKEUSER roles are designed for users responsible for managing host cryptographic adapters. The TKEADM or SCTKEADM roles are designed for users responsible for managing the TKE workstation. Customer defined roles should be modeled off of one of these two pairs of roles. The following lists show which new ACPs were added to these general purpose roles. You can use this information to help you decide which ACPs you need to add to your customer defined roles.

In the TKEUSER and SCTKEUSR roles, the following ACPs were added:

- Application Logon ACPs
  - 1003: Open Migrate IBM Host Crypto Module Public Configuration Data
  - 1004: Open Configuration Migration Tasks
  - 1005: Open Smart Card Utility Program
  - 1006: Open Trusted Key Entry
  - 100D: Open Edit TKE Files
  - 100E: Open TKE File Management Utility
- Crypto Module Group ACPs
  - 100A: Create Crypto Module Group

  - 100B: Change Crypto Module Group
  - 100C: Delete Crypto Module Group
- Domain Group ACPs
  - 1007: Create Domain Group
  - 1008: Change Domain Group
  - 1009: Delete Domain Group

In the TKEADM and SCTKEADM role:s, the following ACPs were added:

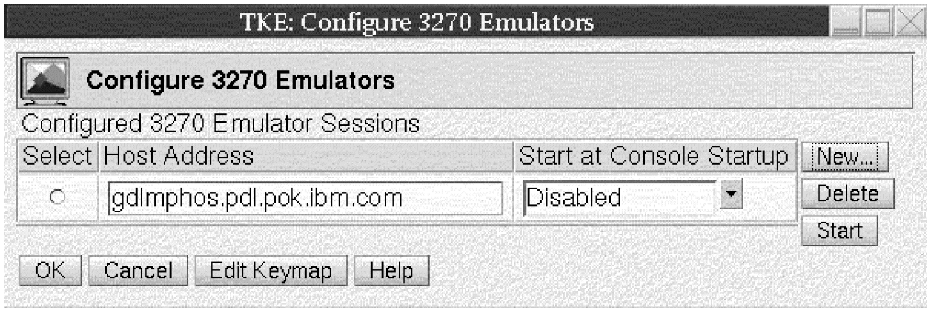
- Application Logon ACPs
  - 1000: Open Begin Zone Remote Enroll Process
  - 1001: Complete Zone Remote Enroll Process
  - 1002: Open Cryptographic Node Management Utility
  - 1005: Open Smart Card Utility Program
  - 100D: Open Edit TKE Files
  - 100E: Open TKE File Management Utility

Configure 3270 Emulators

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



TKE: Configure 3270 Emulators

Configure 3270 Emulators

Configured 3270 Emulator Sessions

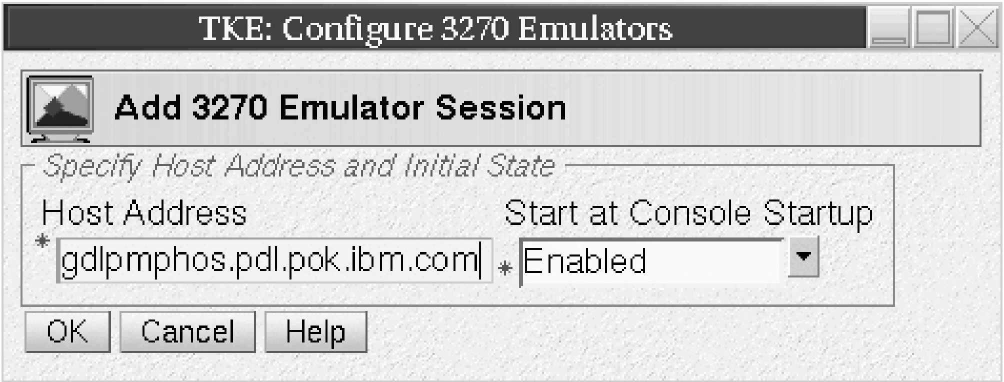
Select	Host Address	Start at Console Startup
○	gdlmphos.pdl.pok.ibm.com	Disabled

Figure 49. 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.



TKE: Configure 3270 Emulators

Add 3270 Emulator Session

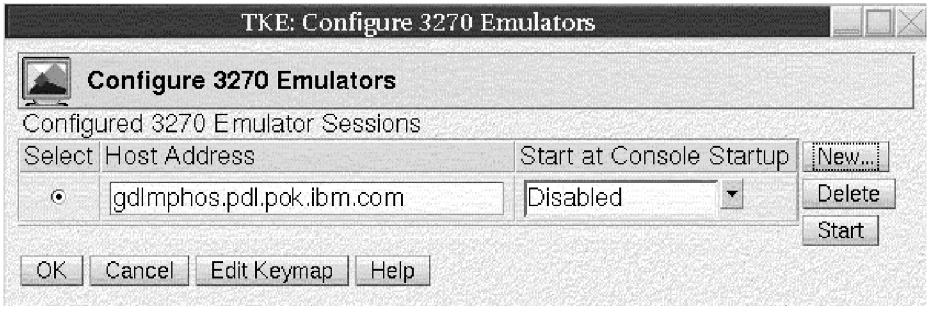
Specify Host Address and Initial State

Host Address: * gdlpmphos.pdl.pok.ibm.com

Start at Console Startup: * Enabled

Figure 50. 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.



TKE: Configure 3270 Emulators

Configure 3270 Emulators

Configured 3270 Emulator Sessions

Select	Host Address	Start at Console Startup
⊙	gdlmphos.pdl.pok.ibm.com	Disabled

Figure 51. 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, 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 81
- Smart card - see “Initializing TKE for smart cards” on page 87

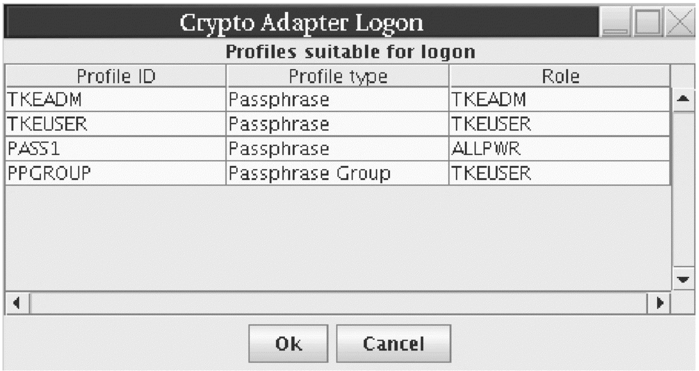
From the Framework tree on the left hand panel of the main TKE console screen, click on **Trusted key Entry**, then click on **Trusted Key Entry 7.1**.

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.



Crypto Adapter Logon

Profiles suitable for logon

Profile ID	Profile type	Role
TKEADM	Passphrase	TKEADM
TKEUSER	Passphrase	TKEUSER
PASS1	Passphrase	ALLPWR
PPGROUP	Passphrase Group	TKEUSER

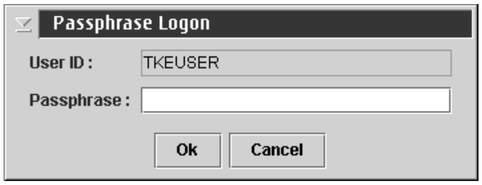
Figure 52. Crypto Adapter logon window with passphrase profiles

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.



User ID : TKEUSER

Passphrase :

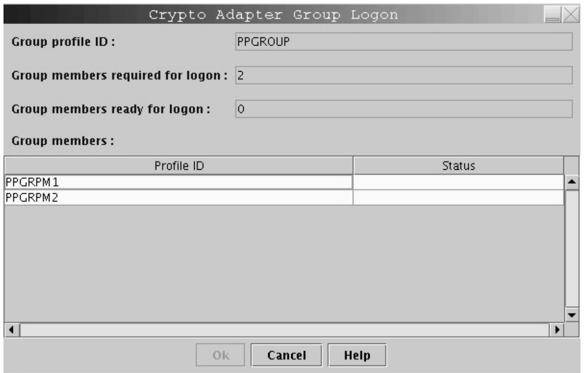
Figure 53. Enter passphrase for logon

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.



Group profile ID : PPGROUP

Group members required for logon : 2

Group members ready for logon : 0

Group members :

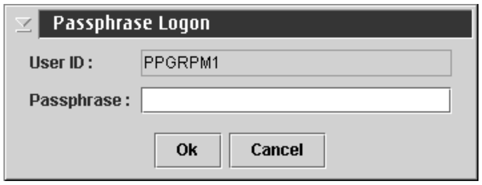
Profile ID	Status
PPGRPM1	
PPGRPM2	

Figure 54. 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.

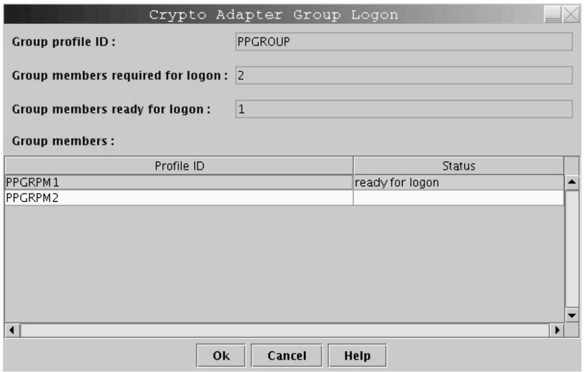


User ID : PPGRPM1

Passphrase :

Figure 55. 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.



Group profile ID : PPGROUP

Group members required for logon : 2

Group members ready for logon : 1

Group members :

Profile ID	Status
PPGRPM1	ready for logon
PPGRPM2	

Figure 56. 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

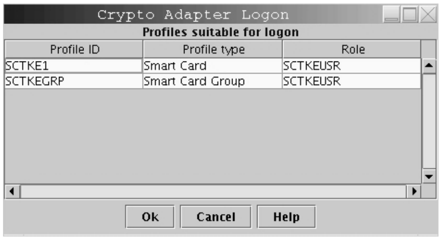
   Note: If the group logon should fail, the *Group members ready for logon* is reset to zero and group logon must start over.

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 241.

Smart card and smart card group logon

Depending on how you have initialized your environment, the Crypto Adapter Logon window will be displayed with profile IDs that represent single and/or group smart card logon.



Profiles suitable for logon

Profile ID	Profile type	Role
SCTKE1	Smart Card	SCTKEUSR
SCTKEGRP	Smart Card Group	SCTKEUSR

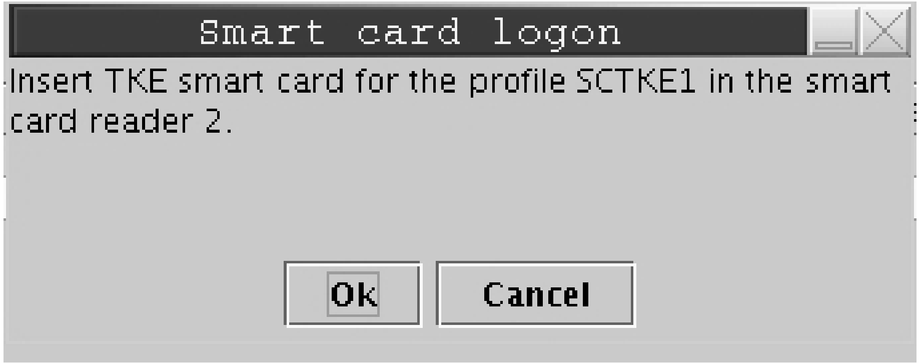
Figure 57. Crypto Adapter Logon Window with smart card profiles

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

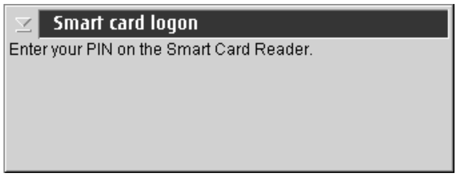
1. The Smart Card Logon window will be displayed.
2. Insert the TKE smart card that contains the TKE workstation crypto adapter logon key for the selected profile ID and select **OK**



Insert TKE smart card for the profile SCTKE1 in the smart card reader 2.

Figure 58. 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.

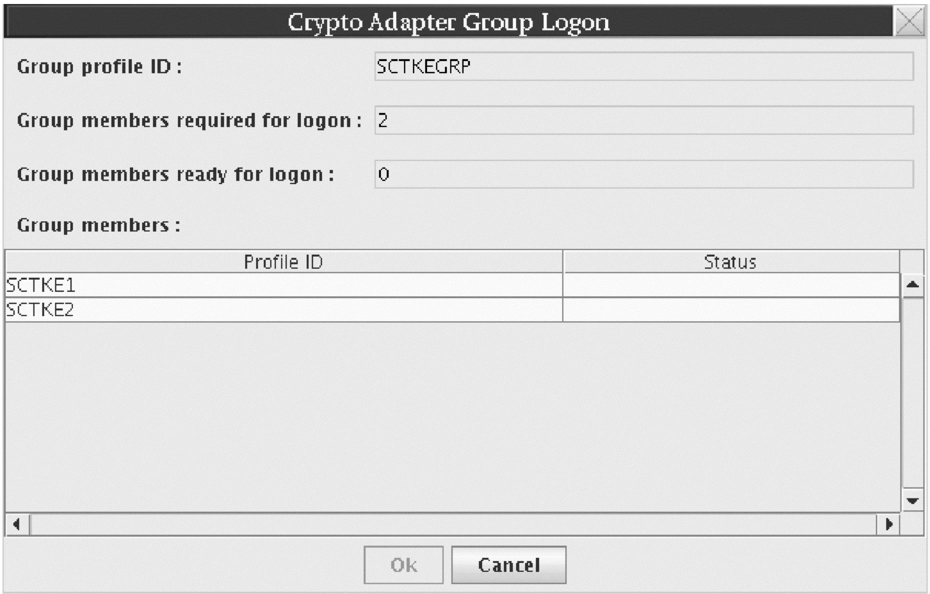


Enter your PIN on the Smart Card Reader.

Figure 59. 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.



Group profile ID : SCTKEGRP

Group members required for logon : 2

Group members ready for logon : 0

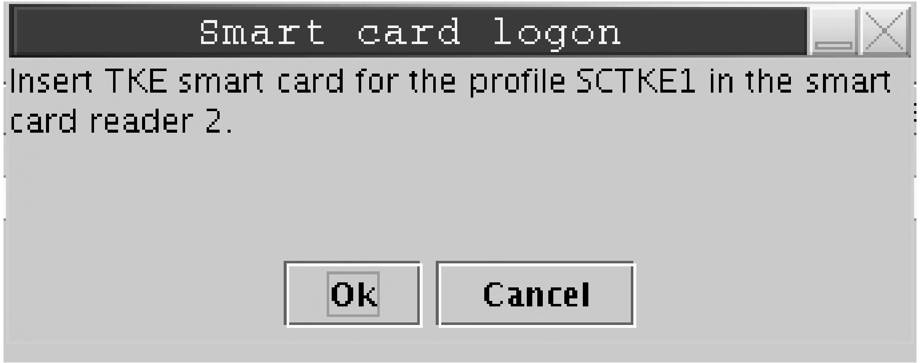
Group members :

Profile ID	Status
SCTKE1	
SCTKE2	

Figure 60. 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**

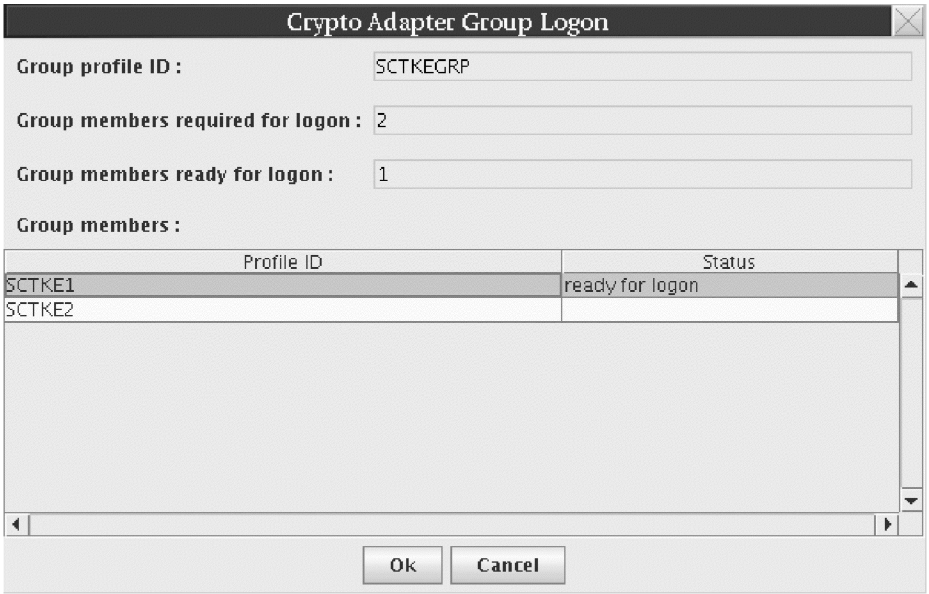
   The Smart card logon window is displayed.
4. Insert the TKE smart card that contains the TKE workstation crypto adapter logon key for the selected profile ID and select **OK**



Insert TKE smart card for the profile SCTKE1 in the smart card reader 2.

Figure 61. 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.



Crypto Adapter Group Logon

Group profile ID : SCTKEGRP

Group members required for logon : 2

Group members ready for logon : 1

Group members :

Profile ID	Status
SCTKE1	ready for logon
SCTKE2	

Figure 62. 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 241.

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

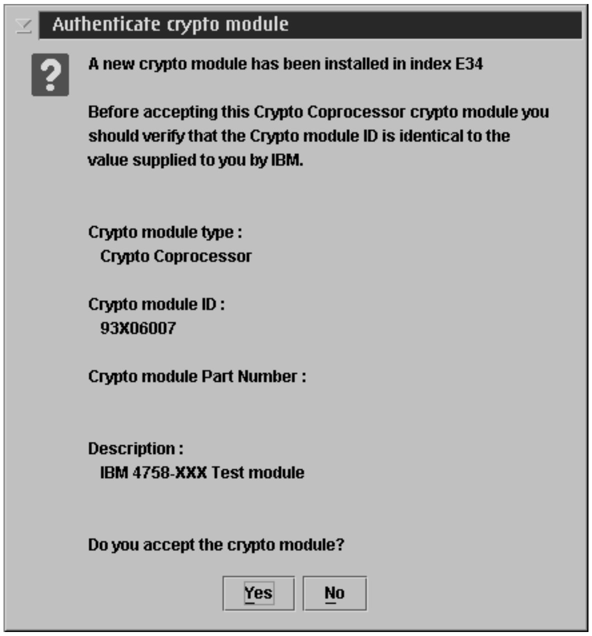
Authenticating the CMID and CMPM

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/E user ID. From the ICSF main panel, choose option 1, Coprocessor Management. This panel will list all the crypto modules available to this host. Verify the coprocessor index and serial number with the information on the 'Authenticate crypto module' window on TKE.

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.



Authenticate crypto module

A new crypto module has been installed in index E34

Before accepting this Crypto Coprocessor crypto module you should verify that the Crypto module ID is identical to the value supplied to you by IBM.

Crypto module type :
Crypto Coprocessor

Crypto module ID :
93X06007

Crypto module Part Number :

Description :
IBM 4758-XXX Test module

Do you accept the crypto module?

Figure 63. 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 109. 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 344 and “TKE File Management Utility” on page 332 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_71.rol
  - tempdefault_71.rol
  - tkeusr_71.rol
  - tkeadm_71.rol
  - keyman1_71.rol
  - keyman2_71.rol
  - tkeuser.pro
  - tkeadm.pro
  - keyman1.pro
  - keyman2.pro
- Smart card
  - default_71.rol
  - tempdefault_71.rol
  - sctkeusr_71.rol
  - sctkeadm_71.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 69).

- 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.

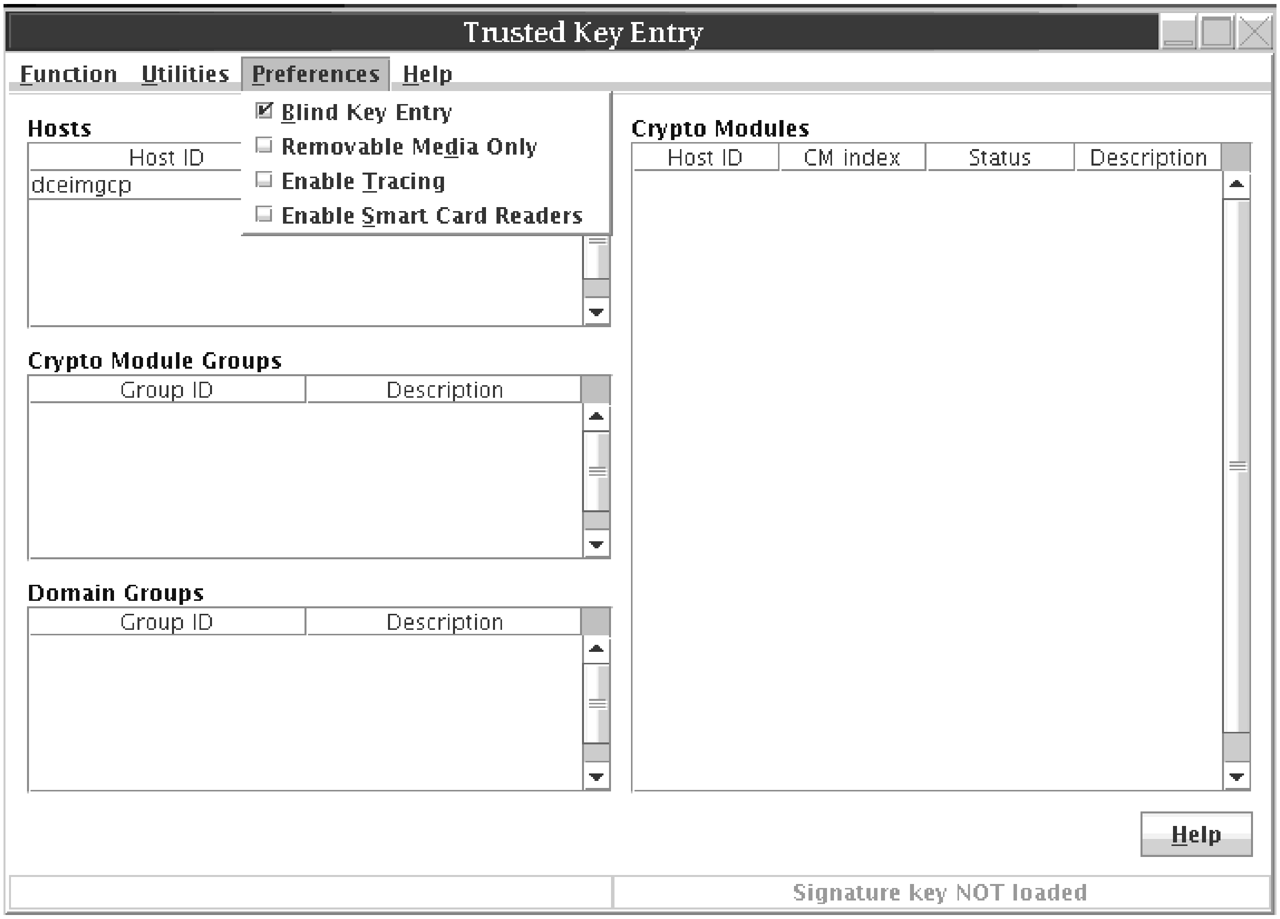
There are other host installation files that contain the TKE programs that execute on the host. Once these files have been installed, no updates to them are required. The weekly system dumps should be sufficient for backup of these files. These files are documented in Chapter 4, “TKE Setup and Customization,” on page 69.

Chapter 6. Main Window

The purpose of the TKE application is to allow administrators to manage host cryptographic modules, either individually or through groups. From the main window, you also create host definitions and group definitions.

Note: Many screen captures show smart card options. If "Enable Smart Card Readers" is not checked, you will not see the smart card options.

Beginning in TKE 7.1, when you initialize a TKE's local crypto adapter for use with smart card profiles, the "Enable Smart Card Readers" option is automatically selected.



☑ Blind Key Entry
☐ Removable Media Only
☐ Enable Tracing
☐ Enable Smart Card Readers

Host ID
dceimgcp

Figure 64. TKE Preferences

You can update the TKE application preferences using the Preferences pull-down menu. To display the menu, click on Preferences in the toolbar. Click on individual items to enable or disable them. A check mark indicates the preference is enabled. For details on each of the preferences, see “TKE Customization” on page 138.

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 129.

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.

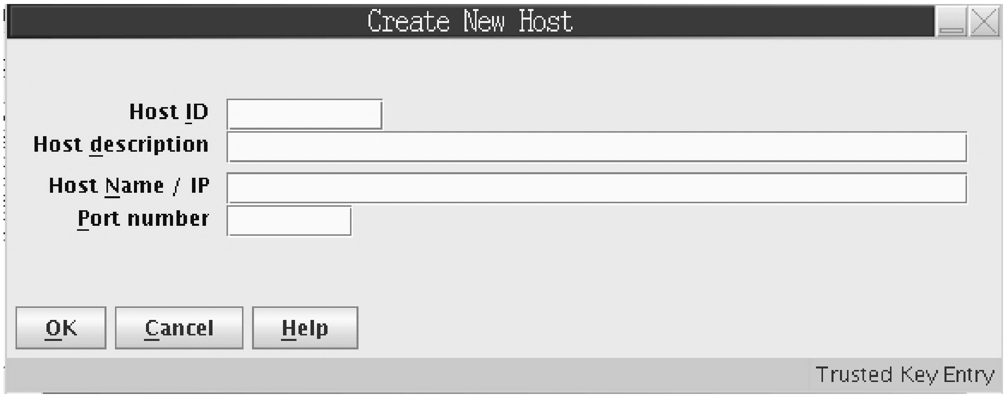


Figure 65. Create Host

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 69.

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

For additional details on LPAR setup, refer to Appendix B, “LPAR Considerations,” on page 313.

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.

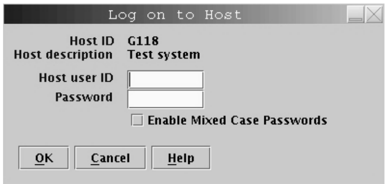
Deleting Host Entries

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.

Host Logon

To log on, 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 log on to all hosts that are to be accessed within that group.

The Logon panel is displayed for the host logon.



Log on to Host

Host ID G118
Host description Test system
Host user ID
Password
□ Enable Mixed Case Passwords

Figure 66. Host Logon Window

Enter your RACF-defined TSO/E host user ID and password. This is the user ID of the TKE administrator.

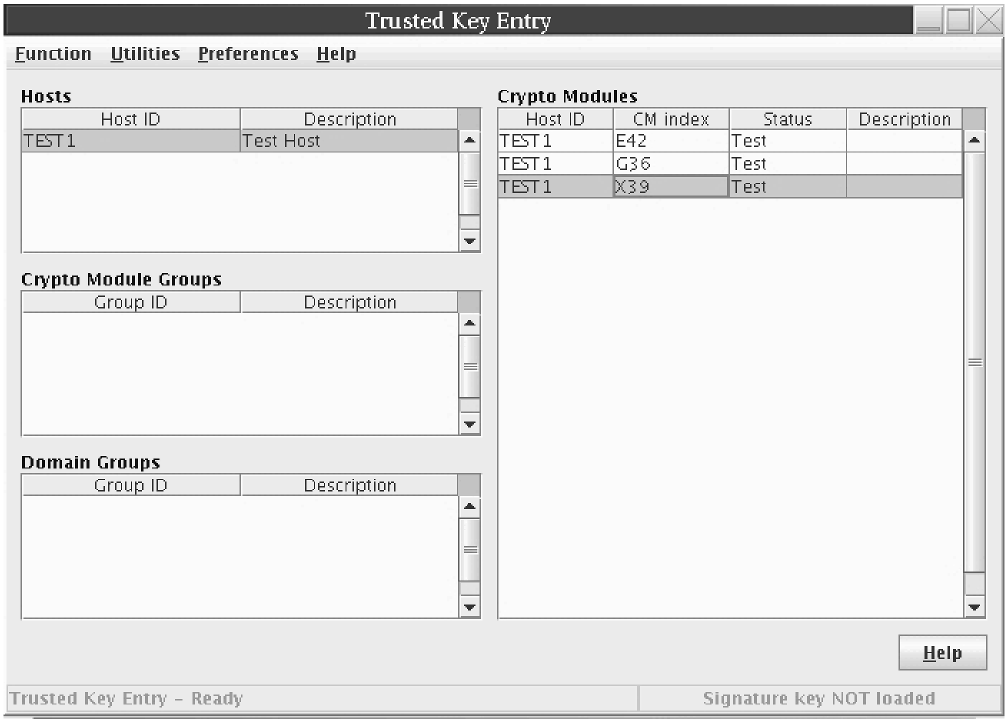
If z/OS V1R7 or higher is installed, mixed case passwords are supported by RACF. If the Enable Mixed Case Passwords check box is enabled on the Log on to Host panel, passwords will be used as entered and will not automatically be folded to upper case. You must enter your password as it was defined in 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/E 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 Crypto Modules

The crypto module container of the TKE Main Window displays the crypto modules that are available for use with the host or group you have selected. The container lists the host ID that the crypto module belongs to, the crypto module index, the status of the crypto module and the description of the crypto module. You are not able to change any of these fields from this container.

Figure 67 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 129.



Hosts

Host ID	Description
TEST1	Test Host

Crypto Module Groups

Group ID	Description

Domain Groups

Group ID	Description

Crypto Modules

Host ID	CM index	Status	Description
TEST1	E42	Test	
TEST1	G36	Test	
TEST1	X39	Test	

Trusted Key Entry - Ready

Signature key NOT loaded

Figure 67. Main Window

As discussed in “Automated Crypto Module Recognition” on page 106, the Crypto Module container is filled in automatically once you have logged onto the host or hosts.

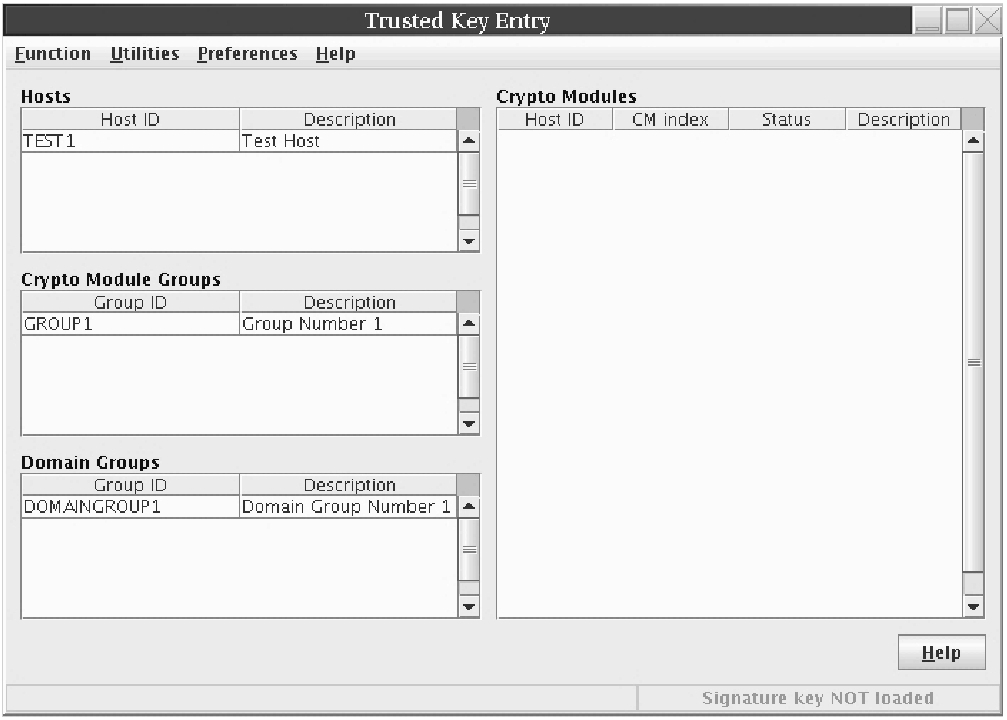
If you have selected a host to work with, you will be able to choose the crypto module you would like to open by highlighting it.

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.



Hosts

Host ID	Description
TEST1	Test Host

Crypto Module Groups

Group ID	Description
GROUP1	Group Number 1

Domain Groups

Group ID	Description
DOMAINGROUP1	Domain Group Number 1

Crypto Modules

Host ID	CM index	Status	Description

Figure 68. 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 and later allows you to manage ECC master 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.

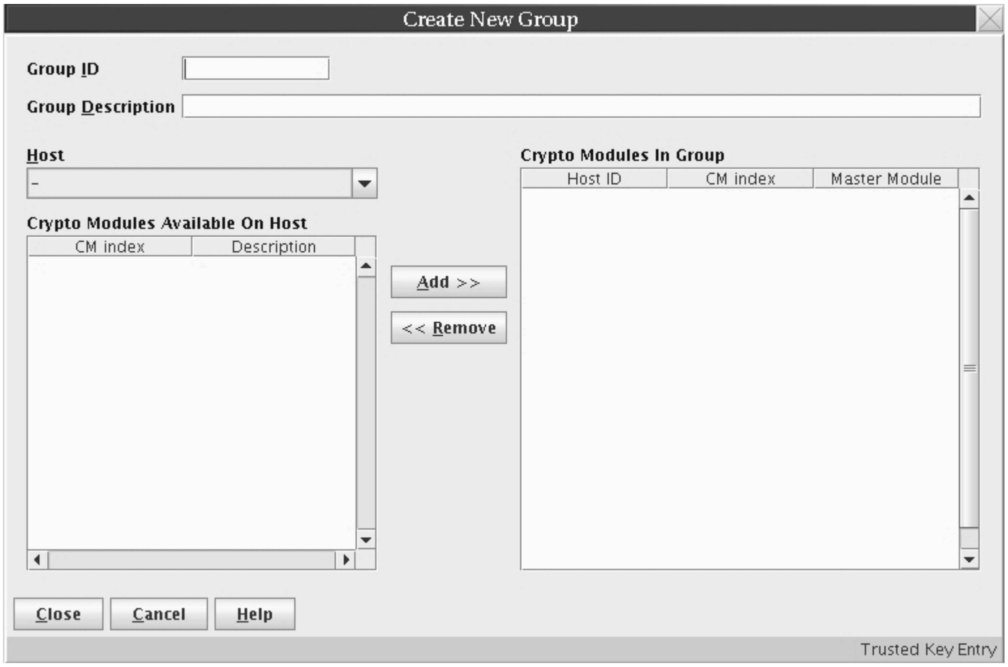


Figure 69. Create New Group

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 necessary.

    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 and later allows you to manage ECC master 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

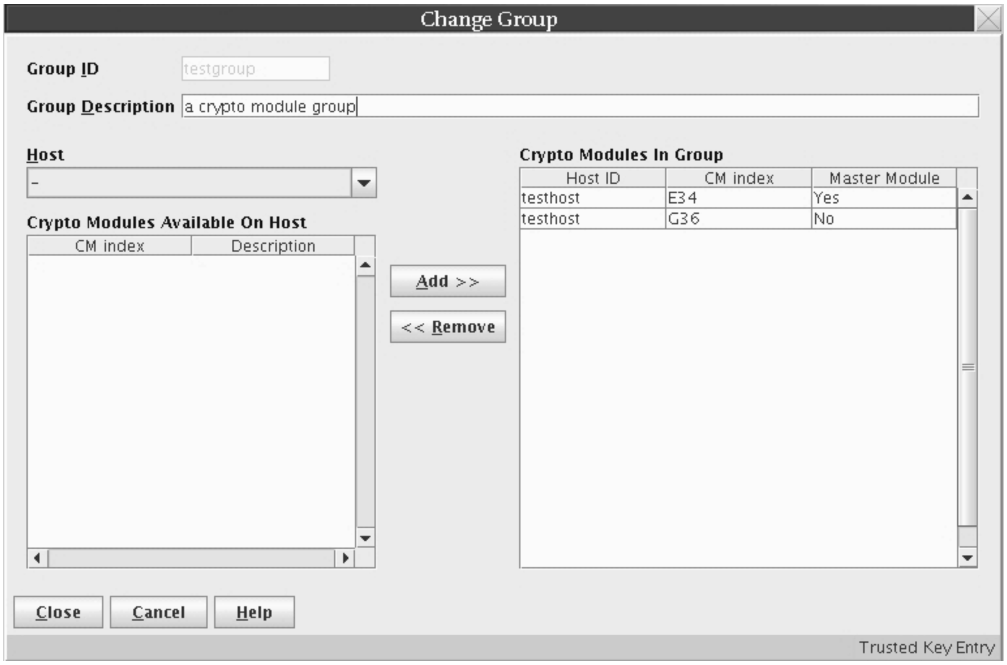
To change a crypto module group:

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.



Group ID: testgroup

Group Description: a crypto module group

Host: –

Crypto Modules Available On Host

CM index	Description

Crypto Modules In Group

Host ID	CM index	Master Module
testhost	E34	Yes
testhost	G36	No

Figure 70. 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 log on 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 necessary.
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 and later allows you to manage ECC master 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 rather compares the crypto modules within a group.

To compare the crypto modules, do the following:

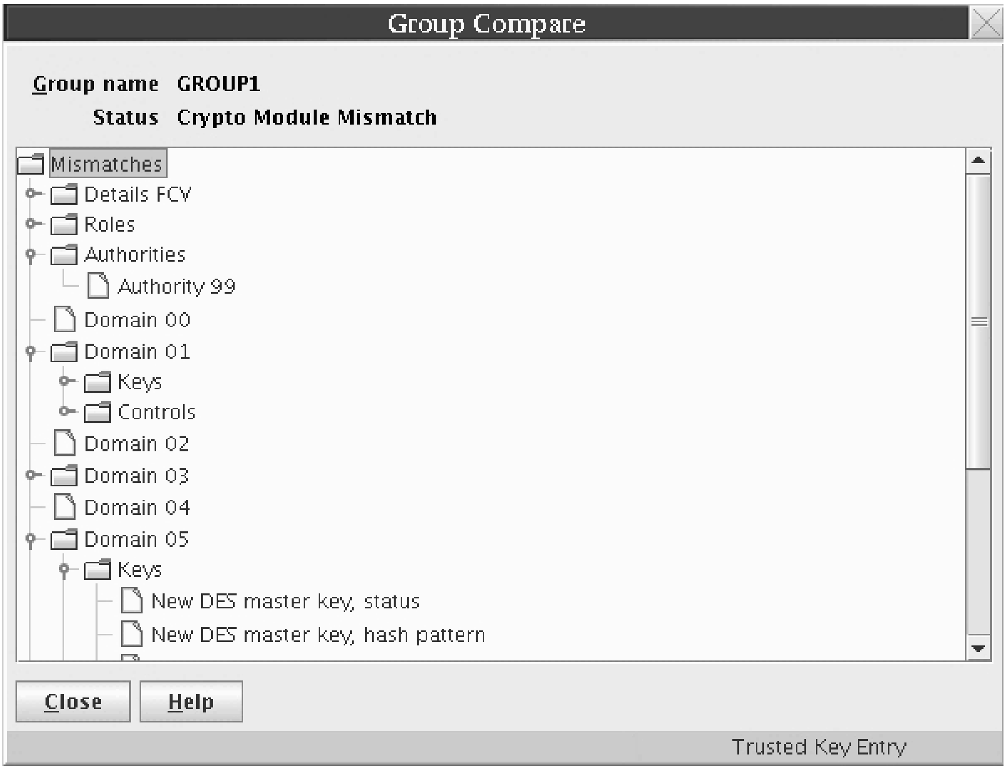
1. From the main window, highlight a specific crypto module group in the Crypto Module Groups container.
2. Right click on the highlighted entry to display a popup menu, and select **Open Group** from the menu.

   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 Crypto Module Group Notebook's **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.



Group Compare

Group name GROUP1

Status Crypto Module Mismatch

Figure 71. 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

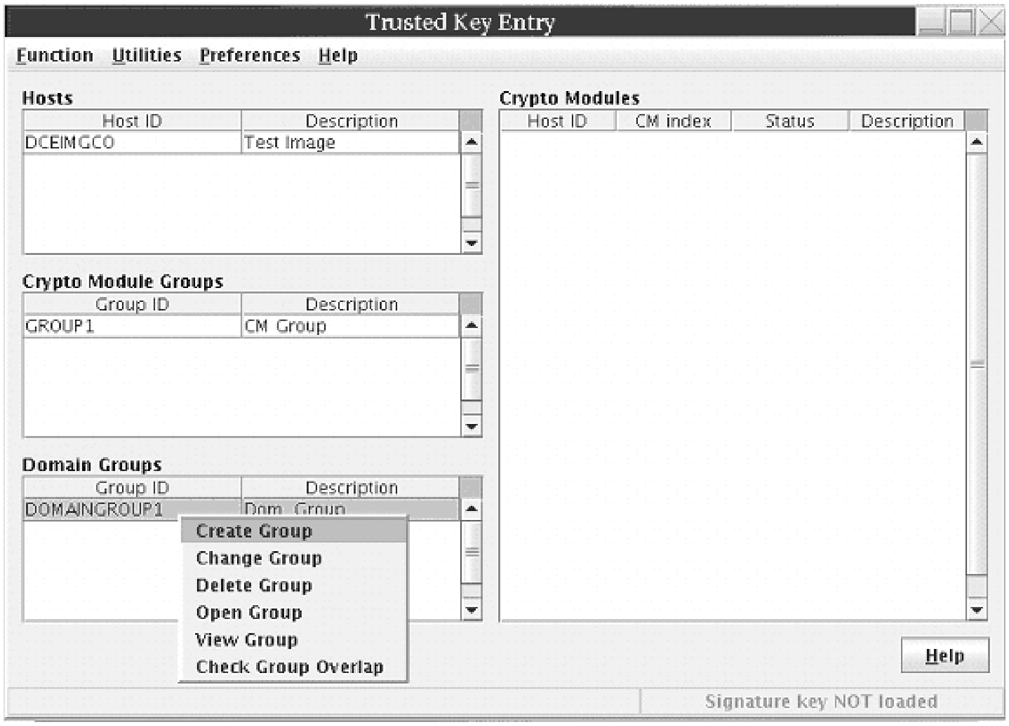
All displayed values in a notebook for a crypto module group are retrieved from the master module. You can perform the following crypto module functions from a crypto module group notebook:

- Create, change, and delete authority
- Create, change, and delete role
- Zeroize domain
- Domain Controls changes
- Decimalization table administration
- Enable/disable crypto modules
- Domain keys:
  - Load key part to new master key register
  - Clear old and new master key registers
  - Set Asymmetric Master Key (ASYM)
  - Load RSA key to the Public Key Data Set (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.



Hosts

Host ID	Description
DCEIMGCO	Test Image

Crypto Module Groups

Group ID	Description
GROUP1	CM Group

Domain Groups

Group ID	Description
DOMAINGROUP1	Dom. Group

Crypto Modules

Host ID	CM index	Status	Description

Signature key NOT loaded

Figure 72. 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 and later allows you to manage ECC master 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

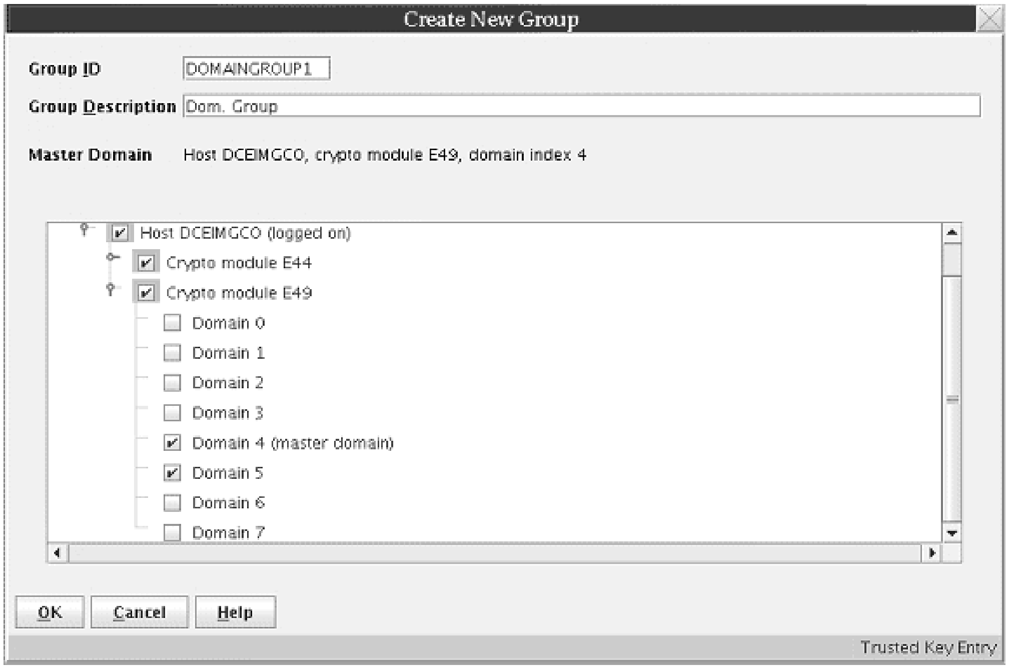
To create a new domain group:

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.



Create New Group

Group ID DOMAINGROUP1

Group Description Dom. Group

Master Domain Host DCEIMGCO, crypto module E49, domain index 4

- ☑ Host DCEIMGCO (logged on)
  - ☑ Crypto module E44
  - ☑ Crypto module E49
    - □ Domain 0
    - □ Domain 1
    - □ Domain 2
    - □ Domain 3
    - ☑ Domain 4 (master domain)
    - ☑ Domain 5
    - □ Domain 6
    - □ Domain 7

Figure 73. 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.

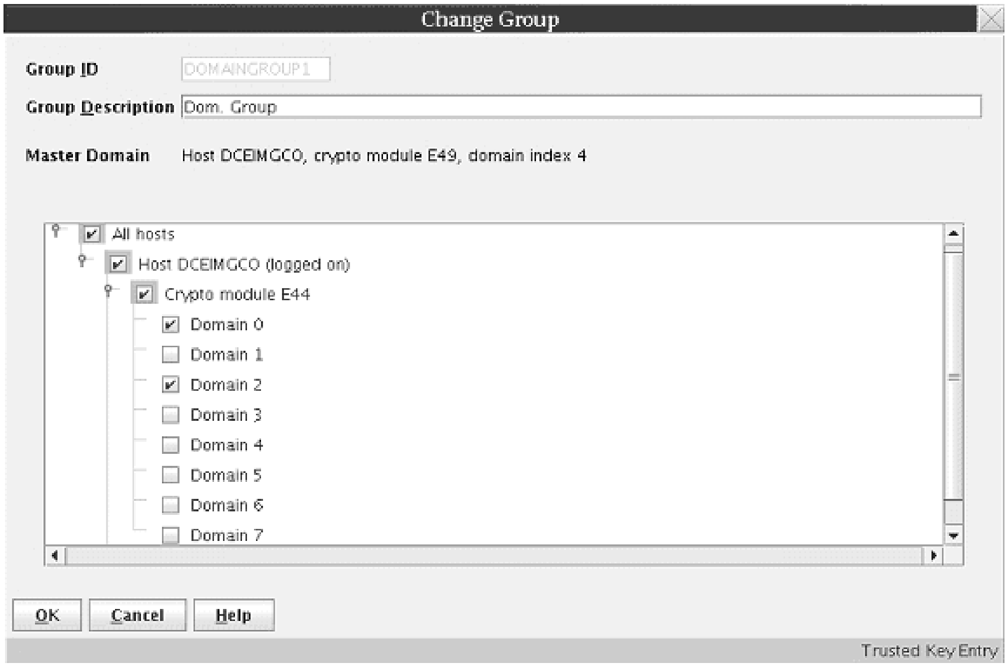
      TKE 6.0 and later allows you to work with AES keys if you have a CEX2C that is AES capable, or a CEX3C. To perform AES functions on a domain group, the master domain must be associated with a crypto module that is AES capable. You can mix AES and non-AES cards together, but the master domain must be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

      TKE 7.0 and later allows you to manage ECC master 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.



Change Group

Group ID: DOMAINGROUP1

Group Description: Dom. Group

Master Domain: Host DCEIMGCO, crypto module E49, domain index 4

- ☑ All hosts
  - ☑ Host DCEIMGCO (logged on)
    - ☑ Crypto module E44
      - ☑ Domain 0
      - □ Domain 1
      - ☑ Domain 2
      - □ Domain 3
      - □ Domain 4
      - □ Domain 5
      - □ Domain 6
      - □ Domain 7

Figure 74. 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:

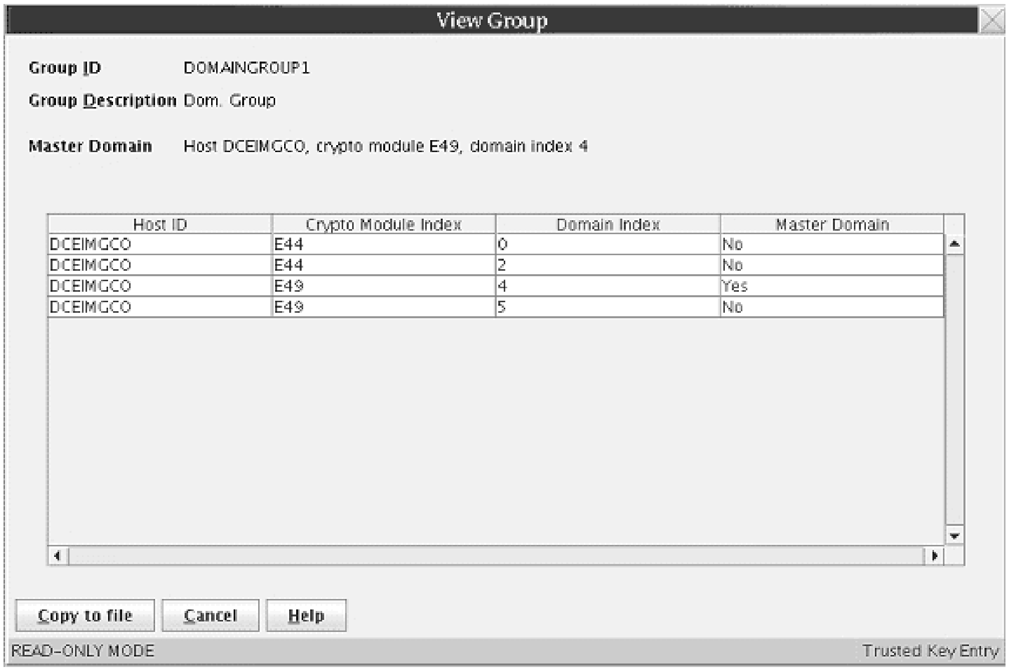
1. Highlight a checked domain with the left mouse button.
2. Click the right mouse button to display a pop-up selection menu.
3. Select **Make this the master domain** menu item from the popup menu.

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.



Group ID DOMAINGROUP1

Group Description Dom. Group

Master Domain Host DCEIMGCO, crypto module E49, domain index 4

Host ID	Crypto Module Index	Domain Index	Master Domain
DCEIMGCO	E44	0	No
DCEIMGCO	E44	2	No
DCEIMGCO	E49	4	Yes
DCEIMGCO	E49	5	No

Figure 75. View Domain Group

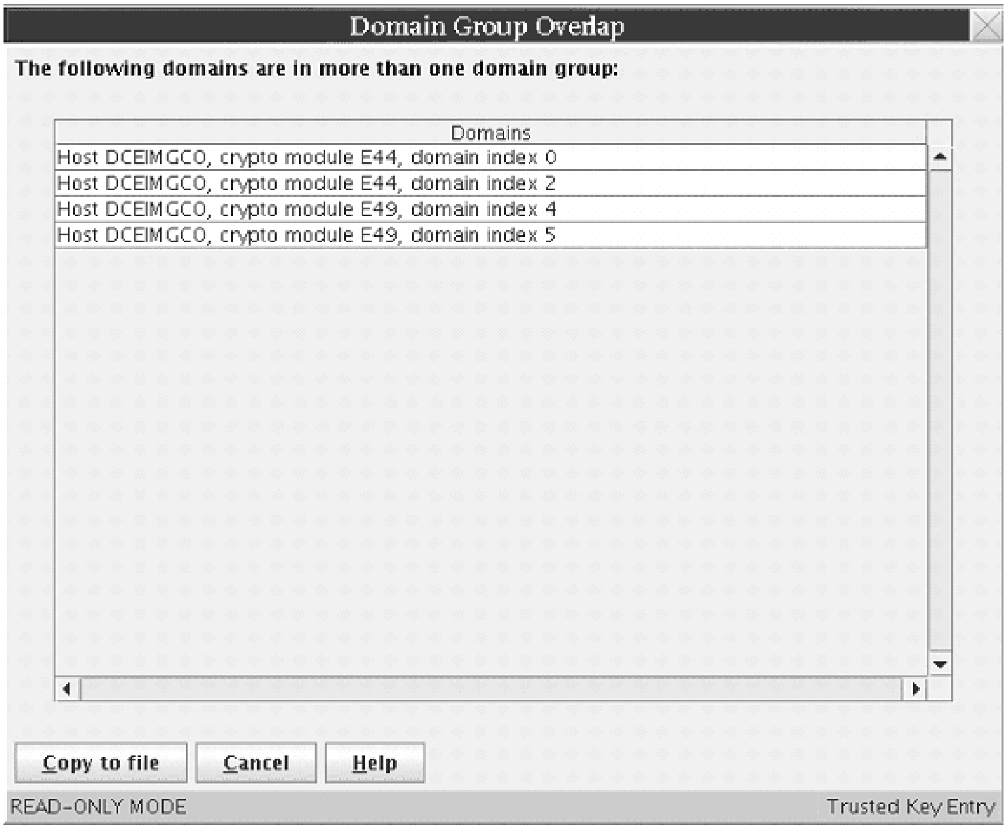
The “View Group” window is opened. The following information is displayed:

- *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.



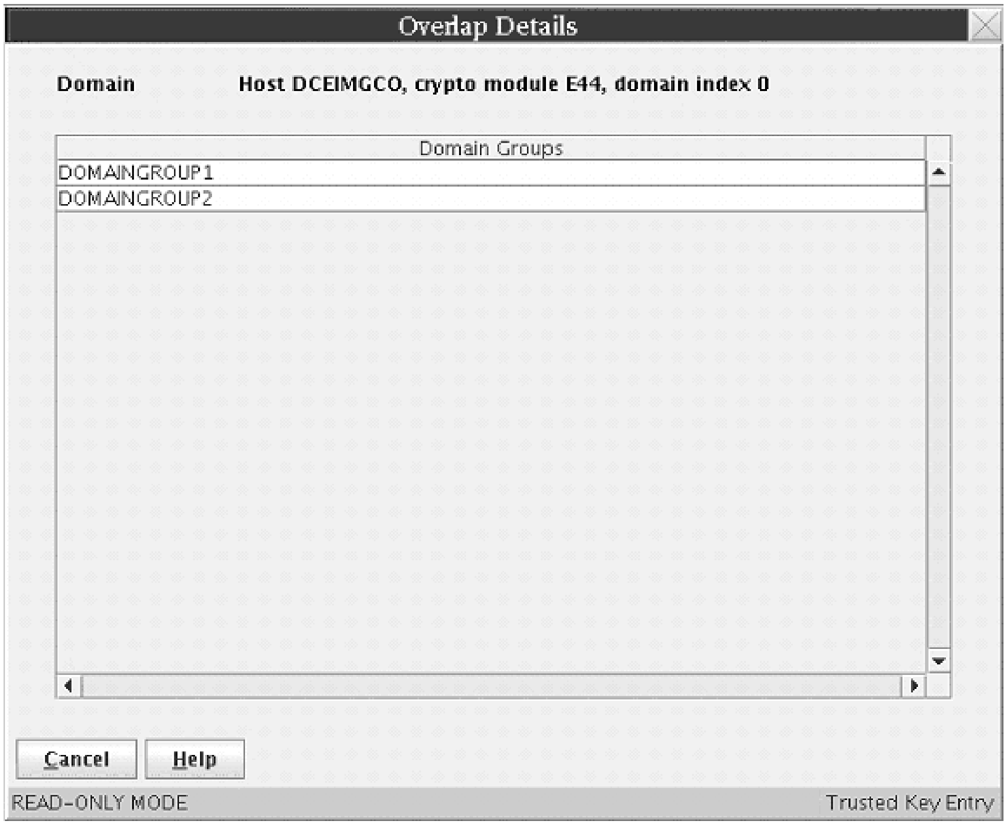
Domain Group Overlap

The following domains are in more than one domain group:

Domains
Host DCEIMGC0, crypto module E44, domain index 0
Host DCEIMGC0, crypto module E44, domain index 2
Host DCEIMGC0, crypto module E49, domain index 4
Host DCEIMGC0, crypto module E49, domain index 5

Figure 76. 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.



Overlap Details

Domain Host DCEIMGCO, crypto module E44, domain index 0

Domain Groups
DOMAINGROUP1
DOMAINGROUP2

Figure 77. Domain Group Overlap Details

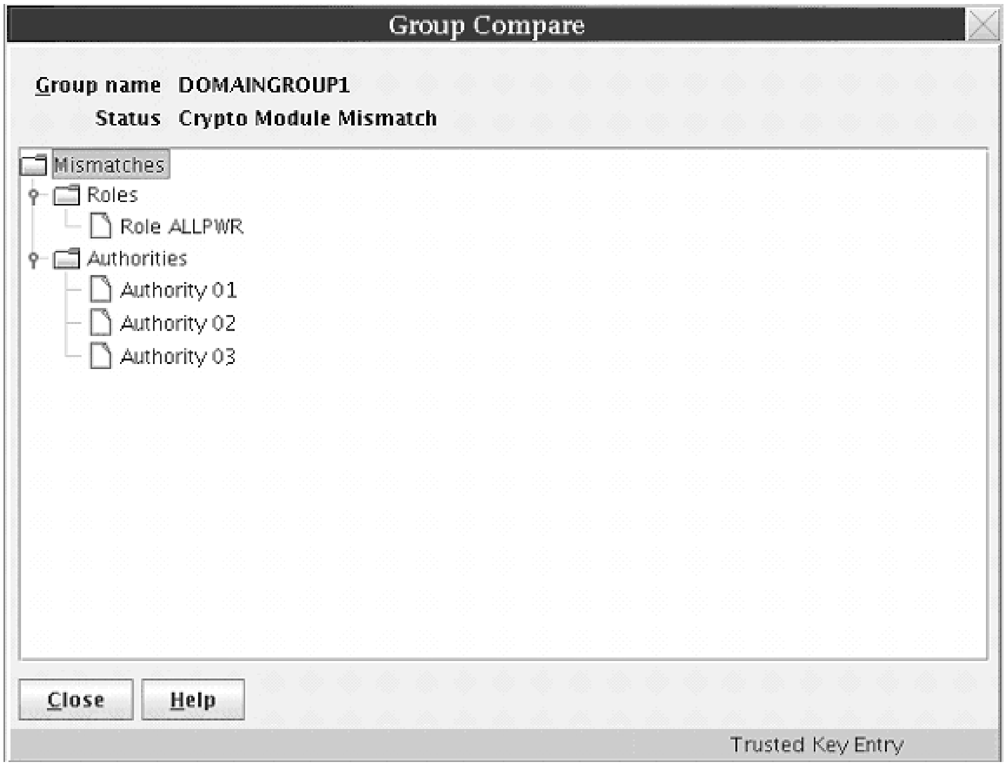
You can copy the domain group overlap information to a file by selecting **Copy to file** and specifying the file name and location to be saved. Otherwise, when finished, press **Cancel**.

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** in the domain group's Crypto Module Notebook, 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.


Group Compare

Group name DOMAINGROUP1

Status Crypto Module Mismatch

- Mismatches
  - Roles
    - Role ALLPWR
  - Authorities
    - Authority 01
    - Authority 02
    - Authority 03

Figure 78. 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
- Decimalization table administration
- Enable/disable crypto module
- Domain keys:
  - Load key part to new master key register
  - Clear old and new master key registers
  - Set Asymmetric Master Key (ASYM)
  - Load RSA key to the Public Key Data Set (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

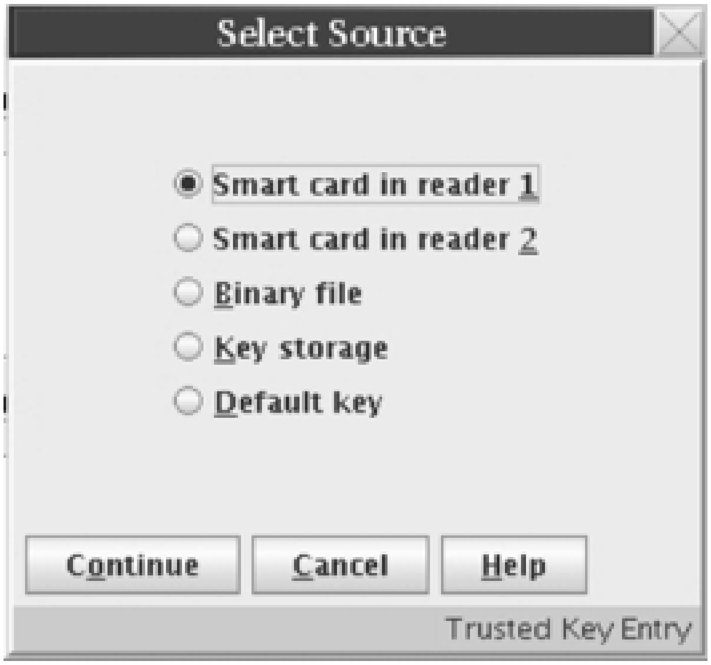
This function is used to load the authority signature key. This authority signature key is active for all operations until explicitly changed by clicking on this option again to load a different authority signature key.

A message is displayed in the lower right hand corner of the TKE main window, indicating what signature key is active. If no signature key has been loaded, the message `SIGNATURE KEY NOT LOADED` is displayed. If a signature key has been loaded, the message `SIGNATURE KEY LOADED` is displayed, along with the index and name associated with the active signature key.

The CEX2C 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 151.

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.



Select Source

● Smart card in reader 1

○ Smart card in reader 2

○ Binary file

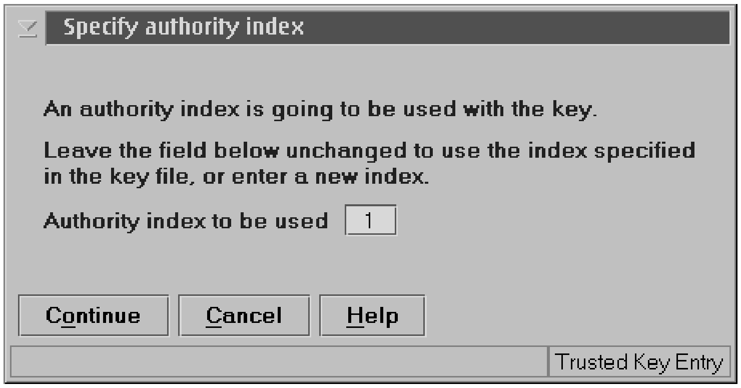
○ Key storage

○ Default key

Figure 79. 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.



Specify authority index

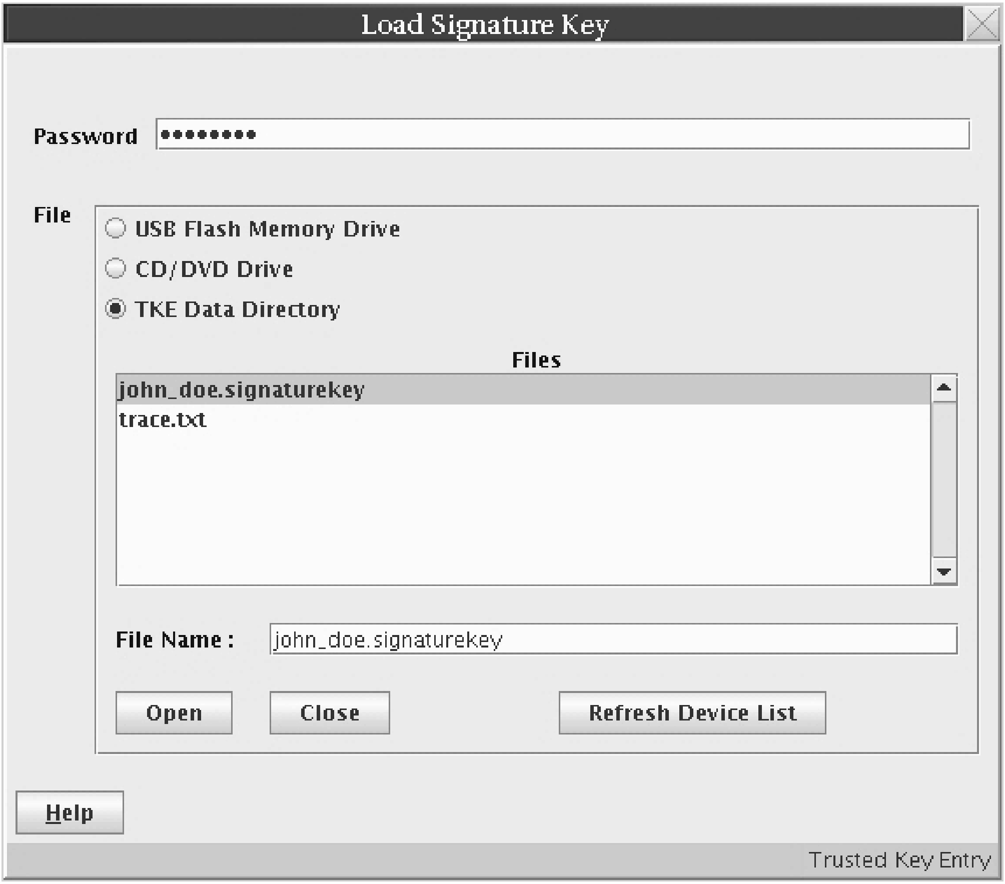
An authority index is going to be used with the key.

Leave the field below unchanged to use the index specified in the key file, or enter a new index.

Authority index to be used 1

Figure 80. 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.



Load Signature Key

Password ••••••••

File

○ USB Flash Memory Drive

○ CD/DVD Drive

● TKE Data Directory

Files

john_doe.signaturekey
trace.txt

File Name : john_doe.signaturekey

Figure 81. 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 2**, you will be prompted to insert your TKE smart card into the smart card reader. You will then be prompted to enter the PIN on the TKE smart card reader's PIN pad.

You will then be prompted to specify the authority index.

Display signature key information

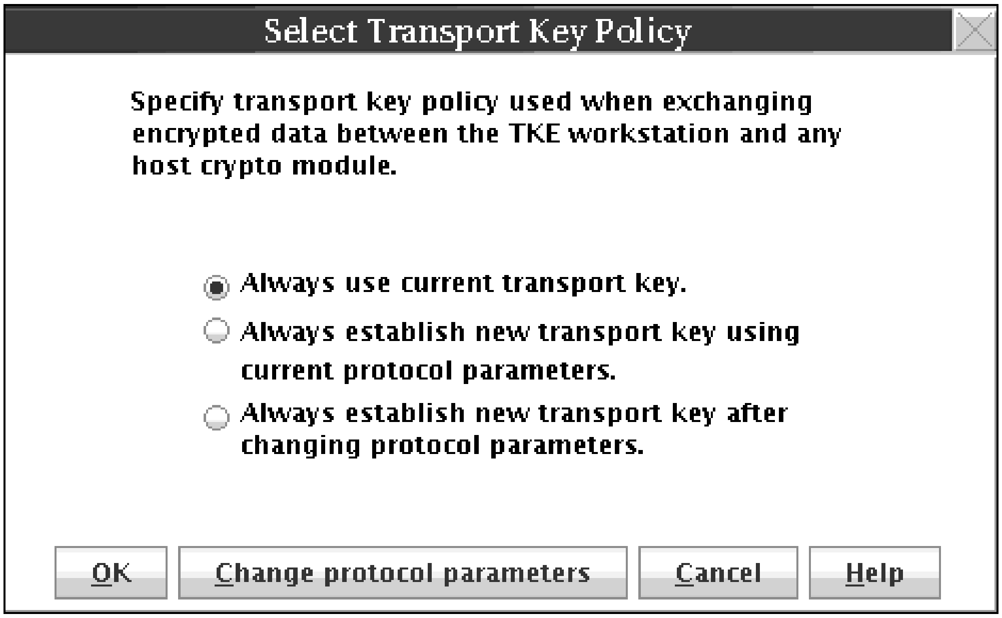
Selecting **Display signature key information** displays a panel showing the current signature index and the key identifier for the current authority signature key.

Define Transport Key Policy

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

Note: When the TKE workstation exchanges encrypted material with a Crypto Express3 at CCA level V4.2, Elliptic Curve Diffie-Hellman (ECDH) is used to derive the shared secret from which the 256-bit AES transport key (key-encrypting-key) is derived.

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.



Select Transport Key Policy

Specify transport key policy used when exchanging encrypted data between the TKE workstation and any host crypto module.

● Always use current transport key.
○ Always establish new transport key using current protocol parameters.
○ Always establish new transport key after changing protocol parameters.

Figure 82. Select Transport Key Policy

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

- **Always use current transport key.** .

  This is the default selection. TKE uses the current transport key or establishes a new transport key if one is not available. This avoids other key agreement protocol actions.
- **Always establish new transport key using current protocol parameters.**

  If TKE is communicating with a host crypto module using DH, it reuses the current Diffie-Hellman modulus and generator values to generate a new transport key for each key transfer. If they are not the correct key length or do not exist, TKE will automatically generate the correct Diffie-Hellman values. This selection avoids the time-consuming generation of the Diffie-Hellman values.

  If TKE is communicating with a host crypto module using ECDH, it uses the current ECDH domain parameters to generate a new transport key for each key transfer.
- **Always establish new transport key after changing protocol parameters.**

  If TKE is communicating with a host crypto module using DH, it will generate a new pair of Diffie-Hellman modulus and generator values and a transport key for each key transfer.

  If TKE is communicating with a host crypto module using ECDH, it uses new ECDH domain parameters to generate a new transport key for each key transfer.

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

If you have selected to reuse the current values of Diffie-Hellman modulus and generator, you can force TKE to generate new Diffie-Hellman values by pressing the **Change protocol parameters button**. For ECDH, the **Change protocol parameters button** will force the TKE to use different ECDH parameters and will cause TKE to establish a new transport key when needed using the new ECDH parameters.

Exit

Selecting **Exit** closes the TKE application window but does not log the current user off the TKE workstation crypto adapter. The TKE application can be restarted without logging in to the TKE workstation crypto adapter.

Exit and logoff

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

Utilities Menu

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

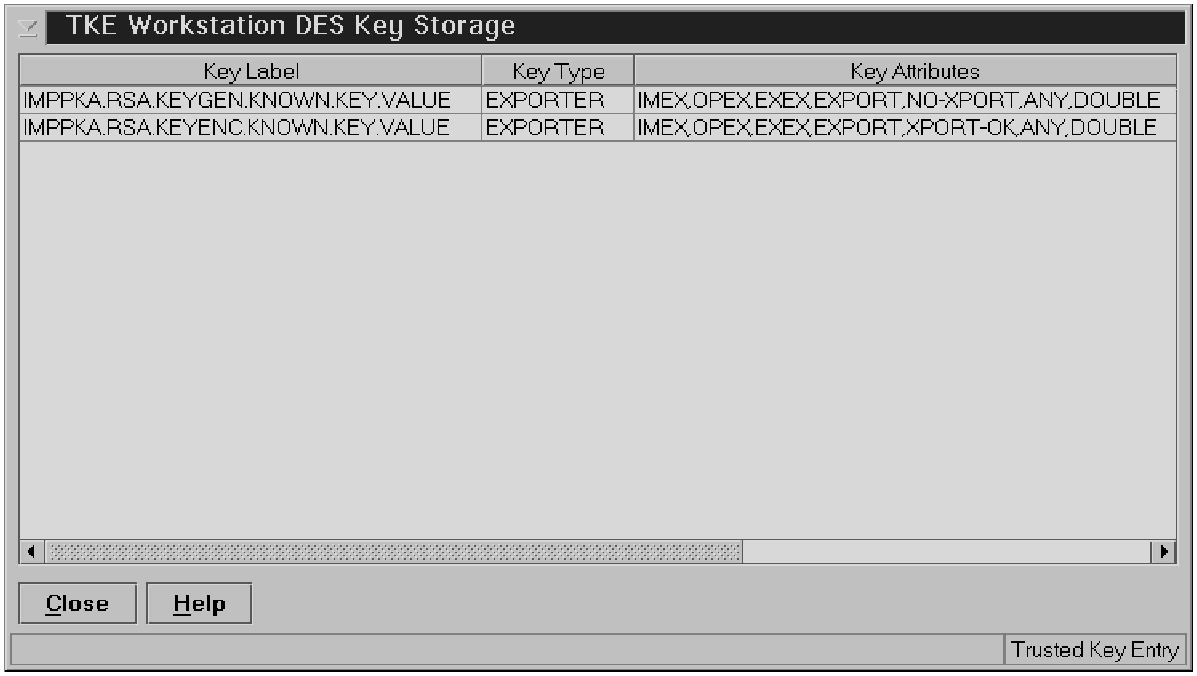
- **Manage Workstation DES keys...**
- **Manage Workstation PKA keys...**
- **Manage smart card contents...**
- **Copy smart card contents...**

These utilities are used for managing the keys in the two TKE 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.



Key Label	Key Type	Key Attributes
IMPPKA.RSA.KEYGEN.KNOWN.KEY.VALUE	EXPORTER	IMEX,OPEX,EXEX,EXPORT,NO-XPORT,ANY,DOUBLE
IMPPKA.RSA.KEYENC.KNOWN.KEY.VALUE	EXPORTER	IMEX,OPEX,EXEX,EXPORT,XPORT-OK,ANY,DOUBLE

Figure 83. 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

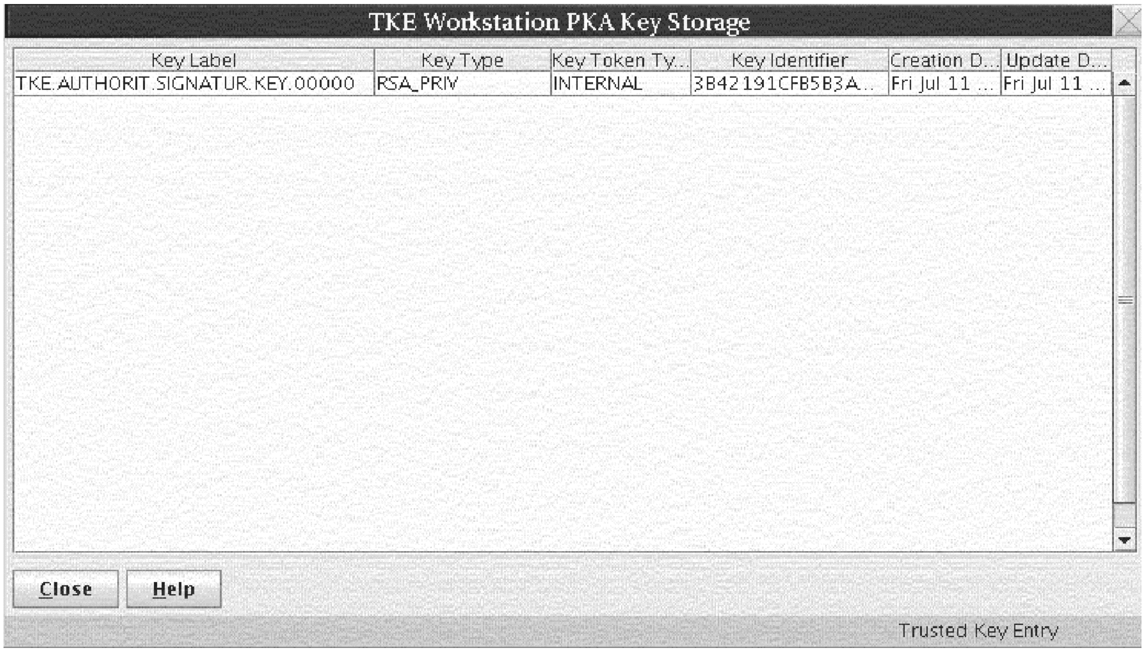
  Following is a list of some of the key words used by the TKE workstation crypto adapter card for defining the control vector.
  - KEY-PART - The initial key part has been loaded but the last key part has not been loaded.
  - NO-XPORT - The key cannot be exported. IMP-PKAs used to protect generated RSA keys have this attribute.
  - XPORT-OK - The key is exportable. IMP-PKAs used to protect entered RSA keys have this attribute.
- Control vector - The CCA control vector.
- Created date and time
- Updated date and time

Deleting an Entry

When you 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.



Key Label	Key Type	Key Token Ty...	Key Identifier	Creation D...	Update D...
TKE.AUTHORIT.SIGNATUR.KEY.00000	RSA_PRIV	INTERNAL	3B42191CFB5B3A...	Fri Jul 11 ...	Fri Jul 11 ...

Figure 84. TKE Workstation PKA Key Storage Window

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

- Key label
- Key type

  The type of key is one of the following:

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

  – RSA-PUB - A token holding the public part of a PKA key pair.

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

  The type of token is one of the following:

  – Internal - The key token is internal and the key value is enciphered under the TKE workstation crypto adapter master key.

  – External - The key token is external and the key value is either enciphered by a key-encrypting key or unenciphered.

  – No_Key - The key token is empty.
- Key Identifier - Identifies the RSA key in PKA key storage. The key identifier is the SHA-256 hash of the DER-encoded public modulus and public exponent of the RSA key pair.
- Created date and time
- Updated date and time

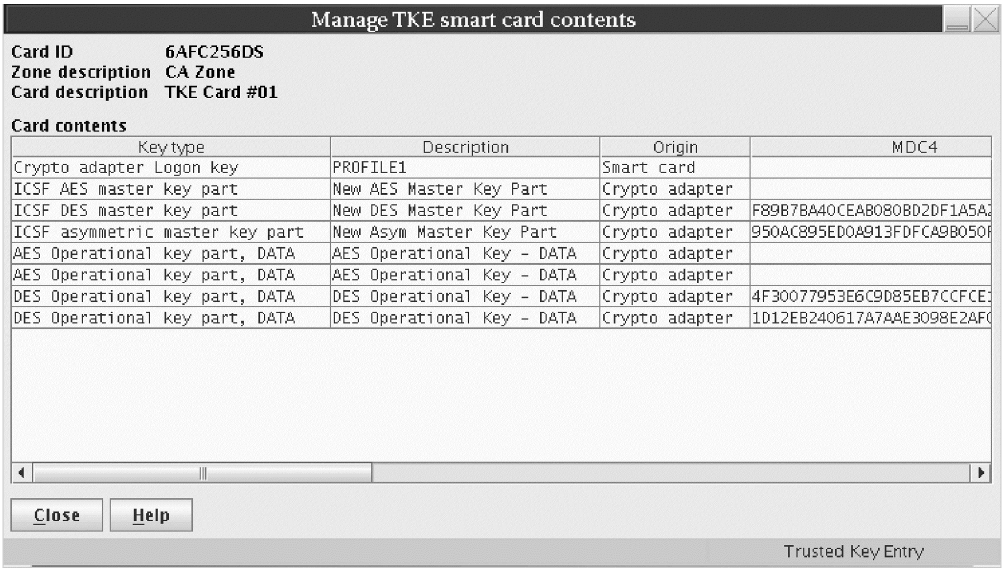
Deleting an Entry

When you 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 the list of key types contained on the smart card, delete keys from your TKE smart card, and display the information about the AES Exporter, Importer, and Cipher operational keys.

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.



Card ID	6AFC256DS
Zone description	CA Zone
Card description	TKE Card #01

Card contents

Key type	Description	Origin	MDC4
Crypto adapter Logon key	PROFILE1	Smart card	
ICSF AES master key part	New AES Master Key Part	Crypto adapter	
ICSF DES master key part	New DES Master Key Part	Crypto adapter	F89B7BA40CEAB080BD2DF1A5A
ICSF asymmetric master key part	New Asym Master Key Part	Crypto adapter	950AC895ED0A913FDFCA9B050
AES Operational key part, DATA	AES Operational Key - DATA	Crypto adapter	
AES Operational key part, DATA	AES Operational Key - DATA	Crypto adapter	
DES Operational key part, DATA	DES Operational Key - DATA	Crypto adapter	4F30077953E6C9D85EB7CCFCE
DES Operational key part, DATA	DES Operational Key - DATA	Crypto adapter	1D12EB240617A7AAE3098E2AF

Figure 85. 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, SHA1, ENC-Zero, AES-VP, Control Vector or Key Attributes (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.

8. You can display the key attributes associated with a CIPHER, EXPORTER, or IMPORTER AES operational key part stored on the smart card. Left click to select the key part, then right click to display a popup menu. Select the **Display key attributes** option to display the key attributes.

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 signature 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 the TKE application and use either the Cryptographic Node Management Utility or the Smart Card Utility Program found in the Trusted Key Entry category's Applications list on the TKE Workstation Console. See Chapter 10, “Cryptographic Node Management Utility (CNM),” on page 241 or Chapter 11, “Smart Card Utility Program (SCUP),” on page 285.
2. To copy ECC key parts, the applet version of the target smart card must be 0.6 or greater.

To copy a smart card:

1. Select **Copy smart card contents...** from the **Utilities** menu.

   A message box prompts you to “Insert source TKE 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 prompts 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

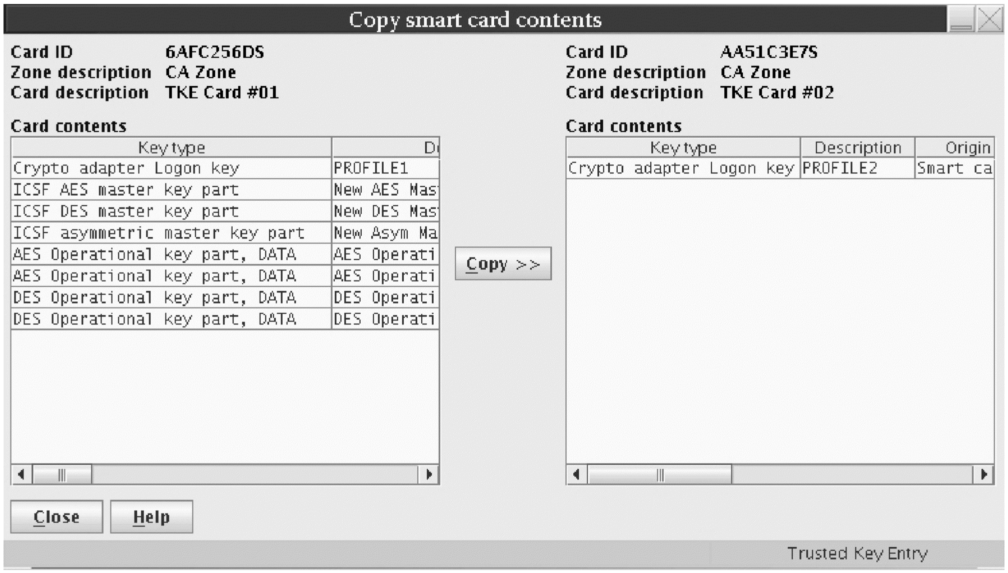
   Zone description
   Description of the zone in which the TKE smart card is enrolled

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

   Card contents
   Key type, Description, Origin, MDC4, SHA1, ENC-Zero, AES-VP, Control Vector or Key Attributes (for operational keys only), and Length.
4. 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 136) or use a different TKE smart card.



Copy smart card contents

Card ID 6AFC256DS
Zone description CA Zone
Card description TKE Card #01

Card contents

Key type	D
Crypto adapter Logon key	PROFILE1
ICSF AES master key part	New AES Mas
ICSF DES master key part	New DES Mas
ICSF asymmetric master key part	New Asym Ma
AES Operational key part, DATA	AES Operati
AES Operational key part, DATA	AES Operati
DES Operational key part, DATA	DES Operati
DES Operational key part, DATA	DES Operati

Card ID AA51C3E7S
Zone description CA Zone
Card description TKE Card #02

Card contents

Key type	Description	Origin
Crypto adapter Logon key	PROFILE2	Smart ca

Figure 86. Select keys to copy

5. 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.

Note: You can display the key attributes associated with a CIPHER, EXPORTER, or IMPORTER AES operational key part stored on either the source or target smart card. Left click to select the key part, then right click to display a popup menu. Select the **Display key attributes** option to display the key attributes.

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.

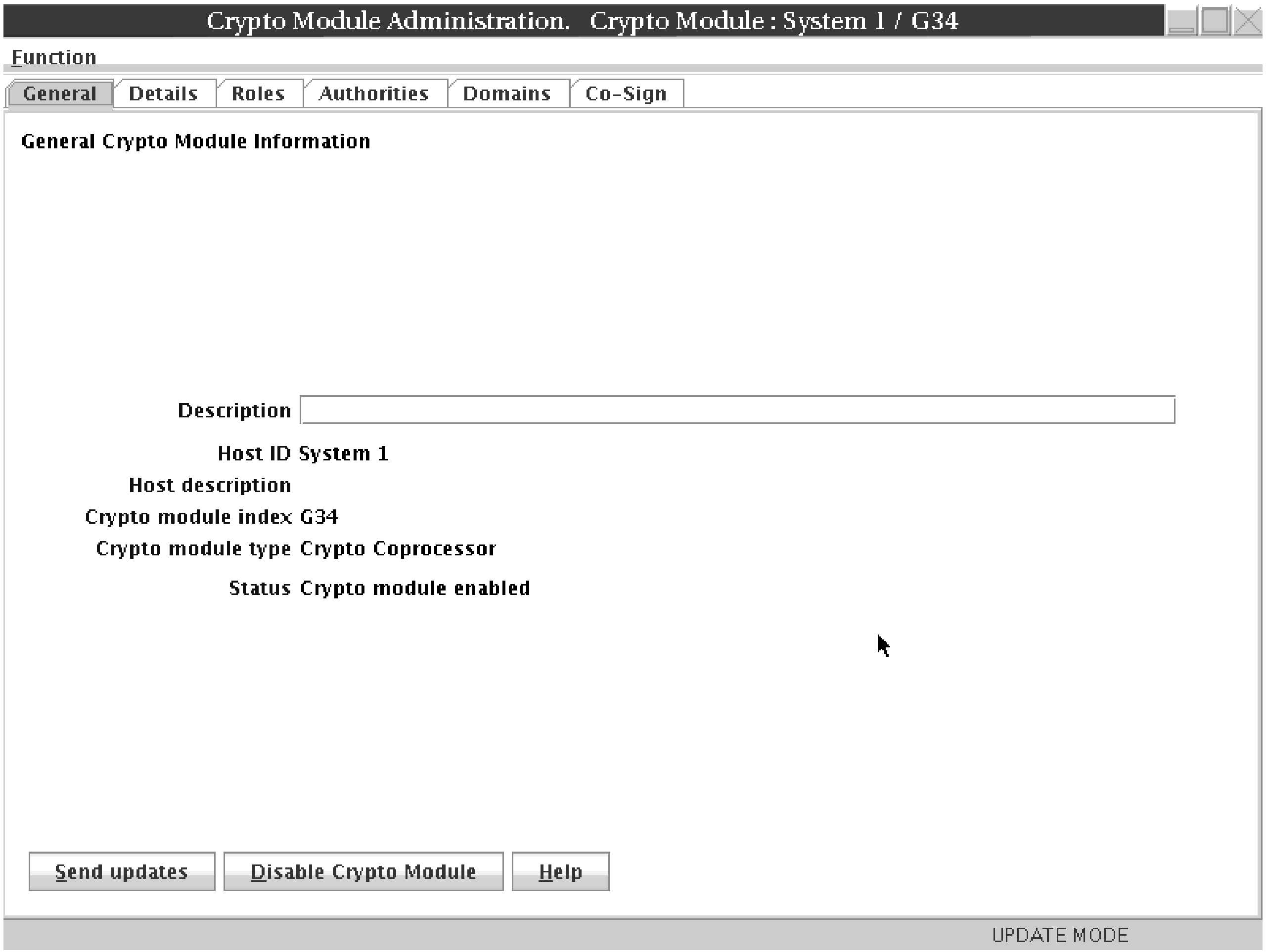
If the menu item is unchecked, TKE will hide all smart card options from the user.

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.



Description

Host ID System 1

Host description

Crypto module index G34

Crypto module type Crypto Coprocessor

Status Crypto module enabled

Figure 87. 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.

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.

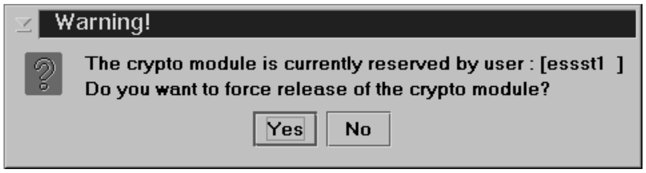
In `PENDING COMMAND MODE`, a command is waiting to be co-signed. A multi-signature command issued by an authority, but not yet executed, is called a pending command. You must perform the co-sign. You cannot issue other commands in this mode. For information about co-signing a pending command, refer to “Crypto Module Notebook Co-Sign Tab” on page 204.

In `LOCKED READ-ONLY MODE`, you are able to display crypto module information for the master module and to compare the reduced group of crypto modules. You are not allowed to do updates. TKE was not able to access one or more crypto modules of the group or domain group.

Crypto Module Notebook Function Menu

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

- **Refresh Notebook** - The content of the notebook is refreshed by reading information from the host. Be aware that performing a refresh may change the mode of the notebook.
- **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.


Warning!

The crypto module is currently reserved by user : [essst1]
Do you want to force release of the crypto module?

Figure 88. 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 119.
- **Close** - This selection closes the Crypto Module Notebook.

Tabular Pages

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

- **General:** see "Crypto Module Notebook General Tab."
- **Details:** see "Crypto Module Notebook Details Tab" on page 145.
- **Roles:** see "Crypto Module Notebook Roles Tab" on page 146.
- **Authorities:** see "Crypto Module Notebook Authorities Tab" on page 150.
- **Domains:** see "Domains Keys Page" on page 160.
- **Co-sign:** see "Crypto Module Notebook Co-Sign Tab" on page 204.

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

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 **Enable Crypto Module**/**Disable Crypto Module** button changes from **Disable Crypto Module** to **Enable Crypto Module**.

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/E user ID on the Host System where the card will be removed.
2. From the ICSF Primary Option Menu, select Option 1 for Coprocessor Management.
3. Leave the Coprocessor Management panel displayed during the rest of this procedure. You will be required to 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. The Support Element is a dedicated workstation used for monitoring and operating IBM System z hardware. A user authorized to perform actions on the Support Element must complete this step.
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. The Support Element is a dedicated workstation used for monitoring and operating IBM System z hardware. A user authorized to perform actions on the Support Element must complete this step.
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.

Crypto Module Notebook Details Tab

The Details tab contains four pages, two for crypto modules and two for crypto module and diagnostic information. These four pages are accessible through tabs found on the right side of the Details tab screen. To view these pages, click on the corresponding tabs. The pages and their contents are:

- **Crypto Module:**
  - **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 transport key for this crypto module
- **Crypto Services (Function Control Vector Values)**
  - Base CCA services availability
  - CDMF availability
  - 56-bit DES availability
  - Triple DES availability
  - 128-bit AES availability
  - 192-bit AES availability
  - 256-bit AES availability
  - SET services
  - Maximum length of RSA keys used to encipher DES keys
  - Maximum elliptic curve field size in bits for key management
- **Other CM Info** - The following crypto module infomation is displayed:
  - CCA Version
  - CCA Build Date
  - DES Hardware Level
  - RSA Hardware Level
  - Power-On Self Test Version (0,1,2)
  - Operating System Name
  - Operating System Version
  - Part Number
  - Engineering Change Level
  - Miniboot Version (0,1)
  - Adapter ID
  - Processor Speed
  - Flash Memory Size
  - Dynamic RAM Memory Size
  - Battery-Backed Memory Size
- **Diagnostic Info** - The following diagnostic information is displayed:

  - Intrusion Latch
  - Battery State
  - Error Log Status
  - Command Information

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.

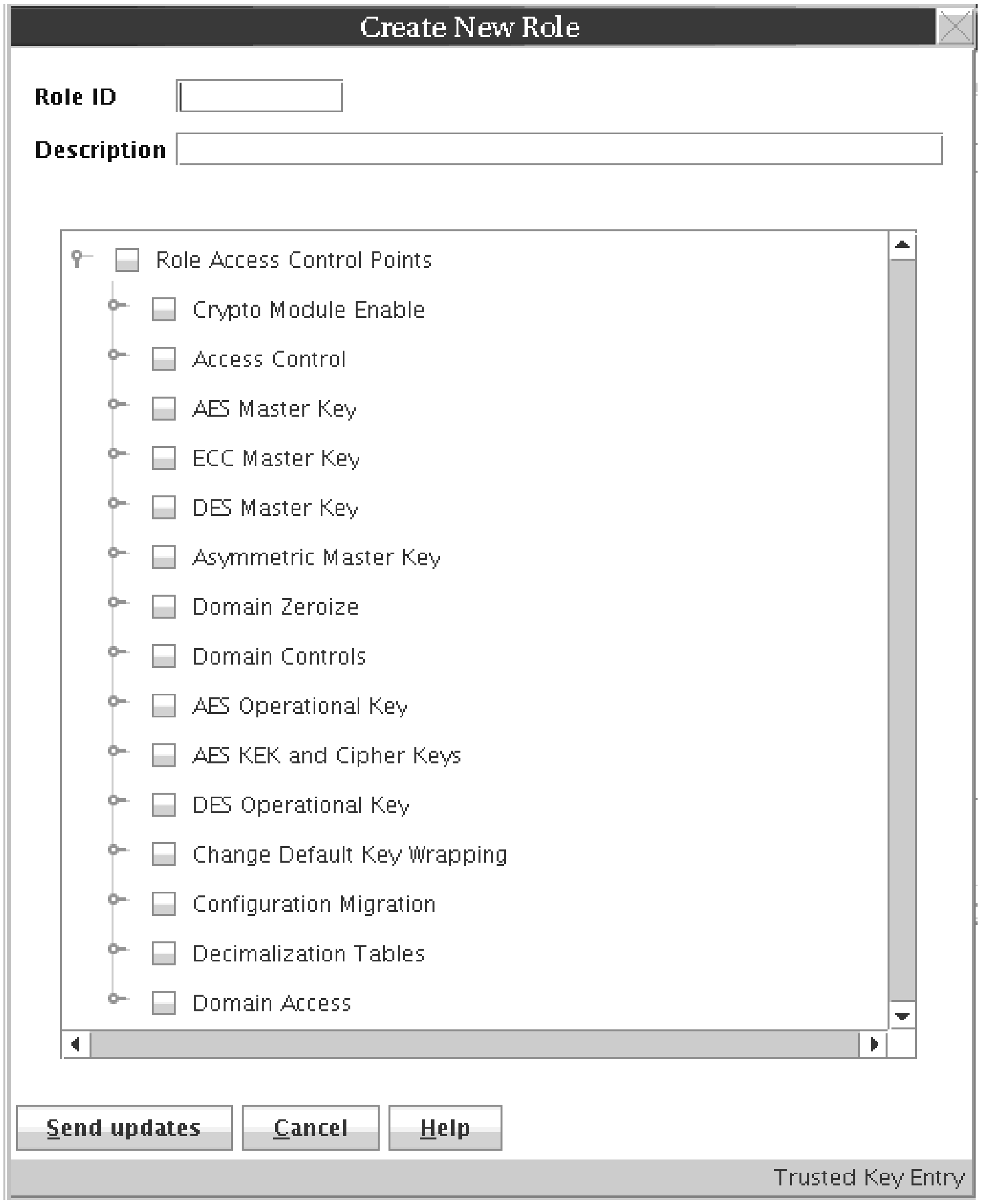
Single Signature Commands

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
- *Decimalization Tables* - Load Decimalization Tables
- *Decimalization Tables* - Delete Decimalization Tables
- *Decimalization Tables* - Activate Decimalization Tables

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
- □ AES KEK and Cipher Keys
- □ DES Operational Key
- □ Change Default Key Wrapping
- □ Configuration Migration
- □ Decimalization Tables
- □ Domain Access

Figure 89. Create New Role Page

If you select **Create** or **Change** from 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. Following is a list of role categories that can be selected, depending on what the role requires:
  - **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.

- **AES KEK and Cipher Keys**

  Choose whether the role can load First and Additional key parts to AES KEK and Cipher 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). Operations on AES KEK and Cipher keys are only supported on CEX3C crypto modules (with FMID HCR7790 or later of ICSF and CCA level 4.2 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.

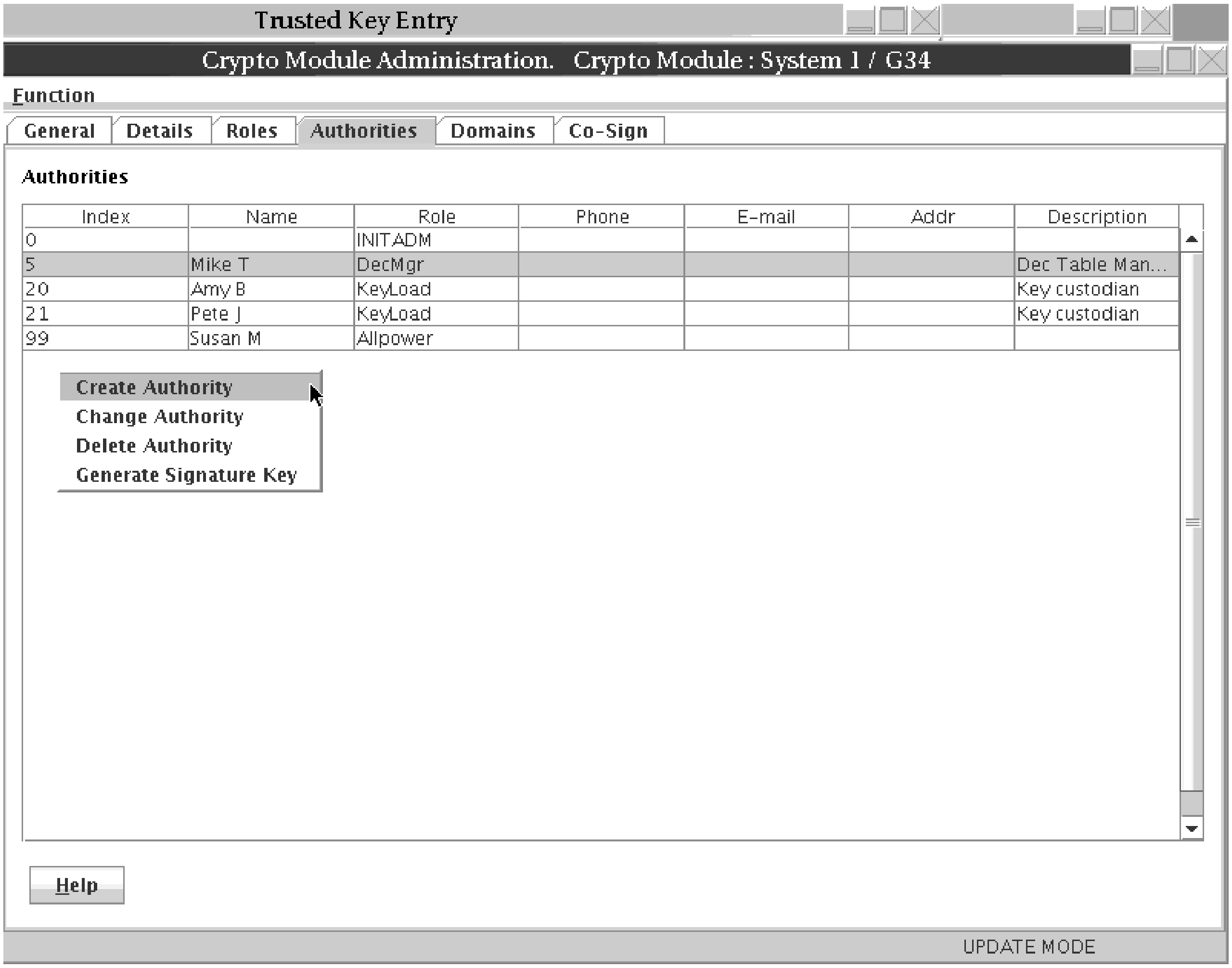
You must delete or reassign all authorities associated with a role before you delete the role.

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).



Index	Name	Role	Phone	E-mail	Addr	Description
0		INITADM				
5	Mike T	DecMgr				Dec Table Man...
20	Amy B	KeyLoad				Key custodian
21	Pete J	KeyLoad				Key custodian
99	Susan M	Allpower				

Figure 90. Authorities Page

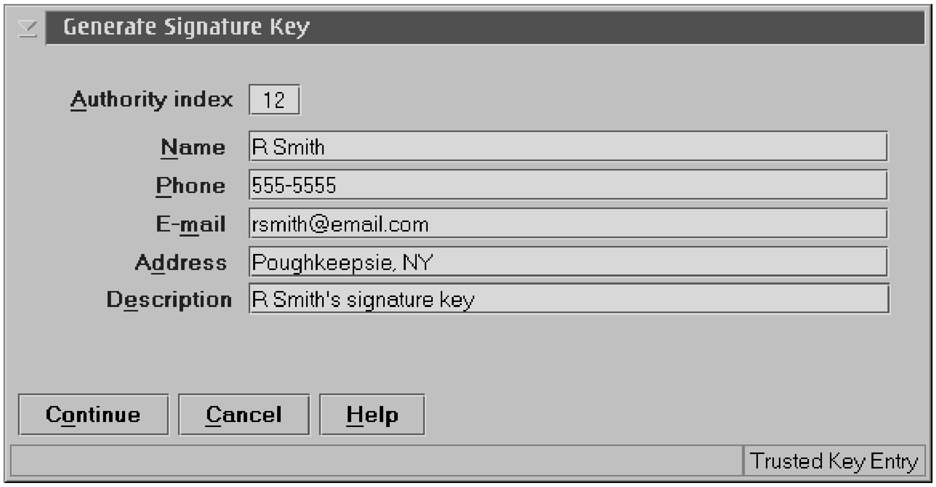
Generating Authority Signature Keys

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:

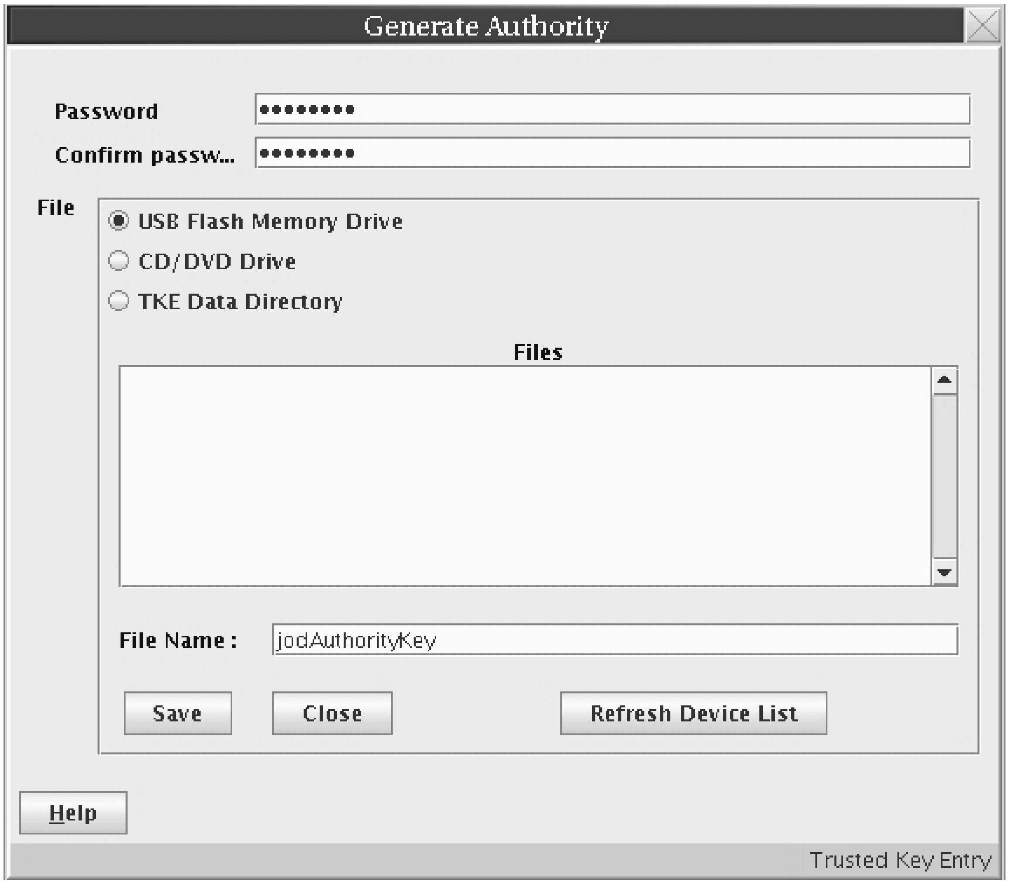
1. Enter **Authority index**. This is a mandatory field with the index of the authority. Valid range is 00 through 99. The authority index will be saved with the key and is called the Default Authority index. The Default Authority index for a saved authority signature key can be overridden when the authority 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**.



Authority index	12
Name	R Smith
Phone	555-5555
E-mail	rsmith@email.com
Address	Poughkeepsie, NY
Description	R Smith's signature key

Figure 91. 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** or **key storage**, or generated and saved on a **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 target. If the signature key target is a smart card, you can generate 1024-bit or 2048-bit authority signature keys. If the signature key target is a binary file or key storage, you can generate 1024-bit, 2048-bit, or 4096-bit authority signature keys.
5. If the authority signature key is to be saved to a **binary file**, a password and file name are required to encrypt and save the key file. After 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.



Password ●●●●●●●●●

Confirm passw... ●●●●●●●●●

File
- ● USB Flash Memory Drive
- ○ CD/DVD Drive
- ○ TKE Data Directory

File Name : jodAuthorityKey

Figure 92. 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 334.

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.

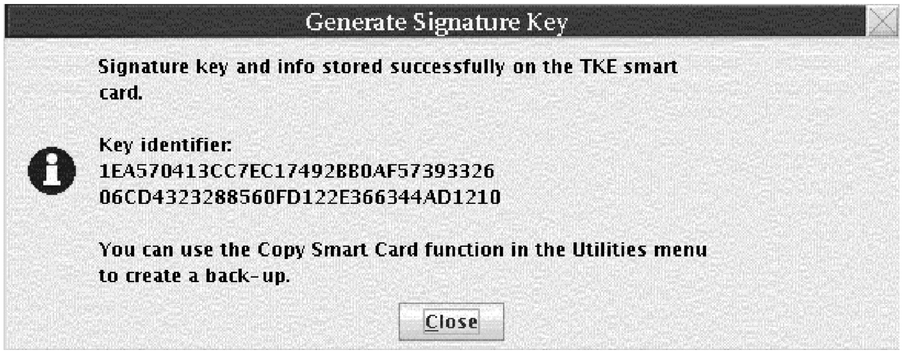
6. If the key is to be generated and saved on a **TKE smart card**, a message box displays, prompting you to "Insert TKE smart card in smart card reader 2.

   a. Insert the TKE smart card into Smart Card Reader 2. Press **OK**.

   b. When the authority signature key is generated and saved to a TKE smart card, it is protected by the PIN of the TKE smart card. A message box 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.



Signature key and info stored successfully on the TKE smart card.

Key identifier:
1EA570413CC7EC17492BB0AF57393326
06CD4323288560FD122E366344AD1210

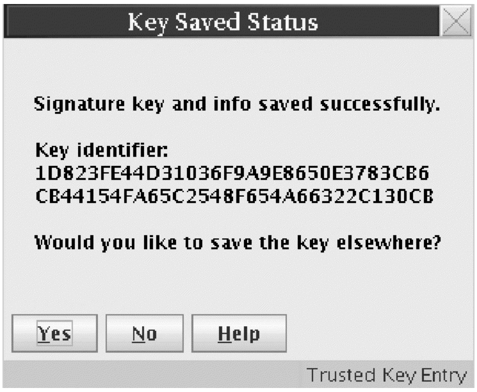
You can use the Copy Smart Card function in the Utilities menu to create a back-up.

Figure 93. Generate signature key

When generating and saving an authority signature key on a TKE smart card, you are not given the option to save it again. You should use the **Copy smart card contents** utility to save the signature key again. See “Copy smart cards” on page 137.

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.



Signature key and info saved successfully.

Key identifier:
1D823FE44D31036F9A9E8650E3783CB6
CB44154FA65C2548F654A66322C130CB

Would you like to save the key elsewhere?

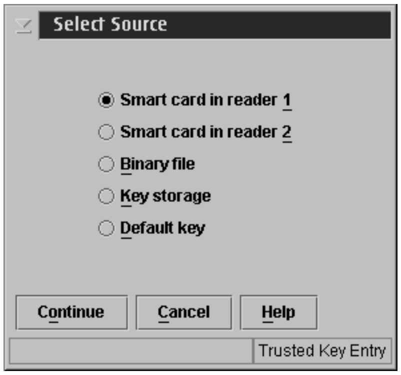
Figure 94. Key saved status message

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 151).

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** button.



● Smart card in reader 1

○ Smart card in reader 2

○ Binary file

○ Key storage

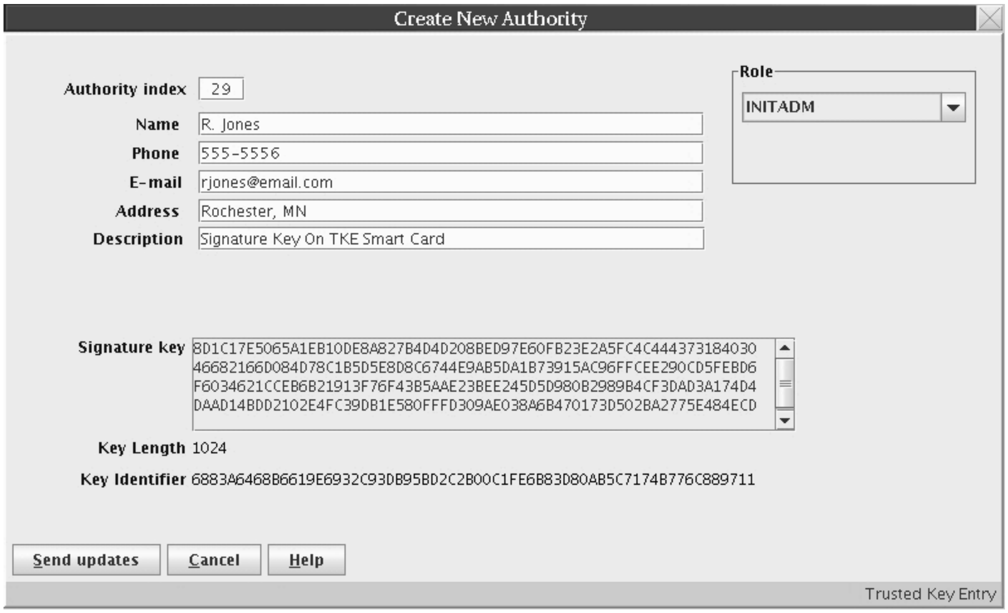
○ Default key

Figure 95. 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.



Authority index	29
Name	R. Jones
Phone	555-5556
E-mail	rjones@email.com
Address	Rochester, MN
Description	Signature Key On TKE Smart Card
Role	INITADM
Signature key	8D1C17E5065A1EB10DE8A827B4D4D208BED97E60FB23E2A5FC4C444373184030 46682166D084D78C1B5D5E8D8C6744E9AB5DA1B73915AC96FFCEE290CD5FEBD6 F6034621CCEB6B21913F76F43B5AAE23BEE245D5D980B2989B4CF3DAD3A174D4 DAAD14BDD2102E4FC39DB1E580FFFD309AE038A6B470173D502BA2775E484ECD
Key Length	1024
Key Identifier	6883A6468B6619E6932C93DB95BD2C2B00C1FE6B83D80AB5C7174B776C889711

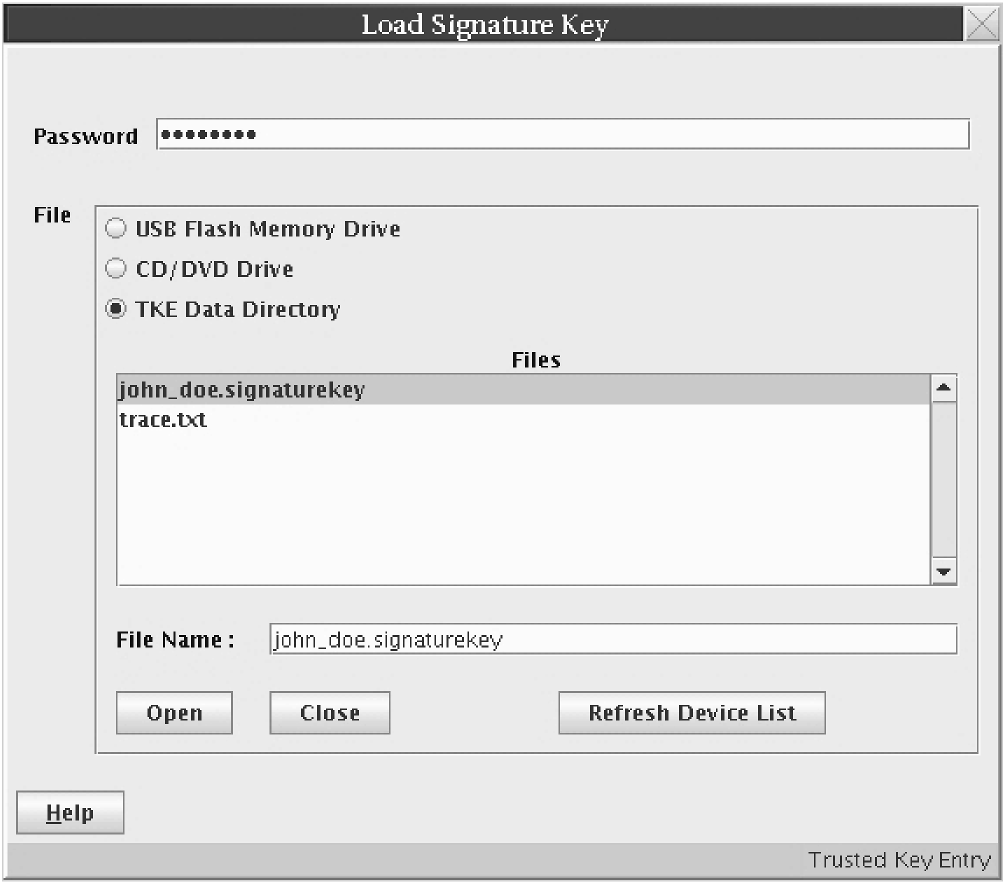
Figure 96. Create new authority

- 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 334.

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 Signature Key

Password ••••••••

File

○ USB Flash Memory Drive

○ CD/DVD Drive

● TKE Data Directory

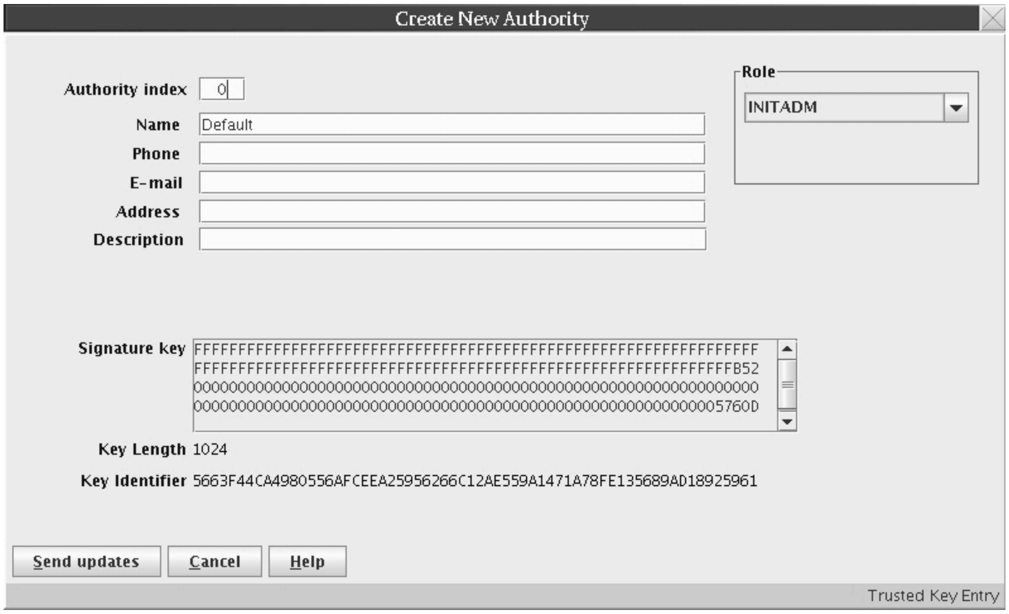
Files

john_doe.signaturekey
trace.txt

File Name : john_doe.signaturekey

Figure 97. Load Signature Key from binary file

- If you select **Default key** from the Select Source dialog, the word "Default" is automatically placed in the **Name** field of the Create New Authority window.



Authority index: 0

Name: Default

Phone:

E-mail:

Address:

Description:

Role: INITADM

Signature key:

```
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFB52
0000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000005760D
```

Key Length: 1024

Key Identifier: 5663F44CA4980556AFCEEA25956266C12AE559A1471A78FE135689AD18925961

Figure 98. 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.

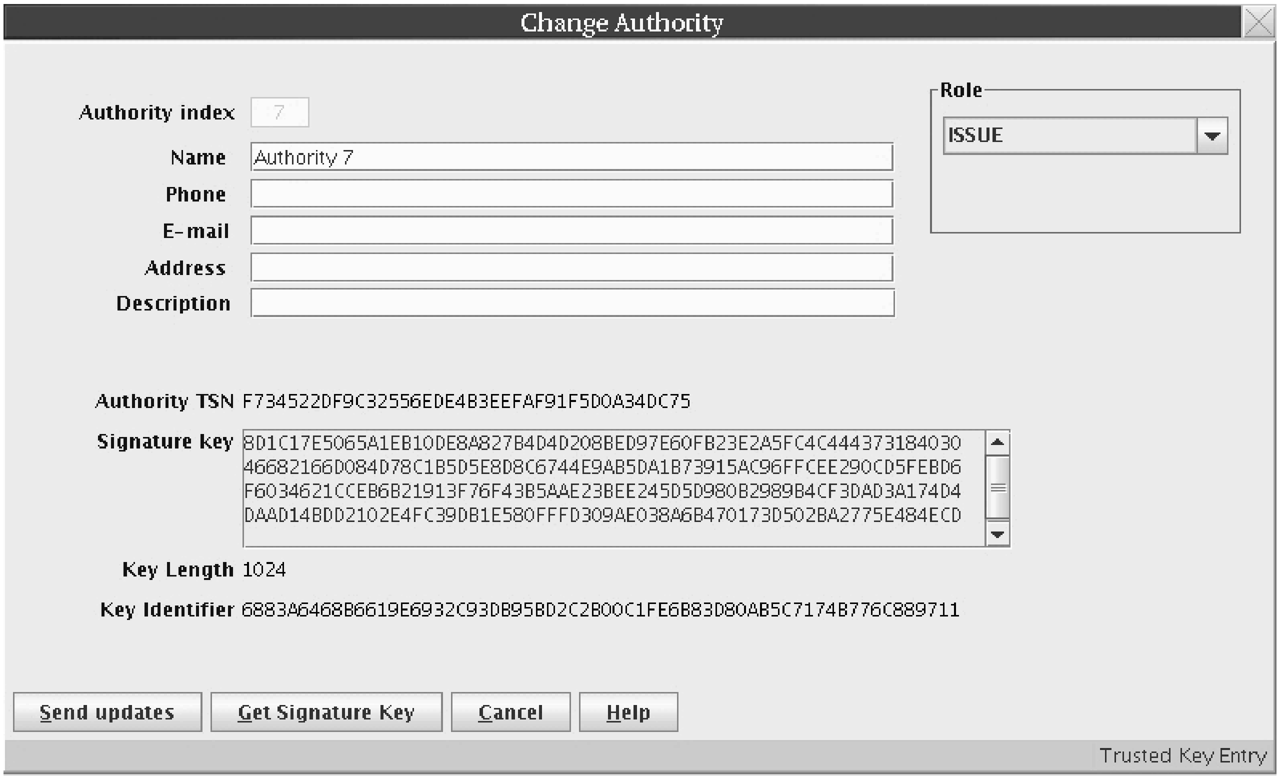
In the **Role** container there is a drop-down list. Select one of the previously defined roles. The authority is mapped to the access rights of that role. This is available only when creating or changing a crypto module authority.

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



Authority index 7

Name Authority 7

Phone

E-mail

Address

Description

Role: ISSUE

Authority TSN F734522DF9C32556EDE4B3EEFAF91F5D0A34DC75

Signature key
```
8D1C17E5065A1EB10DE8A827B4D4D208BED97E60FB23E2A5FC4C444373184030
46682166D084D78C1B5D5E8D8C6744E9AB5DA1B73915AC96FFCEE290CD5FEBD6
F6034621CCEB6B21913F76F43B5AAE23BEE245D5D980B2989B4CF3DAD3A174D4
DAAD14BDD2102E4FC39DB1E580FFFD309AE038A6B470173D502BA2775E484ECD
```

Key Length 1024

Key Identifier 6883A6468B6619E6932C93DB95BD2C2B00C1FE6B83D80AB5C7174B776C889711

Figure 99. 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.

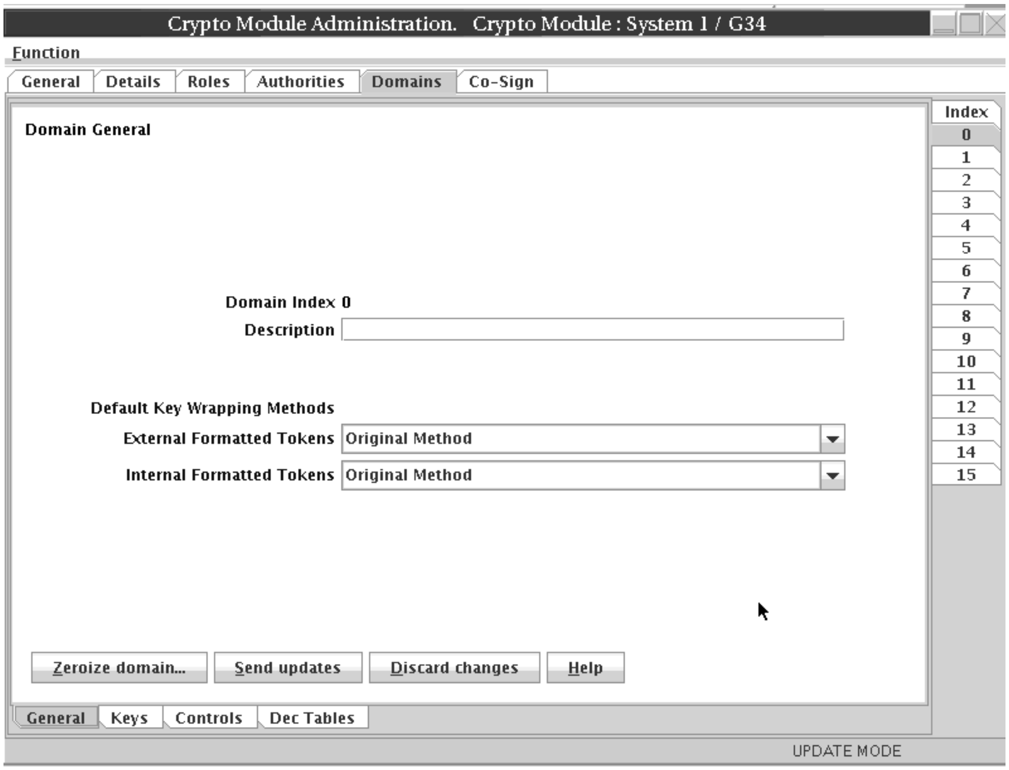
Crypto Module Notebook Domains Tab

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 domain 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 four associated pages: the General page, the Keys page, the Controls page, and the Dec Tables page. From the Domains General page, you can update the description, zeroize the domain, and discard changes.



Domain General

Domain Index 0

Description

Default Key Wrapping Methods

External Formatted Tokens Original Method

Internal Formatted Tokens Original Method

Figure 100. 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.

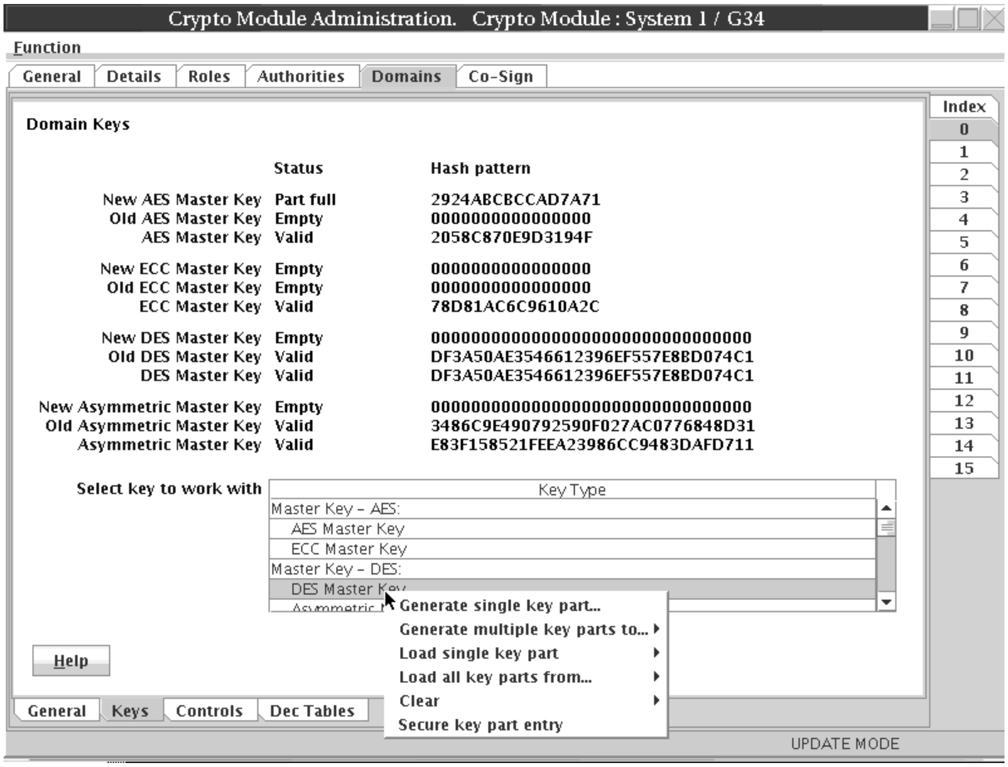
Note: Unlike the Global Zeroize issued from the Support Element, Zeroize Domain does not affect the enablement of TKE Commands on the supported crypto modules (CEX2C and CEX3C). Refer to “TKE Enablement” on page 8.

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, ECC, 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 or the Smart Card Utility Program under Trusted Key Entry Applications. See “Display smart card details” on page 277 or Chapter 11, “Smart Card Utility Program (SCUP),” on page 285.



Domain Keys

	Status	Hash pattern
New AES Master Key	Part full	2924ABCBCCAD7A71
Old AES Master Key	Empty	0000000000000000
AES Master Key	Valid	2058C870E9D3194F
New ECC Master Key	Empty	0000000000000000
Old ECC Master Key	Empty	0000000000000000
ECC Master Key	Valid	78D81AC6C9610A2C
New DES Master Key	Empty	00000000000000000000000000000000
Old DES Master Key	Valid	DF3A50AE3546612396EF557E8BD074C1
DES Master Key	Valid	DF3A50AE3546612396EF557E8BD074C1
New Asymmetric Master Key	Empty	00000000000000000000000000000000
Old Asymmetric Master Key	Valid	3486C9E490792590F027AC0776848D31
Asymmetric Master Key	Valid	E83F158521FEEA23986CC9483DAFD711

Figure 101. 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 30 on page 161 illustrates the possibilities for the supported crypto modules.

Table 30. Key types and actions for the supported crypto modules

Key Type	Popup	Sub-popup	Action Description
AES Master Key ECC Master Key DES Master Key Asymmetric Master Key	Generate single key part		Generate one master key part and store it on a TKE smart card or save it to a binary or print file.
	Generate multiple key parts to ...	Smart card Binary file Print file	Run a wizard-like feature to generate a user specified number of master key parts and store them on TKE smart cards or save them to binary or print files. **Note:** You can use the same smart card or switch smart cards between key part generations.
	Load single key part	First Intermediate Last	Load one key part into the appropriate "new" master key register. **Notes:** 1. To load a first part, the "new" master register status must be "empty". 2. To load an intermediate or last part, the "new" master register status must be "part full" (partially full).
	Load all key parts from	Smart card Binary file Print file	Run a wizard-like feature to load an entire "new" master key register. At the beginning of the process, you specify the total number of key parts and have the option of clearing the "new" master key register. **Note:** No new security controls are introduced by this feature. ALL authority and dual control requirements you put in place remain in effect. It takes the same number of people to load an entire key using this procedure as it does loading an entire key one part at a time.
	Clear	New Master Key Register Old Master Key Register	Clear the new or old master key register. The status of the register will be "empty" when the operation is complete.
	Set (Option only shown on Asymmetric MK)		Sets the new asymmetric master key. **Notes:** 1. If you are running HCR7790 or later, you will no longer be able to set the asymmetric master key from the TKE. The set must be done from ICSF. 2. The current ASYM-MK is transferred to the old ASYM-MK register. 3. The new ASYM-MK register is transferred to the current ASYM-MK register. 4. The new ASYM-MK register is reset to zeros.
	Secure key part entry		Enter known key part value to a TKE smart card; see Appendix A, “Secure Key Part Entry,” on page 307.

Table 30. Key types and actions for the supported crypto modules (continued)

Key Type	Popup	Sub-popup	Action Description
DES or AES Operational Keys	Generate single key part		Generate one key part and store it on a TKE smart card or save it to a binary or print file.
	Generate multiple key parts to ...	Smart card Binary file Print file	Run a wizard-like feature to generate a user specified number of key parts and store them on TKE smart cards or save them to binary or print files. **Note:** You can use the same smart card or switch smart cards between key part generations.
	Load single key part	First First (minimum of 2 parts) First (minimum of 3 parts) Add part Complete **Note:** First (minimum of x parts)" options only shown on Operational Keys - AES key types EXPORTER, IMPORTER, and CIPHER.	Load one key part into a key part register. **Notes:** 1. The minimum number of parts for the **load single key part –> first** is 2. 2. When the first key part is loaded, you must enter a unique register label. 3. You can only add parts to an existing register label. 4. You can only complete a register when it has meet its minimum parts requirement.
	Load to Key Storage **Note:** Options only shown on DES operational key types IMPORTER or IMP-PKA.	First Intermediate Last	Load a key part to the TKE workstations DES key storage.
	Load all key parts from	Smart card Binary file Print file	Run a wizard-like feature to load an entire operational key register. At the beginning of the process, you specify the total number of key parts and have the option of clearing the "new" master key register. **Note:** No new security controls are introduced by this feature. ALL authority and dual control requirements you put in place remain in effect. It takes the same number of people to load an entire key using this procedure as it does loading an entire key one part at a time.
	View		View key part register information
	Clear		Clear (reset) the operational key part register.
	Secure key part entry		Enter known key part value to a TKE smart card; see Appendix A, “Secure Key Part Entry,” on page 307.

Table 30. Key types and actions for the supported crypto modules (continued)

Key Type	Popup	Sub-popup	Action Description
RSA Keys	Generate single key part		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 the host data set

Master Keys - AES, ECC, DES, or Asymmetric

Generate single key part: The generate action for a new AES, ECC, 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 single key part**, a Select Target window opens, enabling you to specify the target.

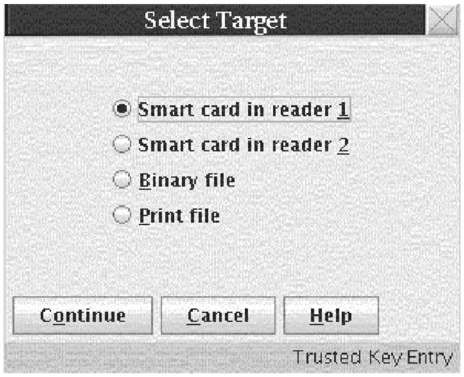


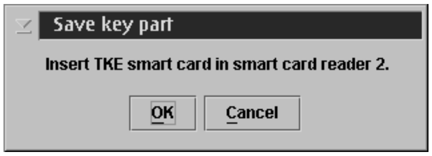
Figure 102. Select Target

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 or the Smart Card Utility Program under Trusted Key Entry Applications. See “Display smart card details” on page 277 or “Display smart card information” on page 287.

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.

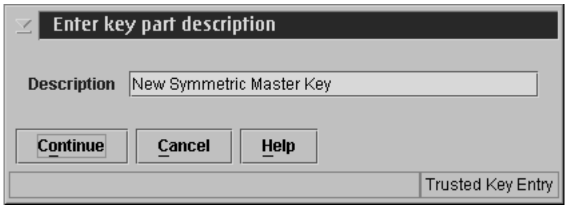

Save key part

Insert TKE smart card in smart card reader 2.

Figure 103. 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.

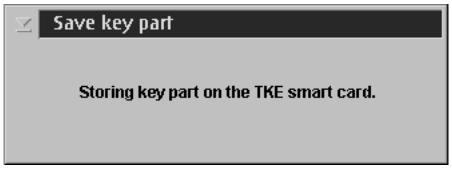
A dialog is displayed prompting you for a key part description.


Enter key part description

Description: New Symmetric Master Key

Figure 104. Enter key part description

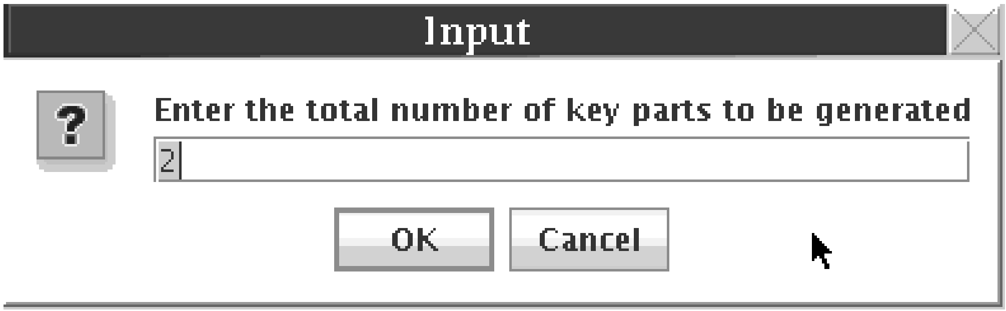
Enter a description for the key part, and press the **Continue** command button.


Save key part

Storing key part on the TKE smart card.

Figure 105. Save key part

Generate Multiple Key Parts to: If you are going to create more than one key part at a time, use the “generate multiple key part to” feature. When this feature is started, you are asked to provide the total number of key parts you want to create. The minimum number of key parts that can be specified is 2.


Input

Enter the total number of key parts to be generated

2

Figure 106. Enter number of keys to be generated

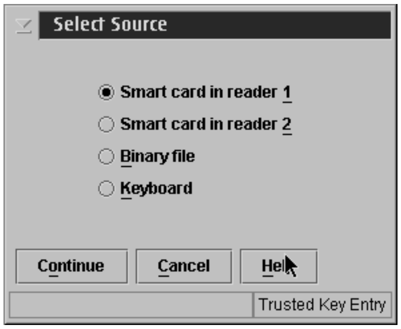
The feature will walk you through the process of creating the requested number of key parts.

Load single key part: 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 binary file, or a 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 single key part**, 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.



Select Source

● Smart card in reader 1
○ Smart card in reader 2
○ Binary file
○ Keyboard

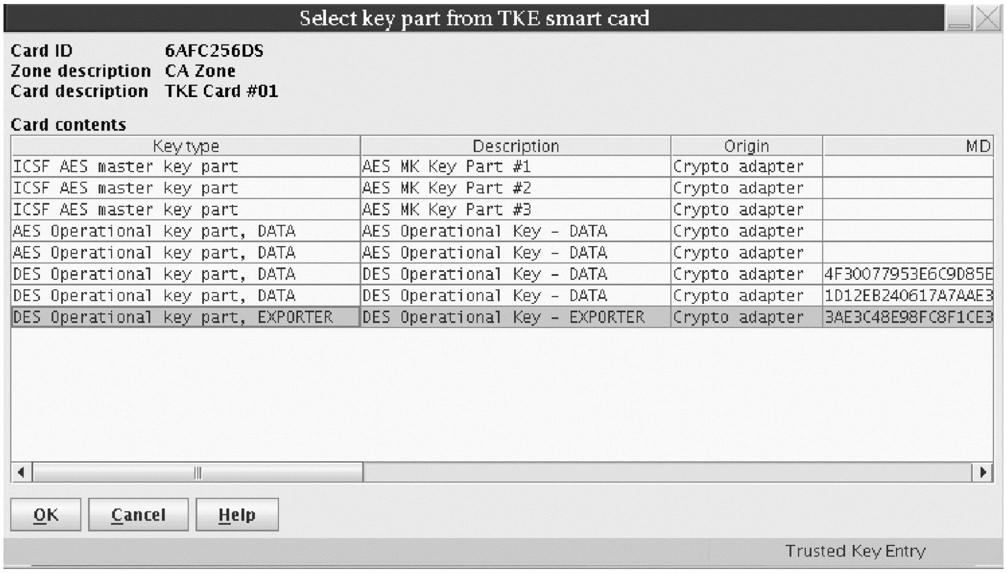
Figure 107. Select key source - smart card

   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 or the Smart Card Utility Program under Trusted Key Entry Applications. See "Display smart card details" on page 277 or "Display smart card information" on page 287.

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



Select key part from TKE smart card

Card ID 6AFC256DS
Zone description CA Zone
Card description TKE Card #01

Card contents

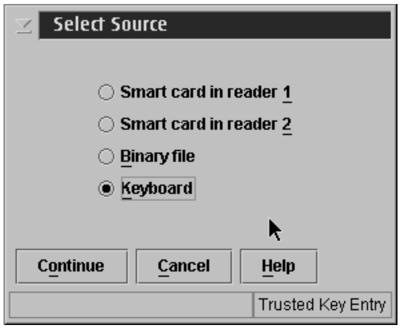
Key type	Description	Origin	MD
ICSF AES master key part	AES MK Key Part #1	Crypto adapter	
ICSF AES master key part	AES MK Key Part #2	Crypto adapter	
ICSF AES master key part	AES MK Key Part #3	Crypto adapter	
AES Operational key part, DATA	AES Operational Key - DATA	Crypto adapter	
AES Operational key part, DATA	AES Operational Key - DATA	Crypto adapter	
DES Operational key part, DATA	DES Operational Key - DATA	Crypto adapter	4F30077953E6C9D85E
DES Operational key part, DATA	DES Operational Key - DATA	Crypto adapter	1D12EB240617A7AAE3
DES Operational key part, EXPORTER	DES Operational Key - EXPORTER	Crypto adapter	3AE3C48E98FC8F1CE3

Figure 108. 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.

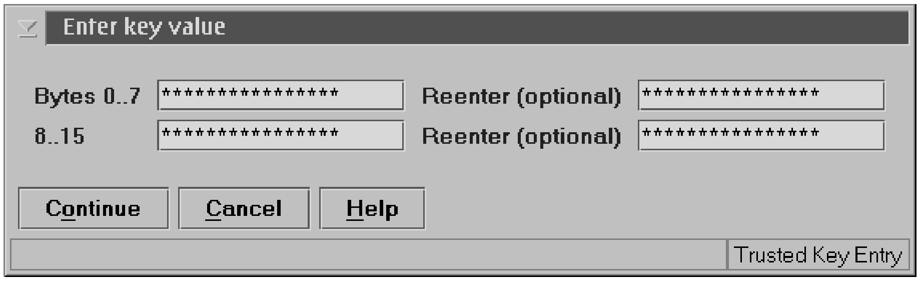


Select Source

○ Smart card in reader 1
○ Smart card in reader 2
○ Binary file
● Keyboard

Figure 109. 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.



Bytes 0..7 ***************** Reenter (optional) *****************
8..15 ***************** Reenter (optional) *****************

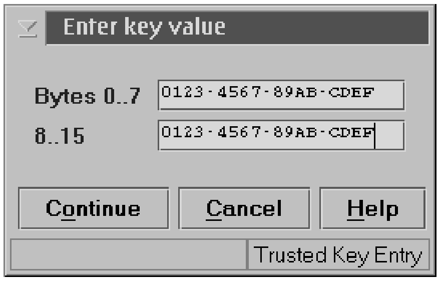
Figure 110. Enter Key Value - Blind Key Entry

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 138.

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

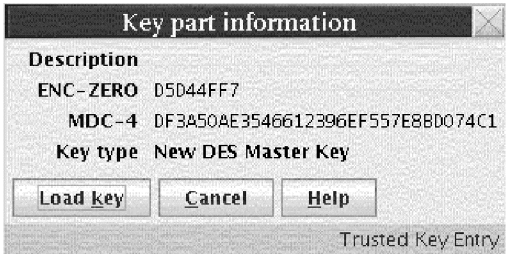
Enter the key values and press the **Continue** command button.



Bytes 0..7 0123-4567-89AB-CDEF
8..15 0123-4567-89AB-CDEF

Figure 111. 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.

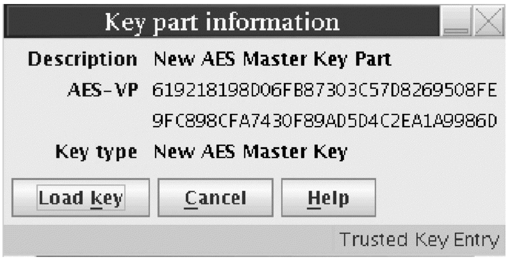


Description
ENC-ZERO D5D44FF7
MDC-4 DF3A50AE3546612396EF557E8BD074C1
Key type New DES Master Key

Figure 112. 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.



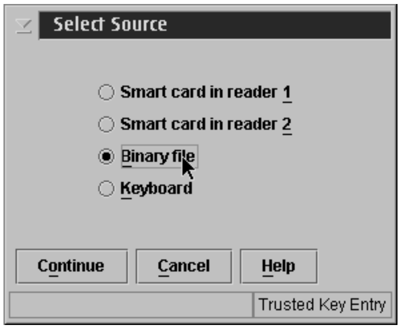
Description New AES Master Key Part
AES-VP 619218198D06FB87303C57D8269508FE
9FC898CFA7430F89AD5D4C2EA1A9986D
Key type New AES Master Key

Figure 113. Key Part Information Window

Press **Load key**.

Input from Binary File:

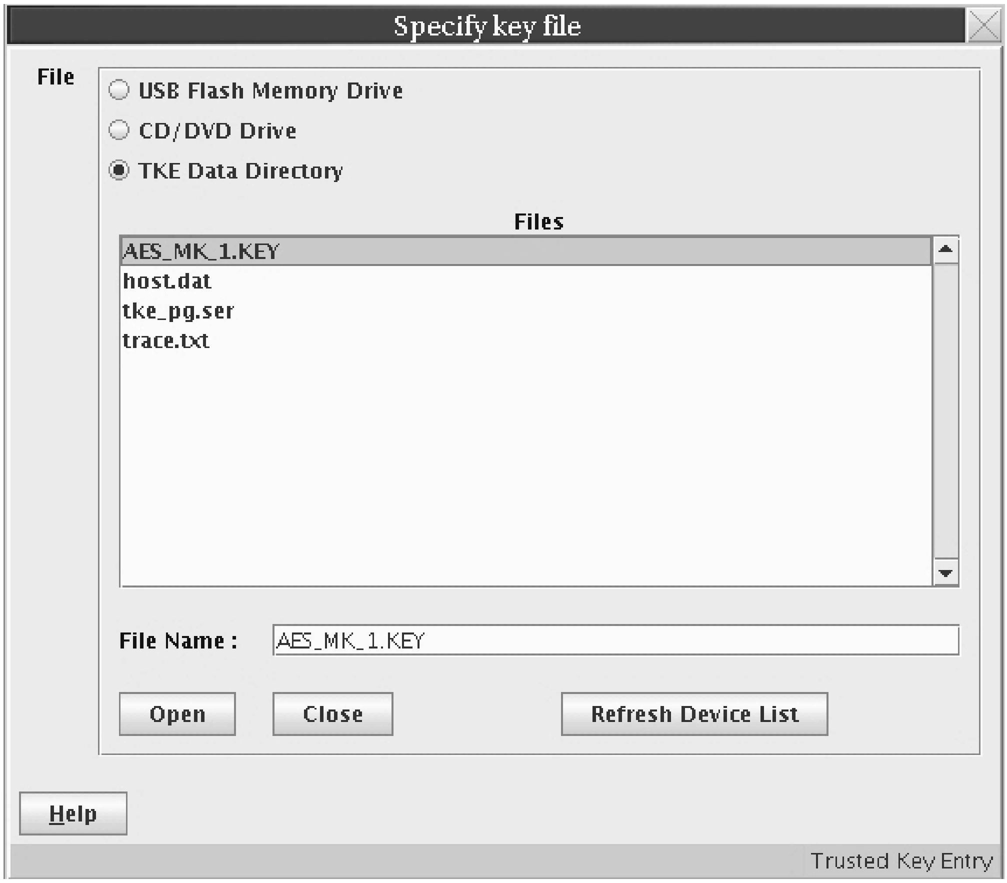
A dialog box is displayed for selecting the input source. Select "Binary file" and press the **Continue** command button.



○ Smart card in reader 1
○ Smart card in reader 2
● Binary file
○ Keyboard

Figure 114. Select key source - binary file

The Specify key file window is displayed.



File

○ USB Flash Memory Drive
○ CD/DVD Drive
● TKE Data Directory

Files

AES_MK_1.KEY
host.dat
tke_pg.ser
trace.txt

File Name : AES_MK_1.KEY

Figure 115. Specify Key File

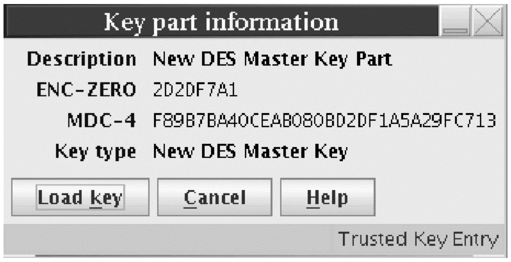
Using the Specify key file window, specify the file location (Floppy, CD/DVD Drive, USB flash memory drive, or TKE Data Directory) and file name. Select **Open**.

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 AES and ECC Master Keys, 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 CD/DVD, you must deactivate the CD/DVD drive before removing the disc. If the disc is removed prior to deactivating the drive, data could be lost or corrupted. For details on deactivating media see “TKE Media Manager” on page 334.
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.



Key part information

Description	New DES Master Key Part
ENC-ZERO	2D2DF7A1
MDC-4	F89B7BA40CEAB080BD2DF1A5A29FC713
Key type	New DES Master Key

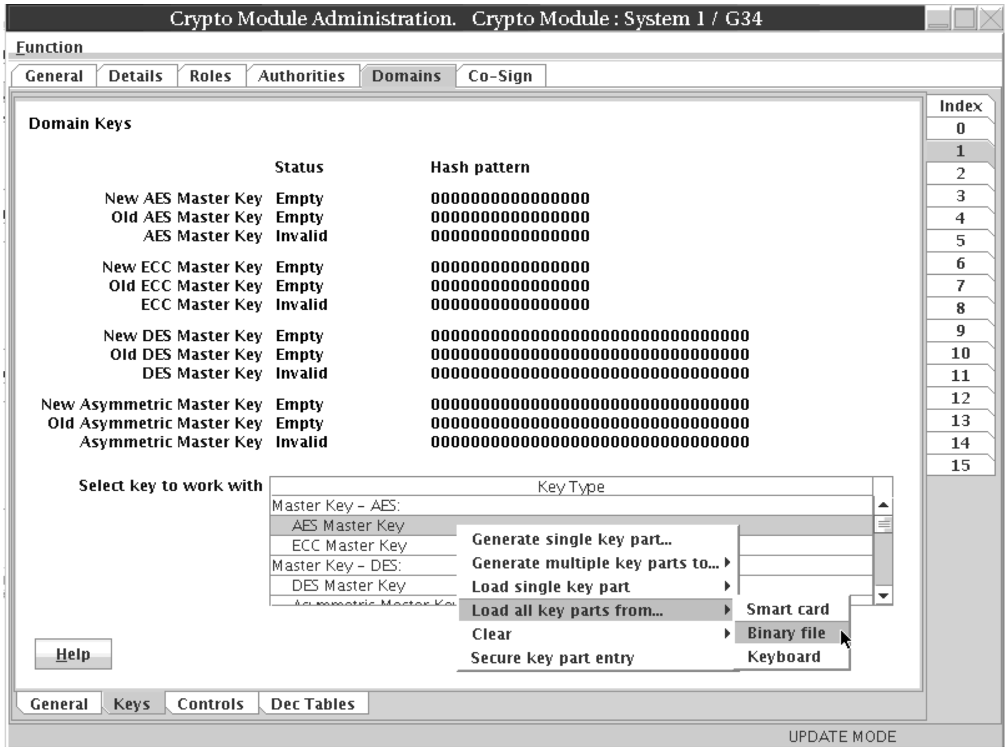
Figure 116. Key Part Information Window

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

Load All Key Parts From: If you have all of the people and key material necessary to load an entire key, you can use this wizard-like feature to walk you through the process of loading an entire key. Below is an example for loading a key from binary files:

To start the load process:

1. Right click on the appropriate key type in the "Select key to work with" area to display a pop-up menu. In this example we select **Load all key parts from... –> Binary file** from the pop-up menu. Options for loading all key parts from a smart card or keyboard input are also available.



Crypto Module Administration. Crypto Module : System 1 / G34

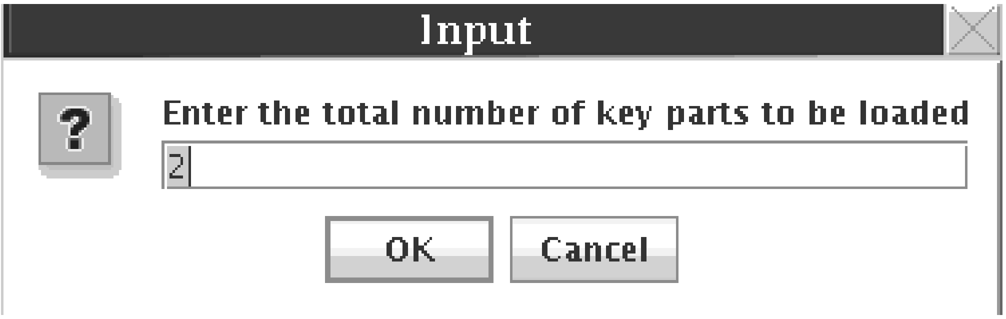
Domain Keys

	Status	Hash pattern
New AES Master Key	Empty	0000000000000000
Old AES Master Key	Empty	0000000000000000
AES Master Key	Invalid	0000000000000000
New ECC Master Key	Empty	0000000000000000
Old ECC Master Key	Empty	0000000000000000
ECC Master Key	Invalid	0000000000000000
New DES Master Key	Empty	00000000000000000000000000000000
Old DES Master Key	Empty	00000000000000000000000000000000
DES Master Key	Invalid	00000000000000000000000000000000
New Asymmetric Master Key	Empty	00000000000000000000000000000000
Old Asymmetric Master Key	Empty	00000000000000000000000000000000
Asymmetric Master Key	Invalid	00000000000000000000000000000000

Figure 117. Load all key parts from...

2. A dialog box is displayed prompting you for the number of key parts to be loaded. In the text entry field of this dialog, enter the number of key parts to be loaded and click the OK command button. In this example, there are two key parts.

Note: The minimum number of key parts that can be specified is 2.



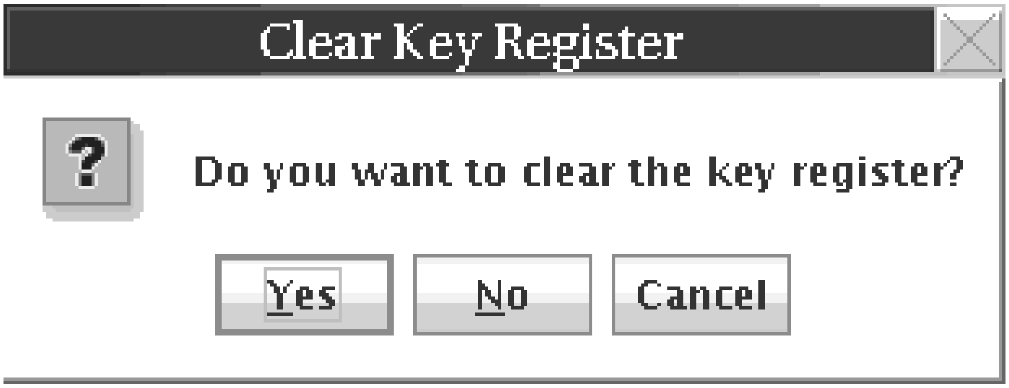
Input

Enter the total number of key parts to be loaded

2

Figure 118. Enter the total number of key parts

3. A dialog box is displayed asking if you want to clear the key register. In this example, we click the **Yes** command button to clear the key register before loading the key parts from the binary file.



Clear Key Register

Do you want to clear the key register?

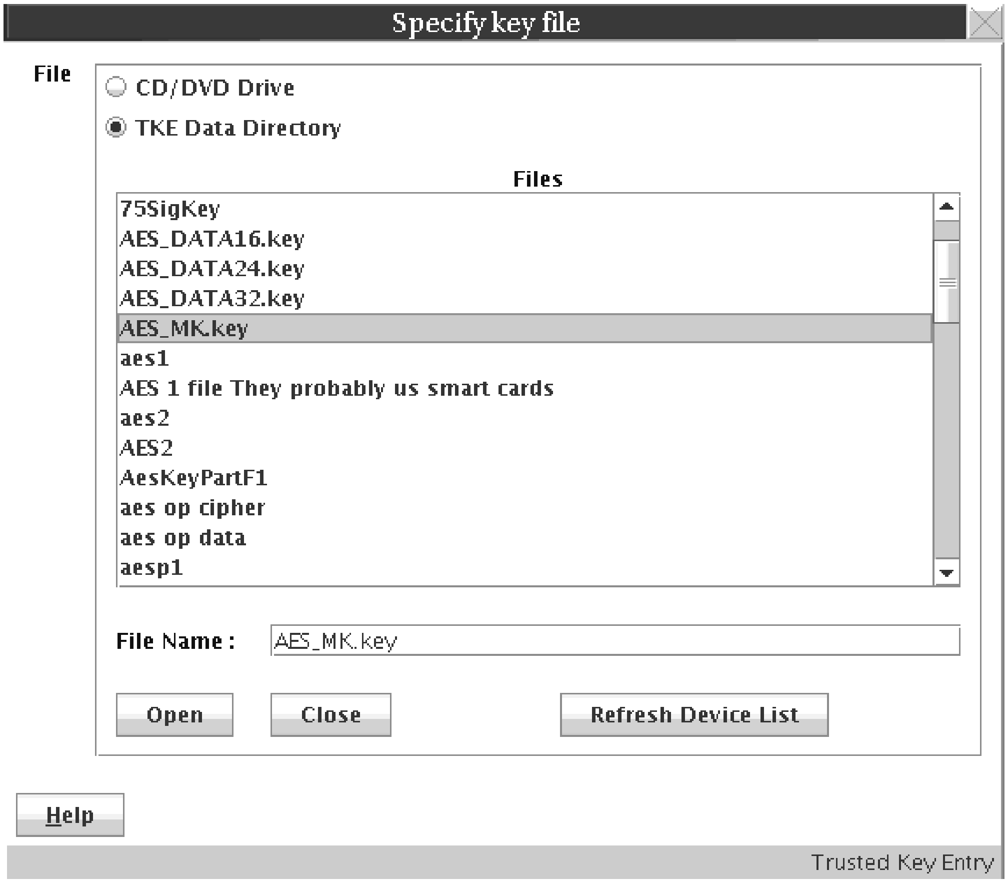
Figure 119. Do you want to clear the key register?

If you choose to clear the key register, a command is sent to the Host Cryptographic Module. This requires an authority signature key. When an authority key is needed and no key is currently loaded (or the current key is associated with an Authority that does not have enough authority to execute the command), a dialog will display asking if you want to load a signature key. Follow your normal process for loading a key.

Note: When your key loading process requires you to use different authority signature keys at different steps in the process, you will be asked for new signature keys at the proper times.

When the register is cleared, a message box displays a "Command was executed successfully" message. Press the **Close** button on this message box to continue the process.

4. A message box reading "Select first key part" is displayed. Press the **OK** button on this message box to continue to select the first key part.
5. In this example, we are loading key parts from binary files, so a "Specify key file" dialog box is displayed. Files can be selected from a CD/DVD drive, USB Flash Memory Drive, or from the TKE Data Directory. Select the appropriate file for the first key part, and press the **Open** command button.


Specify key file

File

○ CD/DVD Drive

● TKE Data Directory

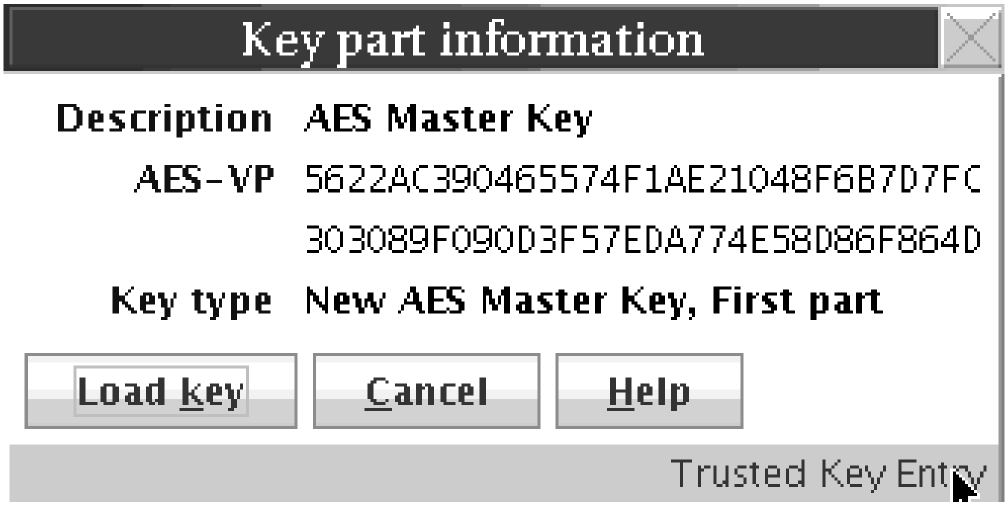
Files

75SigKey
AES_DATA16.key
AES_DATA24.key
AES_DATA32.key
AES_MK.key
aes1
AES 1 file They probably us smart cards
aes2
AES2
AesKeyPartF1
aes op cipher
aes op data
aesp1

File Name : AES_MK.key

Figure 120. Specify key file (first key part)

6. A dialog box displays the key part information contained in the binary file. To load the key material, press the **Load key** command button.


Key part information

Description AES Master Key

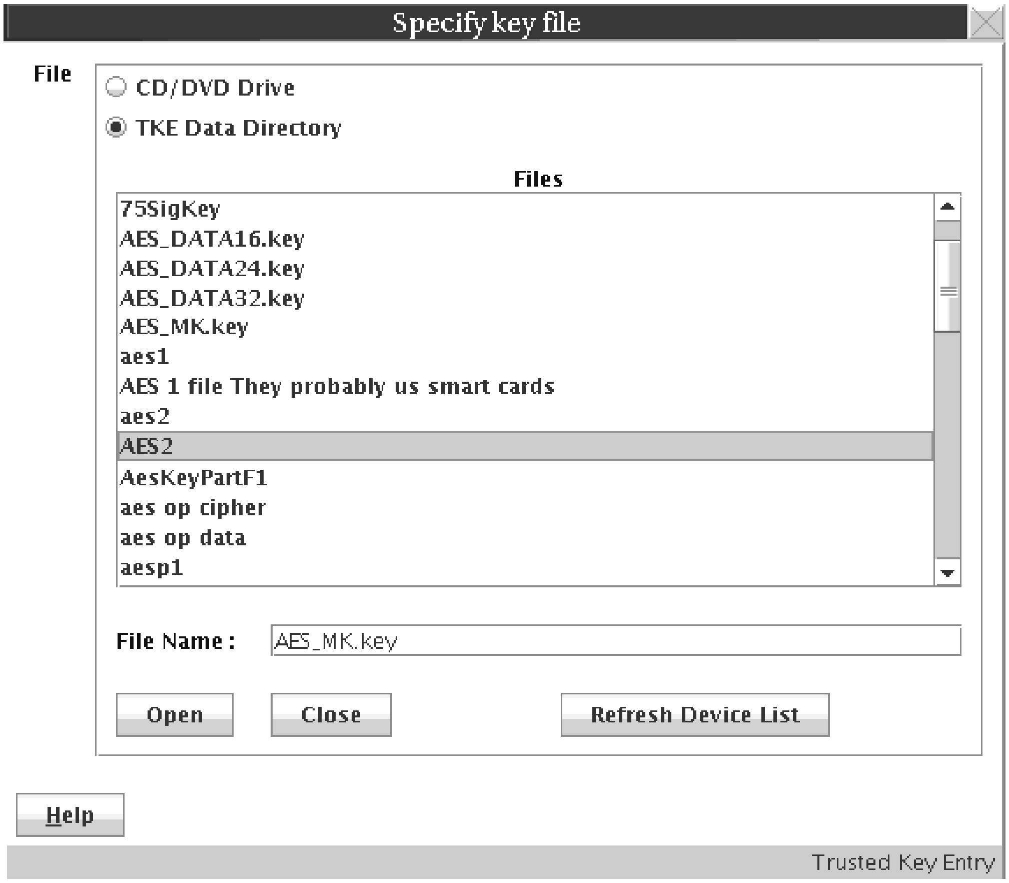
AES-VP 5622AC390465574F1AE21048F6B7D7FC
303089F090D3F57EDA774E58D86F864D

Key type New AES Master Key, First part

Figure 121. Key part information (first key part)

When load of the key part completes, a message box displays a "Command was executed successfully" message. Press the **Close** button on this message box to continue the process.

7. In our example, we are loading two key parts. A message box reading "Select last key part" is displayed. Press the **OK** button on this message box to continue to select this key part.
8. A "Specify key file" dialog box is displayed. Select the appropriate file for this key part, and press the **Open** command button.

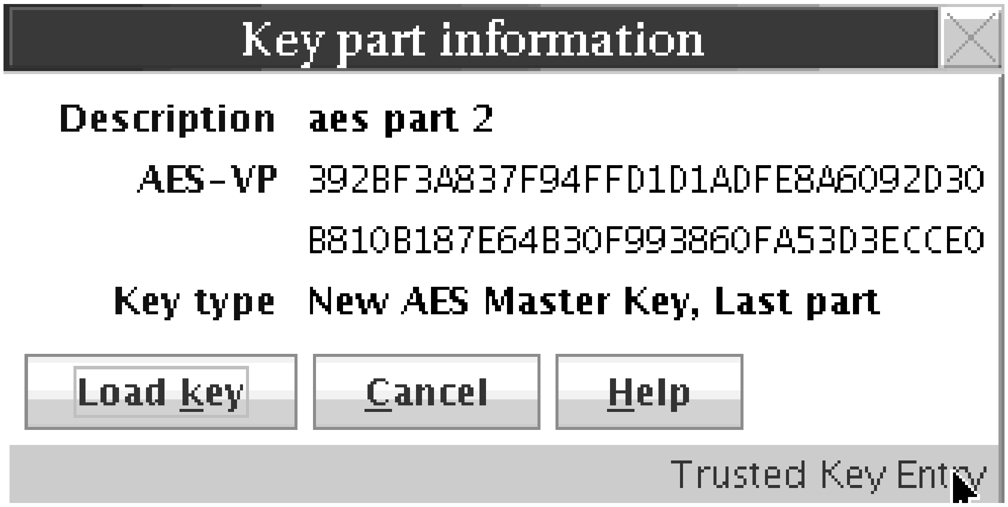


○ CD/DVD Drive
● TKE Data Directory

File Name : AES_MK.key

Figure 122. Specify key file (second key part)

9. A dialog box displays the key part information contained in the binary file. To load the key material, press the **Load key** command button.



Description aes part 2

AES-VP 392BF3A837F94FFD1D1ADFE8A6092D30
B810B187E64B30F993860FA53D3ECCE0

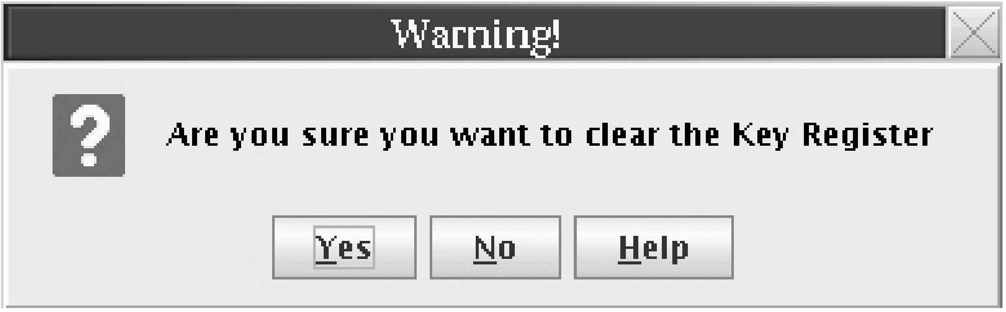
Key type New AES Master Key, Last part

Figure 123. Key part information (second key part)

When load of the key part completes, a message box displays a "Command was executed successfully" message. Press the **Close** button on this message box. The process is complete.

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.

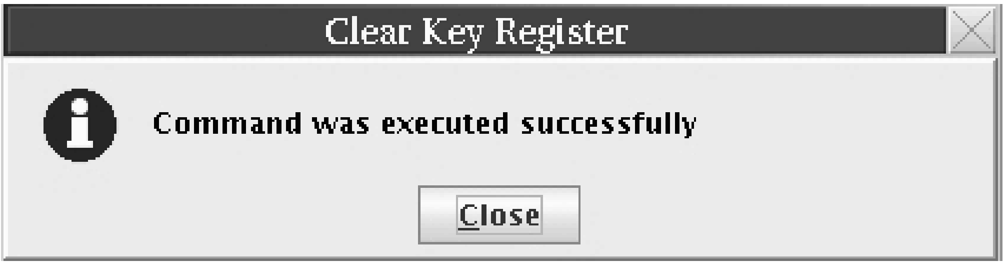


Are you sure you want to clear the Key Register

Figure 124. 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.



Clear Key Register

Command was executed successfully

Figure 125. Clear new or old new master key successful message

Set (Asymmetric Master Key only): If you select SET for an Asymmetric 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 Asymmetric master key. That is, the current Asymmetric master key is transferred to the old Asymmetric master key register and the new Asymmetric master key register is transferred to the current Asymmetric master key register. The new Asymmetric master key 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 233) or using an option on Key Generator Utility Processes (KGUP) Job Control Language (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.

An AES EXPORTER, IMPORTER or CIPHER key part register can be in one of the following states:

- Incomplete, need at least two more parts - Load to key part register (First, minimum of 3 parts) has completed successfully
- Incomplete, need at least one more part - Load to key part register (First, minimum of 2 parts or Add part) 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

A DES operational key or AES DATA 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 single key part
- Load all key parts from...
- View
- Clear

AES EXPORTER, IMPORTER, and CIPHER keys have the following "Load single key part" tasks:

- First (minimum of 2 parts)
- First (minimum of 3 parts)
- Add part
- Complete

Tasks for "Load all key parts from..." are as follows:

- Smart card
- Binary file
- Keyboard

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, AES, and ECC master keys and for DES operational keys, AES operational keys, and AES KEK and CIPHER keys.

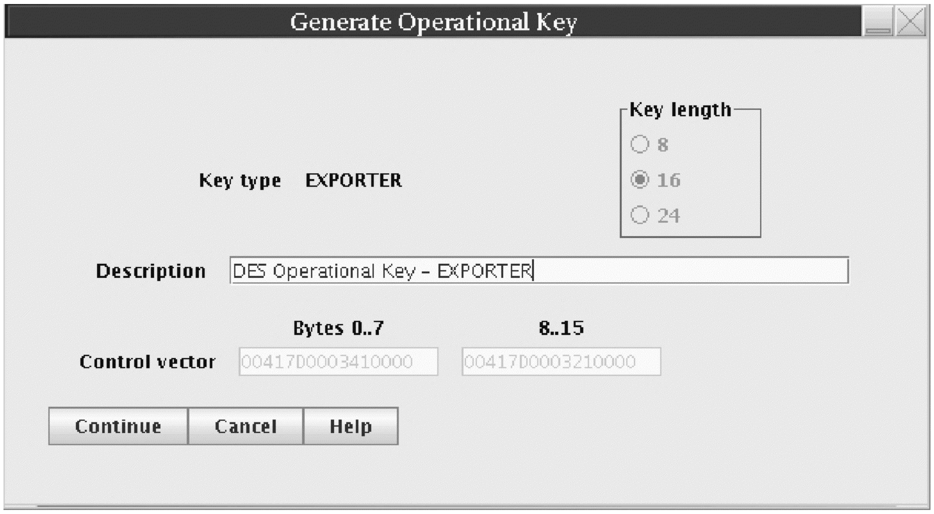
The host crypto module supports all ICSF operational key types. A `USER DEFINED` key type is also available, and allows the user to specify his or her own control vector for DES keys. This `USER DEFINED` control vector must still conform to the rules of a valid control vector. For more details on control vectors, see Appendix C in the *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

Instead of a control vector, AES EXPORTER, IMPORTER, and CIPHER keys have key attributes associated with them that specify the key usage and key management attributes of the key. The key attributes are specified either at the time a key part is generated or when the first key part is loaded to the key part register on the host crypto module. For more information about key attributes, see Appendix B 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 binary file or a print 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.



Generate Operational Key

Key type EXPORTER

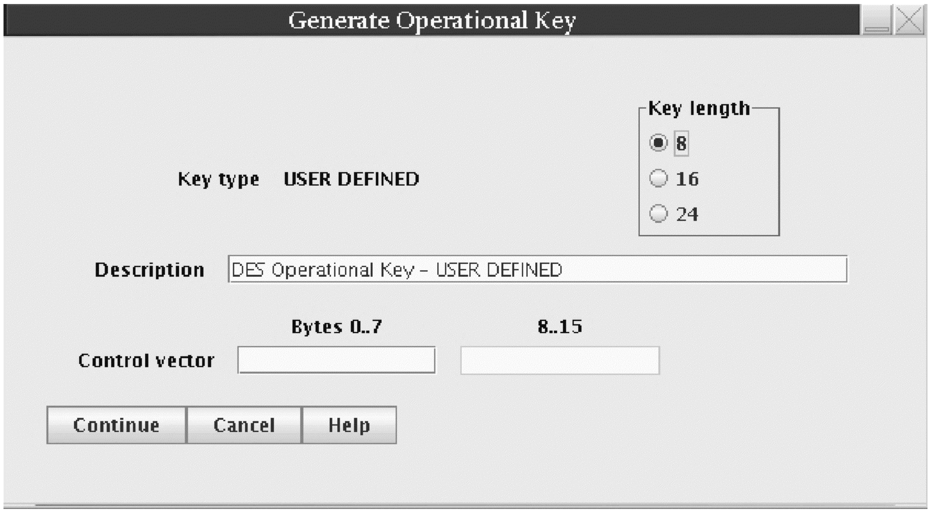
Key length: ○ 8 ● 16 ○ 24

Description: DES Operational Key – EXPORTER

Control vector: Bytes 0..7 00417D0003410000 8..15 00417D0003210000

Figure 126. 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.



Generate Operational Key

Key type USER DEFINED

Key length: ● 8 ○ 16 ○ 24

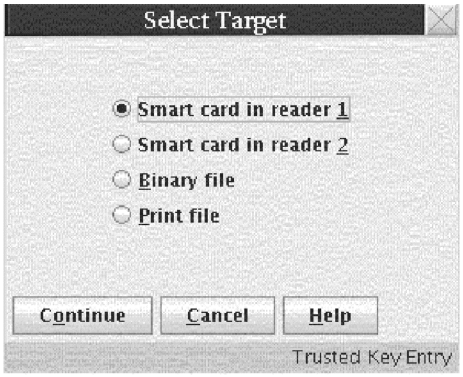
Description: DES Operational Key – USER DEFINED

Control vector: Bytes 0..7 8..15

Figure 127. Generate Operational Key - USER DEFINED

When Generate is selected for an AES EXPORTER, IMPORTER, or CIPHER key, the Generate Operational Key window is displayed showing the key type, key length, description, and key attributes fields. The key attributes fields indicate whether the key attributes contain default or custom values. The key attributes may be changed by pressing the **Change key attributes** button.

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



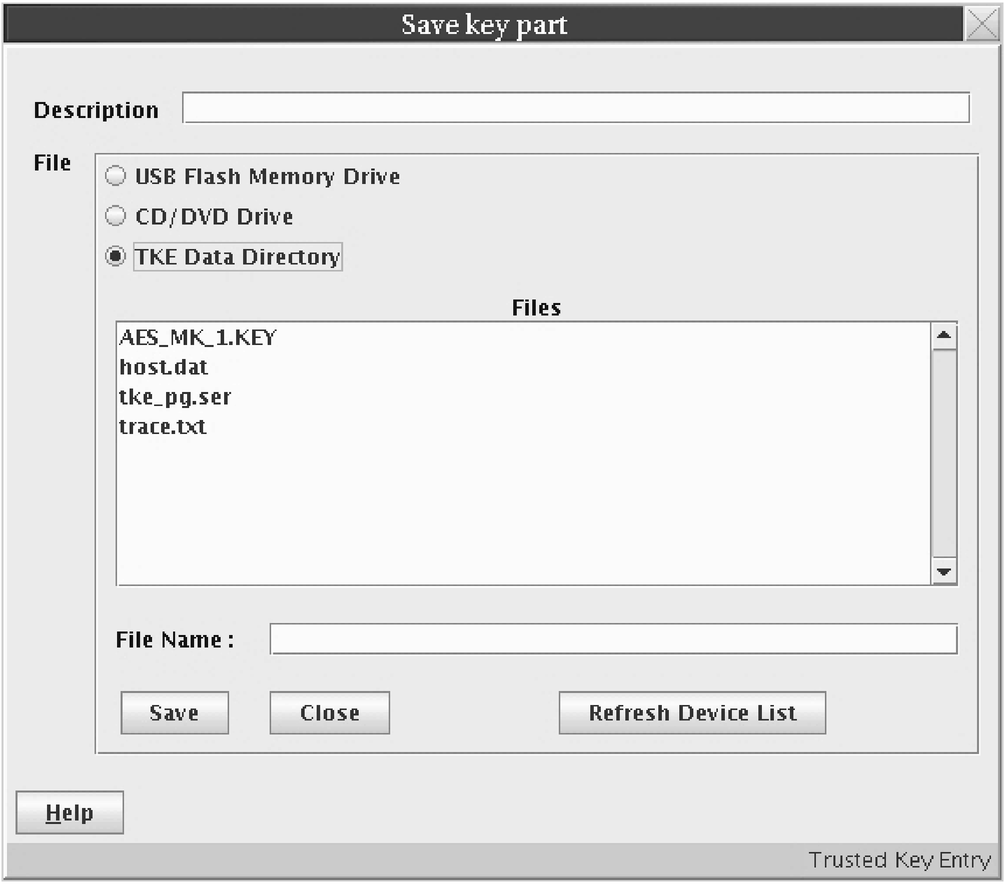
Select Target

● Smart card in reader 1
○ Smart card in reader 2
○ Binary file
○ Print file

Figure 128. 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.



Save key part

Description

File

○ USB Flash Memory Drive

○ CD/DVD Drive

● TKE Data Directory

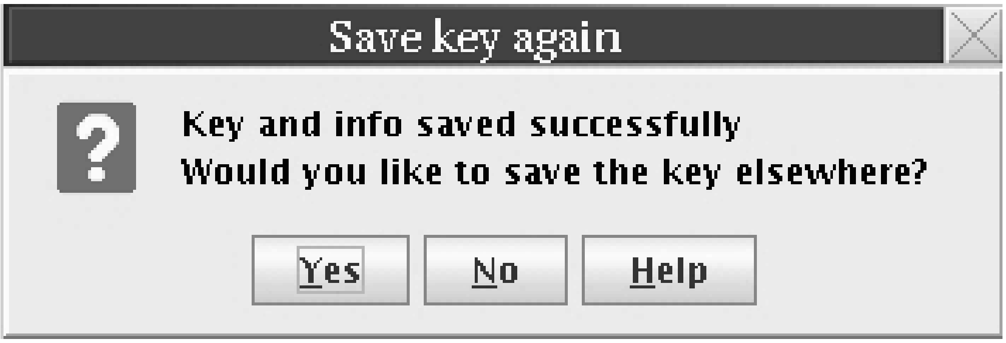
Files

AES_MK_1.KEY
host.dat
tke_pg.ser
trace.txt

File Name :

Figure 129. 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.



Save key again

Key and info saved successfully
Would you like to save the key elsewhere?

Figure 130. 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 334.
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 or the Smart Card Utility Program under Trusted Key Entry Applications. See “Display smart card details” on page 277, “Display smart card information” on page 287 or “View current zone” on page 306.

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

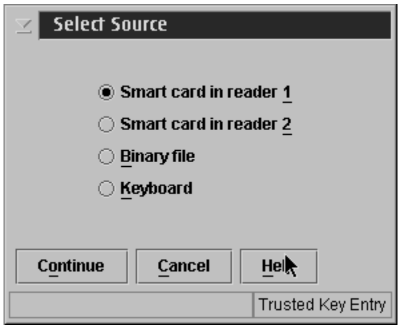
1. When prompted, insert TKE smart card into Smart Card Reader 2
2. Press OK
3. Enter the PIN on the smart card reader PIN pad
4. A pop up message will indicate that the key part was successfully stored on the TKE smart card.

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 137.

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 binary 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.

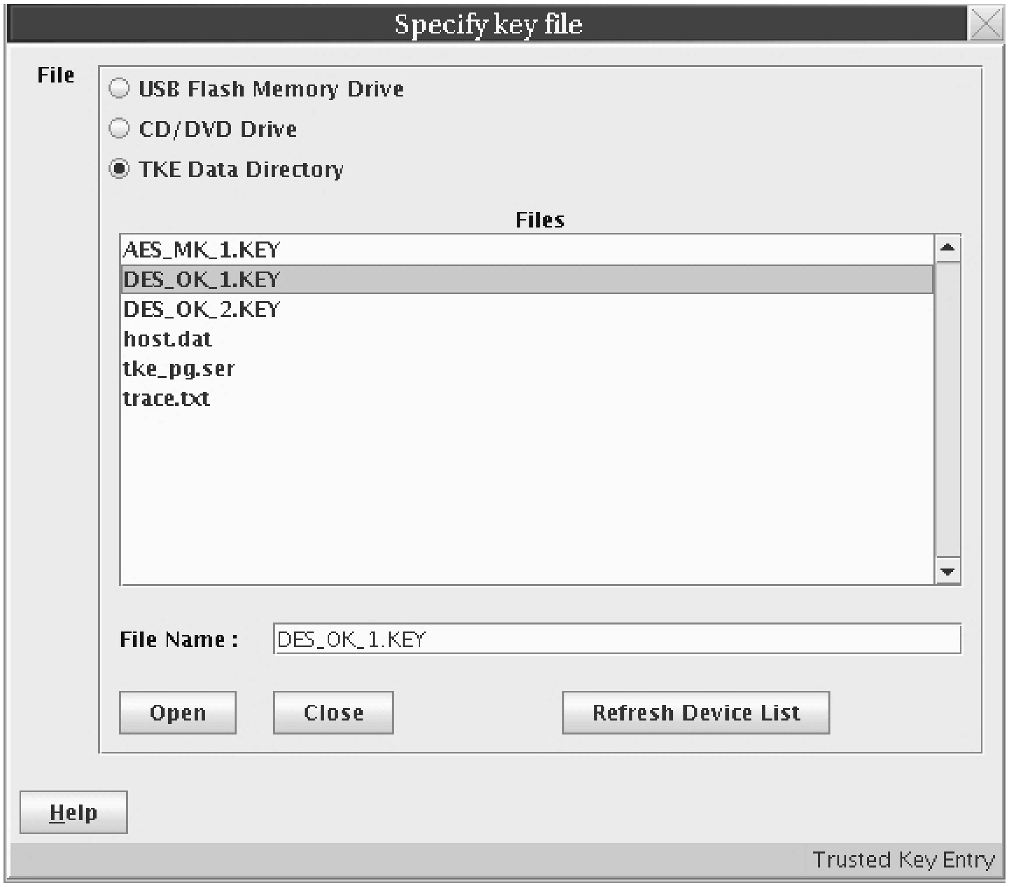
When you select Load to Key Part Register First, the Select Source window is displayed, prompting you to select the source for the key part.



● Smart card in reader 1
○ Smart card in reader 2
○ Binary file
○ Keyboard

Figure 131. 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.



File

○ USB Flash Memory Drive

○ CD/DVD Drive

● TKE Data Directory

Files

AES_MK_1.KEY
DES_OK_1.KEY
DES_OK_2.KEY
host.dat
tke_pg.ser
trace.txt

File Name : DES_OK_1.KEY

Figure 132. Specify key file for binary file source

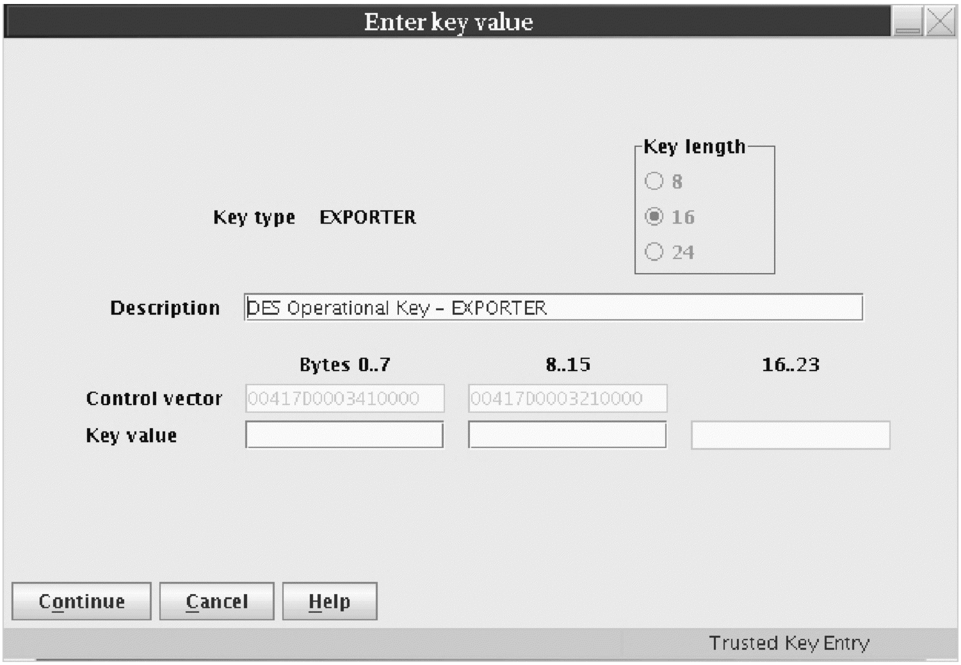
If the binary file contains a key type that does not match the key type selected for loading, a warning is displayed asking for confirmation to continue. If continue is chosen, TKE will load the key part as the key type defined in the binary file and not the key type originally selected by the user.

Warnings:

1. If the file is loaded from a floppy or CD/DVD, you must deactivate the drive before removing the diskette. If it is removed prior to deactivating the drive, data could be lost or corrupted. For details on deactivating media see “TKE Media Manager” on page 334.
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" fields. 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.



Key type EXPORTER

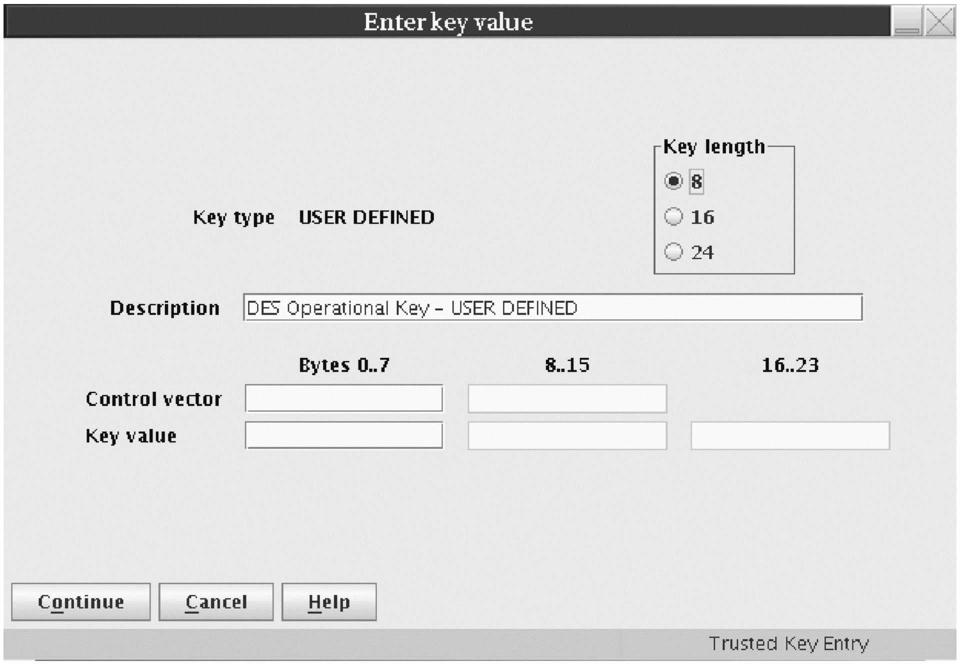
Key length
○ 8
● 16
○ 24

Description DES Operational Key – EXPORTER

	Bytes 0..7	8..15	16..23
Control vector	00417D0003410000	00417D0003210000	
Key value			

Figure 133. 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*.



Enter key value

Key type USER DEFINED

Key length
● 8
○ 16
○ 24

Description: DES Operational Key – USER DEFINED

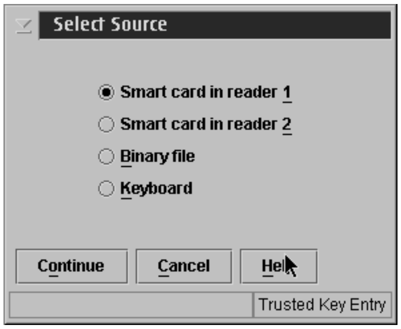
	Bytes 0..7	8..15	16..23
Control vector			
Key value			

Figure 134. Enter key value - keyboard source for USER DEFINED key type

When the key type is AES EXPORTER, IMPORTER, or CIPHER, the Key value fields can be updated and the **Change key attributes** button can be pressed to modify the key attributes values.

If TKE smart card is selected:

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



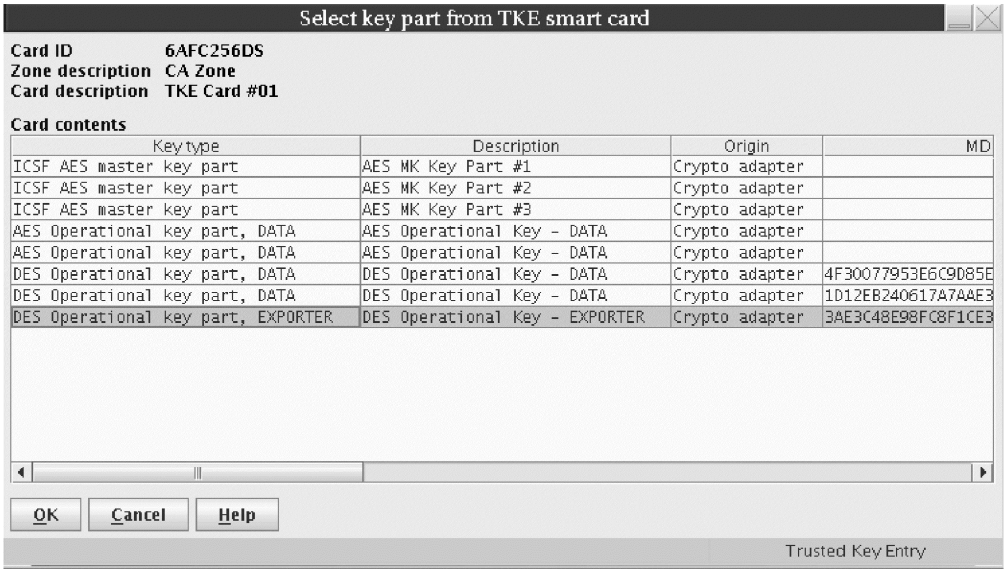
Select Source

● Smart card in reader 1
○ Smart card in reader 2
○ Binary file
○ Keyboard

Figure 135. 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.



Card ID 6AFC256DS
Zone description CA Zone
Card description TKE Card #01

Card contents

Key type	Description	Origin	MD
ICSF AES master key part	AES MK Key Part #1	Crypto adapter	
ICSF AES master key part	AES MK Key Part #2	Crypto adapter	
ICSF AES master key part	AES MK Key Part #3	Crypto adapter	
AES Operational key part, DATA	AES Operational Key - DATA	Crypto adapter	
AES Operational key part, DATA	AES Operational Key - DATA	Crypto adapter	
DES Operational key part, DATA	DES Operational Key - DATA	Crypto adapter	4F30077953E6C9D85E
DES Operational key part, DATA	DES Operational Key - DATA	Crypto adapter	1D12EB240617A7AAE3
DES Operational key part, EXPORTER	DES Operational Key - EXPORTER	Crypto adapter	3AE3C48E98FC8F1CE3

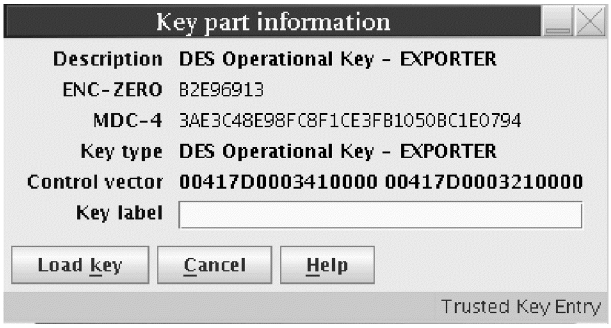
Figure 136. Select key part from TKE smart card

3. Enter a PIN on the smart card reader's 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 DATA operational key, the AES-VP is calculated and displayed along with the description, key type, and control vector on the Key part information window. For an AES EXPORTER, IMPORTER, or CIPHER key, the AES-VP is calculated and displayed along with the description, key type, and key attributes values (default or custom) on the Key part information window. The actual key attributes values may be displayed by pressing the Display key attributes button.

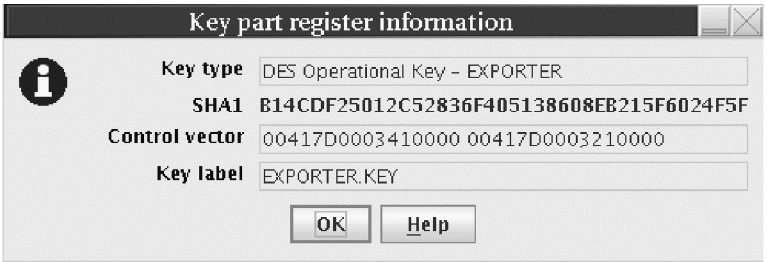
The user must enter a key label for the key part register. When loading additional key parts, the key part register will be selected based on the key label entered. The key label entered must not already exist. If it does, an error will occur. The key label must conform to valid key label names in the 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.



Description DES Operational Key - EXPORTER
ENC-ZERO B2E96913
MDC-4 3AE3C48E98FC8F1CE3FB1050BC1E0794
Key type DES Operational Key - EXPORTER
Control vector 00417D0003410000 00417D0003210000
Key label

Figure 137. 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 will be adjusted to odd.


Key part register information

Key type: DES Operational Key – EXPORTER

SHA1: B14CDF25012C52836F405138608EB215F6024F5F

Control vector: 00417D0003410000 00417D0003210000

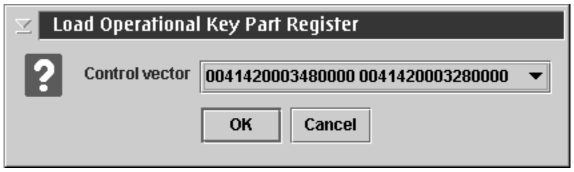
Key label: EXPORTER.KEY

Figure 138. 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.

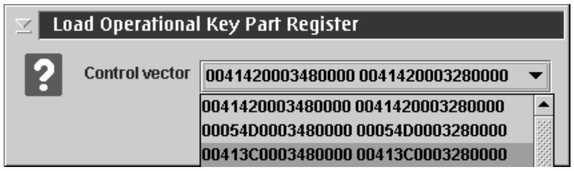
If **Binary file** is selected, the user chooses the file to load. If **Smart card in reader 1** or **Smart card in reader 2** is selected, the user chooses the key part to load. If **Keyboard** is selected and the key type is a predefined operational key, the **Enter Key Value** window is displayed. 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.


Load Operational Key Part Register

Control vector: 0041420003480000 0041420003280000

Figure 139. 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 140 on page 186, 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.



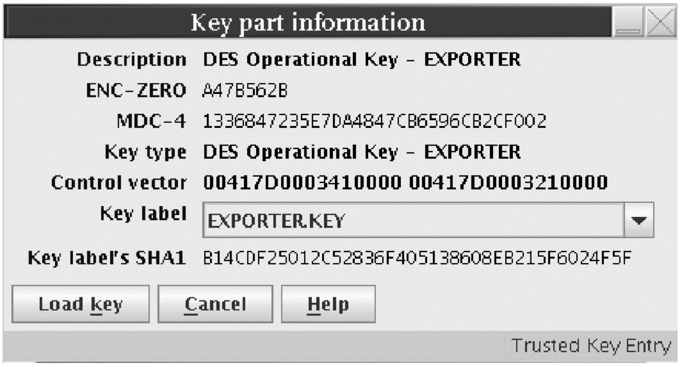
Load Operational Key Part Register

Control vector 0041420003480000 0041420003280000

0041420003480000 0041420003280000
00054D0003480000 00054D0003280000
00413C0003480000 00413C0003280000

Figure 140. 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.

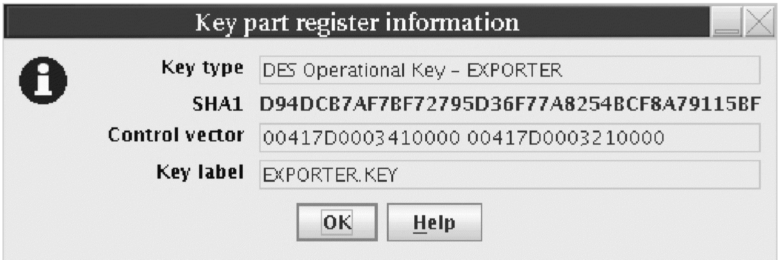


Key part information

Description DES Operational Key – EXPORTER
ENC-ZERO A47B562B
MDC-4 1336847235E7DA4847CB6596CB2CF002
Key type DES Operational Key – EXPORTER
Control vector 00417D0003410000 00417D0003210000
Key label EXPORTER.KEY
Key label's SHA1 B14CDF25012C52836F405138608EB215F6024F5F

Figure 141. 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.



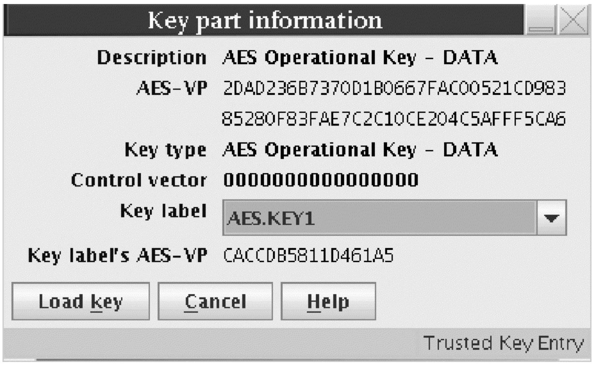
Key part register information

Key type DES Operational Key – EXPORTER
SHA1 D94DCB7AF7BF72795D36F77A8254BCF8A79115BF
Control vector 00417D0003410000 00417D0003210000
Key label EXPORTER.KEY

Figure 142. DES Key part register information - add part with SHA-1 for combined key

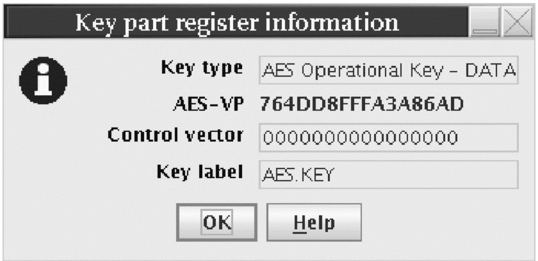
When the **Add Part** is successfully processed, a message is displayed indicating the command was successfully executed.

Equivalent panels for AES DATA keys are shown below:



Description AES Operational Key - DATA
AES-VP 2DAD236B7370D1B0667FAC00521CD983
85280F83FAE7C2C10CE204C5AFFF5CA6
Key type AES Operational Key - DATA
Control vector 0000000000000000
Key label AES.KEY1
Key label's AES-VP CACCDB5811D461A5

Figure 143. AES key part information - add part

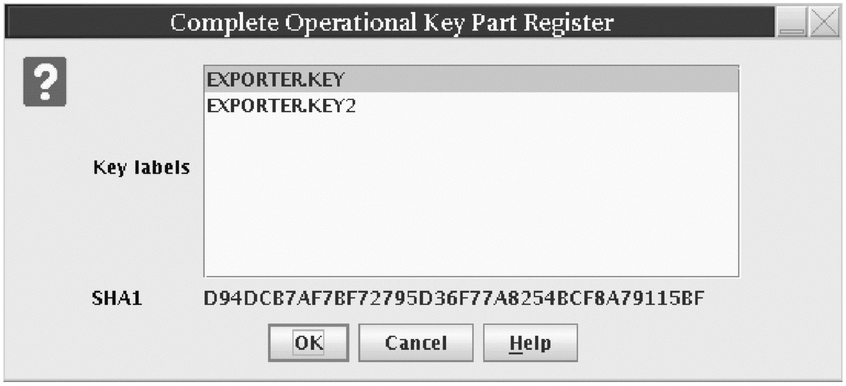


Key type AES Operational Key - DATA
AES-VP 764DD8FFFA3A86AD
Control vector 0000000000000000
Key label AES.KEY

Figure 144. 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.



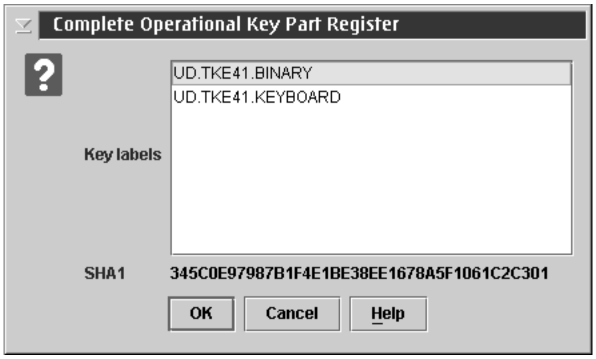
Key labels
EXPORTER.KEY
EXPORTER.KEY2

SHA1 D94DCB7AF7BF72795D36F77A8254BCF8A79115BF

Figure 145. 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 '-'.

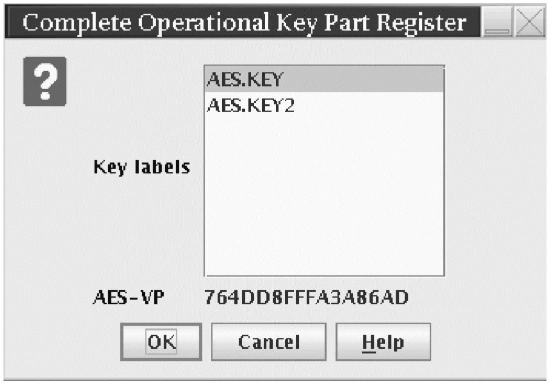
When **Load Key Part Register Complete** is selected for `USER DEFINED` key type, the **Complete Operational Key Part Register** window is displayed with all the domains' key part registers containing DES keys that are in the intermediate state.


Complete Operational Key Part Register

Key labels
UD.TKE41.BINARY
UD.TKE41.KEYBOARD

SHA1 345C0E97987B1F4E1BE38EE1678A5F1061C2C301

Figure 146. Complete DES Operational Key Part Register - USER DEFINED key type

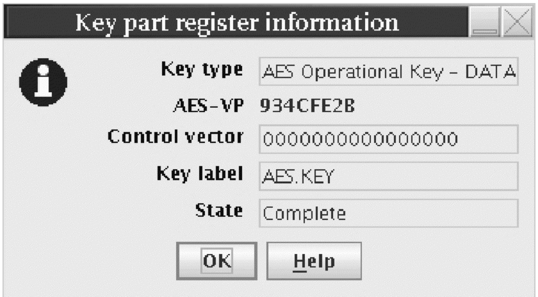

Complete Operational Key Part Register

Key labels
AES.KEY
AES.KEY2

AES-VP 764DD8FFFA3A86AD

Figure 147. Complete AES Operational Key Part Register

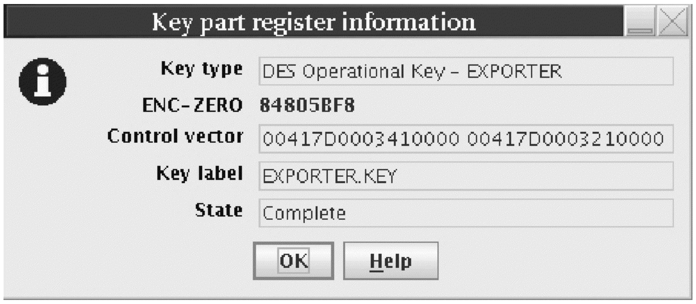
When only one key label is selected for an AES key, the AES-VP of the accumulated key in the key part register is displayed. If more than one key label is selected then the AES-VP field on the window contains a '-'.


Key part register information

Key type: AES Operational Key - DATA
AES-VP: 934CFE2B
Control vector: 0000000000000000
Key label: AES.KEY
State: Complete

Figure 148. 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.



Key part register information

Key type DES Operational Key – EXPORTER

ENC-ZERO 84805BF8

Control vector 00417D0003410000 00417D0003210000

Key label EXPORTER.KEY

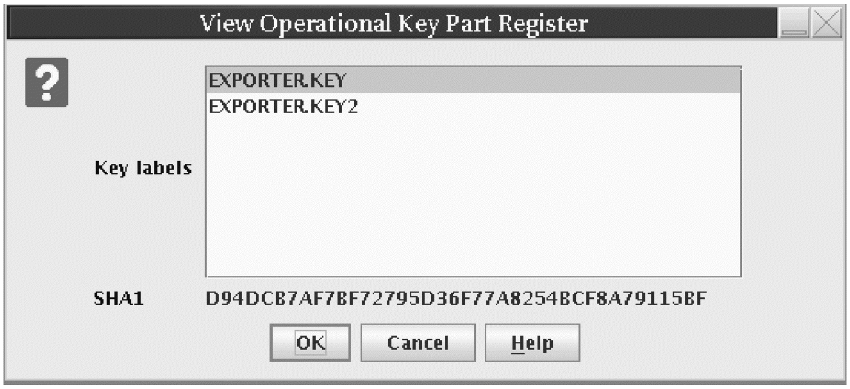
State Complete

Figure 149. 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.



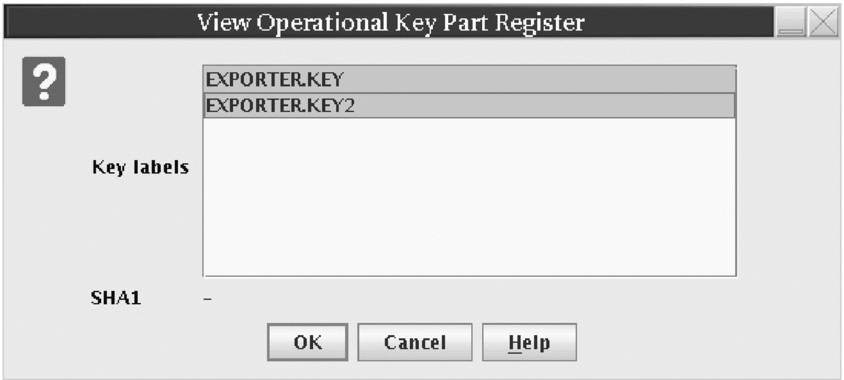
View Operational Key Part Register

Key labels
EXPORTER.KEY
EXPORTER.KEY2

SHA1 D94DCB7AF7BF72795D36F77A8254BCF8A79115BF

Figure 150. 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 '-'.



View Operational Key Part Register

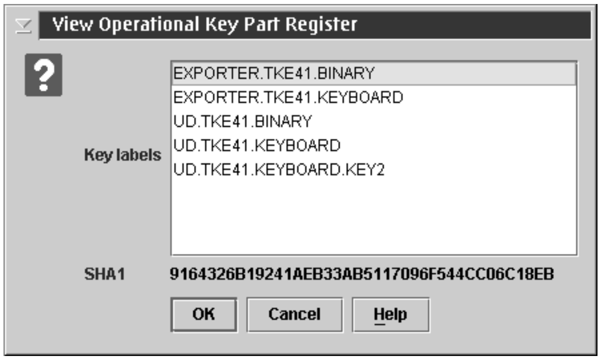
Key labels

EXPORTER.KEY
EXPORTER.KEY2

SHA1 -

Figure 151. 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.



View Operational Key Part Register

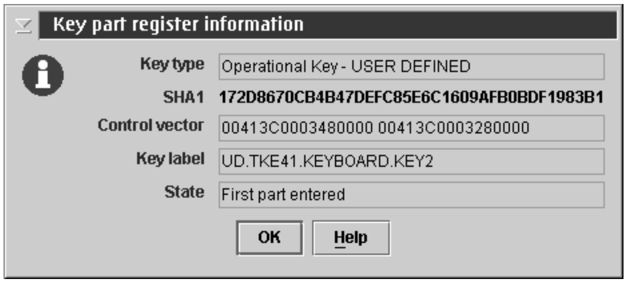
Key labels

EXPORTER.TKE41.BINARY
EXPORTER.TKE41.KEYBOARD
UD.TKE41.BINARY
UD.TKE41.KEYBOARD
UD.TKE41.KEYBOARD.KEY2

SHA1 9164326B19241AEB33AB5117096F544CC06C18EB

Figure 152. 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.

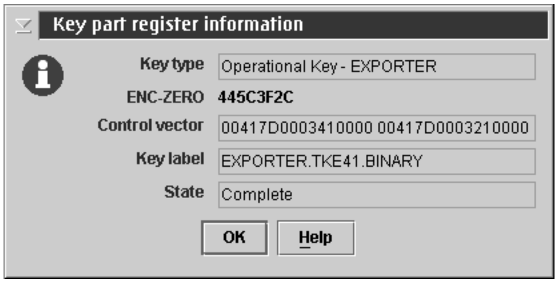


Key part register information

Key type: Operational Key - USER DEFINED
SHA1: 172D8670CB4B47DEFC85E6C1609AFB0BDF1983B1
Control vector: 00413C0003480000 00413C0003280000
Key label: UD.TKE41.KEYBOARD.KEY2
State: First part entered

Figure 153. 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.


Key part register information

Key type Operational Key - EXPORTER

ENC-ZERO 445C3F2C

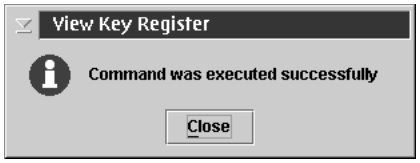
Control vector 00417D0003410000 00417D0003210000

Key label EXPORTER.TKE41.BINARY

State Complete

Figure 154. 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.

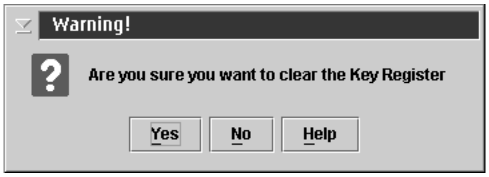

View Key Register

Command was executed successfully

Figure 155. View key register successful message

Clear

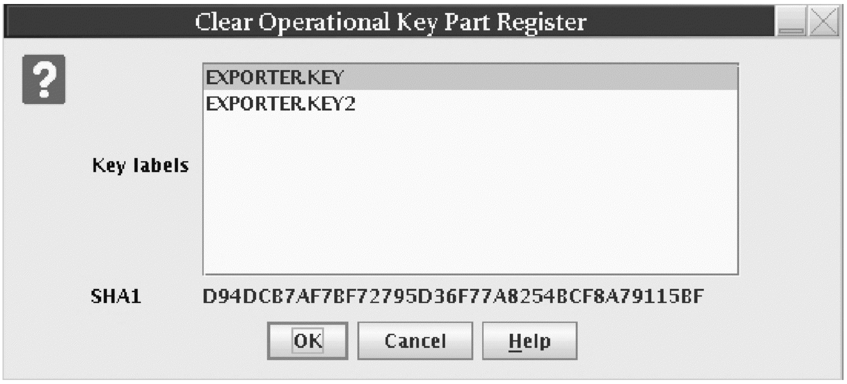
Operational Key Clear is used to clear the contents of key part registers. When **Clear** is selected, a **Warning!** window is displayed, prompting the user to confirm that he or she wants to clear the key part registers.


Warning!

Are you sure you want to clear the Key Register

Figure 156. 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.

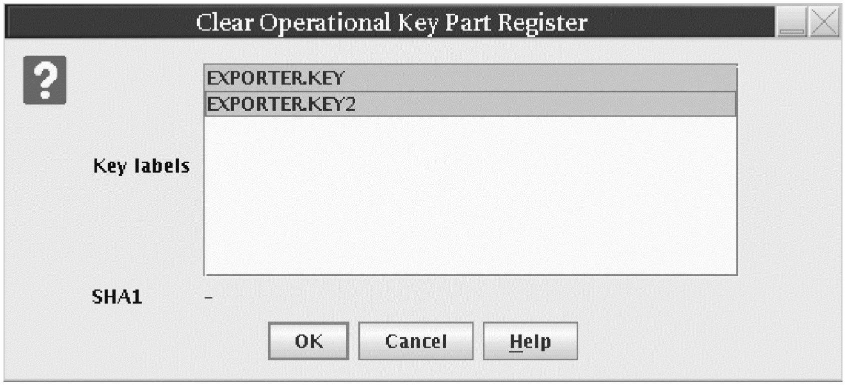


Key labels
EXPORTER.KEY
EXPORTER.KEY2

SHA1 D94DCB7AF7BF72795D36F77A8254BCF8A79115BF

Figure 157. 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 field on the window contains a '-'.

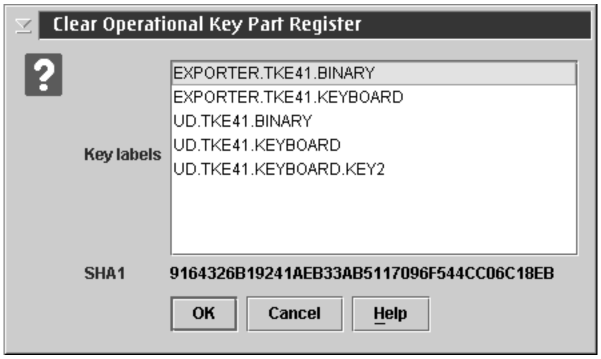


Key labels
EXPORTER.KEY
EXPORTER.KEY2

SHA1 -

Figure 158. 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.



Clear Operational Key Part Register

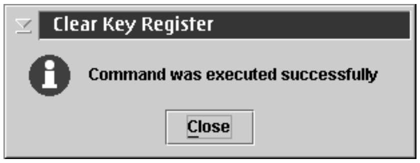
Key labels

- EXPORTER.TKE41.BINARY
- EXPORTER.TKE41.KEYBOARD
- UD.TKE41.BINARY
- UD.TKE41.KEYBOARD
- UD.TKE41.KEYBOARD.KEY2

SHA1 9164326B19241AEB33AB5117096F544CC06C18EB

Figure 159. 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.



Clear Key Register

Command was executed successfully

Figure 160. Clear Key Register successful message

Load to Key Storage

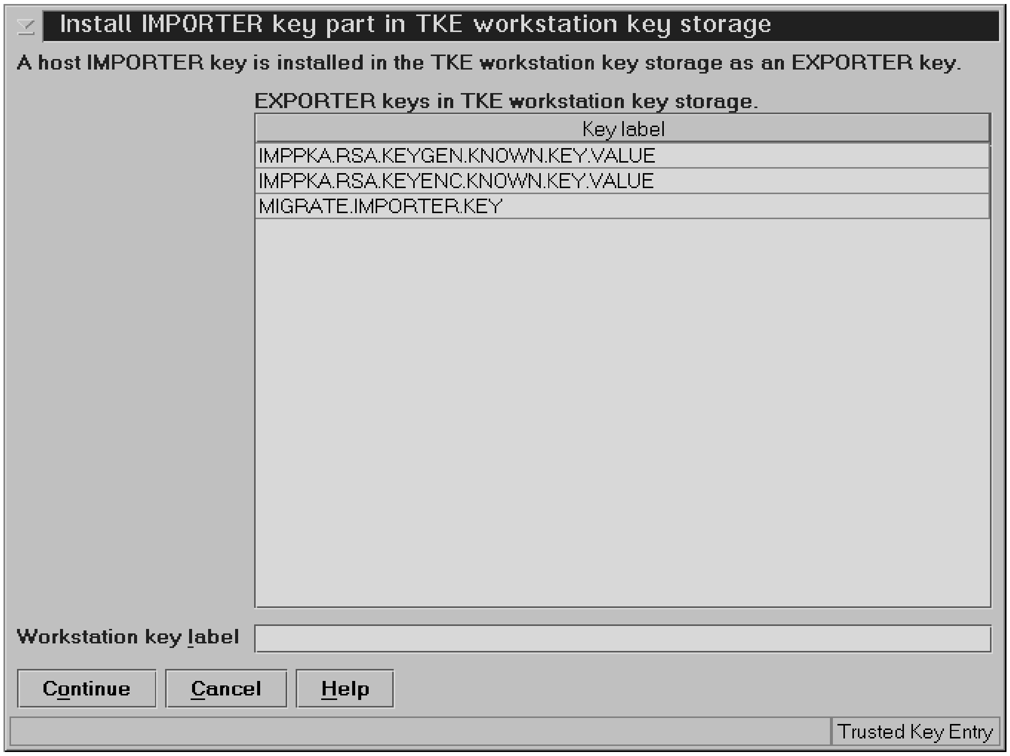
This selection is only possible for operational IMP-PKA or IMPORTER keys. The IMP-PKA key-encrypting keys are used to protect RSA keys during transport from the workstation to ICSF. Having selected **Load to Key Storage**, the user chooses one of the following key parts to load to the workstation key 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.



Install IMPORTER key part in TKE workstation key storage

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

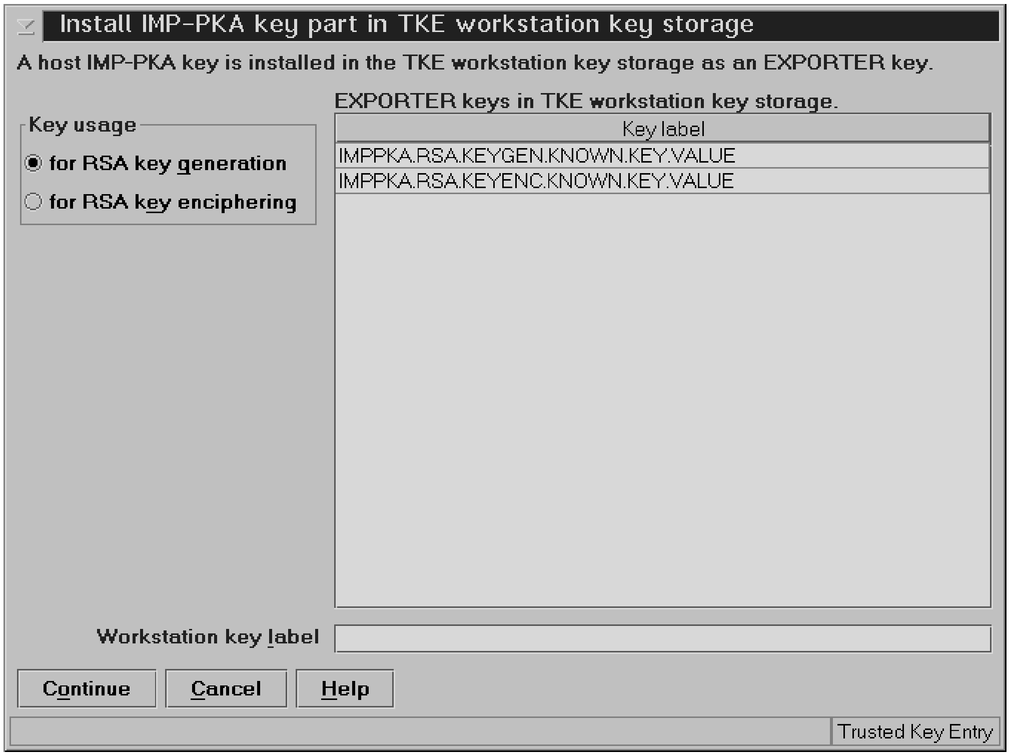
EXPORTER keys in TKE workstation key storage.

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

Workstation key label

Figure 161. 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.



Install IMP-PKA key part in TKE workstation key storage

A host IMP-PKA key is installed in the TKE workstation key storage as an EXPORTER key.

Key usage

● for RSA key generation

○ for RSA key enciphering

EXPORTER keys in TKE workstation key storage.

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

Workstation key label

Figure 162. 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 180.

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 307 for details on using this function.

RSA Keys

Generate RSA Key

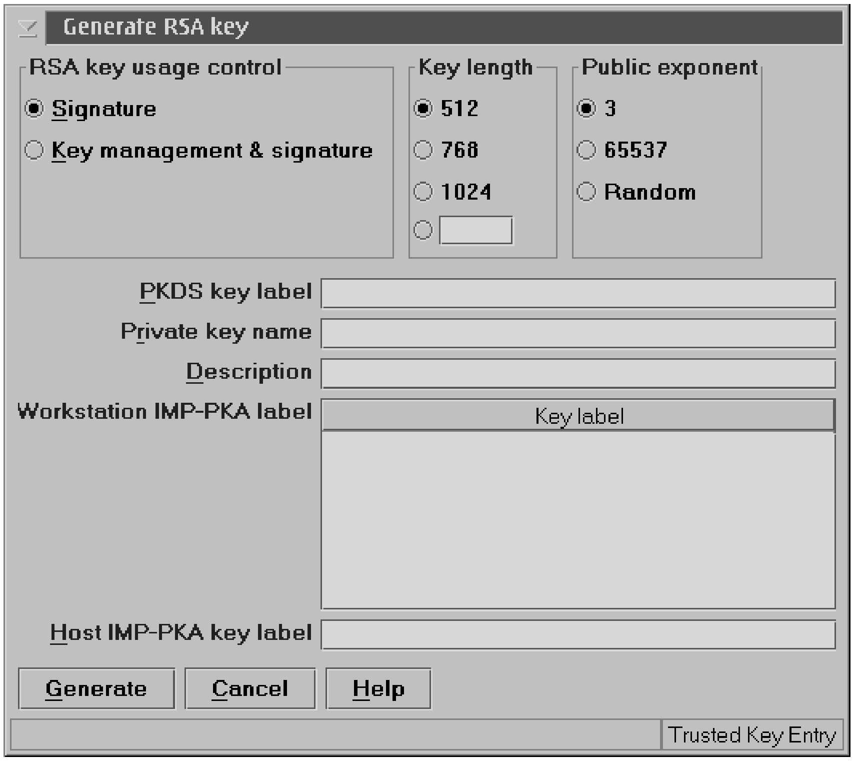
Note: On z10 EC, z10 BC, and z196, it is strongly recommended that customers use the PKA key generate (CSNDPKG) API to generate RSA keys.

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.



Generate RSA key

RSA key usage control

● Signature
○ Key management & signature

Key length

● 512
○ 768
○ 1024
○

Public exponent

● 3
○ 65537
○ Random

PKDS key label

Private key name

Description

Workstation IMP-PKA label

Key label

Host IMP-PKA key label

Figure 163. 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.

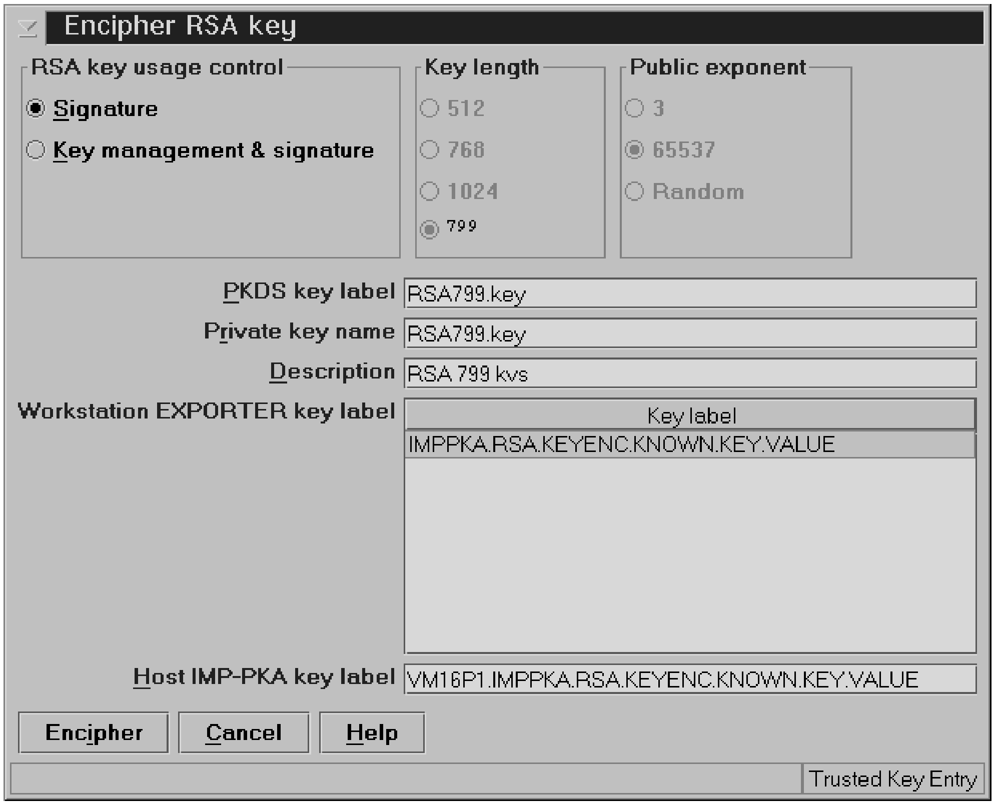
Warnings:

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 334.
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 D, "Clear RSA Key Format," on page 323.

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

Figure 164. 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.

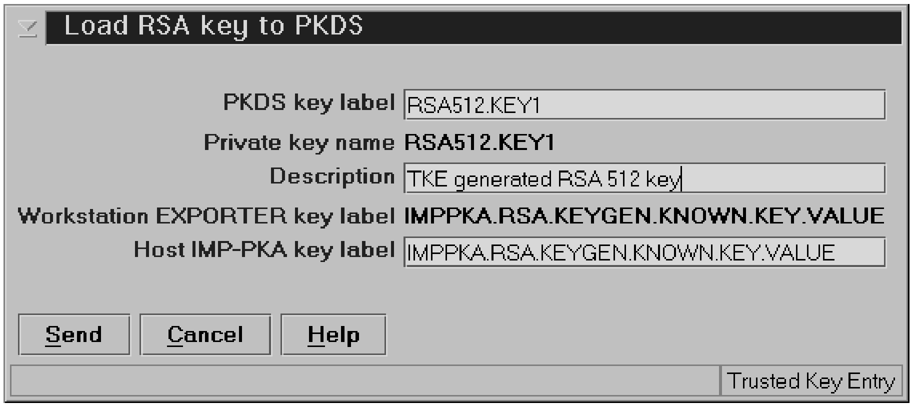
Warnings:

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 334.
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 logical partition (LPAR). For loading RSA keys to TKE target LPARs, see “Load RSA Key to Host Dataset” on page 199.

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.



Load RSA key to PKDS

PKDS key label: RSA512.KEY1

Private key name: RSA512.KEY1

Description: TKE generated RSA 512 key

Workstation EXPORTER key label: IMPPKA.RSA.KEYGEN.KNOWN.KEY.VALUE

Host IMP-PKA key label: IMPPKA.RSA.KEYGEN.KNOWN.KEY.VALUE

Figure 165. Load RSA Key to PKDS

In the **Load RSA key to PKDS** window, specify the following information:

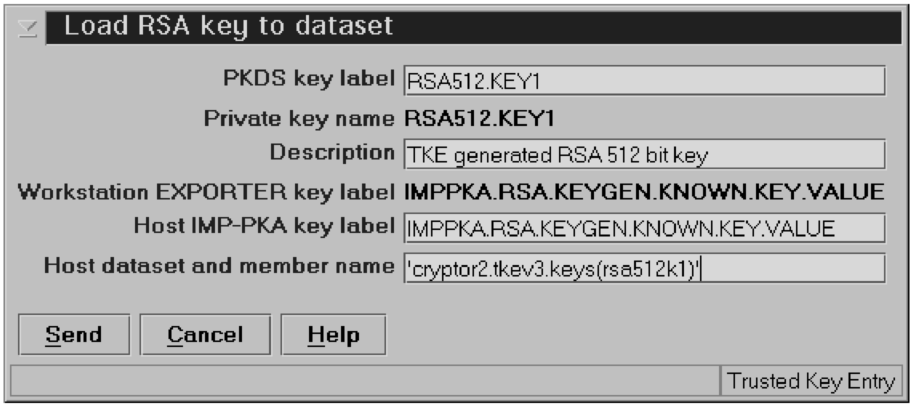
- **PKDS key label** — Label to be given the imported RSA key at the host. Change this field as needed.
- **Private key name** — Text string that is included in the RSA key token and cryptographically related to the key. The private key name can be used for access control for the key. The information 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/E 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/E ICSF interface, see “Installing RSA Keys in the PKDS from a Data Set” on page 239.

The steps are the same as for loading an RSA key to PKDS (see “Load RSA Key to PKDS” on page 198), 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/E logon of the administrator/host user ID.



Load RSA key to dataset

PKDS key label: RSA512.KEY1

Private key name: RSA512.KEY1

Description: TKE generated RSA 512 bit key

Workstation EXPORTER key label: IMPPKA.RSA.KEYGEN.KNOWN.KEY.VALUE

Host IMP-PKA key label: IMPPKA.RSA.KEYGEN.KNOWN.KEY.VALUE

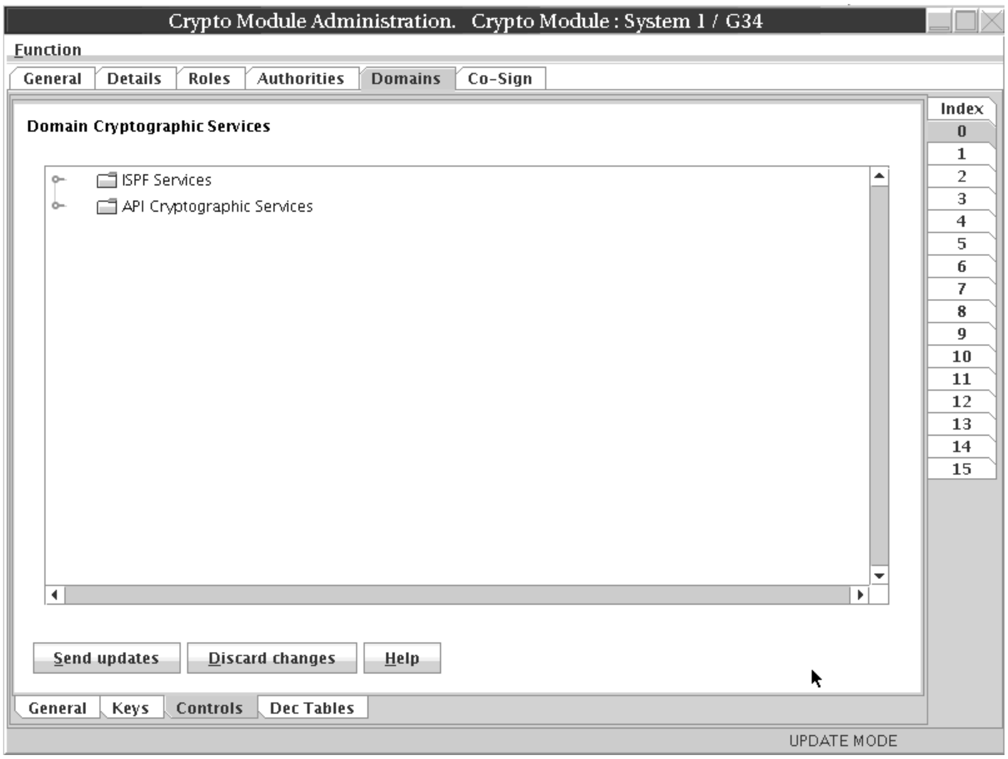
Host dataset and member name: 'cryptor2.tkev3.keys(rsa512k1)'

Figure 166. Load RSA Key to Dataset

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**



Crypto Module Administration. Crypto Module : System 1 / G34

Domain Cryptographic Services

- ISPF Services
- API Cryptographic Services

Figure 167. Controls Page

Note: When managing domain controls through a TKE 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 7.1 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 7.1 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.

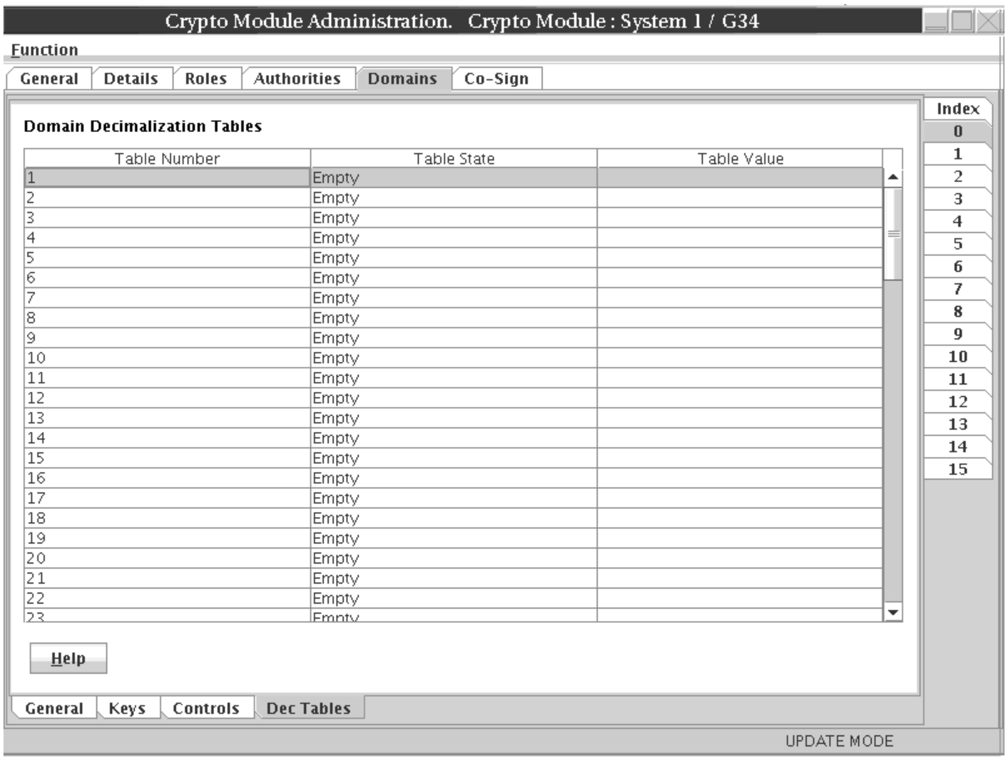
If you are using a TKE workstation for the first time, your settings under ISPF Services will indicate that all services are enabled.

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 *z/OS Cryptographic Services ICSF Application Programmer's Guide* for the correlation between the access control point and the ICSF callable service.

UDXs: The UDX folder appears only if there are User Defined Extensions on your system. The UDXs folder lists your extensions and allows you to enable or disable them.

Dec Tables Page

Decimalization tables map hexadecimal digits to decimal digits, and are used in certain host crypto module operations that process Personal Identification Numbers (PINs). Decimalization tables may contain only decimal digits ('0' through '9') and must be exactly 16 digits long. Every domain has slots for 100 decimalization tables. These tables can only be managed from a TKE. You can load, activate, or delete tables from this page.



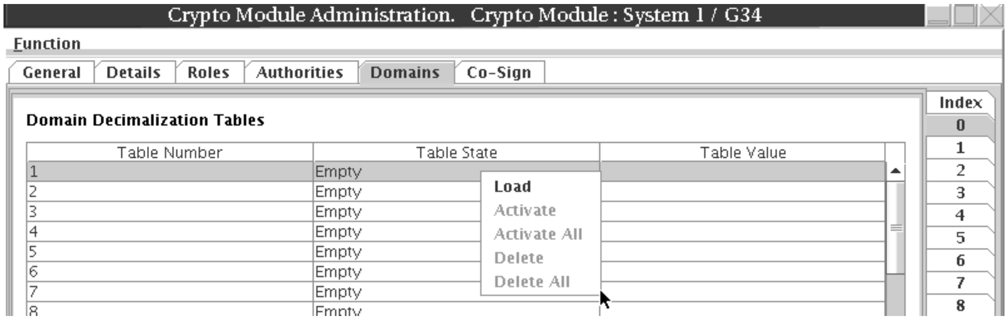
Domain Decimalization Tables

Table Number	Table State	Table Value
1	Empty	
2	Empty	
3	Empty	
4	Empty	
5	Empty	
6	Empty	
7	Empty	
8	Empty	
9	Empty	
10	Empty	
11	Empty	
12	Empty	
13	Empty	
14	Empty	
15	Empty	
16	Empty	
17	Empty	
18	Empty	
19	Empty	
20	Empty	
21	Empty	
22	Empty	
23	Empty	

Figure 168. Dec Tables page

To manage a table entry, left click to select an entry and right click to display command options. The available options are:

- Load
- Activate
- Activate All
- Delete
- Delete All



Domain Decimalization Tables

Table Number	Table State	Table Value
1	Empty	
2	Empty	
3	Empty	
4	Empty	
5	Empty	
6	Empty	
7	Empty	
8	Empty	

Figure 169. Table entry options

There are three access control points that control the ability to manage decimalization Tables. They are:

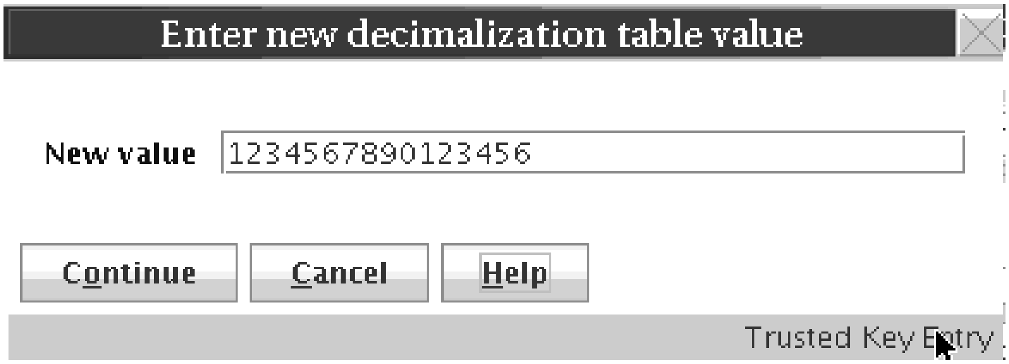
- Load Decimalization Tables
- Delete Decimalization Tables
- Activate Decimalization Tables

A table entry can be in any of the following states:

- Empty
- Active
- Loaded

Load Table

Left click to select a table entry, and right click to bring up the table options. Select the load option. From the “enter new decimalization table value” screen, enter a 16 digit decimalization table value. The table can only contain decimal digits ('0' through '9'). Press the continue button to create the table entry.


Enter new decimalization table value

New value 1234567890123456

Figure 170. Enter new decimalization table value

Notes:

1. You must have the “load” ACP in order to load a table.
2. If the current status of a table entry is Active, you must also have the “Delete” ACP in order to load a new table. You must be allowed to delete the current table.
3. If you load a table, and you also have the “activate” ACP, the new table will be immediately activated.

Activate or Activate All

Left click to select a table entry and right click to bring up the table options. Select the Activate or Activate All option. After the command completes successfully, press the Close button in the information message box.

Notes:

1. Only tables with a current state of Loaded can be activated.
2. You must have the “activate” ACP in order to activate a table.

Delete or Delete All

Left click to select a table entry and right click to bring up the table options. Select the Delete or Delete All option. After the command completes successfully, press the Close button in the information message box.

Notes:

1. Only tables with a current state of Loaded or Active can be deleted.
2. You must have the “delete” ACP in order to delete a table.

Crypto Module Notebook Co-Sign Tab

For co-signing a pending command in a host crypto module, open the notebook for that crypto module and select the **Co-Sign** tab. The **Co-Sign** tab panel displays the following information on the command to co-sign:

- **Pending command** – Name of the pending command
- **Pending command reference** – Unique hexadecimal number returned to the issuer of the command
- **Loading Authority** – Issuer of the command
- **Pending command details container** – Important parts of the pending command
- **Signature requirements container** – Current status for the fulfillment of the signature requirements

  For 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 in which you can choose the source of the authority signature key and then choose the authority index associated with that key. The possible authority signature key sources are as follows:

- **Current key** - Uses the currently loaded signature key
- **Smart card** - Reads an authority signature key from a TKE smart card
- **Binary file** - Reads an authority signature key from a hard disk or diskette
- **Key storage** - Reads an authority signature key from PKA key storage
- **Default key** - Uses the default authority signature key hardcoded into TKE

Press **Delete** if you want to delete the pending command.

Chapter 8. Auditing

TKE implements logging of security relevant operations that occur on the TKE workstation. TKE provides auditors with a trail of activities on the TKE workstation that are not currently tracked. Security actions performed on the TKE workstation are recorded in a security log and tied to a user identity. TKE security audit records are in addition to the System Management Facilities (SMF) records that are already cut on the host system that are triggered by requests from TKE.

To perform auditing tasks or configure auditing settings on the TKE workstation, you must log on with the AUDITOR user name. When logged on to the TKE Workstation as AUDITOR, you are able to:

- Use the TKE Audit Configuration Utility to turn TKE auditing on and off.
- Use Service Management functions to:
  - View the security log
  - Archive the security logs
- Use the TKE Audit Record Upload Configuration Utility to configure audit record upload to a System z host, where the audit records will be saved in the z/OS SMF dataset.

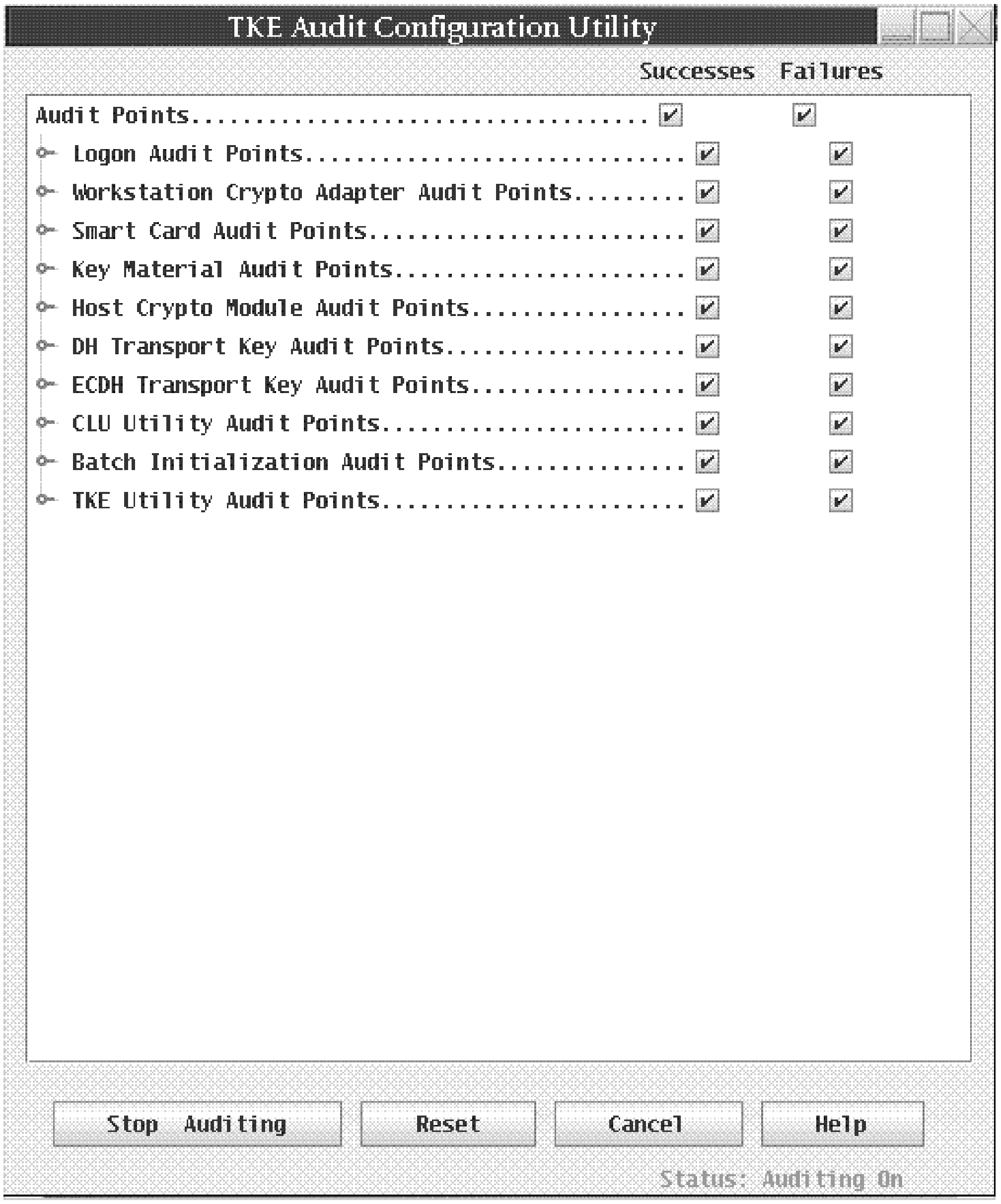
ICSF also uses SMF record type 82 to record certain ICSF events. ICSF writes to subtype 16 whenever a TKE workstation either issues a command request to, or receives a reply response from, a Crypto Express2 Coprocessor or Crypto Express3 Coprocessor. In addition to the subtype 16 records, you can use 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.

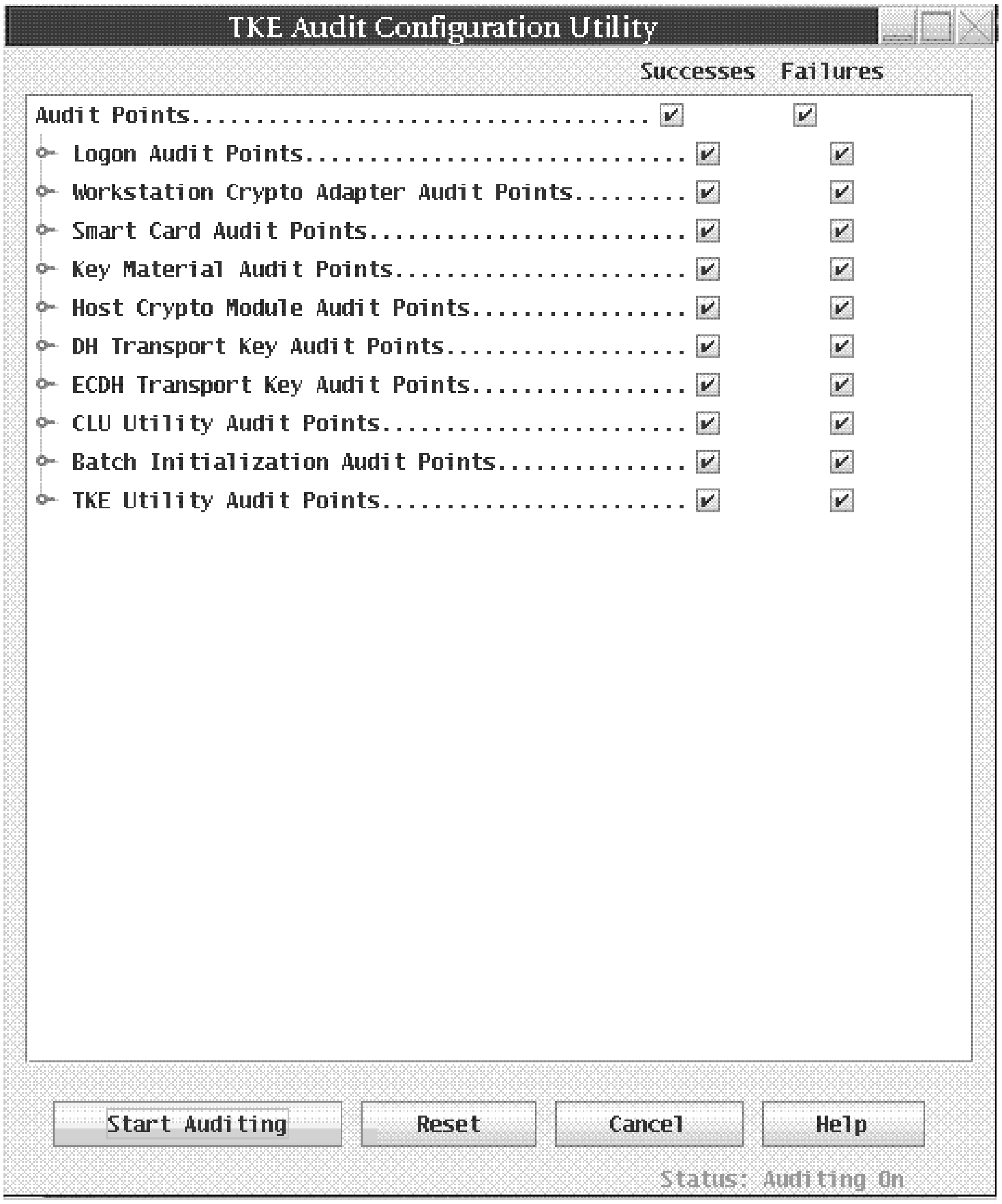


	Successes	Failures
Audit Points..................................	☑	☑
Logon Audit Points............................	☑	☑
Workstation Crypto Adapter Audit Points.........	☑	☑
Smart Card Audit Points........................	☑	☑
Key Material Audit Points......................	☑	☑
Host Crypto Module Audit Points................	☑	☑
DH Transport Key Audit Points..................	☑	☑
ECDH Transport Key Audit Points................	☑	☑
CLU Utility Audit Points.......................	☑	☑
Batch Initialization Audit Points..............	☑	☑
TKE Utility Audit Points.......................	☑	☑

Status: Auditing On

Figure 171. 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**.

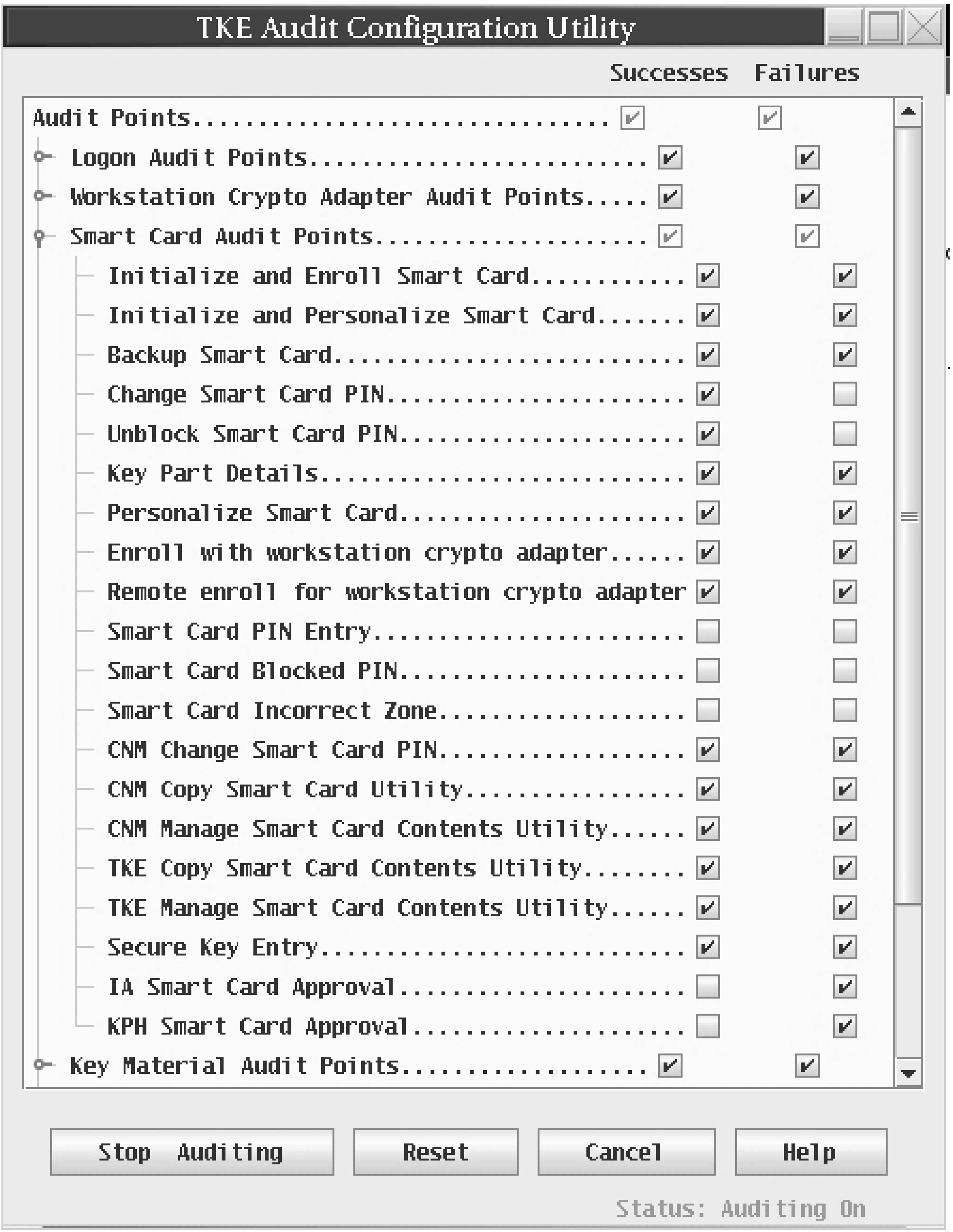

TKE Audit Configuration Utility

	Successes	Failures
Audit Points	☑	☑
Logon Audit Points	☑	☑
Workstation Crypto Adapter Audit Points	☑	☑
Smart Card Audit Points	☑	☑
Key Material Audit Points	☑	☑
Host Crypto Module Audit Points	☑	☑
DH Transport Key Audit Points	☑	☑
ECDH Transport Key Audit Points	☑	☑
CLU Utility Audit Points	☑	☑
Batch Initialization Audit Points	☑	☑
TKE Utility Audit Points	☑	☑

Status: Auditing On

Figure 172. 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.



	Successes	Failures
Audit Points	☑	☑
Logon Audit Points	☑	☑
Workstation Crypto Adapter Audit Points	☑	☑
Smart Card Audit Points	☑	☑
Initialize and Enroll Smart Card	☑	☑
Initialize and Personalize Smart Card	☑	☑
Backup Smart Card	☑	☑
Change Smart Card PIN	☑	□
Unblock Smart Card PIN	☑	□
Key Part Details	☑	☑
Personalize Smart Card	☑	☑
Enroll with workstation crypto adapter	☑	☑
Remote enroll for workstation crypto adapter	☑	☑
Smart Card PIN Entry	□	□
Smart Card Blocked PIN	□	□
Smart Card Incorrect Zone	□	□
CNM Change Smart Card PIN	☑	☑
CNM Copy Smart Card Utility	☑	☑
CNM Manage Smart Card Contents Utility	☑	☑
TKE Copy Smart Card Contents Utility	☑	☑
TKE Manage Smart Card Contents Utility	☑	☑
Secure Key Entry	☑	☑
IA Smart Card Approval	□	☑
KPH Smart Card Approval	□	☑
Key Material Audit Points	☑	☑

Status: Auditing On

Figure 173. 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

View Security Logs

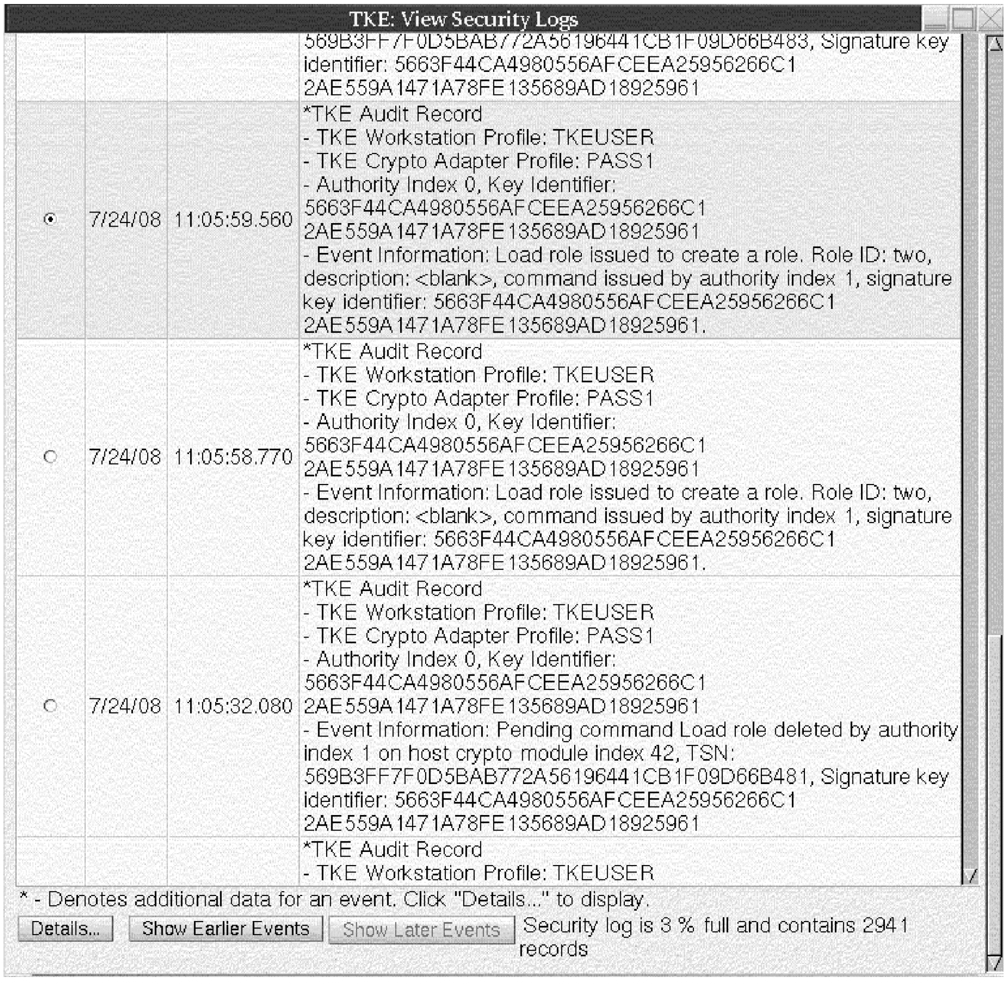
The security logs can be viewed on the TKE, but only when you are logged in with the AUDITOR user name. The security log has a max size allowed of 30MB.

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 archive the security logs (see “Archive Security Logs” on page 213).

In order to view the security logs, log in as the AUDITOR user, select **Service Management** and select **View Security Logs**.


TKE: View Security Logs

			569B3FF7F0D5BAB772A56196441CB1F09D66B483, Signature key identifier: 5663F44CA4980556AFCEEA25956266C1 2AE559A1471A78FE135689AD18925961
●	7/24/08	11:05:59.560	*TKE Audit Record - TKE Workstation Profile: TKEUSER - TKE Crypto Adapter Profile: PASS1 - Authority Index 0, Key Identifier: 5663F44CA4980556AFCEEA25956266C1 2AE559A1471A78FE135689AD18925961 - Event Information: Load role issued to create a role. Role ID: two, description: <blank>, command issued by authority index 1, signature key identifier: 5663F44CA4980556AFCEEA25956266C1 2AE559A1471A78FE135689AD18925961.
○	7/24/08	11:05:58.770	*TKE Audit Record - TKE Workstation Profile: TKEUSER - TKE Crypto Adapter Profile: PASS1 - Authority Index 0, Key Identifier: 5663F44CA4980556AFCEEA25956266C1 2AE559A1471A78FE135689AD18925961 - Event Information: Load role issued to create a role. Role ID: two, description: <blank>, command issued by authority index 1, signature key identifier: 5663F44CA4980556AFCEEA25956266C1 2AE559A1471A78FE135689AD18925961.
○	7/24/08	11:05:32.080	*TKE Audit Record - TKE Workstation Profile: TKEUSER - TKE Crypto Adapter Profile: PASS1 - Authority Index 0, Key Identifier: 5663F44CA4980556AFCEEA25956266C1 2AE559A1471A78FE135689AD18925961 - Event Information: Pending command Load role deleted by authority index 1 on host crypto module index 42, TSN: 569B3FF7F0D5BAB772A56196441CB1F09D66B481, Signature key identifier: 5663F44CA4980556AFCEEA25956266C1 2AE559A1471A78FE135689AD18925961
			*TKE Audit Record - TKE Workstation Profile: TKEUSER

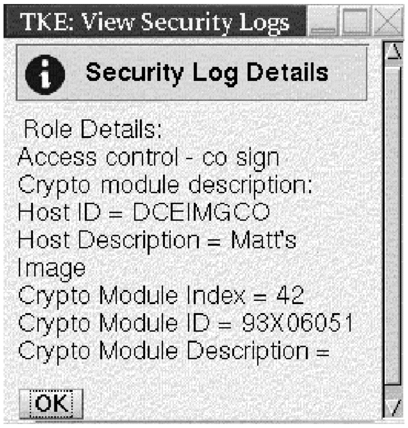
* - Denotes additional data for an event. Click "Details..." to display.

Security log is 3 % full and contains 2941 records

Figure 174. 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...** .



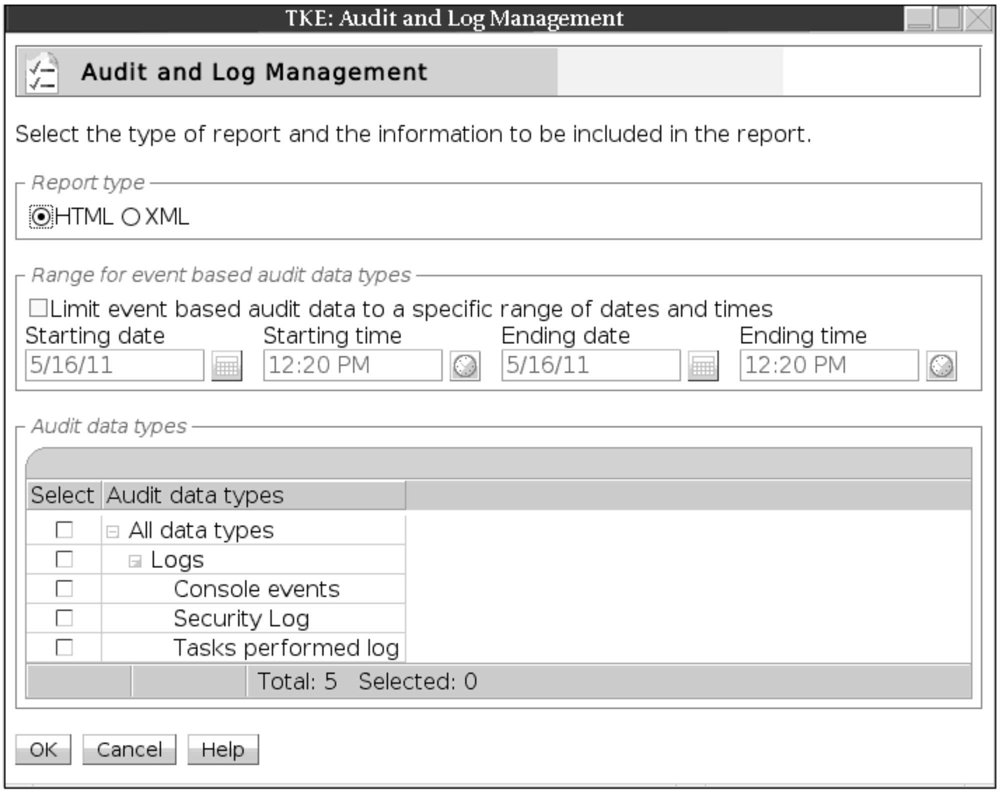
Role Details:
Access control - co sign
Crypto module description:
Host ID = DCEIMGCO
Host Description = Matt's
Image
Crypto Module Index = 42
Crypto Module ID = 93X06051
Crypto Module Description =

Figure 175. Viewing additional details of the security logs

Audit and Log Management

Audit and log management copies the console events log, security log, and tasks performed log to a DVD-RAM or USB flash memory drive. If you wish to copy the logs, you must be logged onto the TKE console with the AUDITOR user name. Select **Service Management** and, from the service management window, select **Audit and Log Management**.

The Audit and Log Management dialog box is displayed.



TKE: Audit and Log Management

Audit and Log Management

Select the type of report and the information to be included in the report.

Report type

● HTML ○ XML

Range for event based audit data types

□ Limit event based audit data to a specific range of dates and times

Starting date	Starting time	Ending date	Ending time
5/16/11	12:20 PM	5/16/11	12:20 PM

Audit data types

Select	Audit data types
□	⊟ All data types
□	⊟ Logs
□	Console events
□	Security Log
□	Tasks performed log

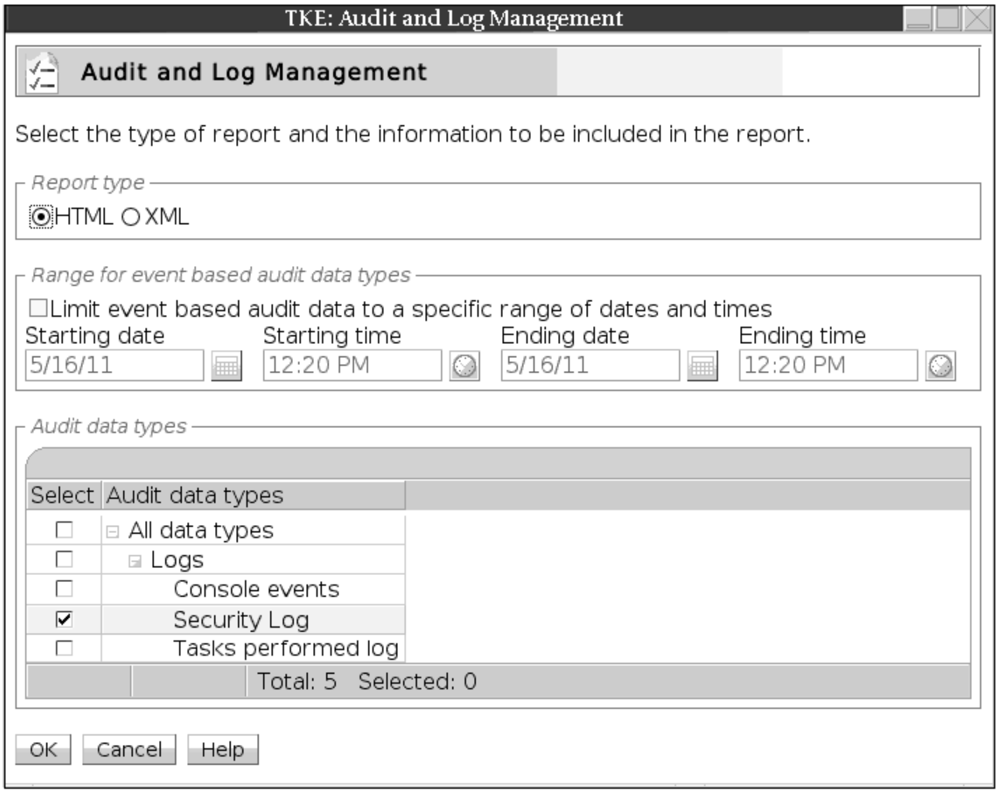
Total: 5 Selected: 0

Figure 176. Audit and Log Management dialog

The log data can be formatted in either HTML or XML format.

The starting and ending date and time values may be specified to limit the amount of log data that will appear in the report.

The types of data (console events, security log, and tasks performed log) can also be specified to limit the amount of data that appears in the report. Note that the events related to the TKE utilities are logged in the security log.



Audit and Log Management

Select the type of report and the information to be included in the report.

Report type

● HTML ○ XML

Range for event based audit data types

☐ Limit event based audit data to a specific range of dates and times

Starting date	Starting time	Ending date	Ending time
5/16/11	12:20 PM	5/16/11	12:20 PM

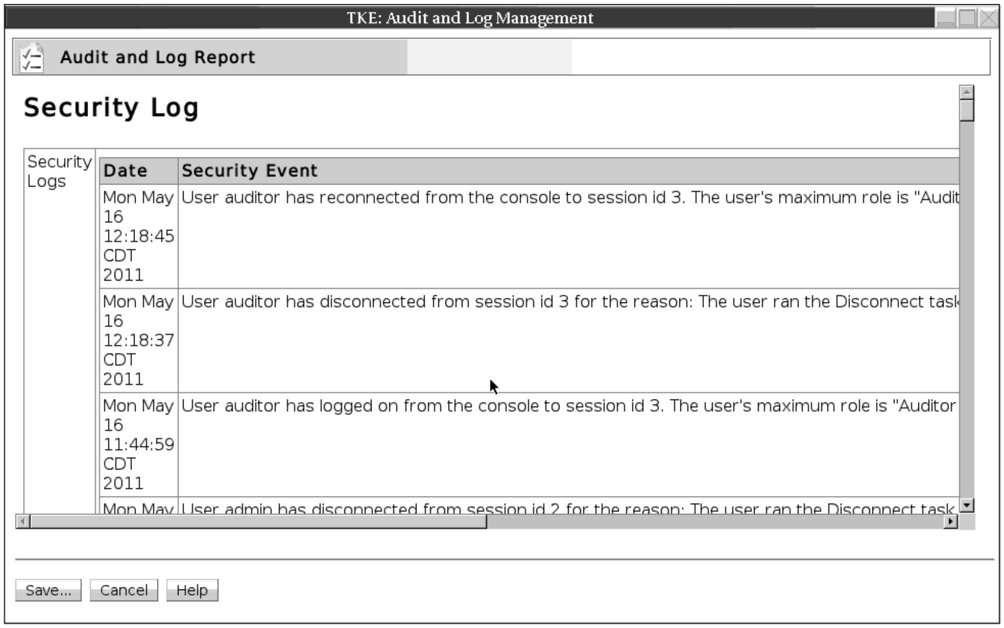
Audit data types

Select	Audit data types
☐	⊟ All data types
☐	⊟ Logs
☐	Console events
☑	Security Log
☐	Tasks performed log

Total: 5 Selected: 0

Figure 177. Audit and Log Management dialog (security log data selected)

After pressing OK, the log data is formatted in either HTML or XML format, and is displayed in a window.



Audit and Log Report

Security Log

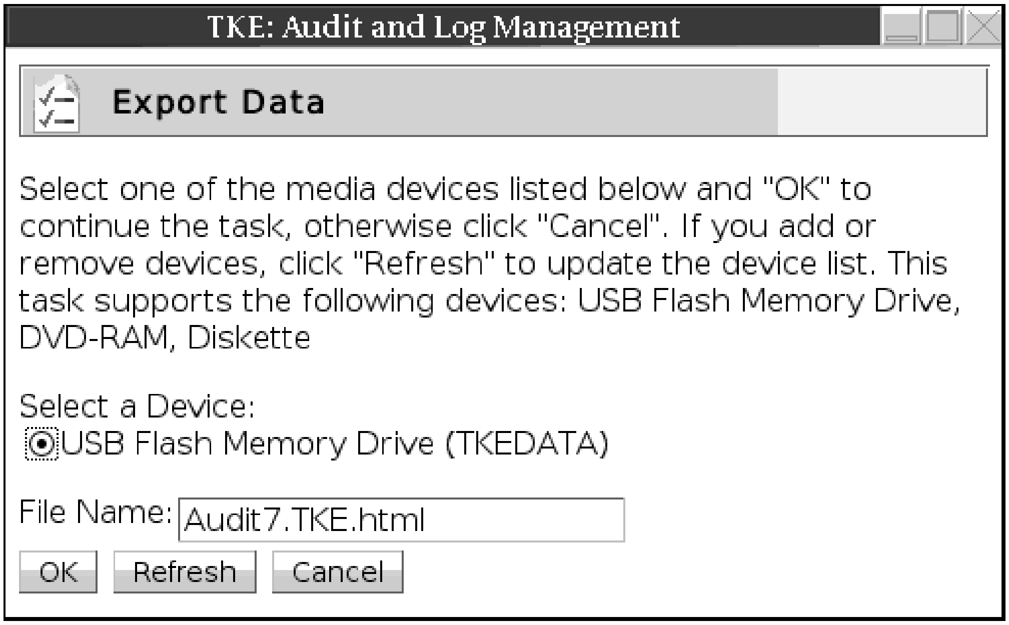
Security Logs

Date	Security Event
Mon May 16 12:18:45 CDT 2011	User auditor has reconnected from the console to session id 3. The user's maximum role is "Audit
Mon May 16 12:18:37 CDT 2011	User auditor has disconnected from session id 3 for the reason: The user ran the Disconnect task
Mon May 16 11:44:59 CDT 2011	User auditor has logged on from the console to session id 3. The user's maximum role is "Auditor
Mon May	User admin has disconnected from session id 2 for the reason: The user ran the Disconnect task

Figure 178. Security Log

This window contains the report produced from the log data. To save the report to a DVD-RAM or a USB flash memory drive, press the **Save...** button. After pressing

Save..., the Export Data window is displayed.



Select one of the media devices listed below and "OK" to continue the task, otherwise click "Cancel". If you add or remove devices, click "Refresh" to update the device list. This task supports the following devices: USB Flash Memory Drive, DVD-RAM, Diskette

Select a Device:
● USB Flash Memory Drive (TKEDATA)

File Name: Audit7.TKE.html

Figure 179. Export Data

Note: If a DVD-RAM or USB flash memory drive is not currently present, nothing is listed under **Select a Device**. To write to a DVD-RAM, insert the DVD-RAM into the drive, wait for the drive light to stop blinking, and then press the **Refresh** button. To write to a USB flash memory drive insert the drive, wait for the USB Device Status window to appear, and then press the **Refresh** button. When the **OK** button is pressed, the report is saved with the specified file name to the DVD-RAM or USB flash memory drive.

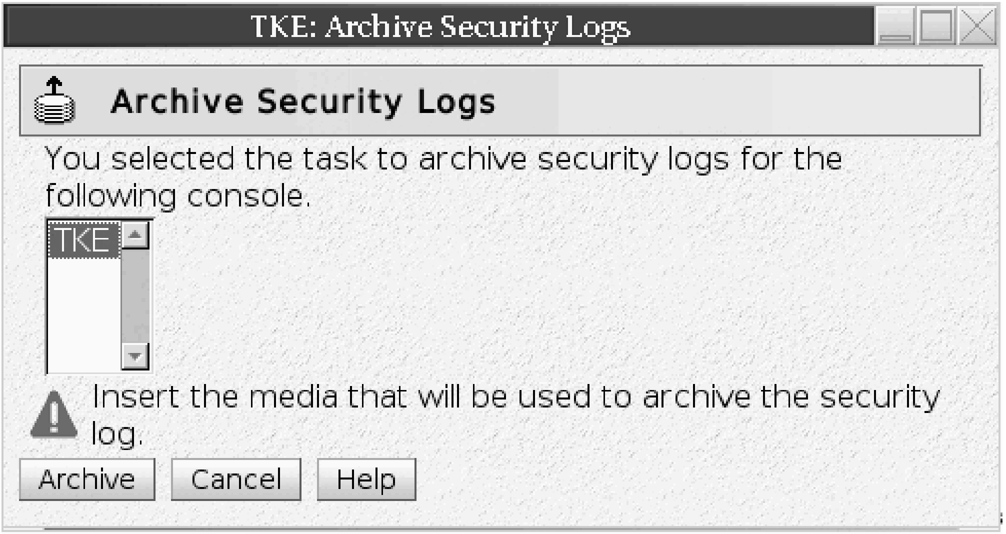
A popup window is displayed to indicate that the report was saved successfully.

Archive Security Logs

If you wish to archive the security logs you must be logged onto the TKE console with the AUDITOR user name. Archiving the security logs saves the security log's event data in another file on the 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 351).



TKE: Archive Security Logs

Archive Security Logs

You selected the task to archive security logs for the following console.

TKE

Insert the media that will be used to archive the security log.

Figure 180. 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.

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.

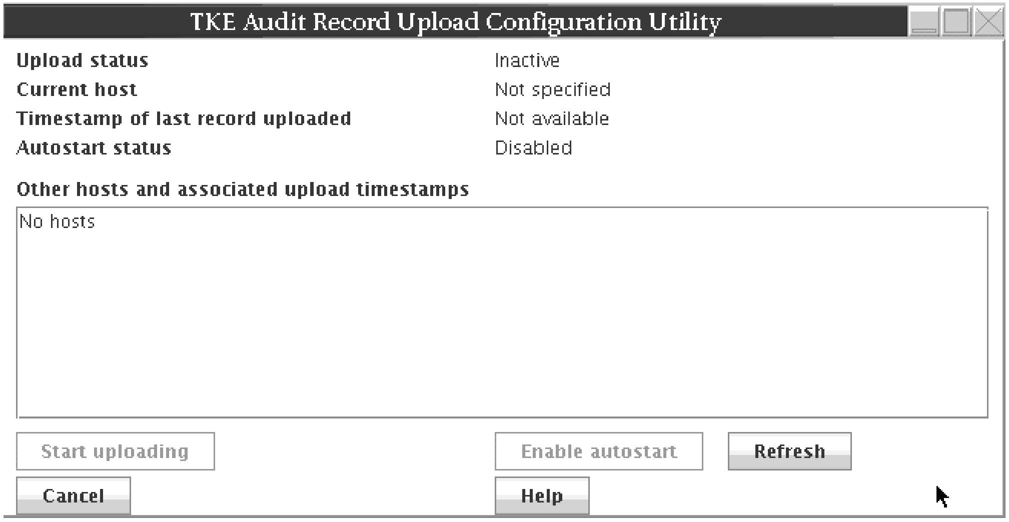
Starting TKE Audit Record Upload Configuration Utility

To use the TKE Audit Record Upload Configuration Utility, you must first sign on to the Trusted Key Entry console in **Privileged Mode Access** with the AUDITOR user ID. To do this:

1. Close the Trusted Key Entry Console.
2. From the Welcome to the Trusted Key Entry Console screen select *Privileged Mode Access*.
3. From the Trusted Key Entry Console Logon screen, enter the user name AUDITOR and the password. (The default password is PASSWORD, but this can be changed by the user. See “Change Password” on page 345.)
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.



TKE Audit Record Upload Configuration Utility

Upload status Inactive
Current host Not specified
Timestamp of last record uploaded Not available
Autostart status Disabled

Other hosts and associated upload timestamps

No hosts

Figure 181. TKE Audit Record Upload Configuration Utility

Using the TKE Audit Record Upload Configuration Utility, you can:

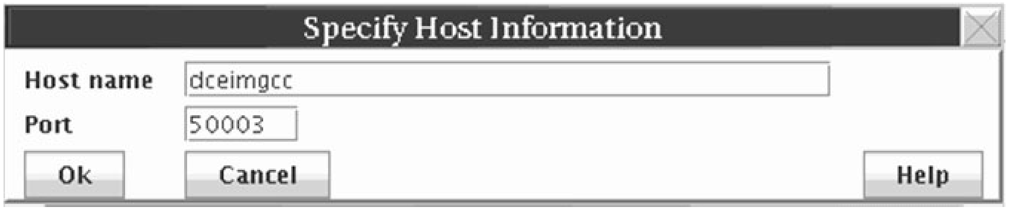
- Specify the host machine to which the audit records will be sent. See “Configure TKE for Audit Data Upload” for more information.
- Upload audit records to the target host. See “Uploading Audit Records” on page 217 for more information.
- Enable automatic audit record upload. When enabled, audit records will be uploaded every time the workstation is rebooted. See “Enabling and Disabling Automatic Audit Record Upload” on page 217 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.



Specify Host Information

Host name dceimgcc
Port 50003

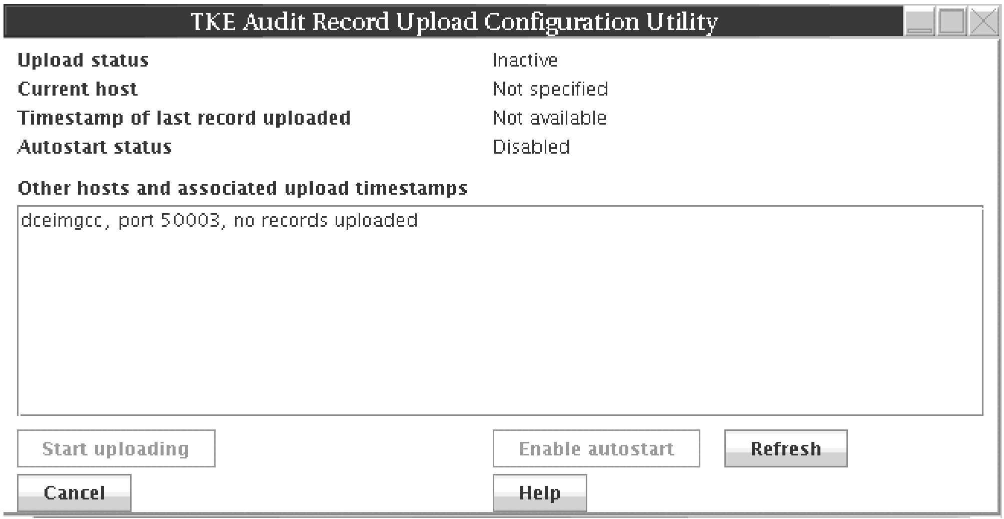
Figure 182. Specify Host Information dialog

   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.



TKE Audit Record Upload Configuration Utility

Upload status	Inactive
Current host	Not specified
Timestamp of last record uploaded	Not available
Autostart status	Disabled

Other hosts and associated upload timestamps

dceimgcc, port 50003, no records uploaded

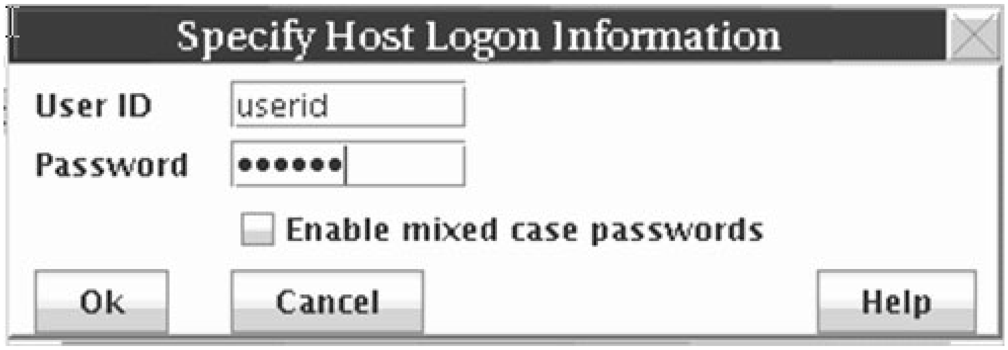
Figure 183. Other hosts and associated timestamps

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.



Specify Host Logon Information

User ID: userid

Password: ••••••

□ Enable mixed case passwords

Figure 184. 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 target host has been identified in the TKE Audit Record Upload Utility, 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” 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 215), you can upload audit records to the target host. If you have not already logged onto the host system during this session, the Specify Host Logon Information dialog will prompt you for a user ID and password before the audit records will be uploaded. To complete this task, you must have a user ID and password for the target host.

In the TKE Audit Record Upload Utility window, click the **Start uploading** command button.

Note: If you have not already logged onto the host system, the Specify Host Logon Information dialog will prompt you for a user ID and password.

The TKE Audit Record Upload Configuration Utility will begin uploading the audit records to the target host. The TKE Audit Record Upload Configuration Utility window's Upload status field will indicate the status of the upload operation.

- Pressing the **Refresh** 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 215), you can enable automatic audit record upload. This is called autostart mode. In autostart mode, audit records will be uploaded every time the workstation is rebooted. If you have not already logged onto 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 logged onto the host system, the Specify Host Logon Information dialog will prompt you for a user ID and password.

The TKE Audit Record Upload Configuration Utility will 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 220)
- Changing the DES-MK or AES-MK periodically (page 222)
- Reentering the master keys (page 226)
- Adding Additional Coprocessors (page 228)
- Changing the ASYM-MK master keys (page 228)
- Loading Operational Keys to the CKDS (page 233)
- Refreshing the CKDS (page 236)
- Install RSA Keys (page 239)

Master Key Parts

| Master key parts are loaded using binary files, the keyboard, or smart cards. If loading key parts with the keyboard, record the key parts and the associated hash patterns.

The key parts are generated from the Domain Keys page. For more information, see "Domains Keys Page" on page 160.

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 236.

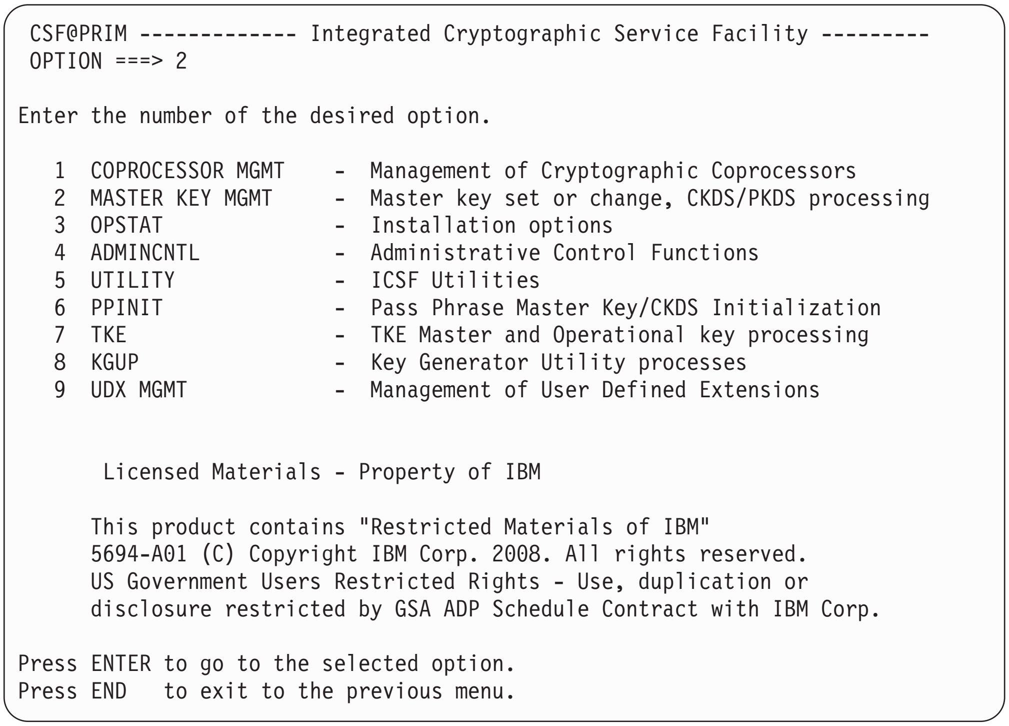
Initialize the CKDS

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:

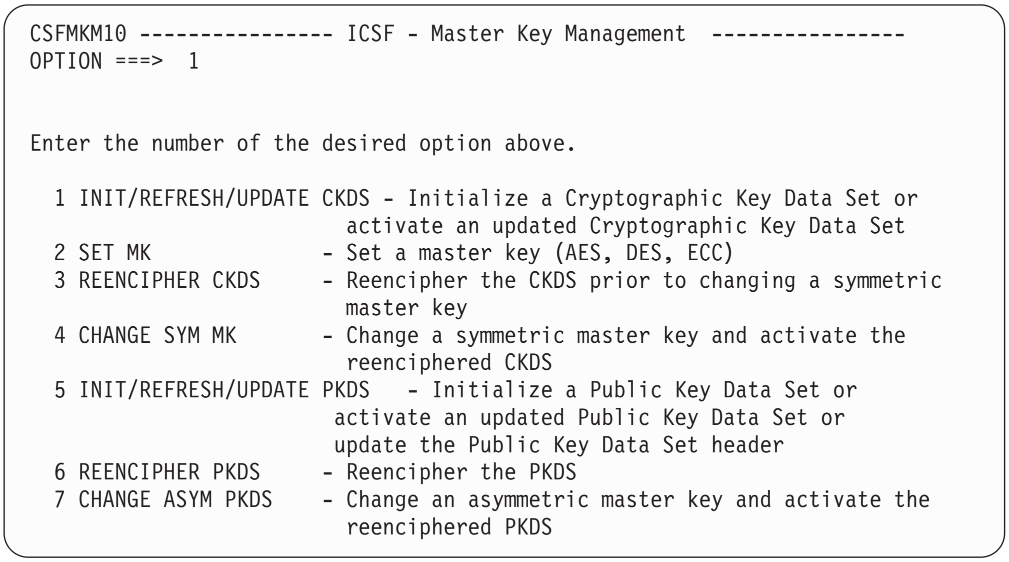
1. Select Option 2, MASTER KEY MGMT, as shown in Figure 185 on page 221.



```
 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

      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 185. ICSF Selecting the Master Key Option on the Primary Menu Panel

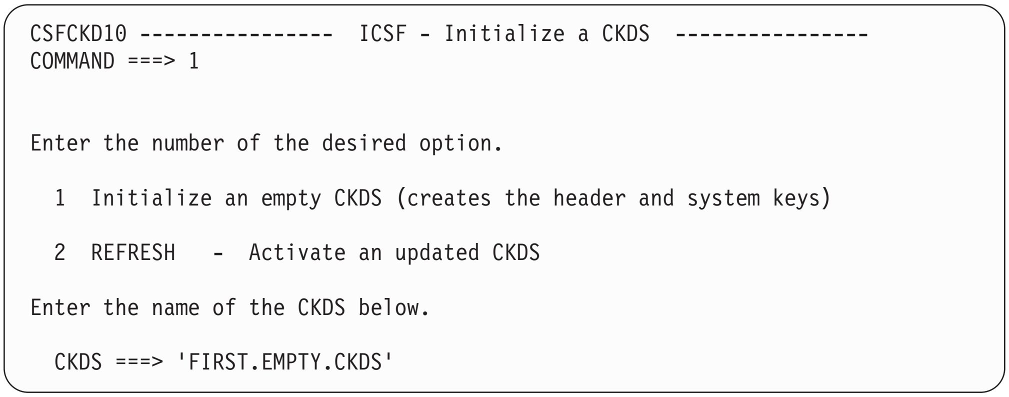
2. The Master Key Management panel appears. Select Option 1, INIT/REFRESH/UPDATE CKDS, as shown in Figure 186.



```
 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 186. 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 187. 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.

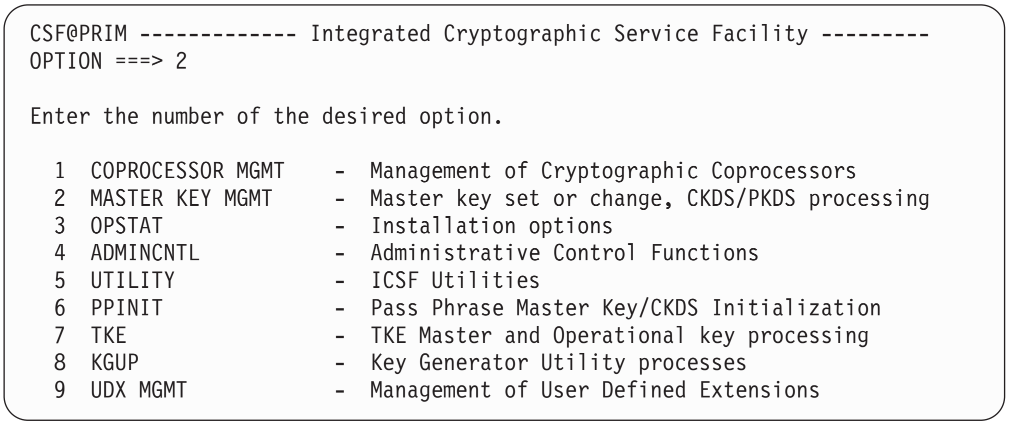
Changing the Master Key Using the Master Key Panels

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/E 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.

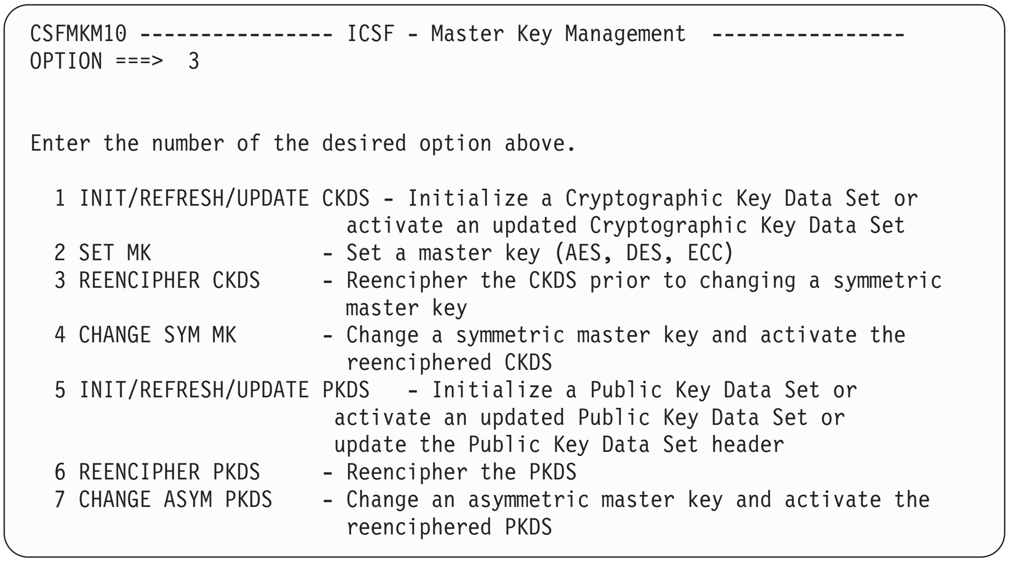
1. Select option 2, MASTER KEY MGMT, on the ICSF Primary Menu.



```
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 188. Selecting the Master Key Option on the ICSF Primary Menu Panel

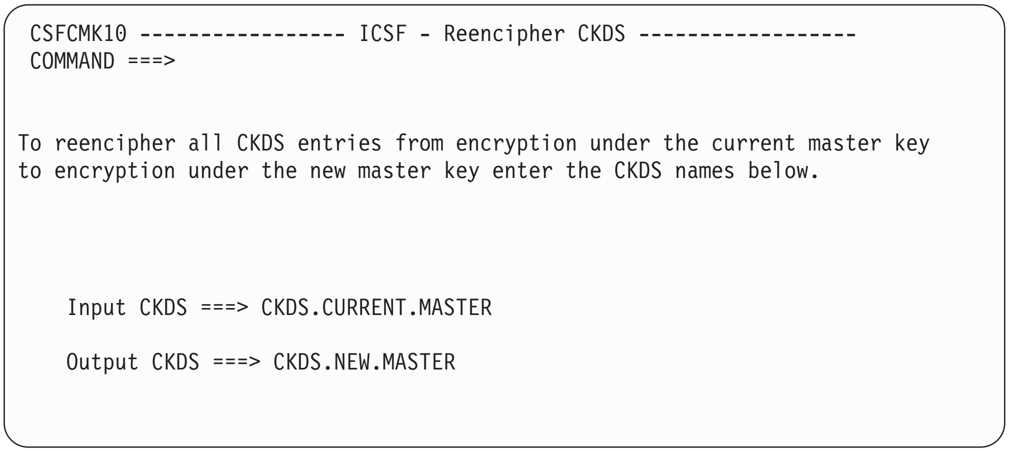
2. Before you change the master key, you must first reencipher the disk copy of the CKDS under the new master key. Select option 3, REENCIPHER CKDS, on the Master Key Management panel, as shown in Figure 189 on page 224, and press ENTER.



```
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 189. Selecting the Reencipher CKDS Option on the ICSF Master Key Management Panel

3. The Reencipher CKDS panel appears. See Figure 190.



```
 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 190. 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.

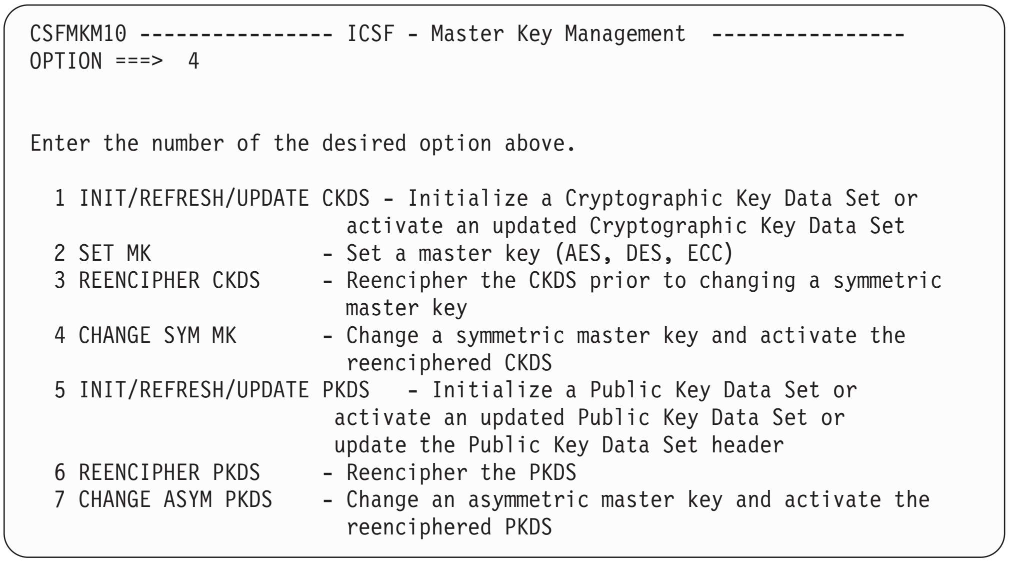
   Note: The output data set should already exist although it must be empty. For more information about defining a CKDS, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

   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.

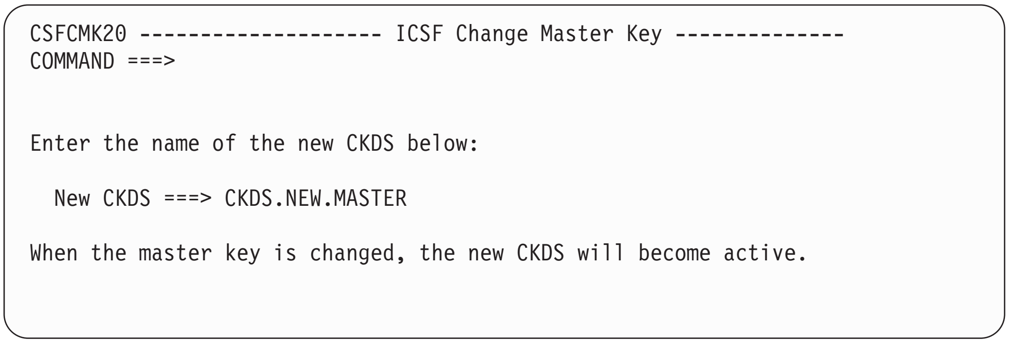
7. Press END to return to the Master Key Management panel.
   a. Changing the master key involves refreshing the in-storage copy of the CKDS with a disk copy and activating the new master key.
   b. If you are running in compatibility or co-existence mode, *do not* select option 4, the Change option. 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 191.



```
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 191. 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 192.



```
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 192. 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 190 on page 224, 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

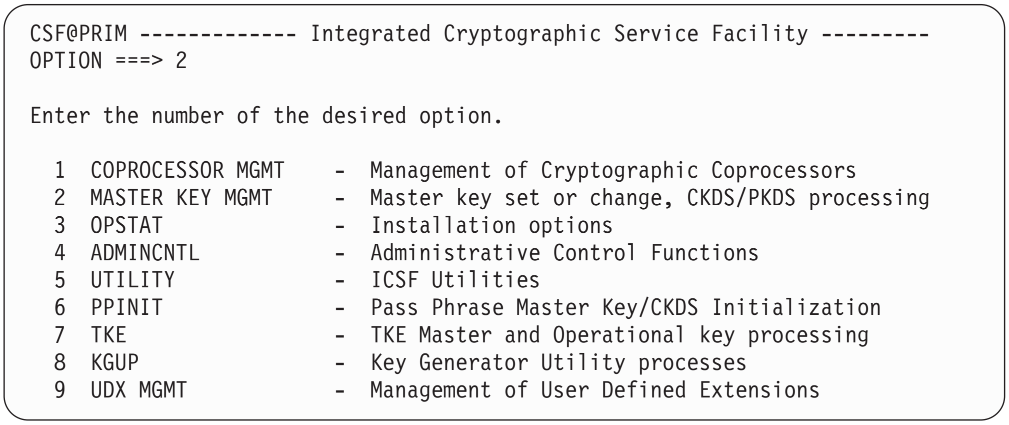
When running in PR/SM logical partition (LPAR) mode, a tamper situation causes all installation data; master keys, retained keys, operational key part registers, roles and authorities on the crypto card to be cleared. All installation data will need to be reloaded and recreated. If you zeroize a domain 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 single key part” on page 165.

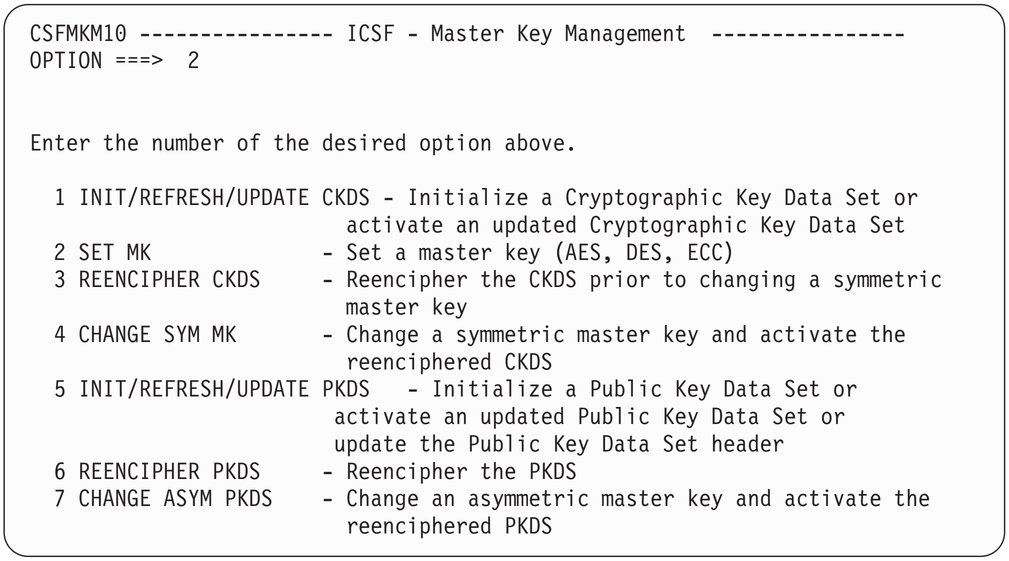
   These values should be stored in a secure place as specified in your enterprises security process.
2. Retrieve the key parts, checksums, verification patterns, and hash patterns you used when you loaded the master keys originally. These values should have been stored in a secure place.
3. To activate the DES or AES master key you just entered, you need to set it. On the ICSF Primary Menu panel, 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  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 193. 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 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 194. 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 222.

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 227) 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 229.

| To enter an asymmetric master key, you can either enter a first key part and a final
| key part or a first key part, one or more intermediate key parts, 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.

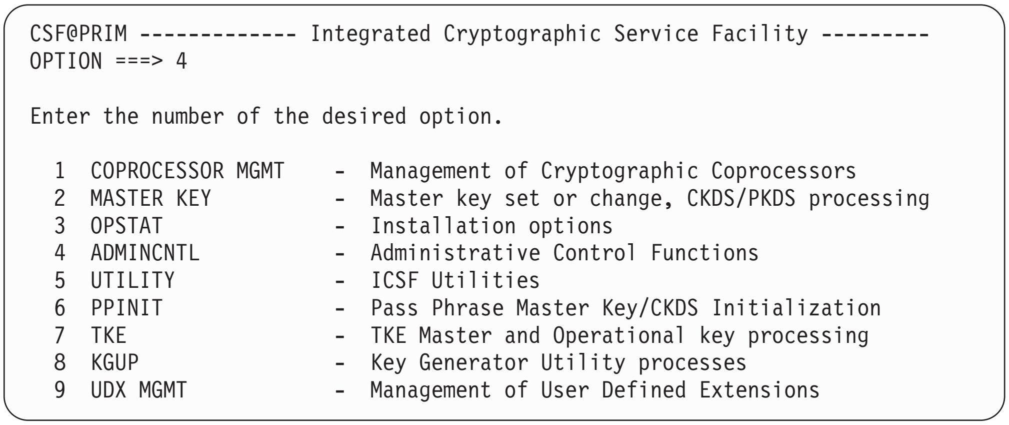
Tasks necessary for changing the asymmetric-keys master keys are listed here. Note that steps 2 through 4 are done at the TKE workstation.

1. Disable PKA Services
2. Clear New ASYM-MK (*if not empty*)
3. Load New ASYM-MK — first, one or more middle parts, 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:

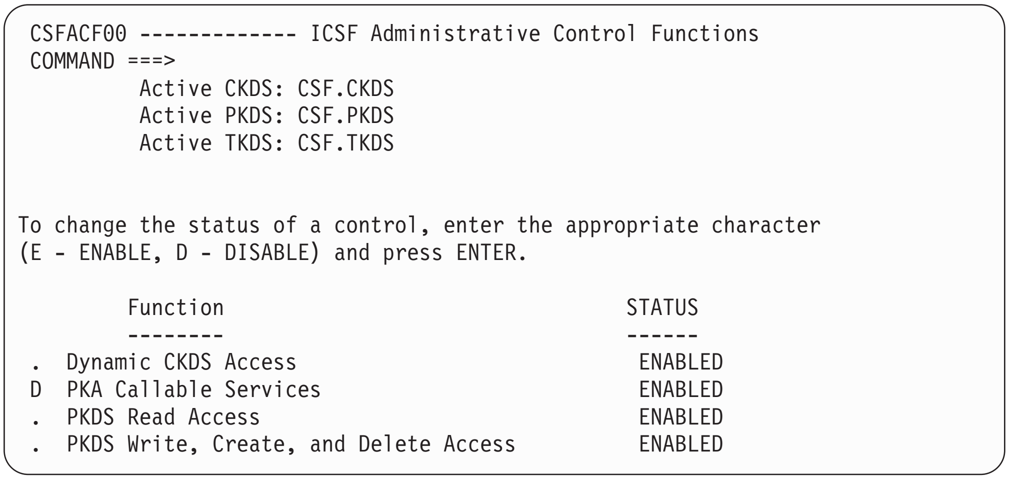
1. From TSO/E, access the user control functions by choosing option 4, ADMINCNTL, on the Primary Menu panel of ICSF, as shown in Figure 195.



```
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 195. Selecting the Administrative Control Option on the ICSF Primary Menu Panel

2. The Administrative Control Function panel appears. See Figure 196 on page 230.



```
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 196. Disabling the PKA Callable Services

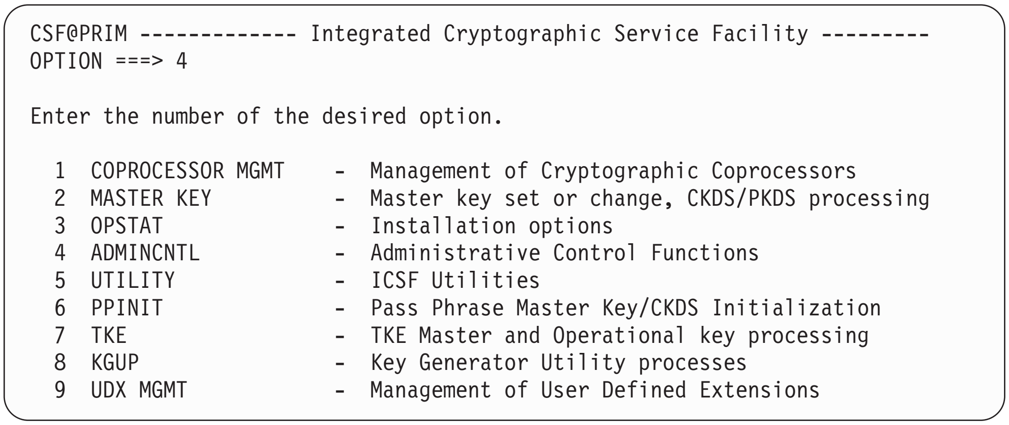
3. Type a 'D' to the left of the functions you want disabled and press ENTER.

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:

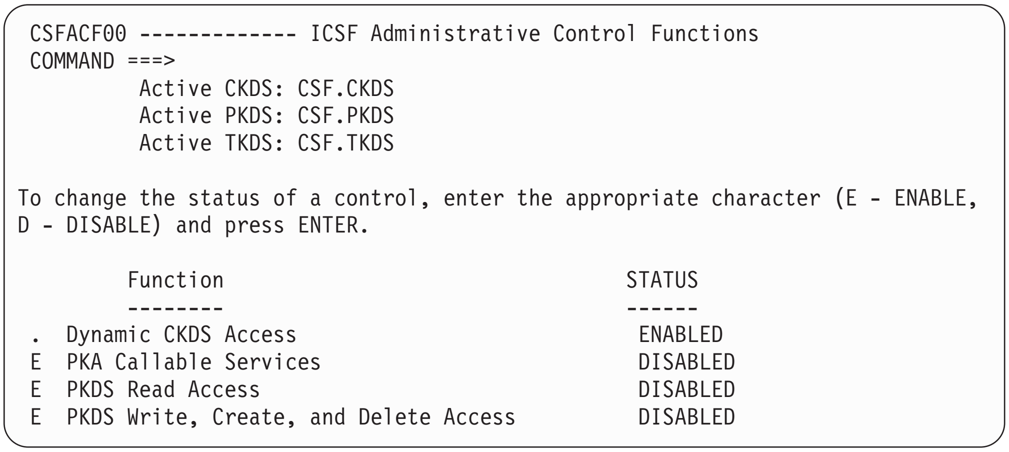
1. From TSO/E, access the user control functions by choosing option 4, ADMINCNTL, on the Primary Menu panel of ICSF, as shown in Figure 197.



```
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 197. Selecting the Administrative Control Option on the ICSF Primary Menu Panel

2. The Administrative Control Function panel appears. See Figure 198 on page 231.



```
 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 198. 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 160 and “Operational Keys” on page 175). Select the asymmetric master key and then select **Clear**.

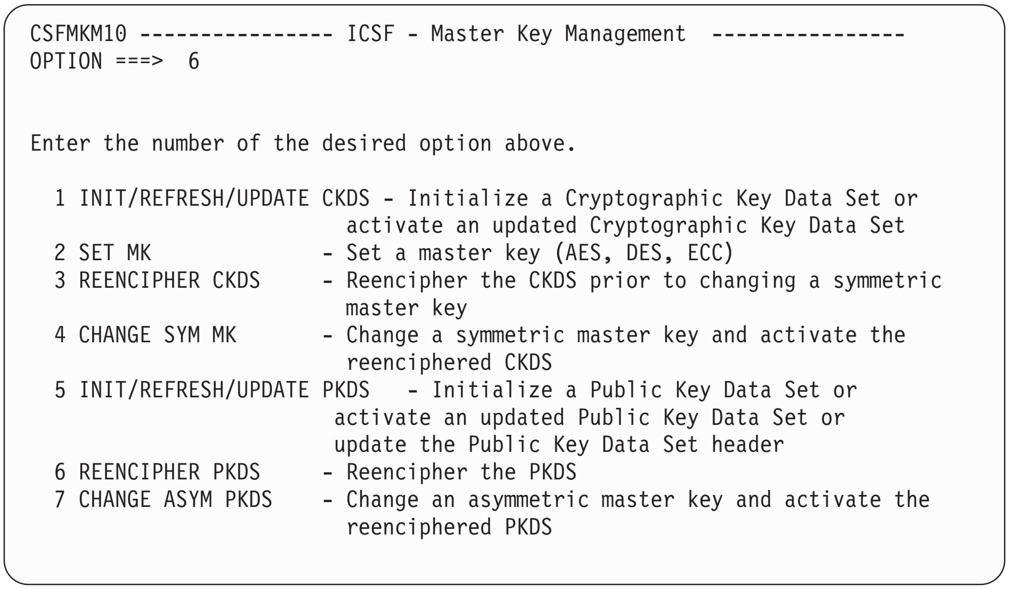
Notes:

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 198 and “Installing RSA Keys in the PKDS from a Data Set” on page 239 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.

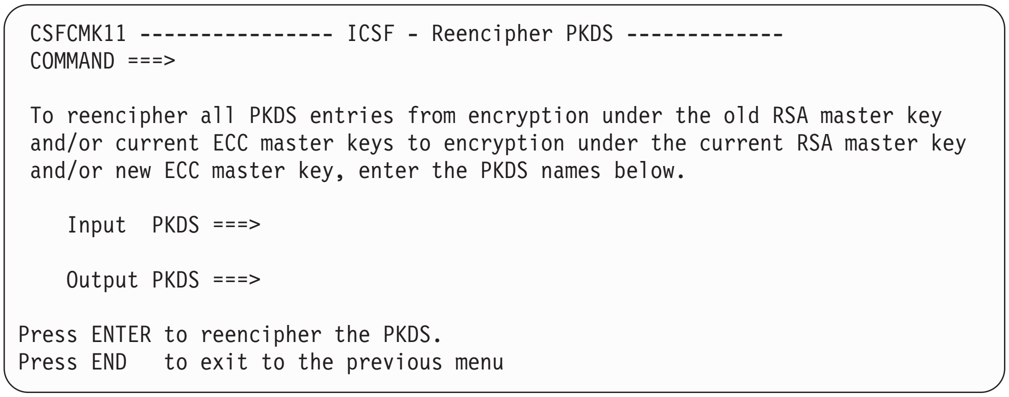


```
CSFMKM10 ---------------- ICSF - Master Key Management  ----------------
OPTION ===>  6


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 199. 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.

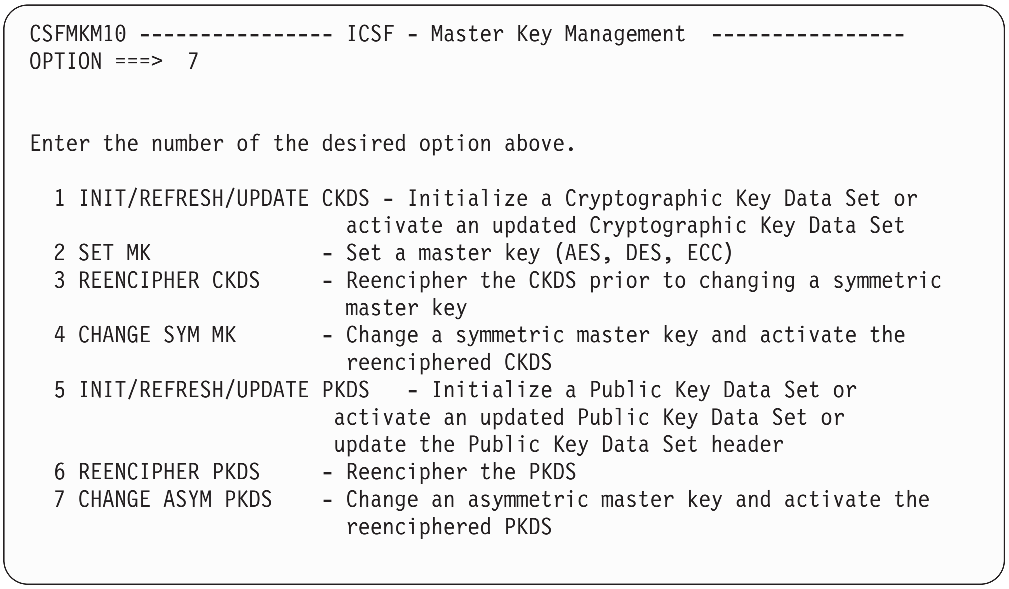
In the Output PKDS field, specify the name of an empty VSAM data set. ICSF writes the reenciphered keys in this data set.



```
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 200. Reencipher PKDS

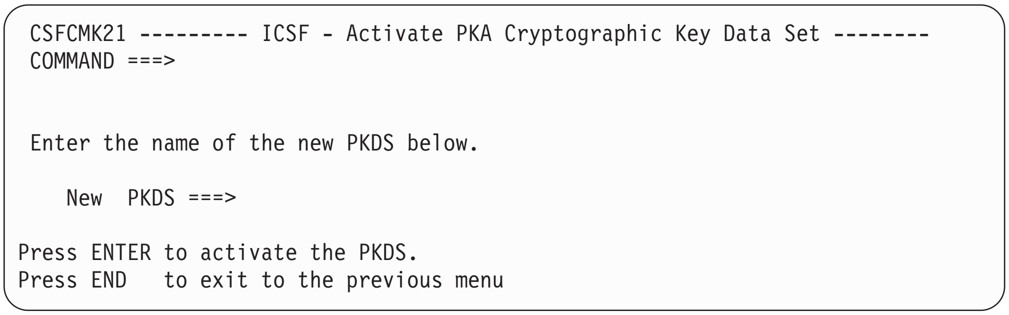
Press enter to reencipher the PKDS. Once successful, you will then want to refresh the PKDS. Return to the Master Key Management panel and select option 5.



```
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 201. 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 202. Refresh PKDS

After you press ENTER, the PKDS becomes active.

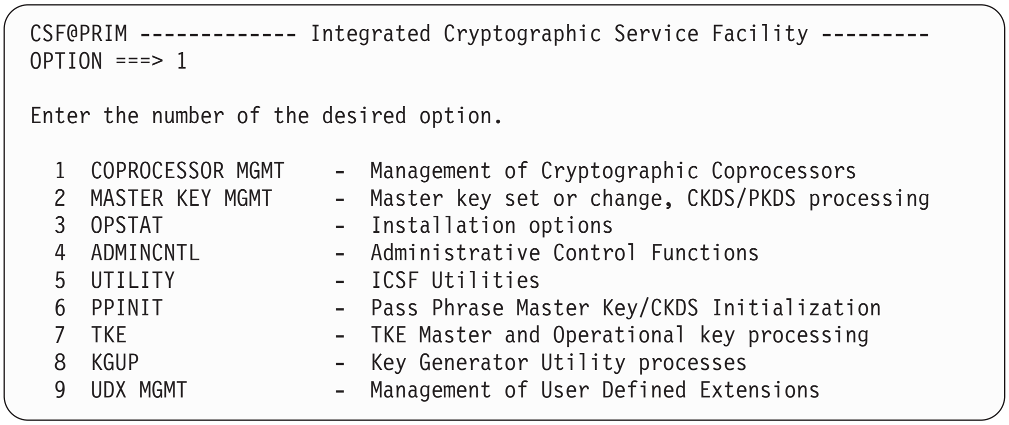
Loading Operational Keys to the CKDS

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:

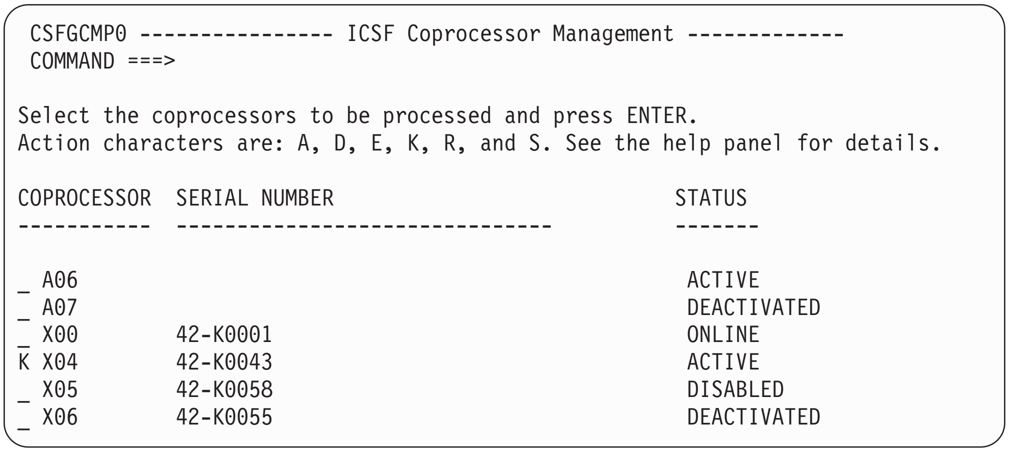
1. Select option 1, `COPROCESSOR MGMT`, on the primary menu panel



```
 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 203. ICSF Primary Menu Panel

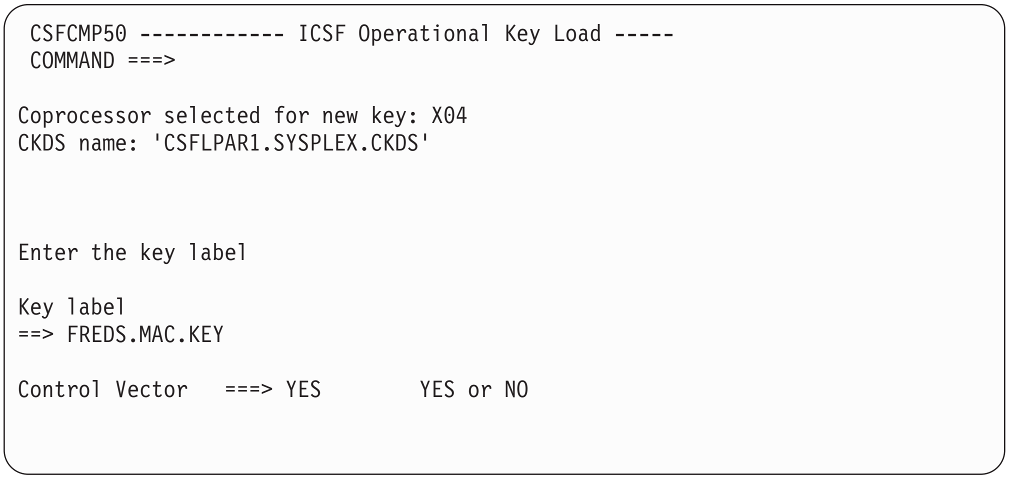
2. The Coprocessor Management panel appears. Put a 'K' by the coprocessor that contains the key part register to load.



```
 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 204. 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.



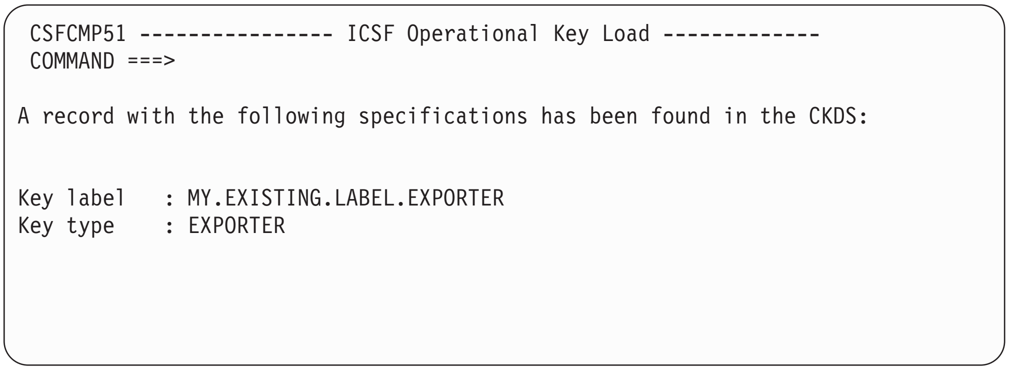
```
 CSFCMP50 ------------ ICSF Operational Key Load -----
 COMMAND ===>

Coprocessor selected for new key: X04
CKDS name: 'CSFLPAR1.SYSPLEX.CKDS'



Enter the key label

Key label
==> FREDS.MAC.KEY

Control Vector   ===> YES        YES or NO
```

Figure 205. 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 180.

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.

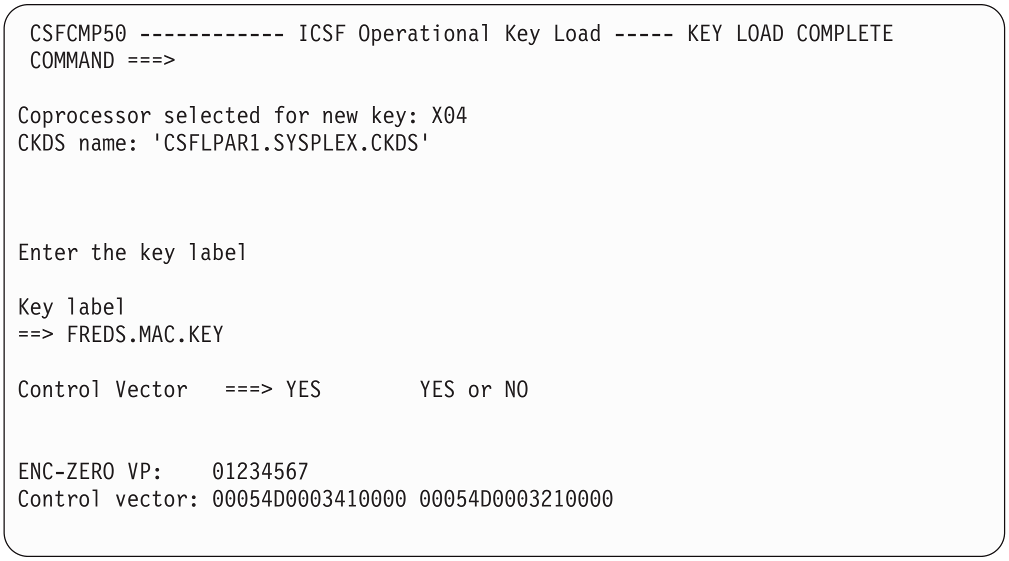
If a record already exists in the CKDS with a label that matches the key label specified, the Operational Key Load panel appears alerting you that CKDS RECORD EXISTS. If you want to replace the existing key with the new key you are trying to load, press ENTER.



```
 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
```

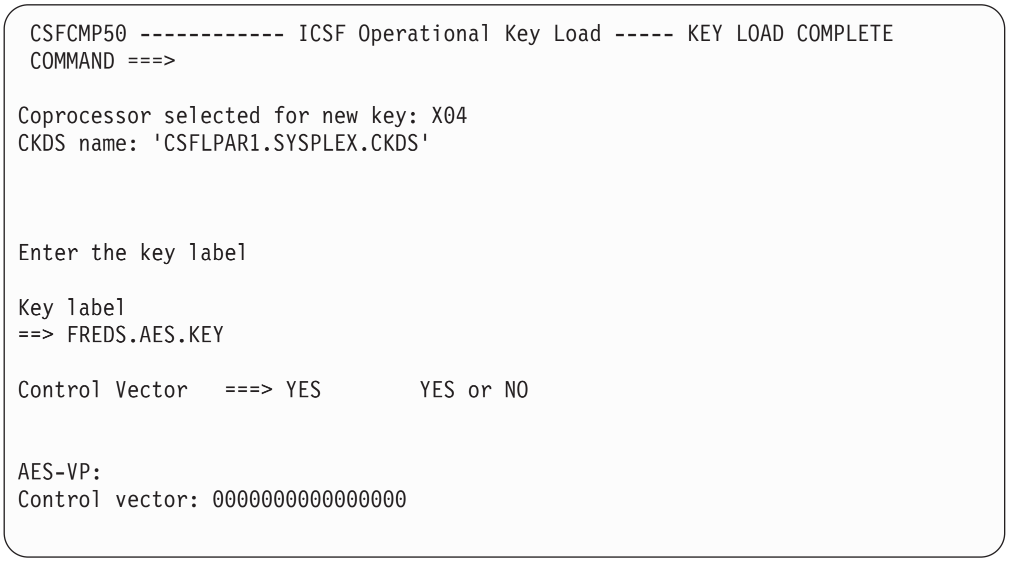
Figure 206. Operational Key Load Panel

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 ===>

Coprocessor selected for new key: X04
CKDS name: 'CSFLPAR1.SYSPLEX.CKDS'



Enter the key label

Key label
==> FREDS.MAC.KEY

Control Vector   ===> YES        YES or NO


ENC-ZERO VP:    01234567
Control vector: 00054D0003410000 00054D0003210000
```

Figure 207. Operational Key Load Panel - ENC-ZERO and CV values displayed



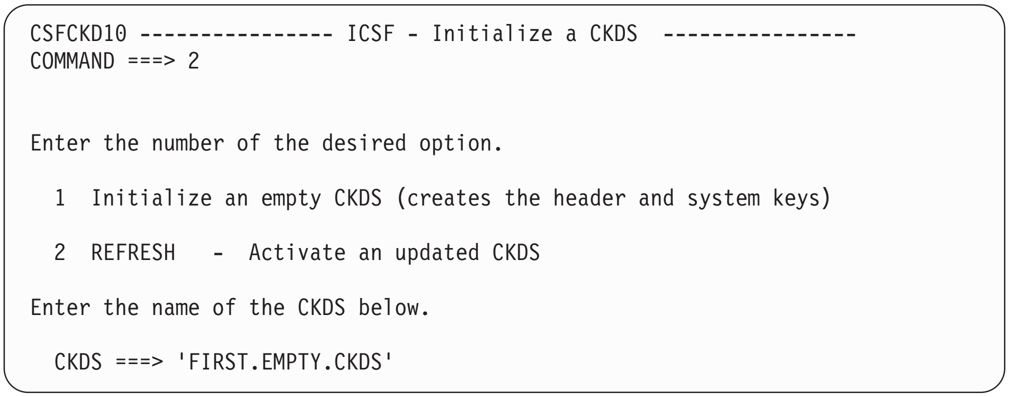
```
 CSFCMP50 ------------ ICSF Operational Key Load ----- KEY LOAD COMPLETE
 COMMAND ===>

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 208. 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 209.



```
 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 209. 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.

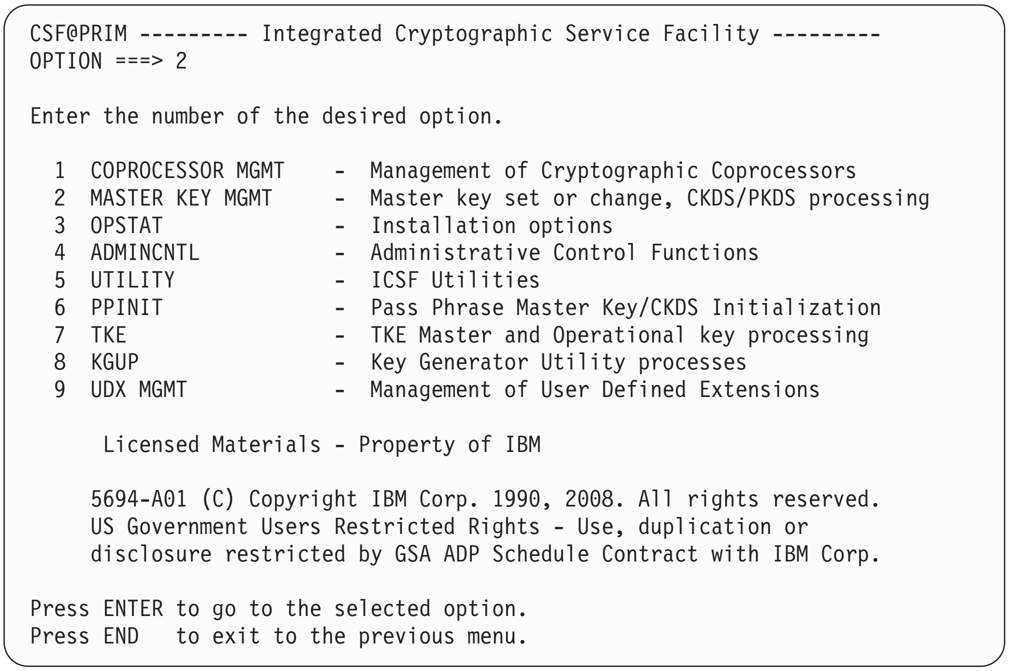
4. Press END to return to the Primary Menu panel.

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:

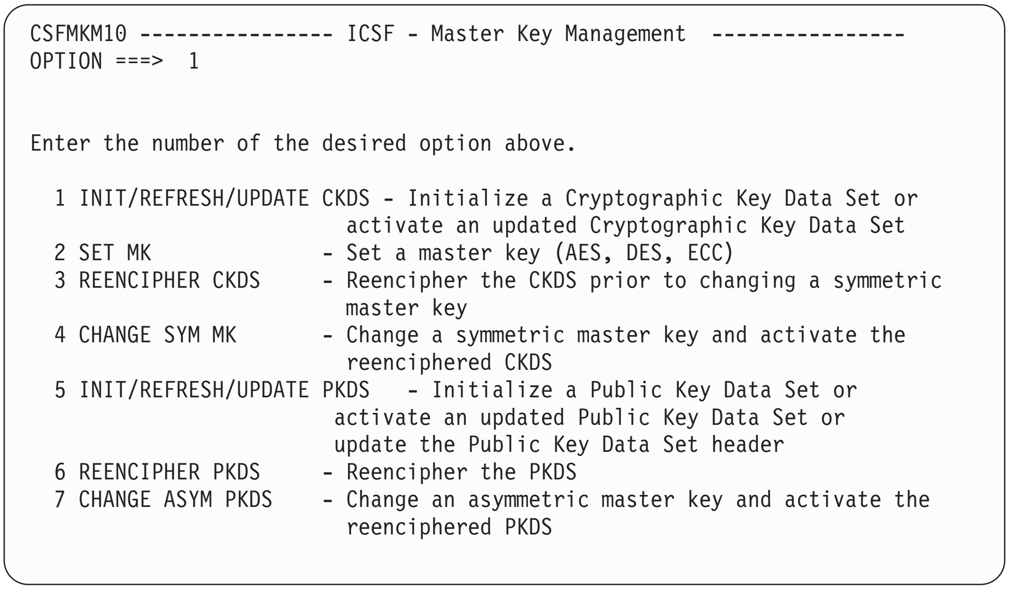
1. Load the new AES master key by using the master key entry panels or by using TKE. The AES master key must be loaded on all active coprocessors.
2. From the Primary Menu, select option 2, MASTER KEY MGMT:



```
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 210. Selecting the Master Key option on the primary menu panel

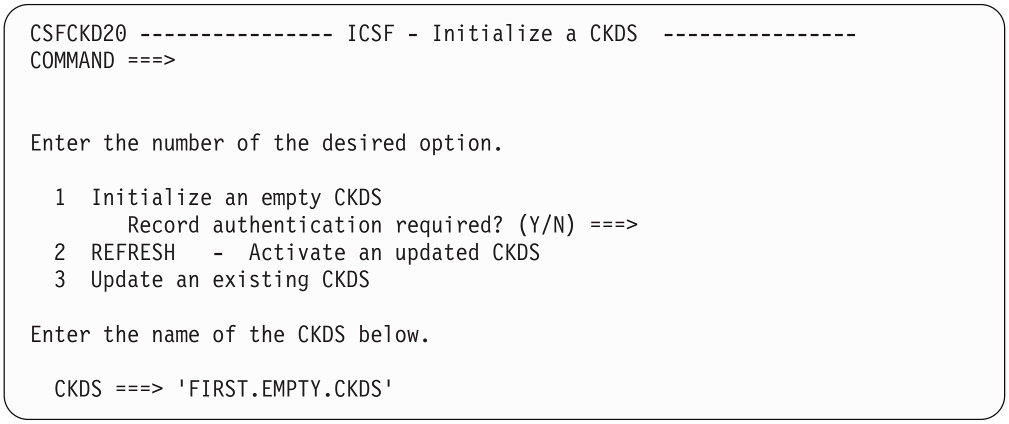
3. Select option 1, INIT/REFERSH/UPDATE CKDS.



```
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 211. ICSF Master Key Management Panel

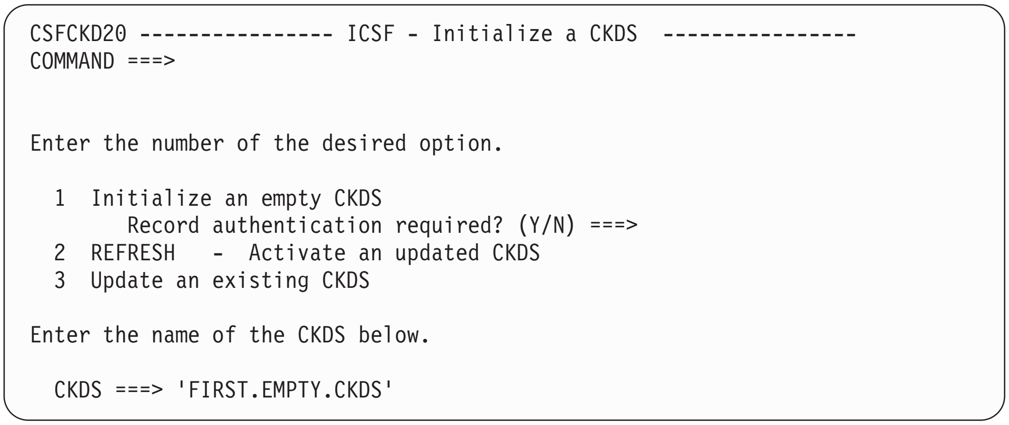
4. The Initialize a CKDS panel appears. In the CKDS field, enter the name of an existing, initialized CKDS.



```
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 212. 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'
```

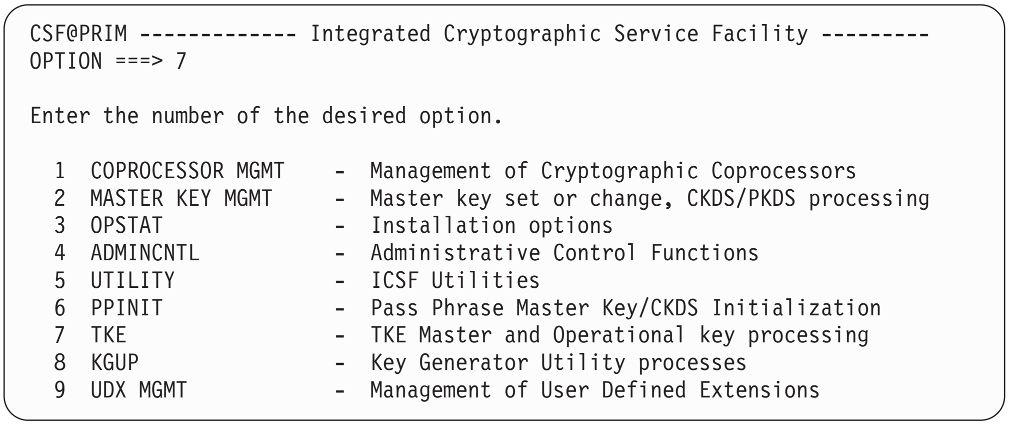
Figure 213. ICSF Initialize a CKDS Panel

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 233), you load it from the data set to the PKDS by this method.

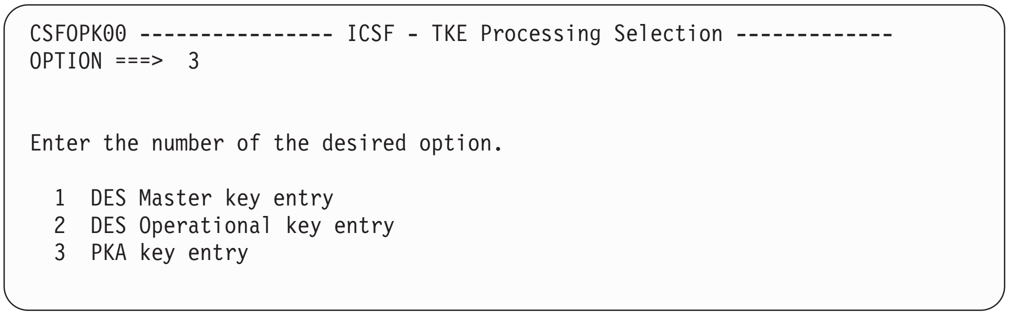
1. Select Option 7, TKE, on the ICSF Primary Option Menu.



```
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 214. Selecting the TKE Option on the ICSF Primary Menu Panel

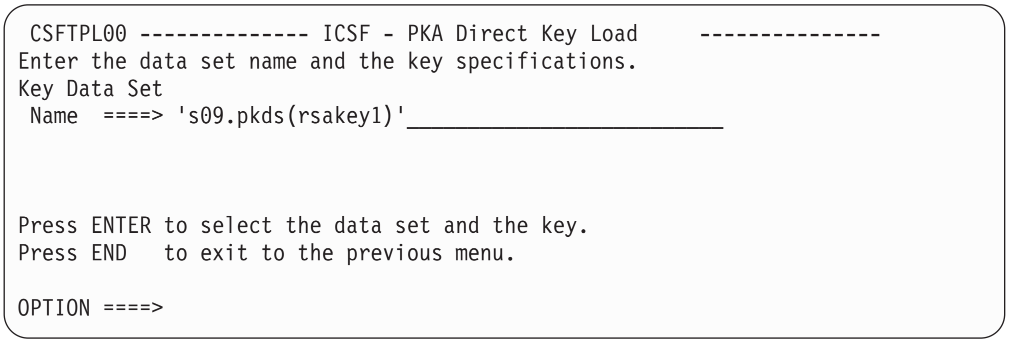
2. The TKE Processing Selection panel appears. Select option 3.



```
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 215. 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 216. 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 87.

To start CNM, click with the left mouse button on the "Trusted Key Entry" link in the left-hand panel of the main Trusted Key Entry Console page. Then, under the "Applications" section displayed in the right-hand panel, click with the left mouse button on "Cryptographic Node Management Utility".

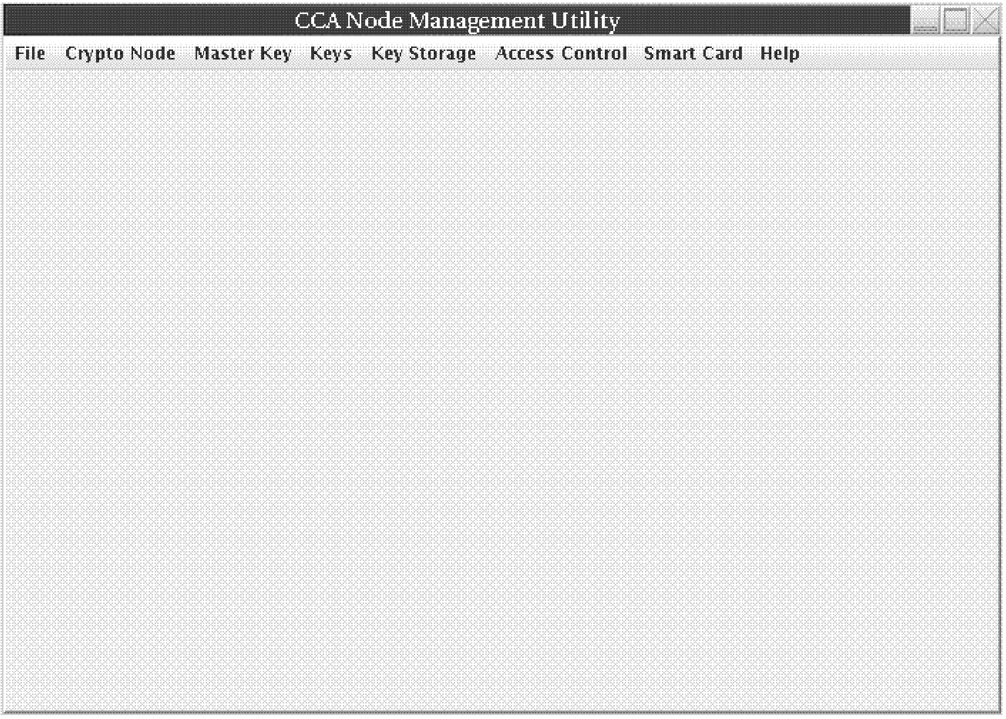


Figure 217. CNM main window

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.

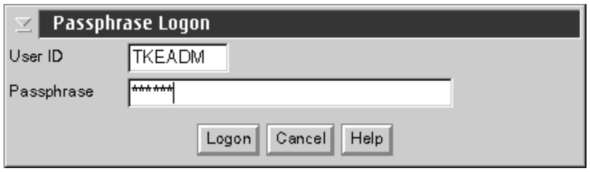
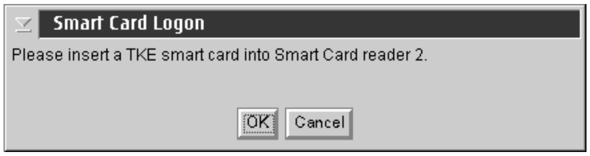


Figure 218. Passphrase logon prompt

Smart Card Logon

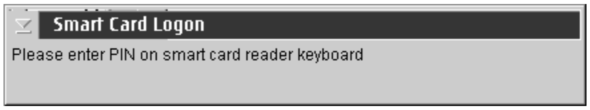
When you click on the CNM Utility's Smart Card Logon button, you will be prompted to insert your TKE smart card into smart card reader 2 and to enter your PIN.

Note: Smart card support must be activated in CNM before logon with a TKE smart card is available.



Please insert a TKE smart card into Smart Card reader 2.

Figure 219. TKE smart card prompt



Please enter PIN on smart card reader keyboard

Figure 220. 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 box will prompt you to enter a group profile name for Group ID. Profile names are case sensitive.

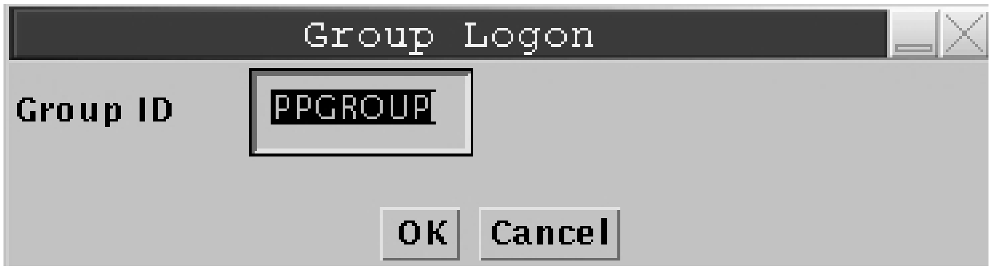


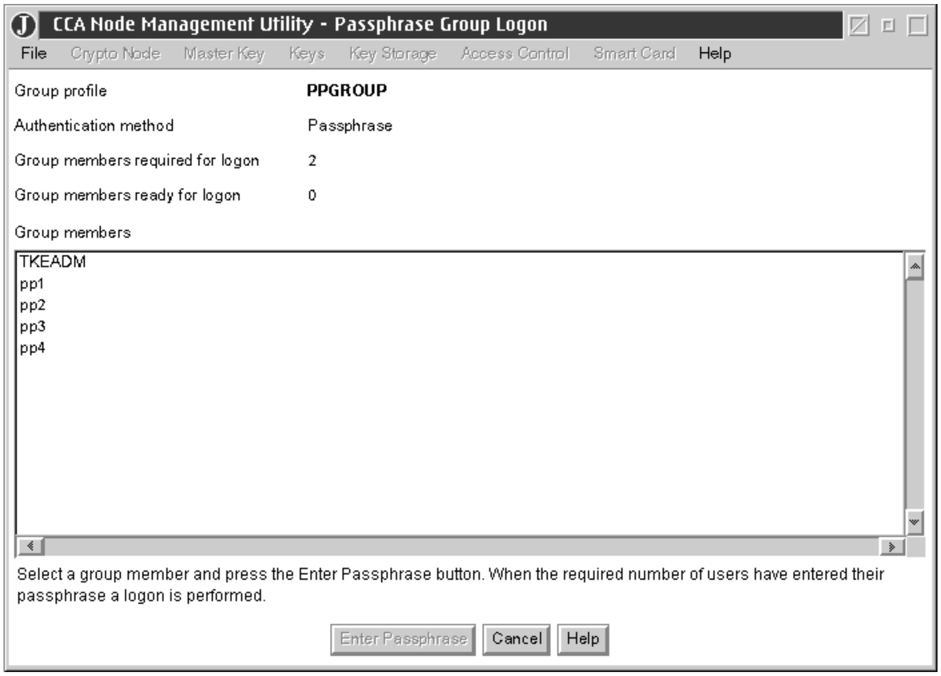
Figure 221. Passphrase group logon - group member list

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.



Group profile PPGROUP

Authentication method Passphrase

Group members required for logon 2

Group members ready for logon 0

Group members

TKEADM
pp1
pp2
pp3
pp4

Select a group member and press the Enter Passphrase button. When the required number of users have entered their passphrase a logon is performed.

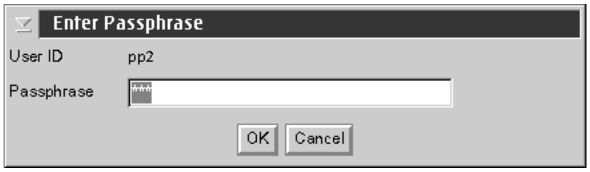
Figure 222. Group logon prompt

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 who 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.

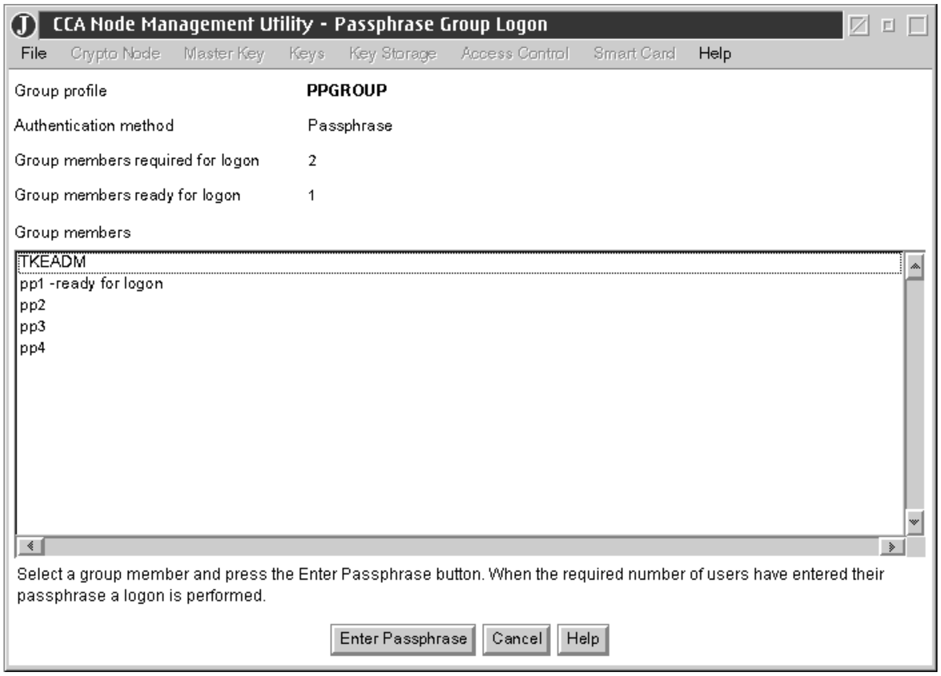


User ID pp2

Passphrase ****

Figure 223. 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.



Group profile PPGROUP

Authentication method Passphrase

Group members required for logon 2

Group members ready for logon 1

Group members

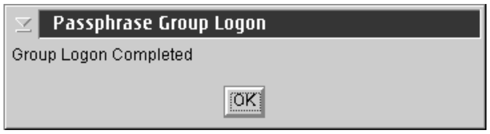
TKEADM
pp1 -ready for logon
pp2
pp3
pp4

Select a group member and press the Enter Passphrase button. When the required number of users have entered their passphrase a logon is performed.

Figure 224. 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.



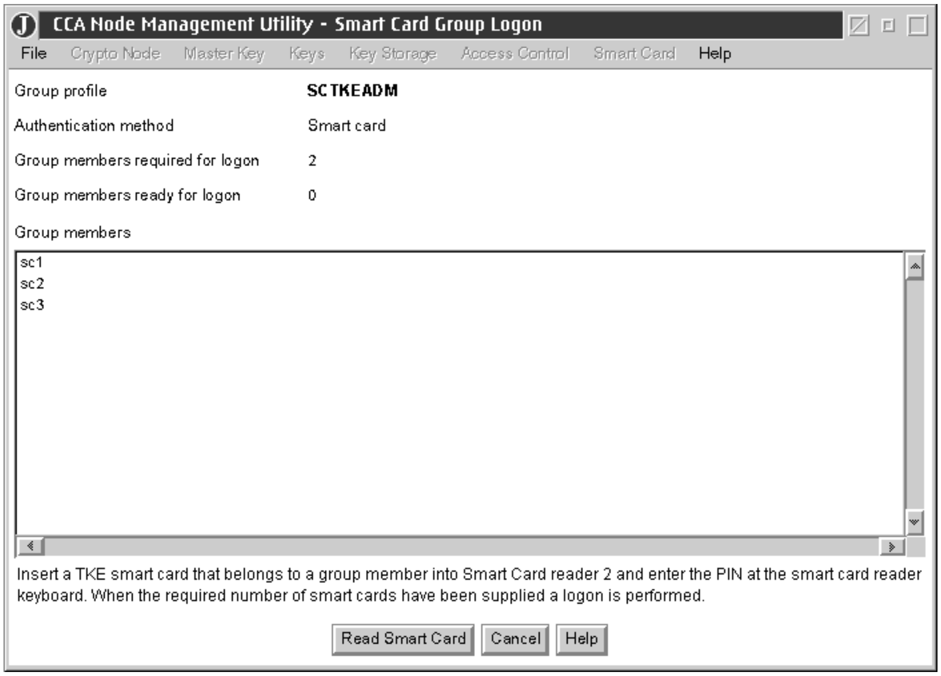
Group Logon Completed

Figure 225. 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.



Group profile SCTKEADM

Authentication method Smart card

Group members required for logon 2

Group members ready for logon 0

Group members

sc1
sc2
sc3

Insert a TKE smart card that belongs to a group member into Smart Card reader 2 and enter the PIN at the smart card reader keyboard. When the required number of smart cards have been supplied a logon is performed.

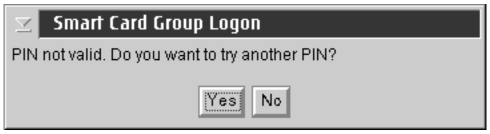
Figure 226. Smart card group logon window

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 who 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.

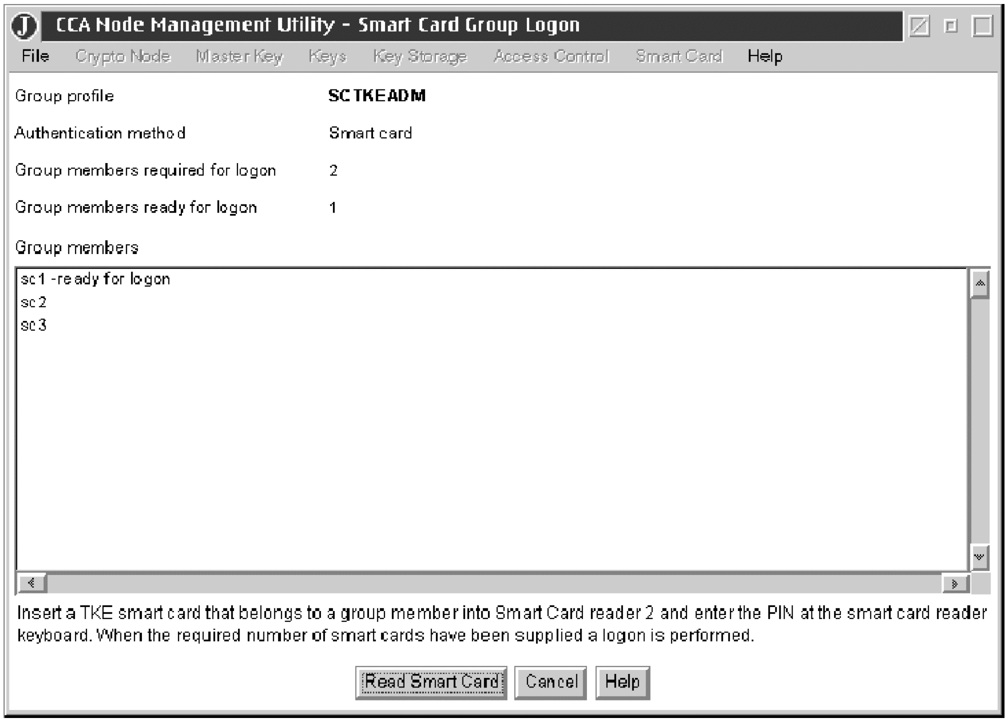
Group members ready for logon is the number of users who have signed the logon with their TKE smart card and PIN. This counter is incremented each time a user signs the logon.

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.



PIN not valid. Do you want to try another PIN?

Figure 227. Smart card group logon — retry PIN prompt



Group profile SCTKEADM

Authentication method Smart card

Group members required for logon 2

Group members ready for logon 1

Group members

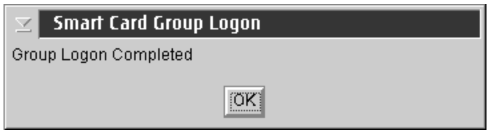
sc1 -ready for logon
sc2
sc3

Insert a TKE smart card that belongs to a group member into Smart Card reader 2 and enter the PIN at the smart card reader keyboard. When the required number of smart cards have been supplied a logon is performed.

Figure 228. 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 the Smart Card Utility Program (SCUP). (Refer to “Unblock PIN on a TKE smart card” on page 297.)

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.



Group Logon Completed

Figure 229. 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

CNI Editor

The CNI Editor is a utility within the CNM Utility that is used to create CNI scripts to automate some of the functions of CNM.

Enable Smart Card Readers

This option enables smart card readers. This not only enables smart card readers for CNM, but also for other TKE applications.

Exit

Exit the CNM application.

Exit and Logoff

To log off 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.

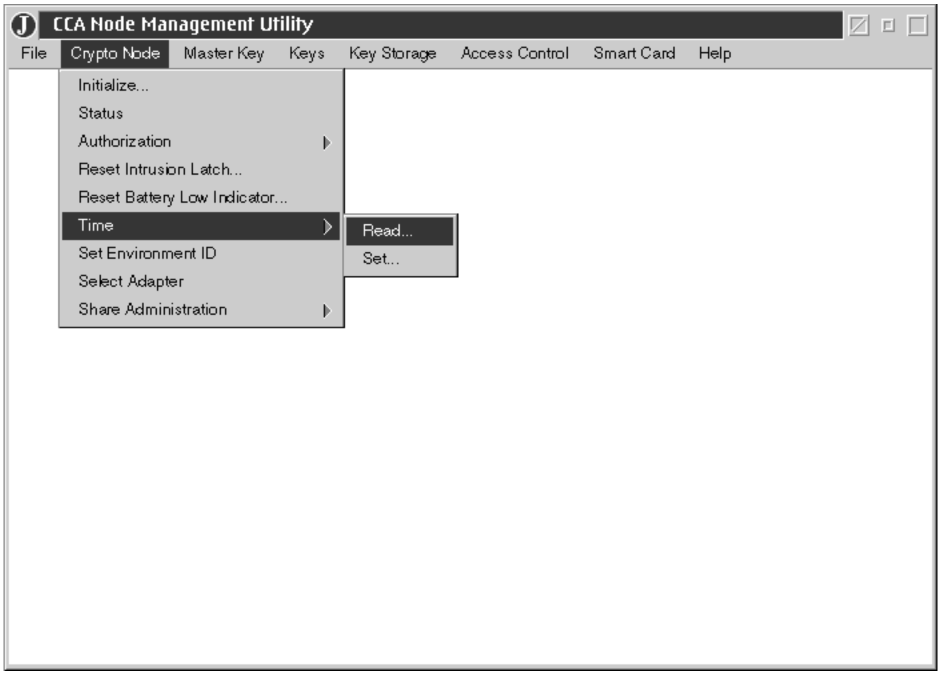


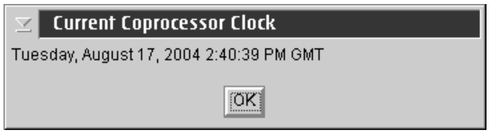
Figure 230. CNM main window — Crypto Node Time sub-menu

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).



Tuesday, August 17, 2004 2:40:39 PM GMT

Figure 231. Current Coprocessor Clock

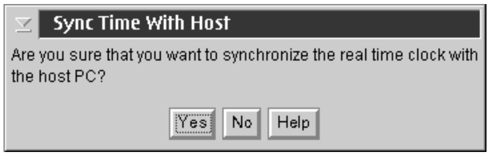
3. Finish the task by selecting **OK**.

Synchronize Clock-Calendar

To synchronize the TKE crypto adapter clock-calendar with the TKE workstation clock:

Note: If not already logged on, log on 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.



Are you sure that you want to synchronize the real time clock with the host PC?

Figure 232. 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 log on 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.

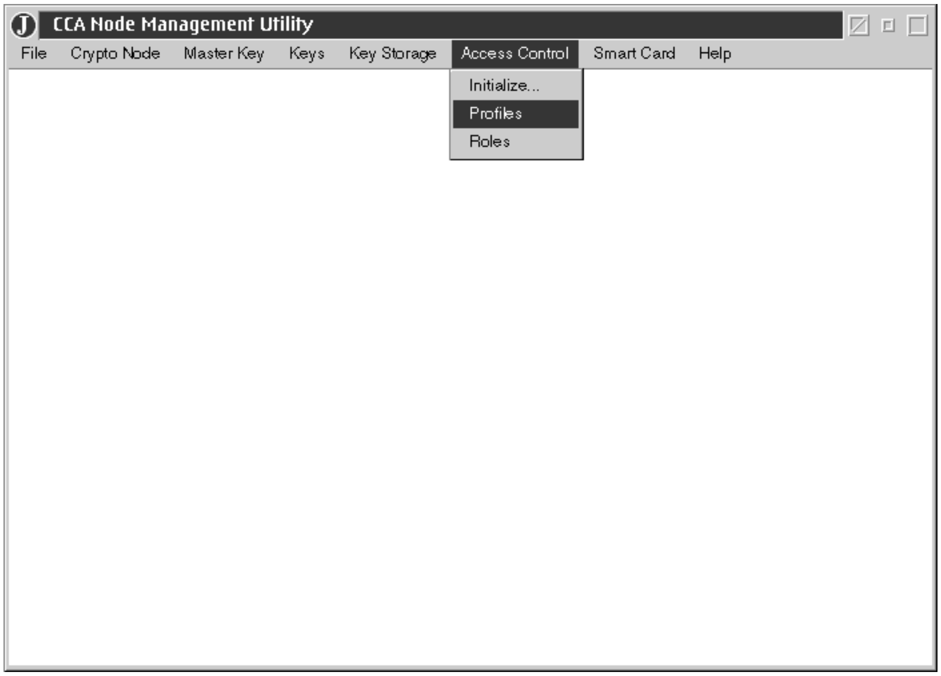


Figure 233. CNM main window — Access Control menu

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:

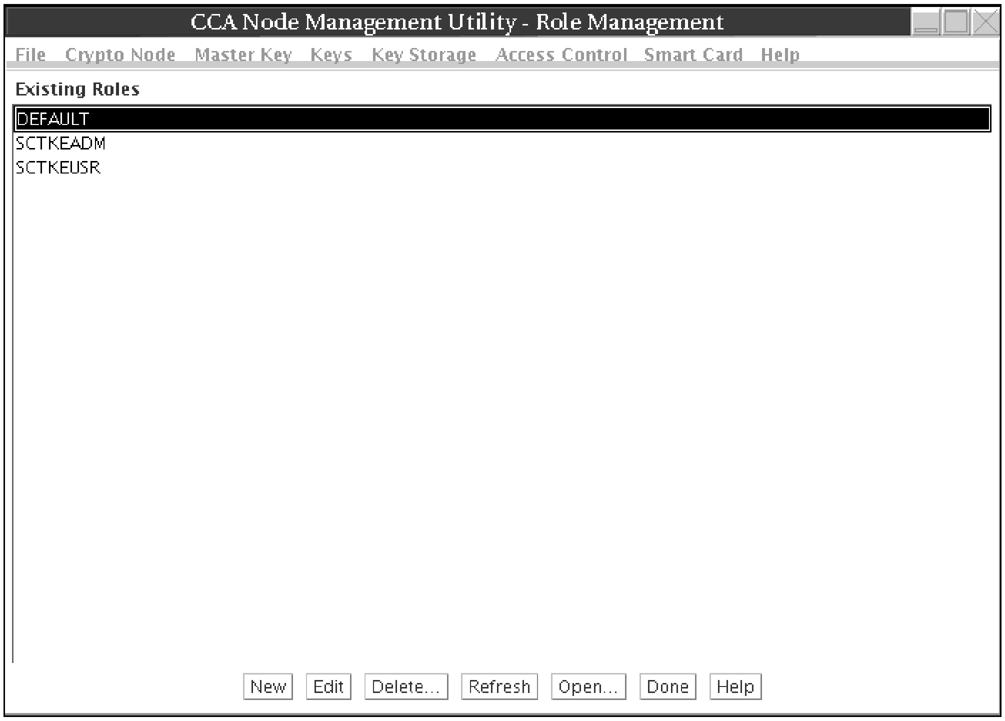
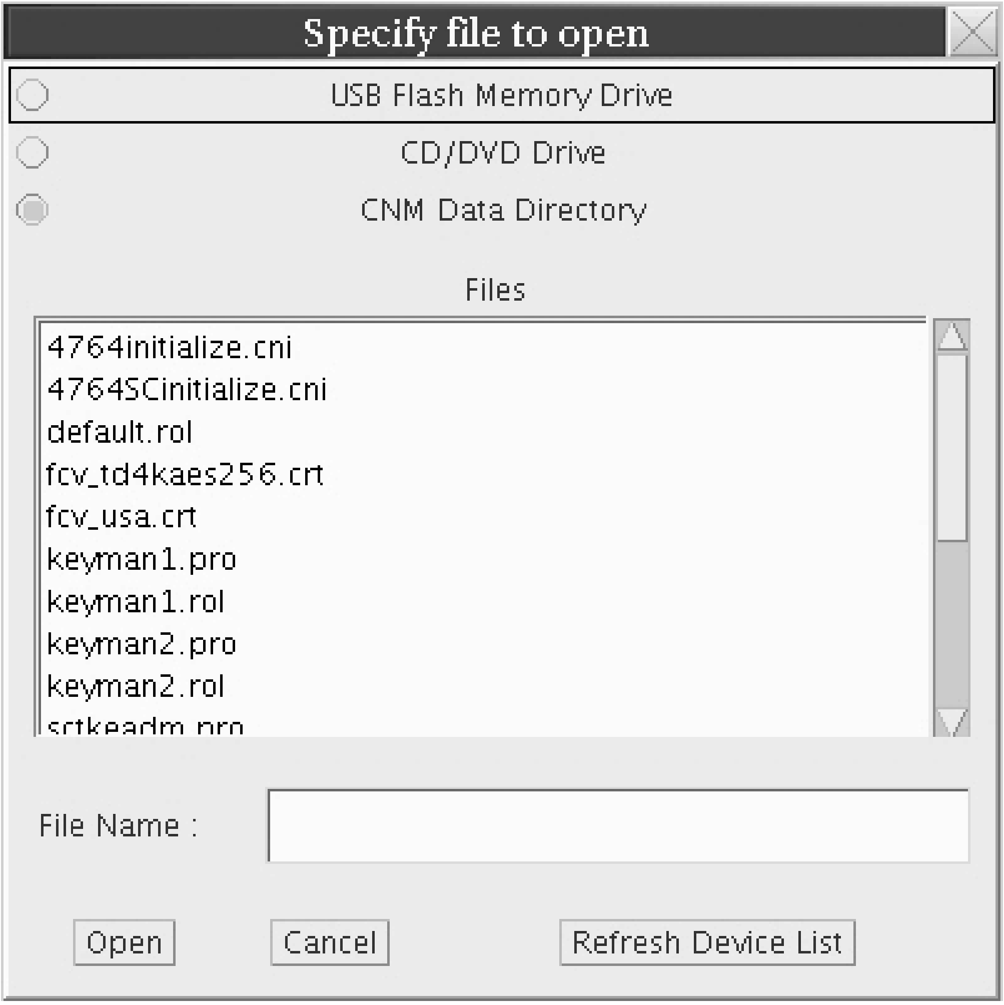

CCA Node Management Utility - Role Management
File Crypto Node Master Key Keys Key Storage Access Control Smart Card Help
Existing Roles
DEFAULT
SCTKEADM
SCTKEUSR
New
Edit
Delete...
Refresh
Open...
Done
Help

Figure 234. 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.



Specify file to open

○ USB Flash Memory Drive

○ CD/DVD Drive

● CNM Data Directory

Files

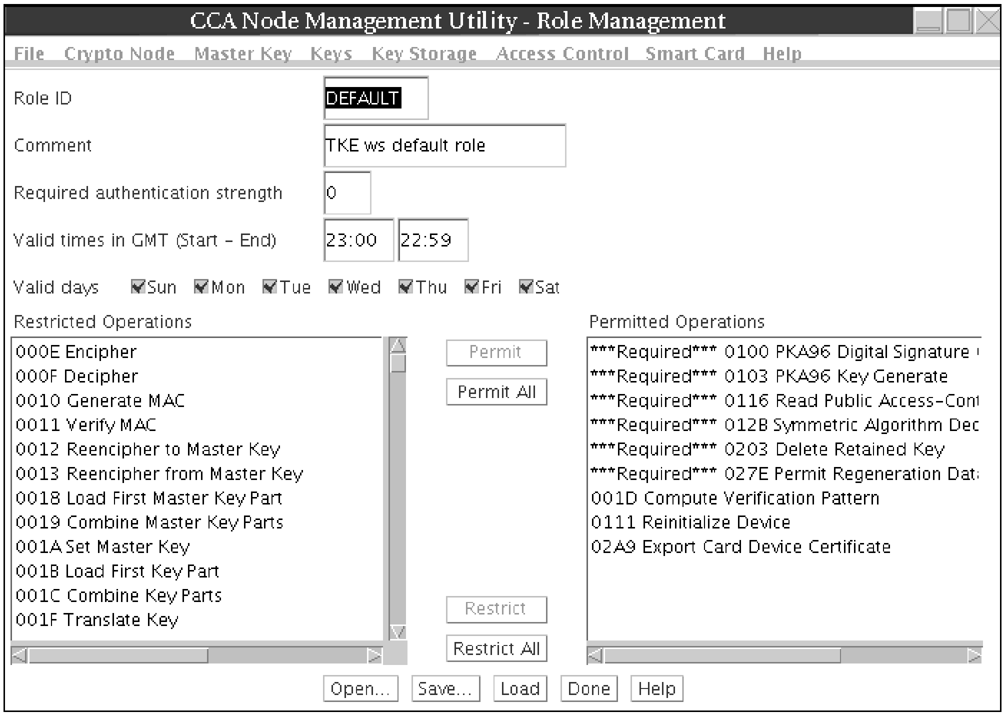
```
4764initialize.cni
4764SCinitialize.cni
default.rol
fcv_td4kaes256.crt
fcv_usa.crt
keyman1.pro
keyman1.rol
keyman2.pro
keyman2.rol
sctkeadm.pro
```

File Name :

Figure 235. 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.


CCA Node Management Utility - Role Management
File Crypto Node Master Key Keys Key Storage Access Control Smart Card Help
Permit
Permit All
Restrict
Restrict All
Open...
Save...
Load
Done
Help

Role ID: DEFAULT

Comment: TKE ws default role

Required authentication strength: 0

Valid times in GMT (Start – End): 23:00 22:59

Valid days ☑Sun ☑Mon ☑Tue ☑Wed ☑Thu ☑Fri ☑Sat

Restricted Operations

```
000E Encipher
000F Decipher
0010 Generate MAC
0011 Verify MAC
0012 Reencipher to Master Key
0013 Reencipher from Master Key
0018 Load First Master Key Part
0019 Combine Master Key Parts
001A Set Master Key
001B Load First Key Part
001C Combine Key Parts
001F Translate Key
```

Permitted Operations

```
***Required*** 0100 PKA96 Digital Signature
***Required*** 0103 PKA96 Key Generate
***Required*** 0116 Read Public Access-Cont
***Required*** 012B Symmetric Algorithm Dec
***Required*** 0203 Delete Retained Key
***Required*** 027E Permit Regeneration Dat
001D Compute Verification Pattern
0111 Reinitialize Device
02A9 Export Card Device Certificate
```

Figure 236. 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.

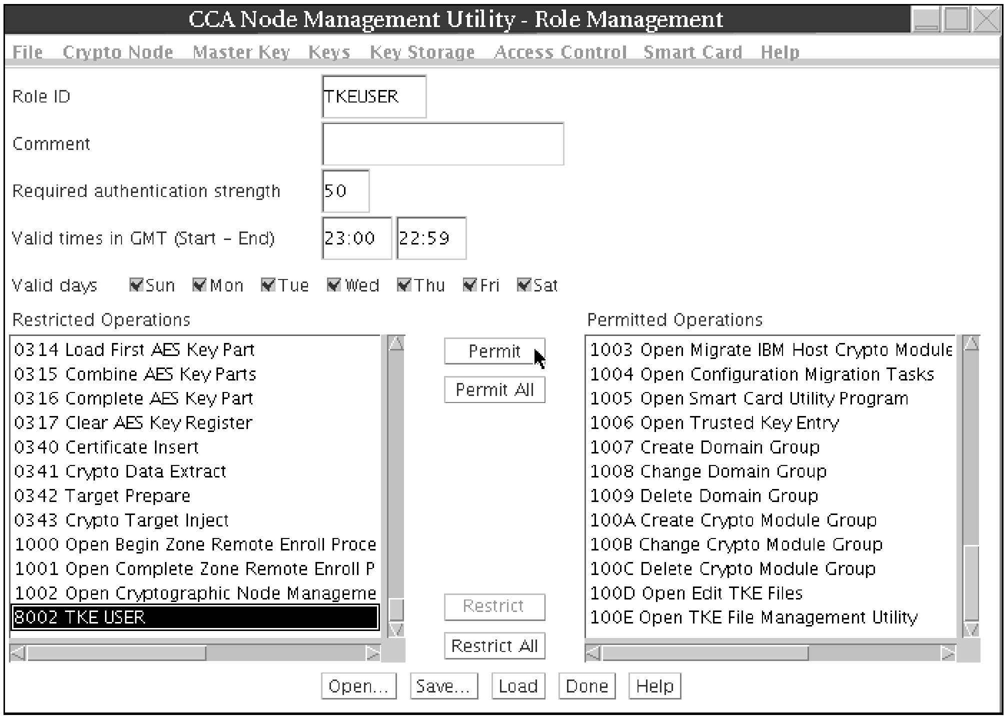
Edit a role loaded in the TKE crypto adapter

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 recommend not 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 7.1, you may need to add access control points to your roles. See Chapter 3, “TKE migration overview,” on page 41.


CCA Node Management Utility - Role Management
File Crypto Node Master Key Keys Key Storage Access Control Smart Card Help
Permit
Permit All
Restrict
Restrict All
Open... Save... Load Done Help

Role ID TKEUSER

Comment

Required authentication strength 50

Valid times in GMT (Start – End) 23:00 22:59

Valid days ☑Sun ☑Mon ☑Tue ☑Wed ☑Thu ☑Fri ☑Sat

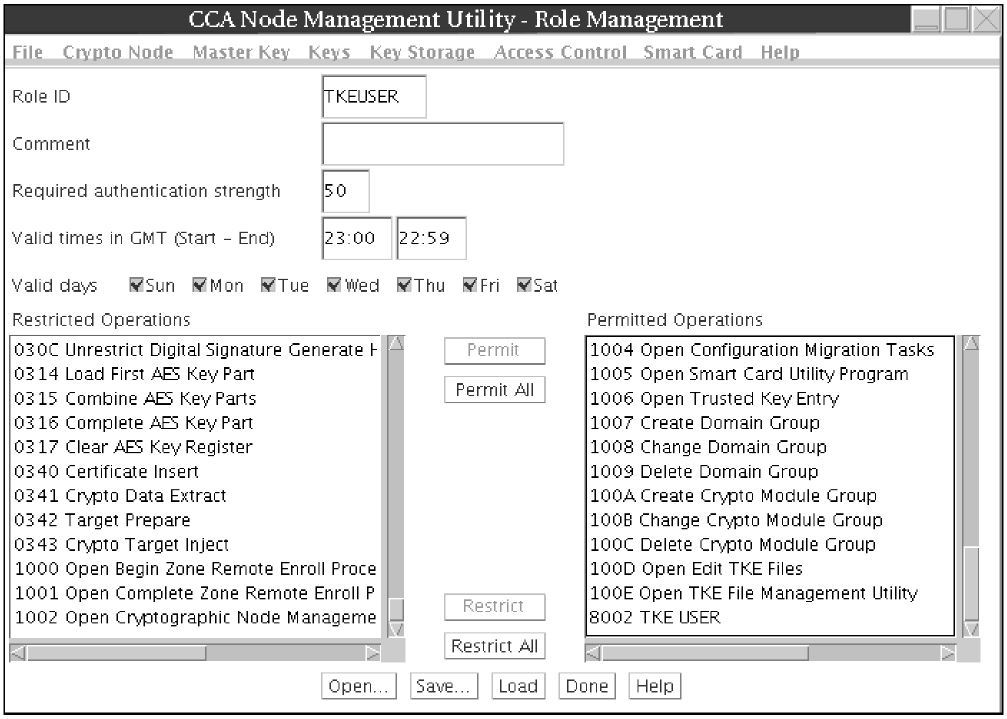
Restricted Operations

0314 Load First AES Key Part
0315 Combine AES Key Parts
0316 Complete AES Key Part
0317 Clear AES Key Register
0340 Certificate Insert
0341 Crypto Data Extract
0342 Target Prepare
0343 Crypto Target Inject
1000 Open Begin Zone Remote Enroll Proce
1001 Open Complete Zone Remote Enroll P
1002 Open Cryptographic Node Manageme
8002 TKE USER

Permitted Operations

1003 Open Migrate IBM Host Crypto Module
1004 Open Configuration Migration Tasks
1005 Open Smart Card Utility Program
1006 Open Trusted Key Entry
1007 Create Domain Group
1008 Change Domain Group
1009 Delete Domain Group
100A Create Crypto Module Group
100B Change Crypto Module Group
100C Delete Crypto Module Group
100D Open Edit TKE Files
100E Open TKE File Management Utility

Figure 237. Edit a role - highlight access point to permit


CCA Node Management Utility - Role Management
File Crypto Node Master Key Keys Key Storage Access Control Smart Card Help
Permit
Permit All
Restrict
Restrict All
Open... Save... Load Done Help

Role ID TKEUSER

Comment

Required authentication strength 50

Valid times in GMT (Start – End) 23:00 22:59

Valid days ☑Sun ☑Mon ☑Tue ☑Wed ☑Thu ☑Fri ☑Sat

Restricted Operations

030C Unrestrict Digital Signature Generate H
0314 Load First AES Key Part
0315 Combine AES Key Parts
0316 Complete AES Key Part
0317 Clear AES Key Register
0340 Certificate Insert
0341 Crypto Data Extract
0342 Target Prepare
0343 Crypto Target Inject
1000 Open Begin Zone Remote Enroll Proce
1001 Open Complete Zone Remote Enroll P
1002 Open Cryptographic Node Manageme

Permitted Operations

1004 Open Configuration Migration Tasks
1005 Open Smart Card Utility Program
1006 Open Trusted Key Entry
1007 Create Domain Group
1008 Change Domain Group
1009 Delete Domain Group
100A Create Crypto Module Group
100B Change Crypto Module Group
100C Delete Crypto Module Group
100D Open Edit TKE Files
100E Open TKE File Management Utility
8002 TKE USER

Figure 238. 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 334.

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.

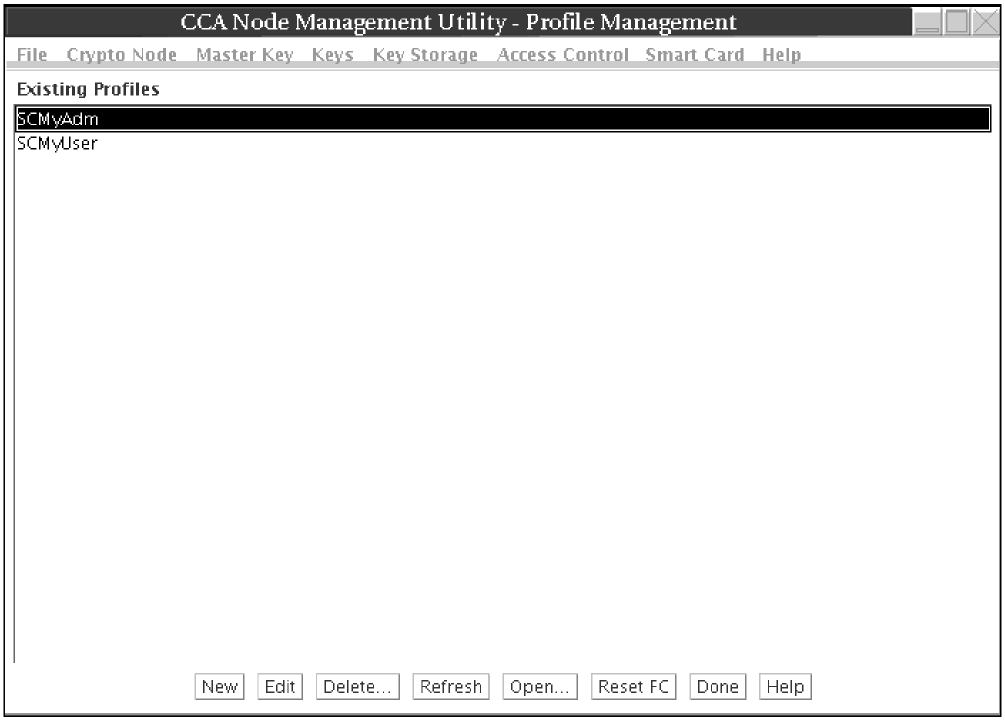

CCA Node Management Utility - Profile Management
File Crypto Node Master Key Keys Key Storage Access Control Smart Card Help
Existing Profiles
SCMyAdm
SCMyUser
New
Edit
Delete...
Refresh
Open...
Reset FC
Done
Help

Figure 239. Profile management panel — profile list

Passphrase profiles

TKE supplies the following predefined profiles:

TKEUSER Associated with role TKEUSER. Use this profile for logging onto the TKE application and performing TKE functions.

TKEADM Associated with role TKEADM. Use this profile for managing the TKE crypto adapter using CNM, including defining roles/profiles

KEYMAN1 Associated with role KEYMAN1. Use this profile to load the first master key part to the TKE crypto adapter new master key register

KEYMAN2 Associated with role KEYMAN2. Use this profile to load any middle and last master key parts to the TKE crypto adapter new master key register, set the master key and reencipher key storage.

Smart card profiles

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.

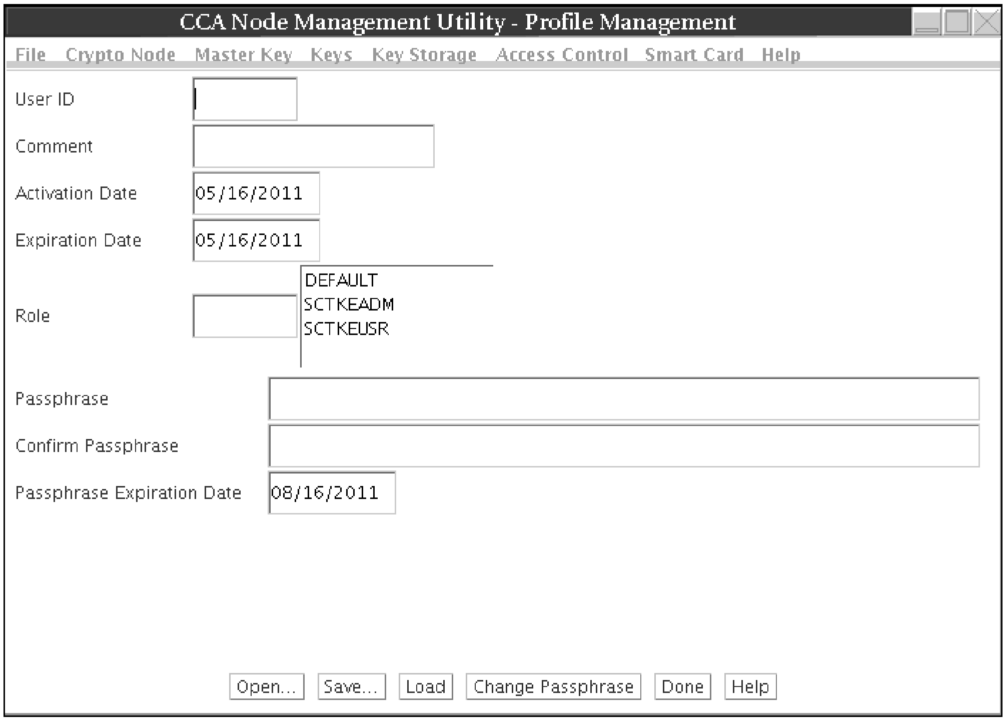
2. Select **New** to define a new user profile. A dialog is displayed, enabling you to select the profile type – either **Passphrase**, **Smart card** or **Group**. Select the type of profile you want to define, and press **Continue**.

Depending on your choice, see the following topics:

- "Define a Passphrase Profile"
- "Define a Smart Card Profile" on page 257
- "Define a Group Profile" on page 260

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.



CCA Node Management Utility - Profile Management

User ID

Comment

Activation Date 05/16/2011

Expiration Date 05/16/2011

Role

DEFAULT
SCTKEADM
SCTKEUSR

Passphrase

Confirm Passphrase

Passphrase Expiration Date 08/16/2011

Figure 240. 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 log on. This field defaults to the current date. Change this date as appropriate.

Expiration Date
Determines the last date when the user can log on. 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.

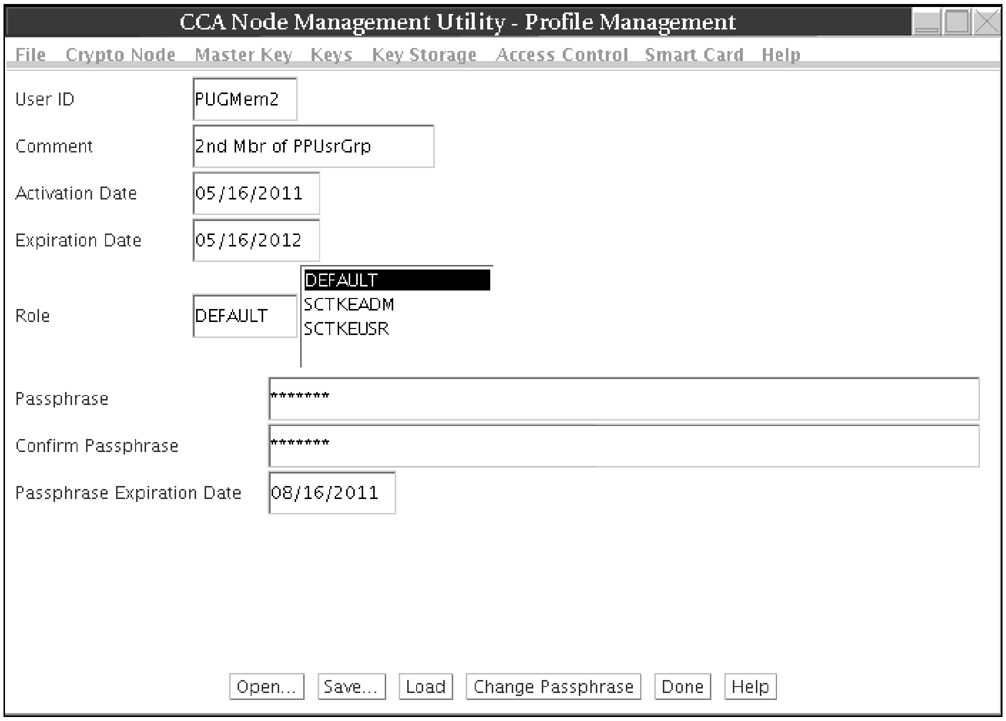
Passphrase The character string that the user must enter to log on to the TKE cryptographic adapter. The passphrase must:

- 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.



User ID PUGMem2

Comment 2nd Mbr of PPUsrGrp

Activation Date 05/16/2011

Expiration Date 05/16/2012

Role DEFAULT

DEFAULT
SCTKEADM
SCTKEUSR

Passphrase ********

Confirm Passphrase ********

Passphrase Expiration Date 08/16/2011

Figure 241. Profile Management panel — Passphrase profile fields filled in

3. Select **Save** to save the profile to disk.

   Warnings:

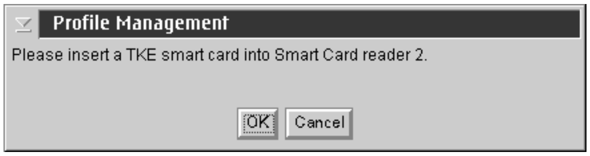
   a. If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “TKE Media Manager” on page 334.
   b. Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or 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 **Done** to return to the list of existing profiles.

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.

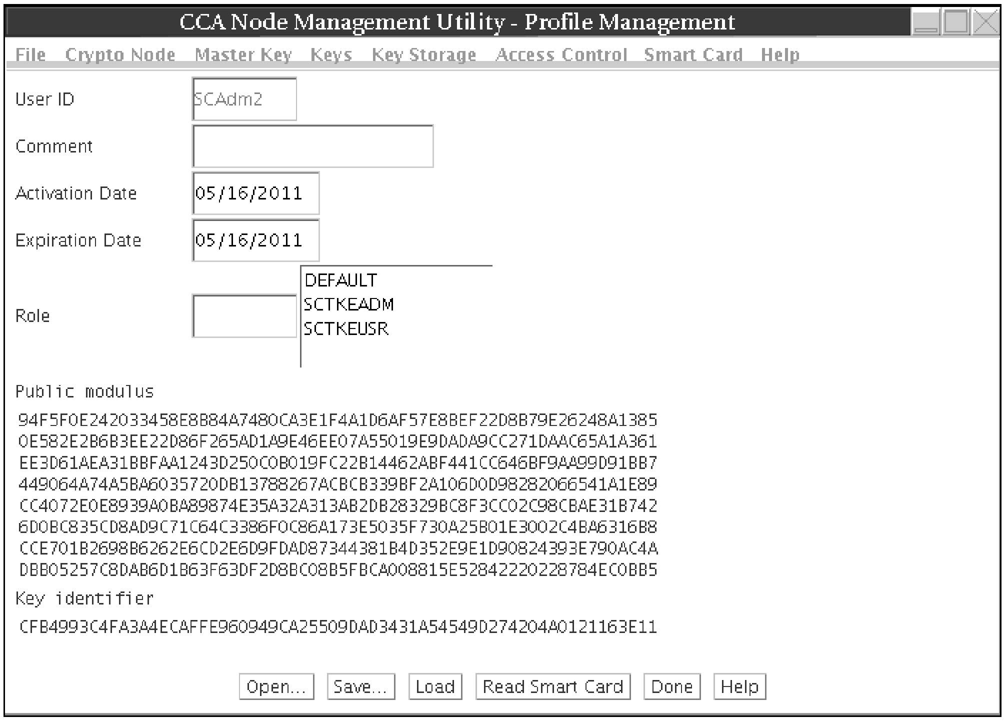


Profile Management

Please insert a TKE smart card into Smart Card reader 2.

Figure 242. 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.



CCA Node Management Utility - Profile Management

User ID: SCAdm2

Comment:

Activation Date: 05/16/2011

Expiration Date: 05/16/2011

Role:

Public modulus

```
94F5F0E242033458E8B84A7480CA3E1F4A1D6AF57E8BEF22D8B79E26248A1385
0E582E2B6B3EE22D86F265AD1A9E46EE07A55019E9DADA9CC271DAAC65A1A361
EE3D61AEA31BBFAA1243D250C0B019FC22B14462ABF441CC646BF9AA99D91BB7
449064A74A5BA6035720DB13788267ACBCB339BF2A106D0D98282066541A1E89
CC4072E0E8939A0BA89874E35A32A313AB2DB28329BC8F3CC02C98CBAE31B742
6D0BC835CD8AD9C71C64C3386F0C86A173E5035F730A25B01E3002C4BA6316B8
CCE701B2698B6262E6CD2E6D9FDAD87344381B4D352E9E1D90824393E790AC4A
DBB05257C8DAB6D1B63F63DF2D8BC08B5FBCA008815E52842220228784EC0BB5
```

Key identifier

```
CFB4993C4FA3A4ECAFFE960949CA25509DAD3431A54549D274204A0121163E11
```

Figure 243. Profile management panel — smart card profile

3. Fill in the fields on the panel as follows:

User ID
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).

Comment
An optional character string. A maximum of 20 characters may be specified.

Activation Date
Determines the first date when the user can log on. This field defaults to the current date. Change this date as appropriate.

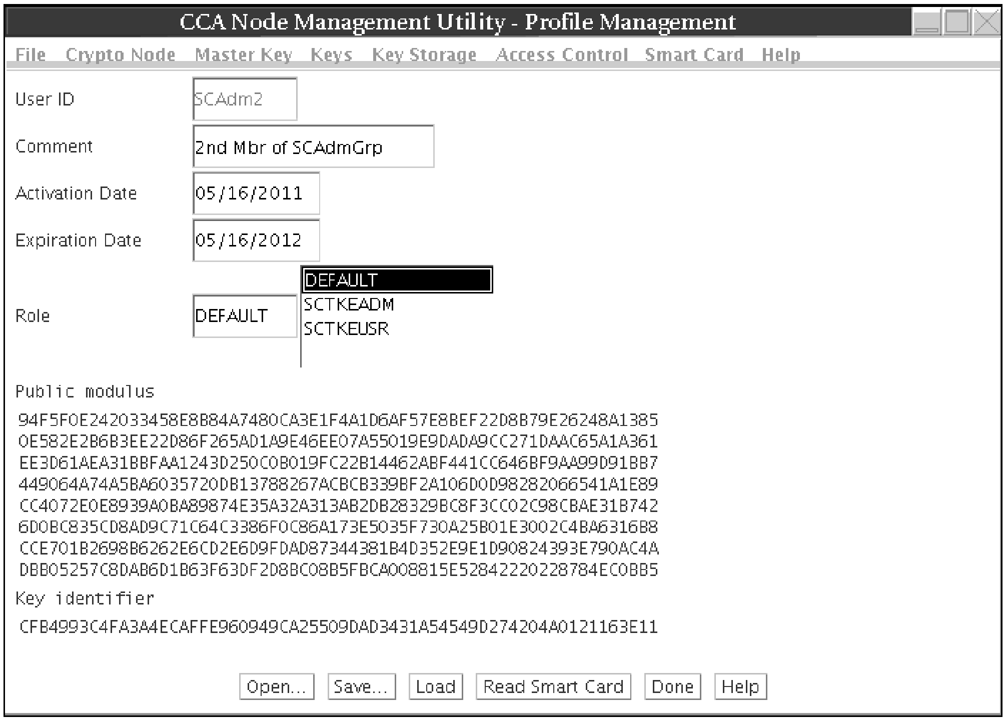
Expiration Date
Determines the last date when the user can log on. This field defaults to the current date. Change this date as appropriate.

Role
The name of the role that defines the permissions granted to the profile. Select a role from the list.

Note: If this user profile will be assigned to a group profile, we recommend mapping the DEFAULT role to this user profile. This limits the access this profile has outside of the group.

Public Modulus
This is the public modulus of the TKE crypto adapter logon key read from the TKE smart card. This field cannot be changed. See "Generate TKE Crypto Adapter logon key" on page 276.

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.



User ID SCAdm2

Comment 2nd Mbr of SCAdmGrp

Activation Date 05/16/2011

Expiration Date 05/16/2012

Role DEFAULT

Public modulus

```
94F5F0E242033458E8B84A7480CA3E1F4A1D6AF57E8BEF22D8B79E26248A1385
0E582E2B6B3EE22D86F265AD1A9E46EE07A55019E9DADA9CC271DAAC65A1A361
EE3D61AEA31BBFAA1243D250C0B019FC22B14462ABF441CC646BF9AA99D91BB7
449064A74A5BA6035720DB13788267ACBCB339BF2A106D0D98282066541A1E89
CC4072E0E8939A0BA89874E35A32A313AB2DB28329BC8F3CC02C98CBAE31B742
6D0BC835CD8AD9C71C64C3386F0C86A173E5035F730A25B01E3002C4BA6316B8
CCE701B2698B6262E6CD2E6D9FDAD87344381B4D352E9E1D90824393E790AC4A
DBB05257C8DAB6D1B63F63DF2D8BC08B5FBCA008815E52842220228784EC0BB5
```

Key identifier

```
CFB4993C4FA3A4ECAFFE960949CA25509DAD3431A54549D274204A0121163E11
```

Figure 244. 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 334.

   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.

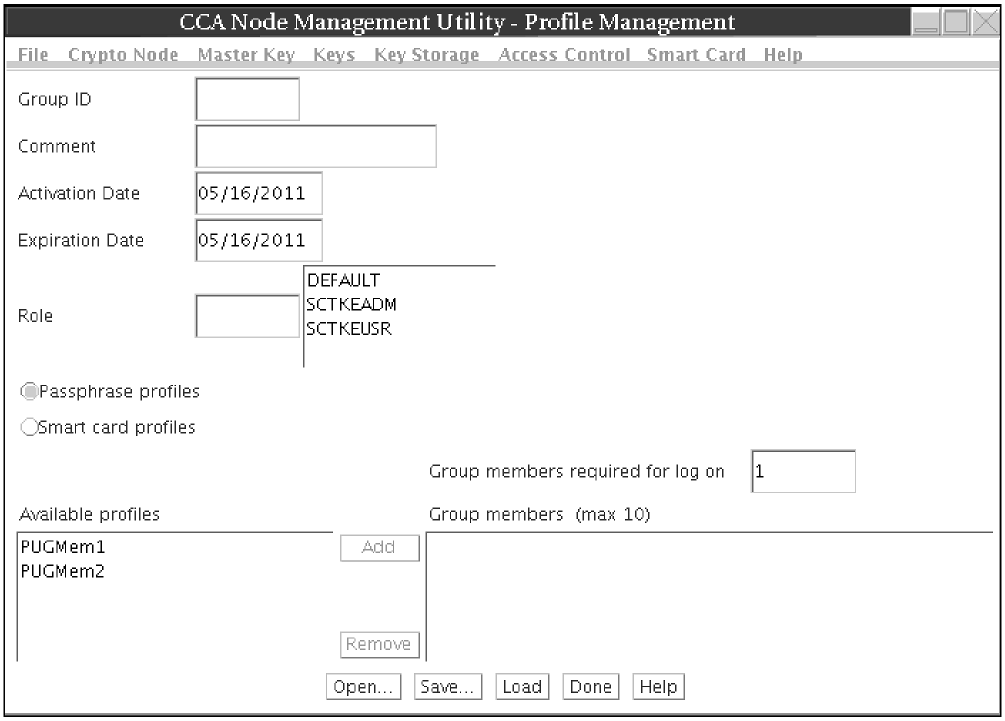
Other actions and tasks available from this panel are as follows:

- 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 **Done** to return to the list of existing profiles.

Define a Group Profile

1. If Group is selected as the profile type, a panel is displayed for defining a group profile.



Group ID

Comment

Activation Date 05/16/2011

Expiration Date 05/16/2011

Role

DEFAULT
SCTKEADM
SCTKEUSR

● Passphrase profiles

○ Smart card profiles

Group members required for log on 1

Available profiles

PUGMem1
PUGMem2

Group members (max 10)

Figure 245. 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 log on. This field defaults to the current date. Change this date as appropriate.

Expiration Date
Determines the last date when the group can log on. 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.

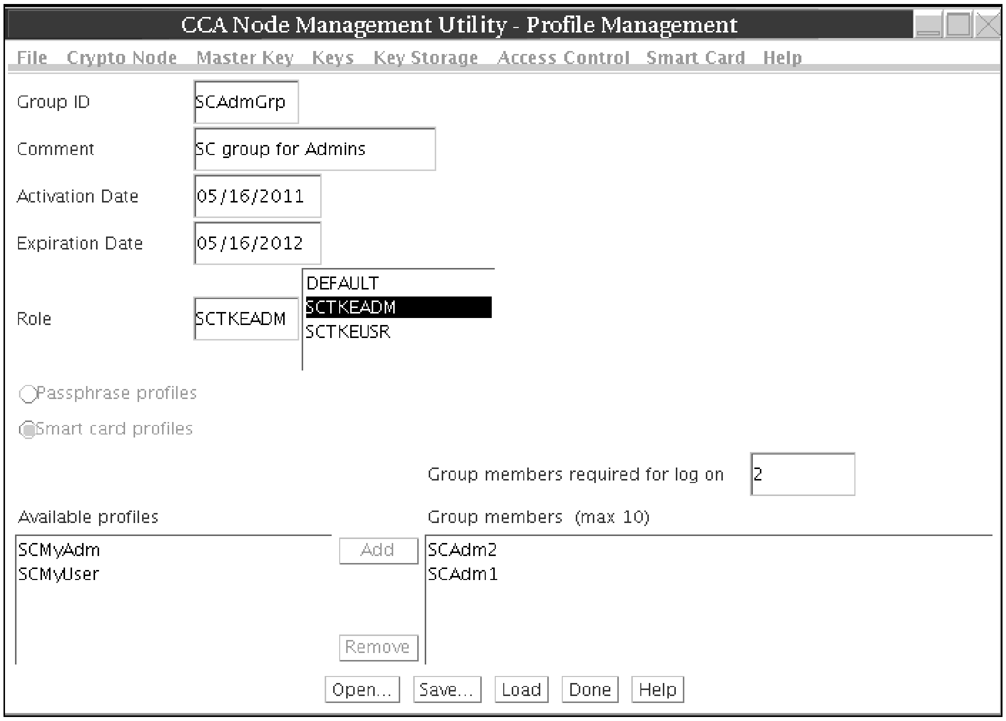
Note: The role of the group overrides the roles of the individual user profiles.

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 logon
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.



Group ID SCAdmGrp
Comment SC group for Admins
Activation Date 05/16/2011
Expiration Date 05/16/2012
Role SCTKEADM

DEFAULT
SCTKEADM
SCTKEUSR

○ Passphrase profiles
● Smart card profiles

Group members required for log on 2

Available profiles
SCMyAdm
SCMyUser

Group members (max 10)
SCAdm2
SCAdm1

Figure 246. 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 334.
   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 **Done** to return to the list of existing profiles.

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 334.

   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 334.

   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

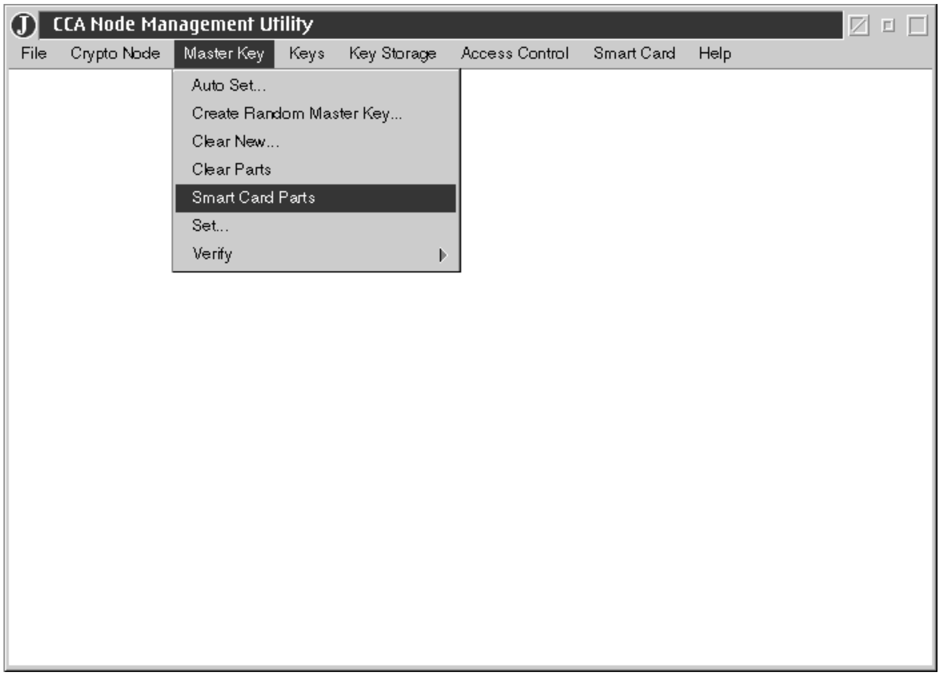


Figure 247. CNM main window — Master Key pull-down menu

The master key is stored in the tamper-resistant TKE cryptographic adapter. It is used to encipher other keys. The master key is a 24 byte DES key (192 bits), but, because DES keys contain 1 parity bit per byte, it has an effective length of 168 bits of "real" key material. 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.

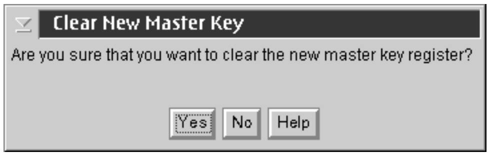
The TKE crypto adapter has three master key registers:

- **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 is 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.

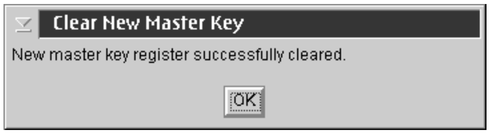


Clear New Master Key

Are you sure that you want to clear the new master key register?

Figure 248. 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.



Clear New Master Key

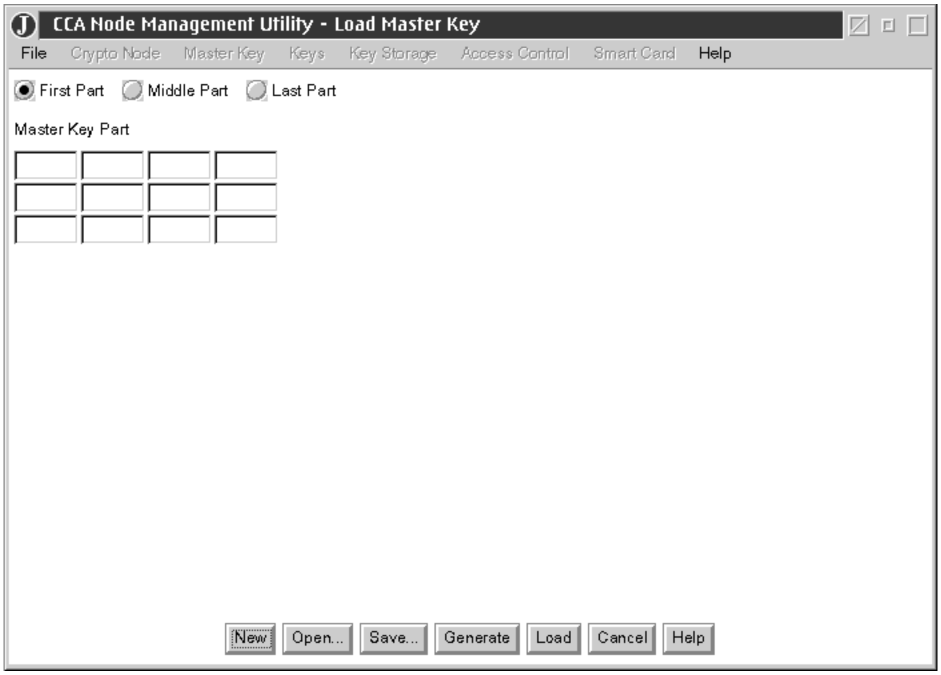
New master key register successfully cleared.

Figure 249. 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.



CCA Node Management Utility - Load Master Key

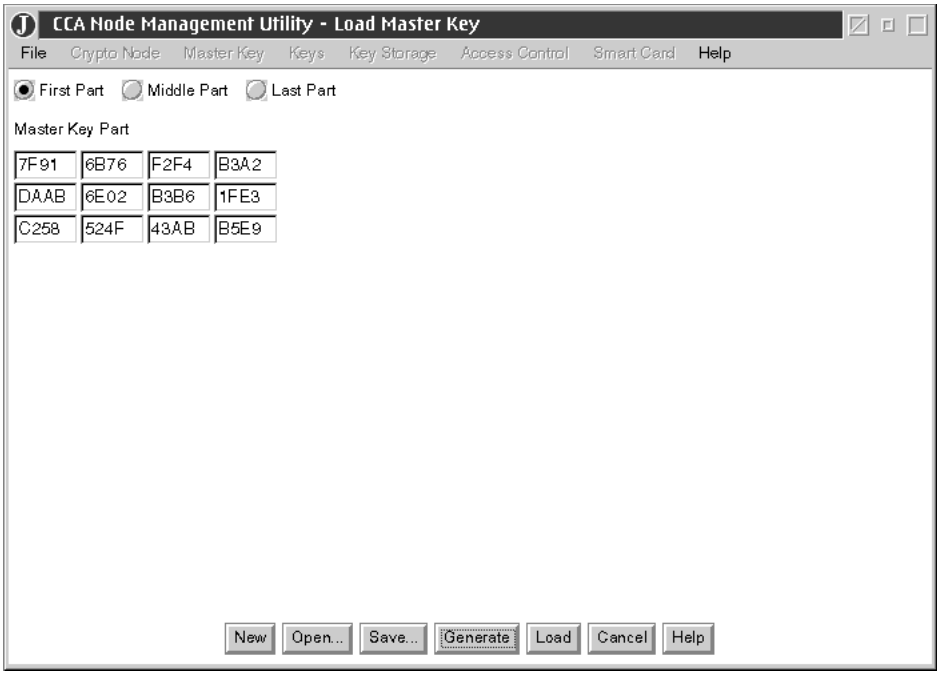
● First Part ○ Middle Part ○ Last Part

Master Key Part

Figure 250. 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.



● First Part ○ Middle Part ○ Last Part

Master Key Part

7F91	6B76	F2F4	B3A2
DAAB	6E02	B3B6	1FE3
C258	524F	43AB	B5E9

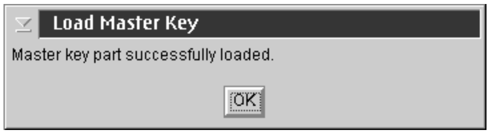
Figure 251. Load Master Key from Clear Parts — key part randomly generated

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 334.

   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.



Master key part successfully loaded.

Figure 252. Load Master Key from Clear Parts — key part successfully loaded

   Note: Key parts saved to disk are not enciphered.

5. Repeat the preceding steps to load the remaining key parts into the new master key register.
6. From the **Master Key** pull-down menu, select **Set**... This will do the following:

a. Transfer the key in the current master key register to the old master key register and delete the former old master key.

b. Transfer the key in the new master key register to the current master key register.

After setting a new master key, reencipher the keys currently in key storage. (Refer to “Reenciphering key storage” on page 274.)

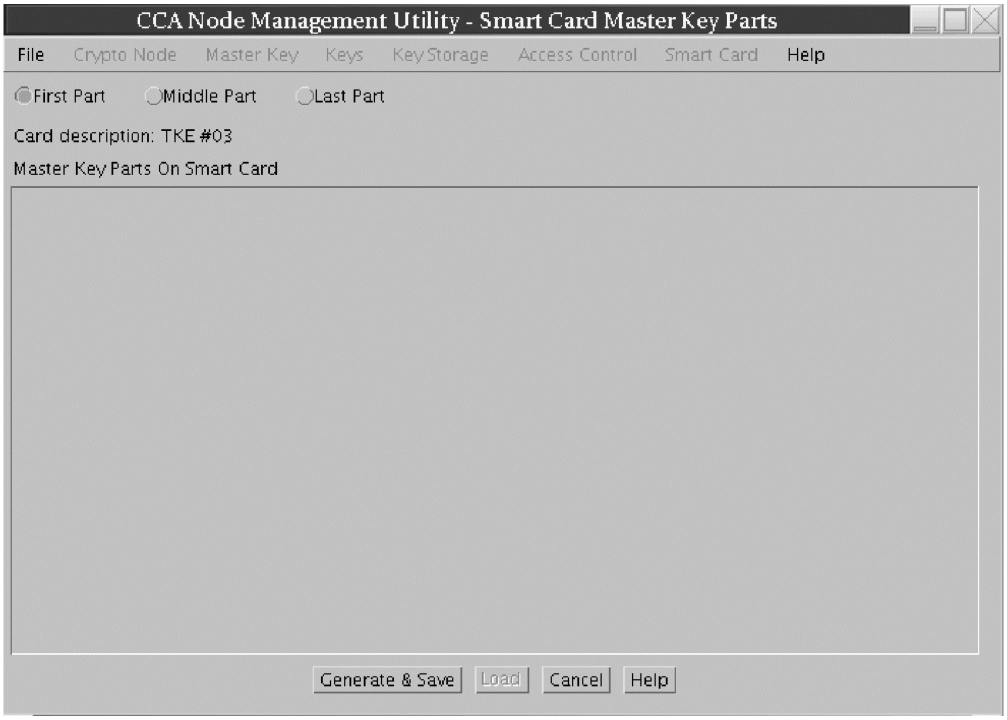
We recommend a dual control security policy. With a dual control security policy, the first and last key parts are loaded by different people.

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 277 or SCUP “Display smart card information” on page 287. To determine the zone of a TKE cryptographic adapter, use SCUP “View current zone” on page 306. To use SCUP, you must first exit from CNM.

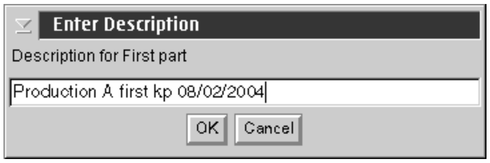


Card description: TKE #03

Figure 253. 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.



Enter Description

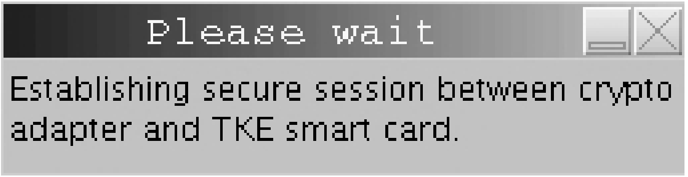
Description for First part

Production A first kp 08/02/2004

Figure 254. 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.

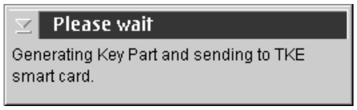
A secure session is established between the TKE crypto adapter and the TKE smart card. The key part is generated to the TKE smart card. The key part list is refreshed.



Please wait

Establishing secure session between crypto adapter and TKE smart card.

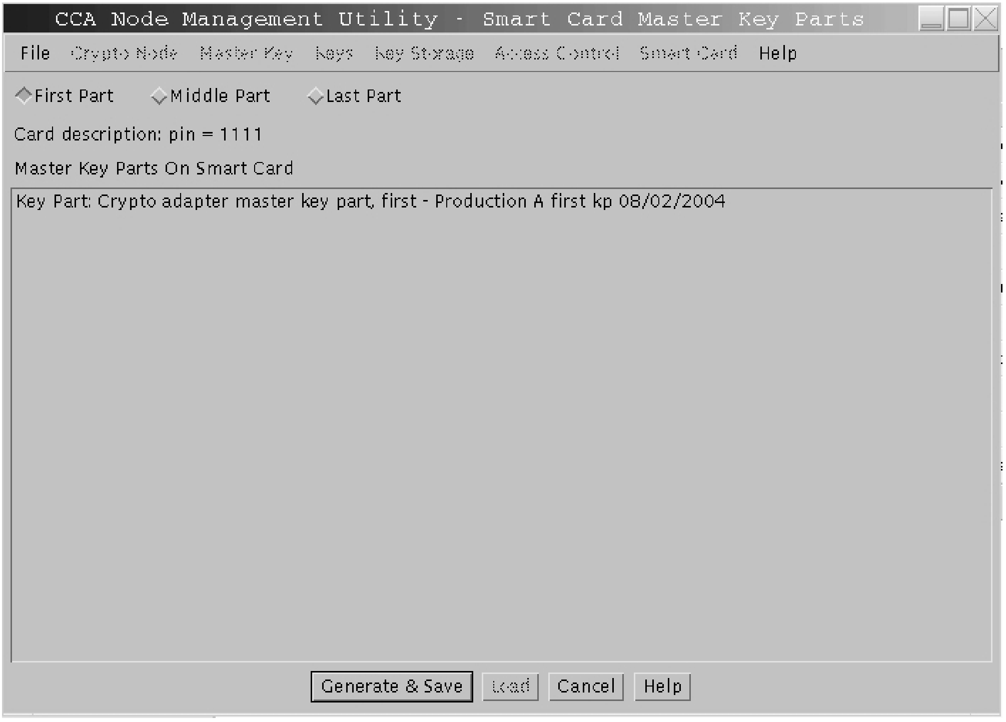
Figure 255. Establishing a secure session between TKE crypto adapter and TKE smart card



Please wait

Generating Key Part and sending to TKE smart card.

Figure 256. Generating key part to TKE smart card



◆First Part ◇Middle Part ◇Last Part

Card description: pin = 1111

Master Key Parts On Smart Card

Key Part: Crypto adapter master key part, first - Production A first kp 08/02/2004

Figure 257. Smart Card Master Key Parts panel — key part generated to TKE smart card

Note: The key parts in the list are prefixed as follows:

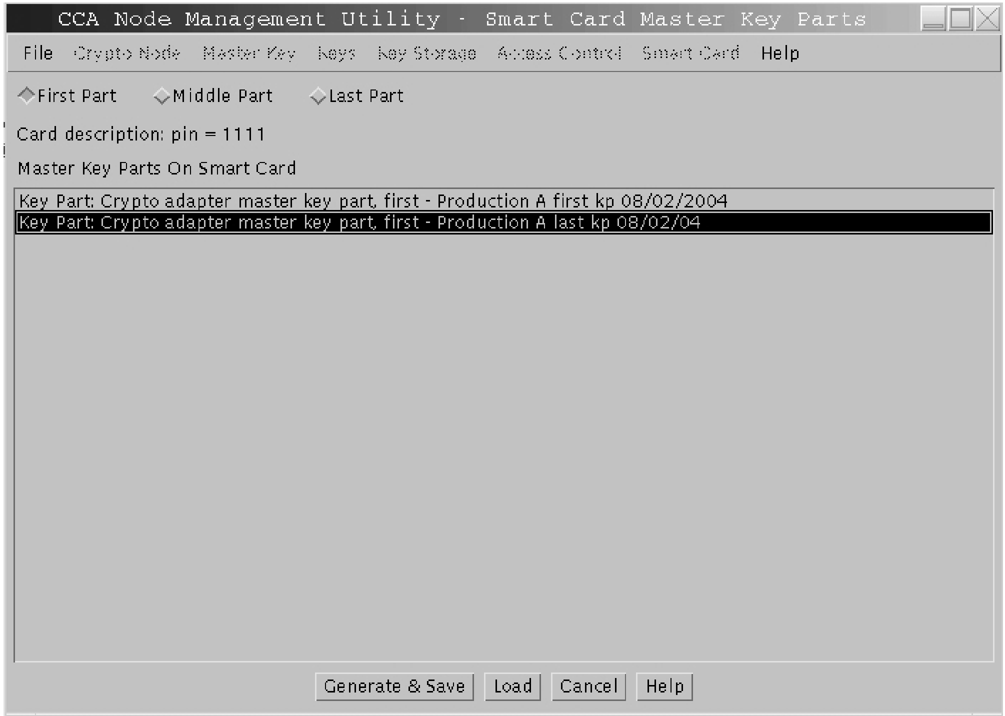
- Key Part: Crypto Adapter master key part, first - <optional description follows>
- Key Part: Crypto Adapter master key part, middle - <optional description follows>
- Key Part: Crypto Adapter master key part, last - <optional description follows>

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.



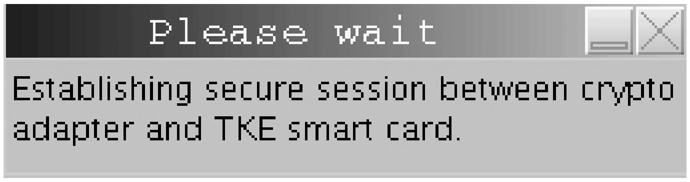
Card description: pin = 1111

Master Key Parts On Smart Card

Key Part: Crypto adapter master key part, first - Production A first kp 08/02/2004
Key Part: Crypto adapter master key part, first - Production A last kp 08/02/04

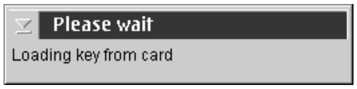
Figure 258. Master Key Part Smart Card panel — loading a Crypto Adapter key part from TKE smart card

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.



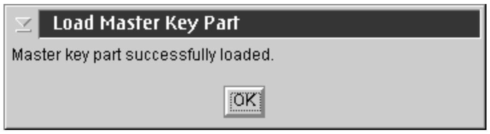
Establishing secure session between crypto adapter and TKE smart card.

Figure 259. Establishing a secure session between Crypto Adapter and TKE smart card



Loading key from card

Figure 260. Loading key part from TKE smart card



Master key part successfully loaded.

Figure 261. Master key part successfully loaded

4. Repeat steps 1 on page 269 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 274.

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.

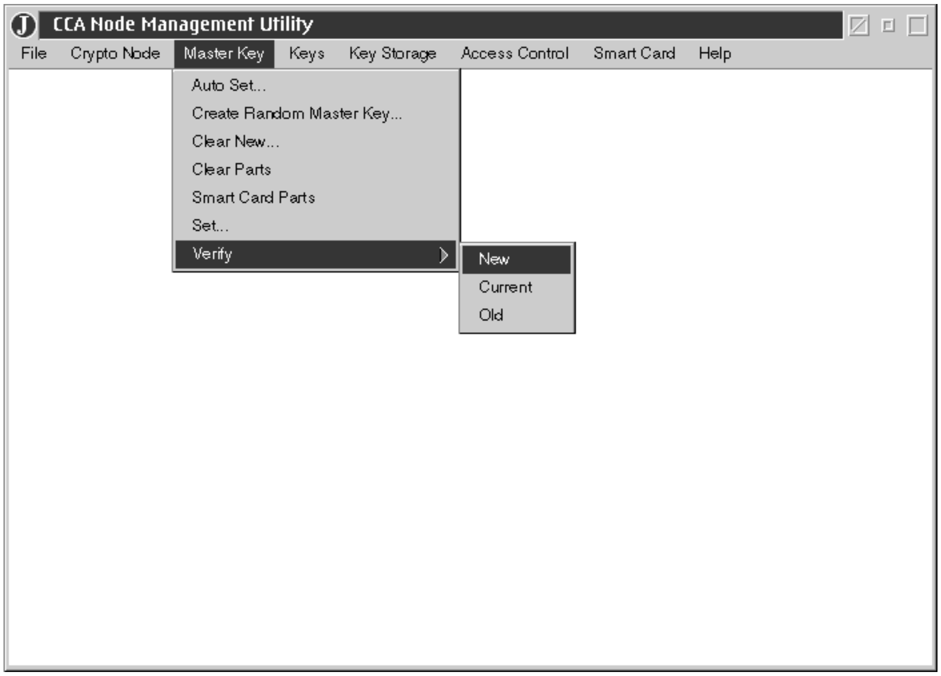
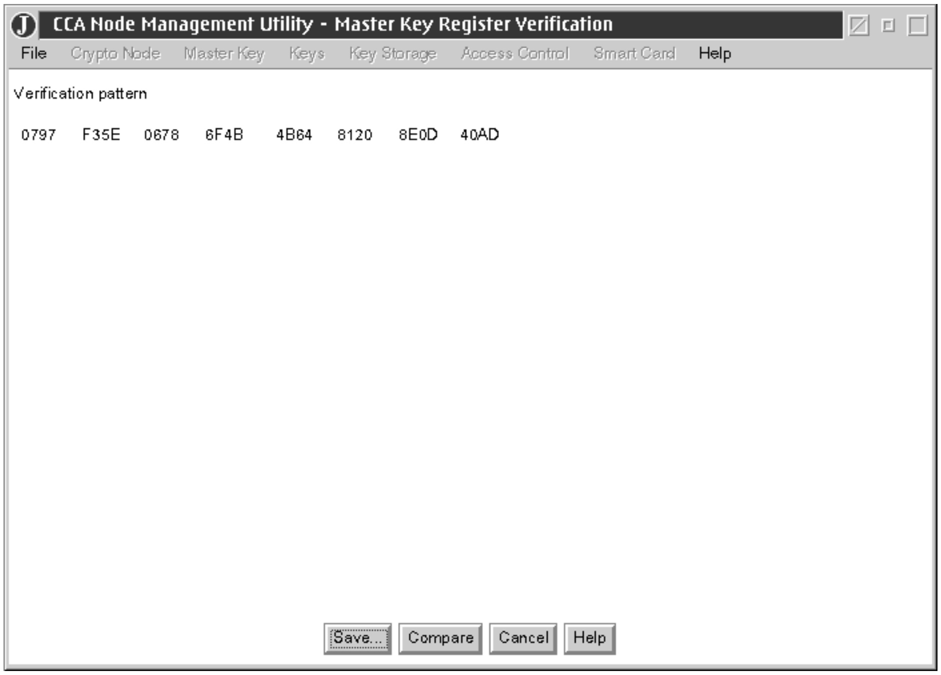


Figure 262. Master Key Verify sub-menu

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.



Verification pattern

```
0797   F35E   0678   6F4B    4B64   8120   8E0D   40AD
```

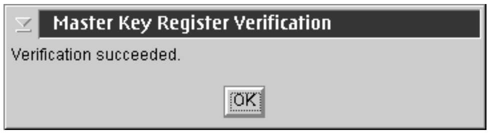
Figure 263. Master Key Register Verification panel - verification pattern is displayed

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 334.
   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.


Master Key Register Verification

Verification succeeded.

Figure 264. 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.

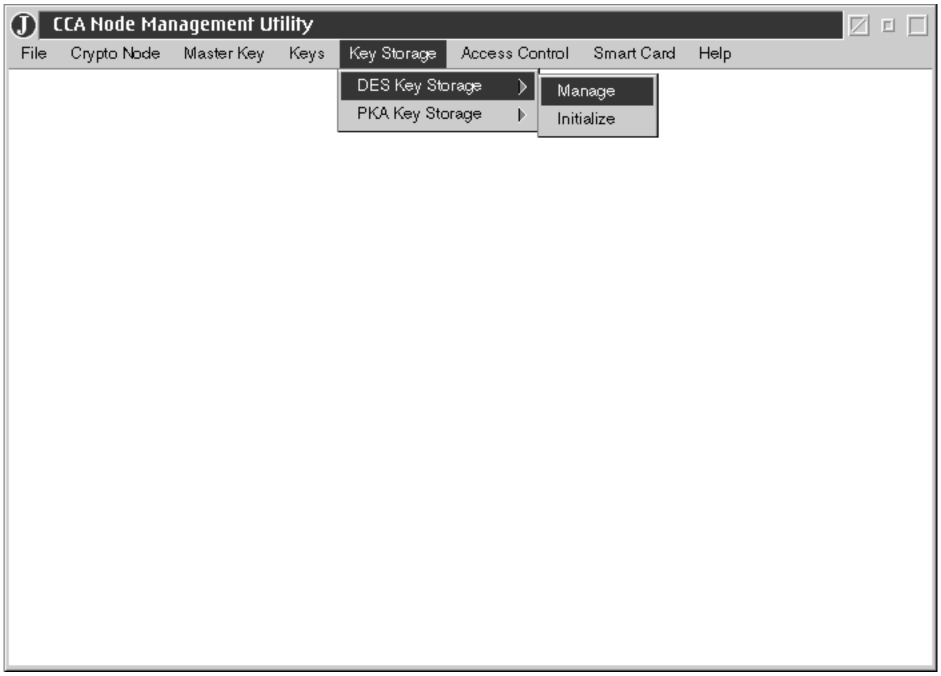


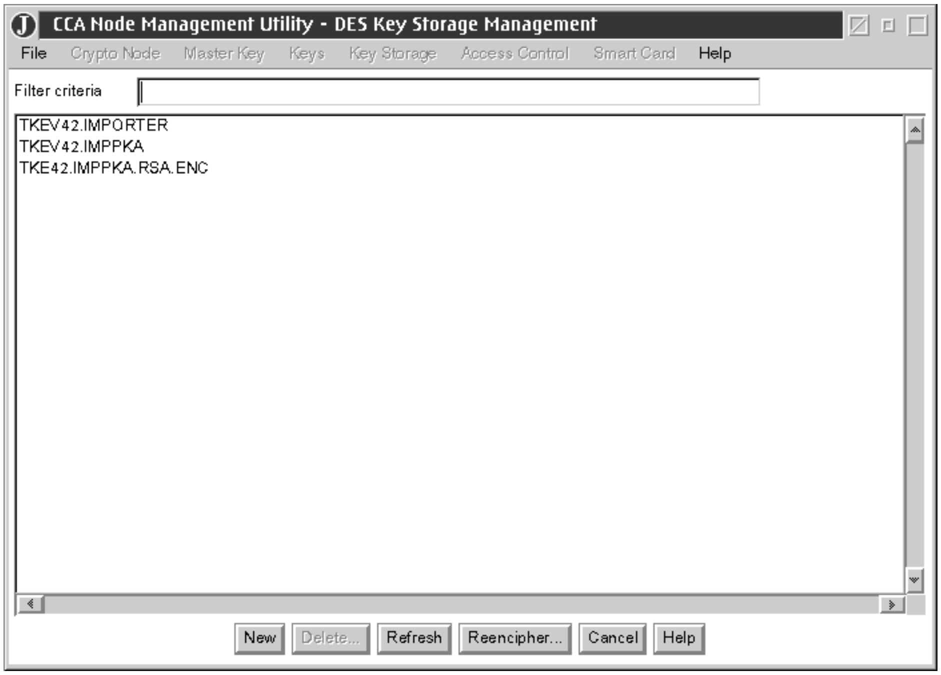
Figure 265. CNM main window — Key Storage pull-down menu

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.



TKEV42.IMPORTER
TKEV42.IMPPKA
TKE42.IMPPKA.RSA.ENC

Figure 266. 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

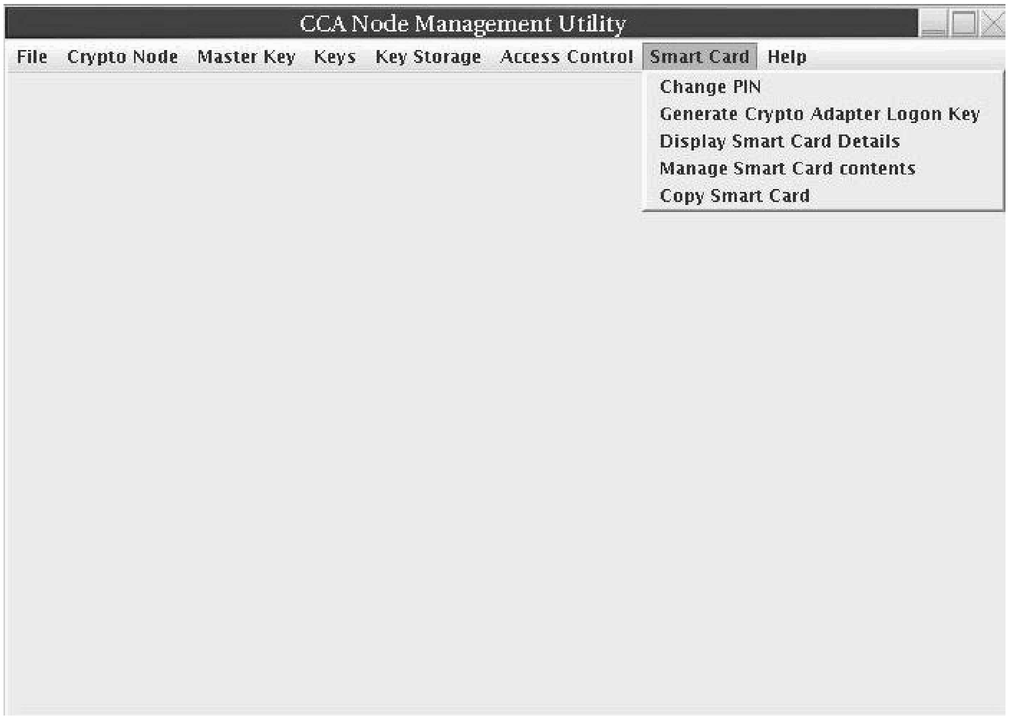

CCA Node Management Utility
File
Crypto Node
Master Key
Keys
Key Storage
Access Control
Smart Card
Help
Change PIN
Generate Crypto Adapter Logon Key
Display Smart Card Details
Manage Smart Card contents
Copy Smart Card

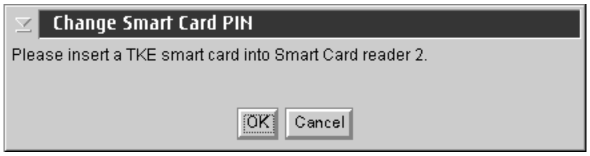
Figure 267. CNM main menu — Smart Card pull-down menu

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 log on to the TKE crypto adapter to perform this function.

To change the PIN, perform the following steps:

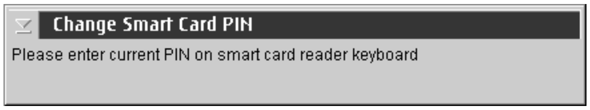
1. From the **Smart Card** pull-down menu, select **Change PIN**. An informational window will prompt you to insert your TKE smart card into Smart Card Reader 2. Insert your TKE smart card and press **OK** to continue.


Change Smart Card PIN

Please insert a TKE smart card into Smart Card reader 2.

Figure 268. Change PIN — insert TKE smart card prompt

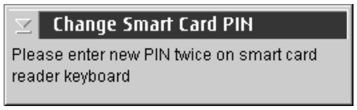
2. You will be prompted for your current PIN. Enter your current PIN on the smart card reader 2 PIN pad.



Please enter current PIN on smart card reader keyboard

Figure 269. 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.



Please enter new PIN twice on smart card reader keyboard

Figure 270. Change PIN — enter new PIN prompt

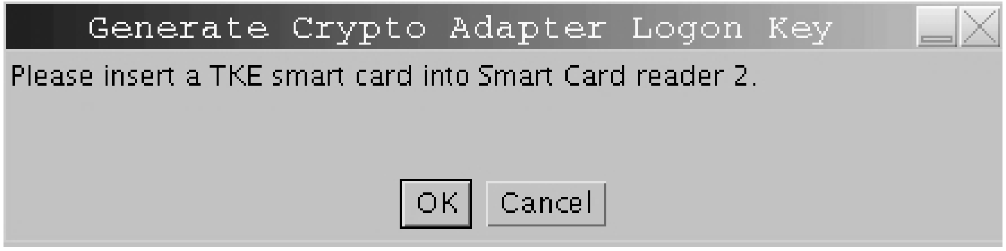
4. The PIN is successfully changed on the TKE smart card.

Generate TKE Crypto Adapter logon key

A Crypto Adapter logon key allows a user to log on 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 public/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:

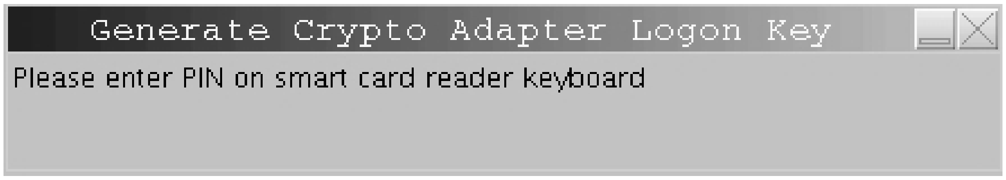
1. From the Smart Card pull-down menu, select Generate Crypto Adapter Logon Key. You will be prompted for a TKE smart card. Insert the TKE smart card into smart card reader 2.



Please insert a TKE smart card into Smart Card reader 2.

Figure 271. Generate Crypto Adapter Logon Key — insert TKE smart card

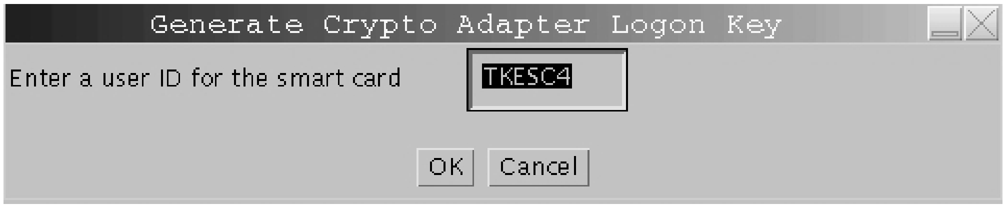
2. You will be prompted for a PIN. Enter the PIN on the smart card reader 2 PIN pad.



Please enter PIN on smart card reader keyboard

Figure 272. Generate Crypto Adapter Logon Key — PIN prompt

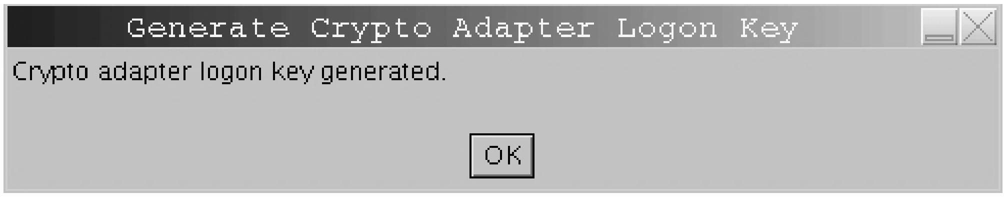
3. You will be prompted for a user ID for the TKE smart card. This user ID will be read from the TKE smart card when defining a smart card user profile.


Generate Crypto Adapter Logon Key

Enter a user ID for the smart card TKESC4

Figure 273. Generate Crypto Adapter Logon Key — User ID prompt

4. The Crypto Adapter logon key is generated.


Generate Crypto Adapter Logon Key

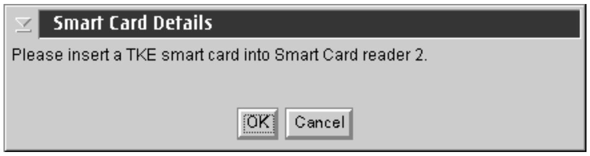
Crypto adapter logon key generated.

Figure 274. Generate Crypto Adapter Logon Key — key generated

Display smart card details

Use this function to display public information about a TKE smart card.

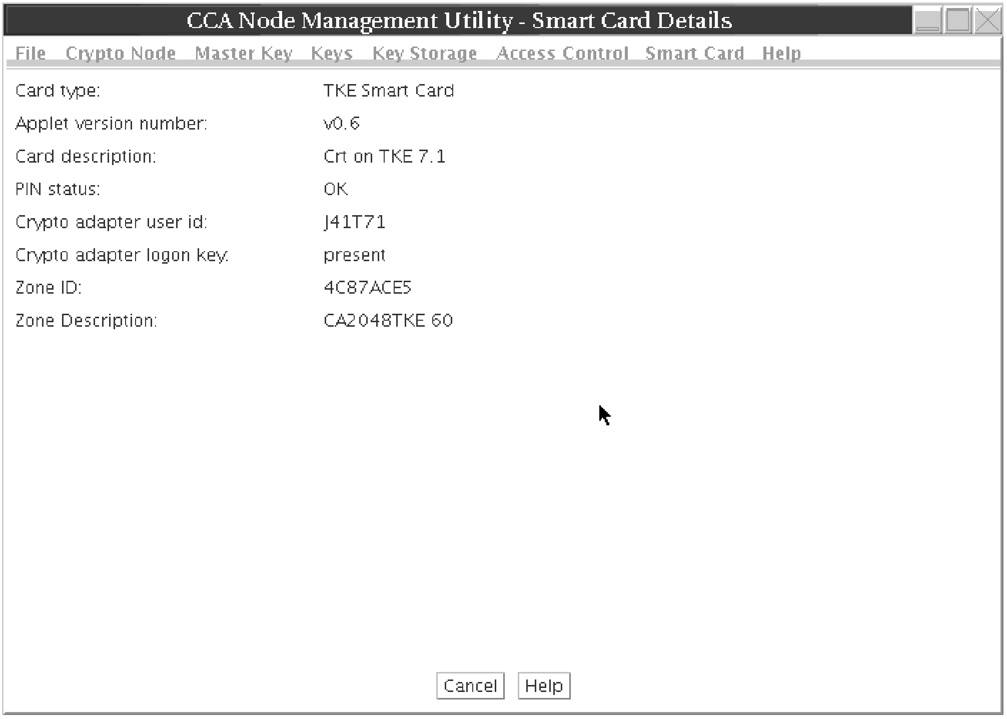
1. From the **Smart Card** pull-down menu, select **Display Smart Card Details**. You will be prompted for a TKE smart card. Insert the TKE smart card into Smart Card Reader 2.


Smart Card Details

Please insert a TKE smart card into Smart Card reader 2.

Figure 275. Display Smart Card Details — insert TKE smart card prompt

The TKE smart card is read and the public information is displayed.



Card type: TKE Smart Card

Applet version number: v0.6

Card description: Crt on TKE 7.1

PIN status: OK

Crypto adapter user id: J41T71

Crypto adapter logon key: present

Zone ID: 4C87ACE5

Zone Description: CA2048TKE 60

Figure 276. 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

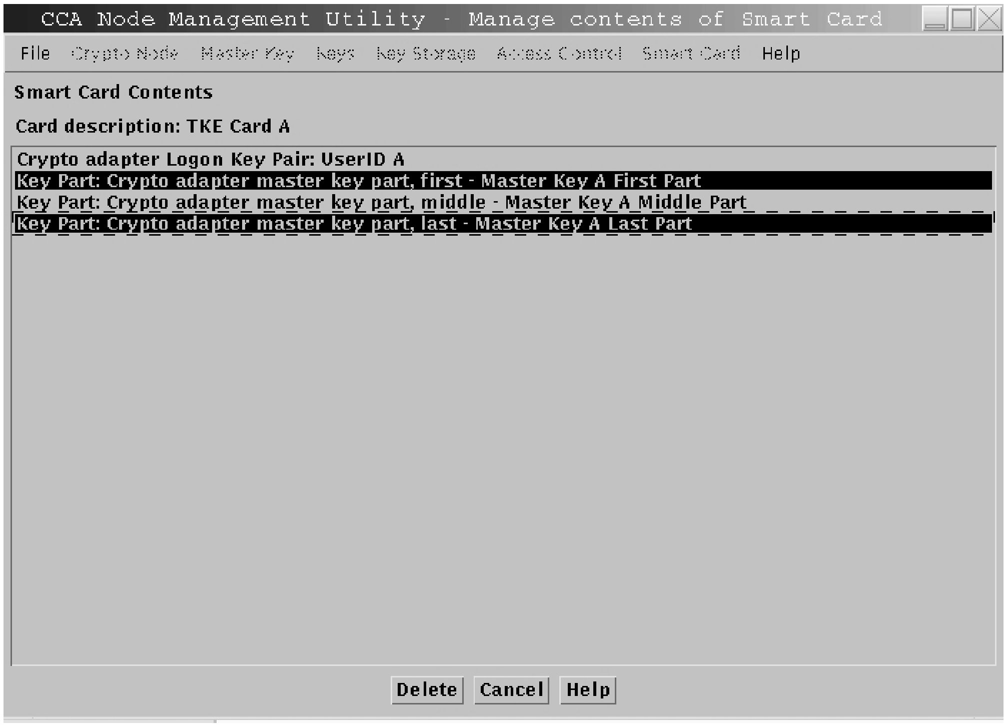
Zone Description
Set when the TKE smart card is initialized

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 50 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.



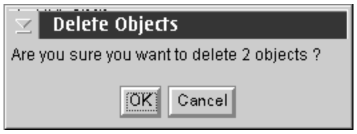
Smart Card Contents

Card description: TKE Card A

Crypto adapter Logon Key Pair: UserID A
Key Part: Crypto adapter master key part, first - Master Key A First Part
Key Part: Crypto adapter master key part, middle - Master Key A Middle Part
Key Part: Crypto adapter master key part, last - Master Key A Last Part

Figure 277. Manage Smart Card contents — contents of TKE smart card are displayed

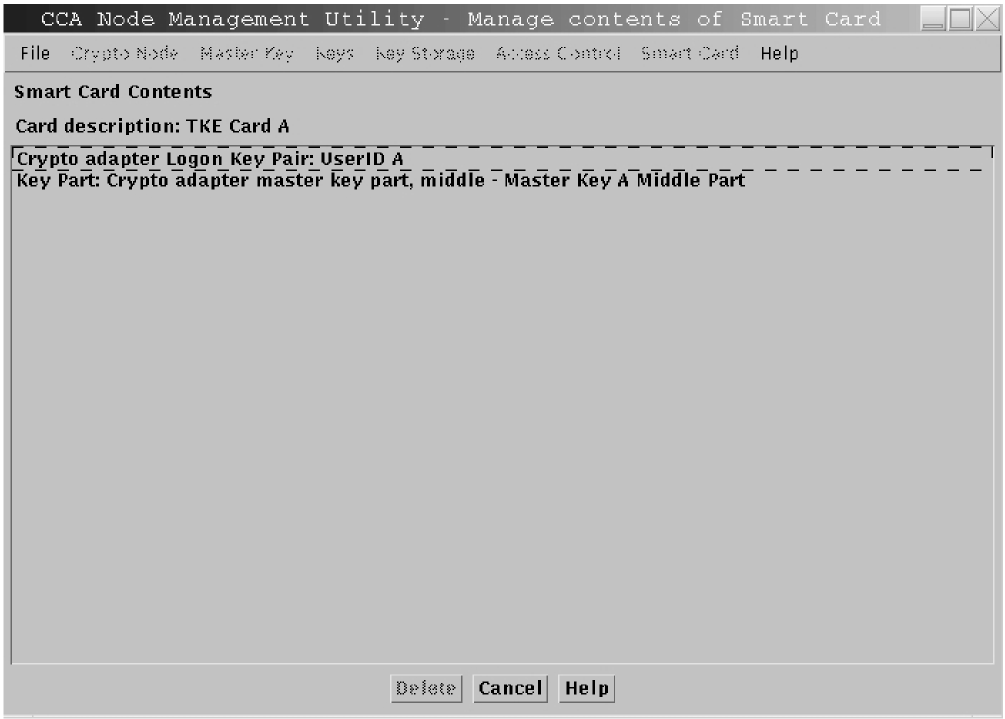
2. The TKE smart card description is displayed. Ensure this is the correct TKE smart card you want to work with. Highlight the keys and/or key parts you want to delete. Press the **Delete** button.
3. You will be prompted for your PIN. Enter your PIN on the Smart Card Reader 2 PIN pad.
4. You will be asked to confirm the deletion of the selected objects. Press **OK** to continue.



Are you sure you want to delete 2 objects ?

Figure 278. Manage Smart Card contents — confirm delete prompt

5. The objects are deleted and the list is refreshed.



Smart Card Contents

Card description: TKE Card A

Crypto adapter Logon Key Pair: UserID A
Key Part: Crypto adapter master key part, middle - Master Key A Middle Part

Figure 279. 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

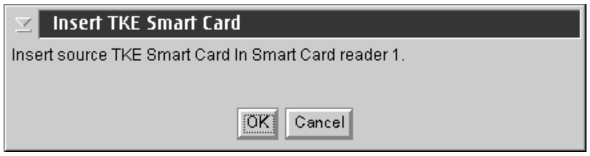
Use this function to copy a key or key part(s) from one TKE smart card to another. The two TKE smart cards must belong to the same zone. Specifically, the Zone ID of the TKE smart cards must be identical. Use **Display Smart Card Details** to verify the Zone ID of the TKE smart cards.

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 278) 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:

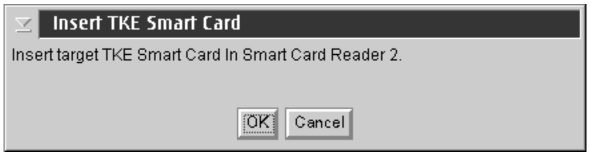
1. From the Smart Card pull-down menu, select Copy Smart Card. You will be prompted for a source TKE smart card. This is the TKE smart card you want to copy from. Insert the source TKE smart card into Smart Card Reader 1. The contents of the TKE smart card are displayed in the source container on the top.



Insert source TKE Smart Card In Smart Card reader 1.

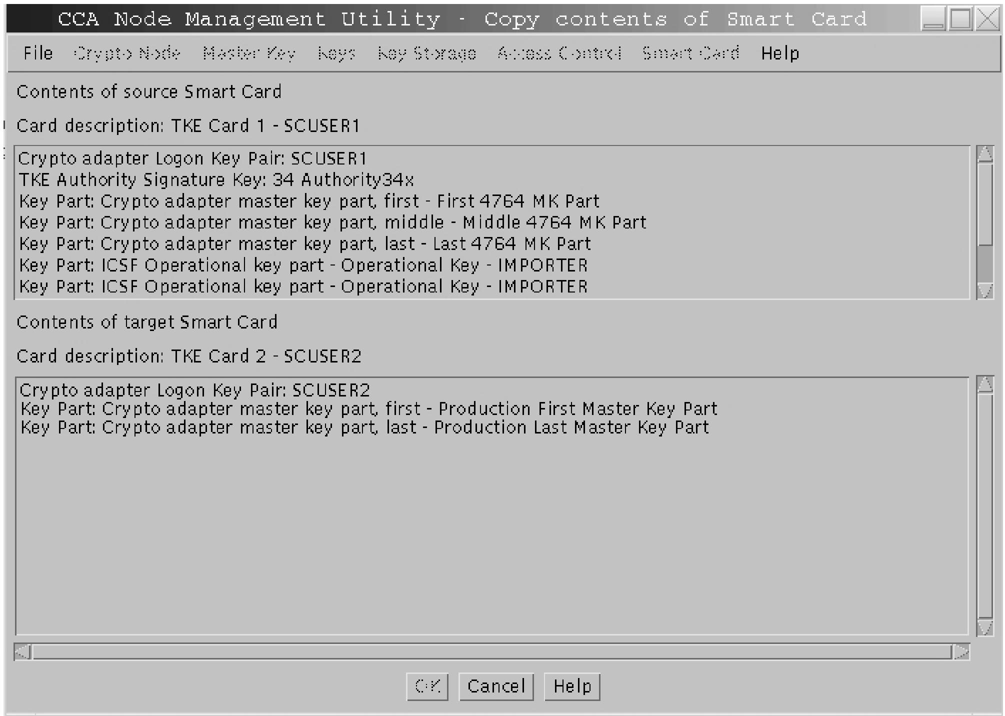
Figure 280. Copy Smart Card — insert source TKE smart card

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.



Insert target TKE Smart Card In Smart Card Reader 2.

Figure 281. Copy Smart Card — insert target TKE smart card



Contents of source Smart Card

Card description: TKE Card 1 - SCUSER1

```
Crypto adapter Logon Key Pair: SCUSER1
TKE Authority Signature Key: 34 Authority34x
Key Part: Crypto adapter master key part, first - First 4764 MK Part
Key Part: Crypto adapter master key part, middle - Middle 4764 MK Part
Key Part: Crypto adapter master key part, last - Last 4764 MK Part
Key Part: ICSF Operational key part - Operational Key - IMPORTER
Key Part: ICSF Operational key part - Operational Key - IMPORTER
```

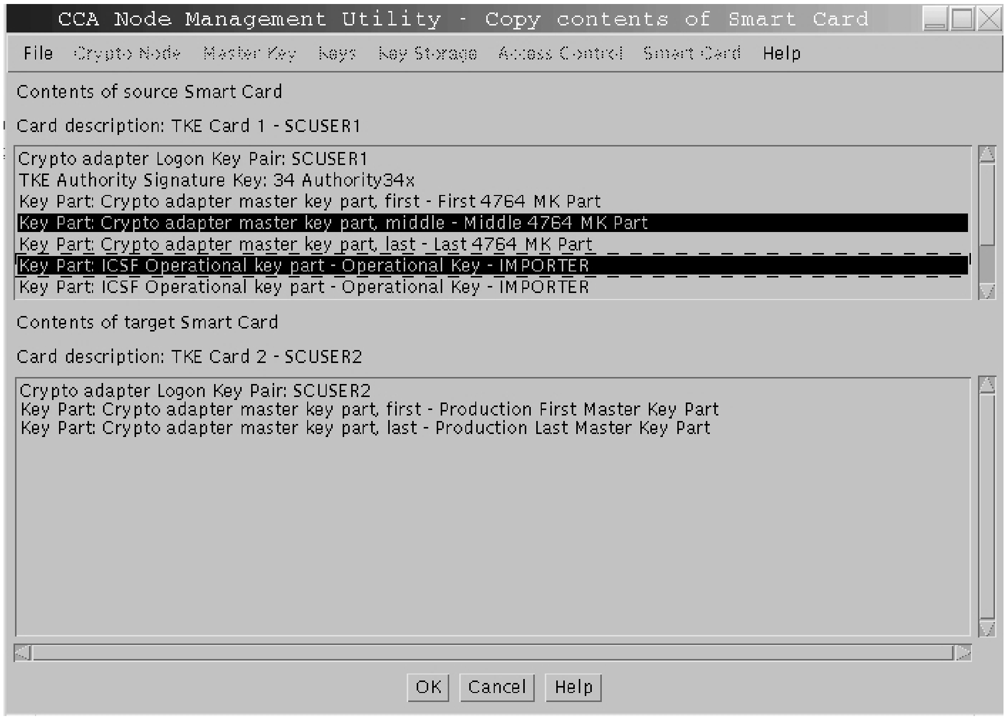
Contents of target Smart Card

Card description: TKE Card 2 - SCUSER2

```
Crypto adapter Logon Key Pair: SCUSER2
Key Part: Crypto adapter master key part, first - Production First Master Key Part
Key Part: Crypto adapter master key part, last - Production Last Master Key Part
```

Figure 282. 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.



Contents of source Smart Card

Card description: TKE Card 1 - SCUSER1

Crypto adapter Logon Key Pair: SCUSER1
TKE Authority Signature Key: 34 Authority34x
Key Part: Crypto adapter master key part, first - First 4764 MK Part
Key Part: Crypto adapter master key part, middle - Middle 4764 MK Part
Key Part: Crypto adapter master key part, last - Last 4764 MK Part
Key Part: ICSF Operational key part - Operational Key - IMPORTER
Key Part: ICSF Operational key part - Operational Key - IMPORTER

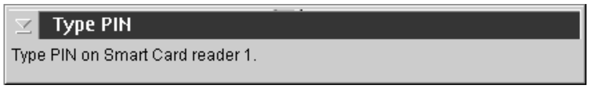
Contents of target Smart Card

Card description: TKE Card 2 - SCUSER2

Crypto adapter Logon Key Pair: SCUSER2
Key Part: Crypto adapter master key part, first - Production First Master Key Part
Key Part: Crypto adapter master key part, last - Production Last Master Key Part

Figure 283. 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.

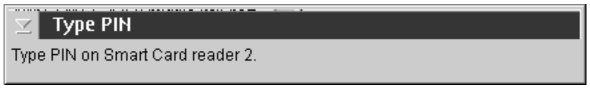


Type PIN

Type PIN on Smart Card reader 1.

Figure 284. Copy Smart Card — source TKE smart card PIN prompt

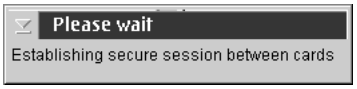
5. You will be prompted for the PIN of the target TKE smart card in Smart Card Reader 2. Enter the PIN on the Smart Card Reader 2 PIN pad. A secure session is established between the two TKE smart cards and the selected object(s) are copied. The contents of the target container is refreshed.



Type PIN

Type PIN on Smart Card reader 2.

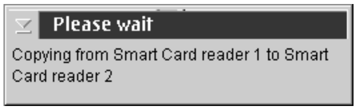
Figure 285. Copy Smart Card — target TKE smart card PIN prompt



Please wait

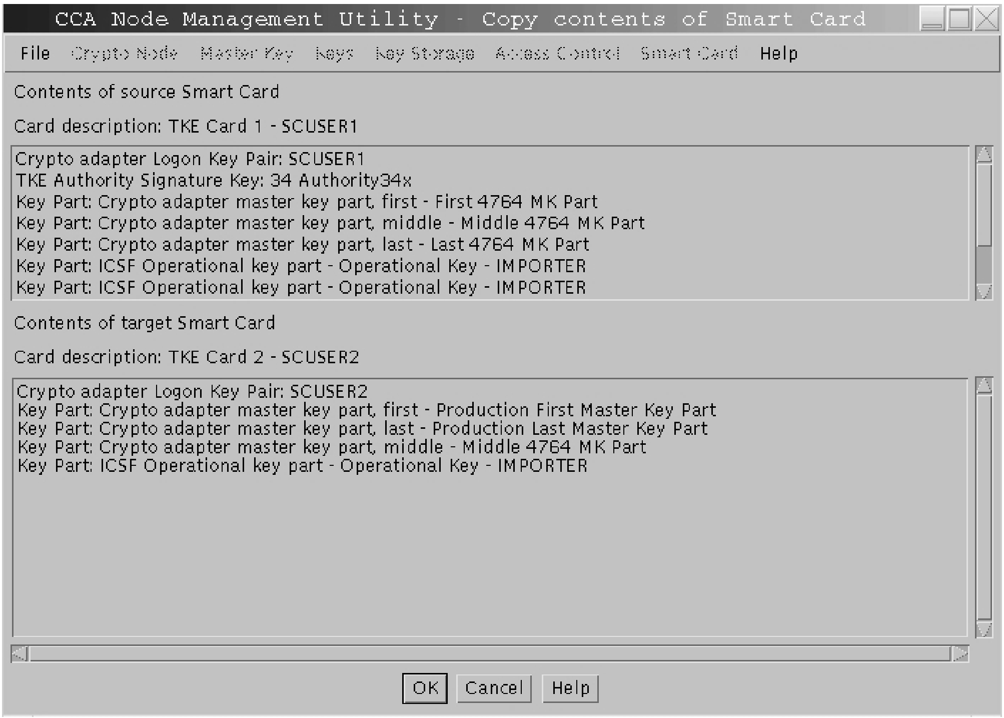
Establishing secure session between cards

Figure 286. Establishing a secure session between source and target TKE smart cards



Copying from Smart Card reader 1 to Smart Card reader 2

Figure 287. Objects are copied to the target TKE smart card



Contents of source Smart Card

Card description: TKE Card 1 - SCUSER1

```
Crypto adapter Logon Key Pair: SCUSER1
TKE Authority Signature Key: 34 Authority34x
Key Part: Crypto adapter master key part, first - First 4764 MK Part
Key Part: Crypto adapter master key part, middle - Middle 4764 MK Part
Key Part: Crypto adapter master key part, last - Last 4764 MK Part
Key Part: ICSF Operational key part - Operational Key - IMPORTER
Key Part: ICSF Operational key part - Operational Key - IMPORTER
```

Contents of target Smart Card

Card description: TKE Card 2 - SCUSER2

```
Crypto adapter Logon Key Pair: SCUSER2
Key Part: Crypto adapter master key part, first - Production First Master Key Part
Key Part: Crypto adapter master key part, last - Production Last Master Key Part
Key Part: Crypto adapter master key part, middle - Middle 4764 MK Part
Key Part: ICSF Operational key part - Operational Key - IMPORTER
```

Figure 288. Copy Smart Card — objects are copied to the target container

A TKE smart card can hold a maximum of 50 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 287
- “Display smart card key identifiers” on page 288
- “Initialize and personalize the CA smart card” on page 290
- “Backup a CA smart card” on page 293
- “Change PIN of a CA smart card” on page 294
- “Initialize and enroll a TKE smart card” on page 295
- “Personalize a TKE smart card” on page 296
- “Change PIN of a TKE smart card” on page 297
- “Unblock PIN on a TKE smart card” on page 297
- “Enroll a TKE cryptographic adapter” on page 297
- “View current zone” on page 306

General Information

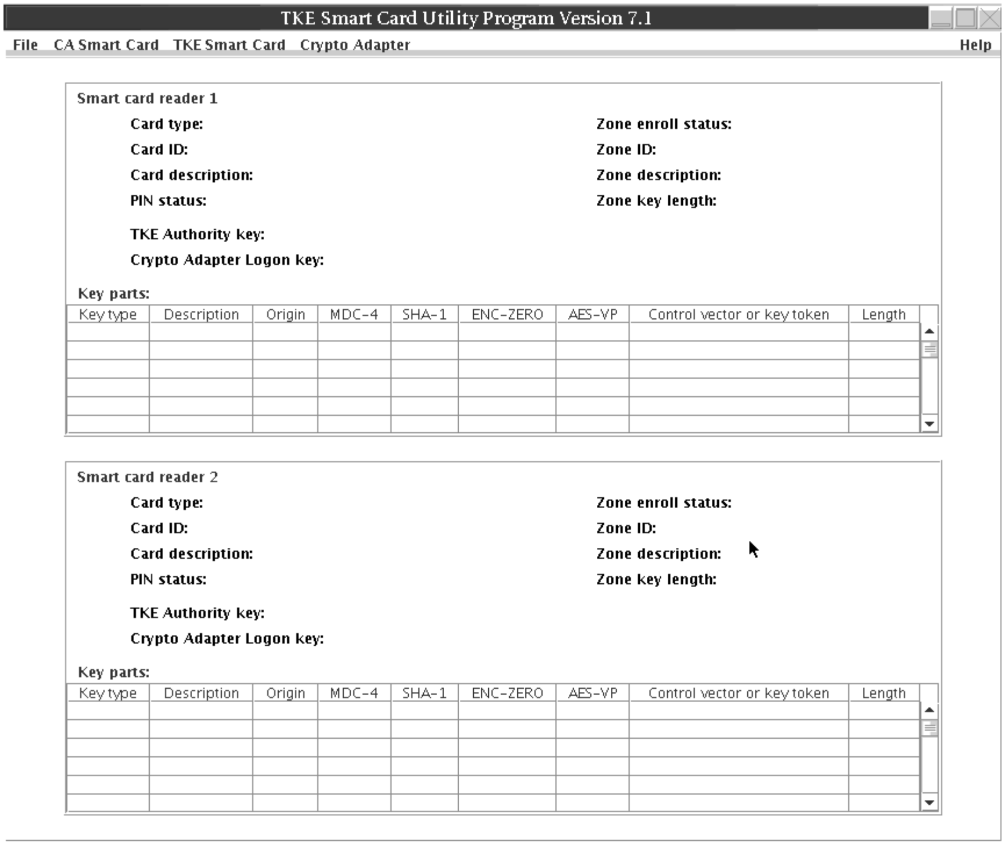
When entering PINs, the PIN prompt appears on both the TKE workstation screen as well as on the smart card reader. When certain tasks will take over one minute for SCUP to execute, information messages are returned. Be patient so that you do not have to restart the task.

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 TKE workstation crypto adapter with a profile defined when you configured the TKE workstation from CNM. You are prompted to logon to the TKE workstation crypto adapter if you are not currently logged on.

Click on **Applications**. Under Applications, click on **Smart Card Utility Program**. The Smart Card Utility Program screen appears.



Smart card reader 1

Card type:
Card ID:
Card description:
PIN status:

Zone enroll status:
Zone ID:
Zone description:
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 or key token	Length

Smart card reader 2

Card type:
Card ID:
Card description:
PIN status:

Zone enroll status:
Zone ID:
Zone description:
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 or key token	Length

Figure 289. 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 287.
- “Display smart card key identifiers” on page 288
- 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 290.
- “Backup a CA smart card” on page 293.
- “Change PIN of a CA smart card” on page 294.

Tasks associated with the drop down menu for **TKE Smart Card** are:

- “Initialize and enroll a TKE smart card” on page 295.
- “Personalize a TKE smart card” on page 296.
- “Unblock PIN on a TKE smart card” on page 297.
- “Change PIN of a TKE smart card” on page 297..

Tasks associated with the drop down menu for **Crypto Adapter** are:

- "Enroll a TKE cryptographic adapter" on page 297.
- "View current zone" on page 306.

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.

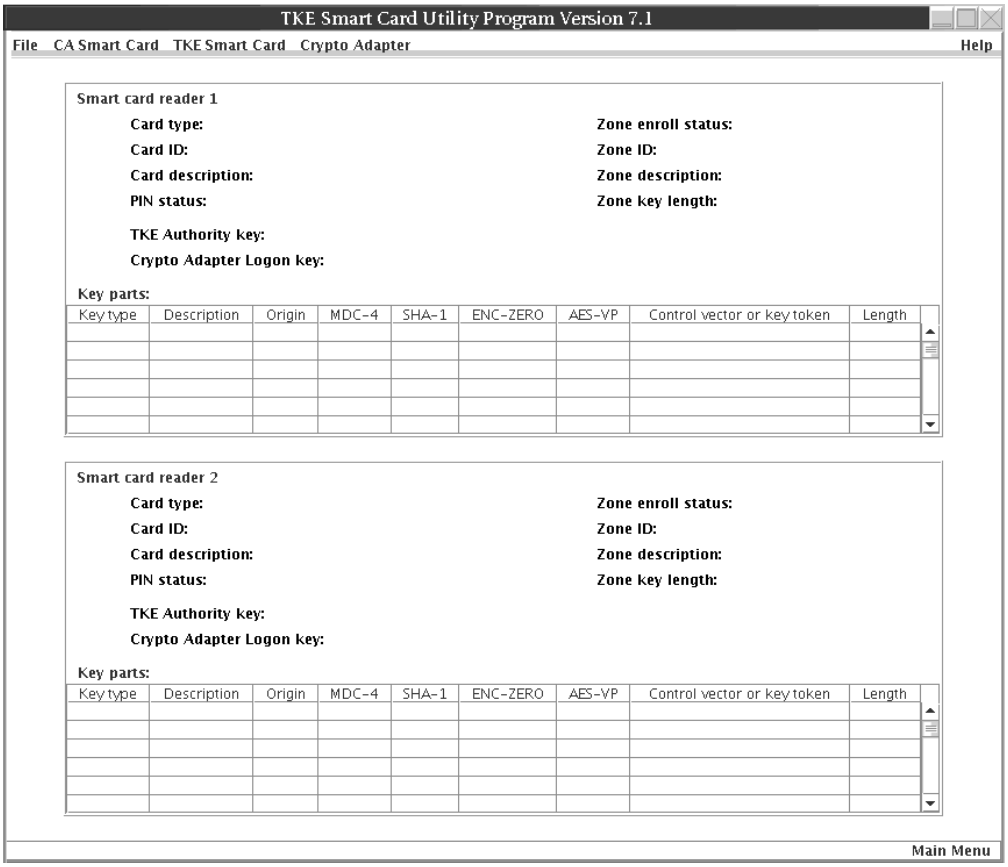


Figure 290. Display smart card information

The panel provides the following information on the smart card:

- **Card type**: Identifies the type and applet version of the smart card in the reader. TKE supports CA, TKE, MCA, IA, and KPH smart cards.
- **Card ID**: A 9-digit identifier generated when the smart card is initialized.
- **Card description**: This is the description you entered when creating the smart card. Can be 30 characters in length.
- **PIN status**: OK, Blocked or Not set
- **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 or MCA smart card is created, the system will generate an 8-digit zone number.
- **Zone Description**: This is the description you entered when creating the CA or MCA smart card. Can be 12 characters in length.
- **Zone key length:** The length of the zone certificate public modulus in bits.

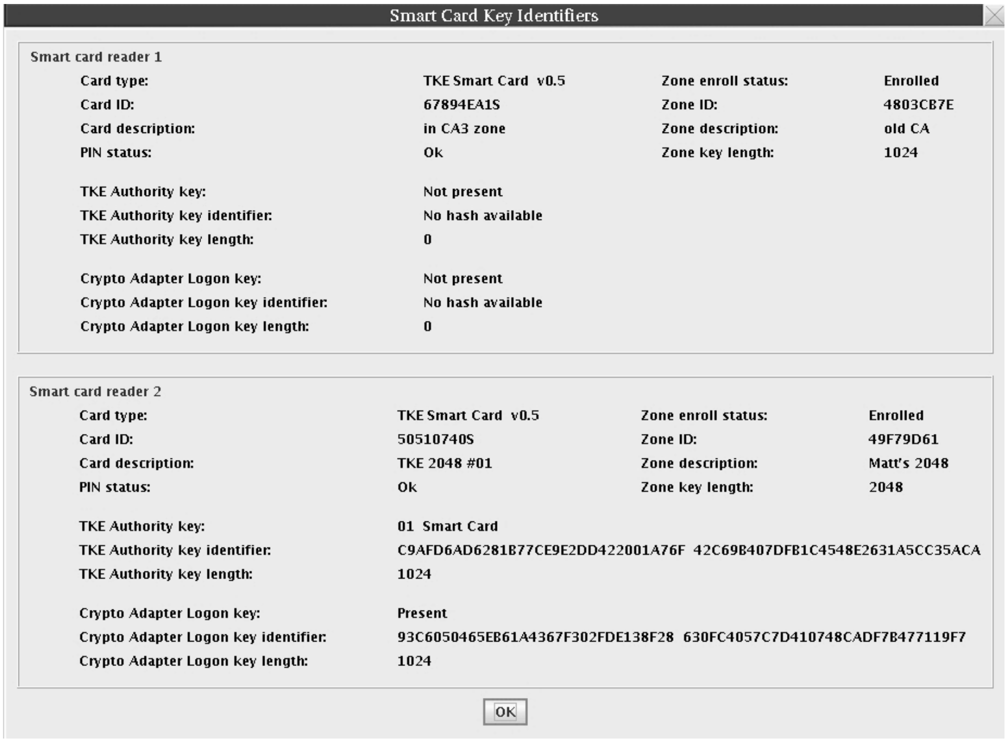
Only TKE smart cards store key parts, so fields in the **Key parts** table are filled in only for TKE smart cards.

- **Key type**: operational key parts, TKE crypto adapter master key parts, or ICSF master key parts
- **Description**: description of key part (optional)
- **Origin**: Crypto Adapter or PIN-PAD
- **MDC-4**: MDC-4 hash value of the key part
- **SHA-1**: SHA-1 hash value of the key part
- **ENC-ZERO**: ENC-ZERO hash value of the key part
- **AES-VP**: AES verification pattern of the key part
- **Control vector or key attributes**: For DES operational key parts and AES DATA operational key parts, contains the control vector. For AES CIPHER, EXPORTER, and IMPORTER operational key parts, indicates whether the key part uses the default key attributes or custom key attributes. Blank for master key parts.
- **Length**: 8, 16, 24 or 32 bytes

Display smart card key identifiers

This function displays the key identifiers and key lengths for the TKE Authority Key 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.



Smart Card Key Identifiers

Smart card reader 1

Card type:	TKE Smart Card v0.5	Zone enroll status:	Enrolled
Card ID:	67894EA1S	Zone ID:	4803CB7E
Card description:	in CA3 zone	Zone description:	old CA
PIN status:	Ok	Zone key length:	1024
TKE Authority key:	Not present		
TKE Authority key identifier:	No hash available		
TKE Authority key length:	0		
Crypto Adapter Logon key:	Not present		
Crypto Adapter Logon key identifier:	No hash available		
Crypto Adapter Logon key length:	0		

Smart card reader 2

Card type:	TKE Smart Card v0.5	Zone enroll status:	Enrolled
Card ID:	50510740S	Zone ID:	49F79D61
Card description:	TKE 2048 #01	Zone description:	Matt's 2048
PIN status:	Ok	Zone key length:	2048
TKE Authority key:	01 Smart Card		
TKE Authority key identifier:	C9AFD6AD6281B77CE9E2DD422001A76F 42C69B407DFB1C4548E2631A5CC35ACA		
TKE Authority key length:	1024		
Crypto Adapter Logon key:	Present		
Crypto Adapter Logon key identifier:	93C6050465EB61A4367F302FDE138F28 630FC4057C7D410748CADF7B477119F7		
Crypto Adapter Logon key length:	1024		

Figure 291. Display of smart card key identifiers

The panel provides this information on the smart card:

- **Card type**: Identifies the type and applet version of the smart card in the reader. TKE supports CA, TKE, MCA, IA, and KPH smart cards.
- **Card ID**: A 9-digit identifier generated when the smart card is initialized.
- **Card description**: This is the description you entered when creating the smart card. Can be 30 characters in length.
- **PIN status**: OK, Blocked or Not set
- **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 or MCA smart card is created, the system will generate an 8-digit zone number.

- **Zone Description**: This is the description you entered when creating the CA or MCA smart card. Can be 12 characters in length.
- **Zone key length**: The length of the zone certificate public modulus in bits.

CA Smart Card Menu Functions

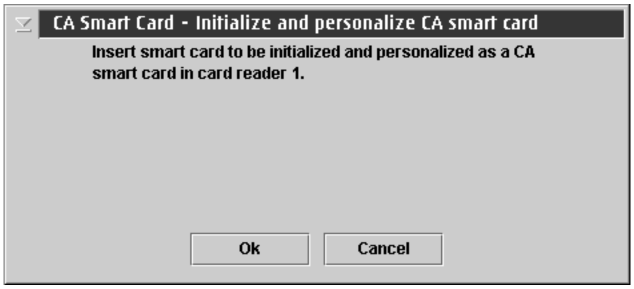
Initialize and personalize the CA smart card

A zone is created when a CA smart card is initialized and personalized.

Note: In general, CA smart cards created on a particular TKE release cannot be used on TKE workstations that are at prior release levels. There are exceptions. See “Smart Card Usage” on page 34 for more information.

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.

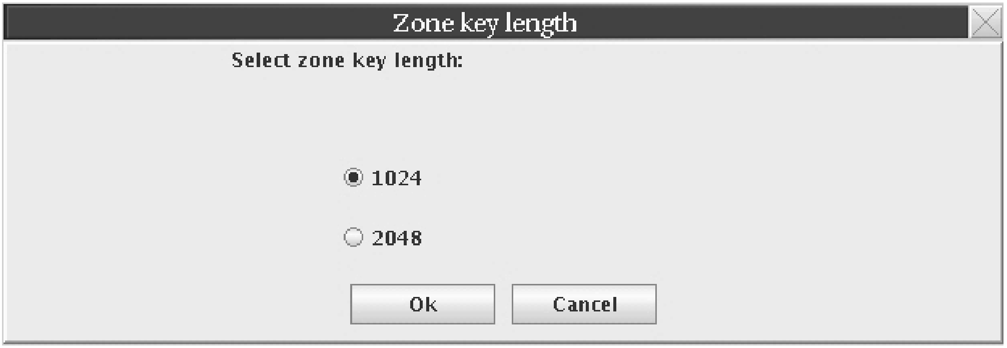


CA Smart Card - Initialize and personalize CA smart card

Insert smart card to be initialized and personalized as a CA smart card in card reader 1.

Figure 292. 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.



Zone key length

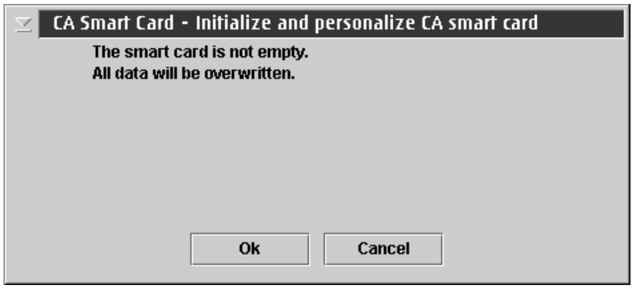
Select zone key length:

● 1024

○ 2048

Figure 293. Zone key length window

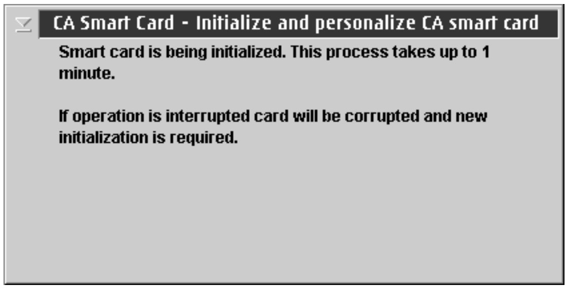
4. If the smart card is not empty, a message is displayed indicating that the smart card is not empty and all data will be overwritten. If this is acceptable click **OK**.



The smart card is not empty.
All data will be overwritten.

Figure 294. Message if card is not empty

5. The smart card will now be initialized.

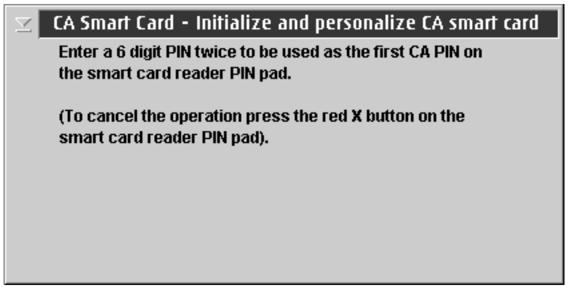


Smart card is being initialized. This process takes up to 1 minute.

If operation is interrupted card will be corrupted and new initialization is required.

Figure 295. 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.

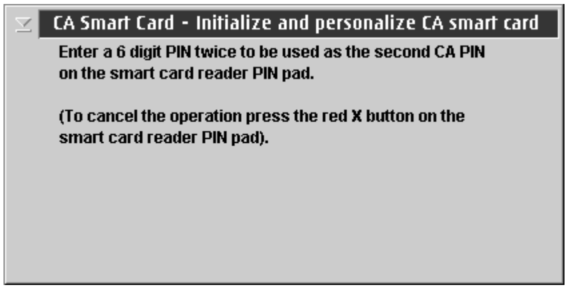


Enter a 6 digit PIN twice to be used as the first CA PIN on the smart card reader PIN pad.

(To cancel the operation press the red X button on the smart card reader PIN pad).

Figure 296. 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.

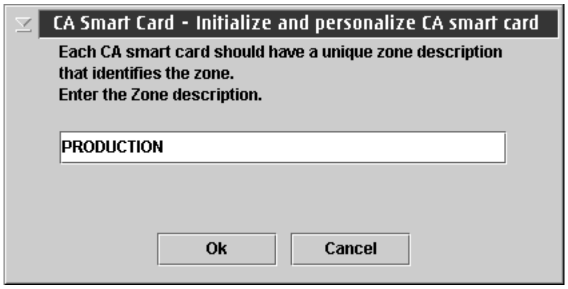

CA Smart Card - Initialize and personalize CA smart card

Enter a 6 digit PIN twice to be used as the second CA PIN
on the smart card reader PIN pad.

(To cancel the operation press the red X button on the
smart card reader PIN pad).

Figure 297. 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.

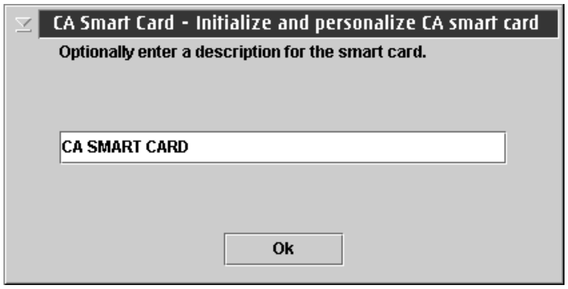

CA Smart Card - Initialize and personalize CA smart card

Each CA smart card should have a unique zone description
that identifies the zone.
Enter the Zone description.

PRODUCTION

Figure 298. Enter zone description for CA smart card

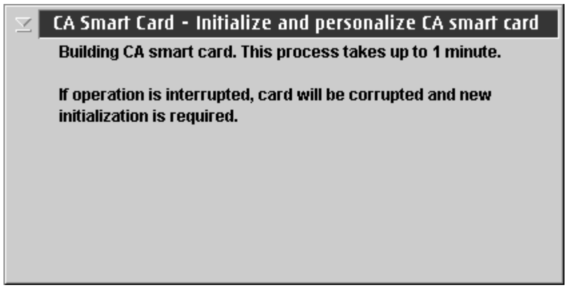
9. A dialog displays, prompting you to enter a CA smart card description. Although a smart card description is optional, it is recommended that you specify one. After the description is entered the CA Smart Card will be built.


CA Smart Card - Initialize and personalize CA smart card

Optionally enter a description for the smart card.

CA SMART CARD

Figure 299. Enter card description for CA smart card


CA Smart Card - Initialize and personalize CA smart card

Building CA smart card. This process takes up to 1 minute.

If operation is interrupted, card will be corrupted and new
initialization is required.

Figure 300. Building a CA smart card

10. You will get a message that a CA Smart Card was successfully created.

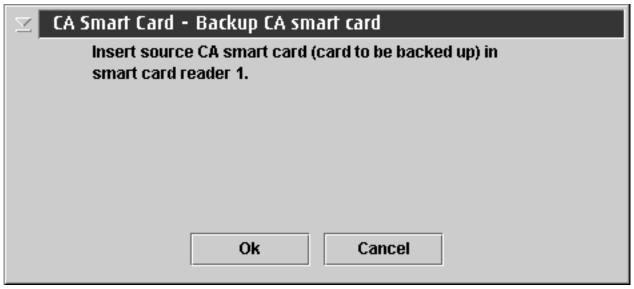
Backup a CA smart card

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 JCOP 41 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.

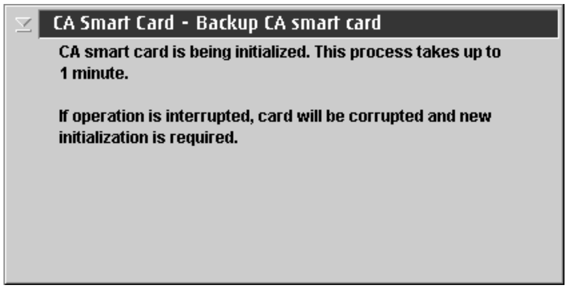


CA Smart Card - Backup CA smart card

Insert source CA smart card (card to be backed up) in smart card reader 1.

Figure 301. 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.

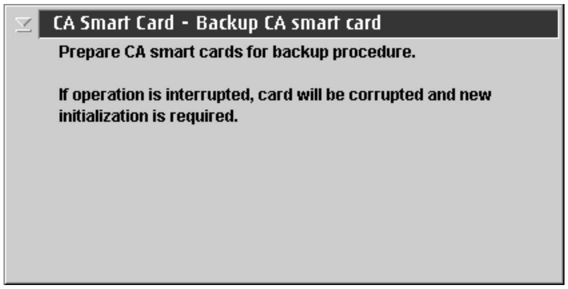


CA Smart Card - Backup CA smart card

CA smart card is being initialized. This process takes up to 1 minute.

If operation is interrupted, card will be corrupted and new initialization is required.

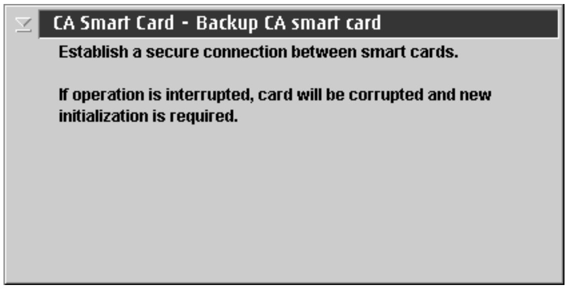
Figure 302. Initialization of backup CA smart card


CA Smart Card - Backup CA smart card

Prepare CA smart cards for backup procedure.

If operation is interrupted, card will be corrupted and new initialization is required.

Figure 303. Continue creation of backup CA smart card

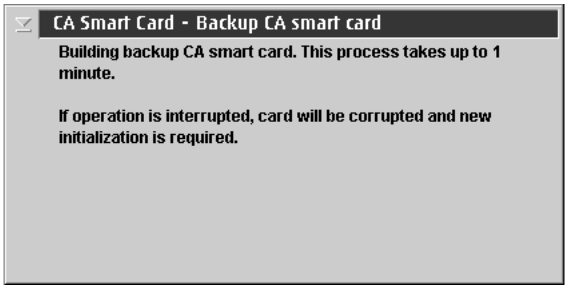

CA Smart Card - Backup CA smart card

Establish a secure connection between smart cards.

If operation is interrupted, card will be corrupted and new initialization is required.

Figure 304. 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.


CA Smart Card - Backup CA smart card

Building backup CA smart card. This process takes up to 1 minute.

If operation is interrupted, card will be corrupted and new initialization is required.

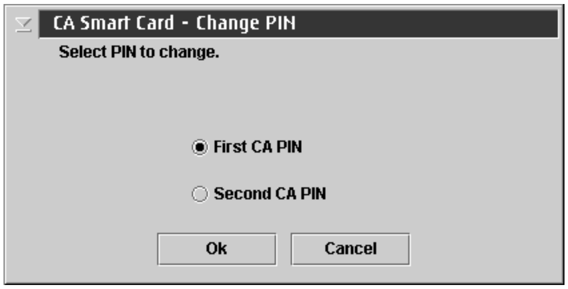
Figure 305. Building backup CA smart card

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.


CA Smart Card - Change PIN

Select PIN to change.

● First CA PIN

○ Second CA PIN

Figure 306. 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.

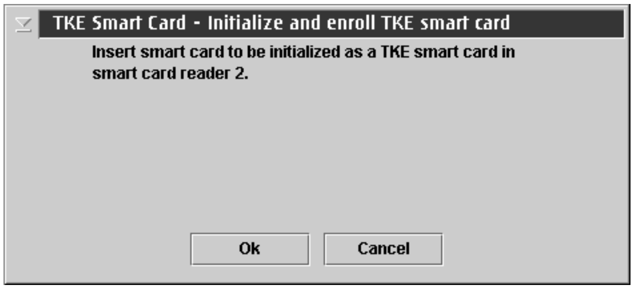
Initialize and enroll a TKE smart card

In general, TKE smart cards created on a particular TKE release cannot be used on TKE workstations that are at prior release levels. There are exceptions. See “Smart Card Usage” on page 34 for more information.

To initialize a TKE smart card, follow these steps:

1. From the *TKE Smart Card* drop down menu, select *Initialize and enroll TKE smart card* option.
2. At the prompt, insert a CA smart card (into smart card reader 1) belonging to the zone you want to enroll the TKE smart card in.
3. Enter the first CA PIN on the PIN pad of smart card reader 1.
4. Enter the second CA PIN on the PIN pad of smart card reader 1.

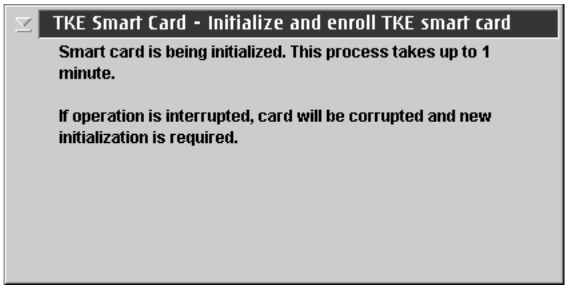
   Note: If you have entered the two PINs for the CA card, have not restarted SCUP, and have not removed the CA card, the two PINs (of the CA smart card) may not require reentry when you are initializing TKE smart cards. This feature is only used when initializing TKE smart cards. All other functions that require the CA PINs will require reentry every time.
5. At the prompt, insert in smart card reader 2 a smart card to be initialized as a TKE smart card.


TKE Smart Card - Initialize and enroll TKE smart card

Insert smart card to be initialized as a TKE smart card in smart card reader 2.

Figure 307. Initialize and enroll TKE smart card

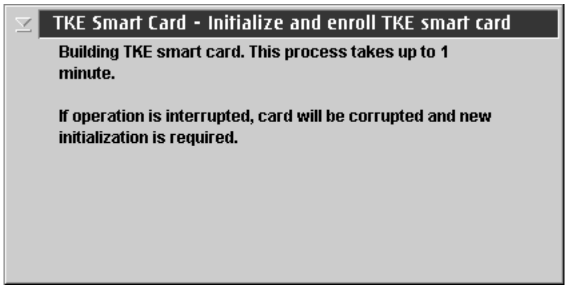
6. If the card is not empty, you will be asked to overwrite all of the data on the smart card.
7. You will see screens indicating that the smart card is being initialized and then the TKE smart card is being built.


TKE Smart Card - Initialize and enroll TKE smart card

Smart card is being initialized. This process takes up to 1 minute.

If operation is interrupted, card will be corrupted and new initialization is required.

Figure 308. Initializing TKE smart card


TKE Smart Card - Initialize and enroll TKE smart card

Building TKE smart card. This process takes up to 1 minute.

If operation is interrupted, card will be corrupted and new initialization is required.

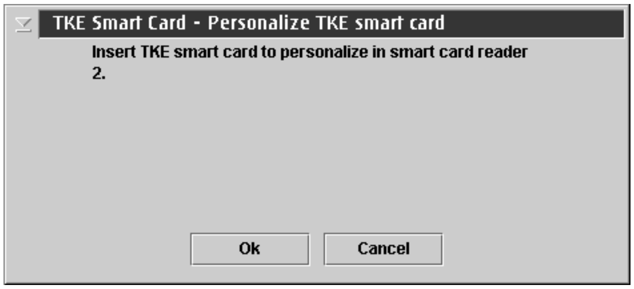
Figure 309. Building TKE smart card

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.



TKE Smart Card - Personalize TKE smart card

Insert TKE smart card to personalize in smart card reader 2.

Figure 310. 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.

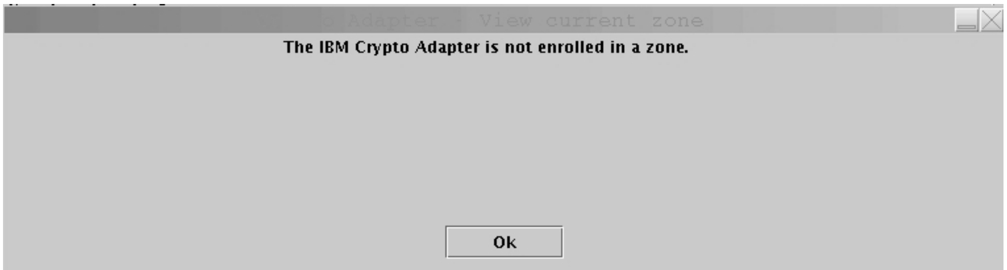
Crypto Adapter Menu Functions

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.



The IBM Crypto Adapter is not enrolled in a zone.

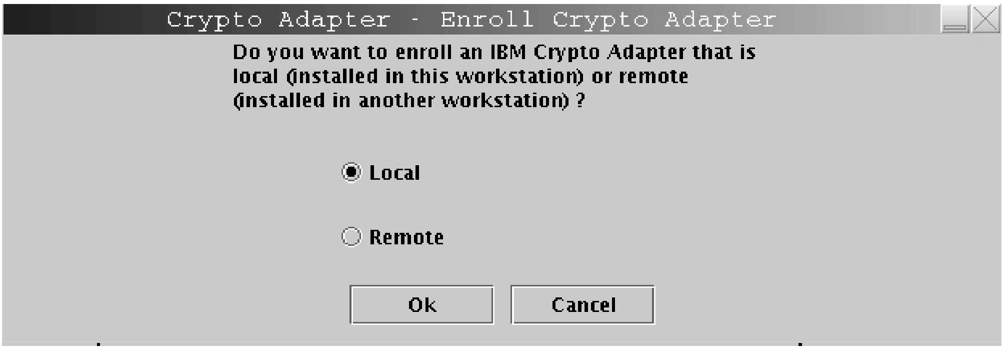
Figure 311. View current zone for a TKE cryptographic adapter

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 250). 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.



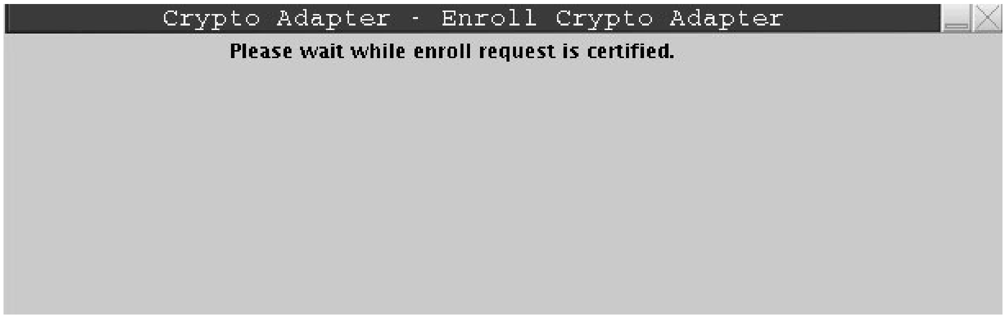
Do you want to enroll an IBM Crypto Adapter that is local (installed in this workstation) or remote (installed in another workstation) ?

● Local

○ Remote

Figure 312. Select local zone

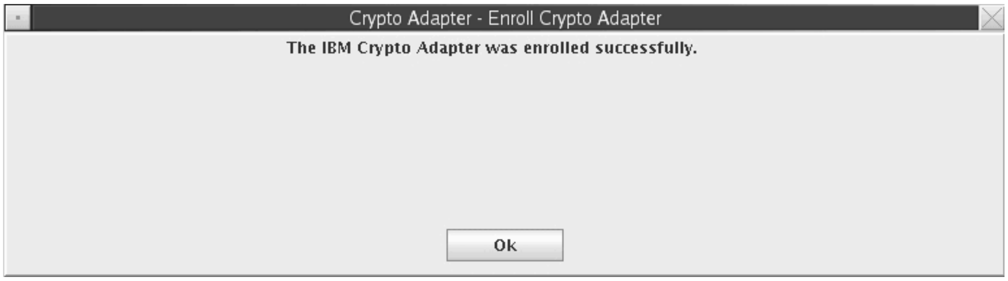
3. At the prompt, insert the CA smart card in smart card reader 1.
4. At the prompt, enter the first CA PIN on the PIN pad of smart card reader 1.
5. At the prompt, enter the second CA PIN on the PIN pad of smart card reader 1.
6. You will get a message that the enrollment for the crypto adapter was successful.



Crypto Adapter - Enroll Crypto Adapter

Please wait while enroll request is certified.

Figure 313. Certifying request for local Crypto Adapter enrollment

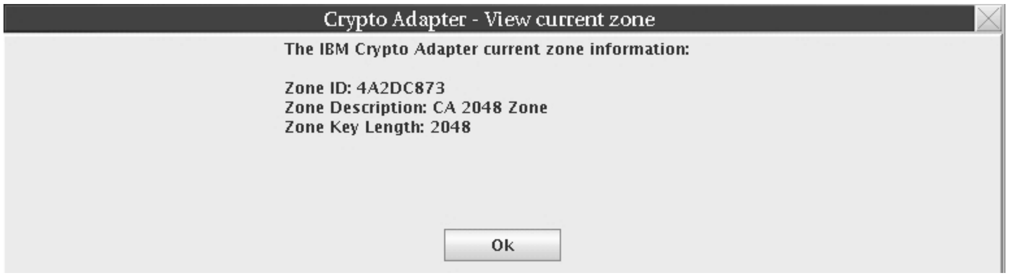


Crypto Adapter - Enroll Crypto Adapter

The IBM Crypto Adapter was enrolled successfully.

Figure 314. 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.



Crypto Adapter - View current zone

The IBM Crypto Adapter current zone information:

Zone ID: 4A2DC873
Zone Description: CA 2048 Zone
Zone Key Length: 2048

Figure 315. View current zone after Crypto Adapter enrollment

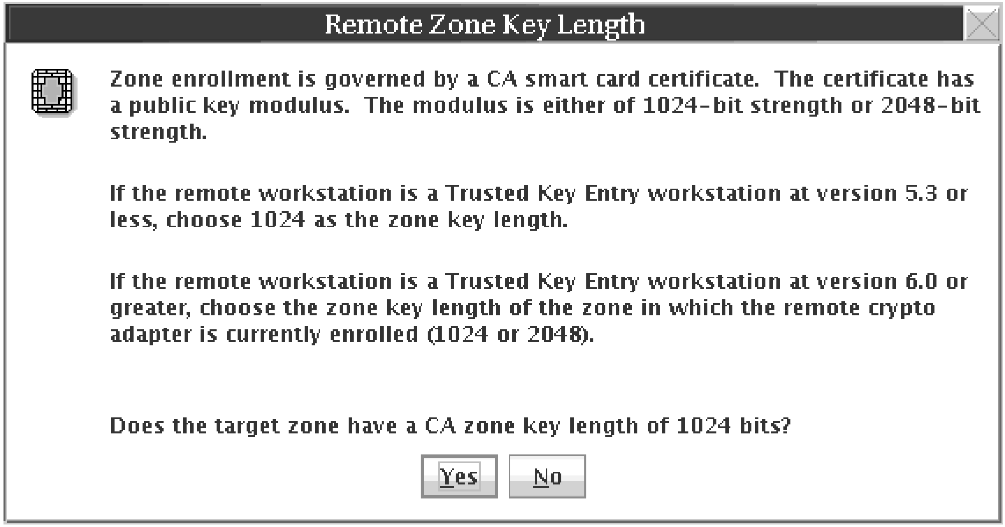
Remote/Secondary Crypto Adapter Enrollment

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 Crypto Adapter installed in this workstation. Continue?"`
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".



Remote Zone Key Length

Zone enrollment is governed by a CA smart card certificate. The certificate has a public key modulus. The modulus is either of 1024-bit strength or 2048-bit strength.

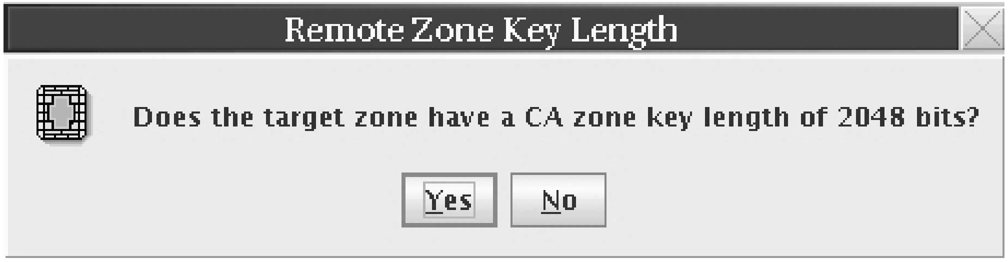
If the remote workstation is a Trusted Key Entry workstation at version 5.3 or less, choose 1024 as the zone key length.

If the remote workstation is a Trusted Key Entry workstation at version 6.0 or greater, choose the zone key length of the zone in which the remote crypto adapter is currently enrolled (1024 or 2048).

Does the target zone have a CA zone key length of 1024 bits?

Figure 316. 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?"



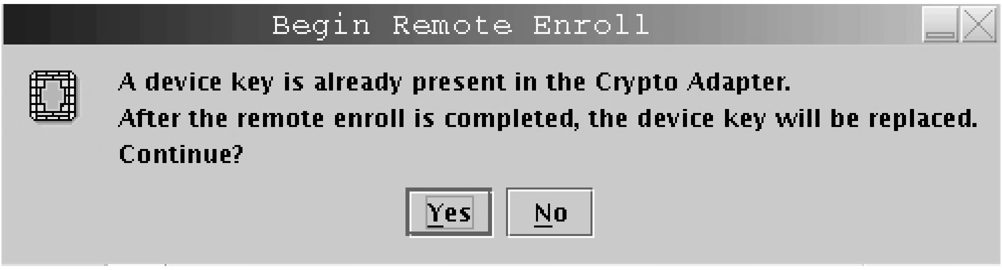
Remote Zone Key Length

Does the target zone have a CA zone key length of 2048 bits?

Figure 317. 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.

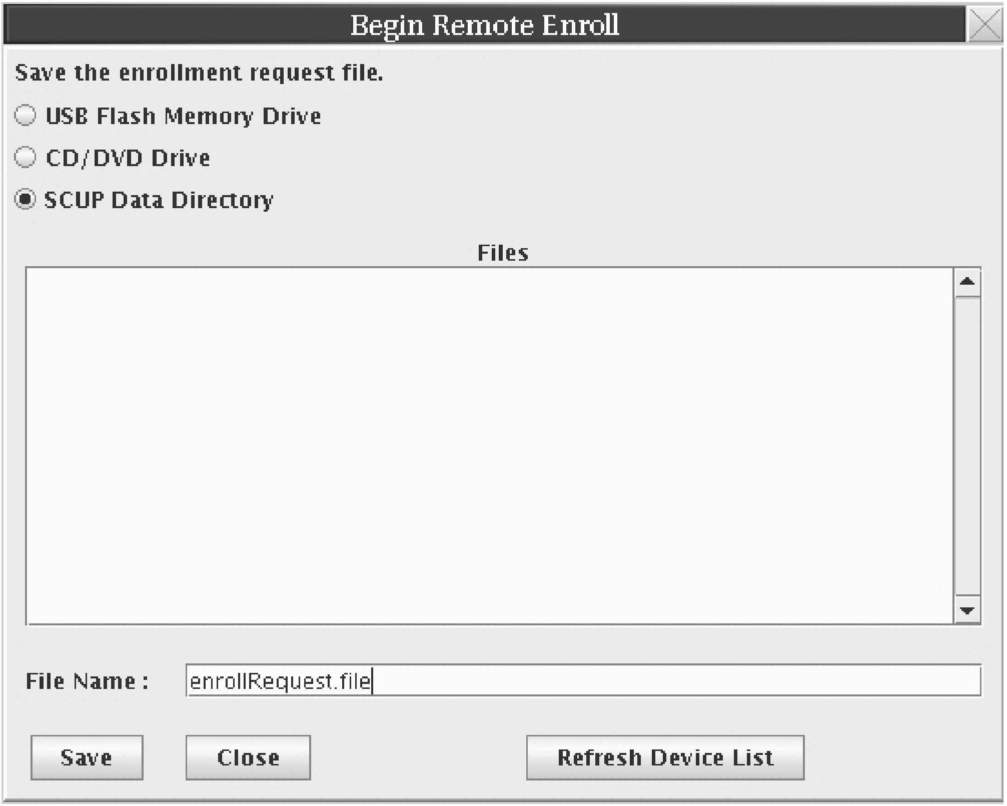


Begin Remote Enroll

A device key is already present in the Crypto Adapter.
After the remote enroll is completed, the device key will be replaced.
Continue?

Figure 318. Crypto Adapter Enrolled

6. A panel will display, asking you where to save the enrollment request file. Enter the destination and file name and click on Save.



Begin Remote Enroll

Save the enrollment request file.

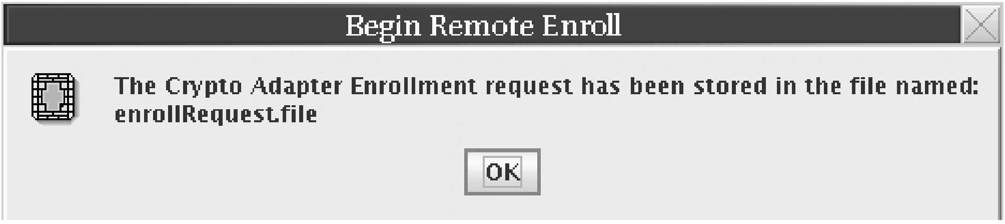
○ USB Flash Memory Drive

○ CD/DVD Drive

● SCUP Data Directory

File Name : enrollRequest.file

Figure 319. Save Enrollment Request



Begin Remote Enroll

The Crypto Adapter Enrollment request has been stored in the file named: enrollRequest.file

Figure 320. Enrollment Request Stored

Warnings:

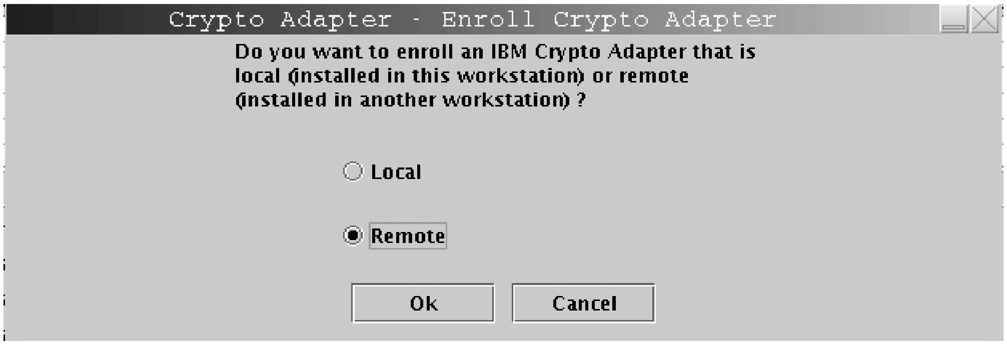
a. If the file is saved to DVD-RAM, you must deactivate the CD/DVD drive before removing the DVD-RAM disc. For details on deactivating media see “TKE Media Manager” on page 334.

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.

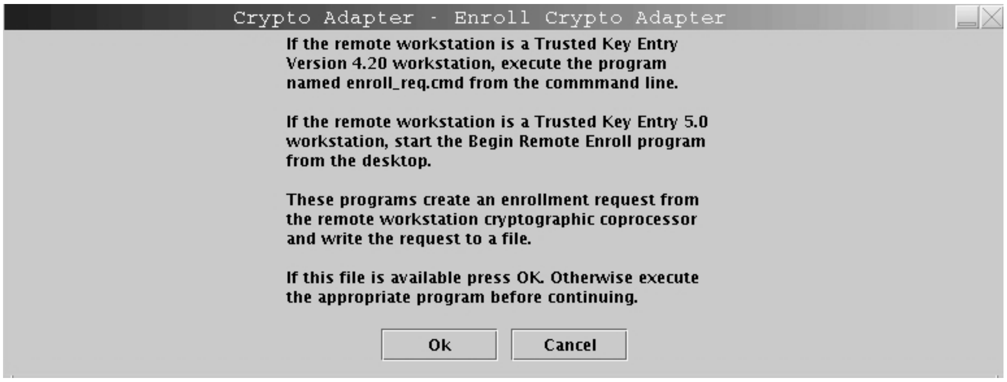


Do you want to enroll an IBM Crypto Adapter that is local (installed in this workstation) or remote (installed in another workstation) ?

○ Local

● Remote

Figure 321. Select remote zone



If the remote workstation is a Trusted Key Entry Version 4.20 workstation, execute the program named enroll_req.cmd from the commmand line.

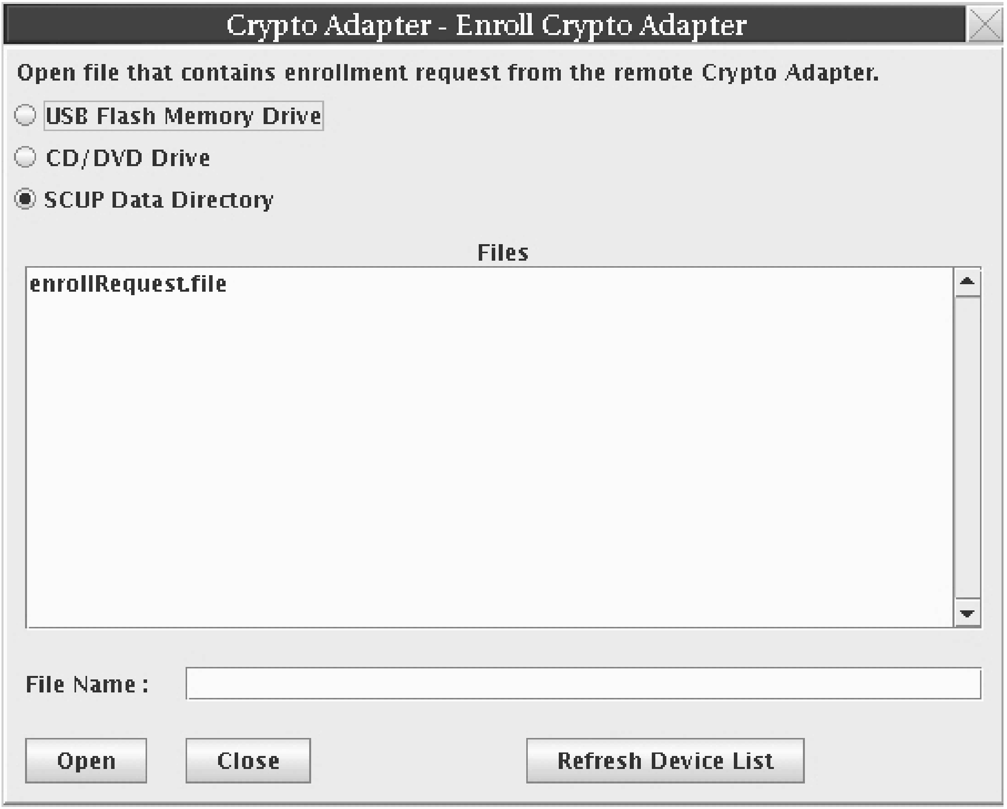
If the remote workstation is a Trusted Key Entry 5.0 workstation, start the Begin Remote Enroll program from the desktop.

These programs create an enrollment request from the remote workstation cryptographic coprocessor and write the request to a file.

If this file is available press OK. Otherwise execute the appropriate program before continuing.

Figure 322. 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 301).



Crypto Adapter - Enroll Crypto Adapter

Open file that contains enrollment request from the remote Crypto Adapter.

○ USB Flash Memory Drive

○ CD/DVD Drive

● SCUP Data Directory

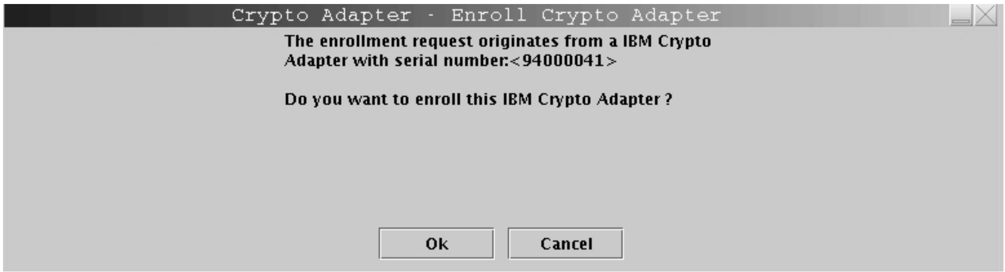
Files

enrollRequest.file

File Name :

Figure 323. 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.



Crypto Adapter - Enroll Crypto Adapter

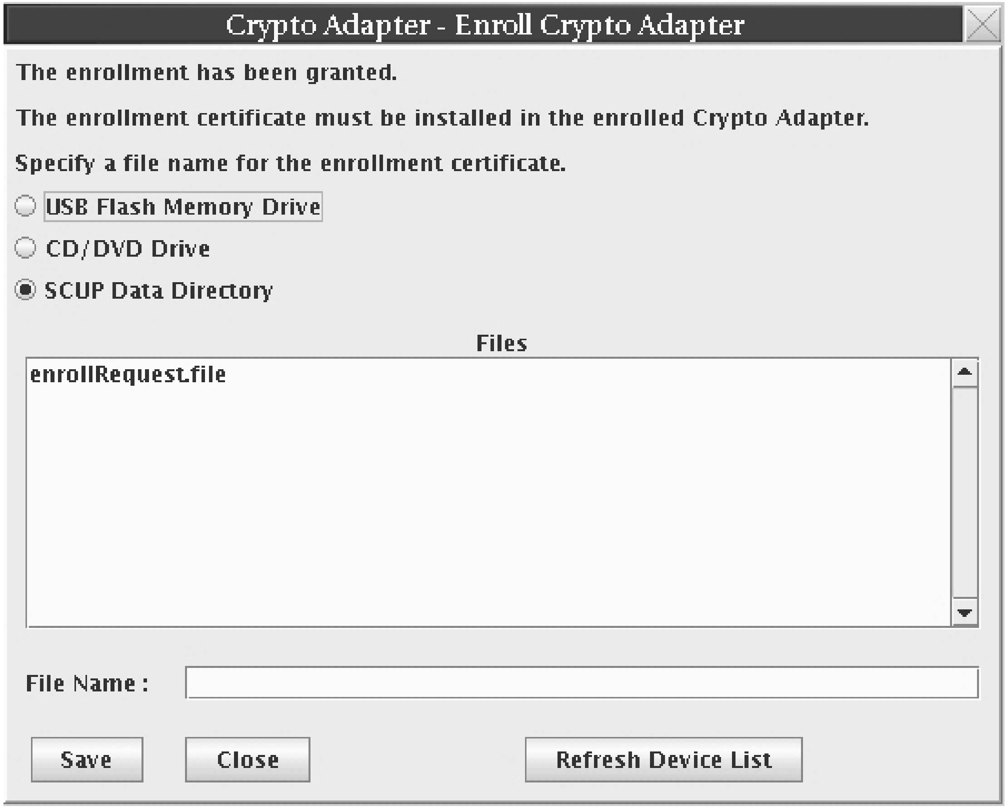
The enrollment request originates from a IBM Crypto Adapter with serial number:<94000041>

Do you want to enroll this IBM Crypto Adapter ?

Figure 324. 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.



Crypto Adapter - Enroll Crypto Adapter

The enrollment has been granted.

The enrollment certificate must be installed in the enrolled Crypto Adapter.

Specify a file name for the enrollment certificate.

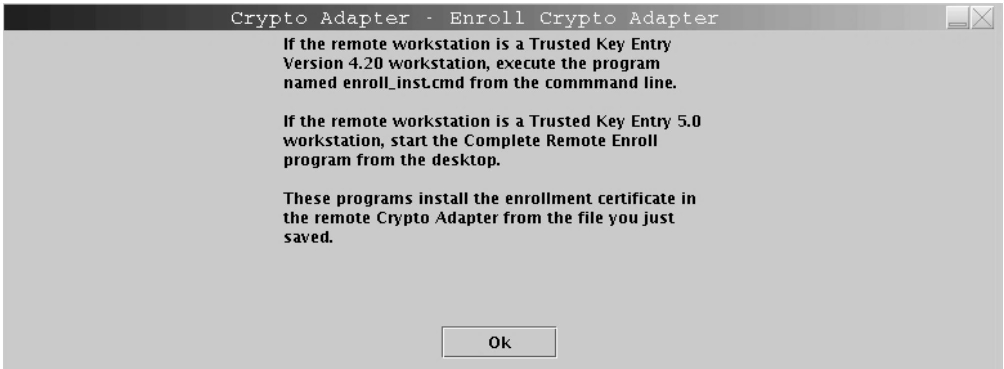
○ USB Flash Memory Drive
○ CD/DVD Drive
● SCUP Data Directory

Files

enrollRequest.file

File Name :

Figure 325. Save the enrollment certificate



Crypto Adapter - Enroll Crypto Adapter

If the remote workstation is a Trusted Key Entry Version 4.20 workstation, execute the program named enroll_inst.cmd from the commmand line.

If the remote workstation is a Trusted Key Entry 5.0 workstation, start the Complete Remote Enroll program from the desktop.

These programs install the enrollment certificate in the remote Crypto Adapter from the file you just saved.

Figure 326. 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 334.

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.

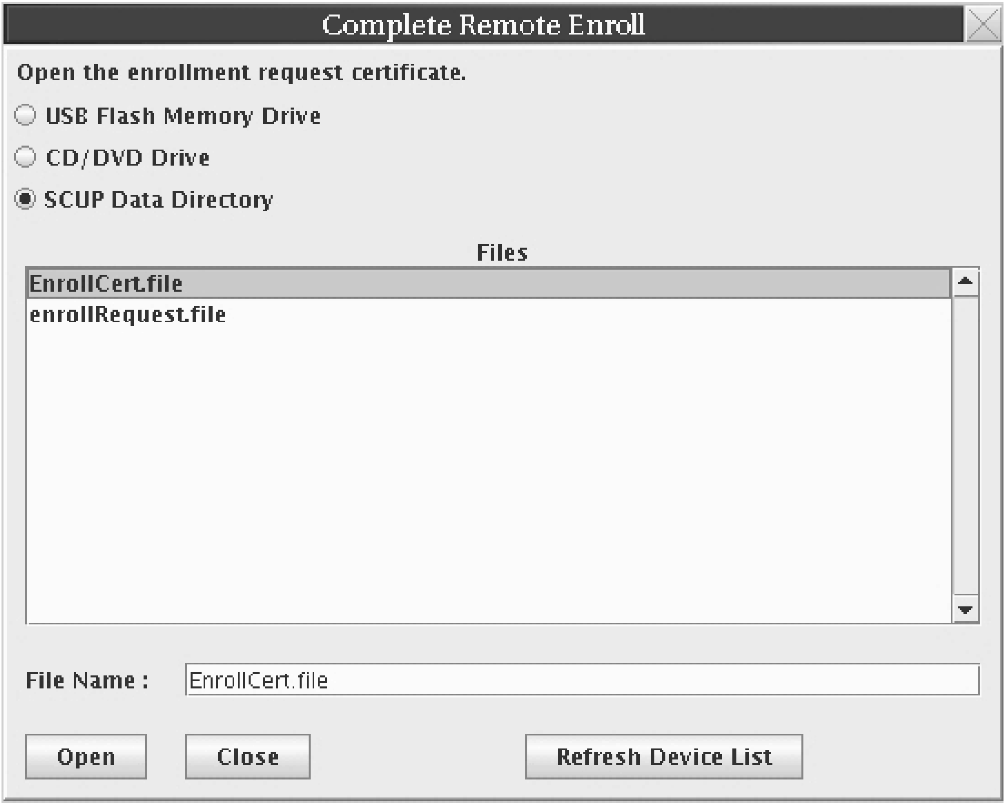
Note: If the remote workstation is TKE 4.2, refer to the TKE Workstation User's Guide, SA22-7524, on Resource Link for details.

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 certificate in the IBM Crypto Adapter installed in this workstation. Continue?"`
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 to identify the file containing the enrollment certificate (from step 16). Select the source and file name and click on Open.

    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 334.

    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.



Complete Remote Enroll

Open the enrollment request certificate.

○ USB Flash Memory Drive

○ CD/DVD Drive

● SCUP Data Directory

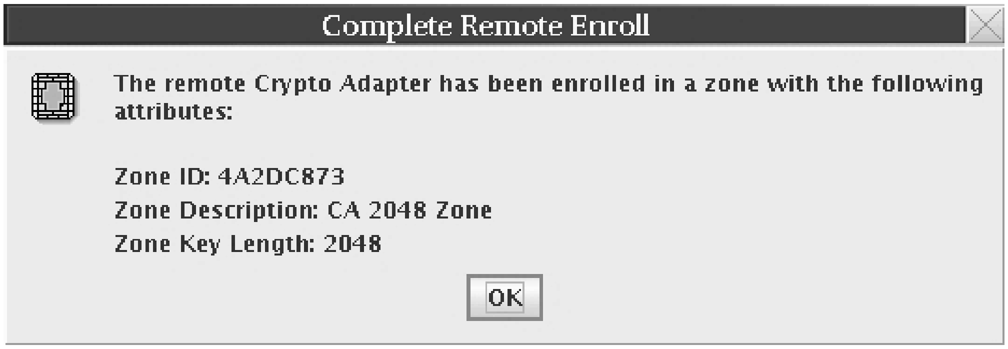
Files

EnrollCert.file
enrollRequest.file

File Name : EnrollCert.file

Figure 327. 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).


Complete Remote Enroll

The remote Crypto Adapter has been enrolled in a zone with the following attributes:

Zone ID: 4A2DC873
Zone Description: CA 2048 Zone
Zone Key Length: 2048

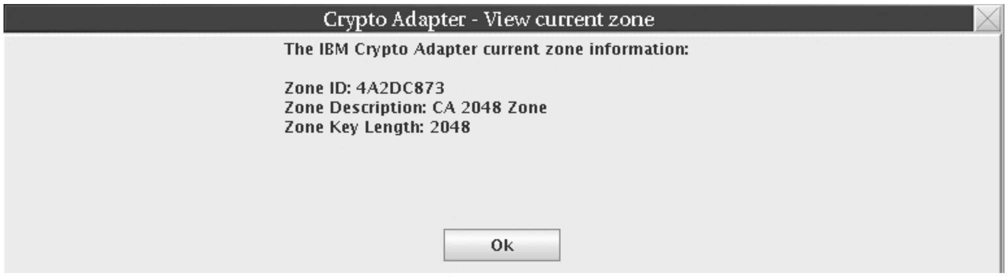
Figure 328. Remote Enroll Success

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.


Crypto Adapter - View current zone

The IBM Crypto Adapter current zone information:

Zone ID: 4A2DC873
Zone Description: CA 2048 Zone
Zone Key Length: 2048

Figure 329. 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

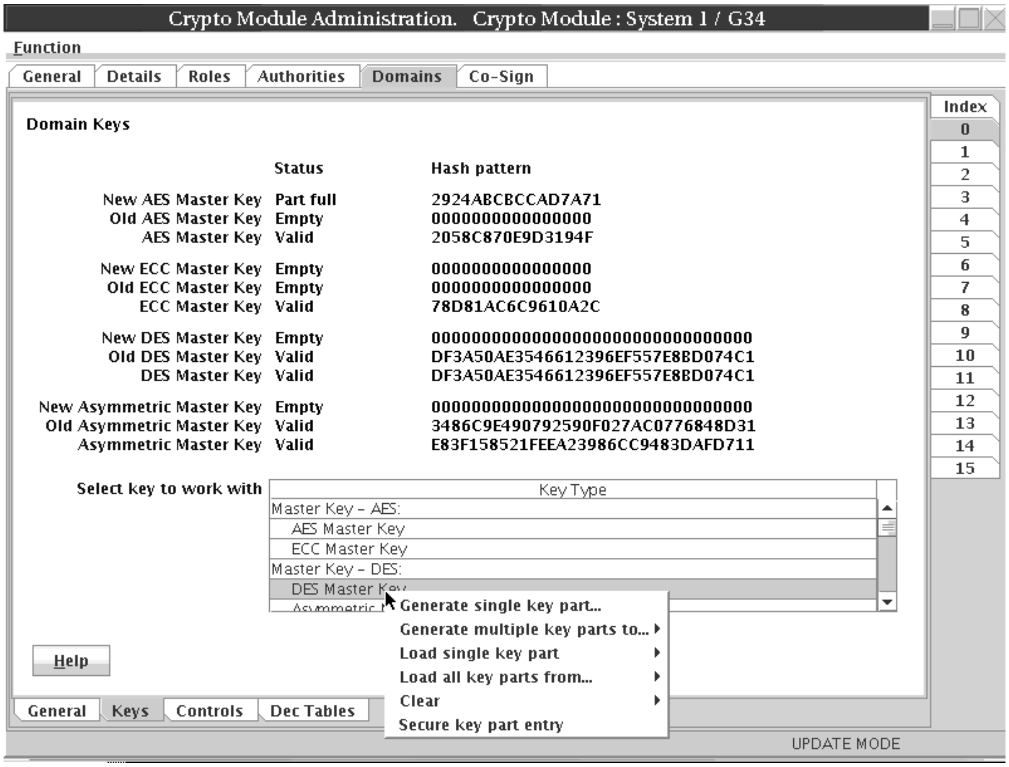
This topic describes how you can enter a known key part value onto a TKE smart card. A known key part will have been saved on paper or in a binary file.

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 310.

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.



Domain Keys

	Status	Hash pattern
New AES Master Key	Part full	2924ABCBCCAD7A71
Old AES Master Key	Empty	0000000000000000
AES Master Key	Valid	2058C870E9D3194F
New ECC Master Key	Empty	0000000000000000
Old ECC Master Key	Empty	0000000000000000
ECC Master Key	Valid	78D81AC6C9610A2C
New DES Master Key	Empty	00000000000000000000000000000000
Old DES Master Key	Valid	DF3A50AE3546612396EF557E8BD074C1
DES Master Key	Valid	DF3A50AE3546612396EF557E8BD074C1
New Asymmetric Master Key	Empty	00000000000000000000000000000000
Old Asymmetric Master Key	Valid	3486C9E490792590F027AC0776848D31
Asymmetric Master Key	Valid	E83F158521FEEA23986CC9483DAFD711

Select key to work with

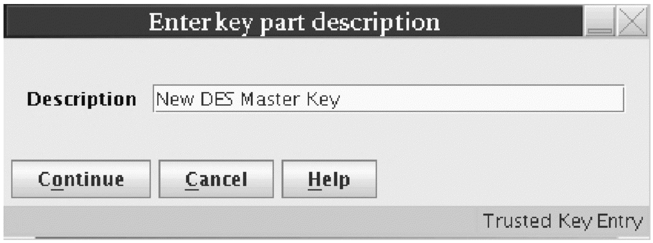
Key Type
Master Key – AES:
AES Master Key
ECC Master Key
Master Key – DES:
DES Master Key
Asymmetric M

Figure 330. 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**.

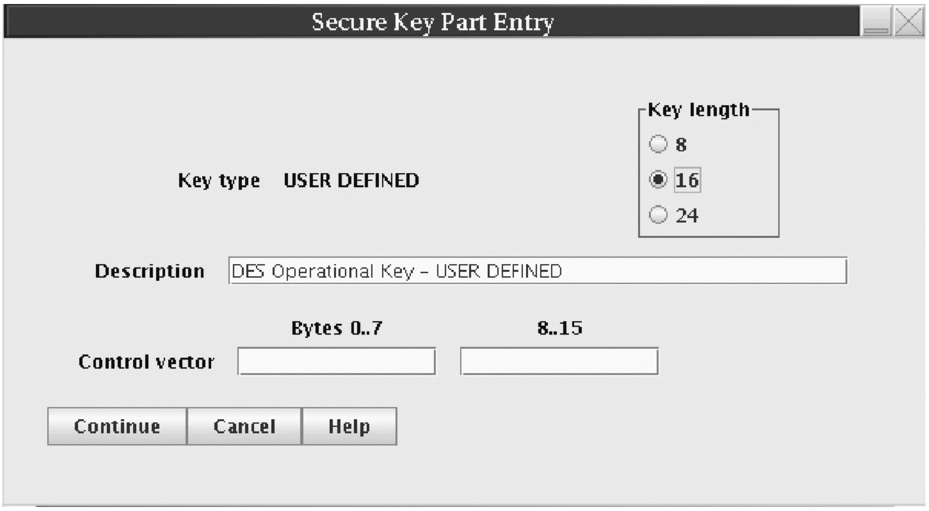
For master keys on all host crypto modules, a panel for entering a key part description displays.



Description: New DES Master Key

Figure 331. Enter description panel for secure key part entry

For operational keys, the Secure Key Part Entry panel displays.



Key type: USER DEFINED

Key length: ○ 8 ● 16 ○ 24

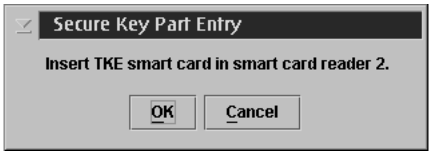
Description: DES Operational Key – USER DEFINED

Figure 332. 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.

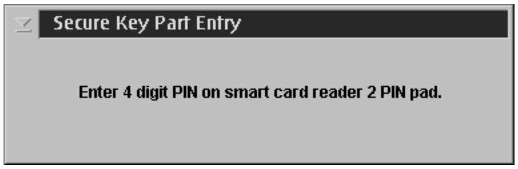
2. After all the appropriate information has been entered for master and operational keys, the user is prompted to insert a TKE smart card into reader 2.



Insert TKE smart card in smart card reader 2.

Figure 333. Secure key part entry — enter TKE smart card into reader

3. Enter the PIN on the smart card reader PIN pad when prompted.

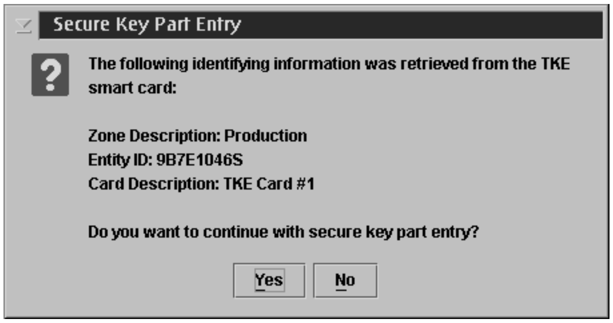

Secure Key Part Entry

Enter 4 digit PIN on smart card reader 2 PIN pad.

Figure 334. 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.


Secure Key Part Entry

The following identifying information was retrieved from the TKE smart card:

Zone Description: Production
Entity ID: 9B7E1046S
Card Description: TKE Card #1

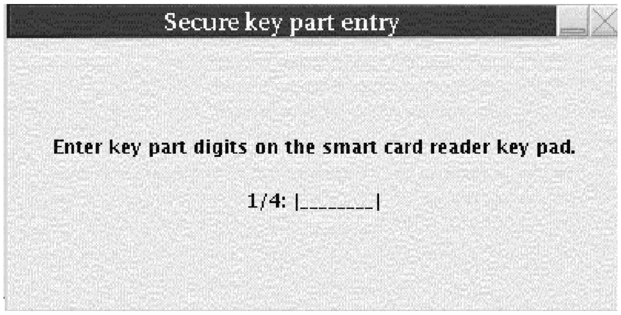
Do you want to continue with secure key part entry?

Figure 335. 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 310.

   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 or the Smart Card Utility Program under Trusted Key Entry Applications. See “Display smart card information” on page 287 or “Display smart card key identifiers” on page 288.


Secure key part entry

Enter key part digits on the smart card reader key pad.

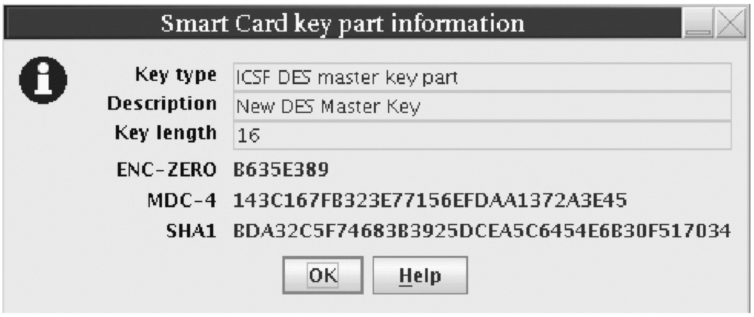
1/4: |________|

Figure 336. Secure key part entry — enter PIN

The dialog shows the progress of each hexadecimal digit entered with an asterisk (*).

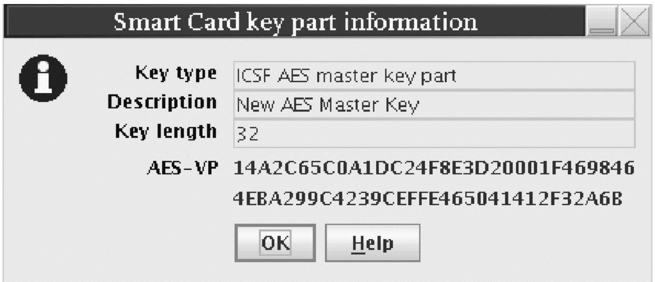
6. After the key part value has been successfully entered on the PIN pad, a panel is displayed with information regarding the key part just entered. The ENC-ZERO, MDC-4, and SHA1 values are shown to the user for verification that the DES key part was entered correctly. The AES-VP value is shown to the 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



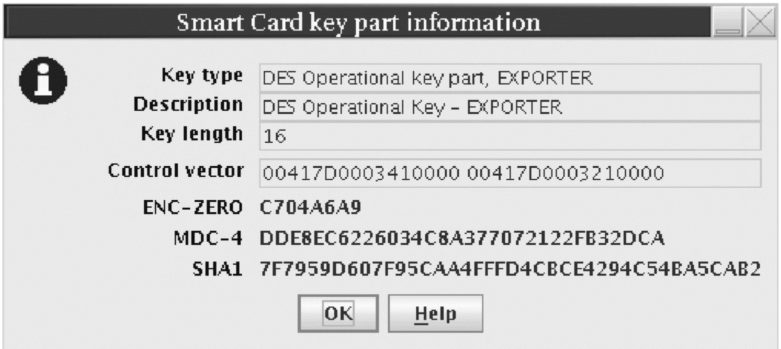
Key type: ICSF DES master key part
Description: New DES Master Key
Key length: 16
ENC-ZERO B635E389
MDC-4 143C167FB323E77156EFDAA1372A3E45
SHA1 BDA32C5F74683B3925DCEA5C6454E6B30F517034

Figure 337. Secure key part entry — DES key part information for a master key



Key type: ICSF AES master key part
Description: New AES Master Key
Key length: 32
AES-VP 14A2C65C0A1DC24F8E3D20001F469846
4EBA299C4239CEFFE465041412F32A6B

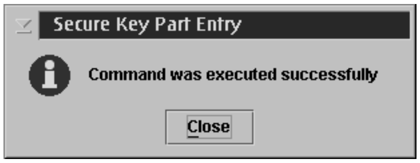
Figure 338. Secure key part entry — AES key part information for a master key



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 7F7959D607F95CAA4FFFD4CBCE4294C54BA5CAB2

Figure 339. Secure key part entry — DES key part information for operational key

7. A message is displayed if the command executed successfully.



Command was executed successfully

Figure 340. 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 31).

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 31. 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 31. 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. 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 command is sent to a domain that is not in a logical partition's control domain index, ICSF returns an error (return code 12, reason code 2015).

There is no specific field to identify a logical partition as a TKE host when you are customizing image profiles. You must decide which logical partition will be the TKE host and set up the control domain index and 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 341 on page 314 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.

TKE Host	TKE Target	TKE Target
LPAR 0	LPAR 1	LPAR 2
Control Domain 0 1 2	Control Domain 1	Control Domain 2
Usage Domain 0	Usage Domain 1	Usage Domain 2
Candidate List 00 01 02 03	Candidate List 00 01 02 03	Candidate List 00 01 02 03

Figure 341. An Example of TKE Host and TKE Target LPARs without Domain Sharing

The example in Figure 342 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.

TKE Host	TKE Target	TKE Target	TKE Target
LPAR 0	LPAR 1	LPAR 2	LPAR 3
Control Domain 0 1 3	Control Domain 1	Control Domain 1	Control Domain 3
Usage Domain 0	Usage Domain 1	Usage Domain 1	Usage Domain 3
Candidate List 00 01 02 03	Candidate List 00 01	Candidate List 02 03	Candidate List 00 01 02 03

Figure 342. 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 C. Trusted Key Entry - Workstation Cryptographic Adapter Initialization

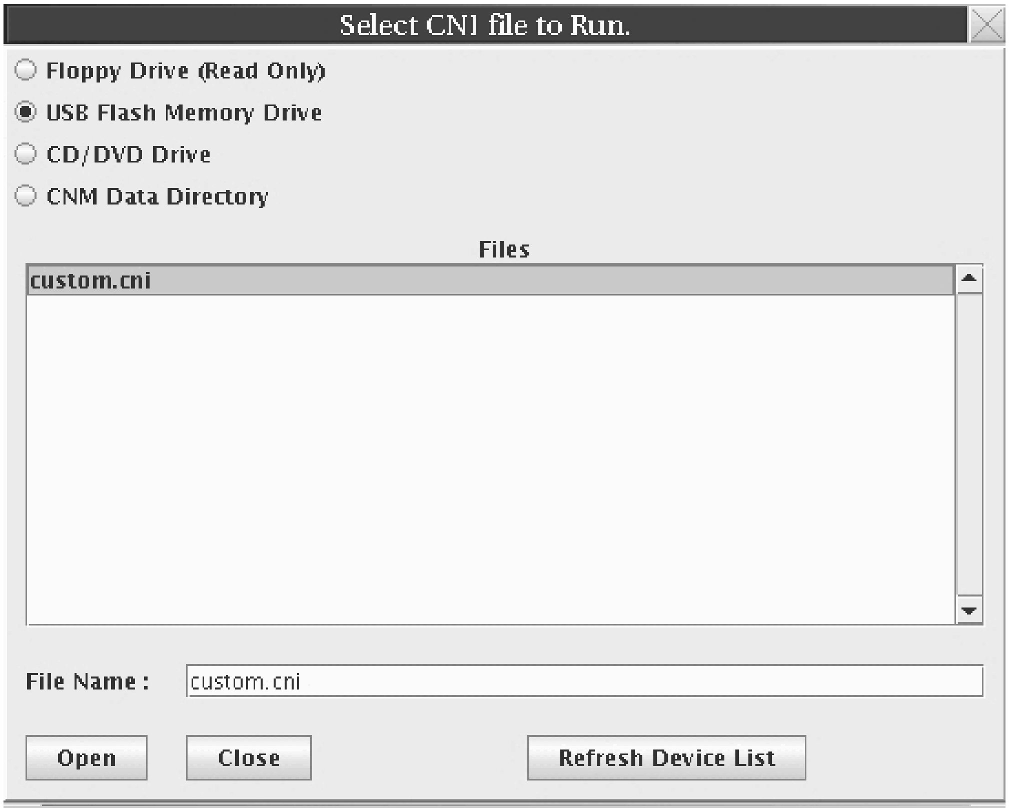
Cryptographic Node Management Batch Initialization

The Cryptographic Node Management Batch Initialization task allows the user to execute user created scripts.

User-defined scripts can be created using the CNI editor in the Cryptographic Node Management Utility. Open the Cryptographic Node Management Utility. Click 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 81 and “Initializing TKE for smart cards” on page 87.

To execute a user-defined CNI script, click on **Trusted Key Entry**, and then **Cryptographic Node Management Batch Initialization**. You must be logged onto the console as ADMIN to access this task. The Select CNI file to Run window 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**.



Select CNI file to Run.

○ Floppy Drive (Read Only)

● USB Flash Memory Drive

○ CD/DVD Drive

○ CNM Data Directory

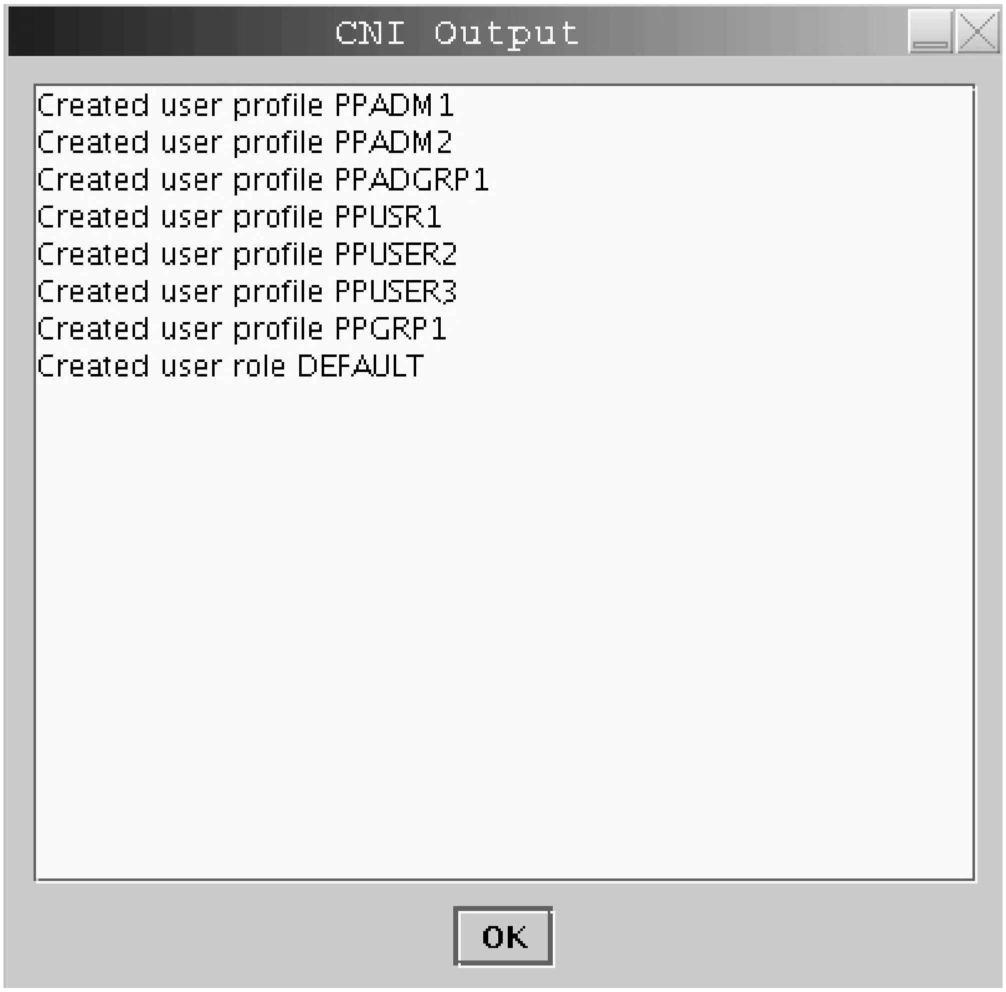
Files

custom.cni

File Name : custom.cni

Figure 343. Cryptographic Node Management Batch Initialization Task Window

The output window shows the operations performed. Select **OK** to exit this task.



```
Created user profile PPADM1
Created user profile PPADM2
Created user profile PPADGRP1
Created user profile PPUSR1
Created user profile PPUSER2
Created user profile PPUSER3
Created user profile PPGRP1
Created user role DEFAULT
```

Figure 344. Cryptographic Node Management Batch Initialization Task Output Window

CCA CLU

The CCA CLU task is used for loading and checking code on the TKE workstation crypto adapter.

For most options, CLU requires exclusive access to the TKE workstation crypto adapter. If another TKE application is running that is using the TKE workstation crypto adapter, CLU will fail and the return code in the Output Log will be 80400010.

To allow CLU to run, the other applications must be ended. If you are using the autostart capability of the TKE Audit Record Upload Configuration Utility, you must disable this feature. To do this, sign onto the TKE console using the AUDITOR logon, select "Trusted Key Entry" in the left window, and select "TKE Audit Record Upload Utility" in the right window. Click on the "Disable autostart" button, if it is present. Then, restart the TKE console application to end all applications that may be using the TKE workstation crypto adapter. Select "Service Management" in the left window, and select "Shutdown or Restart" in the right window. Select "Restart console" and click on the "OK" button.

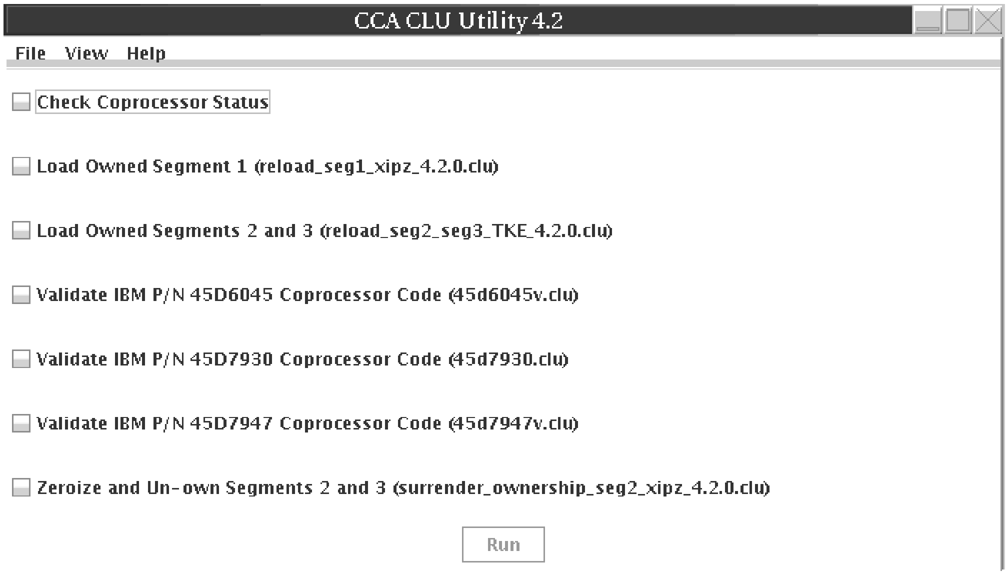
After the TKE console application restarts, run CLU before running any other TKE applications. After you have finished using CLU, re-enable the autostart capability of the TKE Audit Record Upload Utility, if desired.

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**. 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.



□ Check Coprocessor Status

□ Load Owned Segment 1 (reload_seg1_xipz_4.2.0.clu)

□ Load Owned Segments 2 and 3 (reload_seg2_seg3_TKE_4.2.0.clu)

□ Validate IBM P/N 45D6045 Coprocessor Code (45d6045v.clu)

□ Validate IBM P/N 45D7930 Coprocessor Code (45d7930.clu)

□ Validate IBM P/N 45D7947 Coprocessor Code (45d7947v.clu)

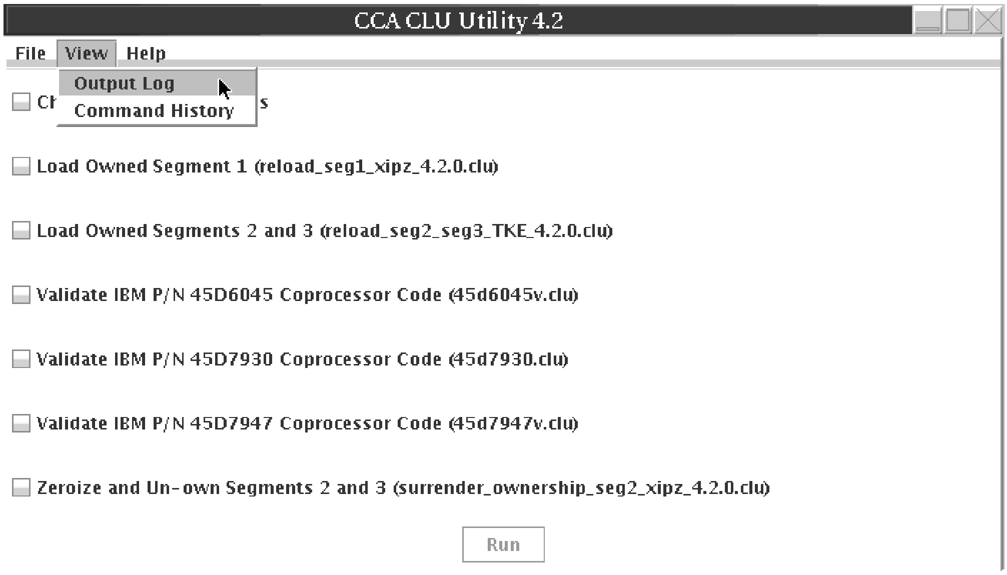
□ Zeroize and Un-own Segments 2 and 3 (surrender_ownership_seg2_xipz_4.2.0.clu)

Figure 345. CLU Command Check Boxes

When RUN is pressed, the commands will execute in the order they appear on the application window.

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.



□ Ch s

□ Load Owned Segment 1 (reload_seg1_xipz_4.2.0.clu)

□ Load Owned Segments 2 and 3 (reload_seg2_seg3_TKE_4.2.0.clu)

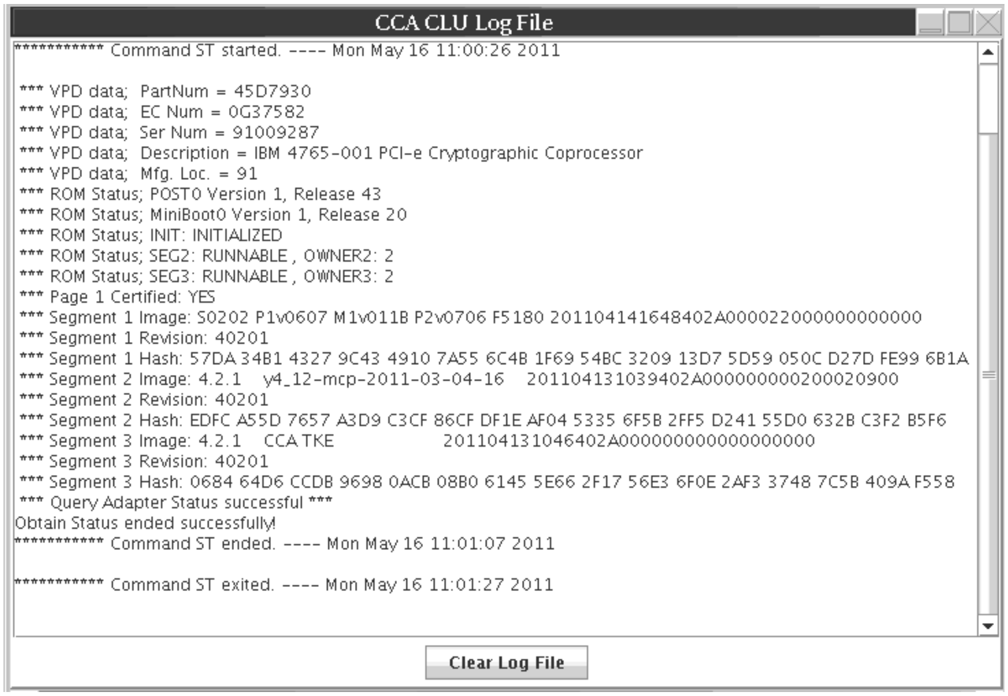
□ Validate IBM P/N 45D6045 Coprocessor Code (45d6045v.clu)

□ Validate IBM P/N 45D7930 Coprocessor Code (45d7930.clu)

□ Validate IBM P/N 45D7947 Coprocessor Code (45d7947v.clu)

□ Zeroize and Un-own Segments 2 and 3 (surrender_ownership_seg2_xipz_4.2.0.clu)

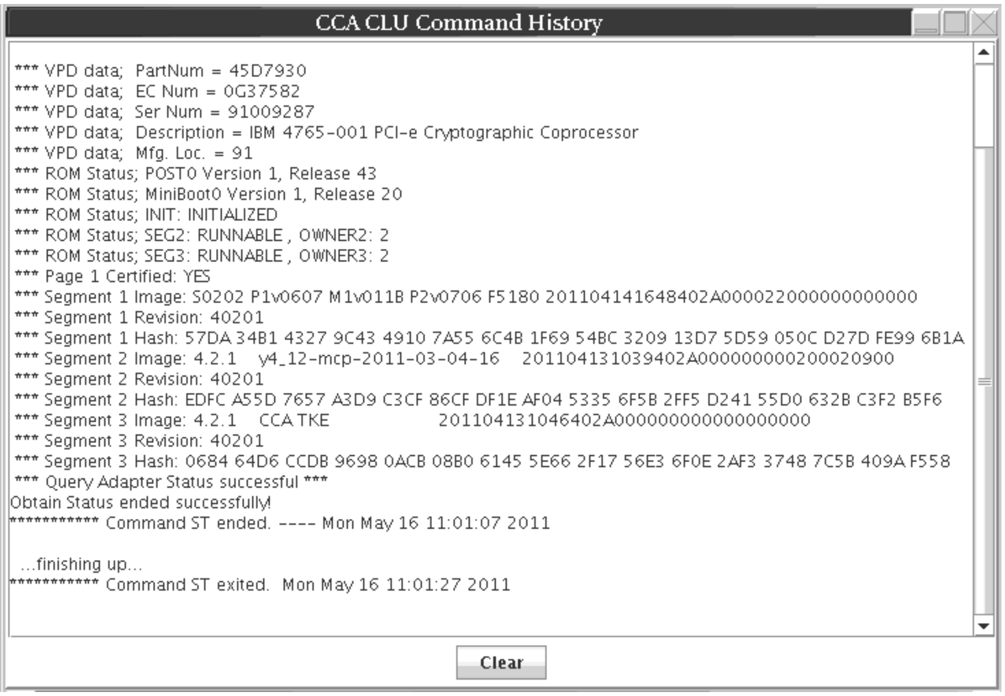
Figure 346. CLU View Menu



```
*********** Command ST started. ---- Mon May 16 11:00:26 2011

 *** VPD data;  PartNum = 45D7930
 *** VPD data;  EC Num = 0G37582
 *** VPD data;  Ser Num = 91009287
 *** VPD data;  Description = IBM 4765-001 PCI-e Cryptographic Coprocessor
 *** VPD data;  Mfg. Loc. = 91
 *** ROM Status; POST0 Version 1, Release 43
 *** ROM Status; MiniBoot0 Version 1, Release 20
 *** ROM Status; INIT: INITIALIZED
 *** ROM Status; SEG2: RUNNABLE , OWNER2: 2
 *** ROM Status; SEG3: RUNNABLE , OWNER3: 2
 *** Page 1 Certified: YES
 *** Segment 1 Image: S0202 P1v0607 M1v011B P2v0706 F5180 201104141648402A00002200000000000
 *** Segment 1 Revision: 40201
 *** Segment 1 Hash: 57DA 34B1 4327 9C43 4910 7A55 6C4B 1F69 54BC 3209 13D7 5D59 050C D27D FE99 6B1A
 *** Segment 2 Image: 4.2.1    y4_12-mcp-2011-03-04-16    201104131039402A000000000200020900
 *** Segment 2 Revision: 40201
 *** Segment 2 Hash: EDFC A55D 7657 A3D9 C3CF 86CF DF1E AF04 5335 6F5B 2FF5 D241 55D0 632B C3F2 B5F6
 *** Segment 3 Image: 4.2.1    CCA TKE                  201104131046402A0000000000000000000
 *** Segment 3 Revision: 40201
 *** Segment 3 Hash: 0684 64D6 CCDB 9698 0ACB 08B0 6145 5E66 2F17 56E3 6F0E 2AF3 3748 7C5B 409A F558
 *** Query Adapter Status successful ***
Obtain Status ended successfully!
*********** Command ST ended. ---- Mon May 16 11:01:07 2011

*********** Command ST exited. ---- Mon May 16 11:01:27 2011
```

Figure 347. Output Log file

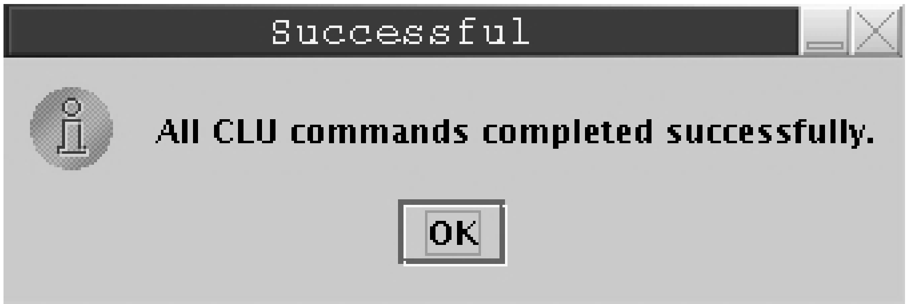
The CLU output log file is available to the user in the CNM Data Directory.



```
*** VPD data;  PartNum = 45D7930
*** VPD data;  EC Num = 0G37582
*** VPD data;  Ser Num = 91009287
*** VPD data;  Description = IBM 4765-001 PCI-e Cryptographic Coprocessor
*** VPD data;  Mfg. Loc. = 91
*** ROM Status; POST0 Version 1, Release 43
*** ROM Status; MiniBoot0 Version 1, Release 20
*** ROM Status; INIT: INITIALIZED
*** ROM Status; SEG2: RUNNABLE , OWNER2: 2
*** ROM Status; SEG3: RUNNABLE , OWNER3: 2
*** Page 1 Certified: YES
*** Segment 1 Image: S0202 P1v0607 M1v011B P2v0706 F5180 201104141648402A00002200000000000
*** Segment 1 Revision: 40201
*** Segment 1 Hash: 57DA 34B1 4327 9C43 4910 7A55 6C4B 1F69 54BC 3209 13D7 5D59 050C D27D FE99 6B1A
*** Segment 2 Image: 4.2.1    y4_12-mcp-2011-03-04-16    201104131039402A00000000200020900
*** Segment 2 Revision: 40201
*** Segment 2 Hash: EDFC A55D 7657 A3D9 C3CF 86CF DF1E AF04 5335 6F5B 2FF5 D241 55D0 632B C3F2 B5F6
*** Segment 3 Image: 4.2.1    CCA TKE                 201104131046402A00000000000000000
*** Segment 3 Revision: 40201
*** Segment 3 Hash: 0684 64D6 CCDB 9698 0ACB 08B0 6145 5E66 2F17 56E3 6F0E 2AF3 3748 7C5B 409A F558
 *** Query Adapter Status successful ***
Obtain Status ended successfully!
************ Command ST ended. ---- Mon May 16 11:01:07 2011

  ...finishing up...
************ Command ST exited.  Mon May 16 11:01:27 2011
```

Figure 348. CLU Command History

If all CLU commands complete without error, a message indicating that all CLU commands completed successfully will be displayed.



All CLU commands completed successfully.

Figure 349. 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 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.

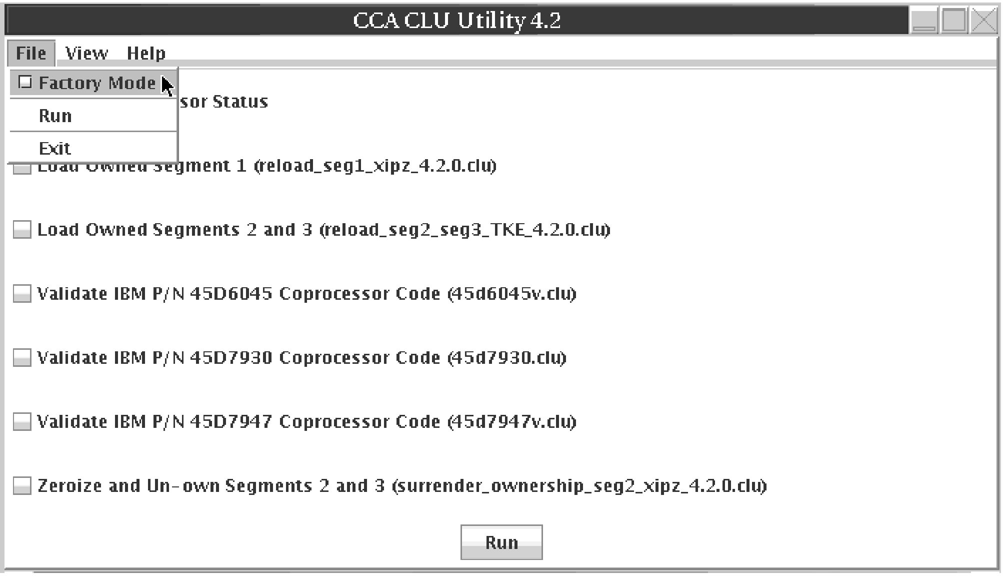

CCA CLU Utility 4.2
File View Help
□ Factory Mode
Run
Exit
sor Status
□ Load Owned Segment 1 (reload_seg1_xipz_4.2.0.clu)
□ Load Owned Segments 2 and 3 (reload_seg2_seg3_TKE_4.2.0.clu)
□ Validate IBM P/N 45D6045 Coprocessor Code (45d6045v.clu)
□ Validate IBM P/N 45D7930 Coprocessor Code (45d7930.clu)
□ Validate IBM P/N 45D7947 Coprocessor Code (45d7947v.clu)
□ Zeroize and Un-own Segments 2 and 3 (surrender_ownership_seg2_xipz_4.2.0.clu)
Run

Figure 350. CLU File Menu

Reload segment 1 with the CCA segment 1 file by selecting the Load Factory Segment 1 check box and pressing **Run**.

b. If the segment 1 image name does not indicate ... Factory ..., and the segment 1 revision level is less than 40200, reload segment 1 with the CCA segment 1.

Note: This choice is only available when the application is not in Factory Mode (File -> Factory Mode).

2. Change segments 2 and 3:
   a. If segment 2 ROM status indicates Unowned... Set the application to Factory Mode (File->Factory Mode). Select the 'Load IBM Factory Segments 2 and 3 (establish_ownership_then_emergency_reload_seg2_seg3_TKE_4.2.0.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_4.2.0.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: P1v0607 M1v011B
Segment 2 Image: 4.2.1 y4_12-mcp-2011-03-04-16
Segment 3 Image: 4.2.1 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**.

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" 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 D. Clear RSA Key Format

An RSA key can be imported from a file holding the unencrypted RSA key. The file must be an ASCII text file. CR/LF can be inserted at any place for enhanced readabilitly of the file.

The contents of the file are:

Description	Length (characters)
Key modulus length in bits (hex value)	4
Length of Modulus field in bytes (hex value)	4
Length of Public exponent field in bytes (hex value)	4
Length of Private exponent field in bytes (hex value)	4
Modulus (hex value)	-
Public exponent (hex value)	-
Private exponent (hex value)	-

The format follows the key_value_structure format defined for the PKA Key token Build (CSNDPKB) callable service.

These are examples of two file contents for the same clear RSA key. The key length is 512 bits and the public exponent is 65537.

Example 1:

```
0200
0080
0003
0080
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
80000000000000001AE28DA4606D885EB7E0340D6BAAC51991C0CD0EAE835AF
D9CFF3CD7E7EA74141DADD24A6331BEDF41A6626522CCF15767D167D01A16F97
010001
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0252BDAD4252BDAD425A8C6045D41AFAF746BEBD5F085D574FCD9C07F0B38C2C
45017C2A1AB919ED2551350A76606BFA6AF2F1609A00A0A48DD719A55E9CA801
```

Example 2:

```
0200004000030040
80000000000000001AE28DA4606D885EB7E0340D6BAAC51991C0CD0EAE835AF
D9CFF3CD7E7EA74141DADD24A6331BEDF41A6626522CCF15767D167D01A16F97
010001
0252BDAD4252BDAD425A8C6045D41AFAF746BEBD5F085D574FCD9C07F0B38C2C
45017C2A1AB919ED2551350A76606BFA6AF2F1609A00A0A48DD719A55EDCA801
```

Appendix E. Trusted Key Entry Applications and Utilities

The TKE console supports a variety of tasks, applications, and utilities.

The set of tasks, applications, and utilities available depends on the console user name specified when the console is initially started. The default console user name is TKEUSER. Other console user names are AUDITOR, ADMIN, and SERVICE. See "Trusted Key Entry Console" on page 8 for more information.

Table 32. Tasks, applications and utilities accessible by console user name

Navigation	Task	TKEUSER	ADMIN	AUDITOR	SERVICE
Trusted Key Entry					
	Begin Zone Remote Enroll Process for an IBM Crypto Adapter	X	X		
	CCA CLU		X		
	Complete Zone Remote Enroll Process for an IBM Crypto Adapter	X	X		
	Cryptographic Node Management Batch Initialization		X		
	Cryptographic Node Management Utility	X	X		
	Smart Card Utility Program	X	X		
	TKE's IBM Crypto Adapter Initialization		X		
	Trusted Key Entry	X	X		
	Edit TKE Files	X	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	
	Migrate Roles Utility		X		X
Service Management					
	Lock Console	X	X	X	X
	Shutdown or Restart	X	X	X	X
	Hardware Messages	X	X	X	X
	Network Diagnostic Information	X	X	X	X
	Users and Tasks	X	X	X	X
	View Console Information	X	X	X	X
	View Console Service History				X
	View Licenses	X	X	X	X
	Format Media	X	X	X	X
	Backup Critical Console Data		X		X

Table 32. Tasks, applications and utilities accessible by console user name (continued)

Navigation	Task	TKEUSER	ADMIN	AUDITOR	SERVICE
	Offload Virtual RETAIN Data to Removable Media				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
	Audit and Log Management	X	X	X	
	View Security Logs			X	
	Archive Security Logs			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 327
- “CCA CLU” on page 327
- “Complete Zone Remote Enroll Process” on page 327
- “Cryptographic Node Management Batch Initialization” on page 327
- “Cryptographic Node Management Utility” on page 327
- “Edit TKE Files” on page 327
- “Smart Card Utility Program” on page 331
- “TKE Audit Configuration Utility” on page 331
- “TKE Audit Record Upload Configuration Utility” on page 331
- “TKE File Management Utility” on page 332
- “TKE Media Manager” on page 334
- “TKE Workstation Code Information” on page 336
- “Migrate IBM Host Crypto Module Public Configuration Data” on page 336
- “Configuration Migration Tasks” on page 338
- “Migrate Roles Utility” on page 342
- Trusted Key Entry 7.1
- 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 299.

CCA CLU

This task is for loading code onto the TKE Workstation Crypto Adapter.

See “CCA CLU” on page 316.

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 299

Cryptographic Node Management Batch Initialization

This task is for using a batch interface to execute a user-created CNI file. A user-created CNI file can be used to initialize a TKE crypto adapter differently than the TKE IBM Crypto Adapter Initialization task. To create the user CNI, use the Cryptographic Node Management Utility, CNI Editor function.

See “Cryptographic Node Management Batch Initialization” on page 315

Cryptographic Node Management Utility

This task is for managing the TKE workstation crypto adapter (create and manage Roles and Profiles, manage workstation master keys, et cetera).

See Chapter 10, “Cryptographic Node Management Utility (CNM),” on page 241.

Edit TKE Files

The Edit TKE Files task provides a way to edit/browse files, 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

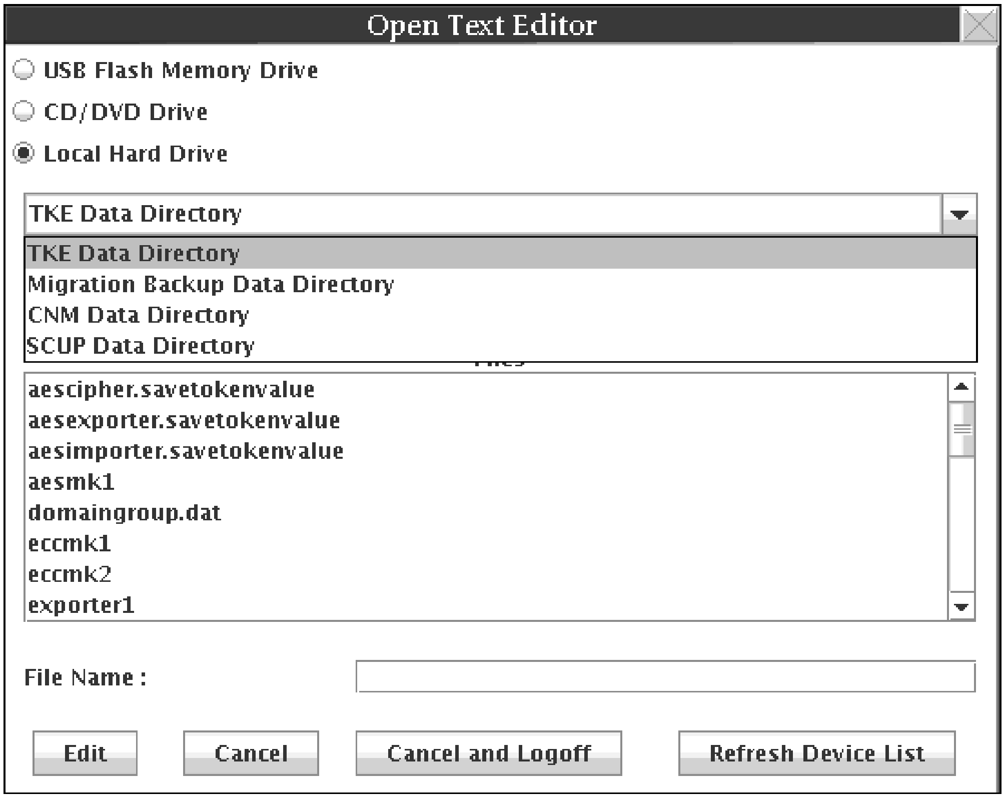
Files in the Configuration Data Directory cannot be accessed by the Edit TKE Files task and should be reviewed using the review functions in the configuration migration applications.

To open the Edit TKE Files task, click 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 log on to the adapter. If you are already logged onto the adapter, no logon window will be displayed (the current logon will be used).

In the Open Text Editor window, select a file from the displayed list or manually enter a file name. If you manually enter a file name that does not exist, a new file by that name will be created in the location specified.

Note: Files on a CD or floppy can only be browsed. Writing to a CD or floppy is not supported.



Open Text Editor

○ USB Flash Memory Drive

○ CD/DVD Drive

● Local Hard Drive

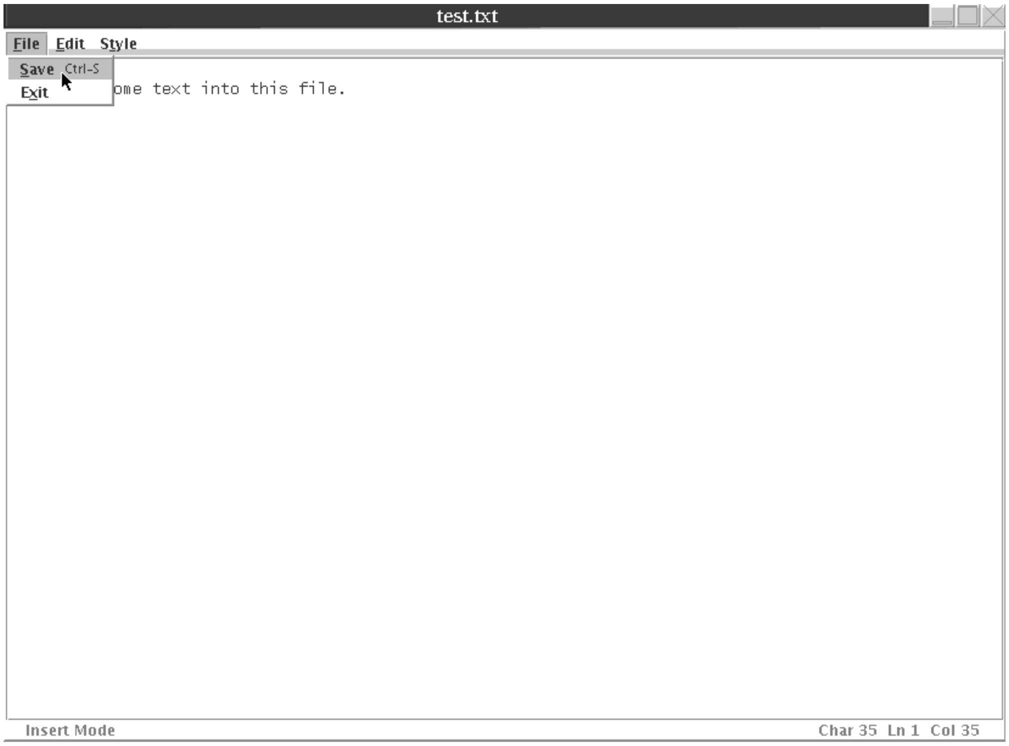
TKE Data Directory

aescipher.savetokenvalue
aesexporter.savetokenvalue
aesimporter.savetokenvalue
aesmk1
domaingroup.dat
eccmk1
eccmk2
exporter1

File Name :

Figure 351. 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.



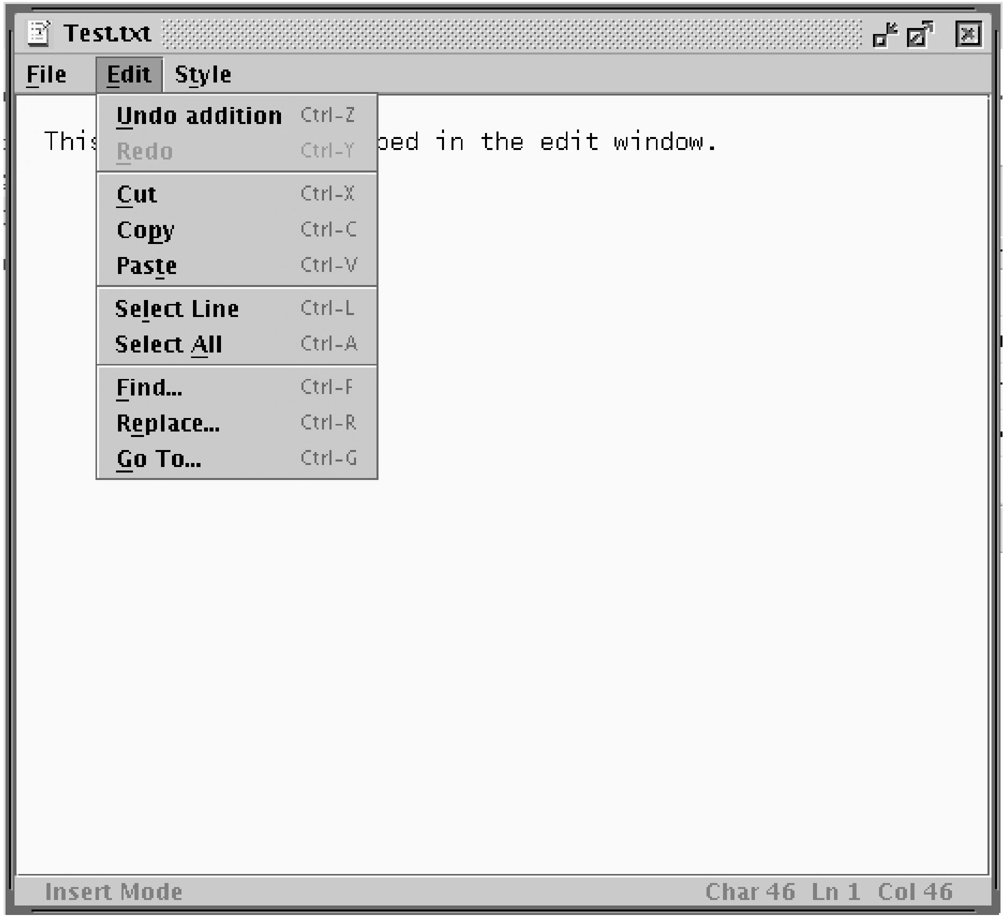
ome text into this file.

Figure 352. 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 334.
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.

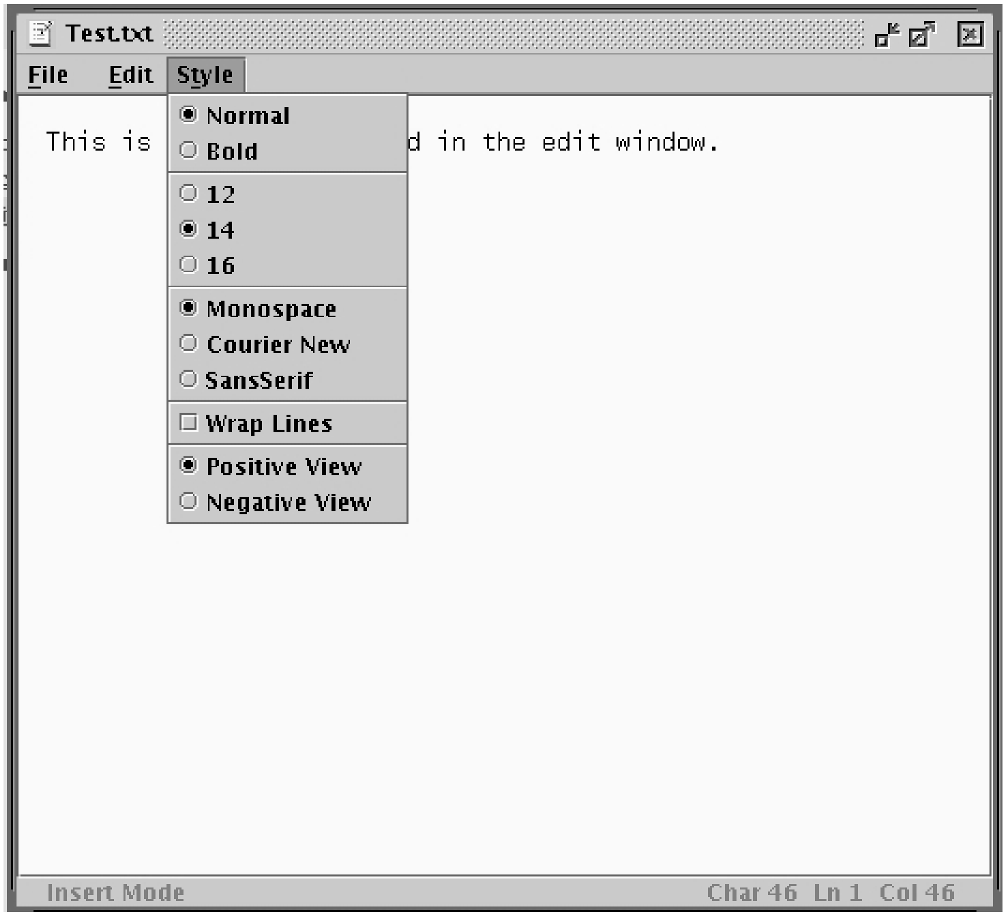


This ped in the edit window.

Insert Mode Char 46 Ln 1 Col 46

Figure 353. Editor - Edit menu items

In addition, there are options for Fonts, line wrap, and background.



```
This is                 d in the edit window.
```

Insert Mode Char 46 Ln 1 Col 46

Figure 354. Editor - Style Menu Items

Smart Card Utility Program

This task is used for initializing smart cards, enrolling smart cards in a zone, and enrolling TKE workstations in a zone.

See Chapter 11, “Smart Card Utility Program (SCUP),” on page 285.

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 205 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 214 for more information

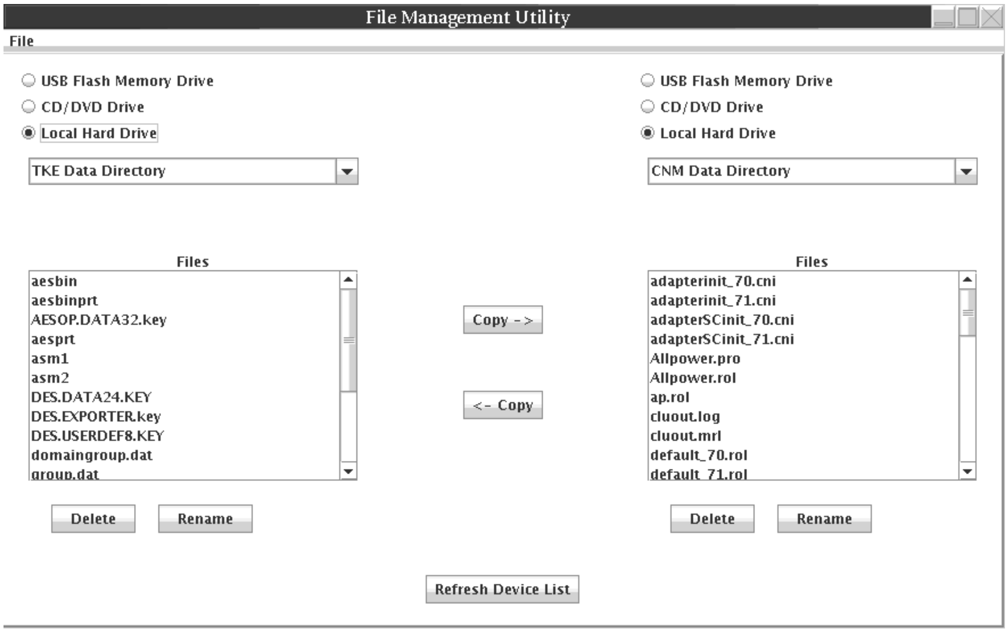
TKE File Management Utility

The TKE File Management Utility task allows you to manage files on 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.



○ USB Flash Memory Drive
○ CD/DVD Drive
● Local Hard Drive

TKE Data Directory

Files

aesbin
aesbinprt
AESOP.DATA32.key
aesprt
asm1
asm2
DES.DATA24.KEY
DES.EXPORTER.key
DES.USERDEF8.KEY
domaingroup.dat
group.dat

○ USB Flash Memory Drive
○ CD/DVD Drive
● Local Hard Drive

CNM Data Directory

Files

adapterinit_70.cni
adapterinit_71.cni
adapterSCinit_70.cni
adapterSCinit_71.cni
Allpower.pro
Allpower.rol
ap.rol
cluout.log
cluout.mrl
default_70.rol
default_71.rol

Figure 355. 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

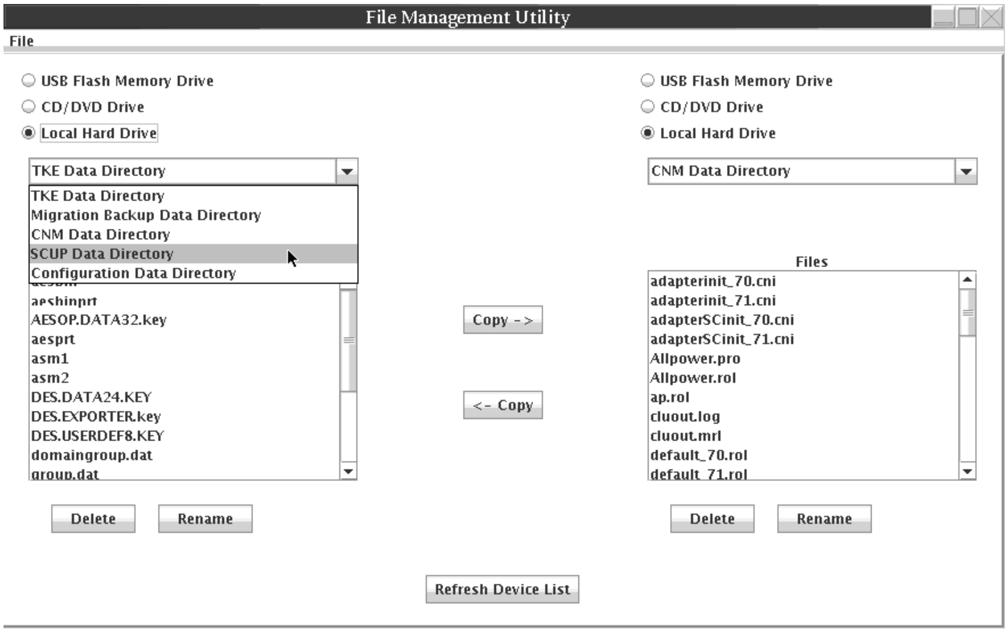
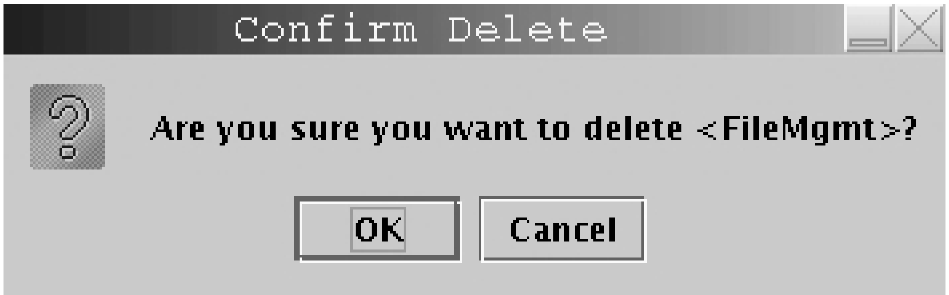


Figure 356. TKE File Management - Directory options

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'.

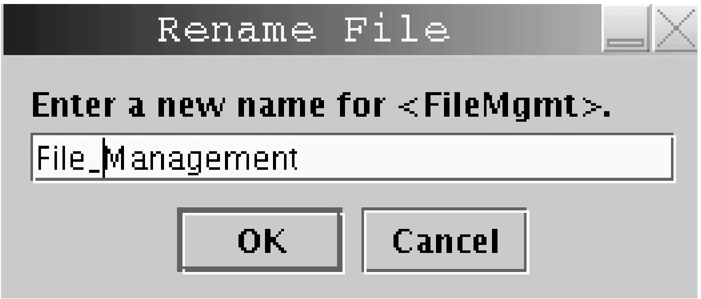
Clicking on **Delete** will display a confirmation window.



Are you sure you want to delete <FileMgmt>?

Figure 357. Delete Confirmation Window

Clicking on **Rename** will present a window for inputting a filename.


Rename File

Enter a new name for <FileMgmt>.

File_Management

Figure 358. Window for Inputting a Filename

Warnings:

1. If updates are done to the 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

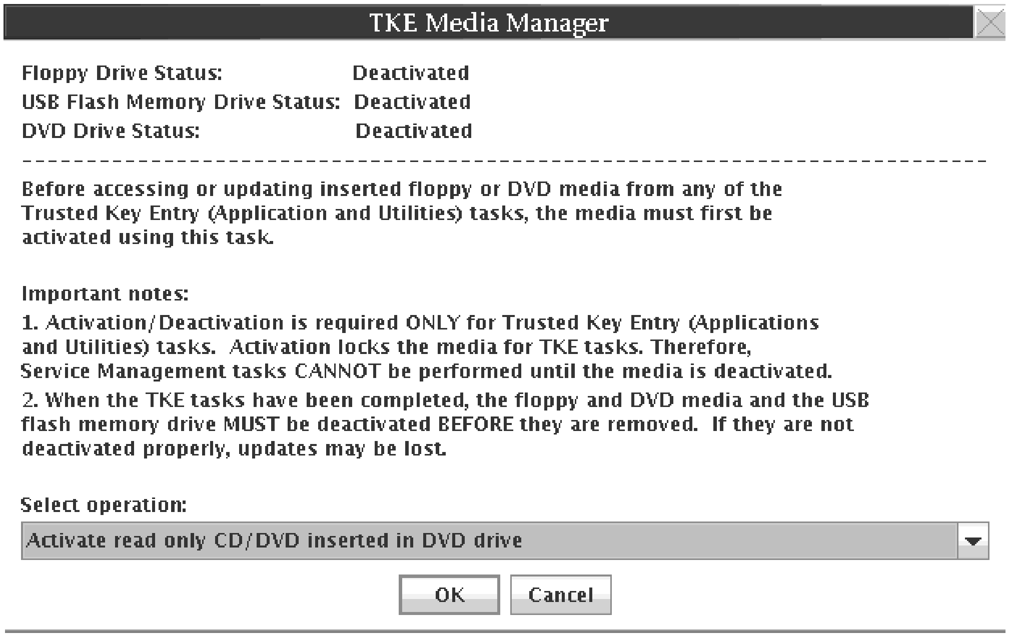
| The TKE Version 7.1 workstation allows the use of these media devices:

- Floppy Disk (read-only)
- Compact Disc (read-only)
- DVD-RAM Disc
- USB flash memory drive

| TKE 7.1 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.



TKE Media Manager

Floppy Drive Status: Deactivated
USB Flash Memory Drive Status: Deactivated
DVD Drive Status: Deactivated

Before accessing or updating inserted floppy or DVD media from any of the Trusted Key Entry (Application and Utilities) tasks, the media must first be activated using this task.

Important notes:
1. Activation/Deactivation is 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 floppy and DVD media and the USB flash memory drive MUST be deactivated BEFORE they are removed. If they are not deactivated properly, updates may be lost.

Select operation:
Activate read only CD/DVD inserted in DVD drive

Figure 359. 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)

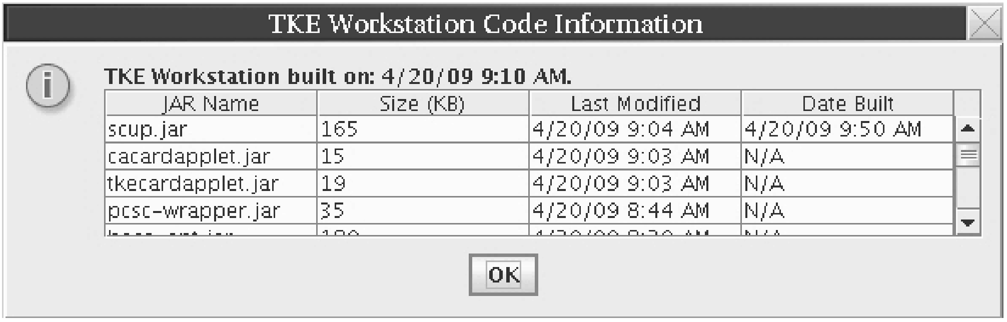
   Otherwise, Trusted Key Entry (Applications and Utilities) tasks will not recognize the drive and you will not be able to use it. Service Management Tasks behave differently and require different labels.
7. Do not remove a USB flash memory drive from the USB port before you complete the operation that 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**.



TKE Workstation built on: 4/20/09 9:10 AM.

JAR Name	Size (KB)	Last Modified	Date Built
scup.jar	165	4/20/09 9:04 AM	4/20/09 9:50 AM
cacardapplet.jar	15	4/20/09 9:03 AM	N/A
tkecardapplet.jar	19	4/20/09 9:03 AM	N/A
pcsc-wrapper.jar	35	4/20/09 8:44 AM	N/A

Figure 360. 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. Otherwise, the migration will not be allowed. To ensure this, the utility checks that the CCA version on the target module is at a higher level than the source configuration. If it is not, migration will not be allowed.

In the apply task, existing roles, authorities, and domain control settings on target crypto modules are removed and replaced with the configuration data from the file. Domains optionally can be zeroized before applying configuration data. This clears the master key registers. Only control domains can be zeroized. See Appendix B, “LPAR Considerations,” on page 313 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 from the application that was holding it and reserves it for the crypto module notebook.
4. Close the crypto module notebook to release the host crypto module.

Configuration Migration Tasks

This application provides access to utilities used to securely migrate configuration data, including secret data such as master key values, from one crypto module to another. When you select this application, the Configuration Migration Tasks panel is displayed.

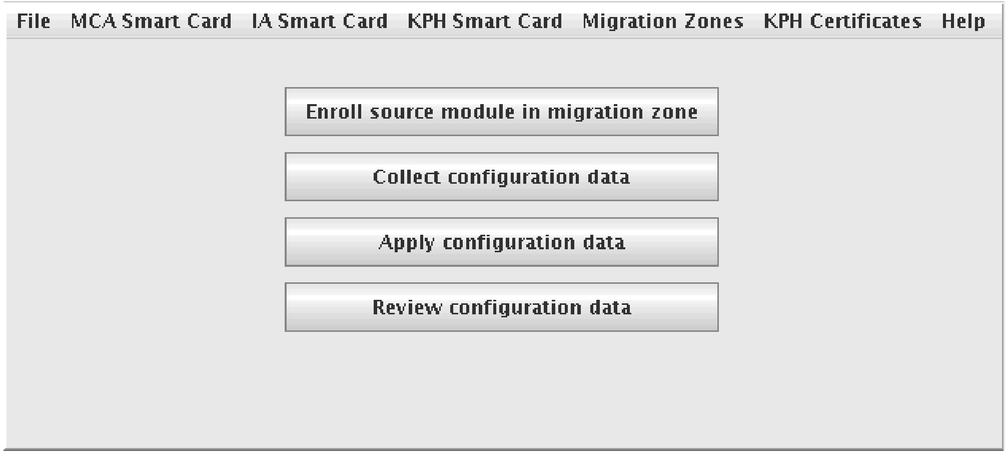


Figure 361. Configuration Migration Tasks panel

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-bit AES key (32 bytes), 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 342).

"M" KPH smart cards approve reconstructing the transport key, with help from the OA proxy (see “OA proxy” on page 342). 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.

Migrate Roles Utility

This utility, introduced in TKE 7.1, simplifies the process of adding new ACPs to existing roles on your TKE's local crypto adapter. This is useful during migration, because new ACPs are not automatically added to existing roles during the migration process.

See “Adding new ACPs to existing roles using the Migrate Roles Utility” on page 95 for more information.

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 343
- “Authorize Internal Code Changes” on page 343
- “Change Console Internal Code” on page 345
- “Offload Virtual RETAIN Data to Removable Media” on page 357
- “Transmit Console Service Data” on page 360
- “View Console Service History” on page 367
- “Rebuild Vital Product Data” on page 356

The following tasks are displayed if you are logged in as **Auditor**:

- “Archive Security Logs”
- “View Security Logs” on page 371

The following tasks are displayed for multiple user names:

- “Audit and Log Management” on page 354
- “Backup Critical Console Data” on page 344
- “Change Password” on page 345
- “Configure 3270 Emulators” on page 99
- “Customize Console Date/Time” on page 79
- “Customize Network Settings” on page 75
- “Customize Scheduled Operations” on page 346
- “Format Media” on page 351
- “Hardware Messages” on page 354
- “Lock console” on page 355
- “Manage Print Screen Files” on page 356
- “Network Diagnostic Information” on page 356
- “Save Upgrade Data” on page 358
- “Shutdown or Restart” on page 359
- “Users and Tasks” on page 363
- “View Console Events” on page 364
- “View Console Information” on page 365
- “View Console Tasks Performed” on page 369
- “View Licenses” on page 370

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 213 for more information.

Authorize Internal Code Changes

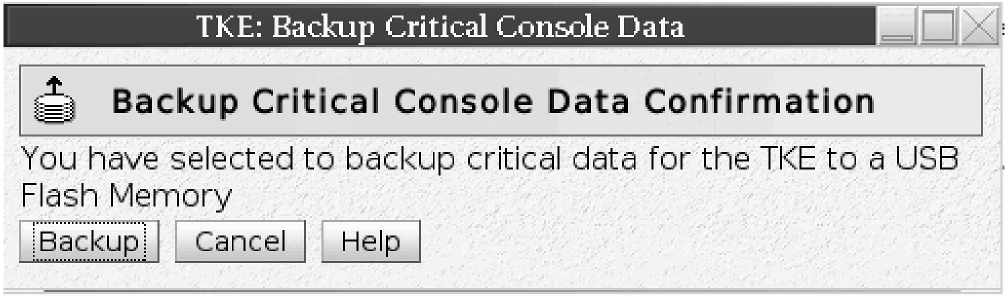
This task is used to verify or change the setting that allows using this TKE workstation to perform installation and activation of internal code changes and other subsequent operations. This task should only be invoked by your IBM Customer Engineer or when directed by IBM Product Engineering. You must 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.

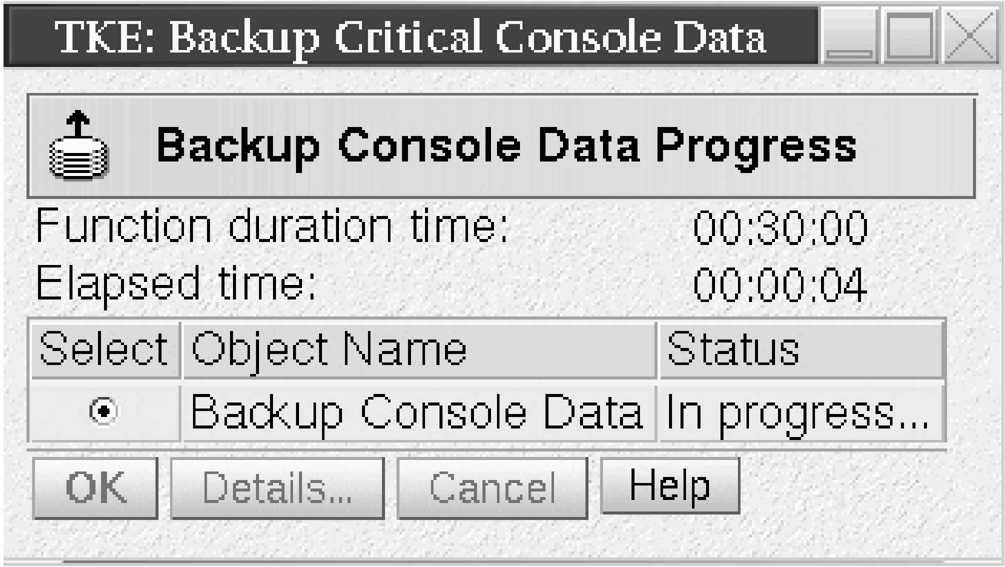
To invoke this task, log on as either ADMIN or SERVICE, click on Service Management and then click on Backup Critical Console Data.


TKE: Backup Critical Console Data
Backup Critical Console Data Confirmation

You have selected to backup critical data for the TKE to a USB Flash Memory

Figure 362. 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.


TKE: Backup Critical Console Data
Backup Console Data Progress

Function duration time: 00:30:00

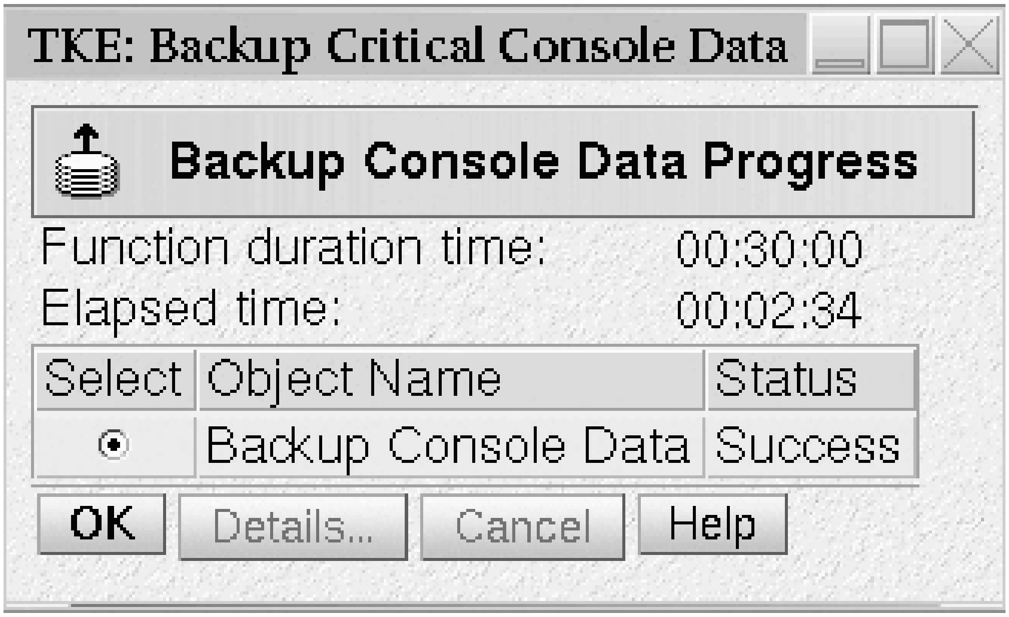
Elapsed time: 00:00:04

Select	Object Name	Status
●	Backup Console Data	In progress...

OK
Details...
Cancel
Help

Figure 363. 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.



TKE: Backup Critical Console Data

Backup Console Data Progress

Function duration time: 00:30:00

Elapsed time: 00:02:34

Select	Object Name	Status
⦿	Backup Console Data	Success

Figure 364. 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.

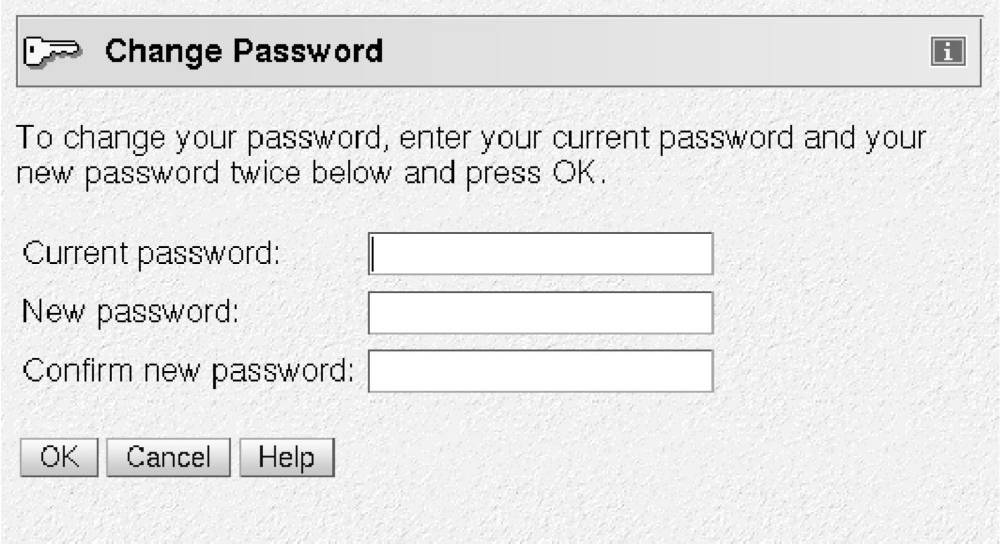
Change Password

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.



Change Password

To change your password, enter your current password and your new password twice below and press OK.

Current password:

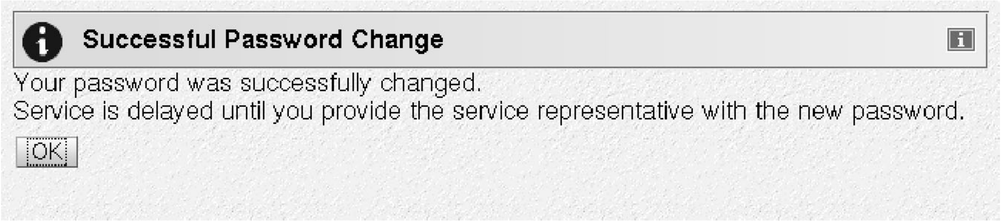
New password:

Confirm new password:

Figure 365. 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.



Successful Password Change

Your password was successfully changed.
Service is delayed until you provide the service representative with the new password.

Figure 366. 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.

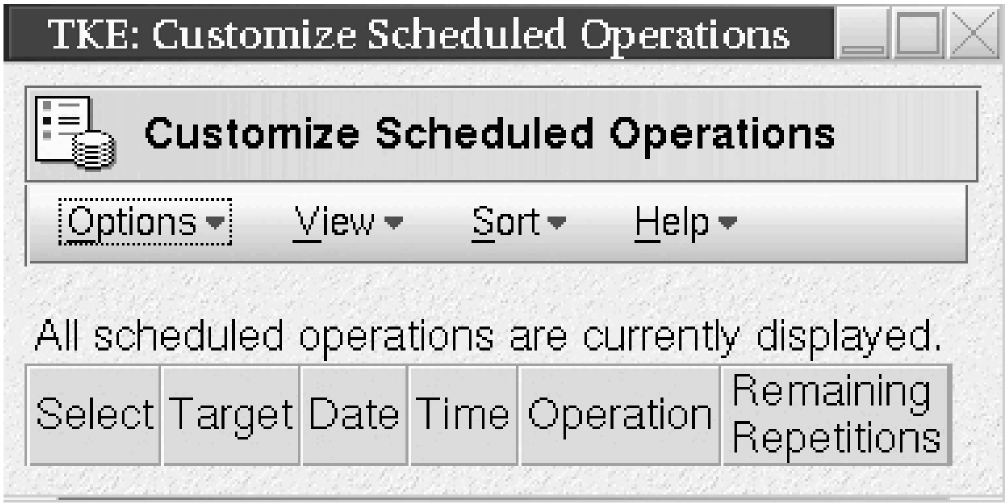
No other restrictions, such as password history rules or repeating characters, apply.

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 351 for details.


TKE: Customize Scheduled Operations

Customize Scheduled Operations

All scheduled operations are currently displayed.

Select	Target	Date	Time	Operation	Remaining Repetitions

Figure 367. 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.

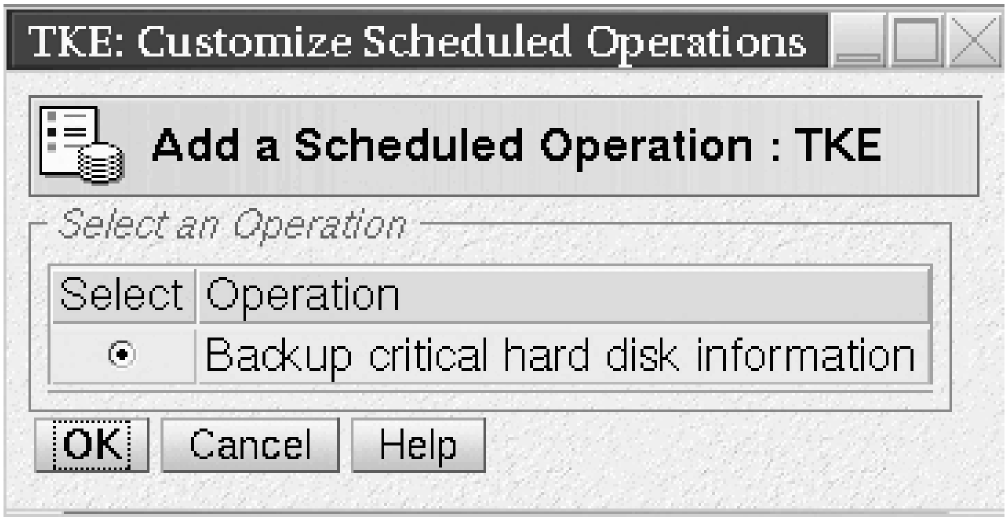
To open this task, click on Service Management and then click on Customize Scheduled Operations.

The Customize Scheduled Operations window displays.

Click Options on the menu bar to select:

`New`	to create a new scheduled operation
`Delete`	to remove a scheduled operation
`Refresh`	to update the current list of scheduled operations
`Select All`	to choose all scheduled operations currently displayed
`Deselect All`	to deselect all scheduled operations that were currently selected
`Exit`	to exit this task

When **New** is selected from the Options menu, the Add a Scheduled Operation screen is displayed.



TKE: Customize Scheduled Operations

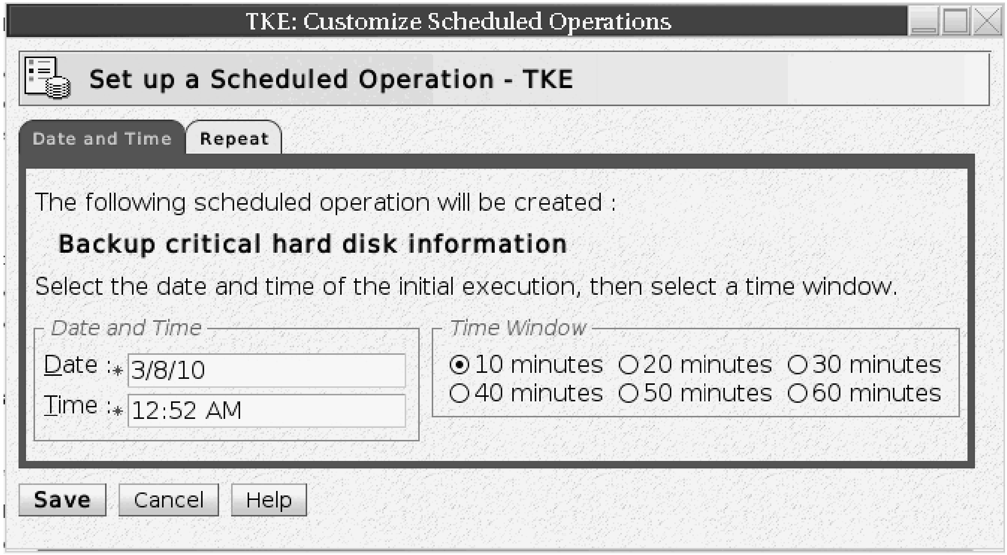
Add a Scheduled Operation : TKE

Select an Operation

Select	Operation
●	Backup critical hard disk information

Figure 368. 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.



TKE: Customize Scheduled Operations

Set up a Scheduled Operation - TKE

The following scheduled operation will be created :

Backup critical hard disk information

Select the date and time of the initial execution, then select a time window.

Date and Time

Date :* 3/8/10

Time :* 12:52 AM

Time Window

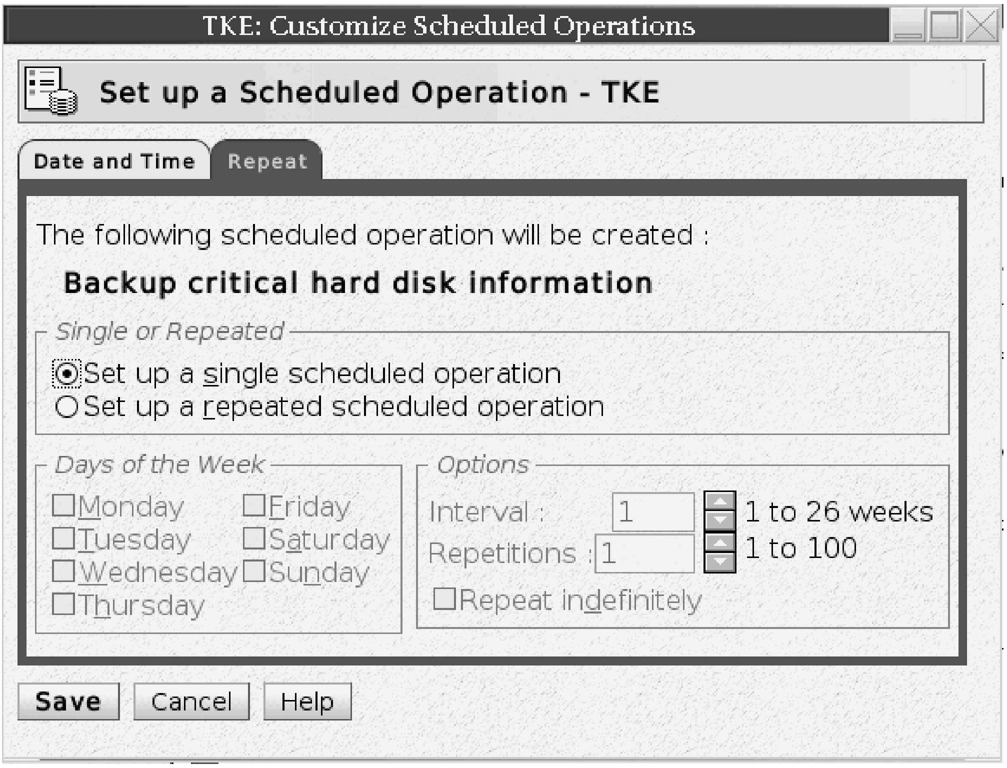
● 10 minutes ○ 20 minutes ○ 30 minutes
○ 40 minutes ○ 50 minutes ○ 60 minutes

Figure 369. 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

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

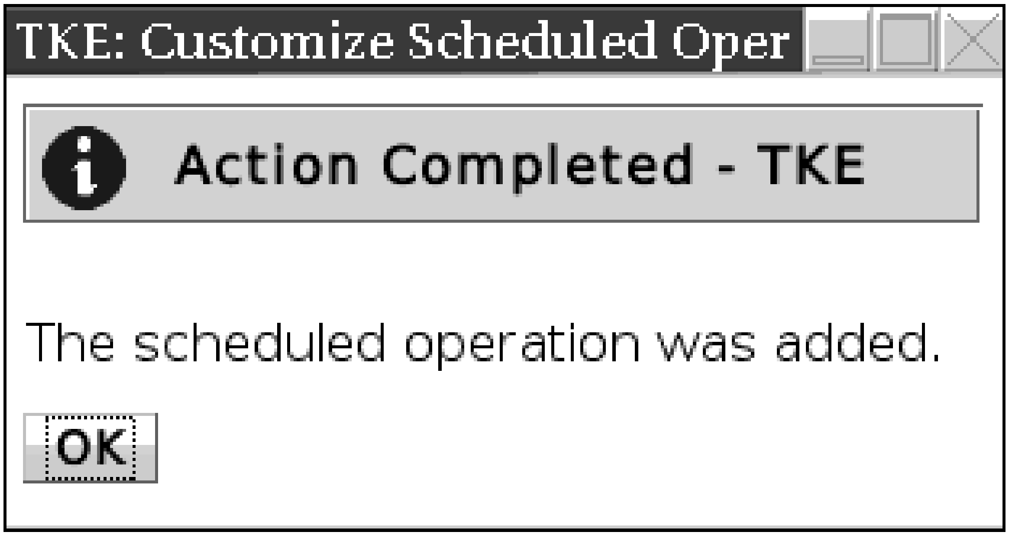
□ Monday □ Friday
□ Tuesday □ Saturday
□ Wednesday □ Sunday
□ Thursday

Options

Interval : 1 1 to 26 weeks
Repetitions : 1 1 to 100
□ Repeat indefinitely

Figure 370. Customize Scheduled Operations - Set Repetition of operation

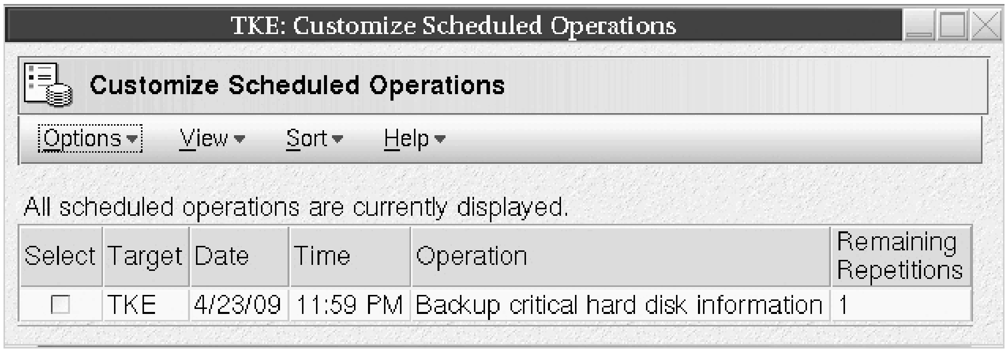
After all the information is selected, press **Save** to complete the scheduling of the operation.


TKE: Customize Scheduled Oper

Action Completed - TKE

The scheduled operation was added.

Figure 371. Completion Window for Adding Scheduled Operation


TKE: Customize Scheduled Operations
Customize Scheduled Operations
Options
View
Sort
Help

All scheduled operations are currently displayed.

Select	Target	Date	Time	Operation	Remaining Repetitions
□	TKE	4/23/09	11:59 PM	Backup critical hard disk information	1

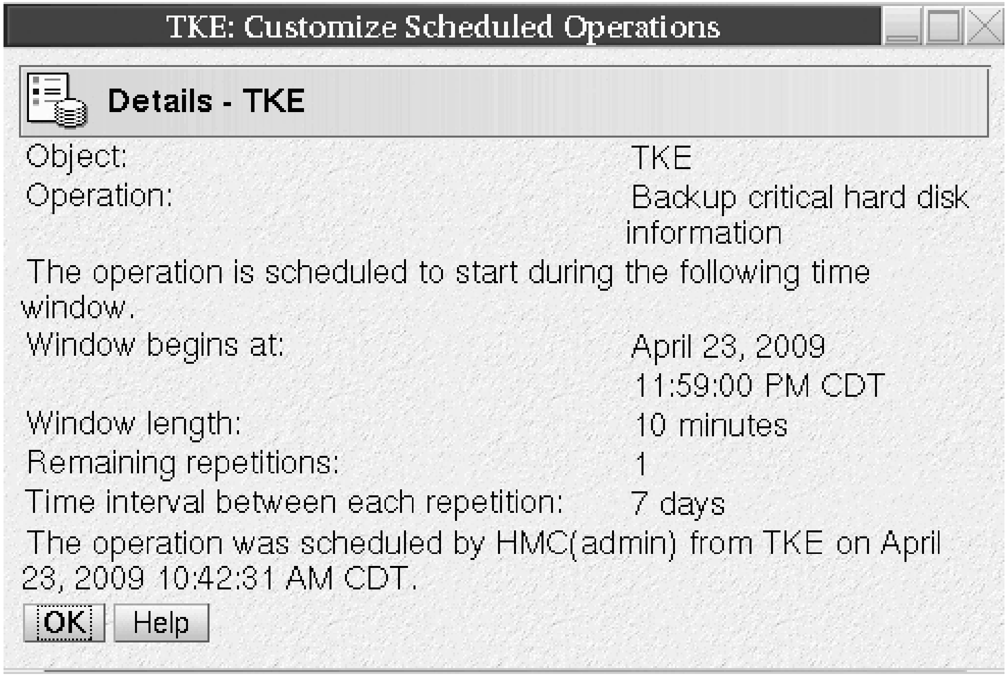
Figure 372. Customize Schedule Operations

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.



Object: TKE

Operation: Backup critical hard disk information

The operation is scheduled to start during the following time window.

Window begins at: April 23, 2009 11:59:00 PM CDT

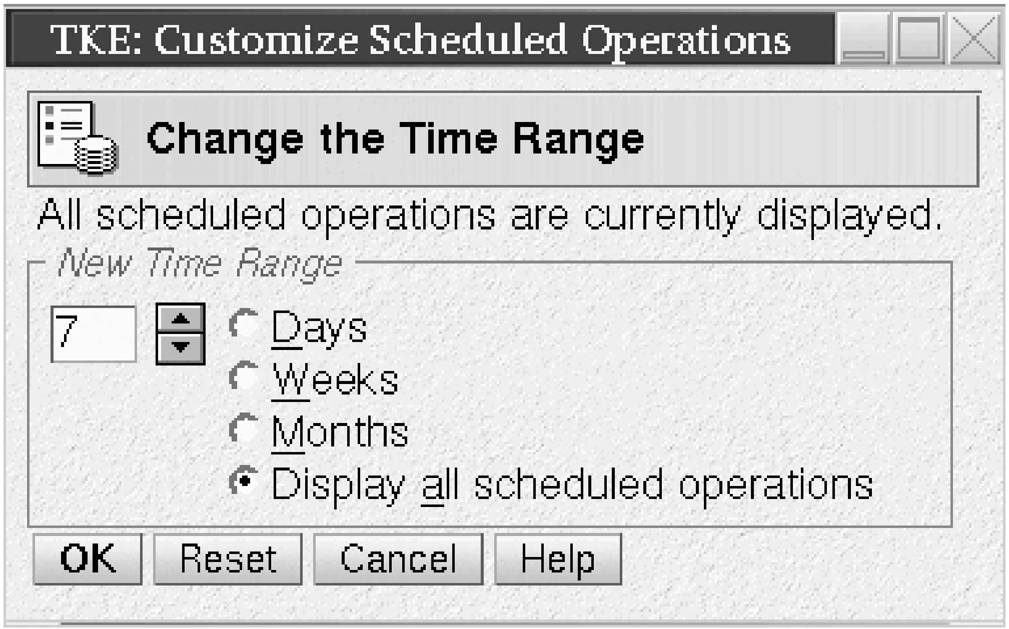
Window length: 10 minutes

Remaining repetitions: 1

Time interval between each repetition: 7 days

The operation was scheduled by HMC(admin) from TKE on April 23, 2009 10:42:31 AM CDT.

Figure 373. Details View of Scheduled Operation



TKE: Customize Scheduled Operations

Change the Time Range

All scheduled operations are currently displayed.

New Time Range

7

○ Days
○ Weeks
○ Months
● Display all scheduled operations

Figure 374. New Time Range window for Scheduled Operation

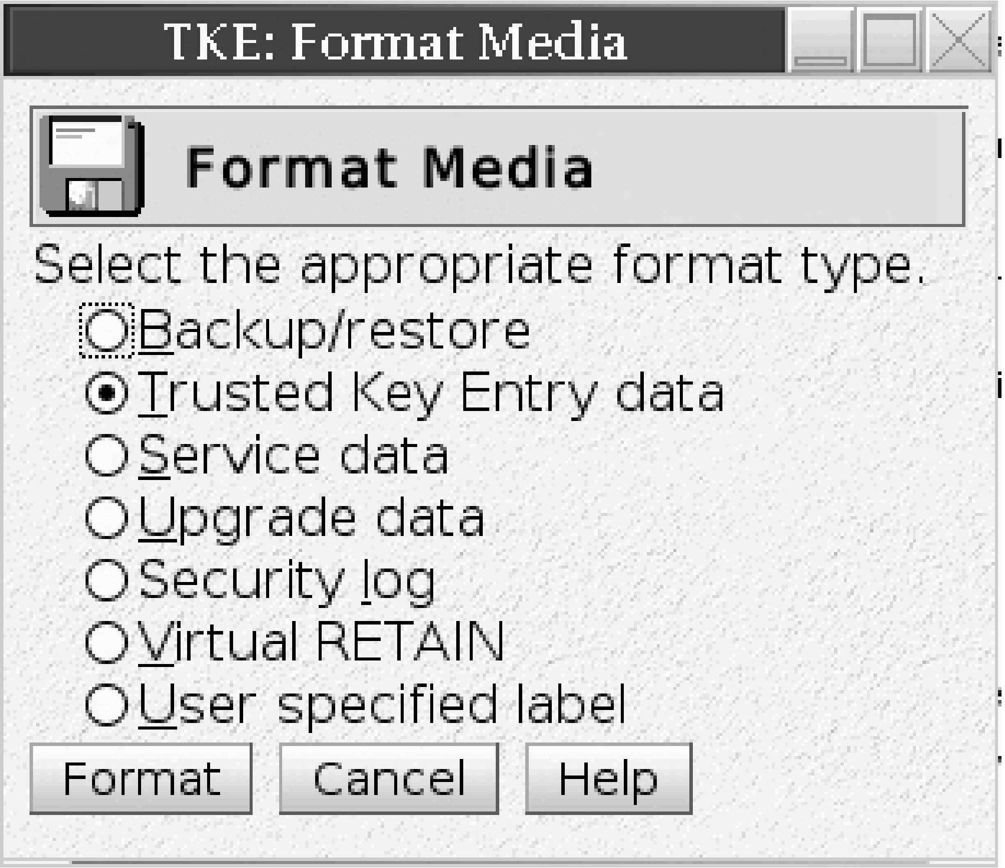
Format Media

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.



TKE: Format Media

Format Media

Select the appropriate format type.

○ Backup/restore
● Trusted Key Entry data
○ Service data
○ Upgrade data
○ Security log
○ Virtual RETAIN
○ User specified label

Figure 375. 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 33. Allowable labels when formatting DVD-RAM or USB flash memory drive

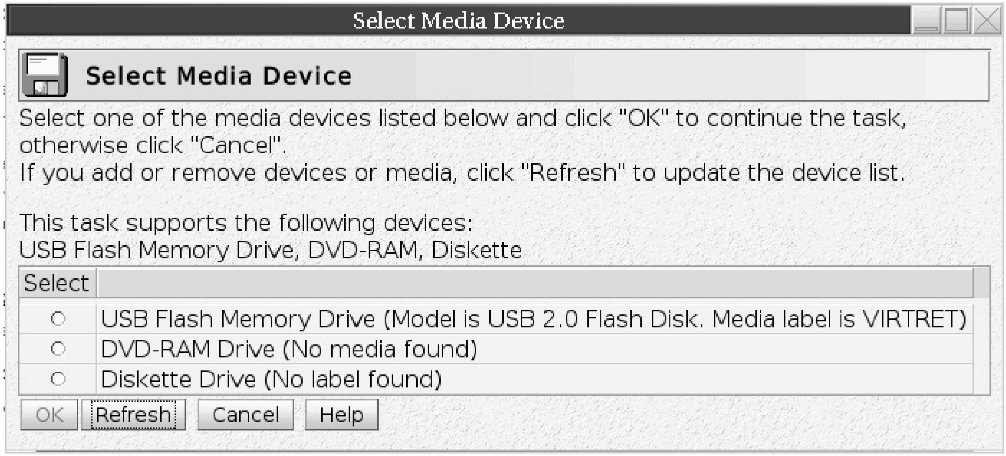
Format	Label	Description:
Backup/restore	ACTBKP	This formatted media is used in the Backup Critical Console Data task and the Customize Scheduled Operations task. To choose this format type, select Backup/restore.
Trusted Key Entry data	TKEDATA	This formatted media is used in the TKE applications and 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 33. 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.		

3. 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.



Select Media Device

Select one of the media devices listed below and click "OK" to continue the task, otherwise click "Cancel".
If you add or remove devices or media, click "Refresh" to update the device list.

This task supports the following devices:
USB Flash Memory Drive, DVD-RAM, Diskette

Select	
○	USB Flash Memory Drive (Model is USB 2.0 Flash Disk. Media label is VIRTRET)
○	DVD-RAM Drive (No media found)
○	Diskette Drive (No label found)

Figure 376. Select Media Device

4. 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.

5. 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.

Audit and Log Management

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 “Audit and Log Management” on page 210 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.

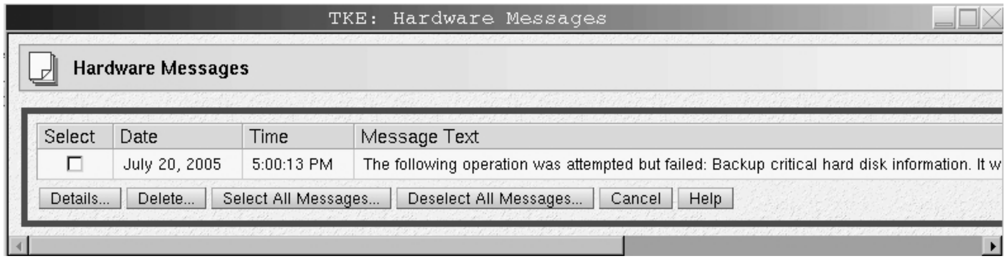
To invoke the Hardware Messages task, click on Service Management and then click on Hardware Messages.

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.



TKE: Hardware Messages

Hardware Messages

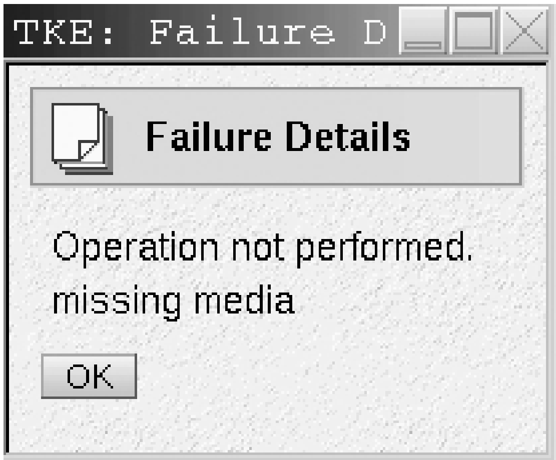
Select	Date	Time	Message Text
□	July 20, 2005	5:00:13 PM	The following operation was attempted but failed: Backup critical hard disk information. It w

Figure 377. 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.



Operation not performed.
missing media

Figure 378. 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.

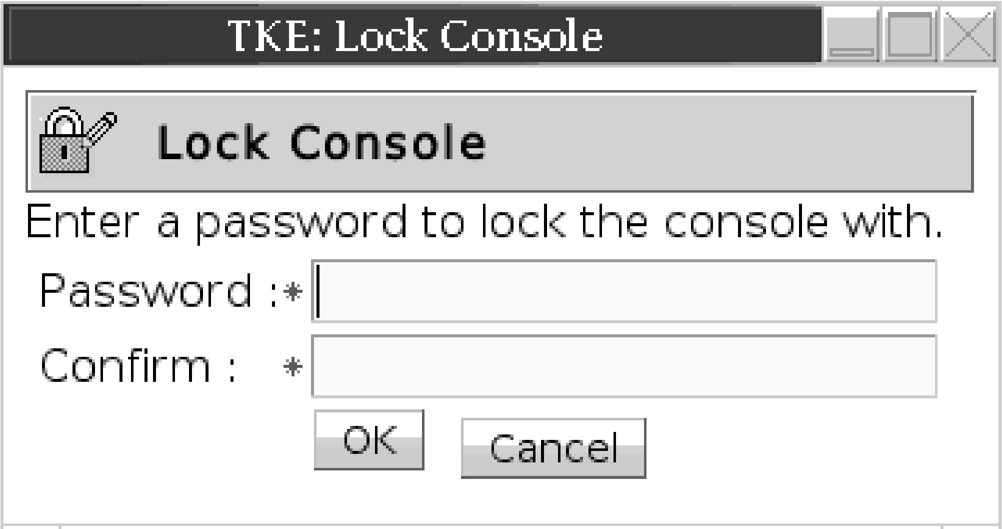
Deleting messages provides greater assurance that new messages will be displayed as they are received.

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.



TKE: Lock Console

Lock Console

Enter a password to lock the console with.

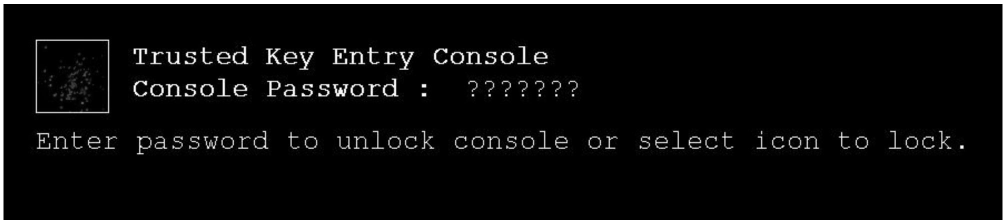
Password :*

Confirm : *

Figure 379. 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.



```
Trusted Key Entry Console
Console Password :  ???????

Enter password to unlock console or select icon to lock.
```

Figure 380. 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.

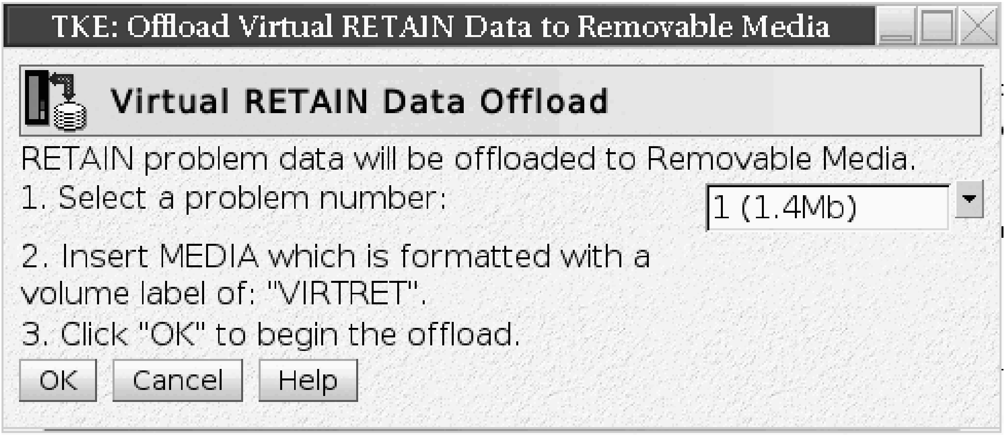
Offload Virtual RETAIN Data to Removable Media

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.



TKE: Offload Virtual RETAIN Data to Removable Media

Virtual RETAIN Data Offload

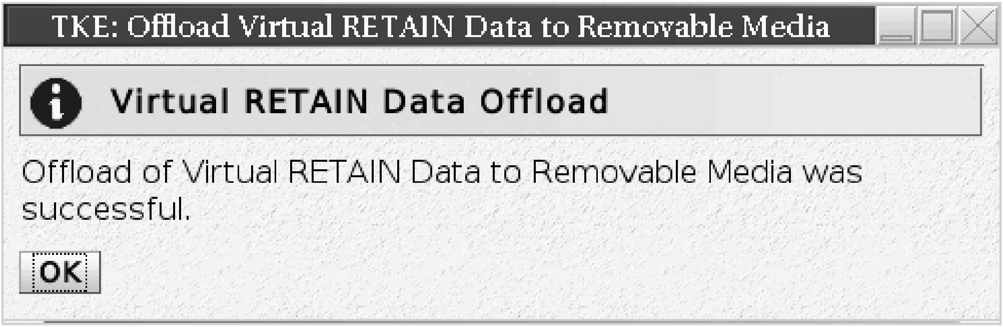
RETAIN problem data will be offloaded to Removable Media.

1. Select a problem number: 1 (1.4Mb)
2. Insert MEDIA which is formatted with a volume label of: "VIRTRET".
3. Click "OK" to begin the offload.

Figure 381. 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.



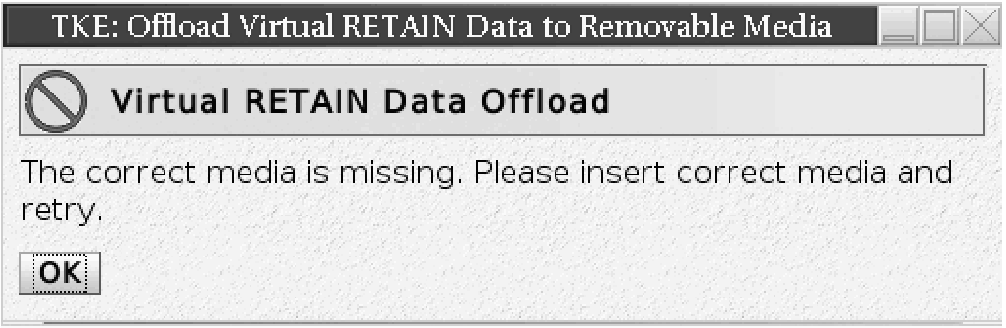
TKE: Offload Virtual RETAIN Data to Removable Media

Virtual RETAIN Data Offload

Offload of Virtual RETAIN Data to Removable Media was successful.

Figure 382. 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.



TKE: Offload Virtual RETAIN Data to Removable Media

Virtual RETAIN Data Offload

The correct media is missing. Please insert correct media and retry.

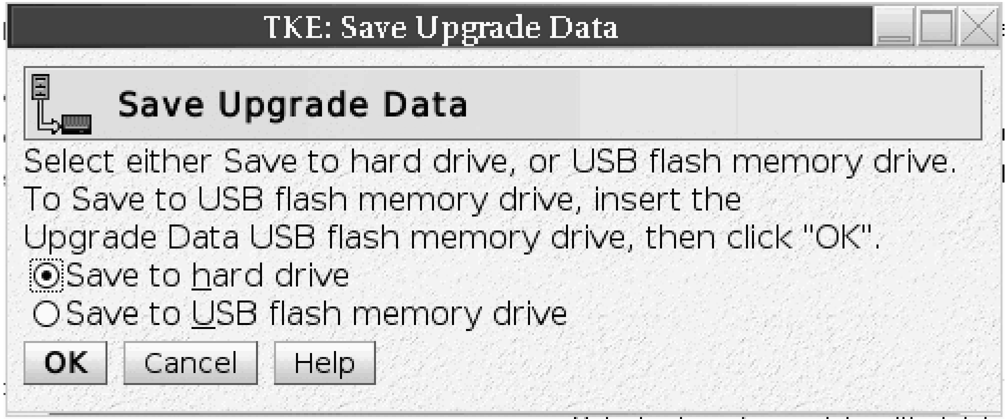
Figure 383. Virtual RETAIN Data Offload Incorrect Media Error

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.



TKE: Save Upgrade Data

Save Upgrade Data

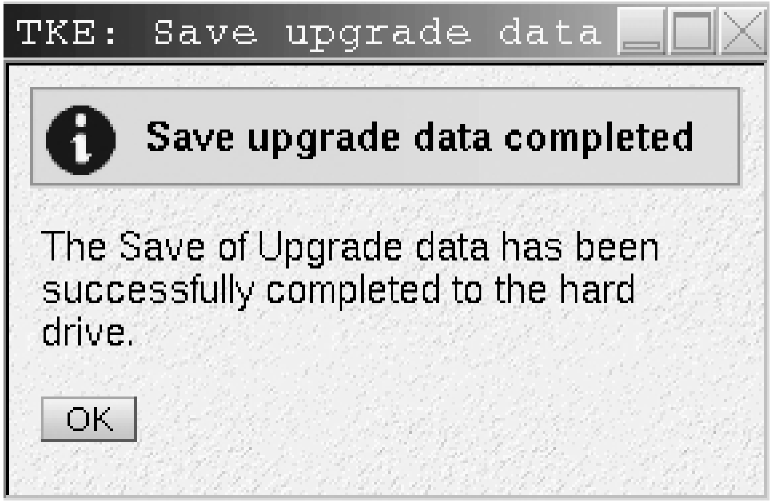
Select either Save to hard drive, or USB flash memory drive.
To Save to USB flash memory drive, insert the
Upgrade Data USB flash memory drive, then click "OK".

● Save to hard drive
○ Save to USB flash memory drive

Figure 384. 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.


TKE: Save upgrade data

Save upgrade data completed

The Save of Upgrade data has been successfully completed to the hard drive.

Figure 385. Save Upgrade Success Window

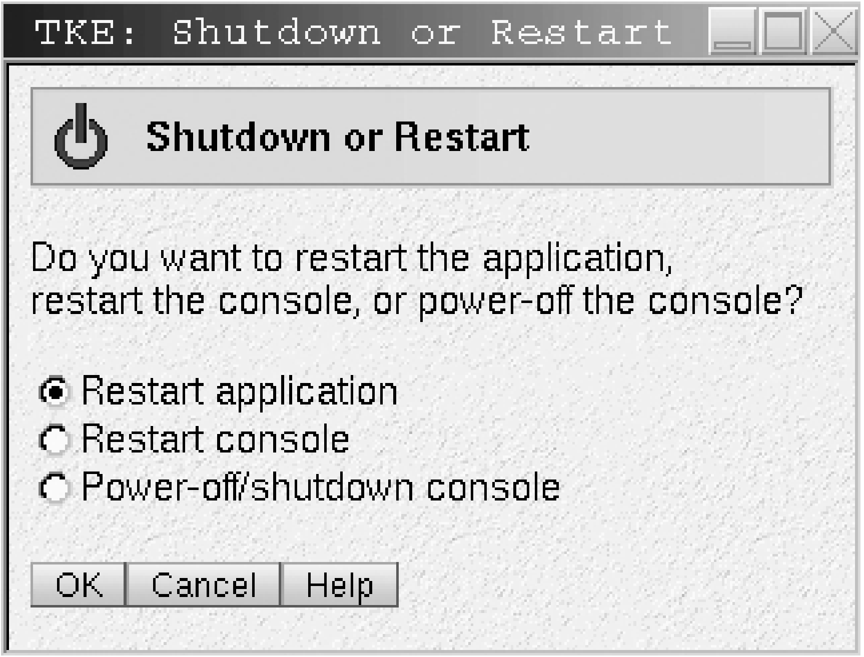
Note: While the Save to DVD-RAM option is available for Save Upgrade Data, it should not be used. The restore of Upgrade Data from a DVD-RAM is currently not supported.

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.


TKE: Shutdown or Restart

Shutdown or Restart

Do you want to restart the application, restart the console, or power-off the console?

● Restart application
○ Restart console
○ Power-off/shutdown console

Figure 386. Shutdown or Restart Task Window

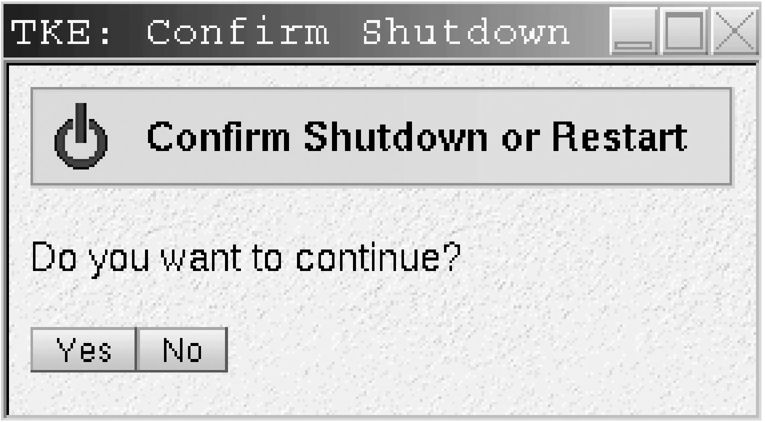
Select one of the following options from the dialog and press **OK**.

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.



TKE: Confirm Shutdown

Confirm Shutdown or Restart

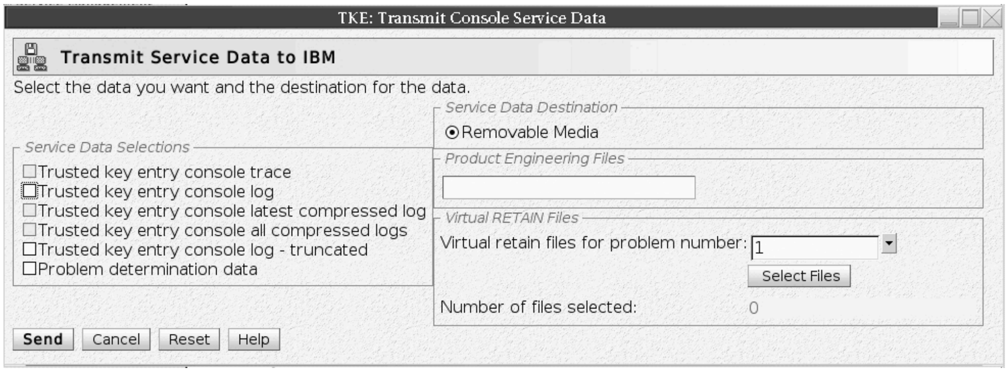
Do you want to continue?

Figure 387. 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.



TKE: Transmit Console Service Data

Transmit Service Data to IBM

Select the data you want and the destination for the data.

Service Data Selections
- □ Trusted key entry console trace
- □ Trusted key entry console log
- □ Trusted key entry console latest compressed log
- □ Trusted key entry console all compressed logs
- □ Trusted key entry console log - truncated
- □ Problem determination data

Service Data Destination
- ● Removable Media

Product Engineering Files

Virtual RETAIN Files

Virtual retain files for problem number: 1

Number of files selected: 0

Figure 388. 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:

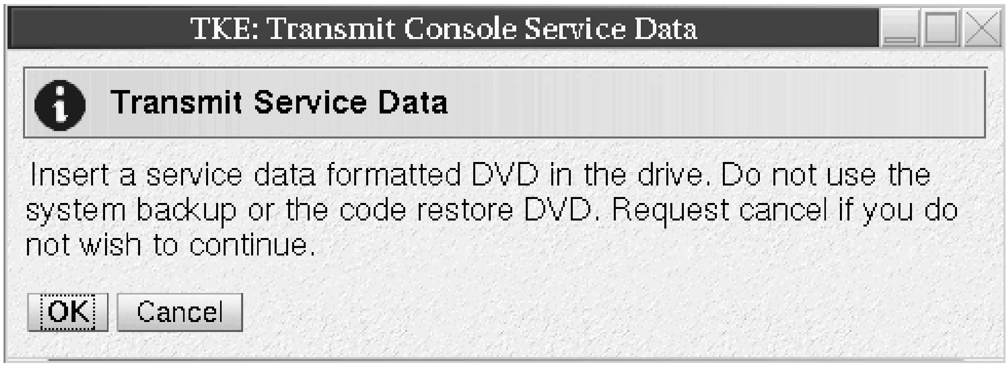
Service Data Selections
Use the displayed categories in this topic to select the types of service data to send to IBM.

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 351 for details.



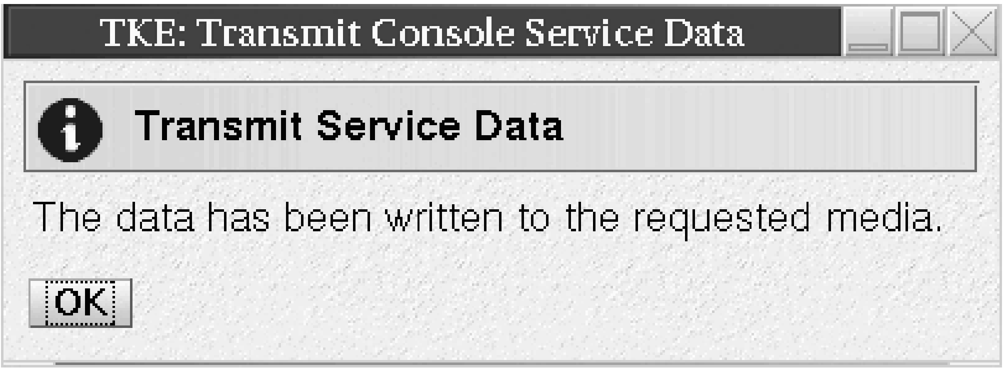
TKE: Transmit Console Service Data

Transmit Service Data

Insert a service data formatted DVD in the drive. Do not use the system backup or the code restore DVD. Request cancel if you do not wish to continue.

Figure 389. Transmit Console Service Data Task Window for DVD-RAM

Successful completion will present the following window.

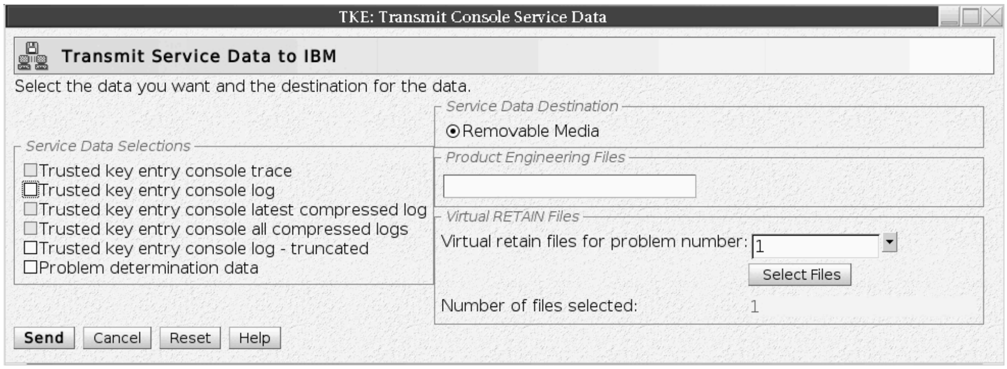

TKE: Transmit Console Service Data

Transmit Service Data

The data has been written to the requested media.

Figure 390. 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.


TKE: Transmit Console Service Data

Transmit Service Data to IBM

Select the data you want and the destination for the data.

Service Data Selections

- □ Trusted key entry console trace
- □ Trusted key entry console log
- □ Trusted key entry console latest compressed log
- □ Trusted key entry console all compressed logs
- □ Trusted key entry console log - truncated
- □ Problem determination data

Service Data Destination

● Removable Media

Product Engineering Files

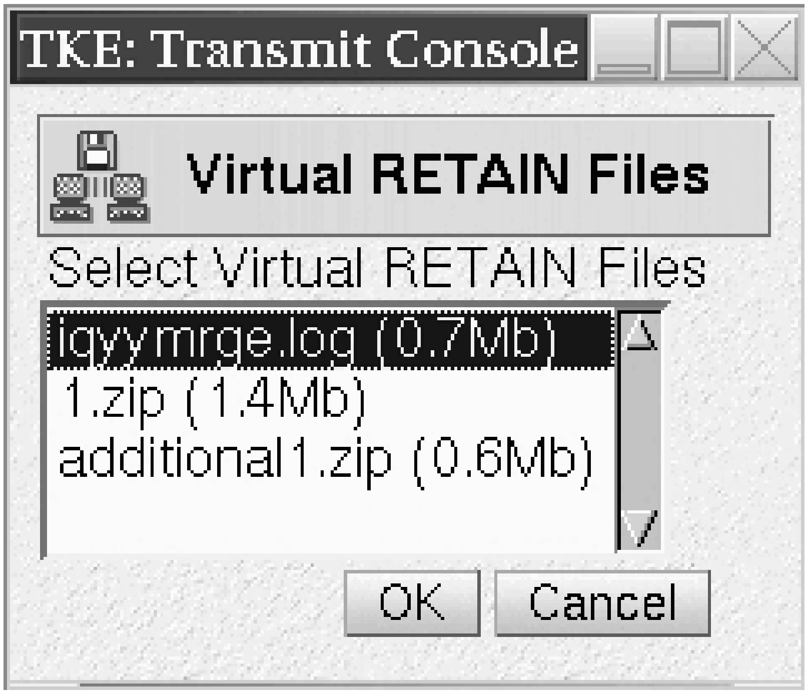
Virtual RETAIN Files

Virtual retain files for problem number: 1

Number of files selected: 1

Figure 391. Update Problem Number for Virtual RETAIN File

Select the applicable Virtual RETAIN Files and click OK.



Select Virtual RETAIN Files

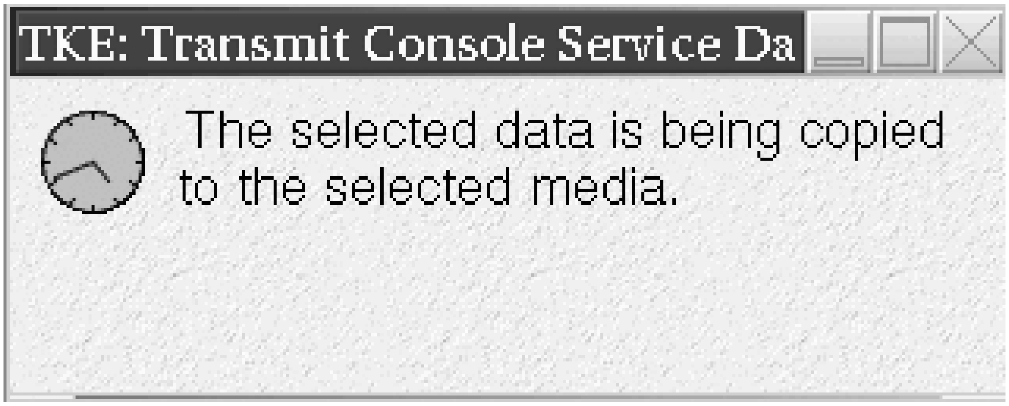
igyymrge.log (0.7Mb)
1.zip (1.4Mb)
additional1.zip (0.6Mb)

Figure 392. 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.



The selected data is being copied to the selected media.

Figure 393. Copying Data to Selected Media

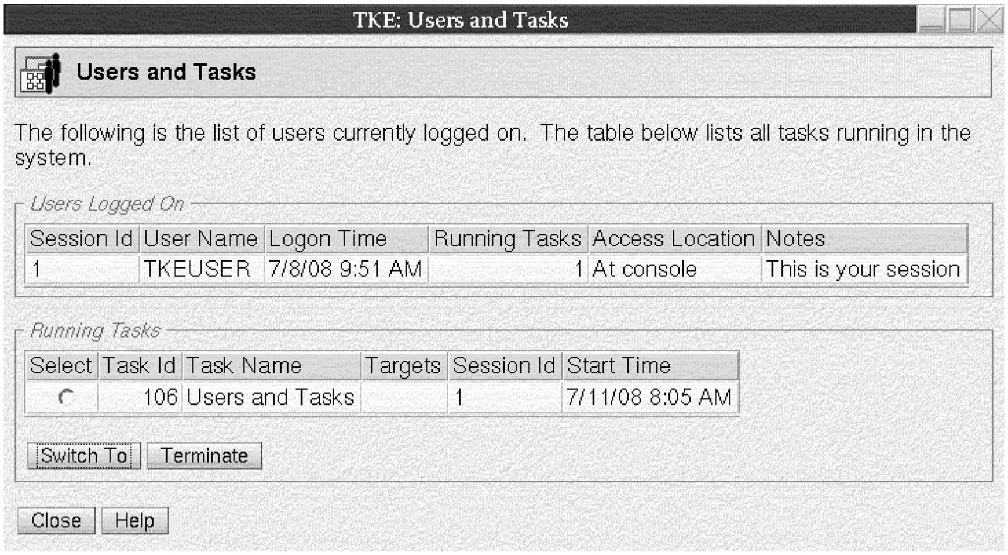
An information window will display when the data has been written to the required media.

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 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.'



The following is the list of users currently logged on. The table below lists all tasks running in the system.

Users Logged On

Session Id	User Name	Logon Time	Running Tasks	Access Location	Notes
1	TKEUSER	7/8/08 9:51 AM	1	At console	This is your session

Running Tasks

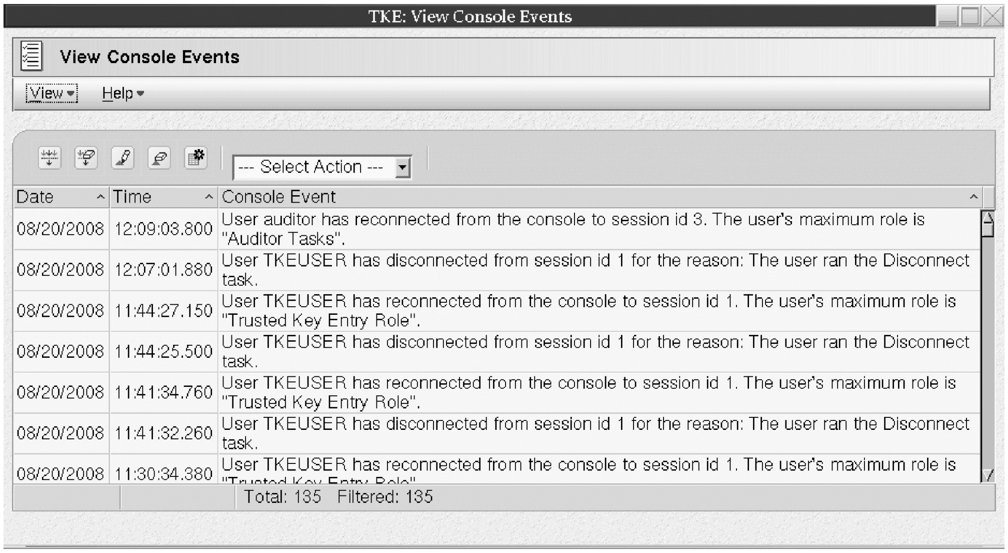
Select	Task Id	Task Name	Targets	Session Id	Start Time
○	106	Users and Tasks		1	7/11/08 8:05 AM

Figure 394. 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.



Date	Time	Console Event
08/20/2008	12:09:03.800	User auditor has reconnected from the console to session id 3. The user's maximum role is "Auditor Tasks".
08/20/2008	12:07:01.880	User TKEUSER has disconnected from session id 1 for the reason: The user ran the Disconnect task.
08/20/2008	11:44:27.150	User TKEUSER has reconnected from the console to session id 1. The user's maximum role is "Trusted Key Entry Role".
08/20/2008	11:44:25.500	User TKEUSER has disconnected from session id 1 for the reason: The user ran the Disconnect task.
08/20/2008	11:41:34.760	User TKEUSER has reconnected from the console to session id 1. The user's maximum role is "Trusted Key Entry Role".
08/20/2008	11:41:32.260	User TKEUSER has disconnected from session id 1 for the reason: The user ran the Disconnect task.
08/20/2008	11:30:34.380	User TKEUSER has reconnected from the console to session id 1. The user's maximum role is "Trusted Key Entry Role".

Figure 395. 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:

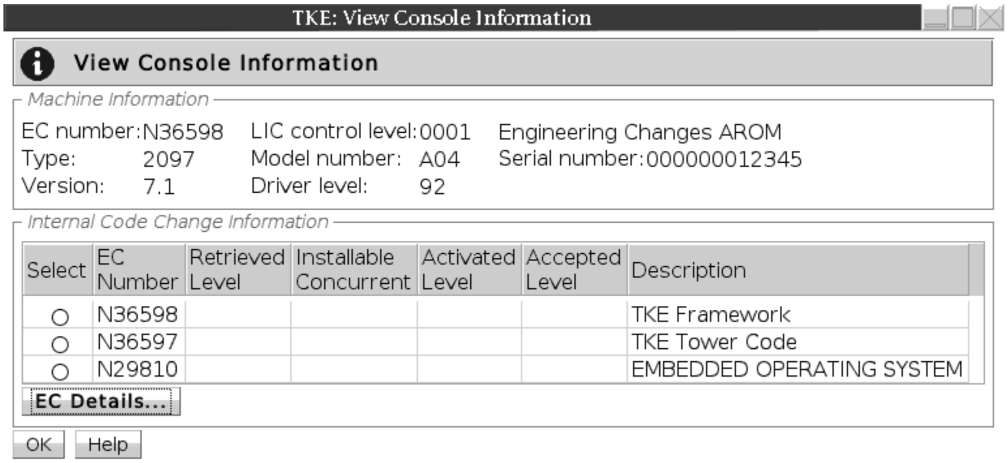
- To change how many events are listed, change list's time range by selecting **Using a different time range**
- To list events from the oldest event to the most recent, select **In order of occurrence**
- To list events from the most recent event to the oldest event, select **In reverse order of occurrence**
- 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.



Machine Information

EC number:	N36598	LIC control level:	0001	Engineering Changes AROM	
Type:	2097	Model number:	A04	Serial number:	000000012345
Version:	7.1	Driver level:	92		

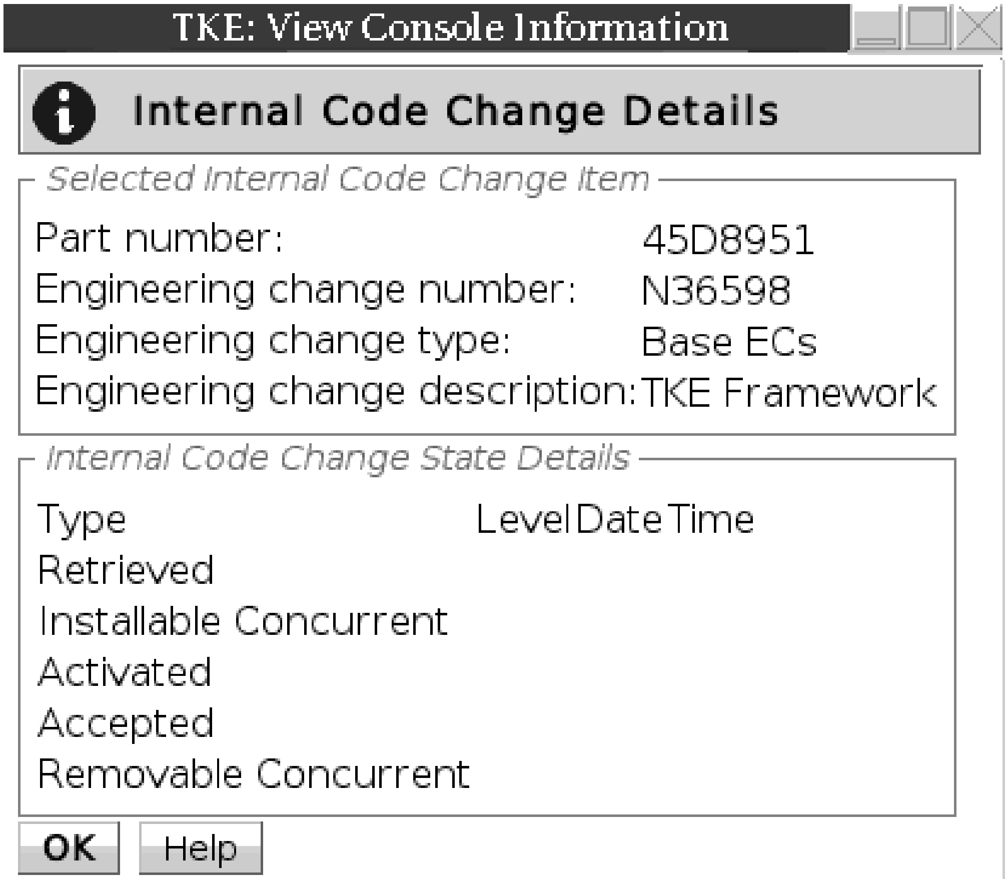
Internal Code Change Information

Select	EC Number	Retrieved Level	Installable Concurrent	Activated Level	Accepted Level	Description
○	N36598					TKE Framework
○	N36597					TKE Tower Code
○	N29810					EMBEDDED OPERATING SYSTEM

Figure 396. 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.



Selected Internal Code Change Item

Part number:	45D8951
Engineering change number:	N36598
Engineering change type:	Base ECs
Engineering change description:	TKE Framework

Internal Code Change State Details

Type	Level	Date	Time
Retrieved			
Installable Concurrent			
Activated			
Accepted			
Removable Concurrent			

Figure 397. 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.

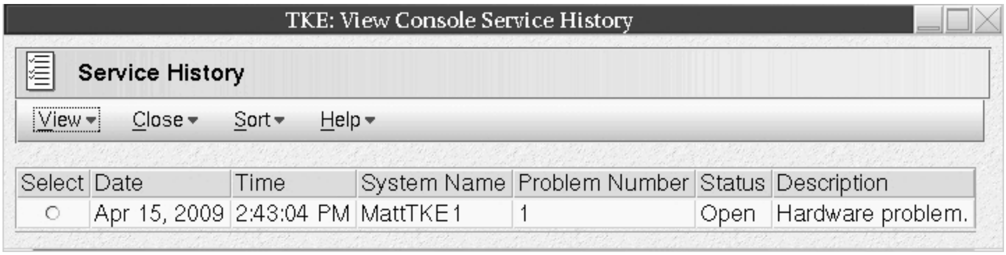
Removable Concurrent
Displays the lowest installed internal code change level that can be removed such that the remaining installed change level can be activated concurrently. That is, you can remove all change levels installed for this console, from the current installed level down to and including 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.



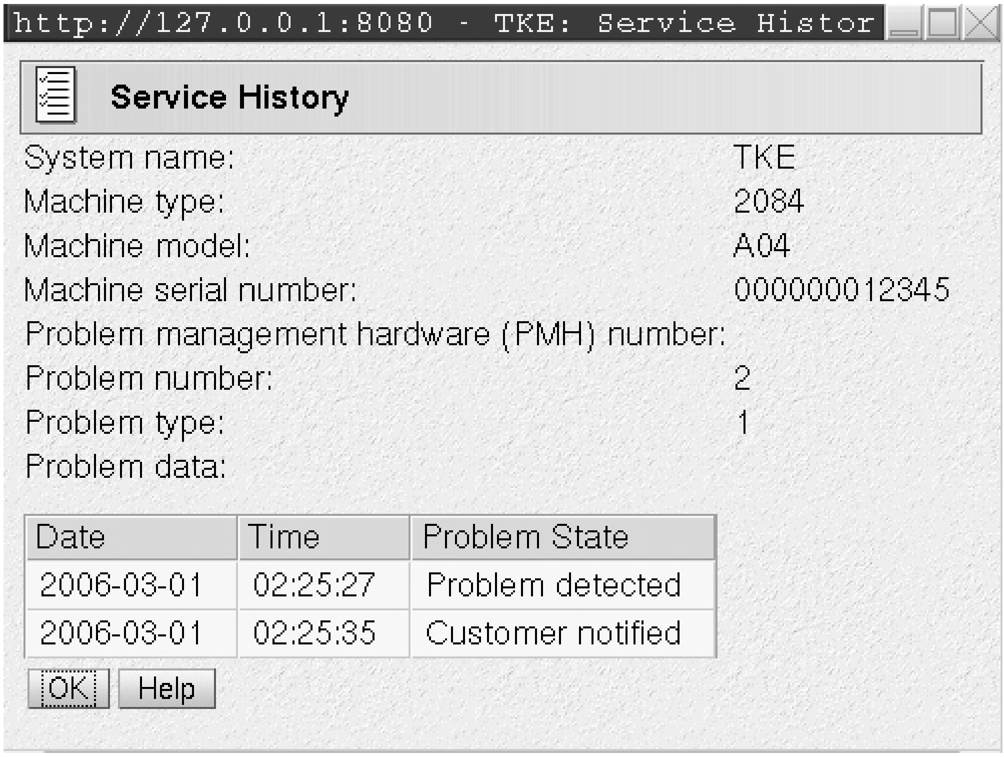
Select	Date	Time	System Name	Problem Number	Status	Description
○	Apr 15, 2009	2:43:04 PM	MattTKE1	1	Open	Hardware problem.

Figure 398. 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

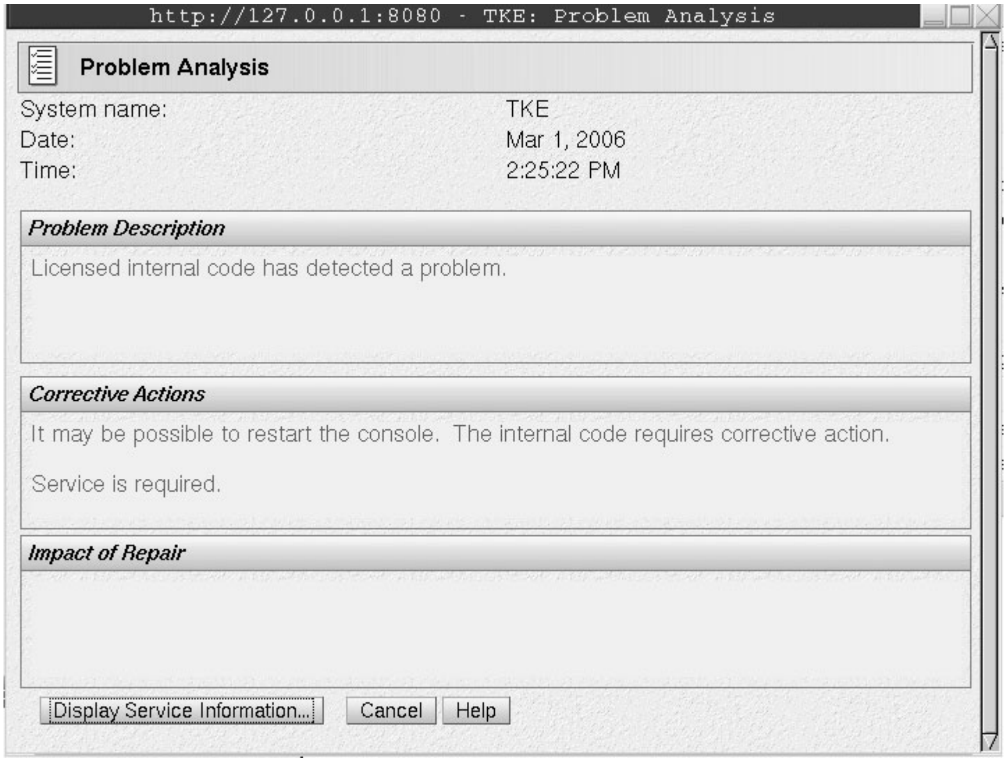
Service History

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 399. 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.


http://127.0.0.1:8080 - TKE: Problem Analysis
Problem Analysis

System name: TKE
Date: Mar 1, 2006
Time: 2:25:22 PM

Problem Description
Licensed internal code has detected a problem.

Corrective Actions
It may be possible to restart the console. The internal code requires corrective action.

Service is required.

Impact of Repair

Display Service Information...
Cancel
Help

Figure 400. Problem Analysis

- **Cancel** exits this task and returns to the Trusted Key Entry Console.

Clicking **Close** on the menu bar brings up two options:

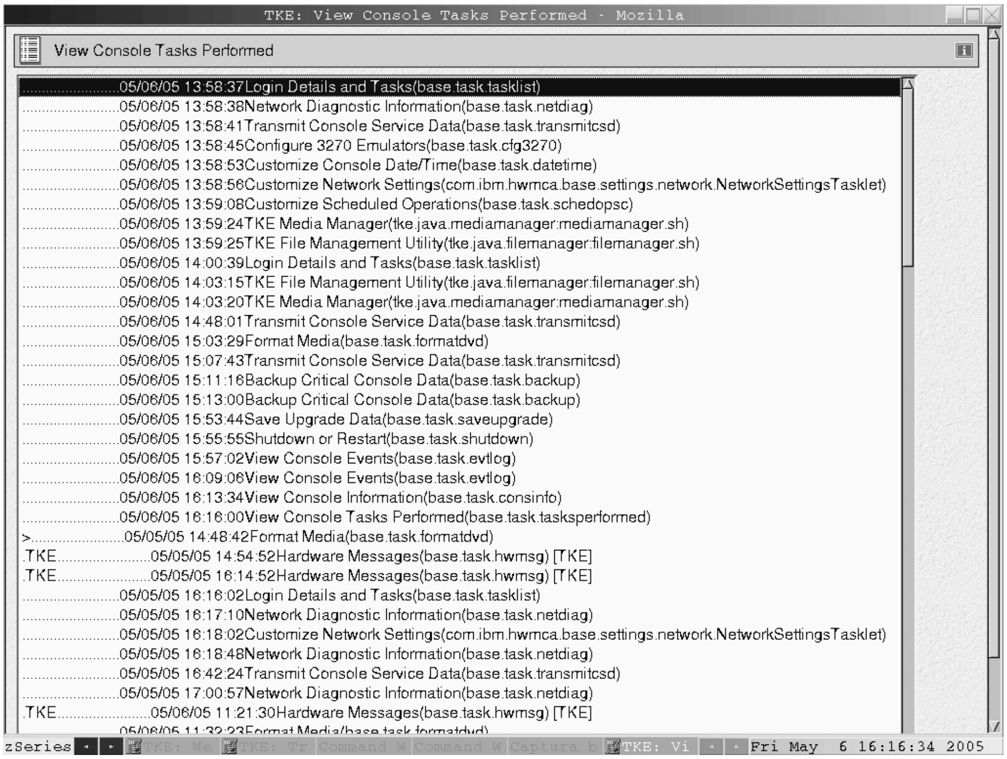
- **Selected Problem** changes the status of the selected problem to Closed.
- **All Problems** changes the status of all open problems to Closed.

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.



```
........................05/06/05 13:58:37Login Details and Tasks(base.task.tasklist)
........................05/06/05 13:58:38Network Diagnostic Information(base.task.netdiag)
........................05/06/05 13:58:41Transmit Console Service Data(base.task.transmitcsd)
........................05/06/05 13:58:45Configure 3270 Emulators(base.task.cfg3270)
........................05/06/05 13:58:53Customize Console Date/Time(base.task.datetime)
........................05/06/05 13:58:56Customize Network Settings(com.ibm.hwmca.base.settings.network.NetworkSettingsTasklet)
........................05/06/05 13:59:08Customize Scheduled Operations(base.task.schedopsc)
........................05/06/05 13:59:24TKE Media Manager(tke.java.mediamanager:mediamanager.sh)
........................05/06/05 13:59:25TKE File Management Utility(tke.java.filemanager:filemanager.sh)
........................05/06/05 14:00:39Login Details and Tasks(base.task.tasklist)
........................05/06/05 14:03:15TKE File Management Utility(tke.java.filemanager:filemanager.sh)
........................05/06/05 14:03:20TKE Media Manager(tke.java.mediamanager:mediamanager.sh)
........................05/06/05 14:48:01Transmit Console Service Data(base.task.transmitcsd)
........................05/06/05 15:03:29Format Media(base.task.formatdvd)
........................05/06/05 15:07:43Transmit Console Service Data(base.task.transmitcsd)
........................05/06/05 15:11:16Backup Critical Console Data(base.task.backup)
........................05/06/05 15:13:00Backup Critical Console Data(base.task.backup)
........................05/06/05 15:53:44Save Upgrade Data(base.task.saveupgrade)
........................05/06/05 15:55:55Shutdown or Restart(base.task.shutdown)
........................05/06/05 15:57:02View Console Events(base.task.evtlog)
........................05/06/05 16:09:06View Console Events(base.task.evtlog)
........................05/06/05 16:13:34View Console Information(base.task.consinfo)
........................05/06/05 16:16:00View Console Tasks Performed(base.task.tasksperformed)
>.......................05/05/05 14:48:42Format Media(base.task.formatdvd)
.TKE.......................05/05/05 14:54:52Hardware Messages(base.task.hwmsg) [TKE]
.TKE.......................05/05/05 16:14:52Hardware Messages(base.task.hwmsg) [TKE]
........................05/05/05 16:16:02Login Details and Tasks(base.task.tasklist)
........................05/05/05 16:17:10Network Diagnostic Information(base.task.netdiag)
........................05/05/05 16:18:02Customize Network Settings(com.ibm.hwmca.base.settings.network.NetworkSettingsTasklet)
........................05/05/05 16:18:48Network Diagnostic Information(base.task.netdiag)
........................05/05/05 16:42:24Transmit Console Service Data(base.task.transmitcsd)
........................05/05/05 17:00:57Network Diagnostic Information(base.task.netdiag)
.TKE.......................05/06/05 11:21:30Hardware Messages(base.task.hwmsg) [TKE]
                        05/06/05 11:32:23Format Media(base.task.formatdvd)
```

Figure 401. View Console Tasks Performed window

View Licenses

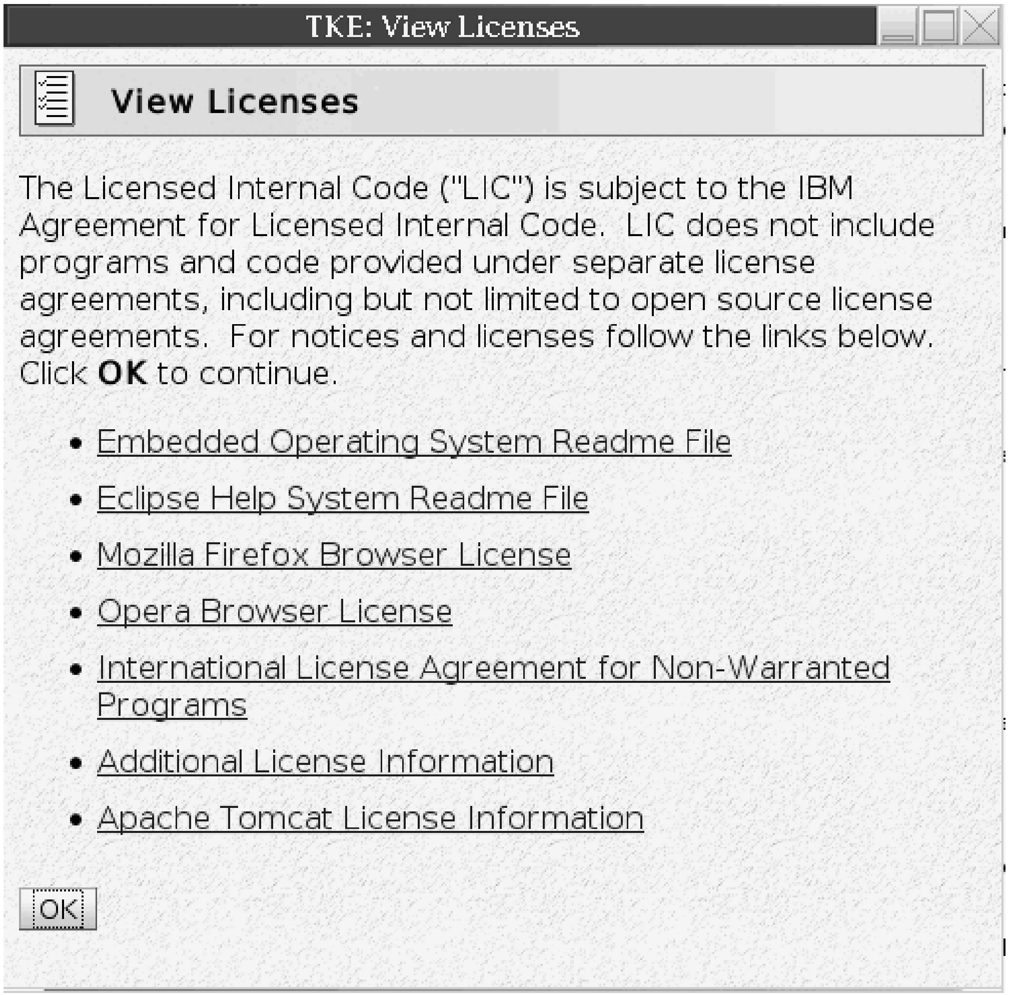
This task is used to view the open source licenses for the Trusted Key Entry Console.

Licenses that can be viewed include:

- Embedded Operating System Readme File
- Eclipse Help System Readme File
- Mozilla Firefox Browser License
- International License Agreement for Non-Warranted Programs
- Additional License Information
- Apache Tomcat License Information
- Boost License Information
- Apache Derby 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.



The Licensed Internal Code ("LIC") is subject to the IBM Agreement for Licensed Internal Code. LIC does not include programs and code provided under separate license agreements, including but not limited to open source license agreements. For notices and licenses follow the links below. Click **OK** to continue.

- 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

Figure 402. 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 209 for more information.

Appendix F. TKE Best Practices

This information describes the setup required for TKE to manage host crypto modules, and a set of setup steps to perform on the TKE workstation. TKE workstations initialized for passphrase and initialized for smart card use are considered separately.

Checklist for Loading a TKE Machine - Passphrase

Expectations

- You are working with CEX2C and CEX3C host crypto modules
- The support element has enabled TKE on these host crypto modules
- LPARs are established
- TKE licensed internal code (LIC) is loaded on the TKE workstation
- Segments 1, 2, and 3 have been loaded on the TKE workstation crypto adapter
- The TKE host transaction program has been configured and started in the host TKE LPAR
- ICSF is started in each LPAR

Setup

- 2 TKEs both running the same level of software
  - One for production
  - One for backup
- 2 Central electronic complex (CEC) cards being shared
  - One Test LPARs (Domain 0)
  - Three Production LPARs (Domain 1, 2, 3)

  TKE can load the master key in 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 - can run the main TKE application
- TKEADM - can create and update TKE roles and profiles
- KEYMAN1 - can clear the TKE new master key register and load the first master key part
- KEYMAN2 - can load TKE middle and last key parts and reencipher TKE 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 host crypto modules is with a minimum of seven host authorities.

- ISSUER
  - Disable host crypto module
  - Enable host crypto module issue

  - Access control issue
  - Zeroize domain issue
  - Domain control change issue
- COSIGN
  - Access control co-sign
  - Enable host crypto module co-sign
  - Zeroize domain co-sign
  - Domain control change co-sign
- MKFIRST
  - AES, DES, ECC, 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 following tasks should be run using the TKE workstation to set up the TKE workstation and the host crypto modules for use. Be aware that the Service Management tasks available to you will vary depending on the console user name you used to log on. Refer to “Service Management Tasks” on page 342 for more information.

1. Customize Network Settings
2. Customize Console Date/Time
3. Initialize the TKE workstation crypto adapter for passphrase use
   a. Predefined TKE roles and profiles are loaded.
   b. The TKE master key is set and TKE key storages are 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 the main TKE application with TKEUSER profile or another profile with the same authority
   a. Load the default authority key for key index 0
   b. Change these options of your security policy via the TKE preferences menu
      - Blind Key Entry
      - Removable media only
   c. Create a Host
   d. Create crypto module groups or domain groups - OPTIONAL
   e. Open a host, a crypto module group, or a domain group (requires host logon)
   f. Open a crypto module notebook, crypto module group notebook, or domain group notebook
   g. Create role(s)
   h. 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.
   i. Create different authorities using the different authority key(s) that were just generated.
   j. Delete the authority 00 or change the authority key to a key that is not the default key. If you delete authority 00 make sure that you have 2 other known authority keys that have the Domain control change issue and co-sign.
8. Configure 3270 Emulators
9. Backup Critical Console Data onto a 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 with CEX2C and CEX3C host crypto modules
- The support element has enabled TKE on these host crypto modules
- LPARs are established (set up and predefined)
- TKE licensed internal code (LIC) is loaded on the TKE workstation
- Segments 1, 2, and 3 have been loaded on the TKE workstation crypto adapter
- The TKE host transaction program has been configured and started in the host TKE LPAR
- ICSF is started in each LPAR
- Smart card readers are attached

Setup

- 2 TKEs both running the same level of software
  - One for production

  - One for backup
- 2 CECs cards being shared
  - One Test LPARs (Domain 0)
  - Three Production LPARs (Domain 1, 2, 3)

  TKE can load the master key in 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 - can run the main TKE application
- SCTKEADM - can run CNM to create and update TKE roles and profiles

Authorities are used to restrict access to the 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 host authorities.

- ISSUER
  - Disable host crypto module
  - Enable host crypto module issue
  - Access control issue
  - Zeroize domain issue
  - Domain control change issue
- COSIGN
  - Access control co-sign
  - Enable host crypto module co-sign
  - Zeroize domain co-sign
  - Domain control change co-sign
- MKFIRST
  - AES, DES, ECC, 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 342 for more information.

1. Customize Network Settings
2. Customize Console Date/Time
3. Initialize the TKE workstation crypto adapter for smart card use:
   a. Predefined TKE roles and profiles are loaded.
   b. The TKE master key is set and TKE key storages are initialized.
4. Open the SCUP application
   a. Create a CA smart card
   b. Backup CA smart cards
   c. Create TKE smart card(s)

      Note: In general, smart cards created on a particular TKE release cannot be used on TKE workstations that are at prior release levels. There are exceptions. See “Smart Card Usage” on page 34.
   d. 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
      - Do this only if you want to 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 main TKE application 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. Open a host, a crypto module group, or a domain group (requires host logon)

   f. Open a crypto module notebook, crypto module group notebook, or domain group notebook

   g. Create role(s)

   h. Generate authority key(s) and save them to TKE smart card(s)

      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.

   i. Create different authorities using the different authority key(s) that were just generated.

   j. Delete the authority 00 or change the authority key to a key that is not the default key. If you delete authority 00 make sure that you have 2 other known authority keys that have the Domain control change issue and cosign.

7. Configure 3270 Emulators
8. Backup Critical Console Data
9. Customize Scheduled Operations to schedule the backup critical console data task
10. If using the same set of smart cards on another TKE, you need to use the Remote Enroll feature for TKE.

Appendix G. 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 mhvrcfs@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.

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

Product Number: 5694-A01

Printed in USA

SA23-2211-07