z/OS

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

Version 2 Release 1

SC14-7511-04

Note
Before using this information and the product it supports, read the information in "Notices" on page 385.

This edition applies to TKE 8.0 and Version 2 Release 1 of z/OS (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

About this information

This information introduces Version 8.0 of the Trusted Key Entry (TKE) customized solution for ICSF.

It includes information to support these tasks for the solution:

- Planning
- Installing
- Administering
- Customizing
- Using

Who should read this information

This information is for technical professionals who will be installing, implementing and administering Version 8.0 of the IBM® Trusted Key Entry product. It is intended for anyone who manages cryptographic keys, usually a security administrator.

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

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

How to use this information

The major topics are:

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

Chapter 2, "Using smart cards with TKE," on page 33, gives an explanation of the smart card support for the TKE workstation.

Chapter 3, "TKE migration and recovery installation," on page 45, provides details on migrating from previous versions of TKE.

Chapter 4, "TKE setup and customization," on page 61, provides information about using TCP/IP and the host files needed by TKE. It also explains how to configure the TKE workstation for TCP/IP and initialize the TKE workstation.

Chapter 5, "TKE up and running," on page 93, provides preliminary setup and initialization tasks that are necessary for operation.

Chapter 6, "Main window," on page 103, explains the beginning window of the TKE program and the functions and utilities accessible from it.

Chapter 7, “Using the Crypto Module Notebook to administer CCA crypto modules,” on page 131, explains how to work with CCA crypto modules. The status of the master keys and key parts are displayed. This window is where the keys can be generated, loaded and cleared. The domain controls are set here. The zeroize domain function is accessed from here. RSA handling is described here.

Chapter 8, “Using the Crypto Module Notebook to administer EP11 crypto modules,” on page 197 explains how to work with EP11 crypto modules.

Chapter 9, “Auditing,” on page 215, provides information on auditing.

Chapter 10, “Managing keys using TKE and ICSF,” on page 229, explains how ICSF is used when loading and importing keys to a host crypto module on IBM S/390®, IBM System z10™, IBM zEnterprise® 196 or IBM zSeries hardware.

Chapter 11, “Cryptographic Node Management utility (CNM),” on page 237, provides information on the CNM utility tasks.

Chapter 12, “Smart Card Utility Program (SCUP),” on page 279, provides information on the SCUP tasks.

Appendix A, “Secure key part entry,” on page 303, provides information on secure entry of a known key part onto a TKE or EP11 smart card.

Appendix B, “LPAR considerations,” on page 313, discusses host setup considerations for managing host crypto modules across multiple logical partitions.

Appendix C, “Trusted Key Entry - workstation crypto adapter initialization,” on page 315, provides information on the TKE Workstation Cryptographic Adapter Initialization.

Appendix D, “Clear RSA key format,” on page 323, provides information on the format of RSA-entered keys.

Appendix E, “Trusted Key Entry applications and utilities,” on page 325, provides information on TKE console applications and utilities and Service Management tasks.

Appendix F, “TKE best practices,” on page 371, provides information on Checklists for Loading a TKE Machine for both passphrase and smart card.

Appendix G, “TKE hardware support and migration information,” on page 377, provides information on TKE release and feature codes available by CEC levels, smart card readers and smart cards orderable by TKE release, TKE (LIC) upgrade paths, and host cryptographic modules managed by TKE.

Appendix H, “Accessibility,” on page 381, provides information on accessibility features that help a user who has a physical disability to use software products successfully.

“Notices” on page 385, provides information on notices, programming interface information, and trademarks.

Where to find more information

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

- *z/OS Cryptographic Services ICSF Administrator's Guide*
- *z/OS Cryptographic Services ICSF System Programmer's Guide*
- *z/OS Cryptographic Services ICSF Application Programmer's Guide*
- *z/OS Cryptographic Services ICSF Overview*
- *z/OS Cryptographic Services ICSF Messages*
- *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 provide any other feedback that you have.

Use one of the following methods to send your comments:

1. Send an email to mhvrcfs@us.ibm.com.
2. Send an email from the "Contact us" web page for z/OS (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
   US
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 TKE Workstation User's Guide
  SC14-7511-04
- The topic and page number that is 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 the comments in any way appropriate without incurring any obligation to you.

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

If you have a technical problem

Do not use the feedback methods that are listed for sending comments. Instead, take one of the following actions:

- Contact your IBM service representative.
- Call IBM technical support.
- Visit the IBM Support Portal at z/OS support page (http://www.ibm.com/systems/z/support/).

Summary of changes

Changes made in z/OS V2R1 as updated April 2015

This document contains information previously presented in *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SC14-7511-03, which supports z/OS Version 2 Release 1.

New

- Added the following note to Table 28 on page 380:

  Important: A minimum level of ICSF HCR77B0 is required when managing Crypto Express5S coprocessors. Older releases of ICSF, even in toleration mode, will not return the list of Crypto Express5S coprocessors to the TKE.

Changes made in z/OS V2R1 as updated February 2015

This document contains information previously presented in *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SC14-7511-01, which supports z/OS Version 2 Release 1.

New

- TKE 8.0 is required for managing the Crypto Express5S coprocessor.

  TKE 8.0 support for the Crypto Express5S includes the ability to use the host adapter migration wizard to collect data from old crypto coprocessors and apply the data to the Crypto Express5S.

  Important: A minimum level of ICSF HCR77B0 is required when managing Crypto Express5S coprocessors. Older releases of ICSF, even in toleration mode, will not return the list of Crypto Express5S coprocessors to the TKE.
- Crypto module groups are no longer supported on TKE. A utility was created to allow you to create Domain Groups from existing Crypto Module group definitions.
- There is a new wizard-like feature that steps you through the process of loading all master keys in one task. In addition, there is a new feature that allows you to create a set of master key parts for all of different master key types in one task.
- For passphrase profiles on the TKE local crypto adapter, a user can now change their own password during the sign on process.

  Note: The new change password option is not available during a group logon.
- The Privileged Mode Access ID of ADMIN now has the capability to configure the size of the verification patterns displayed for keys and key parts.
- TKE applications now include an indicator in the title when the application has access to the smart card readers.
- "Host crypto module index values" on page 195 is new.
- Appendix G, "TKE hardware support and migration information," on page 377 is new.

Deleted

No content was removed from this information.

Changes made in z/OS Version 2 Release 1, as updated December 2013

This book contains information previously presented in *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SC14-7511-00, which supports z/OS Version 2 Release 1.

New information

- DVD-RAM is no longer supported on TKE 7.2 or later systems. If you have a DVD-RAM that is formatted for TKEDATA (TKEDATA DVD-RAM) and you want to use the files from the TKEDATA DVD-RAM on a TKE 7.2 or later system, see "Using files from a TKEDATA DVD-RAM on a TKE 7.2 or later system" on page 45.

Changes made in z/OS V2R1

This book contains information previously presented in *z/OS Cryptographic Services ICSF Trusted Key Entry User's Guide*, SA23-2211-08, which supports z/OS Version 1 Release 13.

New information

- A new Migration Setup wizard simplifies the migration of customer data. For information, see Chapter 3, "TKE migration and recovery installation," on page 45 and "The TKE Workstation Setup wizard" on page 66.
- New information is included on using an SSL 3270 emulation session. See "Using an SSL 3270 emulation session" on page 87.
- A new ACP, "Manage Host List" controls the ability to manage a host list. For information, see "TKE 7.3 role migration considerations for customer-defined roles" on page 85.
- A new function to close a host is provided on the TKE main window. For information, see "Closing a host" on page 106.
- A new function unloads the authority signature key. For information, see "Unload signature key" on page 119.
- On the Crypto Module Notebook **Roles** tab, a new option is added to remove all domain access to all domains on the crypto module. See "Domain access" on page 137.
- A new option on the Domain Keys page of the Crypto Module Notebook, **Set, immediate**, sets a master key. For information, see "Set, immediate" on page 165.
- You can specify up to 20 PIN values whose use is restricted on the new Domain Restricted PINS page of the Crypto Module Notebook. For information, see "Domain Restricted PINs page" on page 193.
- On the Domain controls page of the Crypto Module Notebook for CCA crypto modules, you can save domain controls to a file and load them from a file. See "Domain Controls pages" on page 189.

- On the Domain control points page of the Crypto Module Notebook for EP11 crypto modules, you can save control points to a file and load them from a file. See “Domain Control Points page” on page 212.
- The **Configuration migrations tasks** application supports both CCA and EP11 crypto modules. For more information, see “Configuration migration tasks” on page 337.

Changed information

- The section on remote crypto adapter enrollment was rewritten. See “Remote crypto adapter enrollment” on page 296.
- “Multi-signature commands” are now referred to as “dual-signature commands.”
- “Asymmetric master keys” are now referred to as “RSA master keys”.

Deleted information

- The list of single-signature commands was deleted.

Changes made in z/OS Version 1 Release 13, as updated September 2012

This book contains information previously presented in *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SA23-2211-07, which supports z/OS Version 1 Release 13.

New information

- Support for CEX4P crypto modules. A CEX4P is a host crypto module that provides PKCS #11 services. A new Crypto Module Notebook interface is provided for managing the CEX4P. For a description of the new interface, see Chapter 8, “Using the Crypto Module Notebook to administer EP11 crypto modules,” on page 197.
- Support for EP11 smart cards. These smart cards are required to manage CEX4P crypto modules. They are initialized and personalized through the Smart Card Utility Program (SCUP). For more information, see “EP11 smart card menu functions” on page 292.
- Support for 24-byte DES master keys.
- Support for new DES operational keys.
- A new AES CIPHER key attribute, "key can be used for data translate only".
- A new smart card, part 74Y0551. These cards can be used for any of the types of smart cards used on the TKE, but are required for EP11 smart cards.
- Support for up to 4 smart card readers.

Deleted information

- In Chapter 10, “Managing keys using TKE and ICSF,” on page 229, information that is covered in *z/OS Cryptographic Services ICSF Administrator's Guide* has been deleted. The following sections were deleted:
  - "Master Key Parts"
  - "First-Time Startup"
  - "Changing the Master Key Using the Master Key Panel"
  - "Re-entering Master Keys After They have been Cleared"
  - "Asymmetric-keys Master Key Parts"
  - "Refreshing the CKDS"
  - "Updating the CKDS with the AES master key"

- The TKE Media Manager is no longer provided. Information about it has been deleted.

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 about how to migrate your customer unique data from one version of TKE to another. See Chapter 3, "TKE migration and recovery installation," on page 45.
- New access control points (ACPs), and a new utility for adding ACPs to existing roles on your TKE workstation crypto adapter. For more information , see "Adding new ACPs to existing roles using the Migrate Roles utility" on page 81.
- 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. For more information, see "Domain Decimalization Tables page" on page 191.

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 module configuration data, including roles, authorities, domain control settings, and master keys, securely to a file, and reapply the data to another host crypto module or crypto module group. These tools simplify the task of installing new or replacement host crypto modules, and can be used for backup and disaster recovery as well. For more information about migration wizard tools, see "Configuration migration" on page 335.
- 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) data set. For more information, see "TKE Audit Record Upload Configuration utility" on page 223.
- Support for IBM zEnterprise 196 (z196) hardware.
- Support for AES master keys and operational keys.
- Support for ECC (APKA) 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 IBM part number 45D3398 smart cards. See "Datakey card usage" on page 38.

- 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.

Chapter 1. Overview

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

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

Trusted Key Entry (TKE) is an optional hardware feature of System z that provides a management tool for System z Host Cryptographic Coprocessors. The main features provided by TKE are:

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

  Notes:

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

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

TKE works together with ICSF:

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

disable and enable PKA services so that the Public Key Algorithm (PKA) master keys can be reset and changed and the PKDS can be initialized, reenciphered, and refreshed.

Trusted Key Entry components

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

TKE hardware

- TKE Workstation
- IBM 4767 Cryptographic adapter

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

Also available with a TKE 8.0 workstation are:

- Feature 00JJ019: 2 OmniKey smart card readers and 20 IBM part number 00JA710 smart cards
- Feature 00JJ020: 10 IBM part number 00JA710 smart cards

Notes:

1. To manage EP11 host crypto modules, EP11 smart cards are required. Only IBM part numbers 74Y0551 and 00JA710 can be used to create EP11 smart cards.
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 or later.
4. Older smart cards must be reinitialized on TKE 7.0 or later to be able to store ECC (APKA) master keys.

Two USB flash memory drives are shipped with TKE:

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

TKE software

The following software is preinstalled on the TKE workstation:

- IBM Cryptographic Coprocessor Support Program Release 5.0.
- Trusted Key Entry Version 8.0 - FC 0877.

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.
4. TKE 7.1 software, FC 0867, can only be installed on a TKE 7.0 workstation, FC 0841.
5. TKE 7.2 software, FC 0850, can only be installed on a TKE 7.0 workstation, FC 0841.

6. TKE 7.3 software, FC 0872, can be installed only on a TKE 7.0 workstation, FC 0841 or FC 0842.
7. TKE 8.0 software, FC 0877, can be installed only on a TKE 8.0 workstation, FC 0847.

Supported host cryptographic card features

The host cryptographic cards supported with TKE 8.0 are:

- The Crypto Express2 Coprocessor (CEX2C)
- The Crypto Express3 Coprocessor (CEX3C)
- The Crypto Express4 CCA Coprocessor (CEX4C)
- The Crypto Express4 PKCS #11 Coprocessor (CEX4P)
- The Crypto Express5S CCA Coprocessor (CEX5C)
- The Crypto Express5S PKCS #11 Coprocessor (CEX5P)

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 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.

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

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

Host crypto module

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

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

- Crypto-Module ID (CMID)

  This value 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.
- Device Key

  A unique device key is generated for each host crypto module. The device key and OA certificate chain are used to authenticate responses from the crypto module. The type of device key depends on the type of host crypto module.
  - For the CEX2C, the device key is a 1024-bit RSA key.
  - For the CEX3C, CEX4C, and CEX4P, the device key is a 4096-bit RSA key.
  - For the CEX5C and CEX5P, the device key is a P521 ECC key.

TKE concepts and mechanisms

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

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

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

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

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

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

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

Integrity

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

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

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

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

Authorities

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

All administration of host CCA crypto modules is done with authorities. An authority is identified to the host crypto module 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 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 using the private key of its signature key pair, and the host crypto module verifies the signature using the public key of the same key pair.

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

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

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

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 default signature key is a 1024-bit RSA key.

For CCA host crypto modules, the initialization process creates the authority 00 and assigns the authority default signature key to this authority.

Roles

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

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

Roles are not supported on EP11 host crypto modules.

Administrators

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

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

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

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

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

Crypto module signature key

Each host crypto module signs its replies using the crypto module device key. The device key is loaded into the host crypto module when it is manufactured. Beginning with the CEX5C and CEX5P, the device key is an ECC key. For prior crypto modules, it is an RSA key.

When TKE connects to a host, it queries the attached crypto modules and retrieves their device key certificates and certificate chains. After verifying the certificate chain ends with a certificate signed by the IBM class root key, TKE saves the device public key and uses it to validate all future signed replies from the host crypto module.

Command signatures

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

Command signatures for CCA host crypto modules

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

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

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

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

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

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

The single-signature commands for operational keys are:

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

Command signatures for EP11 host crypto modules

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

If the EP11 host crypto module or the target domain is in imprint mode, no command signatures are required, but only a limited subset of administrative commands can be executed. (See “Imprint mode” on page 198 for more information.) Otherwise, the number of required signatures depends on the command type and on the signature threshold and revocation signature threshold attributes set by the user for the host crypto module or target domain.

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

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

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

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

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

- Set control points
- Zeroize domain
- Zeroize crypto module

Key-exchange protocol

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

Domain controls and domain control points

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

TKE operational considerations

The TKE workstation can manage CEX2C, CEX3C, CEX4C, CEX4P, CEX5C, and CEX5P crypto modules attached to a host System z.

Logically partitioned (LPAR) mode considerations

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

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

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

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

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

Defining your security policy

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

The security plan might include these areas:

- General
  - How many security officers does your organization have?

  - How often is the master key changed?
  - Who is authorized to enter master key parts?
  - Do the key parts you enter from the keyboard need to be masked?
  - Who has access to the secure computer facility?
  - What are the policies for working with service representatives?
  - Will you be using smart card support?
- Workstation Considerations
  - Who will use the TKE workstation?
  - Where will your workstation be located?
  - Is it only accessible to the security administrators or security officers?
  - How many workstations will there be?
  - Will you use group logon?
  - Who will backup the workstations?
  - Where will the passwords of the security officers be saved?
- Command Considerations
  - Which commands require multiple signatures?
  - Which crypto modules should be grouped together?
  - How many signatures will be required?
  - Will this affect the availability of the system?
  - Which commands require a single signature?
  - Who will make these decisions?

TKE enablement

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

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

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

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

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

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

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

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

Trusted Key Entry console

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

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

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

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

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.

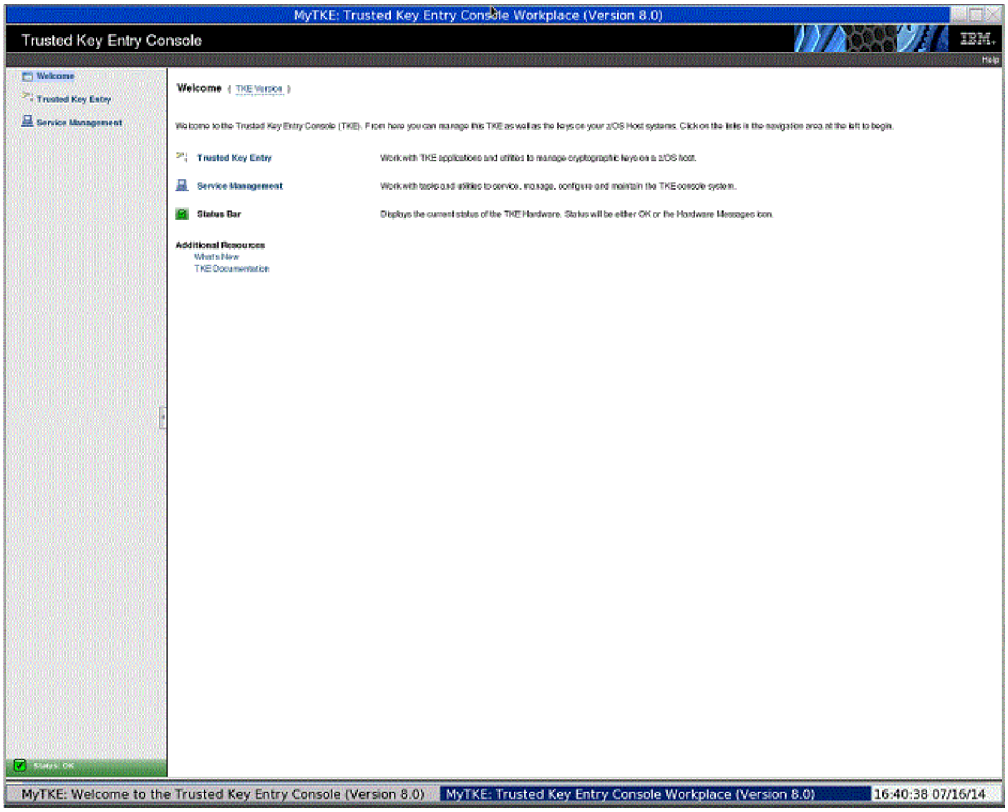


Figure 1. TKE Console - initial panel

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

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

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

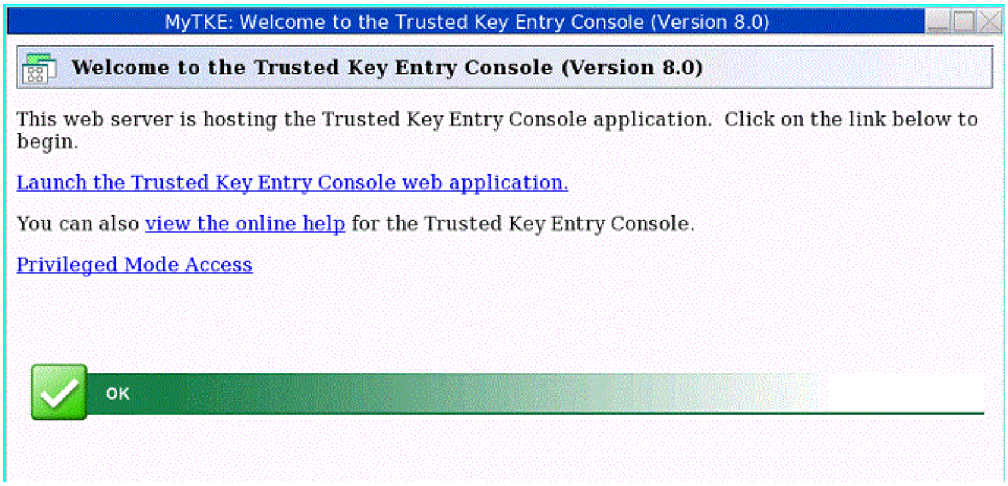


Figure 2. TKE Console - pre-login panel

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

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

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

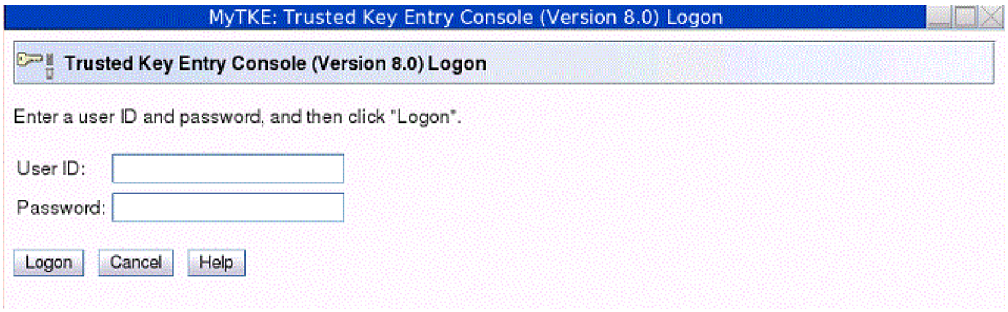


Figure 3. Log on with other privileged mode access console user names

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

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

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

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

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

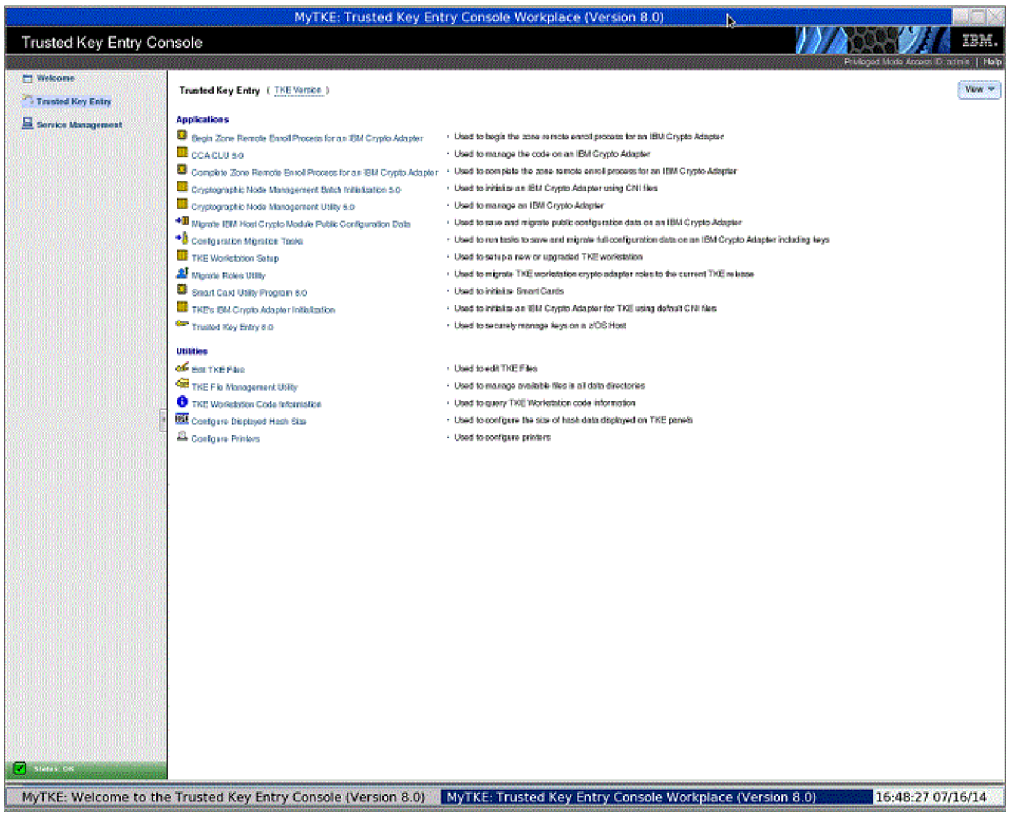


Figure 4. Trusted Key Entry for ADMIN - categorized

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

- **Privileged Mode Access ID** is displayed if the console user is logged on as a privileged mode access user.
- **Crypto Adapter Logon ID** is displayed when the user of a TKE application is logged on to the Crypto Adapter.
- **Smart Card Readers Locked By** is displayed when a TKE application has a lock on the smart card readers.

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

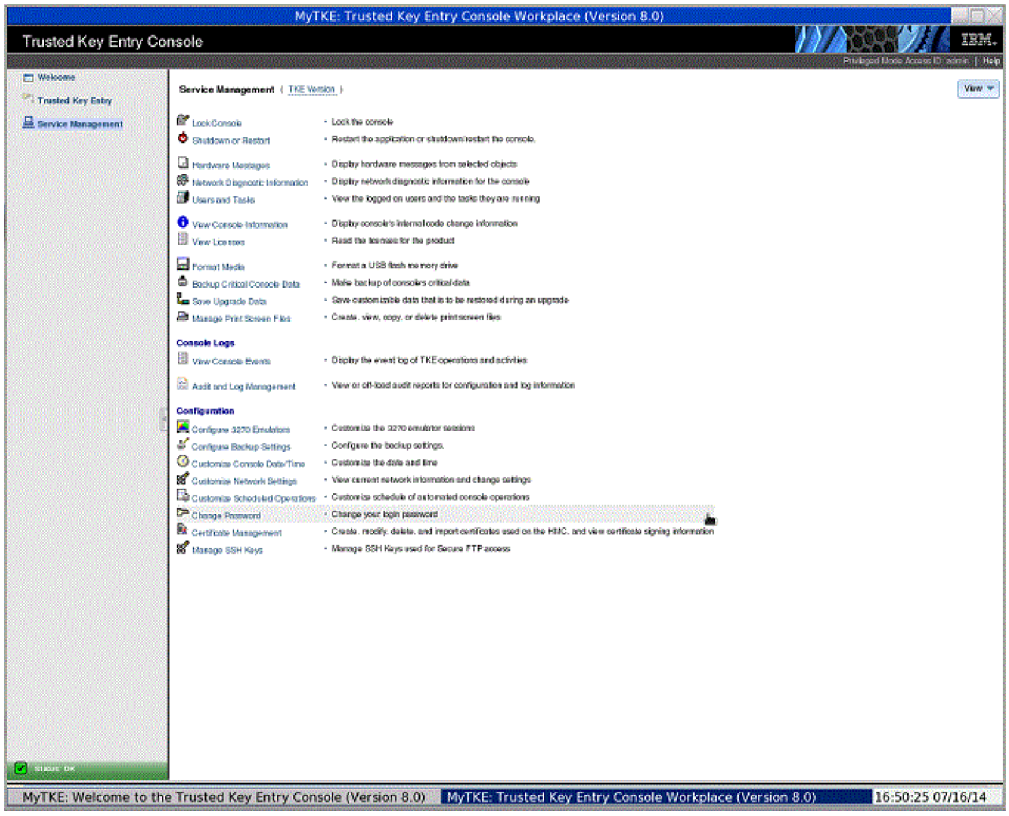


Figure 5. Service Management – No Privileged Mode Access

TKE workstation crypto adapter roles and profiles

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

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

- Run the TKE's IBM Crypto Adapter Initialization application to initialize the 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 its permitted operations list. The list of permitted operations in a role determines what a profile with the role is allowed to do.

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

There is always a current role in effect.

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

Authority checking on the TKE

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

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

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

Types of profiles

A TKE workstation crypto adapter supports 3 types of profiles:

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

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

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

For instructions on creating or changing roles and profiles, refer to Chapter 11, "Cryptographic Node Management utility (CNM)," on page 237.

Initializing a TKE workstation crypto adapter

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

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

Initial adapter conditions

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

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

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

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

Table 1. CAA code loaded for specific releases of TKE

TKE Release	CCA Release
TKE 5.3	CCA 3.4
TKE 6.0	CCA 3.5
TKE 7.0	CCA 4.1
TKE 7.1	CCA 4.2
TKE 7.2	CCA 4.3
TKE 7.3	CCA 4.4
TKE 8.0	CCA 5.0

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

  Notes:

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

Initial adapter conditions on upgraded TKE workstations: When you upgrade an existing TKE workstation to a new level of TKE, the upgrade process states:

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

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

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

IBM-supplied roles and profiles on TKE workstation 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 workstation crypto adapter, you must decide if you want to sign on to the adapter using passphrase profiles, smart card profiles, or both types of profiles.

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

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

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

Guidelines: Make your choice following these guidelines:

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

Initializing for use with smart card profiles: When you initialize a TKE workstation crypto adapter for use with smart card profiles, the following 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 modules.

- 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 workstation 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 crypto modules.

  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 crypto modules.

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

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

Roles and profiles definition files

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

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

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

Table 2. Definition files and their corresponding role or profile

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

Role definition files

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

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

All 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 workstation crypto adapter is initialized, the IBM-supplied roles are created from the IBM-supplied definition files.

Guideline: 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 workstation crypto adapter is initialized for use with passphrase profiles, five 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

TKE Release	DEFAULT	KEYMAN1	KEYMAN2	TKEADM	TKEUSER
TKE 5.0 to 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
TKE 7.2	default_72.rol	keyman1_72.rol	keyman2_72.rol	tkeadm_72.rol	tkeuser_72.rol
TKE 7.3	default_73.rol	keyman1_73.rol	keyman2_73.rol	tkeadm_73.rol	tkeuser_73.rol
TKE 8.0	default_80.rol	keyman1_80.rol	keyman2_80.rol	tkeadm_80.rol	tkeuser_80.rol

Note: Beginning in TKE 7.0, release-specific IBM-supplied role definition files were shipped with the TKE workstation.

Smart card roles

When a TKE workstation crypto adapter is initialized for use with smart card profiles, three 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

TKE Release	DEFAULT	SCTKEADM	KEYMAN2
TKE 5.0 to 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
TKE 7.2	tempdefault_72.rol	sctkeadm_72.rol	sctkeusr_72.rol
TKE 7.3	tempdefault_73.rol	sctkeadm_73.rol	sctkeusr_73.rol
TKE 8.0	tempdefault_80.rol	sctkeadm_80.rol	sctkeusr_80.rol

Note: Beginning in TKE 7.0, release-specific IBM-supplied role definition files were shipped with the TKE workstation.

Customer-defined role definition files

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

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

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

For Instructions on creating or changing role definition files, refer to Chapter 11, "Cryptographic Node Management utility (CNM)," on page 237.

Profile definition files

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

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

All 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 workstation 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.

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

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

Customer-defined profile definition files

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

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

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

For instructions on creating or changing profile definition files, refer to Chapter 11, “Cryptographic Node Management utility (CNM),” on page 237.

IBM-supplied role access control points (ACPs)

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

ACP considerations for user-defined roles

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

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

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

ACPs assigned to IBM-supplied roles

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

Note:

- Beginning in TKE 7.1, the ACP "TKE USER, X'8002’" is no longer used. This ACP was replaced with more granular access control checking. The new ACPs that are checked are ACPs X'1000' through X'100E'.
- Beginning with TKE 8.0, TKE supports a USB-attached printer. In order to print files, the X'1010' (print files) ACP must be enabled. This ACP is not enabled by default in any IBM-supplied role.

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

- SCTKEADM
- SCTKEUSR
- DEFAULT

SCTKEADM

Table 6. ACPs assigned to the SCTKEADM role

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 5.2	Enabled in release TKE 5.3, TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0
Required 0047 Change Own Passphrase	X'0047'						x
Required 008E Generate Key	X'008E'	x	x	x	x	x	x
Required 0100 PKA96 Digital Signature Generate	X'0100'			x	x	x	x
Required 0103 PKA96 Key Generate	X'0103'		x	x	x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x	x	x

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

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 5.2	Enabled in release TKE 5.3, TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0
Required 011F RSA Decipher Clear Key	X'011F'						x
Required 012A Encipher Data Using AES	X'012A'						x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'			x	x	x	x
Required 0203 Delete Retained Key	X'0203'		x	x	x	x	x
Required 027D Permit Regeneration Data	X'027D'						x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'			x	x	x	x
Load First Master Key Part	X'0018'	x	x	x	x	x	x
Combine Master Key Parts	X'0019'	x	x	x	x	x	x
Set Master Key	X'001A'	x	x	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x	x
Clear New Master Key Register	X'0032'	x	x	x	x	x	x
Reencipher to Current Master Key	X'0090'	x	x	x	x	x	x
Reencipher to Current Master Key2	X'00F1'					x	x
PKA96 Key Token Change	X'0102'	x	x	x	x	x	x
One-Way Hash, SHA-1	X'0107'	x	x	x	x	x	x
Reset Intrusion Latch	X'010F'	x	x	x	x	x	x
Set Clock	X'0110'	x	x	x	x	x	x
Reinitialize Device	X'0111'	x	x	x	x	x	x
Initialize Access-Control System	X'0112'	x	x	x	x	x	x
Change User Profile Expiration Date	X'0113'	x	x	x	x	x	x
Change User Profile Authentication Data	X'0114'	x	x	x	x	x	x
Reset User Profile Logon-Attempt-Failure Count	X'0115'	x	x	x	x	x	x
Delete User Profile	X'0117'	x	x	x	x	x	x
Delete Role	X'0118'	x	x	x	x	x	x
Load Function-Control Vector	X'0119'	x	x	x	x	x	x
Clear Function-Control Vector	X'011A'	x	x	x	x	x	x
Clear AES New Master Key Register	X'0124'					x	x
Load First AES Master Key Part	X'0125'					x	x
Load Middle/Last AES Master Key Parts	X'0126'					x	x
Set AES Master Key	X'0128'					x	x
Unrestrict Combine Key Parts	X'027A'	x	x	x	x	x	x
RNX access control point	X'02A2'	x	x	x	x	x	x
Session Key Master	X'02A3'	x	x	x	x	x	x
Session Key Slave	X'02A4'	x	x	x	x	x	x
Import Card Device Certificate	X'02A5'		x	x	x	x	x
Import CA Public Certificate	X'02A6'		x	x	x	x	x
Master Key Extended	X'02A7'	x	x	x	x	x	x
Delete Device Retained Key	X'02A8'		x	x	x	x	x
Export Card Device Certificate	X'02A9'		x	x	x	x	x
Export CA Public Certificate	X'02AA'		x	x	x	x	x
Reset Battery Low Indicator	X'030B'	x	x	x	x	x	x
Open Begin Zone Remote Enroll Process	X'1000'				x	x	x
Open Complete Zone Remote Enroll Process	X'1001'				x	x	x
Open Cryptographic Node Management Utility	X'1002'				x	x	x
Open Smart Card Utility Program	X'1005'				x	x	x
Open Edit TKE Files	X'100D'				x	x	x
Open TKE File Management Utility	X'100E'				x	x	x

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

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 5.2	Enabled in release TKE 5.3, TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0
TKE USER	X'8002'		x	x			

SCTKEUSR

Table 7. ACPs assigned to the SCTKEUSR role

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2	Enabled in release TKE 7.3	Enabled in release TKE 8.0
Required 0047 Change Own Passphrase	X'0047'						x
Required 008E Generate Key	X'008E'	x	x	x	x	x	x
Required 0100 PKA96 Digital Signature Generate	X'0100'	x	x	x	x	x	x
Required 0103 PKA96 Key Generate	X'0103'	x	x	x	x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x	x	x
Required 011F RSA Decipher Clear Key	X'011F'						x
Required 012A Encipher Data Using AES	X'012A'						x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'		x	x	x	x	x
Required 0203 Delete Retained Key	X'0203'			x	x	x	x
Required 027D Permit Regeneration Data	X'027D'						x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'			x	x	x	x
Encipher	X'000E'	x	x	x	x	x	x
Decipher	X'000F'	x	x	x	x	x	x
Reencipher to Master Key	X'0012'	x	x	x	x	x	x
Reencipher from Master Key	X'0013'	x	x	x	x	x	x
Load First Key Part	X'001B'	x	x	x	x	x	x
Combine Key Parts	X'001C'	x	x	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x	x
Generate Key Set	X'008C'	x	x	x	x	x	x
PKA96 Digital Signature Verify	X'0101'	x	x	x	x	x	x
PKA96 Key Import	X'0104'	x	x	x	x	x	x
PKA Clone Key Generate	X'0204'	x	x	x	x	x	x
PKA Clear Key Generate	X'0205'	x	x	x	x	x	x
Load Diffie-Hellman Key mod/gen	X'0250'	x	x	x	x	x	x
Combine Diffie-Hellman Key part	X'0251'	x	x	x	x	x	x
Clear Diffie-Hellman Key values	X'0252'	x	x	x	x	x	x
Unrestrict Combine Key Parts	X'027A'	x	x	x	x	x	x
Import First AES Key Part (min of 2)	X'0298'				x	x	x
Import Last Required AES Key Part	X'029B'				x	x	x
Import Optional AES Key Part	X'029C'				x	x	x
Complete AES Key Import	X'029D'				x	x	x
Process cleartext ICSF key parts	X'02A0'	x	x	x	x	x	x
Process enciphered ICSF key parts	X'02A1'	x	x	x	x	x	x
RNX access control point	X'02A2'	x	x	x	x	x	x
Session Key Master	X'02A3'	x	x	x	x	x	x
Session Key Slave	X'02A4'	x	x	x	x	x	x
Export Card Device Certificate	X'02A9'	x	x	x	x	x	x
OA Proxy Key Generate	X'0344'		x	x	x	x	x

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

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2	Enabled in release TKE 7.3	Enabled in release TKE 8.0
OA Proxy Signature Return	X'0345'		x	x	x	x	x
Open Migrate IBM Host Crypto Module Public Configuration Data	X'1003'			x	x	x	x
Open Configuration Migration Tasks	X'1004'			x	x	x	x
Open Trusted Key Entry	X'1006'			x	x	x	x
Create Domain Group	X'1007'			x	x	x	x
Change Domain Group	X'1008'			x	x	x	x
Delete Domain Group	X'1009'			x	x	x	x
Create Crypto Module Group	X'100A'			x	x	x	x
Change Crypto Module Group	X'100B'			x	x	x	x
Delete Crypto Module Group	X'100C'			x	x	x	x
Open Edit TKE Files	X'100D'			x	x	x	x
Open TKE File Management Utility	X'100E'			x	x	x	x
Manage Host List	X'100F'					x	x
TKE USER	X'8002'	x	x				

DEFAULT role when initialized for use with smart card profiles

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

ACP	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0 to TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0
Required 0047 Change Own Passphrase	X'0047'				x
Required 008E Generate Key	X'008E'	x	x	x	x
Required 0100 PKA96 Digital Signature Generate	X'0100'	x	x	x	x
Required 0103 PKA96 Key Generate	X'0103'	x	x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x
Required 011F RSA Decipher Clear Key	X'011F'	x	x	x	x
Required 012A Encipher Data Using AES	X'012A'				x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'		x	x	x
Required 0203 Delete Retained Key	X'0203'	x	x	x	x
Required 027D Permit Regeneration Data	X'027D'				x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'		x	x	x
Encipher	X'000E'	x	x	x	x
Decipher	X'000F'	x	x	x	x
Generate MAC	X'0010'	x	x	x	x
Verify MAC	X'0011'	x	x	x	x
Reencipher to Master Key	X'0012'	x	x	x	x
Reencipher from Master Key	X'0013'	x	x	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
Load First Key Part	X'001B'	x	x	x	x
Combine Key Parts	X'001C'	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x
Translate Key	X'001F'	x	x	x	x
Generate Random Master Key	X'0020'	x	x	x	x

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

ACP	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0 to TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0
Clear New Master Key Register	X'0032'	x	x	x	x
Clear Old Master Key Register	X'0033'	x	x	x	x
Generate Diversified Key (CLR8-ENC)	X'0040'	x	x	x	x
Generate Diversified Key (TDES-ENC)	X'0041'	x	x	x	x
Generate Diversified Key (TDES-DEC)	X'0042'	x	x	x	x
Generate Diversified Key (SESS-XOR)	X'0043'	x	x	x	x
Enable DKG Single Length Keys and Equal Halves for TDES-ENC, TDES-DEC	X'0044'	x	x	x	x
Load First Asymmetric Master Key Part	X'0053'	x	x	x	x
Combine PKA Master Key Parts	X'0054'	x	x	x	x
Set Asymmetric Master Key	X'0057'	x	x	x	x
Clear New Asymmetric Master Key Buffer	X'0060'	x	x	x	x
Clear Old Asymmetric Master Key Buffer	X'0061'	x	x	x	x
Generate MDC	X'008A'	x	x	x	x
Generate Key Set	X'008C'	x	x	x	x
Reencipher to Current Master Key	X'0090'	x	x	x	x
Generate Clear 3624 PIN	X'00A0'	x	x	x	x
Generate Clear 3624 PIN Offset	X'00A4'	x	x	x	x
Verify Encrypted 3624 PIN	X'00AB'	x	x	x	x
Verify Encrypted German Bank Pool PIN	X'00AC'	x	x	x	x
Verify Encrypted VISA PVV	X'00AD'	x	x	x	x
Verify Encrypted InterBank PIN	X'00AE'	x	x	x	x
Format and Encrypt PIN	X'00AF'	x	x	x	x
Generate Formatted and Encrypted 3624 PIN	X'00B0'	x	x	x	x
Generate Formatted and Encrypted German Bank Pool PIN	X'00B1'	x	x	x	x
Generate Formatted and Encrypted InterBank PIN	X'00B2'	x	x	x	x
Translate PIN with No Format-Control to No Format-Control	X'00B3'	x	x	x	x
Reformat PIN with No Format-Control to No Format-Control	X'00B7'	x	x	x	x
Generate Clear VISA PVV Alternate	X'00BB'	x	x	x	x
Encipher Under Master Key	X'00C3'	x	x	x	x
Lower Export Authority	X'00CD'	x	x	x	x
Translate Control Vector	X'00D6'	x	x	x	x
Generate Key Set Extended	X'00D7'	x	x	x	x
Encipher/Decipher Cryptovariable	X'00DA'	x	x	x	x
Replicate Key	X'00DB'	x	x	x	x
Generate CVV	X'00DF'	x	x	x	x
Verify CVV	X'00E0'	x	x	x	x
Unique Key Per Transaction, ANSI X9.24	X'00E1'	x	x	x	x
Reencipher to Current Master Key2	X'00F1'			x	x
PKA96 Digital Signature Verify	X'0101'	x	x	x	x
PKA96 Key Token Change	X'0102'	x	x	x	x
PKA96 Key Import	X'0104'	x	x	x	x
Symmetric Key Export PKCS-1.2/OAEP	X'0105'	x	x	x	x
Symmetric Key Import PKCS-1.2/OAEP	X'0106'	x	x	x	x
One-Way Hash, SHA-1	X'0107'	x	x	x	x
Data Key Import	X'0109'	x	x	x	x
Data Key Export	X'010A'	x	x	x	x
Compose SET Block	X'010B'	x	x	x	x
Decompose SET Block	X'010C'	x	x	x	x

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

ACP	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0 to TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0
PKA92 Symmetric Key Generate	X'010D'	x	x	x	x
NL-EPP-5 Symmetric Key Generate	X'010E'	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
Force User Logoff	X'011B'	x	x	x	x
Set EID	X'011C'	x	x	x	x
Initialize Master Key Cloning	X'011D'	x	x	x	x
RSA Encipher Clear Key	X'011E'	x	x	x	x
Generate Random Asymmetric Master Key	X'0120'	x	x	x	x
SET PIN Encrypt with IPINENC	X'0121'	x	x	x	x
SET PIN Encrypt with OPINENC	X'0122'	x	x	x	x
Clear AES New Master Key Register	X'0124'			x	x
Load First AES Master Key Part	X'0125'			x	x
Load Middle/Last AES Master Key Parts	X'0126'			x	x
Set AES Master Key	X'0128'			x	x
PKA Register Public Key Hash	X'0200'	x	x	x	x
PKA Public Key Register with Cloning	X'0201'	x	x	x	x
PKA Public Key Register	X'0202'	x	x	x	x
PKA Clone Key Generate	X'0204'	x	x	x	x
PKA Clear Key Generate	X'0205'	x	x	x	x
Clone-info (share) Obtain 1	X'0211'	x	x	x	x
Clone-info (share) Obtain 2	X'0212'	x	x	x	x
Clone-info (share) Obtain 3	X'0213'	x	x	x	x
Clone-info (share) Obtain 4	X'0214'	x	x	x	x
Clone-info (share) Obtain 5	X'0215'	x	x	x	x
Clone-info (share) Obtain 6	X'0216'	x	x	x	x
Clone-info (share) Obtain 7	X'0217'	x	x	x	x
Clone-info (share) Obtain 8	X'0218'	x	x	x	x
Clone-info (share) Obtain 9	X'0219'	x	x	x	x
Clone-info (share) Obtain 10	X'021A'	x	x	x	x
Clone-info (share) Obtain 11	X'021B'	x	x	x	x
Clone-info (share) Obtain 12	X'021C'	x	x	x	x
Clone-info (share) Obtain 13	X'021D'	x	x	x	x
Clone-info (share) Obtain 14	X'021E'	x	x	x	x
Clone-info (share) Obtain 15	X'021F'	x	x	x	x
Clone-info (share) Install 1	X'0221'	x	x	x	x
Clone-info (share) Install 2	X'0222'	x	x	x	x
Clone-info (share) Install 3	X'0223'	x	x	x	x
Clone-info (share) Install 4	X'0224'	x	x	x	x

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

ACP	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0 to TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0
Clone-info (share) Install 5	X'0225'	x	x	x	x
Clone-info (share) Install 6	X'0226'	x	x	x	x
Clone-info (share) Install 7	X'0227'	x	x	x	x
Clone-info (share) Install 8	X'0228'	x	x	x	x
Clone-info (share) Install 9	X'0229'	x	x	x	x
Clone-info (share) Install 10	X'022A'	x	x	x	x
Clone-info (share) Install 11	X'022B'	x	x	x	x
Clone-info (share) Install 12	X'022C'	x	x	x	x
Clone-info (share) Install 13	X'022D'	x	x	x	x
Clone-info (share) Install 14	X'022E'	x	x	x	x
Clone-info (share) Install 15	X'022F'	x	x	x	x
List Retained Key	X'0230'	x	x	x	x
Generate Clear NL-PIN-1 Offset	X'0231'	x	x	x	x
Verify Encrypted NL-PIN-1	X'0232'	x	x	x	x
PKA92 Symmetric Key Import	X'0235'	x	x	x	x
PKA92 Symmetric Key Import with PIN keys	X'0236'	x	x	x	x
ZERO-PAD Symmetric Key Generate	X'023C'	x	x	x	x
ZERO-PAD Symmetric Key Import	X'023D'	x	x	x	x
ZERO-PAD Symmetric Key Export	X'023E'	x	x	x	x
Symmetric Key Generate PKCS-1.2/OAEP	X'023F'	x	x	x	x
Load Diffie-Hellman Key mod/gen	X'0250'	x	x	x	x
Combine Diffie-Hellman Key part	X'0251'	x	x	x	x
Clear Diffie-Hellman Key values	X'0252'	x	x	x	x
Unrestrict Reencipher from Master Key	X'0276'	x	x	x	x
Unrestrict Data Key Export	X'0277'	x	x	x	x
Add Key Part	X'0278'	x	x	x	x
Complete Key Part	X'0279'	x	x	x	x
Unrestrict Combine Key Parts	X'027A'	x	x	x	x
Unrestrict Reencipher to Master Key	X'027B'	x	x	x	x
Unrestrict Data Key Import	X'027C'	x	x	x	x
Generate Diversified Key (DALL with DKYGENKY Key Type)	X'0290'	x	x	x	x
Generate CSC-5, 4 and 3 Values	X'0291'	x	x	x	x
Verify CSC-3 Values	X'0292'	x	x	x	x
Verify CSC-4 Values	X'0293'	x	x	x	x
Verify CSC-5 Values	X'0294'	x	x	x	x
Process cleartext ICSF key parts	X'02A0'	x	x	x	x
Process enciphered ICSF key parts	X'02A1'	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	x
Import CA Public Certificate	X'02A6'	x	x	x	x
Master Key Extended	X'02A7'	x	x	x	x
Delete Device Retained Key	X'02A8'	x	x	x	x
Export Card Device Certificate	X'02A9'	x	x	x	x
Export CA Public Certificate	X'02AA'	x	x	x	x
Reset Battery Low Indicator	X'030B'	x	x	x	x

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

- TKEADM
- TKEUSER
- KEYMAN1
- KEYMAN2
- DEFAULT

TKEADM

Table 9. ACPs assigned to the TKEADM role

TKEADM - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 5.2	Enabled in release TKE 5.3, TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1, TKE 7.2, TKE 7.3	Enabled in release TKE 8.0
Required 0047 Change Own Passphrase	X'0047'					x
Required 008E Generate Key	X'008E'					x
Required 0100 PKA96 Digital Signature Generate	X'0100'			x	x	x
Required 0103 PKA96 Key Generate	X'0103'		x	x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x	x
Required 011F RSA Decipher Clear Key	X'011F'					x
Required 012A Encipher Data Using AES	X'012A'					x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'			x	x	x
Required 0203 Delete Retained Key	X'0203'		x	x	x	x
Required 027D Permit Regeneration Data	X'027D'					x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'			x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x
One-Way Hash, SHA-1	X'0107'	x	x	x	x	x
Reset Intrusion Latch	X'010F'	x	x	x	x	x
Set Clock	X'0110'	x	x	x	x	x
Reinitialize Device	X'0111'	x	x	x	x	x
Initialize Access-Control System	X'0112'	x	x	x	x	x
Change User Profile Expiration Date	X'0113'	x	x	x	x	x
Change User Profile Authentication Data	X'0114'	x	x	x	x	x
Reset User Profile Logon-Attempt-Failure Count	X'0115'	x	x	x	x	x
Delete User Profile	X'0117'	x	x	x	x	x
Delete Role	X'0118'	x	x	x	x	x
Load Function-Control Vector	X'0119'	x	x	x	x	x
Clear Function-Control Vector	X'011A'	x	x	x	x	x
Import Card Device Certificate	X'02A5'		x	x	x	x
Import CA Public Certificate	X'02A6'		x	x	x	x
Delete Device Retained Key	X'02A8'		x	x	x	x
Export Card Device Certificate	X'02A9'		x	x	x	x
Export CA Public Certificate	X'02AA'		x	x	x	x
Reset Battery Low Indicator	X'030B'	x	x	x	x	x
Open Begin Zone Remote Enroll Process	X'1000'				x	x
Open Complete Zone Remote Enroll Process	X'1001'				x	x
Open Cryptographic Node Management Utility	X'1002'				x	x
Open Smart Card Utility Program	X'1005'				x	x
Open Edit TKE Files	X'100D'				x	x
Open TKE File Management Utility	X'100E'				x	x
TKE USER	X'8002'		x	x		

TKEUSER

Table 10. ACPs assigned to the TKEUSER role

TKEUSER - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2	Enabled in release TKE 7.3	Enabled in release TKE 8.0
Required 0047 Change Own Passphrase	X'0047'						x
Required 008E Generate Key	X'008E'	x	x	x	x	x	x
Required 0100 PKA96 Digital Signature Generate	X'0100'	x	x	x	x	x	x
Required 0103 PKA96 Key Generate	X'0103'	x	x	x	x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x	x	x
Required 011F RSA Decipher Clear Key	X'011F'						x
Required 012A Encipher Data Using AES	X'012A'						x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'		x	x	x	x	x
Required 0203 Delete Retained Key	X'0203'			x	x	x	x
Required 027D Permit Regeneration Data	X'027D'						x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'			x	x	x	x
Encipher	X'000E'	x	x	x	x	x	x
Decipher	X'000F'	x	x	x	x	x	x
Reencipher to Master Key	X'0012'	x	x	x	x	x	x
Reencipher from Master Key	X'0013'	x	x	x	x	x	x
Load First Key Part	X'001B'	x	x	x	x	x	x
Combine Key Parts	X'001C'	x	x	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x	x
Generate Key Set	X'008C'	x	x	x	x	x	x
PKA96 Digital Signature Verify	X'0101'	x	x	x	x	x	x
PKA96 Key Import	X'0104'	x	x	x	x	x	x
PKA Clone Key Generate	X'0204'	x	x	x	x	x	x
PKA Clear Key Generate	X'0205'	x	x	x	x	x	x
Load Diffie-Hellman Key mod/gen	X'0250'	x	x	x	x	x	x
Combine Diffie-Hellman Key part	X'0251'	x	x	x	x	x	x
Clear Diffie-Hellman Key values	X'0252'	x	x	x	x	x	x
Unrestrict Combine Key Parts	X'027A'	x	x	x	x	x	x
Import First AES Key Part (min of 2)	X'0298'				x	x	x
Import Last Required AES Key Part	X'029B'				x	x	x
Import Optional AES Key Part	X'029C'				x	x	x
Complete AES Key Import	X'029D'				x	x	x
Process cleartext ICSF key parts	X'02A0'	x	x	x	x	x	x
Process enciphered ICSF key parts	X'02A1'	x	x	x	x	x	x
RNX access control point	X'02A2'	x	x	x	x	x	x
Session Key Master	X'02A3'	x	x	x	x	x	x
Session Key Slave	X'02A4'	x	x	x	x	x	x
Export Card Device Certificate	X'02A9'	x	x	x	x	x	x
OA Proxy Key Generate	X'0344'		x	x	x	x	x
OA Proxy Signature Return	X'0345'		x	x	x	x	x
Open Migrate IBM Host Crypto Module Public Configuration Data	X'1003'			x	x	x	x
Open Configuration Migration Tasks	X'1004'			x	x	x	x
Open Smart Card Utility Program	X'1005'			x	x	x	x
Open Trusted Key Entry	X'1006'			x	x	x	x
Create Domain Group	X'1007'			x	x	x	x

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

TKEUSER - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2	Enabled in release TKE 7.3	Enabled in release TKE 8.0
Change Domain Group	X'1008'			x	x	x	x
Delete Domain Group	X'1009'			x	x	x	x
Create Crypto Module Group	X'100A'			x	x	x	x
Change Crypto Module Group	X'100B'			x	x	x	x
Delete Crypto Module Group	X'100C'			x	x	x	x
Open Edit TKE Files	X'100D'			x	x	x	x
Open TKE File Management Utility	X'100E'			x	x	x	x
Manage Host List	X'100F'					x	x
TKE USER	X'8002'	x	x				

KEYMAN1

Table 11. ACPs assigned to the KEYMAN1 role

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0
Required 0047 Change Own Passphrase	X'0047'					x
Required 008E Generate Key	X'008E'		x	x	x	x
Required 0100 PKA96 Digital Signature Generate	X'0100'		x	x	x	x
Required 0103 PKA96 Key Generate	X'0103'		x	x	x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x	x
Required 011F RSA Decipher Clear Key	X'011F'					x
Required 012A Encipher Data Using AES	X'012A'					x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'		x	x	x	x
Required 0203 Delete Retained Key	X'0203'		x	x	x	x
Required 027D Permit Regeneration Data	X'027D'					x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'		x	x	x	x
Load First Master Key Part	X'0018'	x	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x
Clear New Master Key Register	X'0032'	x	x	x	x	x
Clear AES New Master Key Register	X'0124'				x	x
Load First AES Master Key Part	X'0125'				x	x
Open Cryptographic Node Management Utility	X'1002'			x	x	x

KEYMAN2

Table 12. ACPs assigned to the KEYMAN2 role

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

Table 12. ACPs assigned to the KEYMAN2 role (continued)

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0	Enabled in release TKE 7.1	Enabled in release TKE 7.2, TKE 7.3	Enabled in release TKE 8.0
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x	x	x
Required 011F RSA Decipher Clear Key	X'011F'					x
Required 012A Encipher Data Using AES	X'012A'					x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'		x	x	x	x
Required 0203 Delete Retained Key	X'0203'		x	x	x	x
Required 027D Permit Regeneration Data	X'027D'					x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'		x	x	x	x
Combine Master Key Parts	X'0019'	x	x	x	x	x
Set Master Key	X'001A'	x	x	x	x	x
Compute Verification Pattern	X'001D'	x	x	x	x	x
Reencipher to Current Master Key	X'0090'	x	x	x	x	x
Reencipher to Current Master Key2	X'00F1'				x	x
PKA96 Key Token Change	X'0102'	x	x	x	x	x
Load Middle/Last AES Master Key Parts	X'0126'				x	x
Set AES Master Key	X'0128'				x	x
Open Cryptographic Node Management Utility	X'1002'			x	x	x

DEFAULT role when initialized for use with passphrase profiles

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

ACP - Current description	Numeric value	Enabled in release TKE 5.0 to TKE 6.0	Enabled in release TKE 7.0, TKE 7.1, TKE 7.2, TKE 7.3	Enabled in release TKE 8.0
Required 0047 Change Own Passphrase	X'0047'			x
Required 008E Generate Key	X'008E'			x
Required 0100 PKA96 Digital Signature Generate	X'0100'		x	x
Required 0103 PKA96 Key Generate	X'0103'		x	x
Required 0116 Read Public Access-Control Information	X'0116'	x	x	x
Required 011F RSA Decipher Clear Key	X'011F'			x
Required 012A Encipher Data Using AES	X'012A'			x
Required 012B Symmetric Algorithm Decipher - secure AES keys	X'012B'		x	x
Required 0203 Delete Retained Key	X'0203'		x	x
Required 027D Permit Regeneration Data	X'027D'			x
Required 027E Permit Regeneration Data For Retained Keys	X'027E'		x	x
Compute Verification Pattern	X'001D'	x	x	x
Reinitialize Device	X'0111'	x	x	x
Export Card Device Certificate	X'02A9'	x	x	x

Chapter 2. Using smart cards with TKE

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

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

Terminology

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

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

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

CNM Cryptographic Node Management utility. This utility is a Java™ application that provides a graphical user interface to initialize and manage the TKE workstation crypto adapter. See Chapter 11, “Cryptographic Node Management utility (CNM),” on page 237.

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

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

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

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

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

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

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

SCUP Smart Card Utility Program. Performs maintenance operations, such as the creation/initialization and personalization of CA, TKE, and EP11 smart cards and zone enrollment of the TKE workstation crypto adapter. See Chapter 12, "Smart Card Utility Program (SCUP)," on page 279.

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

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

Zone A security concept ensuring that only members of the same zone can exchange key parts. A zone is established by a CA smart card. See "Zone creation" on page 39.

Preparation and planning

Before beginning a smart card implementation, consider these questions:

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

Using the OmniKey smart card reader

TKE 7.1 and later requires Omnikey smart card readers.

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

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

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

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

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

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

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

The other buttons on the PIN pad are not operational.

Smart card compatibility issues

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

Applet version

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

Table 14. Applet version by TKE release

	CA smart card	**TKE smart card**	**EP11 smart card**	**Smart card part**
TKE 5.2 or earlier	applet version = 0.3	applet version = 0.3	Not supported	Any supported card
TKE 5.3	applet version = 0.3	applet version = 0.4	Not supported	Any supported card
TKE 6.0	applet version = 0.4	applet version = 0.5	Not supported	Any supported card
TKE 7.0	applet version = 0.4	applet version = 0.6	Not supported	Any supported card
TKE 7.1	applet version = 0.4	applet version = 0.7	Not supported	Any supported card

Table 14. Applet version by TKE release (continued)

	CA smart card	TKE smart card	EP11 smart card	Smart card part
TKE 7.2	applet version = 0.4	applet version = 0.8	Not supported	45D3398
TKE 7.2	applet version = 0.4	applet version = 0.8	applet version = 0.1	74Y0551
TKE 7.3	applet version = 0.4	applet version = 0.8	Not supported	45D3398
TKE 7.3	applet version = 0.5	applet version = 0.9	applet version = 0.2	74Y0551
TKE 8.0	applet version = 0.4	applet version = 0.8	Not supported	45D3398
TKE 8.0	applet version = 0.5	applet version = 0.10	applet version = 0.2	74Y0551
TKE 8.0	applet version = 0.5	applet version = 0.10	applet version = 0.2	00JA710

Table 15. Applet version by TKE release

	MCA smart card	IA smart card	KPH smart card	Smart card part
TKE 7.0 to TKE 7.2	applet version = 0.1	applet version = 0.1	applet version = 0.1	Any supported card
TKE 7.3	applet version = 0.1	applet version = 0.1	applet version = 0.1	45D3398
TKE 7.3	applet version = 0.2	applet version = 0.2	applet version = 0.2	74Y0551
TKE 8.0	applet version = 0.1	Not supported	Not supported	45D3398
TKE 8.0	applet version = 0.2	applet version = 0.3	applet version = 0.3	74Y0551
TKE 8.0	applet version = 0.2	applet version = 0.3	applet version = 0.3	00JA710

In general, smart cards that are created on a particular TKE release cannot be used on TKE workstations that are at prior release levels. TKE 5.2 applets are not usable on TKE 7.1 and later because they can only be installed on DataKey smart cards, and DataKey smart cards are not supported.

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 or EP11 smart cards created in the zone and any TKE workstations enrolled in the zone. Key lengths of 1024-bits and 2048-bits are allowed. You are allowed to create EP11 smart cards only when the zone key length is 2048-bits

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

Table 16 on page 37 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 16. CA smart card usage

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

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

Table 17 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 17. TKE smart card usage

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

[1] This smart card could contain:

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

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

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

When creating a TKE or EP11 smart card on TKE 8.0, you must use a smart card associated with part numbers 74Y0551 or 00JA710.

Datakey card usage

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

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

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

Zone concepts

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

These are members of a zone:
- CA smart card
- TKE workstation crypto adapter
- TKE smart cards
- EP11 smart cards

A member of a zone is referred to as an entity. Entities 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, EP11 smart card, or a TKE workstation crypto adapter), the entity inherits the zone description from the CA smart card performing the enrollment. Similarly, when you backup a CA smart card, the zone description will be the same for both cards.

Zone identifier (ID)

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

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

Multiple zones

It may be desirable to 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.

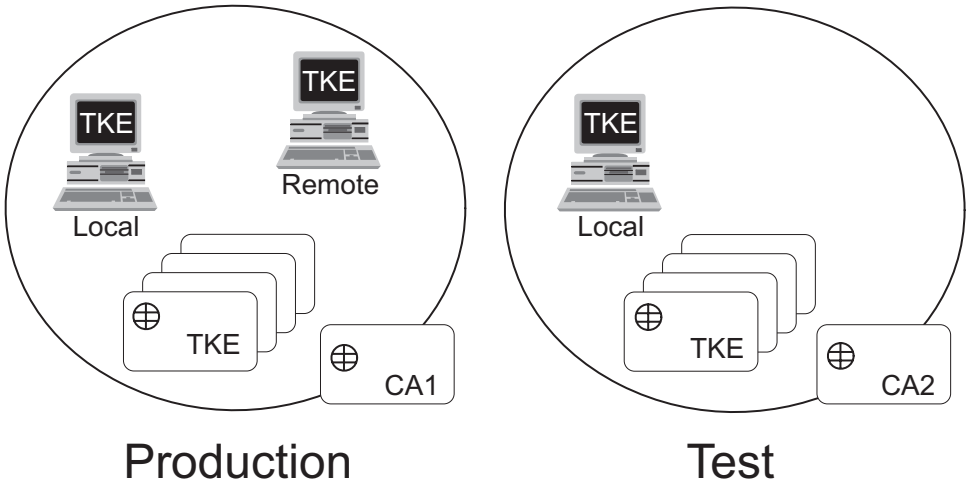


Figure 6. Multiple zones

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
- EP11 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 support CCA host crypto modules. They can hold:

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

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

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

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

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

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

EP11 smart cards

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

- A maximum of 50 key parts. These can be:
  - ICSF P11 master key parts
  - TKE workstation crypto adapter master key parts

- One TKE crypto adapter logon key. This is a 2048-bit RSA key.
- One administrator signature key. This is a 320-bit Brainpool ECC key.

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

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

Steps to set up a smart card installation

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

Notes:

1. This setup is done in conjunction with Table 19 on page 61. 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 18. Smart card task checklist

Task	Person responsible	Where	Completed
1. Attach the smart card readers	IBM CE	TKE workstation	
2. Initialize the TKE workstation crypto adapter for smart card use; see “Initializing the TKE workstation crypto adapter for use with smart card profiles” on page 77.	TKE Administrator	TKE workstation	
3. Create CA smart card (zone); see “Initialize and personalize the CA smart card” on page 284.	TKE Administrator	TKE workstation	
4. Backup the CA smart card; see “Back up a CA smart card” on page 287.	TKE Administrator	TKE workstation	
5. Initialize and enroll TKE smart cards into the zone; see “Initialize and enroll a TKE smart card” on page 289.	TKE Administrator	TKE workstation	
6. Personalize TKE smart cards; see “Personalize a TKE smart card” on page 291.	TKE Administrator	TKE workstation	

Table 18. Smart card task checklist (continued)

Task	Person responsible	Where	Completed
7. Enroll the local TKE workstation crypto adapter (and any remote TKE workstation crypto adapters) in the zone; see "Enroll a TKE cryptographic adapter" on page 294.	TKE Administrator	TKE workstation	
8. CNM utility - generate TKE workstation crypto adapter logon keys; define and load profiles; reset default role. see Chapter 11, "Cryptographic Node Management utility (CNM)," on page 237.	TKE Administrator	TKE workstation	

Chapter 3. TKE migration and recovery installation

Notes:

- In general, you should not need to install TKE code on your workstation. If you must do an installation, see the instructions in "Recovery installation" on page 59.
- If you are going to perform an install, you must be able to boot the TKE from the IBM-supplied installation DVD.

  Beginning with TKE hardware feature 0847, the TKE workstation includes Unified Extensible Firmware Interface (UEFI) code that contains enhanced security settings for bootable media. In addition, some older TKEs may have updated their workstation UEFI code to the same level. The UEFI enhanced security settings are initially configured to only allow the TKE to boot from the workstation's hard drive.

  If your TKE workstation has the UEFI code with the enhanced security feature, you may have to change the UEFI settings to allow the TKE to boot CD/DVD ROM. If necessary, refer to *zEnterprise System Service Guide for Trusted Key Entry Workstations*, GC28-6901, or your MES Installation Instructions for complete details on how to change your UEFI settings to allow your TKE to boot from a CD/DVD ROM.

Using files from a TKEDATA DVD-RAM on a TKE 7.2 or later system

Important

DVD-RAM is not supported on TKE 7.2 or later systems, and file migration may be required.

End of information

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

- Copy the files from the TKEDATA DVD-RAM to the TKE's hard drive before upgrading the TKE to version 7.2 or later. For additional information, see "Copying files to the TKE 7.0 or TKE 7.1 hard drive."
- Copy the files from the TKEDATA DVD-RAM to a USB flash memory drive that is formatted for TKEDATA from a TKE 7.0 or TKE 7.1 system. For additional information, see "Copying files to a USB flash memory drive while on a TKE 7.0 or TKE 7.1 system" on page 47.

Copying files to the TKE 7.0 or TKE 7.1 hard drive

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

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

2. Perform the following setup steps for the source DVD-RAM:
   a. Insert the TKEDATA DVD-RAM into the DVD drive.
   b. Open the TKE Media Manager utility.

      Note: The TKE Media Manager is in the Utilities list on the Trusted Key Entry window pane.
   c. Select “Activate read only CD/DVD inserted in DVD drive” and press OK.

      Note: When complete, the “DVD Drive Status” will be “Active (Read Only)”.
   d. Press Cancel to close the TKE Media Manager.
   e. Press OK to close the informational warning message. Remember, the DVD drawer will not open until the DVD drive is deactivated.
3. Perform the following steps to copy the files from the DVD-RAM to the TKE 7.0 or TKE 7.1 hard drive:
   a. Open the TKE File Management Utility.

      Note: The TKE File Management Utility is in the Utilities list on the Trusted Key Entry window.
   b. On the left side of the File Management Utility window, select the CD/DVD Drive radio button.
   c. On the right side of the File Management Utility window, select the Local Hard Drive radio button.
   d. Select the files from the CD/DVD Drive file list and use the “Copy ->” button to copy files from the CD/DVD Drive to the local hard drive.

      Note: In general, you should store each file from the TKEDATA DVD-RAM into the directory that the file originally came from. General information about the three most common types of files that are saved on TKEDATA DVD-RAM include:
      - Key part files should be stored in the TKE Data Directory.
      - Profile and role definition files should be stored in the CNM Directory.
      - Data from either of the host migration wizards should be stored in the Configuration Data Directory.

      Note: Once the files are saved on the TKE 7.0 or TKE 7.1 system, the files will be included in the data that is saved and applied when the TKE system is upgraded to TKE 7.2 or later.
4. Perform the following clean up steps:
   a. Close the File Management Utility by selecting either "Exit" or "Exit and logoff" to close the TKE application window.
   b. Open the TKE Media Manager utility.

      Note: The TKE Media Manager is in the Utilities list on the Trusted Key Entry window pane.
   c. Select “Deactivate media inserted into DVD drive” and press OK. When complete, the “DVD Drive Status” will be “Deactivated”.
   d. Remove the TKEDATA DVD-RAM from the DVD drive.

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

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

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

      Note: The TKE Media Manager is in the Utilities list on the Trusted Key Entry window pane.
   c. Select "Activate read only CD/DVD inserted in DVD drive" and press OK.

      Note: When complete, the "DVD Drive Status" will be "Active (Read Only)".
   d. Press Cancel to close the TKE Media Manager.
   e. Press OK to close the informational warning message. Remember, the DVD drawer will not open until the DVD drive is deactivated.
3. Perform the following setup steps for the new USB flash memory removable media:
   a. Insert the USB flash memory drive into any open USB port on the TKE 7.0 or TKE 7.1 workstation and wait for the "USB Device Status" message to appear.

      Note:
      - It can take up to 1 minute for the message to appear.
      - You can press OK to close the "USB Device Status" message or wait for it to close in 10 seconds.
   b. Perform the following steps only if you want to format the USB flash memory drive. Proceed to Step 4 on page 48 if you do not want to format the USB flash memory drive.

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

      You can use a USB flash memory drive that was formatted for TKEDATA on a TKE 7.2 or later system. To format the USB flash memory drive:
      1) From the Trusted Key Entry Console on your TKE 7.0 or TKE 7.1 system, open the Service Management window pane.
      2) Open the Format Media application.
      3) Select the "Trusted Key Entry Data" radio button and press the FORMAT button.
      4) Select the radio button for the USB flash memory drive device you want to format and press OK.
      5) You might receive the "file system setting" window before the confirm format message. If you do, take the default setting and press the FORMAT button.

6) Press YES to confirm you want to format the media.
7) Press OK to close the completion message.

4. Perform the following steps to copy the files from the TKEDATA DVD-RAM to the USB flash memory drive:
   a. From the Trusted Key Entry Console on your TKE 7.0 or TKE 7.1 system, open the Trusted Key Entry window pane.
   b. Open the TKE File Management Utility.

      Note: The TKE File Management Utility is in the Utilities list on the Trusted Key Entry window.
   c. On the left side of the File Management Utility window, select the CD/DVD Drive radio button.
   d. On the right side of the File Management Utility window, select the USB Flash Memory Drive radio button.
   e. Select the files from the CD/DVD Drive file list and use the “Copy ->” button to copy files from the CD/DVD Drive to the USB flash memory drive.

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

      Note: After all the files are stored on the USB flash memory drive:
      - The USB flash memory drive can be used as removable media on any TKE 7.0 or later system.
      - You may remove the USB flash memory drive at any time.
5. Perform the following clean up steps:
   a. Close the File Management Utility by selecting either "Exit" or "Exit and logoff" to close the TKE application window.
   b. Open the TKE Media Manager utility.

      Note: The TKE Media Manager is in the Utilities list on the Trusted Key Entry window pane.
   c. Select “Deactivate media inserted into DVD drive” and press OK. When complete, the “DVD Drive Status” will be “Deactivated”.
   d. Remove the TKEDATA DVD-RAM from the DVD drive.

General migration information

This information describes how to migrate your customer data from one version of TKE to another. In some cases, you might want to move your current workstation to a new level of TKE. For example, a TKE workstation with TKE 7.0 can be upgraded to TKE 7.3 without changing the workstation. In other situations, you might 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 that requires a new workstation.

Regardless of the situation, the migration requirements are similar. For existing TKE workstations that are upgraded to new release levels of TKE, you want to preserve the customer data and make it available after the upgrade process is

complete. When you move to a new TKE workstation, you want to collect the customer data from a source TKE workstation and make it available on the new TKE workstation.

Customer data includes:

- Network and time settings for the workstation
- Data that are found in the following TKE directories (Not all directories appear in all 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 workstation crypto adapter

The steps necessary for migrating customer 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 topics describe the migration impacts based on the source and target TKE release level and whether a new TKE workstation is involved.

- "Upgrading an existing TKE workstation to TKE 8.0"
- "Migrating TKE Version 5.*x*, 6.0, 7.*x* to a new workstation at TKE 8.0" on page 50

Upgrading an existing TKE workstation to TKE 8.0

Existing TKE workstations can be upgraded only as follows:

- TKE workstations that use the 4764 as their workstation crypto adapter can be upgraded only to a maximum level of TKE 6.0.
- TKE workstations that use the 4765 as their workstation crypto adapter require a minimum level of TKE 7.0.
- TKE workstations that use the 4767 as their workstation crypto adapter require a minimum level of TKE 8.0.

Only the TKE workstation associated with feature code 0842 can be upgraded to TKE 8.0. This upgrade requires the purchase of the 4767 workstation crypto adapter. When you upgrade an existing workstation to TKE 8.0, TKE firmware is updated on the existing TKE workstation. The firmware upgrade is done by an IBM Customer Engineer (CE). The following steps are an overview of the process:

1. Before the CE starts the firmware upgrade, the CE collects customer data on the workstation by using the Save Upgrade Data utility. The data is placed on a USB flash memory drive.

   Note: The steps that are used to collect this data are similar to the steps described in "Step 1: Collecting data from the source TKE workstation" on page 52.
2. The CE powers down the TKE and replaces the 4765 crypto adapter with the 4767 if necessary.

   Note:

- Only the TKE workstation feature 0842 can be upgraded to TKE 8.0.
- When the 4765 crypto adapter is replaced with the 4767, the workstations feature code changes to 0847.
- Code is not placed on the 4767 until the TKE Workstation Setup wizard is run. Therefore, the crypto adapter can be replaced before or after the CE preforms steps 3 or 4.

3. The CE installs the new TKE firmware on the TKE workstation by running an Install/Recovery installation.
4. The CE reapplies the customer data to the TKE workstation by running a Frame Roll installation. The USB flash memory drive with the saved customer data is used during this install.
5. The CE runs the TKE Workstation Setup wizard to complete the workstation setup process. The wizard includes a step for updating the code on the TKE workstation's local crypto adapter.

Note: The steps that are used to do the code installation, frame roll installation, and final workstation setup are similar to the steps described in "Recovery installation" on page 59.

You can run the TKE Workstation Setup wizard at any time to verify that the TKE workstation is set up correctly. For more information, see "Running the TKE Workstation Setup wizard" on page 69.

Note: The TKE Workstation Setup wizard is only available when you are signed on with the ADMIN privileged access mode profile.

Migrating TKE Version 5.*x*, 6.0, 7.*x* to a new workstation at TKE 8.0

In this case, you have a new TKE 8.0 workstation (the target) with a new crypto adapter that is up and running, and an old TKE workstation (the source) at a lower level. The goal is to copy customer data from the source TKE workstation to the target TKE workstation. Customer data includes data on the TKE hard disk, TKE settings, and data and settings from the TKE workstation local crypto adapter.

Note: Customer data on the TKE workstation crypto adapter includes roles, profiles, TKE zone enrollment, certificates that are used for the host crypto module migration utility, and some adapter settings. Most of this data cannot be collected and moved. However, files can be created that help to move the roles and profiles to the target system. Beginning in TKE 7.3, the TKE Workstation Setup wizard steps you through the process of reloading data onto your new TKE workstation crypto adapter.

Overview of the migration process

This topic provides an overview of the process of migrating data from an old workstation at TKE version 5.*x*, 6.0, or 7.*x* (the source workstation) to a new workstation at TKE version 8.0 (the target workstation).

There are three main steps in the process of migrating data from an old workstation at TKE version 5.*x*, 6.0, or 7.*x* to a new workstation at TKE version 8.0.

Step 1 overview: On the source TKE workstation, collect customer data

- If you have customer-defined roles or profiles on your TKE local crypto adapter, there are some files that you can create that help simplify the process of loading

the roles and profiles on your target TKE. The processes available for creating the files depend on the TKE release level of the source workstation:

  – For TKE level 7.3 or later, use the TKE Workstation Setup wizard to create a file that contains the information that is needed to load all customer-defined roles and profiles on the target TKE workstation. The file is included in the data that is collected during the save upgrade data process.

    For a detailed description of this step, see "Option 1: Using the TKE Workstation Setup wizard to collect data about roles and profiles" on page 53.

  – For TKE at any level, you can use the Cryptographic Node Management (CNM) utility. From CNM, individual role and profile definition files are created for each customer-defined role and profile you are migrating to the new TKE workstation. Each file can be used to load the role or profile on the target TKE workstation. The files are included in the data that is collected during the save upgrade data process.

    For a detailed description of this step, see "Option 2: Using the Cryptographic Node Management (CNM) utility to collect data about roles and profiles" on page 54.

- Use the Save Upgrade Data utility to copy the source workstation's customer data and system settings to USB flash memory in a form that can be applied to the target workstation.

For a detailed description of this step, see "Step 1: Collecting data from the source TKE workstation" on page 52.

Step 2 overview: On the target TKE workstation, perform a frame roll installation

The frame roll installation is a technique for restoring the information gathered by the Save Upgrade utility onto the target TKE workstation. It does not reinstall the workstation code.

For a detailed description of this step, see "Step 2 - Performing a frame roll installation" on page 55

Step 3 overview: On the target TKE workstation, complete the workstation setup

Run the TKE Workstation Setup wizard to verify and complete any tasks that are needed to configure your workstation. In some cases, you only have to run the wizard to complete your setup. In some cases, you also have to manually load customer-defined profiles and roles onto the TKE workstation's local crypto adapter.

- Final configuration - single step

  You can complete the final configuration in one step if one of the following conditions is true:

  – The file that is created by the TKE Workstation Setup wizard task Save User Roles and Profiles is on the target TKE workstation.

  – There are no customer-defined roles and profiles to be moved to the target TKE workstation.

  In these cases, the only step is to run the TKE Workstation Setup wizard.

  For a detailed description of this option, see "Option 1: Using the single-step method to complete workstation setup" on page 57.

- Final configuration - multiple steps

The final workstation configuration takes three steps when customer-defined roles and profiles must be loaded onto the TKE local crypto adapter using individual role and profile definition files. The three steps that are required are:

- Run the TKE Workstation Setup wizard to perform all the setup steps for the workstation except loading the customer-defined roles and profiles.
- Manually load the customer-defined roles and profiles onto the TKE workstation's local crypto adapter.
- Reduce the power of the DEFAULT role, if necessary.

  When an adapter is initialized for use with smart card profiles, the DEFAULT role is powerful. When the workstation setup process is complete, you should load the DEFAULT role from the IBM-supplied role definition files that are used to create the DEFAULT role when the TKE local adapter is initialized for use with passphrase profiles. The TKE Workstation Setup wizard task Load IBM-Supplied DEFAULT Role runs a test, makes a suggestion, and allows you to load the less powerful DEFAULT role from the appropriate IBM-supplied file.

For a detailed description of this option, see "Option 2: Using the multiple-step method to complete workstation setup" on page 57

For a detailed description of this step, see "Step 3 - Completing the workstation setup" on page 56.

Step 1: Collecting data from the source TKE workstation

This step is the first step in migrating customer data from a source TKE workstation to a target TKE workstation.

Procedure

Create files that contain the data that is needed to load customer-defined roles and profiles from the source TKE workstation's local adapter to the target TKE workstation.

1. If you already have files for loading customer-defined roles and profiles, skip to step 3
2. Use either the TKE Workstation Setup wizard or the Cryptographic Node Management (CNM) utility to create the files.
   - Option 1: If the source TKE workstation is at TKE level 7.3 or later, you can use the TKE Workstation Setup wizard. For instructions, see "Option 1: Using the TKE Workstation Setup wizard to collect data about roles and profiles" on page 53
   - Option 2: For any level of TKE, you can use the Cryptographic Node Management (CNM) utility to create the files. For instructions, see "Option 2: Using the Cryptographic Node Management (CNM) utility to collect data about roles and profiles" on page 54

Format the USB flash memory drive to hold save upgrade data.

3. If you already have a formatted USB flash memory drive, install it into your source TKE workstation and skip to step 15 on page 53.
4. Install the USB flash memory drive into any open USB port and wait for the device to report in. The wait can take up to 30 seconds.

Note: If the source workstation is a TKE 6.0 workstation, format the USB flash memory drive on the target TKE 7.0 or later system. Move the flash memory drive to the source TKE 6.0 workstation when the format operation is complete.

5. From the Trusted Key Entry Console select **Service Management**.
6. Open the **Format Media** application.
7. Click **Upgrade data**.
8. Click **Format**.
9. Select your USB flash memory device.
10. Click **OK** to start the format process.
11. Click **Format**. Do not change the file system format.
12. Click **Yes** to allow the media to be overwritten.
13. Click **OK** to close the completion message.
14. If the source workstation is a TKE 6.0 system, move the formatted USB flash memory drive from the target TKE 7.0 or later workstation to the source workstation.

Perform the save upgrade data operation on the source TKE workstation.

Notes:

- Starting in TKE 7.0 save upgrade data can be saved to and read from only the TKE workstation hard drive or USB flash memory
- Starting in TKE 6.0, you can put save upgrade data only onto USB flash memory. You cannot put save upgrade data onto USB flash memory on TKE 5.*x*. One option is to upgrade your TKE 5.*x* to TKE 6.0. If you cannot upgrade your TKE 5.*x* system, you must manually reconfigure the new TKE 7.0 or later system.

15. Close all windows except the pre-login window. The pre-login window has the title Welcome to the Trusted Key Entry Console.
16. Select **Privileged Mode Access**.
17. Enter either `admin` or `service` for the user ID
18. Enter the password. The default password for the admin ID is `password`. The default password for the service ID is `servmode`.
19. From the Trusted Key Entry Console window, select **Service Management**.
20. Open the Save Upgrade Data application.
21. Select **Save to USB Flash memory drive**.
22. Click **OK** to start the save process. A message window opens with a completion message when the save process is complete.
23. Click **OK** to close the message window.

Results

You have completed step 1 in the migration. All customer data from the source TKE workstation is saved to the USB flash memory drive. Continue to step 2. For instructions, see “Step 2 - Performing a frame roll installation” on page 55.

Option 1: Using the TKE Workstation Setup wizard to collect data about roles and profiles

Beginning with TKE level 7.3, you can use the TKE Workstation Setup wizard to create a file that contains the information necessary to load all the customer-defined roles and profiles from a source TKE workstation to a target TKE

workstation. Beginning with TKE 8.0, you can use a new feature in the Cryptographic Node Management (CNM) Utility to create the file that contains the customer-defined roles and profiles information without going through the wizard.

Procedure for TKE 8.0 using the cryptographic node management utility: Procedure

1. On the source TKE workstation, from the Trusted Key Entry Console, select Trusted Key Entry.
2. Open the Cryptographic Node Management utility.
3. Sign on to the crypto adapter if you are prompted to do so.
4. Select **Access Control** and then **Save User Roles and Profiles.**
   - If a file already exists, you are asked whether it can be overwritten.
   - You are told if there are no customer-defined roles and profiles on your system.
5. Click **OK** to close the informational message that tells you how many items were saved.

Procedure for TKE 7.3 or later using the TKE workstation setup wizard: Procedure

1. On the source TKE workstation, close all windows except the pre-logon screen. The pre-logon screen has the title Welcome to the Trusted Key Entry Console.
2. Select **Privileged Mode access**.
3. Enter `admin` for the user ID.
4. Enter the password. The default password for the admin user ID is `password`.
5. From the Trusted Key Entry Console, select **Trusted Key Entry**.
6. Open the TKE Workstation Setup wizard.
7. Click **Next** as many times as necessary to skip to the Save User Roles and Profiles task.
8. Select **Yes**.
9. Click **Next** to perform the save.
   - If a file already exists, you are asked whether it can be overwritten.
   - You are told if there are no customer-defined roles and profiles on your system.
10. Click **Finish** to exit the wizard.

Results

If there are customer-defined roles and profiles on your source workstation, the wizard has created a file on the source workstation that contains the information necessary to load the roles and profiles onto the target TKE workstation. Continue to step 3 on page 52.

Option 2: Using the Cryptographic Node Management (CNM) utility to collect data about roles and profiles

The Cryptographic Node Management (CNM) utility can create individual role and profile definition files for each customer-defined role and profile on the source TKE workstation. The files contain information required to load the roles and profiles onto the target workstation. You can use the CNM utility on any release of TKE.
Note: This is an older method and should only be used if you are not on TKE 7.3 or later yet.

Procedure

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

Results

You have created individual role and profile definition files for each customer-defined role and profile on the source TKE workstation. Continue to step 3 on page 52.

Step 2 - Performing a frame roll installation

This topic describes how to do a frame roll installation. The frame roll installation applies customer data and system settings from a USB flash memory drive to a TKE workstation. This task is the second step in the process of migrating customer data from a source TKE workstation to a target TKE workstation.

About this task

Before you begin, you must have the following things:

- A USB flash memory drive containing the save upgrade data from the source TKE workstation. You collected the data and saved it on the USB flash memory drive in the task "Step 1: Collecting data from the source TKE workstation" on page 52. You can insert the drive in the TKE workstation before you begin this task, or wait until step 5a
- The TKE installation DVD for the target TKE workstation.

Procedure

1. Insert the TKE installation DVD into the DVD drive on the target TKE workstation.
2. Restart the TKE workstation:
   a. Select **Service Management**.
   b. Select **Shutdown or Restart**.
   c. Select **Restart Console**.
   d. Click **OK**. A Confirm Shutdown or Restart window opens.
   e. Click **Yes**.

   The workstation restarts. It can take over seven minutes for it to restart.
3. On the Trusted Key Entry: Upgrade / Install Recovery / Frame roll window, enter 3 to select frame roll and click **Enter**.
4. Enter 1 and click **Enter** to start the frame roll installation. The DVD drive opens and you see a message window with `OPERATION SUCCESSFUL` at the top.
5. Follow the instructions in the message window:
   a. Insert the USB flash memory drive that contains the save upgrade data, if it has not already been inserted.
   b. Remove the TKE installation DVD from the DVD drive. You can manually close the drawer or let it close automatically in the next step.
   c. Click **Enter** to restart the TKE workstation.

   The TKE workstation restarts several times. It can take over ten minutes to complete the restarts. When the frame roll installation is complete, the TKE: Trusted Key Entry Console Workplace window opens.

Results

You have completed step 2 of the migration. The customer data on the USB flash drive memory has been applied to the target TKE workstation. Continue to step 3 to complete the workstation setup.

Step 3 - Completing the workstation setup

This task is the last step in the process of migrating customer data from a source TKE workstation to a target TKE workstation.

About this task

After you collect the customer data from the source TKE workstation, and perform the frame roll installation to apply that data to the target TKE workstation, you have two options for completing the setup of the target TKE workstation:

- Option 1: The single-step method.

  You can use this method if one of the following conditions is true:

  – There are no customer-defined roles and profiles to be moved to the target TKE workstation.

– You used the TKE Workstation Setup wizard task Save User Roles and Profiles, and you put the file that it created onto the target TKE workstation.

For a description of the single-step method, see"Option 1: Using the single-step method to complete workstation setup."

- Option 2: The multiple-step method. Use this method if you cannot use the single-step method. For a description of the multiple-step method, see"Option 2: Using the multiple-step method to complete workstation setup."

Option 1: Using the single-step method to complete workstation setup

About this task

This task completes the workstation setup in a single pass through the TKE Workstation Setup wizard.

Procedure

1. Close all windows except the pre-logon window. The pre-logon window has the title Welcome to the Trusted Key Entry Console.
2. Select **Privileged Mode Access**.
3. Enter `admin` for the user ID.
4. Enter the password. The default password for the admin user ID is `password`.
5. From the Trusted Key Entry Console, select **Trusted Key Entry**.
6. Open the TKE Workstation Setup wizard.
7. Take all appropriate actions as instructed by the wizard.
8. Click **Finish** to exit the wizard.

Results

The final setup of the target TKE workstation is complete. You have migrated all of your customer data from the source TKE workstation to the target TKE workstation.

Option 2: Using the multiple-step method to complete workstation setup

This task completes the workstation setup in three steps.

Procedure

Run the TKE Workstation Setup wizard to perform all setup steps except loading of customer-defined roles and profiles.

1. Close all windows except the pre-logon window. The pre-logon window has the title Welcome to the Trusted Key Entry Console.
2. Select **Privileged Mode Access**
3. Enter `admin` for the user ID.
4. Enter the password. The default password for the admin user ID is `password`.
5. From the Trusted Key Entry Console, select **Trusted Key Entry**.
6. Open the TKE Workstation Setup wizard.
7. Take all appropriate actions as instructed by the wizard.
8. Click **Finish** to exit the wizard.

Manually load the customer-defined roles and profiles into the TKE workstation's local crypto adapter.

9. Open the Cryptographic Node Management utility. Log on if you are prompted to do so.
10. If you do not have customer-defined roles to load, skip to step 14
11. Click **Access Controls > Roles**.
12. Follow these steps for each role:
    a. Click **Open**.
    b. Select the role definition file for the customer-defined role to be loaded.
    c. Click **Open** to open the file.
    d. Click **Load** to load the role onto the crypto adapter.
    e. Click **OK** to close the successful completion message.
13. Click **Done** after the last customer-defined role is loaded.
14. If you do not have customer-defined profiles to load, skip to step 18.
15. Click **Access Controls > Profiles**.
16. Follow these steps for each profile:
    a. Click **Open**.
    b. Select the profile definition file for the customer-defined profile to be loaded.
    c. Click **Open** to open the file.
    d. For passphrase profiles, you must enter the password that will be used on the target TKE workstation. The password does not have to match the password that the profile had when the definition file was created.
    e. Click **Load** to load the role onto the crypto adapter.
    f. Click **OK** to close the successful completion message.
17. Click **Done** after the last customer-defined profile is loaded.
18. Click **File > Exit**.

Reduce the power of the DEFAULT role, if necessary.

19. From the Trusted Key Entry Console, select **Trusted Key Entry**.
20. Open the TKE Workstation Setup wizard.
21. Skip through all the wizard tasks until you get to the "Load IBM-Supplied DEFAULT Role" task.
22. Process the task and exit.
    - If the wizard suggests loading the role:
      a. Click **Next** to reload the role.
      b. Click **OK** to close the success message.
      c. Click **Finish** to exit the wizard.
    - If the wizard states that no action is required, click **Finish** to exit the wizard.
    - If the wizard states that the workstation is not in a state in which the role should be reloaded, note the action that you have to take and click **Finish** to exit the wizard.

Results

The final setup of the target TKE workstation is complete. You have migrated all of your customer data from the source TKE workstation to the target TKE workstation.

Recovery installation

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

Before you begin

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

About this task

There are four parts to this task:

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

Procedure

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

1. Follow the instructions in "Step 1: Collecting data from the source TKE workstation" on page 52.
2. You can install the USB flash memory with the save upgrade data onto your TKE workstation at this time or wait until step 10a on page 60.

Perform the TKE workstation code update.

3. Insert the TKE installation DVD into the DVD drive on the TKE workstation.
4. Restart the TKE workstation:
   a. Select **Service Management**.
   b. Select **Shutdown or Restart**.
   c. Select **Restart Console**.
   d. Click **OK**.
   e. Click **Yes** on the Confirm Shutdown or Restart window.

   It can take over 7 minutes for the restart operation to complete.
5. On the Trusted Key Entry: Upgrade / Install Recovery / Frame role window, enter option **2** (Install Recovery) and click **Enter**.
6. Select option **1** and click **Enter** to start the Install Recovery process. It can take over 15 minutes for the TKE code installation to complete. You might receive the message `if the RC is zero, press ENTER to continue`. If so, click **Enter**.

   Note: If you receive any return code other than 0, contact your support personnel.
   When processing is complete, the DVD drive opens and a message window

opens with OPERATION SUCCESSFUL at the top. Do not remove the TKE installation DVD. You can manually close the door to the DVD drive, or let it close automatically in the next step.

7. Click **Enter** to restart the TKE workstation. The DVD drive closes if you did not close it manually. It can take over 7 minutes for the restart processing to complete.

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

8. On the Trusted Key Entry: Upgrade / Install Recovery / Frame Roll window, enter option 3 (Frame Roll) and click **Enter**.
9. Select option 1 and click **Enter** to start the Frame Roll process. When the Frame Roll installation is complete, the DVD drive opens and a message window opens with OPERATION SUCCESSFUL at the top.
10. Follow the steps listed in the message window.
    a. Insert the USB flash memory drive that contains the Save Upgrade data, if it is not already installed in the workstation.
    b. Remove the TKE installation DVD from the DVD drive. You can manually close the door to the DVD drive, or let it close automatically in the next step.
    c. Click **Enter** to restart the TKE workstation.

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

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

11. Close all windows except the pre-logon window. The pre-logon window has the title Welcome to the Trusted Key Entry Console.
12. Select **Privileged Mode Access**.
13. Enter admin for the user ID.
14. Enter the password. The default password for the admin user id is password.
15. From the Trusted Key Entry Console, select **Trusted Key Entry**.
16. Open the TKE Workstation Setup Wizard
17. Click **Finish** when you are finished.

Results

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

Chapter 4. TKE setup and customization

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

Table 19. 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 Communications Server personnel and ICSF Administrator	Host z/OS System	
6. Customize TKE Host Program started procs (delivered with ICSF)	Client Network or Communications Server personnel and ICSF Administrator	Host z/OS System	
7. Ensure RACF administration is complete.	Client Security Administrator	Host z/OS System	
8. Start ICSF	Client Operations or System Programmer	Host z/OS System Console	
9. Customize the TKE workstation crypto adapter	TKE Administrator	TKE workstation	
10. TKE Application Customization	TKE Administrator	TKE workstation	

For more information on tasks 1 and 2 see *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*, SB10-7153
- "TKE enablement" on page 9.
- Appendix B, "LPAR considerations," on page 313.

TKE TCP/IP setup

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

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

```
HOST   : 9.117.59.140 :
```

Figure 7. Entry example

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

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

Figure 8. Example of reserving a port

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

Any job with jobname CSFTTCP can connect to this port.

TKE host transaction program setup

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

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

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

Perform these steps to install the server:

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

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

Figure 9. Format of AUTHCMD

2. Set up system security

   To protect module CSFTTKE from unauthorized users, you must protect it using RACF. For more information, refer to *z/OS Security Server RACF Security Administrator's Guide* and *z/OS Security Server RACF System Programmer's Guide*.

   See *z/OS Security Server RACF Command Language Reference* for the correct command syntax. You might need to work with your security administrator, because these RACF commands are not available to the general user.

   This example permits the user ID or group assigned to the CSFTTCP started task to the CSFTTKE profile in the FACILITY class:

```
SETR CLASSACT(FACILITY)
SETR RACLIST(FACILITY)
RDEFINE FACILITY CSFTTKE UACC(NONE)
PERMIT CSFTTKE CLASS(FACILITY) ID(userid or group) ACCESS(READ)
SETROPTS RACLIST(FACILITY) REFRESH
```

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

   The module (CSFTTKE) must also be protected, using the APPL class to control which users can use the application when they enter the system.

   This example assigns a user ID or group to the CSFTTKE profile in the APPL class:

```
SETR CLASSACT(APPL)
SETR RACLIST(APPL)
RDEFINE APPL CSFTTKE UACC(NONE)
PERMIT CSFTTKE CLASS(APPL) ID(userid or group) ACCESS(READ)
SETROPTS RACLIST(APPL) REFRESH
```

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

   Note: The user IDs or groups of user IDs must be permitted to use the TKE workstation.

   If you do not have a generic user ID associated to all started procedures, you can associate a user ID to the CSFTTCP proc by issuing a RACF RDEFINE command. For more information, see *z/OS Security Server RACF Security Administrator's Guide*.

   Note: The RACF user ID associated with the CSFTTCP proc must have a valid OMVS segment.

   This example assigns a user ID or group to the started task CSFTTCP:

```
SETR CLASSACT(STARTED)
SETR RACLIST(STARTED)
RDEFINE STARTED CSFTTCP.CSFTTCP STDATA(USER(userid))
SETROPTS RACLIST(STARTED) REFRESH
```

Figure 12. Assign a user ID to a started task

3. The TKE Host Transaction program must be started before you can logon to the host from TKE. A sample startup procedure is shipped in 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 13. Sample startup procedure

TKE startup parameters

Startup parameters may be passed to the TKE Host Transaction Program in a JCL parm field (CPARM) or in a data set referenced in the TKEPARMS DD statement. Parameters specified on the CPARM field override the parameters in the TKEPARMS data set. A sample TKEPARMS data set is shipped in 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 61).

  If a port number is not specified, a default port of 50003 will be used. However, if port 50003 is not reserved in your TCP/IP profile, another application may use it and the TKE HTP will fail.

  For example: PORT;1000

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

You may choose between implicit and explicit allocation.

- Implicit - The name of the configuration data set is constructed at run time, based on rules implemented in the components of TCP/IP. Once a data set name is constructed, TCP/IP uses the dynamic allocation services of z/OS to allocate the configuration data set.
- Explicit - TCP/IP searches for a specific DD name allocation for some configuration data sets. If you allocated a DD name with a DD statement in the JCL used to start a TCP/IP component, TCP/IP will read its configuration data from that allocation. It will not construct a configuration data set name for dynamic allocation.

4. Start the TKE server from the z/OS system console:

```
S CSFTTCP
```

Figure 14. Start the TKE server

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

Cancel the TKE server

To cancel the TKE server:

```
C CSFTCTCP
```

Or

```
STOP CSFTTCP
```

Figure 15. 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 defaults to 50003.

Note: Depending on your system setup, you might have to define the CSFTCTCP task to the RACF STARTED class:

```
REDEFINE STARTED CSFTCTCP.CSFTCTCP STDATA(USER(userid))
SETROPTS RACLIST(STARTED) REFRESH
```

TKE workstation setup and customization

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

The IBM CE installs the TKE cryptographic adapter into your TKE workstation and then powers it up.

Note: When using a KVM switching unit, the TKE windows might appear to be distorted. The TKE should be initialized while it is connected directly to the LCD monitor. After initial boot up on the LCD monitor, the TKE can be connected to the KVM switching unit.

Important: For reliable TKE operation, the customer must ensure an installation area ambient temperature in the range of 10 degrees Celsius to 40 degrees Celsius, plus or minus 5 degrees Celsius.

For TKE storage, the customer must ensure an installation area ambient temperature in the range of 1 degree Celsius to 60 degrees Celsius, plus or minus 5 degrees Celsius. In addition, the ambient relative humidity must not exceed 80 percent.

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

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

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

Figure 16. Login with ADMIN user name

The TKE Workstation Setup wizard

Beginning in TKE 7.3, the TKE workstation includes the TKE Workstation Setup wizard. This wizard takes you through the process of performing the final configuration of your TKE workstation. The wizard tests for critical settings and

ensures that the TKE workstation is set up correctly. After the workstation is set up, you can run the wizard at any time to check the TKE workstation or to make changes to it.

Guideline: Use the TKE Workstation Setup wizard to finish your workstation configuration.

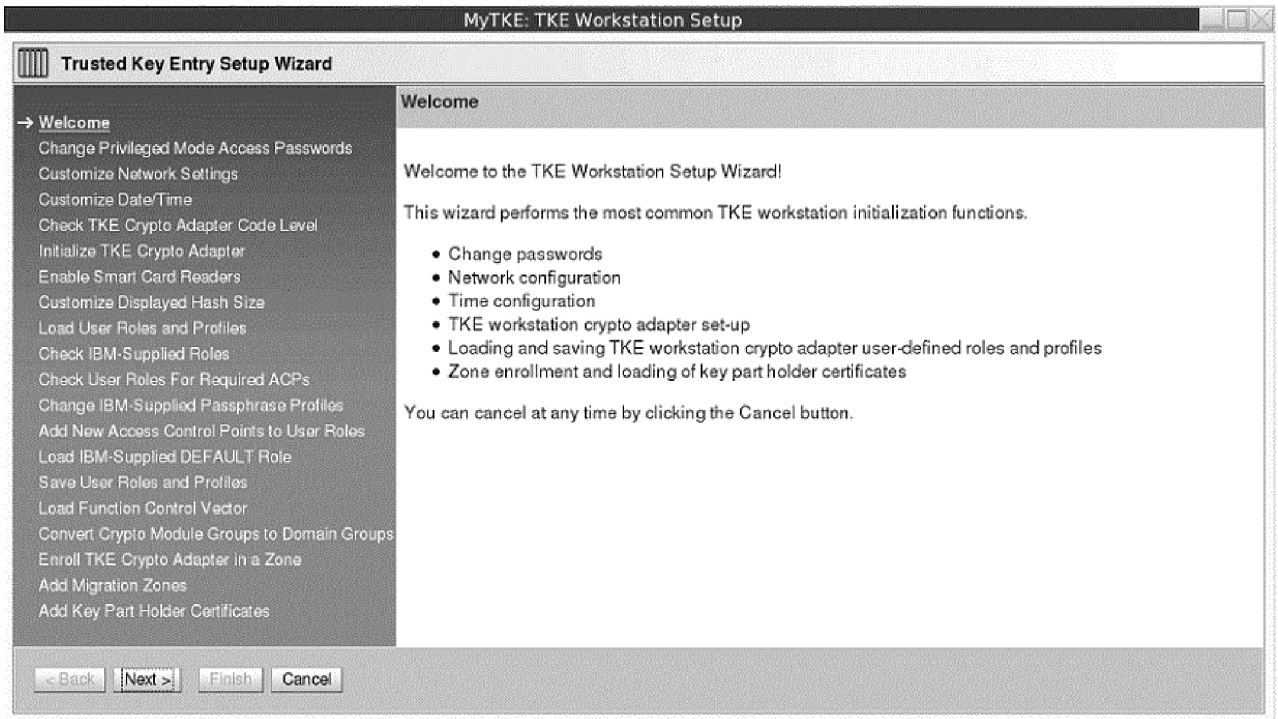


Figure 17. The TKE Workstation Setup wizard Welcome window.

Overview of the TKE Workstation Setup wizard

The TKE Workstation Setup wizard takes you through a series of workstation setup tasks. Perform the tasks in the order in which they are presented. Some conditions are required for the TKE workstation to work correctly. The wizard tests for these conditions and takes you through the process of making the necessary changes.

The wizard tasks fall into five categories:

- Basic Workstation Tasks

  These tasks start workstation configuration utilities. The wizard does not attempt to make any recommendations for these tasks. It is up to you to decide whether you want to perform these tasks. The following tasks are in this category:

  – Customize network settings. (For more information about this task, see "Customize network settings" on page 70, which describes how to perform this task if you do not use the Workstation Setup wizard.)

  – Customize date and time. (For more information about this task, see "Customize console date/time" on page 74, which describes how to perform this task if you do not use the Workstation Setup wizard.)

- Critical tasks

  These tasks check for conditions that are required for the TKE workstation to work correctly. If the wizard determines that the TKE workstation is not set up

correctly, it issues a message that states the situation and suggests an action. When you click **Next**, the wizard performs the action. The following tasks are in this category:
  - Check the TKE crypto adapter code level
  - Load the function control vector
- Important tasks

  These tasks check for conditions that might limit the functionality of the TKE workstation. If the wizard task determines that the TKE workstation is not set up correctly, it issues a message that states the situation and suggests an action. When you click **Next**, the wizard performs the action. The following tasks are in this category:
  - Initialize the TKE crypto adapter.
  - Load user roles and profiles. For more information about this task, see "Wizard tasks to load and save customer-defined roles and profiles."
  - Check IBM-supplied roles.
  - Check user roles for required ACPs.
  - Add new access control points to user roles.
  - Convert crypto module groups, if present, to domain groups.
- Secure workstation tasks

  These tasks change default settings for IBM-supplied items. The wizard can test for the need to reload the DEFAULT role. You decide whether you want to perform the change password tasks. The following tasks are in this category:
  - Change privileged mode access passwords.
  - Change IBM-supplied profile passwords.
  - Load the IBM-supplied DEFAULT role.
- Customer preference tasks

  These tasks configure optional features of the TKE workstation. You decide whether you want to perform these tasks. The following tasks are in this category:
  - Enable smart card readers.
  - Customize displayed hash size.
  - Save user roles and profiles. For more information about this task, see "Wizard tasks to load and save customer-defined roles and profiles."
  - Enroll the TKE crypto adapter in a zone.
  - Add migration zones.
  - Add key part holder certificates.

Wizard tasks to load and save customer-defined roles and profiles:

There are two wizard tasks that deal with customer-defined roles and profiles;
- Save user roles and profiles
- Load user roles and profiles

These two tasks work together to simplify the process of backing up, migrating, and loading customer-defined roles and profiles onto a TKE workstation local crypto adapter.

The save user roles and profiles wizard task performs the following tasks:
- It determines whether there are any customer-defined roles or profiles on the TKE workstation's local crypto adapter.

- If it finds customer-defined roles or profiles, it creates files that contain information that allows the load user roles and profiles wizard task to load the roles and profiles.

Notes:

- Role and profile information is kept in different files.
- The files are saved in the TKE Data Directory.
- The files can be left on the TKE workstation for recovery purposes, or moved to another TKE workstation for migration purposes.
- The save and load user roles and profiles tasks can also be run from the Access Control menu in the Cryptographic Node Management utility (CNM).

The load user roles and profiles wizard task performs the following tasks:

- It determines whether either of the files that are created by the save user roles and profiles wizard task is on the system.
- Depending on which files are found, all the roles, or profiles, or both, are loaded onto the TKE workstation's local adapter.

Note: When a passphrase profile is loaded, you must assign a new password to the profile. This password does not have to match the password that the profile had at the time the profile was saved.

Restriction: The load user roles and profiles wizard task requires data from the save user roles and profiles wizard task. Therefore, you can use the load task only when the roles and profiles come from a system with a minimum release level of TKE 7.3.

For information about how to save and load customer-defined roles and profiles on a workstation that does not have the TKE Workstation Setup wizard, see "Option 2: Using the Cryptographic Node Management (CNM) utility to collect data about roles and profiles" on page 54 and "Option 2: Using the multiple-step method to complete workstation setup" on page 57.

Running the TKE Workstation Setup wizard

The TKE Workstation Setup wizard is supported starting with TKE 7.3. To run the TKE Workstation Setup wizard, follow these steps:

1. Close all windows except the pre-logon screen. The pre-logon screen has the title Welcome to the Trusted Key Entry Console.
2. Select **Privileged Mode Access**.
3. Enter `admin` for the user ID.
4. Enter the password for the admin user ID. The default password for the admin user ID is `password`.
5. From the Trusted Key Entry Console, select **Trusted Key Entry**.
6. Open the **TKE Workstation Setup** wizard.
7. Take all appropriate actions in response to the prompts from the wizard.
8. Click **Finish** when you are done.

Configuring TCP/IP

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

Customize network settings

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

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

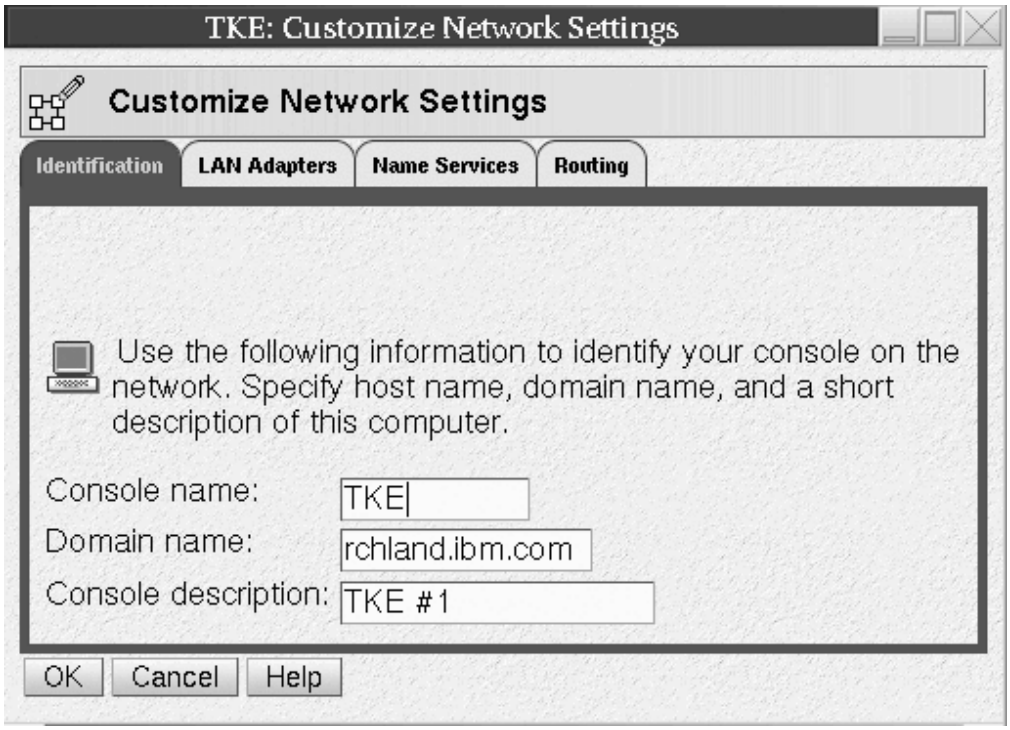


Figure 18. Customize Network Settings - Identification Tab

By default, the Console name is TKE. It is displayed in the title bar of all the window displays. Enter the domain name for your network and a brief description for the workstation. If you do not have any further updates to make, click OK. To continue with updates to your network settings, click on the LAN Adapters Tab.

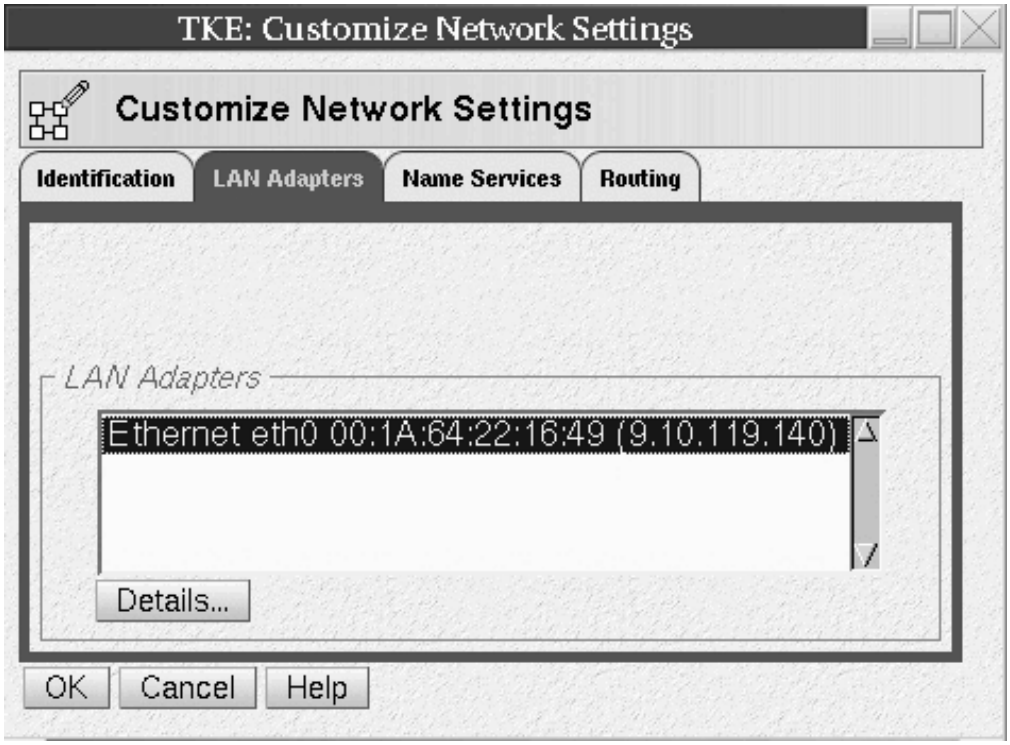


Figure 19. Customize Network Settings LAN Adapters Tab

With the Ethernet LAN adapter highlighted, click on Details.

The LAN Adapter Details window opens.

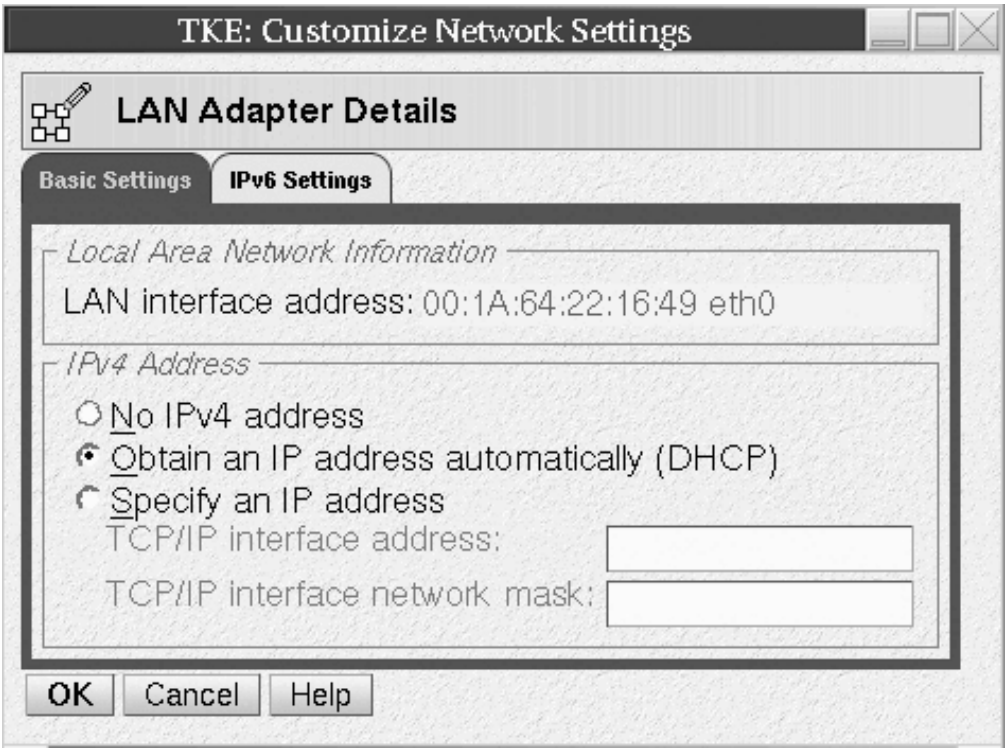


Figure 20. Local Area Network

Specify Local Area Network Information and DHCP Client/IP address information for your network. Press the **OK** push button. If you do not have any further updates to make, click the **OK** push button on the Customize Network Settings Window. To continue with updates to your network settings, click on the Name Services tab.

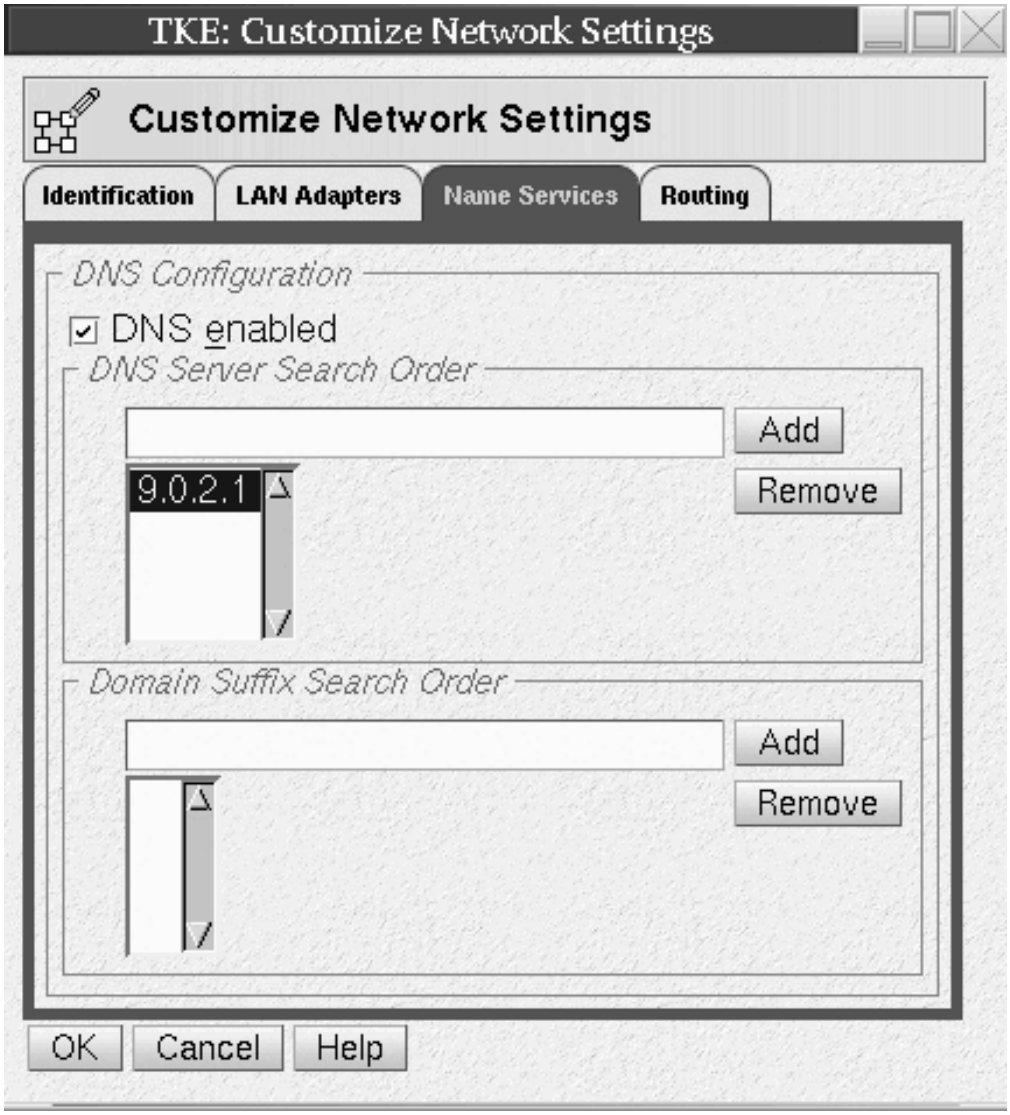


Figure 21. Customize Network Settings - Name Services Tab

Select whether DNS is enabled or disabled. Configure the DNS Server Search Order and the Domain Suffix Search Order for your network. If you do not have any further updates to make, click OK. If Routing information is required for your network, click on the Routing tab and configure as appropriate. When complete, click OK to save all updates to your network settings.

Problems associated with networking can be diagnosed with the Network Diagnostic Information task. To open this task select Service Management, Network Diagnostic Information.

If you are having problems connecting to a host system, test the TCP/IP connection by pinging the address. Enter the host address in the TCP/IP Address to Ping field and click on Ping.

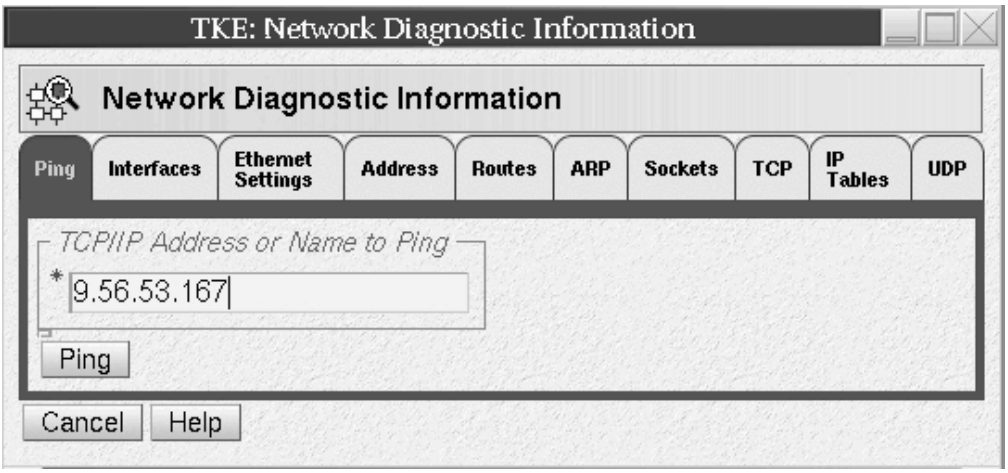


Figure 22. Network Diagnostic Information Task

Customize console date/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.

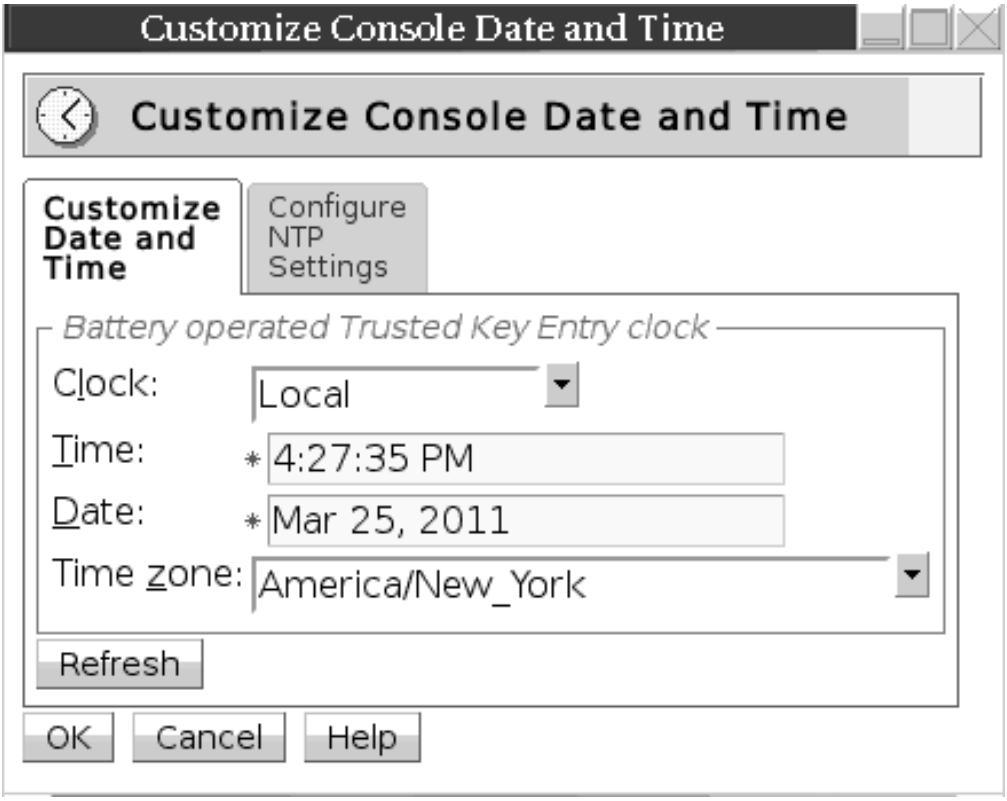


Figure 23. Customize Console Date and Time Window

Setting the assigned time for your system - alternate procedure

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

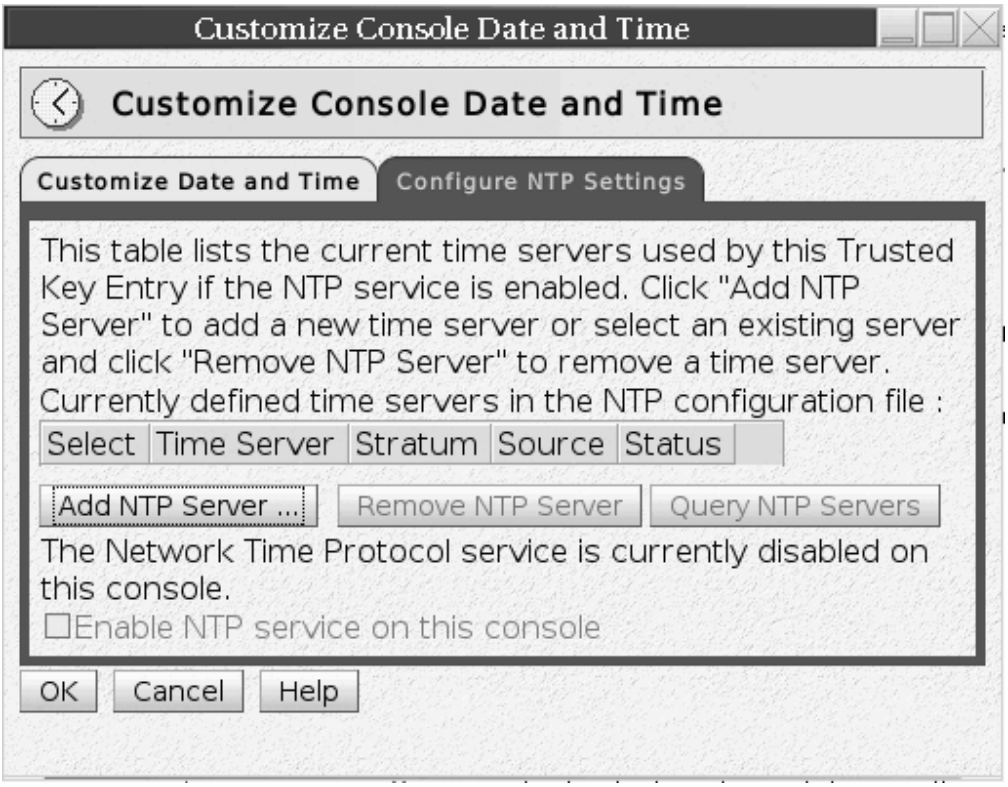


Figure 24. Configure NTP settings

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

The Add a Network Time Server dialog opens.

Figure 25. 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 the TKE workstation crypto adapter

The TKE workstation crypto adapter only needs to be initialized when:

- This is a first time setup for a TKE workstation.

- You want to zeroize the TKE workstation crypto adapter and start over.

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

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

Initialize the TKE workstation crypto adapter using TKE's IBM Crypto Adapter Initialization and Cryptographic Node Management Utility.

- If you are initializing using passphrase, see "Initializing the TKE workstation crypto adapter for use with passphrase profiles."
- If you are initializing using smart cards, see "Initializing the TKE workstation crypto adapter for use with smart card profiles."

Initializing the TKE workstation crypto adapter for use with passphrase profiles

Guideline: The TKE Workstation Setup wizard has a task that takes you through initializing the crypto adapter. If you want to initialize the adapter, use the wizard to do the initialization. For more information, see "The TKE Workstation Setup wizard" on page 66.

To initialize the TKE workstation crypto adapter for use with passphrase profiles:

1. Open the Trusted Key Entry window pane of the Trusted Key Entry Console.
2. From the Applications list, open the TKE's IBM Crypto Adapter Initialization application.

   The initialization script will be run inside of a script window. There are several messages you must reply to as the script runs:

   - A warning indicates that the action will delete any existing data on the card, and you are asked if you want to continue. Select **Y** if you want to continue.
   - A message asks if you want to initialize the adapter for use with passphrase or smart card profiles. Select **P** for passphrase profiles.
3. After the script has completed, you can review status messages that show what initialization actions were performed. After you have reviewed the data, press the **ENTER** key to close the script window.

The TKE workstation crypto adapter is initialized with the roles and profiles required for the passphrase environment. The times on the TKE workstation and the crypto adapter are synchronized. The crypto adapter master keys are set to random values, and DES, PKA, and AES key storages are initialized.

Initializing the TKE workstation crypto adapter for use with smart card profiles

To initialize the TKE workstation crypto adapter for use with smart card profiles:

1. Open the Trusted Key Entry window pane of the Trusted Key Entry Console.
2. From the Applications list, open the TKE's IBM Crypto Adapter Initialization application.

   The initialization script will be run inside of a script window. There are several messages you must reply to as the script runs:

   - A warning indicates that the action will delete any existing data on the card, and you are asked if you want to continue. Select **Y** if you want to continue.

- A message asks if you want to initialize the TKE's adapter for use with passphrase or smart card profiles. Select **S** for smart card profiles.

3. After the script has completed, you can review status messages that show what initialization actions were performed. After you have reviewed the data, press the **ENTER** key to close the script window.

The TKE workstation crypto adapter is initialized with the roles required for the smart card environment. The times on the TKE workstation and the crypto adapter are synchronized. The crypto adapter master keys are set to random values, and DES, PKA, and AES key storages are initialized.

TKE workstation crypto adapter post-initialization tasks

After the TKE workstation adapter is initialized, you may need or want to do the following tasks:

- Verify that Function Control Vector (FCV) has been loaded onto the TKE workstation crypto adapter. The adapter is shipped with the FCV installed. The initialization script does not remove the FCV from the adapter. However, if the FCV was cleared by an administrator or was not properly installed, the TKE will not function properly. Taking the time to verify the FCV is present is highly recommended and taking corrective action if it is not installed is mandatory.
- Change the passwords for the IBM-supplied passphrase profiles that were created on the adapter. We strongly recommend you perform this task.
- Load previously created user defined Roles and Profiles from role and profile definition files.
- Create new user defined Roles and Profiles.
- Load known master keys rather than use the random keys that were generated.
- Redefine the DEFAULT role if the TKE workstation crypto adapter was initialized for use with smart card profiles. We strongly recommend you perform this task.
- Add new ACPs to existing roles using the Migrate Roles utility.
- Customize the TKE application.
- Configure 3270 emulators.

Verifying that the function control vector (FCV) has been loaded

Guideline: The TKE Workstation Setup wizard has a task for testing and loading the FCV. Use the wizard to test and update your workstation. For more information, see "The TKE Workstation Setup wizard" on page 66.

The TKE workstation crypto adapter function control vector governs what cryptographic services can be used on the adapter. If the FCV is not loaded, you will not have access to any cryptographic function. You can use the following steps to verify that the FCV is loaded:

1. Open the Trusted Key Entry window pane of the Trusted Key Entry Console.
2. From the Applications list, open the Cryptographic Node Management (CNM) Utility.
3. The CNM utility will prompt for a profile. Select TKEADM or equivalent profile.
4. From the main CCA Node Management Utility screen, select the **Crypto Node –> Status** pull down.
5. From the CCA Node Management Utility – CCA Application Status screen, press the **Export Control** push button.

The FCV is properly set when:

- The maximum modulus size is 4096.
- All values except CDMF are available.

If the maximum modulus size is 0 and all other values are "not available", you must reload the FCV.

6. Press the **Cancel** push button to return to the main CCA Node Management Utility screen.
7. Exit and logoff the CNM utility.

Reloading the function control vector: This task is only necessary if you determined the FCV is not currently loaded on the TKE workstation crypto adapter.

To reload the Function Control Vector:

1. Open the Trusted Key Entry window pane of the Trusted Key Entry Console.
2. From the Applications list, open the Cryptographic Node Management (CNM) Utility.
3. The CNM utility will prompt for a profile. Select TKEADM or equivalent profile.
4. From the main CCA Node Management Utility screen, select **Crypto Node –> Authorization –> Load** off the pull down menu.
5. Find the file named fcv_4tke80.crt and highlight it.
6. Press the **open** push button.
7. When prompted, press **yes** to confirm you want to load the FCV.
8. An "authorizations have been loaded" message window displays. Press **OK** to close this window.

   Note: If you are unable to load the FCV, contact your IBM service representative.
9. Exit and logoff the CNM utility.

Changing the passwords for IBM-supplied passphrase profiles created on the TKE workstation crypto adapter

Guideline: The TKE Workstation Setup wizard has a task that tests to see if there are any IBM-supplied passphrase profiles on the TKE workstation's local adapter. If there are, you can use the task to change their passwords. If you decide you are going to change IBM-supplied profile passwords, use the wizard to change them. For more information, see "The TKE Workstation Setup wizard" on page 66.

When the TKE workstation crypto adapter was initialized for use with passphrase profiles, IBM-supplied profiles were created with passphrases that match their profile names. The profiles are:

- TKEADM
- TKEUSER
- KEYMAN1
- KEYMAN2

You should change the passwords for all of these profiles. The following steps can be used to change the profile passwords:

1. Open the Trusted Key Entry window pane of the Trusted Key Entry Console.

2. From the Applications list, open the Cryptographic Node Management (CNM) Utility.
3. The CNM utility will prompt for a profile. Select TKEADM or equivalent profile.
4. From the main CCA Node Management Utility screen, select **Access Control –> Profiles** off the pull down menu.
5. Highlight the profile to be changed and press the **edit** push button.
6. Enter the **passphrase** and **confirm passphrase** values.
7. Press the **change passphrase** push button to make the change.
8. Press **OK** on the "passphrase changed" message.
9. Repeat the process for all the profiles you want to change.
10. When finished, press **done** to return to the main CCA Node Management Utility screen.
11. Exit and logoff the CNM utility.

Loading previously created user-defined roles and profiles from role and profile definition files

Guideline: The TKE Workstation Setup wizard has a task that simplifies the process of loading roles and profiles onto a TKE workstation's local adapter. There are limitations. For more information, "Wizard tasks to load and save customer-defined roles and profiles" on page 68.

If you have user-defined role and profile definition files and you want to install the roles and profiles on the TKE workstation crypto adapter, see the following topics for installation instructions:

- To load roles on the adapter, see "Opening a role definition file" on page 242 and "Making changes to a role or role definition file" on page 243.
- To load profile on the adapter, see "Opening a profile definition file" on page 249 and "Making changes to a profile or profile definition file" on page 250.

For more information about role and profile definition files, see "TKE workstation crypto adapter roles and profiles" on page 14.

Creating new user-defined roles and profiles

If you want to create new user defined roles and profiles (including group profiles), see "Managing roles" on page 239 and "Managing profiles" on page 246. For more information about role and profile definition files, see "TKE workstation crypto adapter roles and profiles" on page 14.

Loading a known master key instead of using the randomly generated key

Note: The TKE Workstation Setup wizard does not have a task for this activity.

When the TKE workstation crypto adapter is initialized, new random master key values are loaded. If you want to, you can load a new master key value from clear key parts or a smart card. If you want to load a known master key, see the following sections of this document for installation instructions:

- To load clear key parts, see "Parts — Loading a new master key from clear key parts" on page 258.
- To load smart card key parts, see "Smart card parts — loading master key parts from a smart card" on page 262.

After you load a new master key, you must set the master key and reencipher DES, PKA, or AES key storage. For more information, see “Reenciphering key storage” on page 266.

Note: If you initialized the TKE workstation crypto adapter for use with passphrase profiles, you must log on to the adapter using the profile of:

- KEYMAN1 or equivalent to clear the new master key register and load the first master key part role.
- KEYMAN2 or equivalent to combine master key parts, set the master key, and reencipher key storage.

Redefining the DEFAULT role when the TKE workstation crypto adapter has been initialized for use with smart card profiles

Guideline: The TKE Workstation Setup wizard has a task for testing and loading the DEFAULT role. Use the wizard to test and update your workstation. For more information, see “The TKE Workstation Setup wizard” on page 66.

The DEFAULT role that is created when a TKE workstation crypto adapter is initialized for use with smart card profiles is designed to provide enough authority to perform the initial administration of the adapter. Be aware, however, that the DEFAULT role is a powerful role. After the initial administration is done, you should replace the DEFAULT role with the less powerful DEFAULT role that is created when a TKE workstation crypto adapter is initialized for use with passphrase profiles. To reload the DEFAULT role, follow instructions in “Opening a role definition file” on page 242 and “Making changes to a role or role definition file” on page 243 using the default_80.rol file.

Adding new ACPs to existing roles using the Migrate Roles utility

Guideline: The TKE Workstation Setup wizard has two tasks that are related to this activity. One task tests and updates IBM-supplied roles. The other task starts the Migrate Roles utility for customer-defined roles. Use the wizard to test and update your workstation. For more information, see “The TKE Workstation Setup wizard” on page 66.

Sometimes between TKE releases, new Access Control Points (ACPs) are made available to the roles on the TKE workstation crypto adapter. New ACPs are never automatically added to existing roles during the migration process. For this reason, it might be necessary to add ACPs to existing roles after you upgrade to a new TKE release. Beginning in TKE 7.1, TKE 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 7.1,15 individual ACPs were added to control access to TKE applications and some functions within TKE applications. If you migrated roles from an earlier version of TKE to TKE 7.1 or later, review the information in “TKE 7.1 role migration considerations” on page 83.

The Migrate Roles 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. After you make your selection, you send the command to make the updates.

Notes:

1. After you initialize your TKE workstation crypto adapter, the IBM-supplied roles have the correct Access Control Points for the TKE's release level.
2. In TKE 7.1, many ACPs were added to control access to TKE applications. See "TKE 7.1 role migration considerations" on page 83.
3. User-defined roles are normally based off of one of the IBM-supplied roles. It is highly recommended you view the new ACPs for the base IBM-supplied roles to help you determine what ACPs you might want to add to your user-defined roles.
4. The ACPs for all of the IBM-supplied roles are listed in "IBM-supplied role access control points (ACPs)" on page 22. The tables show what ACPs are new in any given release.

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

   The Migrate Roles utility starts.

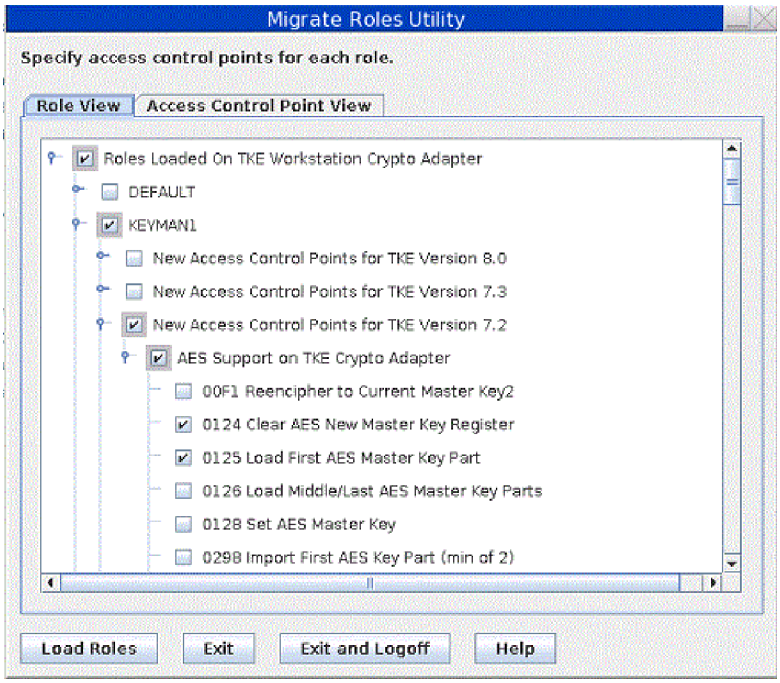


Figure 26. Migrate Roles utility

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

To add new ACPs to existing roles:

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

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

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

- SCTKEUSR
- SCTKEADM

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

- TKEUSER
- TKEADM
- KEYMAN1
- KEYMAN2

When you have determined which roles you need to update, go into the Crypto Node Management utility and reload the 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, see "Managing roles" on page 239.

TKE 7.1 role migration considerations for customer-defined roles: If your customer-defined roles were created before your system was upgraded to TKE 7.1 or later, or your roles were created from role definition files that were created on a TKE that was pre-TKE 7.1, you need to add ACPs to your customer-defined roles. To do this, you must determine which ACPs you want to add to your customer-defined roles. When you have made your choices, use the Migrate Roles utility (described in "Adding new ACPs to existing roles using the Migrate Roles utility" on page 81) 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 crypto modules. The TKEADM or SCTKEADM roles are designed for users responsible for managing the TKE workstation. Customer-defined roles should be modeled off of one of these two pairs of roles. The following lists show which new ACPs were added to these general purpose roles. You can use this information to help you decide which ACPs you need to add to your customer-defined roles.

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

- Application Logon ACPs
  - 1003: Open Migrate 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

TKE 7.3 role migration considerations for customer-defined roles: In TKE 7.3, an ACP was added to control the ability to manage a host entry. The new ACP is:

- 100F: Manage Host List

You must have this ACP to be able to create, delete, or change a host entry. The ACP was added to the IBM-supplied roles TKEUSER and SCTKEUSR. If you have any customer-defined roles that are modeled after these roles, you might want to add this ACP to them.

TKE 8.0 role migration considerations for customer-defined roles: In TKE 8.0, an ACP was added for shipping print support. The new ACP is:

- 1010: Print Files

You must have this ACP to be able to print a file on the TKE workstation. The ACP has not been added to any IBM-supplied roles for security reasons.

Customize the TKE application

Note: The TKE Workstation Setup wizard does not have a task for this activity.

1. Open the TKE application by clicking on Trusted Key Entry and then clicking on Trusted Key Entry 8.0.
2. Logon to the TKE workstation crypto adapter. See Workstation Logon: Passphrase or Smart Card on “Crypto adapter logon: passphrase or smart card” on page 93 for details.
3. Click on Preferences on the task bar.
4. Enable/Disable the Preferences as appropriate. See “TKE customization” on page 128 for details.

Configure 3270 emulators

Note: The TKE Workstation Setup wizard does not have a task for this activity.

A z/OS session is required on the host for several tasks executed on TKE to complete. If you do not have access to the z/OS system outside of the TKE Workstation, create access to the z/OS system on the TKE by configuring a 3270 emulator session.

To configure a 3270 emulator session, click Service Management and then click **Configure 3270 Emulators**.

The Configure 3270 Emulators window is displayed.

Figure 27. Configure 3270 Emulators

1. Click **New** to add a 3270 session.
2. The Add 3270 Emulator Session window is displayed.
3. Enter the Host Address you would like to connect to.
4. Select Enabled or Disabled from the Start at Console Startup drop down menu.

   Enabled
   When the console starts this session also starts.

   Disabled
   When the console starts this session does not start.

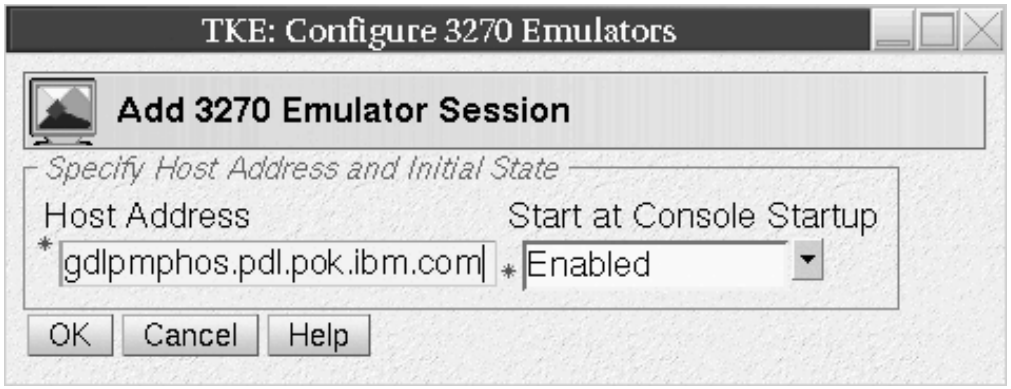


Figure 28. Add 3270 Emulator Session

5. To save the emulator session definition click **OK**.
6. On the Configure 3270 Emulators window click **OK** to save the session. Click **Cancel** to end without saving the session.

Figure 29. Start or Delete a 3270 Emulator Session

7. To start or delete a host address select the host address from the list and click **Start** or **Delete**.

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

Using an SSL 3270 emulation session

To use an SSL 3270 emulation session, you must perform the following tasks:

1. Configure the TKE workstation to use SSL for 3270 emulation. For instructions, see "Configuring the TKE workstation to use SSL for 3270 emulation"
2. Add a 3270 emulation session. See "Adding a 3270 emulator session" on page 89.
3. Ensure that TN3270 is configured correctly on the host system. For instructions, see *z/OS V2R2.0 Communications Server: IP Configuration Reference*.

   Note: When you configure the host Telnet parameters, you must specify `CLIENTAUTH NONE`.

Configuring the TKE workstation to use SSL for 3270 emulation:

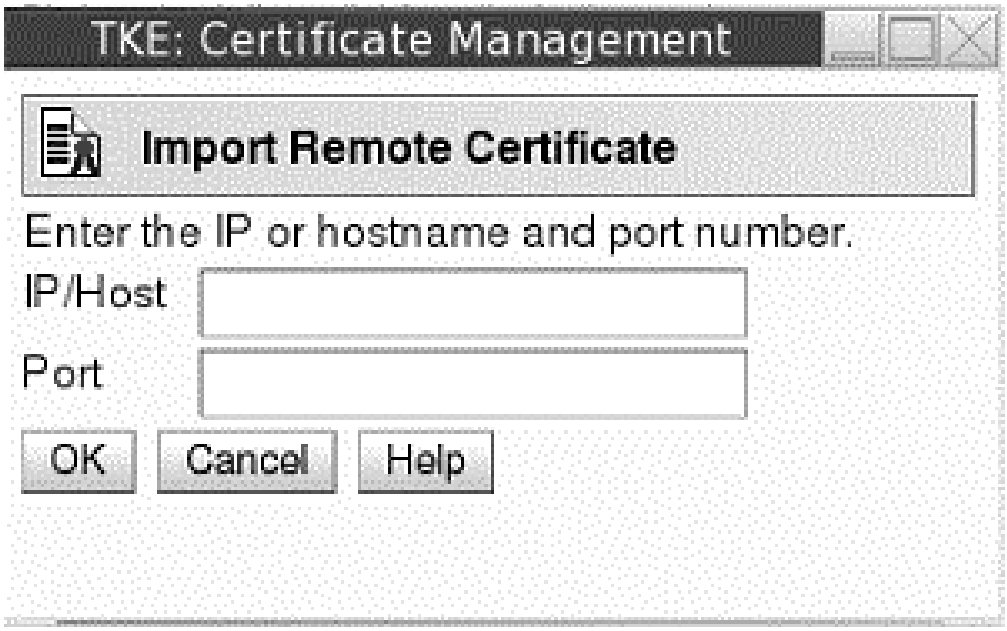
About this task

You must import the certificate for the session. Use the following procedure:

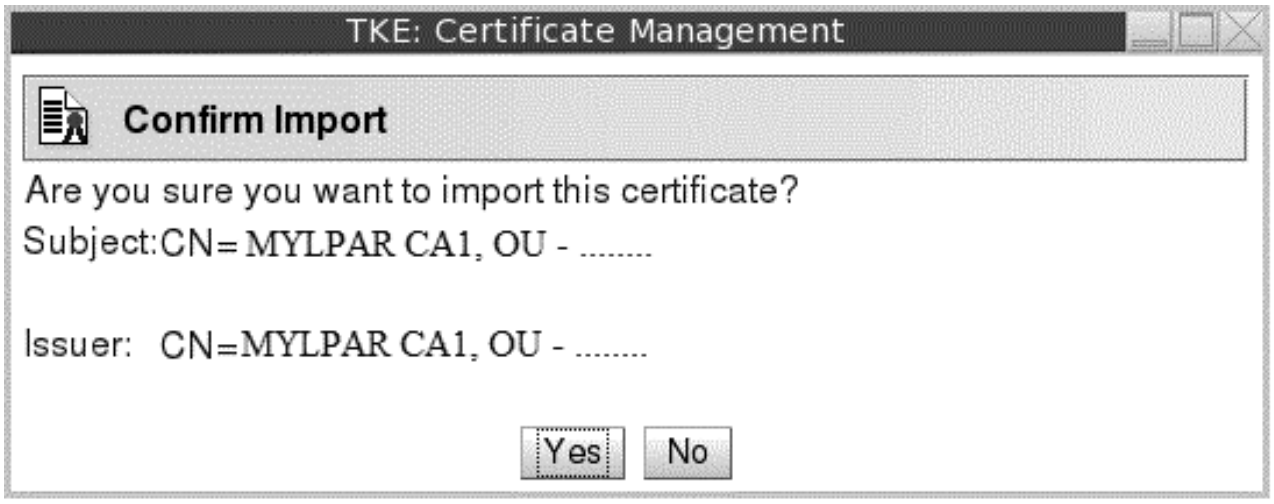
Procedure

1. Sign on to the TKE workstation in Privileged Mode Access with the ADMIN profile.
2. From the Trusted Key Entry Console, click **Service Management**.
3. Under **Configuration**, open the "Certificate Management " application.
4. Click **Import > From Remote Server**

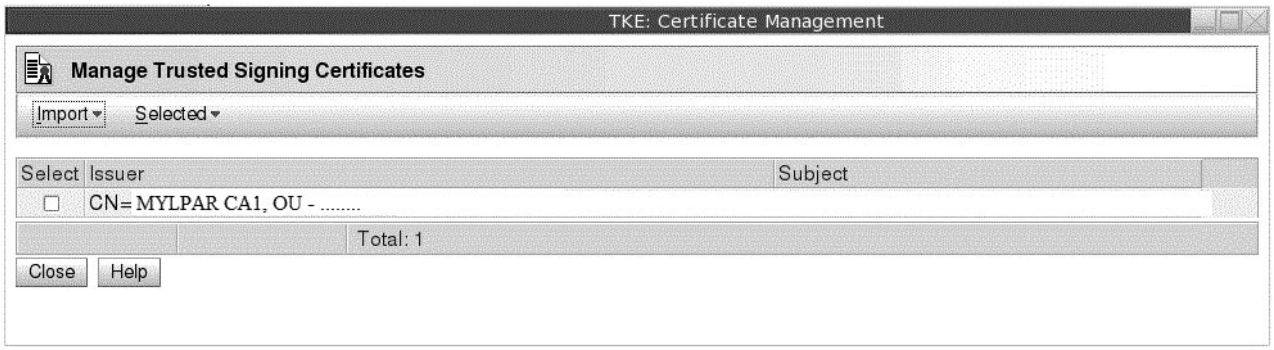
The following window opens:



5. Enter the information about the certificate's location and click **OK**. For example, specify the host's SSL IP address and port to get the host certificate that is presented during the SSL handshake. A confirmation window opens:



6. Click **Yes** to import the certificate. The imported certificate is now in the list of certificates.

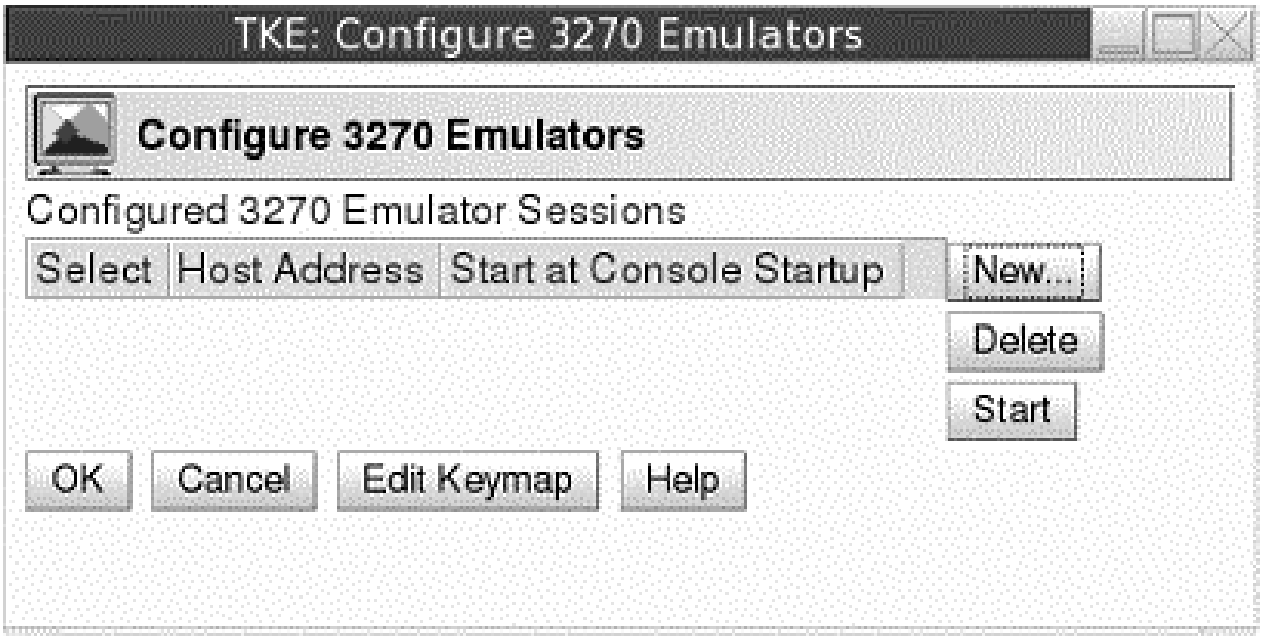


7. Close the Certificate Management utility.
8. Close your Privileged Mode Access session.

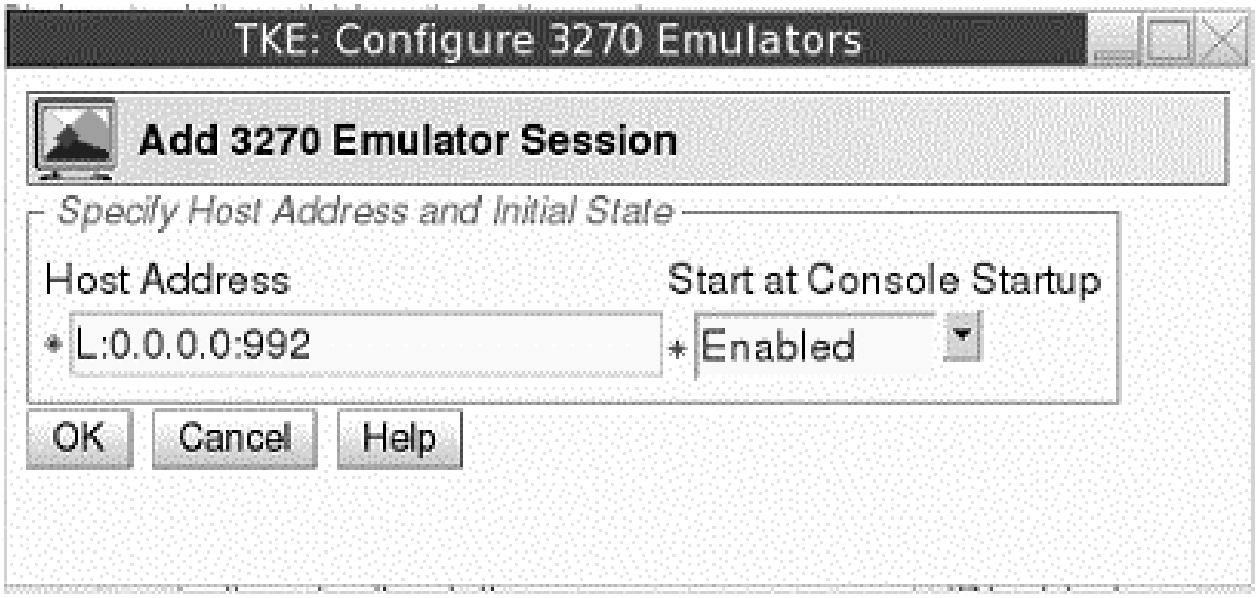
Adding a 3270 emulator session:

Procedure

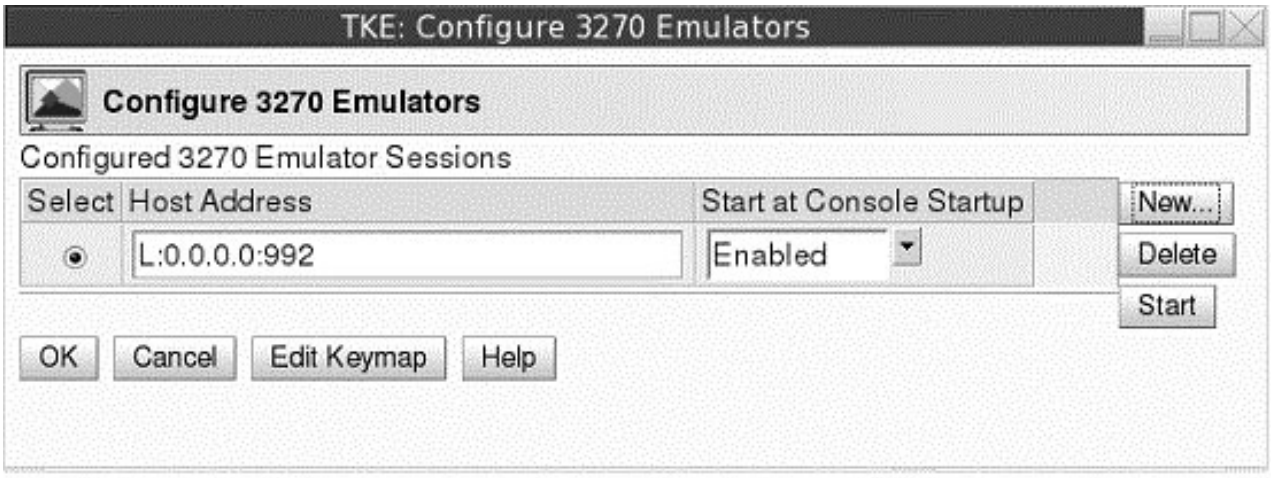
1. From the Trusted Key Entry Console, click **Service Management**.
2. Under **Configuration**, click **Configure 3270 Emulators**. The following window opens:



3. Click **New**. A window opens in which you can enter the host address and initial state of the emulator session.
4. Specify the host address in the form L:*IP address or DNS name:port nmber* and click **OK.** For example:



5. The emulator session is now listed as a configured 3270 emulator session. To initiate a new emulator session, select it from the list of configured sessions and click **Start**. In the following example, the emulator session is started every time that the TKE console is started.


TKE: Configure 3270 Emulators
Configure 3270 Emulators
Configured 3270 Emulator Sessions
Select
Host Address
Start at Console Startup
L:0.0.0.0:992
Enabled
New...
Delete
Start
OK
Cancel
Edit Keymap
Help

Chapter 5. TKE up and running

The Trusted Key Entry console displays the applications and utilities available on the TKE workstation. When you open a TKE application or utility, you must sign on with a profile that is on the TKE workstation crypto adapter. The individual or group profile you choose must have enough authority to do the functions performed by the application or utility.

Crypto adapter logon: passphrase or smart card

When you start any TKE application, you are presented a list of profiles that are allowed to start the application. Depending on how you initialized the TKE workstation crypto adapter and set up the TKE workstation crypto adapter profiles, you may have passphrase, smart card, or group profiles presented when you open an application. If you open a TKE application and the list of available profiles is empty, this may mean that you need to initialize your TKE workstation crypto adapter, or create and load profiles. For instructions on how to do this, refer to "Initializing the TKE workstation crypto adapter" on page 76.

Passphrase and passphrase group logon

From the Framework tree on the left panel of the main TKE console screen, click on **Trusted key Entry**, then click on **Trusted Key Entry 8.0**.

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

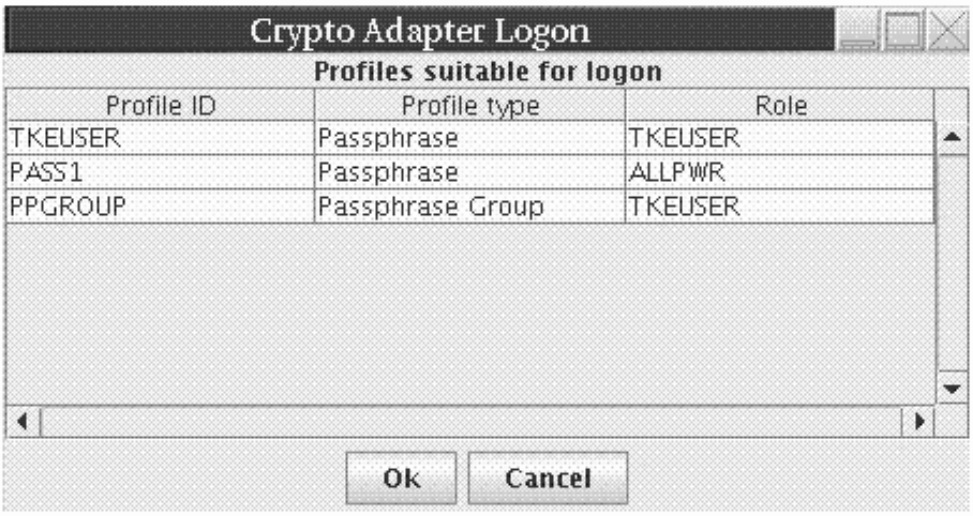


Figure 30. Crypto Adapter logon window with passphrase profiles

Steps for logging on are:

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

If you selected a single passphrase profile ID

1. The Passphrase Logon window will be displayed.

Figure 31. Enter passphrase for logon

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

   Note: The passphrase is case sensitive.
3. Optionally, the passphrase for the crypto adapter profile ID can be changed by the user by selecting the Change Passphrase checkbox before pressing OK to initiate the logon. If the Change Passphrase box was checked, then the Change Logon Passphrase dialog will be displayed after the user profile has been logged on, but before the selected TKE application is started.

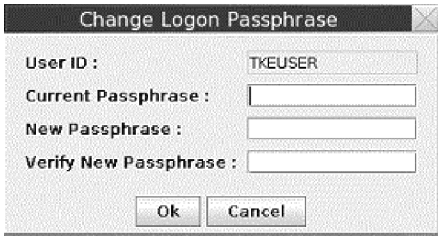


Figure 32. Change logon passphrase

To change the passphrase, enter the current passphrase, the new passphrase and the verify new passphrase, then select **OK**.

If you selected a group passphrase profile ID

1. The Crypto Adapter Group Logon window will be displayed. This window displays the number of members required for logon and the profile IDs available for logon.

Figure 33. Crypto Adapter group logon window with passphrase profiles

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

   The Passphrase Logon window is displayed.
4. Enter the passphrase for this profile ID and select **OK**.

   Note: The passphrase is case sensitive.

Figure 34. Enter passphrase for logon

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

Figure 35. Crypto Adapter Group logon window with passphrase profile ready

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

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

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

You may use the predefined user profile, TKEUSER, for single passphrase logon or another user profile with an equivalent role. If you choose to use passphrase group logon, the TKE Administrator must create a passphrase group profile and add the single user passphrase profiles to the group profile. The passphrase group profile should be mapped to the TKEUSER role or an equivalent role. The single user profiles that will be added to the group profile should be mapped to the DEFAULT role. This is done to limit the services permitted to the single users outside of the group. For details on creating single and group passphrase profiles see Chapter 11, “Cryptographic Node Management utility (CNM),” on page 237.

Smart card and smart card group logon

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

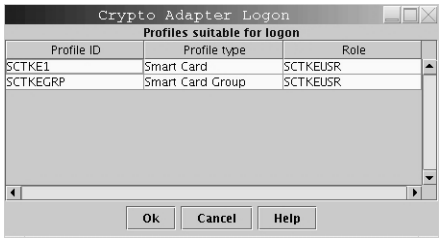


Figure 36. Crypto Adapter Logon Window with smart card profiles

Steps for logging on are:

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

If you selected a single smart card profile ID

1. The Smart Card Logon window will be displayed.
2. Insert the smart card that contains the crypto adapter logon key for the selected profile ID and select **OK**. Both TKE smart cards and EP11 smart cards can contain a TKE workstation crypto adapter logon key.

Figure 37. Insert the smart card

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

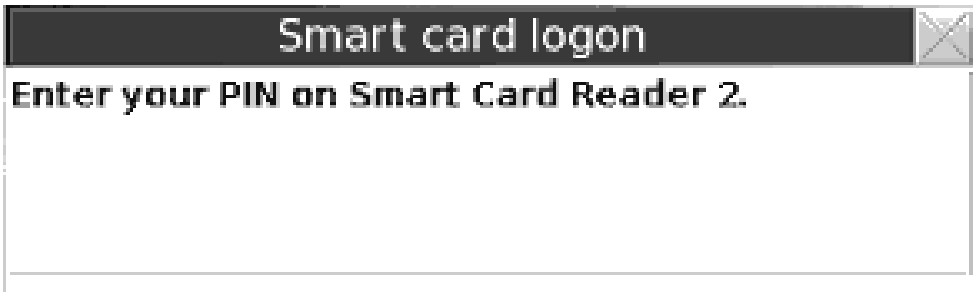


Figure 38. Enter smart card PIN

If you selected a group smart card profile ID

1. The Crypto Adapter Group Logon window will be displayed. This window displays the number of members required for logon and the profile IDs available for logon.

Figure 39. Crypto Adapter Group logon window with smart card profiles

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

   The Smart card logon window is displayed.
4. Insert the smart card that contains the crypto adapter logon key for the selected profile ID and select **OK**. Both TKE smart cards and EP11 smart cards can contain a TKE workstation crypto adapter logon key.

Figure 40. Insert the smart card

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

Figure 41. Crypto Adapter Group logon window with smart card profile ready

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

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

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

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

creating single and group smart card profiles see Chapter 11, “Cryptographic Node Management utility (CNM),” on page 237.

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

Automated crypto module recognition

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

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

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

- A new crypto module has been installed.
- A crypto module has been removed.
- A crypto module has been replaced.
- A new device key has been generated for the crypto module.
- A crypto module has been moved from one slot to another.

Authenticating host crypto modules

The TKE workstation uses the Crypto Module ID (CMID) and the public crypto module device key to verify messages returned from a host crypto module.

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

On the Authenticate crypto module window:

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

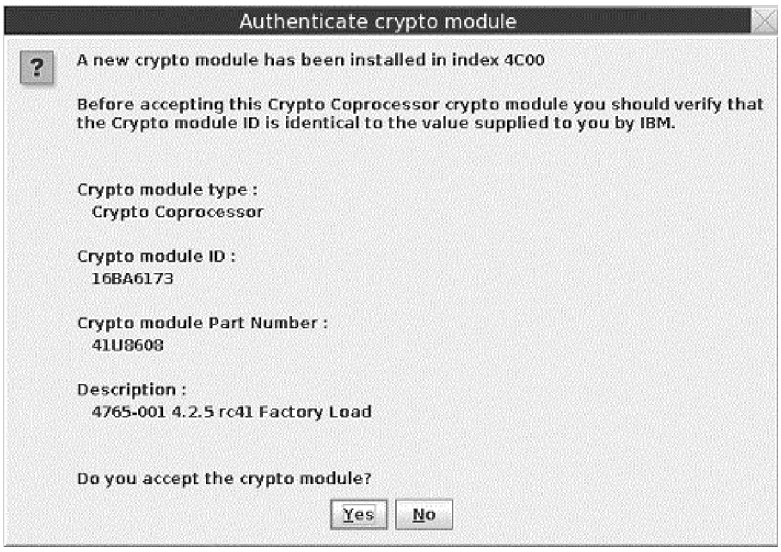


Figure 42. Authenticate Crypto Module

The crypto module type for all currently supported host crypto modules is "Crypto Coprocessor". Prior versions of TKE could manage other crypto module types that are no longer supported.

It is not necessary to authenticate the public crypto module device key. The device key 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 a 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 to back up” on page 101 and “Host file to back up” on page 102

102. 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. See “Backup critical console data” on page 343 and “TKE File Management utility” on page 332 for more information.

Workstation files to back up

The following TKE workstation data 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 and public crypto module device key for each crypto module.
- domaingroup.dat — contains definitions for domain groups.
- desstore.dat and desstore.dat.NDX— DES Key Storage used to hold EXPORTER keys for encrypting RSA keys.
- pkastore.dat and pkastore.dat.NDX — PKA Key Storage used to hold one authority signature key.
- aesstore.dat and aesstore.dat.NDX — AES Key Storage used to hold EXPORTER keys for encrypting RSA keys.
- 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 should also be backed up. These are:

- Passphrase
  - default_80.rol
  - tempdefault_80.rol
  - tkeusr_80.rol
  - tkeadm_80.rol
  - keyman1_80.rol
  - keyman2_80.rol
  - tkeuser.pro
  - tkeadm.pro
  - keyman1.pro
  - keyman2.pro
- Smart card
  - default_80.rol
  - tempdefault_80.rol
  - sctkeusr_80.rol
  - sctkeadm_80.rol
  - sctkeusr.pro
  - sctkeadm.pro

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

Host file to back up

On the z/OS host system, one file (or data set as it is referred to on z/OS) should be saved. The saved file is the name of the crypto module data set 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 61).

- Name of the crypto module data set — 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 61.

Chapter 6. Main window

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

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

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

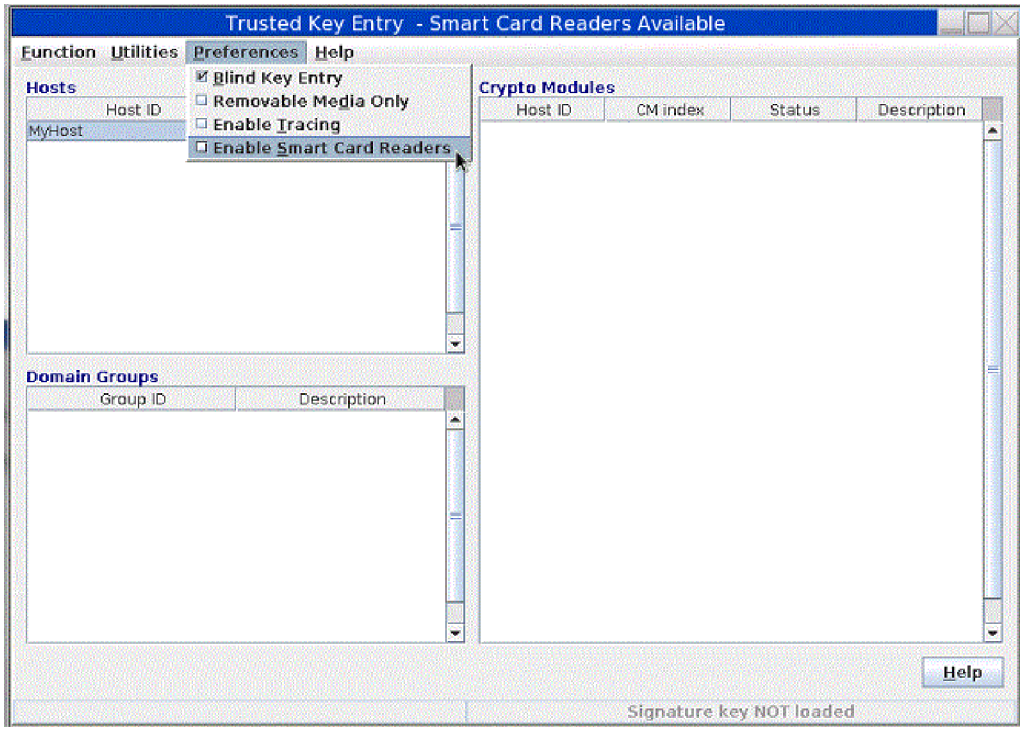


Figure 43. TKE Preferences

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 128.

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

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

When you have created one or more hosts, decide whether you will be working with single crypto modules or with domain groups. To work with domain groups,

right click in the Domain Groups container to display a popup menu. The popup menu contains options to create, change, delete, and open domain groups.

To open a crypto module notebook for a single crypto module, open a host. (Left click on it once and select the Open Host option, or double click on it with the left mouse button.) After you log on to the host, TKE queries it and displays a list of the attached host crypto modules in the Crypto Modules window. To open a crypto module notebook, left click on one of the host crypto modules and select Open Crypto Module, or double click on it with the left mouse button.

To open a crypto module notebook for a domain group, left click on the group once and select the Open Group option, or double click on it with the left mouse button. You are prompted to log on to all host systems with crypto modules that are part of the group. A list of the crypto modules that are part of the group is displayed in the Crypto Modules container. Left click in this list once and select Open Domain Group, or double click on it with the left mouse button.

Note: Support for crypto module groups has been removed beginning with TKE 8.0. If any crypto module groups are defined on your TKE workstation, a fourth container is displayed in the main window, labeled Crypto Module Groups. Right-clicking in this container causes a popup menu to be displayed, but the only options are to delete the group or convert the group to a domain group. See "Crypto module groups" on page 116 for more information.

Note the message in the lower right corner that the signature key is not loaded. See "Load signature key" on page 117.

Working with hosts

The Hosts container of the TKE Main Window lists the host IDs currently defined to the TKE workstation. You can create, change, delete, open, or close host definitions from this container. When you select your host (by double-clicking or selecting open), the host logon window opens if you are not yet logged on. When you are logged on, the crypto modules available for that specific host are displayed in the crypto module container.

Beginning in TKE 7.3, your TKE workstation profile's role must have the Manage Host List ACP to be able to create, change, or delete a host list entry.

Creating a host

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

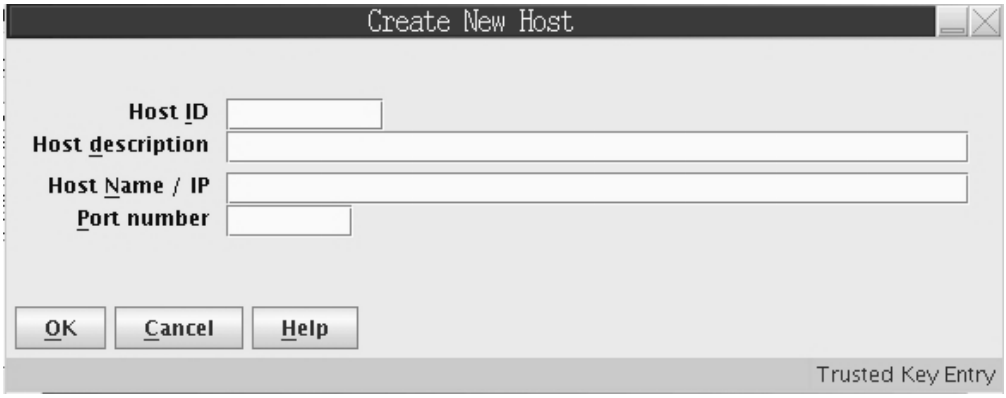


Figure 44. Create Host

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 61.

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.

Logging on to a host

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

The Logon panel is displayed for the host logon.

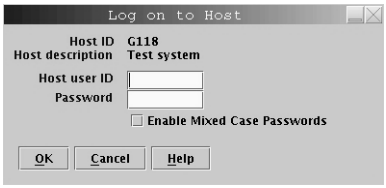


Figure 45. Host Logon window

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 are used as entered and are not automatically 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.

Closing a host

To close a host, in the hosts container right-click the host that you want to close. Then, click **Close host**.

Close a host when you are done working with the crypto modules in the host. The next time that you open the host, a logon is required.

Understanding crypto modules and domain groups

The term *crypto module* refers to one of TKE's supported cryptographic coprocessors (CEX2C, CEX3C, CEX4C, CEX5C, CEX4P, CEX5P). Master keys are installed in domains in the coprocessor, and some coprocessors support up to 85 physical domains.

You can use the TKE Main Window to list the crypto modules available on each host machine to which the TKE Workstation is connected. From the TKE Main Window, you can open the Crypto Module Notebook to display and change all information related to a crypto module, and to issue commands to a crypto module. It is important to understand that some of the information and commands are *module scoped* and some are *domain scoped*.

- The term *module scoped* refers to information or commands that apply to an entire crypto module. For example, there is only one set of Roles and Authorities on a crypto module. Similarly, there are commands that apply to the entire crypto module (such as commands to enable or disable a module).
- The term *domain scoped* refers to information or commands that apply to a domain on a crypto module. For example, each domain on a crypto module has

its own set of master keys and domain controls. Similarly, there are some commands that apply to a specific domain (such as the command to zeroize a domain).

To make the administration of crypto modules easier, you can use the TKE Main Window to organize crypto modules and domains into domain groups. A *domain group* enables you to use a notebook to administer a set of crypto modules and domains as a single unit. For example, you could set the same master key value for a set of domains as easily as setting the master key value for a single domain.

You can create domain groups that contain either CCA host crypto modules or EP11 host crypto modules, but you cannot create a domain group that includes both types of host crypto modules.

Although working with domain groups can be an easier and less error-prone way to administer sets of crypto modules and domains, you need to understand how the module-scoped commands and domain-scoped commands work when issued against a domain group.

You create **domain groups** through the Domain Groups container in the TKE Main Window. When you right click in this container, a dialog box appears. Using this dialog box, you specify the set of domains you want to manage as a unit. The domains can be selected from multiple crypto modules. When you create a domain group, you designate one domain as the *master domain*. When you open a notebook for a domain group, the module-scoped information displayed in the notebook is collected from the crypto module that contains the master domain. The domain-scoped information displayed in the notebook is collected from the master domain.

When you issue a **module-scoped command** against a domain group, the command is sent to each crypto module that contains a domain in the group. For example, if you issue the command to create authority index 10, the authority index will be created in each crypto module in the group. If all of the domains are on the same crypto module, the command is run against just that crypto module.

When a notebook is open for a domain group, information is displayed only for the master domain of the group. When you issue a **domain-scoped command** against a domain group, it is normally sent to every domain in the domain group. For example, if you issue Clear New AES Master Key against the domain group, the AES master key will be cleared in each domain in the domain group. The exceptions are commands on operational keys, which are executed only on the master domain.

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 46 on page 108 illustrates the main window after logging on to a host. Note that in this screen capture, the signature key has not been loaded. To load a signature key, refer to “Load signature key” on page 117.

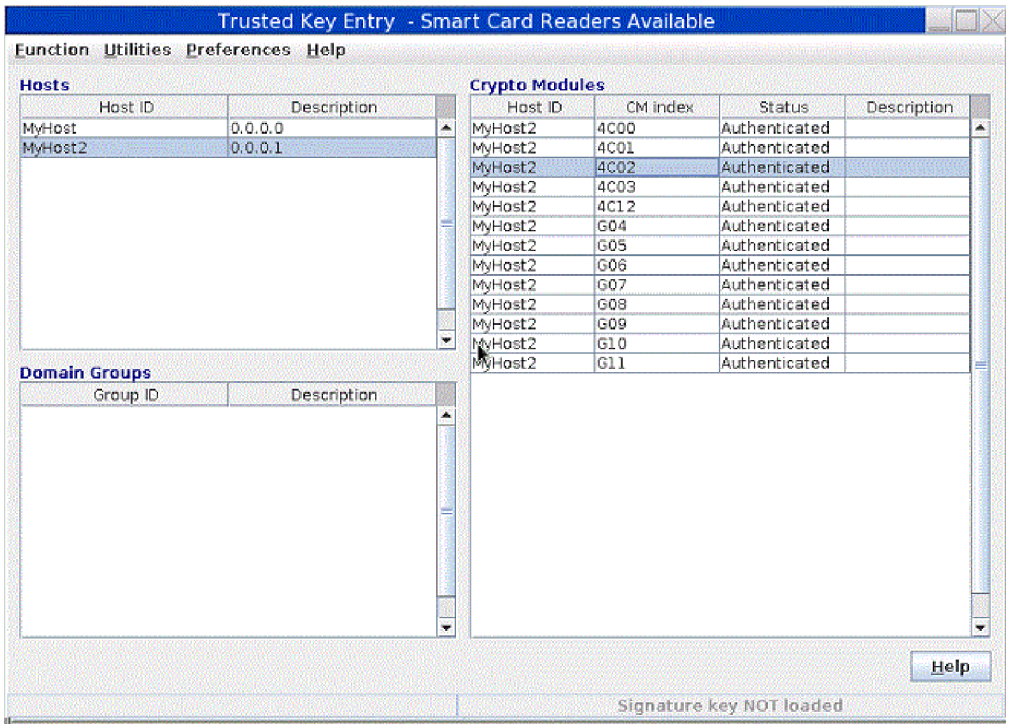


Figure 46. Main window

As discussed in "Automated crypto module recognition" on page 99, 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 domain groups

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

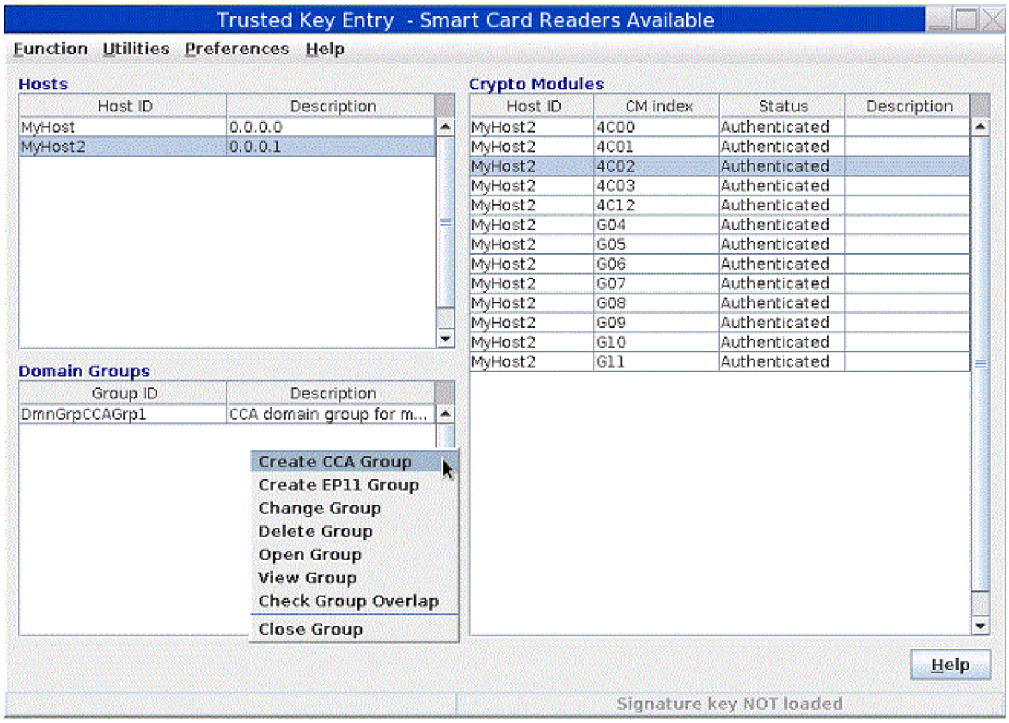


Figure 47. Main window - working with domain groups

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

A domain group can contain domains on one or more crypto modules configured with CCA firmware or else can contain domains on one or more crypto modules configured with EP11 firmware. A domain group cannot contain a mixture of CCA-configured and EP11-configured domains.

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

For most operations, it is important that the crypto modules and domains within a domain group are in the same state. For example, the crypto modules have identical roles and domains have the same master keys. You maintain this by always working on members of the domain group using the domain group interface, and not operating on the crypto modules individually.

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

When you work with a domain group, either 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.

When loading operational key parts using a CCA domain group, only the master domain is changed even if there are other domains in the domain group.

Creating a domain group

You can create a domain group containing domains on one or more crypto modules configured with CCA firmware, or else containing domains on one or more crypto modules configured with EP11 firmware. A domain group cannot contain a mixture of CCA crypto module domains and EP11 crypto module domains.

To create a new domain group:

1. Right-click the mouse button in the Domain Groups container.

   A popup menu displays.
2. To create a domain group containing domains from CCA crypto modules, select the **Create New CCA Domain Group** menu item. To create a domain group containing domains from EP11 crypto modules, select the **Create New EP11 Domain Group** menu item.

   The "Create New Group" window opens.

   Note: For CCA domain groups, the supported crypto module types are CEX2C, CEX3C, CEX4C, and CEX5C. For EP11 domain groups, the supported crypto module types are CEX4P and CEX5P.

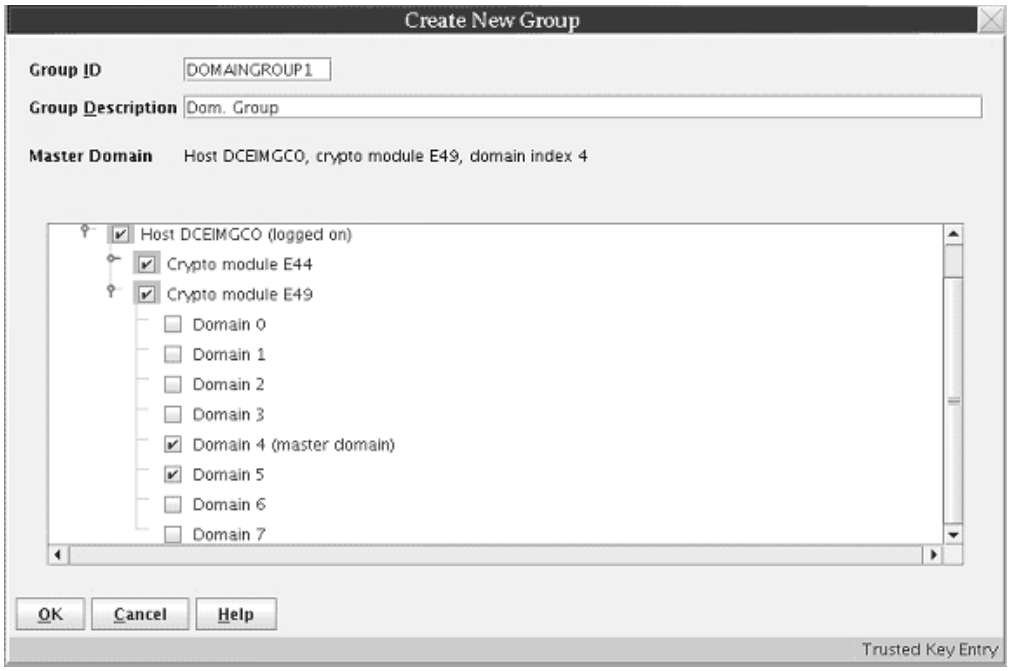


Figure 48. Create Domain Group

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 or hosts if you are not currently logged on.

      Note: Only domains defined as control domains on the crypto module will be available for inclusion in the domain group.
   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.
   e. When finished, press **OK**.

Notes:

1. Crypto modules at different CCA levels may support different features. For example, ECC (APKA) master keys were introduced with the CEX3C crypto module and restricted PIN support was introduced with the CEX4C crypto module. Domain groups can be created using crypto modules at different CCA levels. The notebook for the domain group will reflect the features supported on the crypto module containing the master domain.
2. If the crypto module containing the master domain has capabilities that other crypto modules in the group do not have, what happens during a group operation depends on the specific command executed. Commands to clear and load the AES and ECC (APKA) master keys are ignored on crypto modules that do not support those master key types. All other commands, such as commands to manage decimalization tables and restricted PINs, are attempted on all domains in the group and will fail on crypto modules that do not support those operations.

Changing a domain group

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

The Change Group window is displayed.

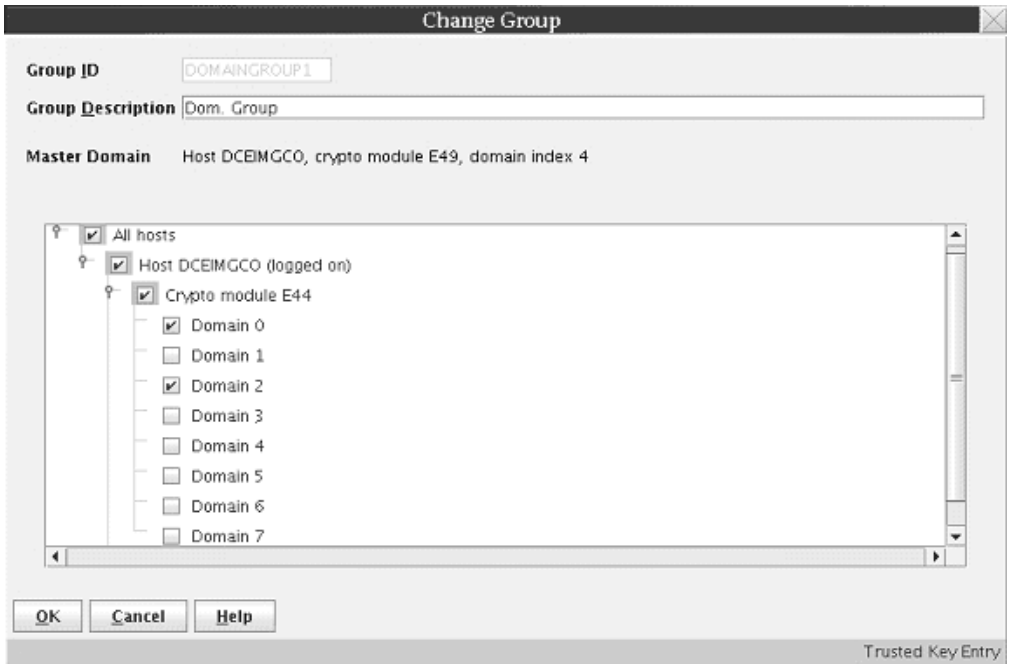


Figure 49. Change Domain Group

To change the description, edit the **Group Description** field.

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

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

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

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

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

One domain must be selected as the master domain.

When finished, press **OK**.

Viewing a domain group

To view a domain group, either right click in the “Domain Groups” container in the TKE main window and select the **View Group** action or open a domain group and press the **View Group** button on the Domain -> General tab.

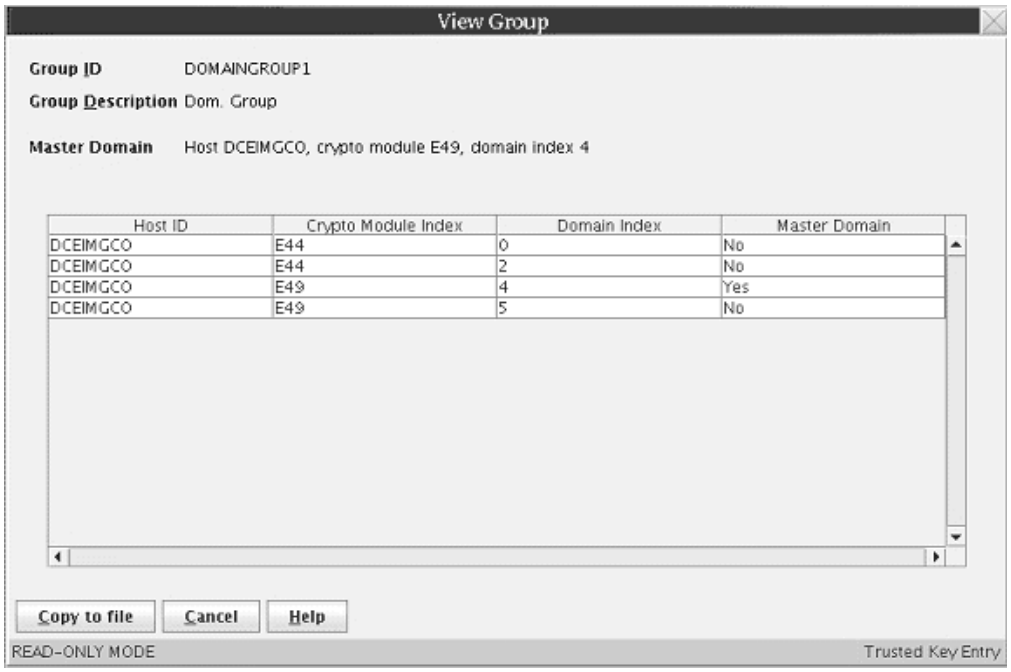


Figure 50. View Domain Group

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

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

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

Checking domain group overlap

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

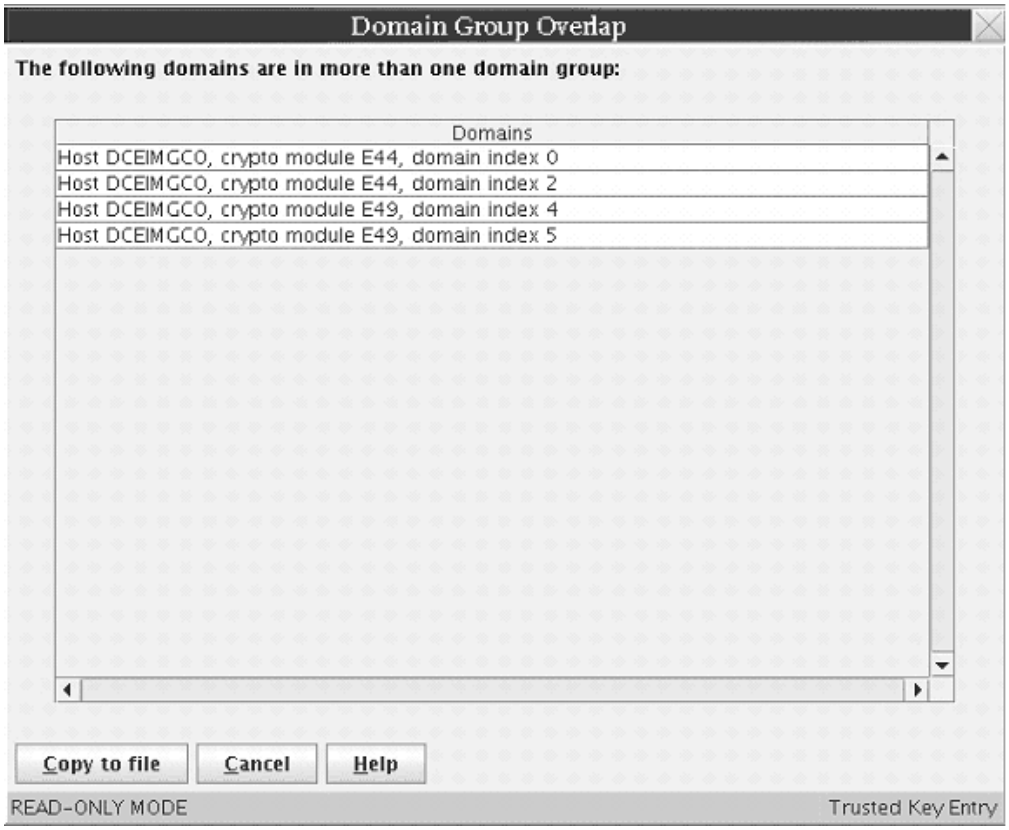


Figure 51. Check Domain Group Overlap

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

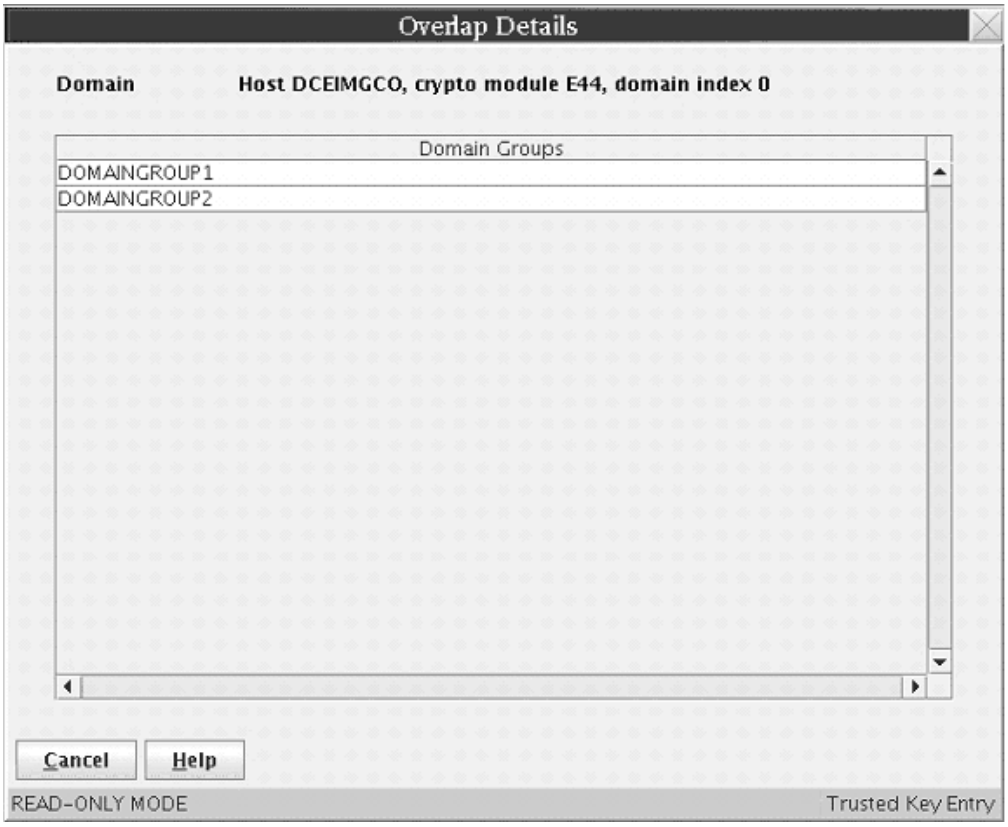


Figure 52. Domain Group Overlap Details

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

Comparing groups

In order for operations on a domain group to be successful, all member domains need to be configured the same. For example, the status of a master key register needs to be the same in each domain of a domain group in order for an operation on that master key register to have the same result in each member domain.

The Group Compare function reads the state of the domains and crypto modules in a domain group and checks for differences. To run the group compare function, open the domain group, click on the **Function** menu at the top of the domain group notebook, and select **Compare Group**.

TKE reads and compares the state of all domains and crypto modules in the group. If differences are found, a Group Compare window is displayed showing the differences.

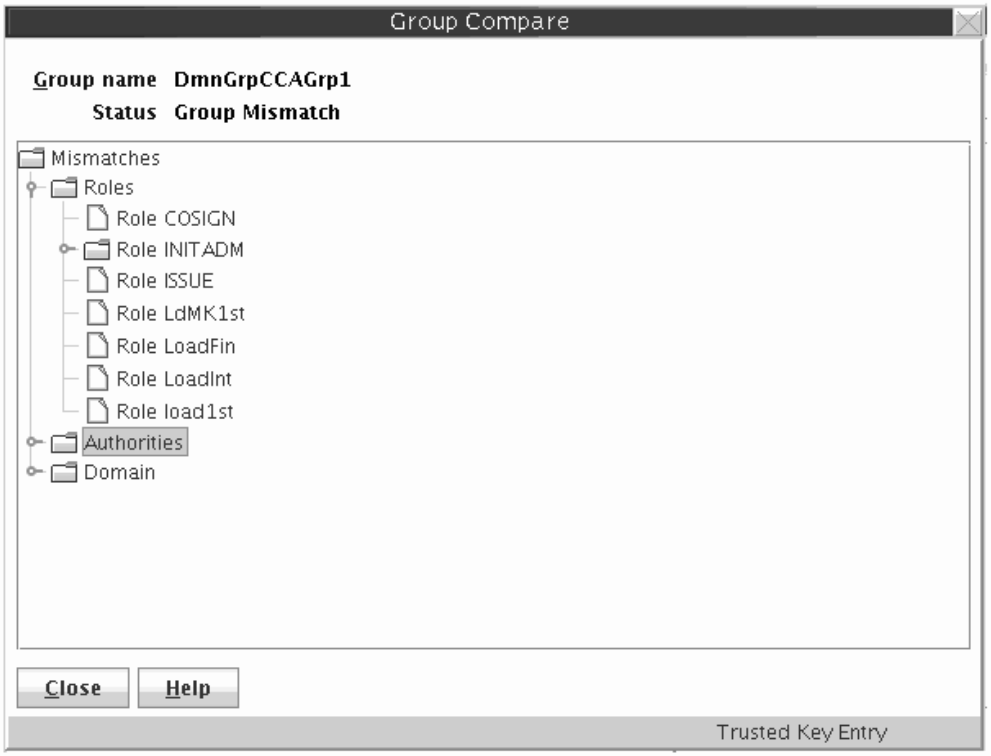


Figure 53. Compare Group

The Group Compare window displays the following results:

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

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

TKE functions supporting domain groups

The values displayed in a domain group notebook are those read from the master domain, or from the crypto module that contains the master domain. In general, updates made in a domain group notebook are made in all member domains or member crypto modules of the group. For CCA domain groups, the following operations are performed only on the master domain:

- Load operational key part to key part register
- View operational key part registers
- Clear operational key part registers

Nearly all operations that can be performed in a crypto module notebook can also be performed in a domain group notebook. The only exception is for CCA domain groups. When creating or changing a role, users are not allowed to directly manage the domain access ACPs. These are automatically set to give the role access to all members of the group.

Crypto module groups

The Trusted Key Entry workstation no longer supports crypto module groups. To manage a group of crypto modules, a domain group can be created instead.

To assist users in converting from crypto module groups to domain groups, TKE provides a utility to create domain groups from crypto module groups. The utility is invoked as part of the TKE Workstation Setup wizard. From the utility, users select a crypto module group to be converted. The utility displays a proposed domain group for the crypto module group, and users may either accept this definition or make changes before creating the domain group.

Crypto module groups can also be converted to domain groups from the main TKE application. If at least one crypto module group is defined on the TKE workstation, the main TKE application displays a Crypto Module Groups container. From this container, you can select a crypto module group and either delete it or convert it to a domain group.

If no crypto module groups are defined on the TKE workstation, a Crypto Module Groups container is not displayed in the main TKE application.

Function menu

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

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

Load signature key

This function is used to load the authority signature key. Authority signature keys are used when managing CCA host crypto modules. The authority signature key is active for all operations until explicitly changed by clicking on this option again to load a different authority signature key, or until the signature key is unloaded.

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

The CEX2C supports only 1024-bit RSA authority signature keys. CEX3C and CEX4C host crypto modules support 1024-bit, 2048-bit and 4096-bit RSA authority signature keys. CEX5C host crypto modules support 1024-bit, 2048-bit, and 4096-bit RSA authority signature keys, and BP-320 ECC authority signature keys.

To create an authority signature key, see “Generating authority signature keys” on page 139.

A Select Source window opens. Select the source of the authority signature key, and click **Continue**.

Notes:

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

- Starting in TKE 7.2, the TKE supports 2, 3 or 4 smart card readers.

Figure 54. Select Authority Signature Key Source

- If you select **Key storage** or **Default key** as the authority signature key source, the **Specify authority index** window opens. Enter the authority index to be used, and click **Continue**.

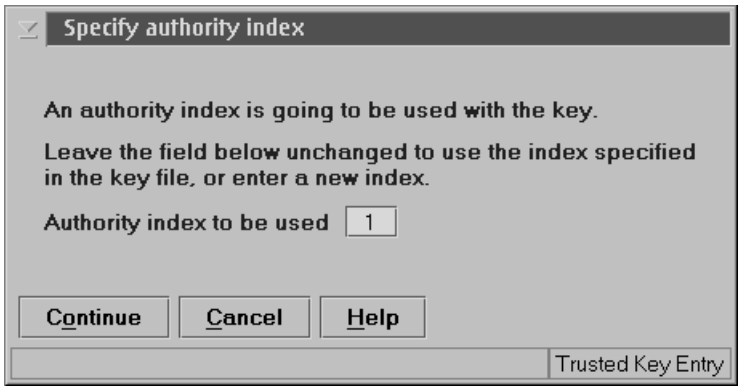


Figure 55. Specify Authority Index

- If you select **Binary file** as the authority signature key source, the Load Signature Key window opens. The authority signature key must have been previously generated and saved to a binary file. Either select a file from the **Files** list or enter a file name. Additionally, you must enter a password.

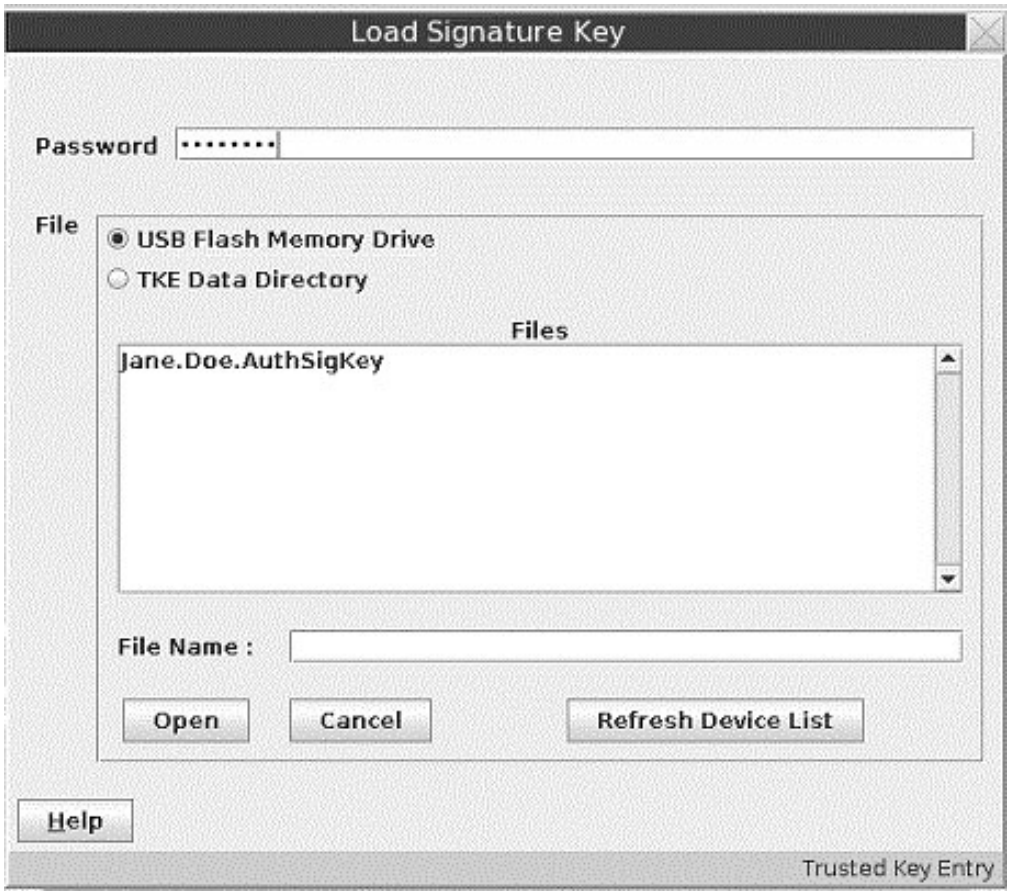


Figure 56. Load Signature Key

You are then prompted to specify the authority index.

- If you select **Smart card in reader 1** or **Smart card in reader 2**, you are prompted to insert your TKE smart card into the smart card reader. You are then prompted to enter the PIN on the TKE smart card reader's PIN pad.

You will then be prompted to specify the authority index.

Unload signature key

This function unloads the authority signature key. Use this function when you are finished using the key and want to ensure that the key is not used until it is loaded again.

Display signature key information

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

Define transport key policy

For CCA host crypto modules, master keys and operational keys are protected by encryption during transfer between the TKE workstation crypto adapter and host crypto modules. The transport encryption keys (key-encrypting keys) are

established by means of a Diffie-Hellman key agreement mechanism. The Select Transport Key Policy Window lets you select the policy for the transport key.

For EP11 host crypto modules, master keys are also protected by encryption during transfer between the TKE workstation and host crypto modules, but a different mechanism is used. The policy selected by the Select Transport Key Policy Window does not apply to EP11 host crypto modules.

For CCA host crypto modules, TKE supports two Diffie-Hellman key agreement protocols: Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH). DH is used when TKE sends key material to a CCA host crypto module with a CCA level earlier than 4.2. ECDH is used when the host crypto module has a CCA level of 4.2 or greater.

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

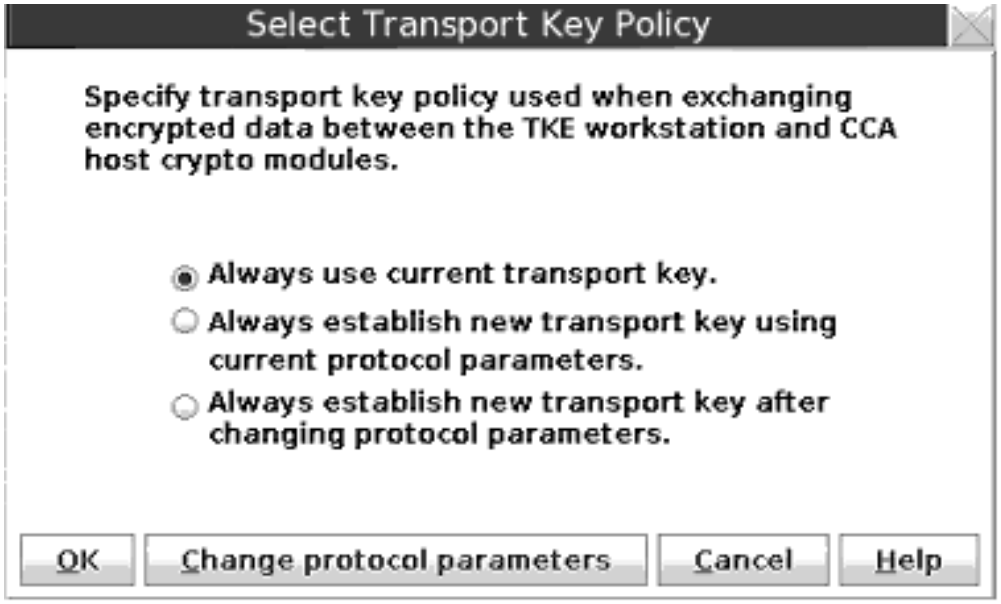


Figure 57. Select Transport Key Policy

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 clicking **Change protocol parameters**. For ECDH, **Change protocol parameters** forces the TKE to use different ECDH parameters and causes TKE to establish a new transport key when needed using the new ECDH parameters.

Exit

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

Exit and logoff

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

Utilities menu

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

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

These utilities are used for managing the keys in TKE workstation DES, PKA, and AES key storage, managing smart card contents, and copying smart card contents. The **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.

Manage workstation DES keys

TKE workstation DES key storage is used to hold DES IMP-PKA keys that encrypt RSA keys for transfer to host systems. DES IMP-PKA keys can be loaded into TKE workstation DES key storage using an option on the Domain Keys page in the crypto module notebook. When DES IMP-PKA keys are loaded into TKE key storage, the key type is changed from IMP-PKA to EXPORTER.

This option lets you view and delete keys in TKE workstation DES key storage.

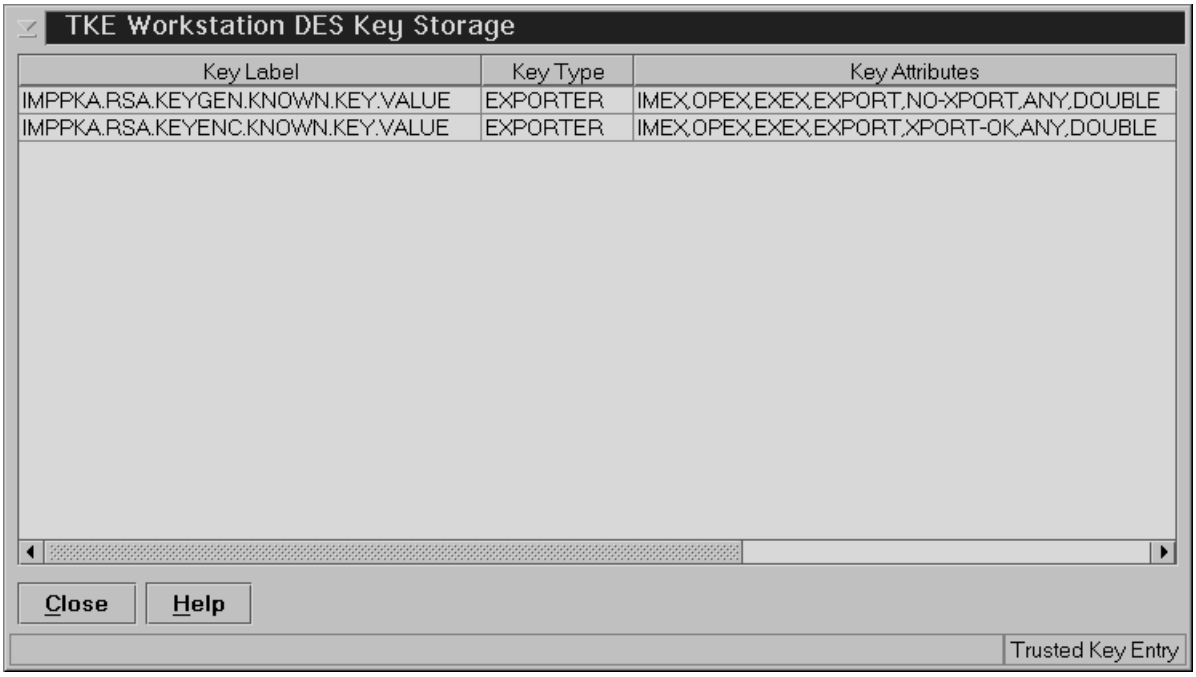


Figure 58. TKE Workstation DES Key Storage Window

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

- Key label
- Key type

  DES IMP-PKA keys written to key storage have the key type *EXPORTER*. Keys with key type *NO_KEY* are empty and can be deleted. There might be other key types if the TKE workstation crypto adapter is used for purposes other than TKE.
- Key Attributes

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

Deleting an entry

When you 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 RSA signature key.

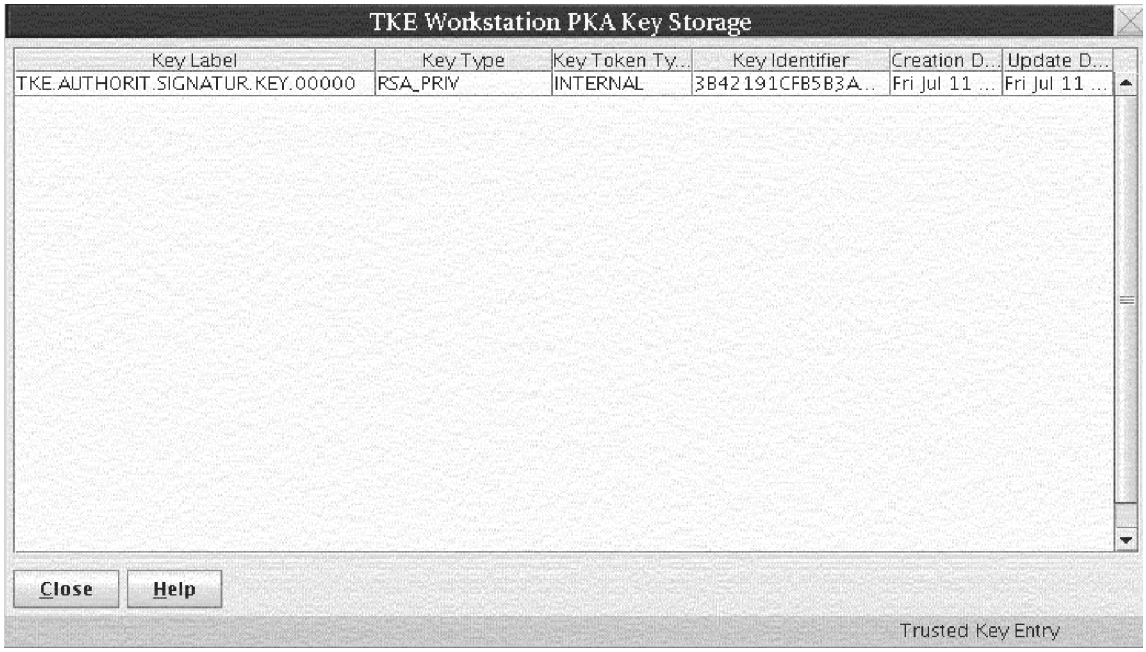


Figure 59. TKE Workstation PKA Key Storage Window

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 workstation AES keys

TKE workstation AES key storage is used to hold AES IMPORTER keys that encrypt RSA keys for transfer to host systems. AES IMPORTER keys can be loaded into TKE workstation AES key storage using an option on the Domain Keys page in the crypto module notebook. When AES IMPORTER keys are loaded into TKE key storage, the key type is changed from IMPORTER to EXPORTER.

This option lets you view and delete keys in TKE workstation AES key storage.

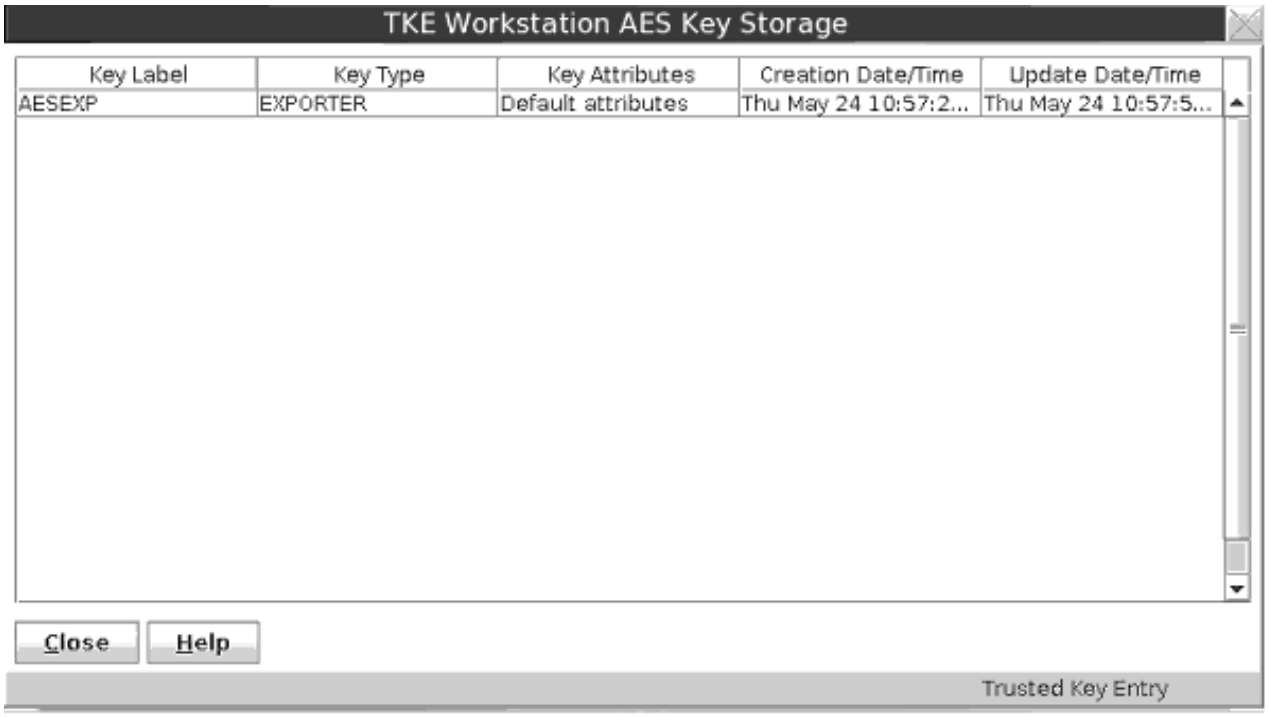


Figure 60. TKE Workstation AES Key Storage window

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

- Key label
- Key type

  AES IMPORTER keys written to key storage have the key type EXPORTER. Keys with key type NO_KEY are empty and can be deleted.
- Key attributes

  Indicates whether the AES EXPORTER key has default or custom attributes. You can display the specific key attributes by selecting an entry and right-clicking to display a popup menu. Select **Display key attributes** to view the attributes of the selected key.
- Created date and time
- Updated date and time

Deleting an entry

When you select an entry, and right-click, a popup menu is displayed. Select **Delete Key** to permanently delete a key from key storage.

Manage smart cards

This function allows you to view a list of the keys and key parts stored on the smart card, delete keys and key parts from the smart card, and, for TKE smart cards, display information about AES EXPORTER, IMPORTER, and CIPHER operational keys stored on the smart card. This function can be used with both TKE smart cards and EP11 smart cards.

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

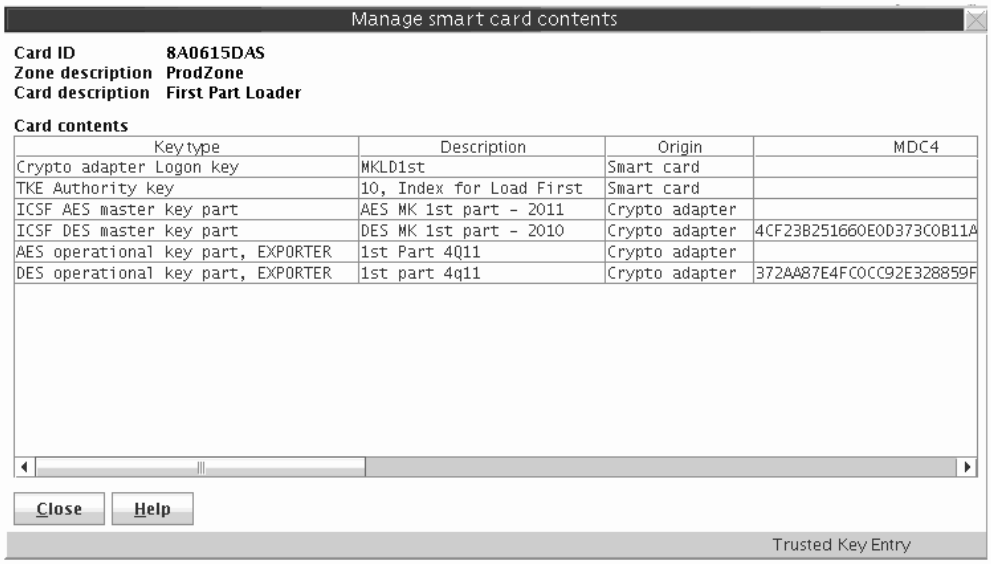


Figure 61. Smart card contents (for TKE smart cards)

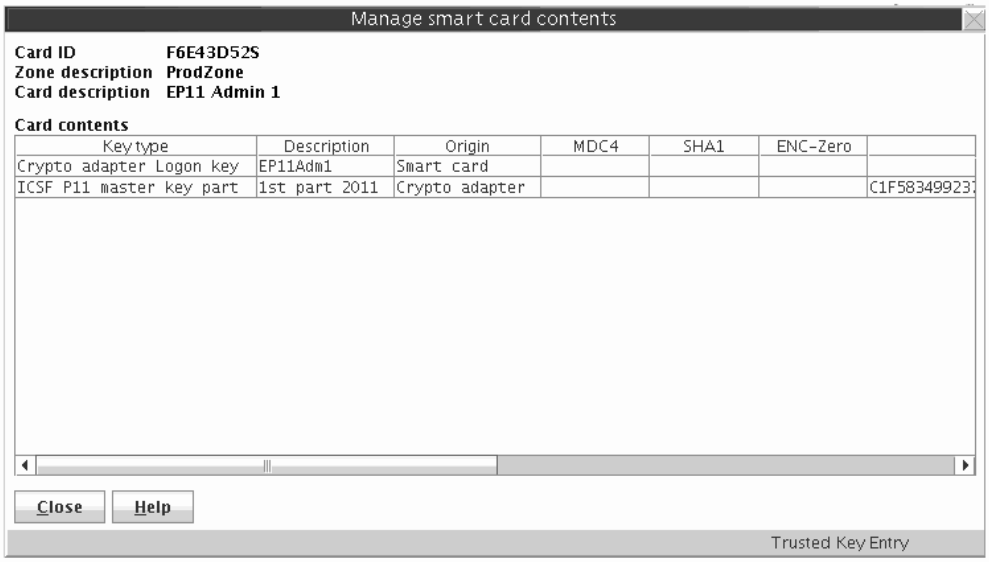


Figure 62. Smart card contents (for EP11 smart cards)

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

Card ID
Identification string for the smart card

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

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

Card contents
Key type, Description, Origin, MDC4, 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, or from one EP11 smart card to another EP11 smart card. You can copy these types of keys:

- Crypto adapter logon key
- TKE authority signature key
- EP11 administrator signature key
- ICSF operational key parts
- ICSF master key parts
- Crypto adapter master key parts

Notes:

1. The two smart cards must be enrolled in the same zone; otherwise the copy will fail. To display the zone of a smart card, exit from the TKE application and use either the Cryptographic Node Management Utility or the Smart Card Utility Program found in the Trusted Key Entry category's Applications list on the TKE Workstation Console. See Chapter 11, “Cryptographic Node Management utility (CNM),” on page 237 or Chapter 12, “Smart Card Utility Program (SCUP),” on page 279.
2. To copy ECC (APKA) master key parts from a source TKE smart card to a target TKE smart card, the applet version of the target TKE smart card must be 0.6 or greater.
3. To copy an ECC authority signature key from a source TKE smart card to a target TKE smart card, the version of the target TKE smart card must be 0.10 or greater.

To copy a smart card:

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

   A message box prompts you to “Insert source TKE or EP11 smart card in smart card reader 1”.
2. Insert the source smart card in smart card reader 1 and press **OK**.

   A message box prompts you to insert the target smart card in smart card reader 2. The target smart card must be the same type (TKE or EP11) as the source card.
3. Insert the target smart card in smart card reader 2 and press **OK**.

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

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

   Card ID
   Identification string for the smart card

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

   Card description
   Description of the smart card; 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 smart card. If there is not enough room on the target smart card, you will get an error message. You can either delete some of the keys on the target smart card (see "Manage smart cards" on page 125) or use a different smart card.

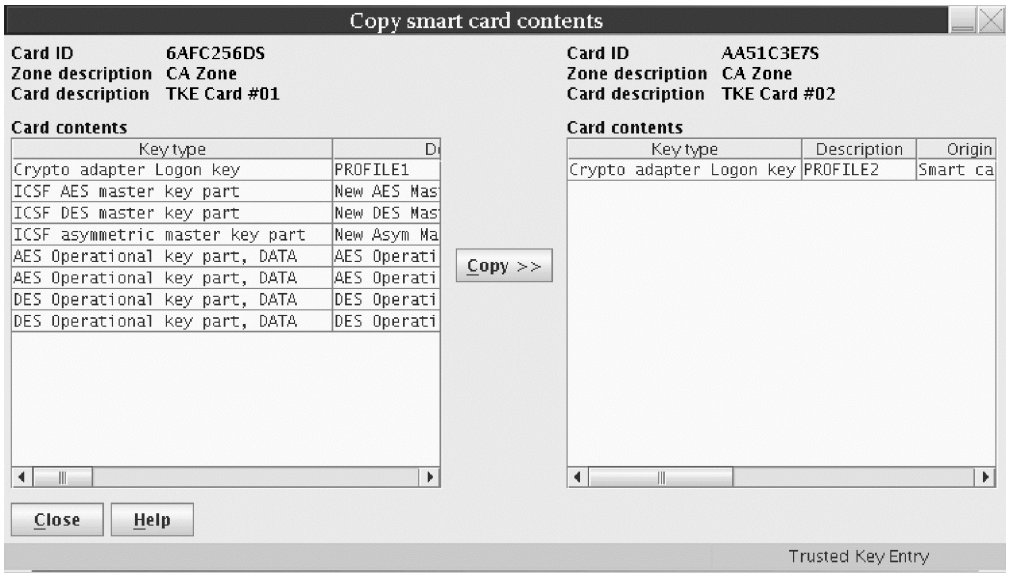


Figure 63. Select keys to copy

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

Note: You can display the key attributes associated with a AES non-DATA operational key part stored on either the source or target TKE 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 whether key values entered at the TKE keyboard are displayed or hidden. With hidden entry, a * character is displayed for each entered hexadecimal character.

Ensure the menu item is checked if you want hidden entry; otherwise uncheck the menu item.

Removable Media Only
Limits file read and write operations to removable media only.

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

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

Notes:

- The TKE application must be closed and reopened for this change to become effective.
- When the TKE workstation crypto adapter is initialized for smart card use, this option is automatically selected.

Chapter 7. Using the Crypto Module Notebook to administer CCA crypto modules

The Crypto Module Notebook is the central point for displaying and changing all information related to a crypto module. It is used for single crypto modules as well as for domain groups. The contents of some of the pages will vary depending on whether you selected a single crypto module or a domain group.

The TKE Main Window lists the crypto modules available on each host machine to which the TKE Workstation is connected and also lists any crypto module groups and domain groups you have created. Double-clicking on a single crypto module or domain group in the TKE Main Window opens the Crypto Module Notebook, which enables you to work with the selected crypto module or domain group. There are two versions of the Crypto Module Notebook — one for CCA crypto modules (CEX2C, CEX3C, CEX4C, and CEX5C) and one for EP11 crypto modules (CEX4P and CEX5P).

This topic describes how to use the Crypto Module Notebook for CCA crypto modules. For information on how to use the Crypto Module Notebook for EP11 crypto modules, refer to Chapter 8, “Using the Crypto Module Notebook to administer EP11 crypto modules,” on page 197.

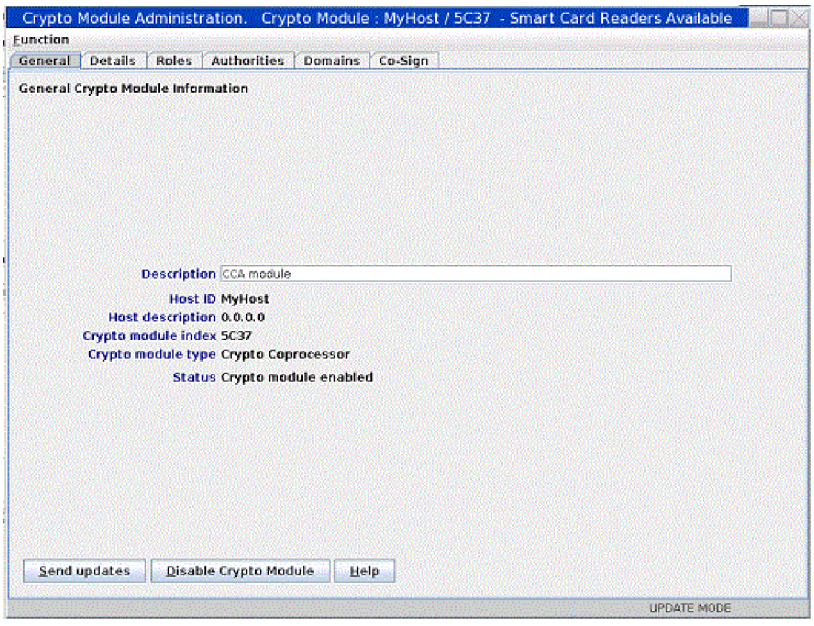


Figure 64. Crypto Module Notebook for CCA - General Page

Notebook mode

The notebook is opened in one of four possible modes:

- **UPDATE MODE**
- **READ-ONLY MODE**
- **PENDING COMMAND MODE**

- **LOCKED READ-ONLY MODE** - group notebooks only

The mode is displayed in the lower-right corner on all of the Crypto Module Notebook pages.

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 195.

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.

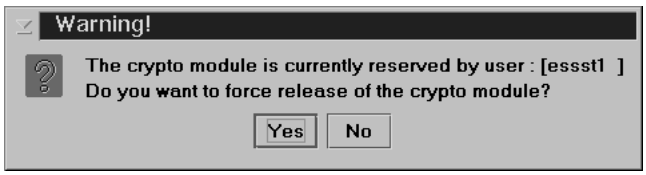


Figure 65. Window to Release Crypto Module

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

Attention: Releasing a crypto module can damage an on-going operation initiated by another authority. Use this option only if you are certain that the crypto module must be released.

- **Compare Group** - This selection is only displayed if working with a domain group. For more information, see "Comparing groups" on page 115.
- **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 134.
- **Roles:** see "Crypto Module Notebook Roles tab" on page 136.
- **Authorities:** see "Crypto Module Notebook Authorities tab" on page 139.
- **Domains:** see "Crypto Module Notebook Domains tab" on page 146.
- **Co-sign:** see "Crypto Module Notebook Co-Sign tab" on page 195.

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 ID**
- **Host 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.
- **Crypto Module Type**
- **Status**

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

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

If you press the **Disable Crypto Module** push 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** push 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 re-created. The setting for TKE Enablement is also returned to the default value of *Denied* when the intrusion latch is tripped.

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

1. Open an Emulator Session on the TKE workstation and log on to your TSO/E user ID on the Host System where the card will be removed.
2. From the ICSF Primary Option Menu, select Option 1 for Coprocessor Management.
3. Leave the Coprocessor Management panel displayed during the rest of this procedure. You will be required to press ENTER on the Coprocessor Management panel at different times. **DO NOT EXIT this panel.**
4. Open the TKE Host where the card will be removed. Open the crypto module notebook and click on the **Disable Crypto Module** push button.
5. After the crypto module has been disabled within TKE, press ENTER on the ICSF Coprocessor Management panel. The status should change to DISABLED.

   Note: You do not need to deactivate a disabled card before configuring it OFFLINE.
6. **Configure Off** the card from the Support Element. The Support Element is a dedicated workstation used for monitoring and operating 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, press ENTER on the Coprocessor Management panel. The status should change to OFFLINE.
8. Remove the card. Perform whatever operation needs to be done. Replace the card.
9. **Configure On** the card from the Support Element. The Support Element is a dedicated workstation used for monitoring and operating 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, press ENTER on the Coprocessor Management panel. The status should change to DISABLED.
11. From the TKE Workstation Crypto Module General page, click on the **Enable Crypto Module** push button.
12. After the card has been enabled from TKE, press ENTER on the Coprocessor Management panel. The Status should return to its original state. If the Status was ACTIVE in step 2, when the card is enabled it should return to ACTIVE.

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

Crypto Module Notebook Details tab

The Details tab contains 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:** Shows basic information needed to recognize a host crypto module. Different information is displayed, depending on the crypto module type. The following fields may be displayed on this page:
  - **Crypto Module ID** - Unique identifier burned into the crypto module during the manufacturing process.
  - **Public Modulus** - For crypto modules with an RSA device key, the modulus of the key. TKE uses the public key to verify signed replies from the host crypto module.
  - **Modulus Length** - For crypto modules with an RSA device key, the length of the modulus, in bits.
  - **ECC Public Key** - For crypto modules with an ECC device key, the ECC public key.
  - **Key Identifier** - The SHA-256 hash over the public part of the device key. For RSA keys, the hash is over the DER-encoded modulus and public exponent. For ECC keys, the hash is over the ECC public key.
  - **Signature Sequence Number** - Each signed reply from the crypto module contains a unique sequence number; the current value is displayed.
  - **Hash pattern of transport key** - For CEX2C crypto modules, the MDC-4 hash value of the current Diffie-Hellman generated triple-DES transport key for the crypto module. For later crypto modules, the first 16 bytes of the SHA-256 hash value of the current Diffie-Hellman generated AES transport key.
- **Crypto Services (Function Control Vector Values)**
  - Base CCA services availability
  - CDMF availability
  - 56-bit DES availability
  - Triple DES availability
  - 128-bit AES availability
  - 192-bit AES availability
  - 256-bit AES availability
  - SET services
  - Maximum length of RSA keys used to encipher DES keys
  - Maximum elliptic curve field size in bits for key management
- **Other CM Info** - The following crypto module information is displayed:
  - CCA Version
  - CCA Build Date
  - DES Hardware Level
  - RSA Hardware Level
  - Power-On Self Test Version (0,1,2)
  - Operating System Name
  - Operating System Version
  - Part Number
  - Engineering Change Level
  - Miniboot Version (0,1)
  - Adapter ID
  - Processor Speed
  - Flash Memory Size
  - Dynamic RAM Memory Size

  - Battery-Backed Memory Size
- **Diagnostic Info** - The following diagnostic information is displayed:
  - Intrusion Latch
  - Battery State
  - Error Log Status
  - Command Information

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

Crypto Module Notebook Roles tab

CCA crypto modules use role-based authority. Each authority has an associated role. This role indicates what operations the authority is permitted to execute and what domains on the crypto module the authority is permitted to change.

With role-based authority, a set of roles can be defined that correspond to different classes of coprocessor users. For example, one class of users might be permitted to access only test domains, while another class of users might be permitted to access production domains. One class of users might be permitted to perform only key operations, while another class of users might be permitted only to change domain controls.

For key operations, further granularity is possible, with separate controls for loading first, middle, and final key parts, and for setting, completing, and clearing keys. Permission to execute these operations can be assigned to different roles, implying that multiple users are needed to manage keys. Or, one role can indicate permission to execute them all.

You can create, change, and delete roles from the **Roles** tab.

INITADM is a pre-defined role available on coprocessors that are shipped from IBM, or after segments 2 and 3 of the coprocessor are zeroized and unowned (ownership surrendered) and then reloaded. It is assigned to authority 00. It allows you to create an initial set of roles and authorities on the crypto module. After you create these initial roles and authorities, you can choose to delete authority 00 or to assign a different role to it.

Dual-signature commands

To complete some commands, two authority signatures are required. For these commands there are two entries in the Role Access Control Points tree, one indicating issue authority and one indicating co-sign authority. If a role contains both permissions, both signatures are collected automatically when an authority with that role is used to execute the command. If an authority with a role containing only issue authority is used to execute the command, the command is held in a pending command buffer until a signature is collected from a second authority whose role contains the co-sign permission.

When working with a single crypto module, use the **Co-Sign** tab in the notebook to collect the second signature for the command. When working with a domain group, a window opens asking you to co-sign the command.

The following operations are dual-signature commands:

- Enable crypto module

- Access control
  - Create role, change role, and delete role commands
  - Create authority, change authority, and delete authority commands
- Zeroize domain
- Update domain controls

Domain access

When you work with a role by using a crypto module notebook, the Role Access Control Points tree contains a Domain Access category that allows you to specify what domains the role gives permission to change.

When you work with a role by using a domain group notebook, the Role Access Control Points tree does not include a Domain Access category. Instead, three Domain Access options are displayed:

- **Set all Domain Access control points**
- **Set Domain Access control points from group definition**
- **Clear all Domain Access control points**

Selecting the first option causes the role to allow access to all domains on the crypto module, whether or not the domain is a member of the domain group.

Selecting the second option causes the role to allow access only to those domains on the crypto module that are members of the domain group. If the domain group includes domains on more than one crypto module, the Domain Access values can be different on different crypto modules. For example, if the domain group includes domains 0, 1, and 2 on crypto module A and domains 3, 4, and 5 on crypto module B, the role on crypto module A has only domains 0, 1, and 2 set in the Domain Access category, and the role on crypto module B has only domains 3, 4, and 5 set.

Selecting the third option causes the role to remove all domain access to all domains on the crypto module, whether or not the domain is a member of the domain group. Select this option when the role does not have any access control points that require access to domains. A role does not need any domain access if it includes only access control points from these categories:

- Crypto Module Enable
- Access Control
- Configuration Migration

Creating or changing a role

When you right click in the Roles tab container, a menu opens and you can select **Create Role**, **Change Role**, or **Delete Role**.

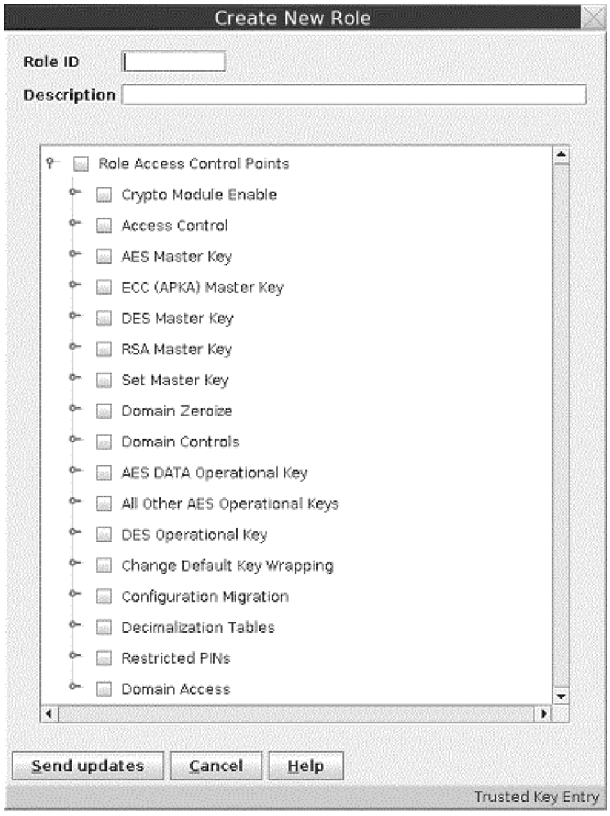


Figure 66. Create New Role page

If you select **Create Role** or **Change Role** from the menu, a window opens displaying the following fields and elements:

- **Role ID**: Enter the Role ID. If you are creating a new role, you must enter a name for that role. If you are changing a role, you cannot change this field.
- **Description** : Optional free text description.
- Tree structure and check boxes: This pane shows the operations and domains that can be allowed or restricted by the role. Figure 66 shows the list of categories. Each category can be expanded to show a list of operations or domains. A check mark indicates that the operation or access to the domain is permitted. The absence of a check mark indicates that the operation or access to the domain is not permitted.

  The Access Control category controls whether an authority can create, change, and delete roles and authorities.

  Dual-signature commands have entries for issue and co-sign authority.

Some categories in the Role Access Control Points tree are not shown if the crypto module does not support the operations in that category. For example, the ECC (APKA) Master Key category is not displayed for crypto modules that do not support ECC (APKA) master keys.

After you complete the fields on the panel and select the operations and domains to be permitted for the role, click **Send Updates** to create or change the role.

Deleting a role

To delete a role, left-click to select the role to be deleted, then right-click to display the menu. Select **Delete role**.

You are not allowed to delete a role if it is currently assigned to one or more authorities. You are only allowed to delete unused roles.

Crypto Module Notebook Authorities tab

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

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

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

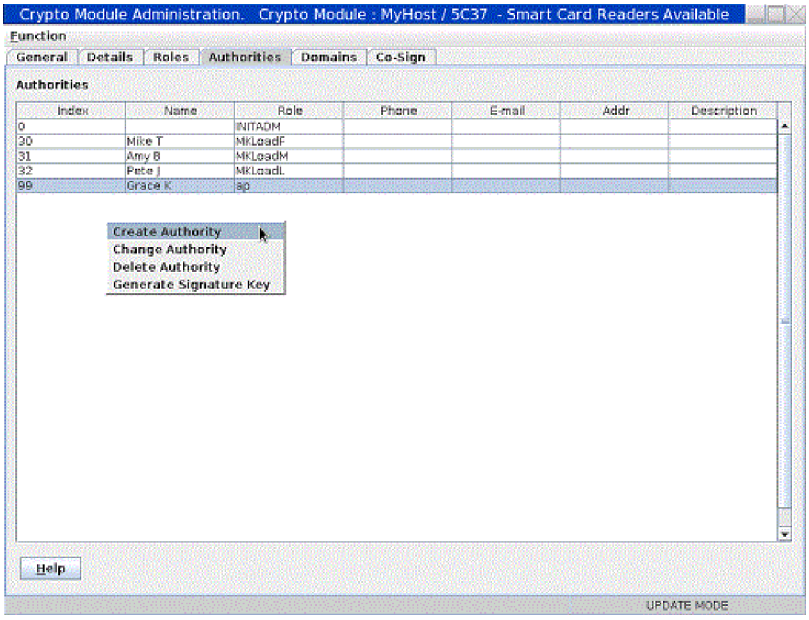


Figure 67. Authorities Page

Generating authority signature keys

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

The Generate Signature Key window is displayed.

Follow this procedure:

1. Enter **Authority index**. This is a mandatory field with the index of the authority. Valid range is 00 through 99. The authority index will be saved with

the key and is called the Default Authority index. The Default Authority index for a saved authority signature key can be overridden when the authority signature key is loaded.

2. Enter **Name**, **Phone**, **E-mail**, **Address** and **Description** to identify the authority. These are optional free text fields. The information that you enter here is saved with the key. It will be filled in automatically when the key is selected for creating a new authority. Press **Continue**.

Figure 68. 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 RSA or BP-320 ECC authority signature keys. BP-320 ECC authority signature keys can only be generated to a TKE smart card with applet version 0.10 or greater. If the signature key target is a binary file or key storage, you can generate 1024-bit, 2048-bit, or 4096-bit RSA authority signature keys.
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.

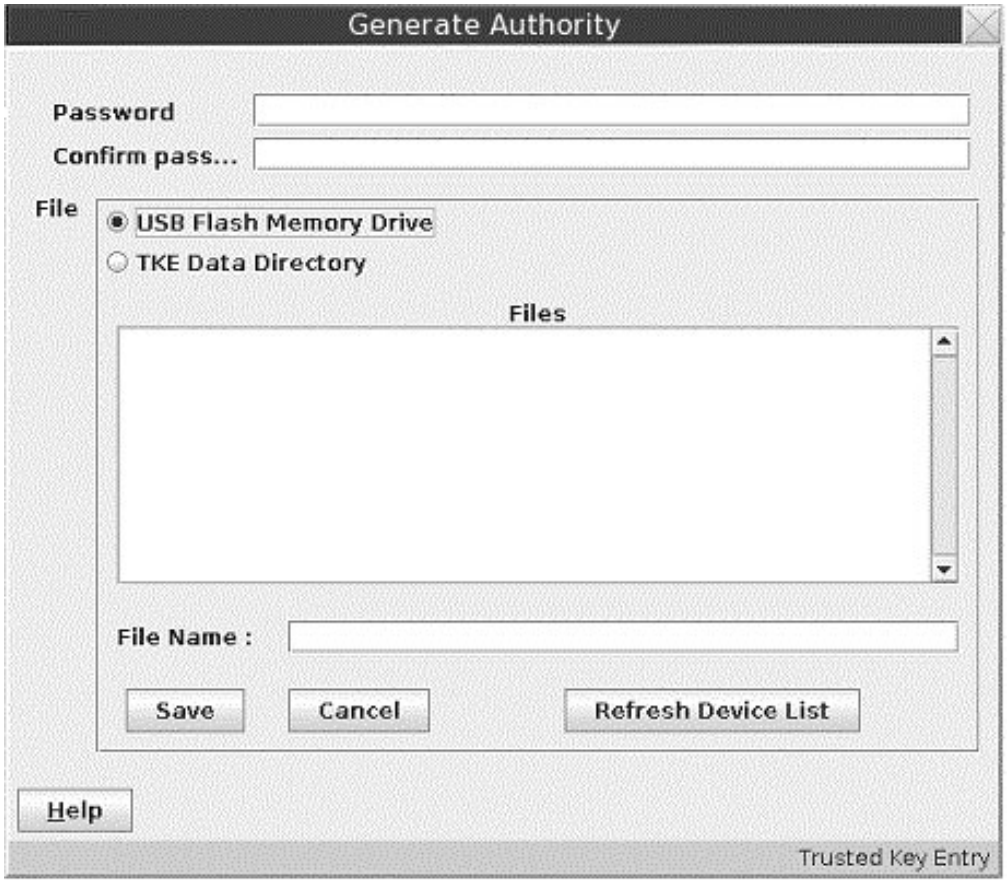


Figure 69. Save authority signature key

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

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.

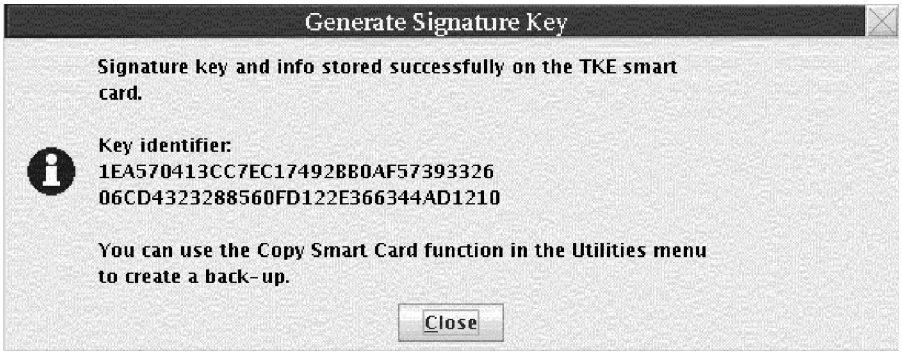


Figure 70. Generate signature key

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 127.

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

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

Figure 71. 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 139).

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** push button.

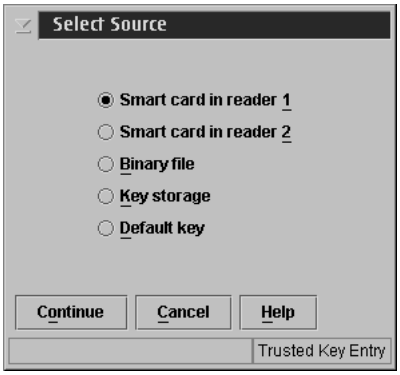


Figure 72. Select source of authority signature key

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

  Notes:

  – Starting in TKE 7.2, you can have 2, 3, or 4 smart card readers. The number of attached smart card readers is detected when the main TKE application starts and controls the options that are displayed on the panel. If no attached smart card readers are detected, no smart card reader options are displayed.

  – BP-320 ECC authority signature keys may be used only on a CEX5C host crypto module.

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

  After the PIN has been verified, the Create New Authority window opens.

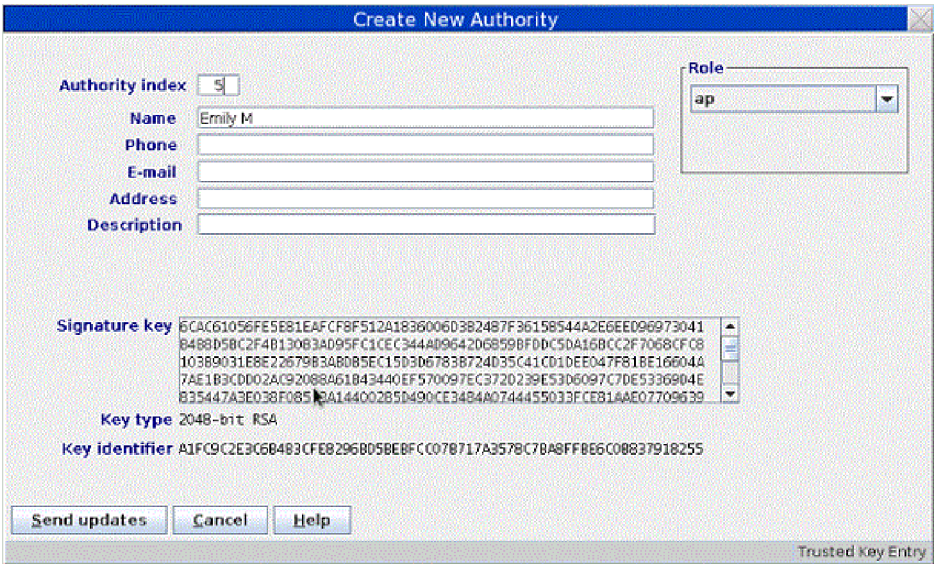


Figure 73. Create new authority

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

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

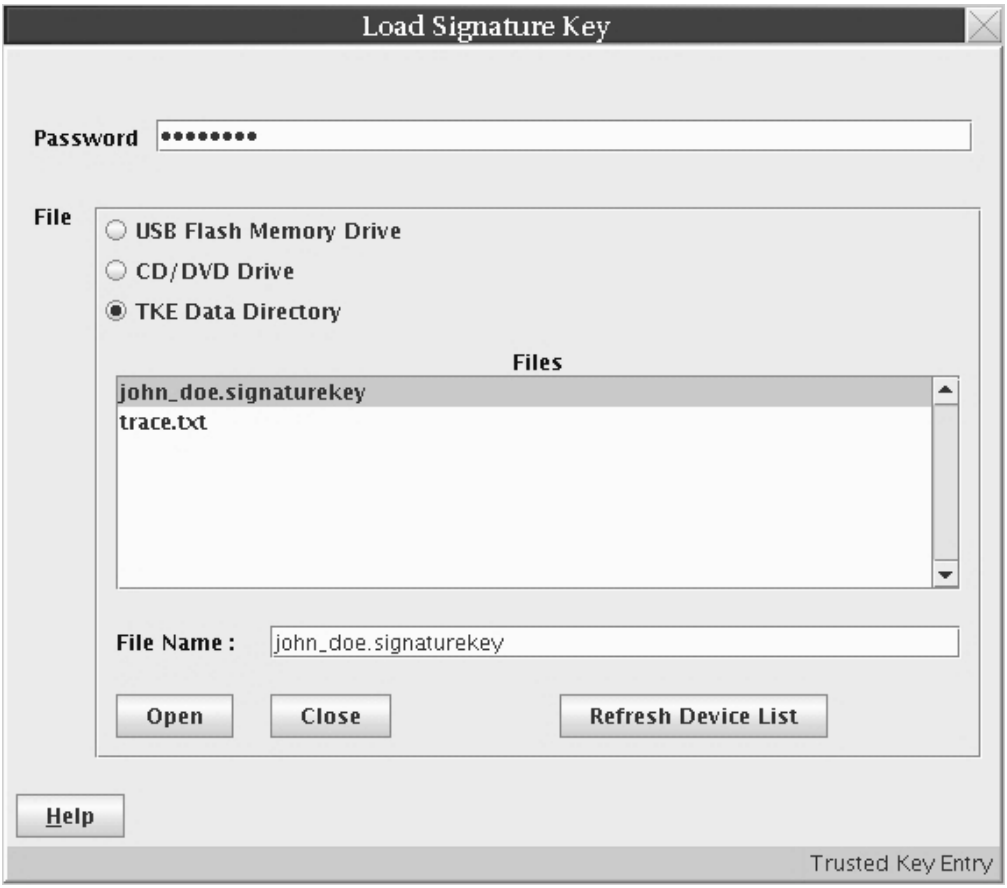


Figure 74. Load Signature Key from binary file

- 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.

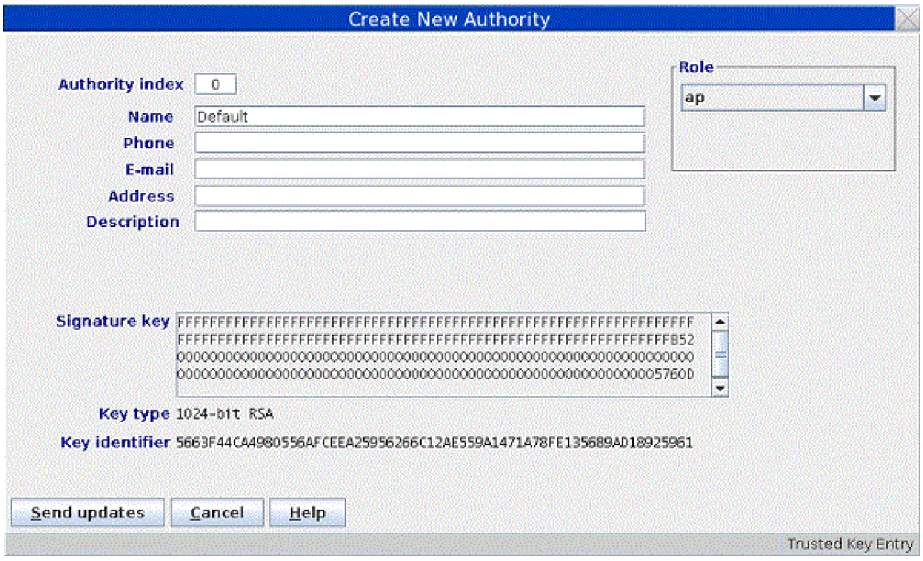


Figure 75. Create New Authority with Role Container

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** - Telephone number of the authority. Optional free text entry field.
- **E-mail** - E-mail address for the authority. Optional free text entry field.
- **Address** - Address of the authority. Optional free text entry field.
- **Description** - Description of the authority. Optional free text entry field.
- **Signature key** - Public modulus of the authority signature key.
- **Key Length** - Length of the authority signature key.
- **Key Identifier** - Identifier for the authority signature key 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, telephone, e-mail and address) is saved in the crypto module data set specified in the TKE host transaction program started procedure on the host.

Change authority

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

Figure 76. 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 allows you to work with the domains on the host crypto module. Master keys and operational keys can be loading using the Domains tab and domain control values can be changed.

When the Domains tab is selected, numbered tabs are displayed on the right for each domain that is configured as a control domain on the host system. Up to 85 domain tabs may be displayed, depending on the host system type and the crypto module type that are accessed.

Domain General page

The Domain General page opens when you select a domain. Each domain can have up to five associated pages: the General page, the Keys page, the Controls

page, the Dec Tables page, and the PINs page. From the Domain General page, you can update the domain description, zeroize the domain, or change the default key wrapping methods.

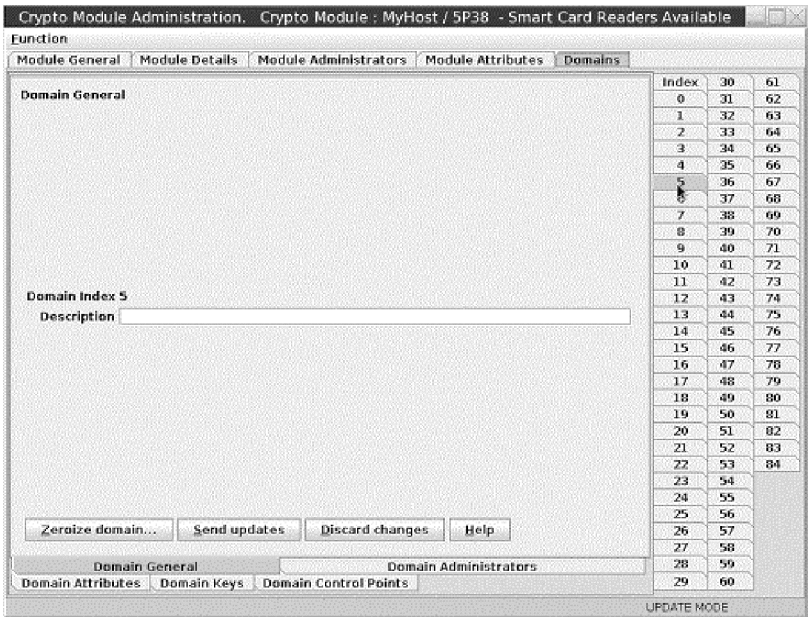


Figure 77. Domain General page

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

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

If you click **Discard changes**, any changes that you made on the panel to the domain description or the default key wrapping methods are discarded, and the current values are refetched from the crypto module.

Zeroize domain

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

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

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

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

Note: Unlike the Global Zeroize issued from the Support Element, Zeroize Domain does not affect the enablement of TKE Commands on the supported crypto modules. Refer to “TKE enablement” on page 9.

Domain 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 (APKA), DES, and RSA key registers.

Note: ICSF uses the term 'ECC master key register' and CCA uses the term 'APKA master key register' to refer to the same entity. On TKE, this is labeled 'ECC (APKA) master key register'.

If you 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 269 or Chapter 12, “Smart Card Utility Program (SCUP),” on page 279.

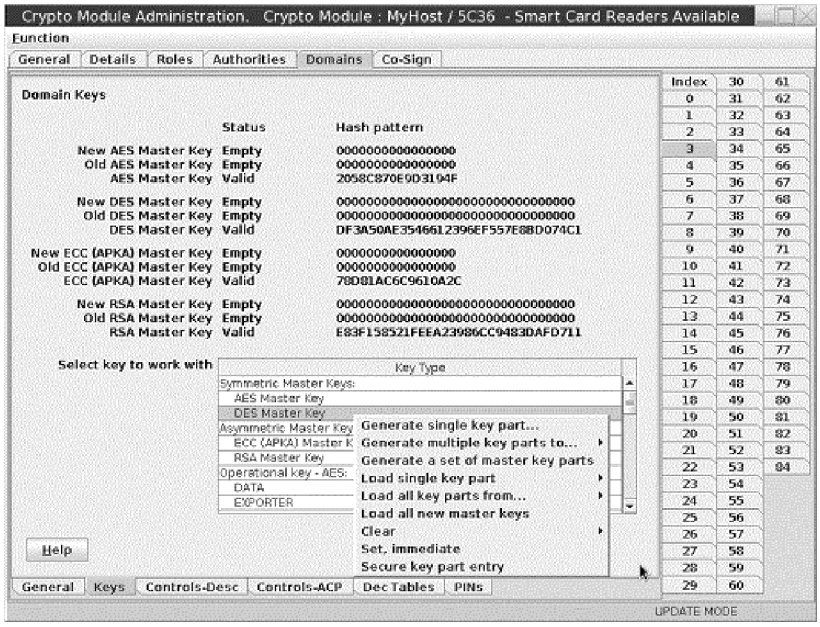


Figure 78. Domain Keys page

The lower part of the Domain 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 20 on page 149 illustrates the possibilities for the supported crypto modules.

Table 20. Key types and actions for the supported crypto modules

Key type	Popup	Sub-popup	Action description
AES master key ECC (APKA) master key DES master key RSA master key	Generate single key part		Generate one master key part and store it on a TKE smart card or save it to a binary or print file.
	Generate multiple key parts to ...	Smart card Binary file Print file	Run a wizard-like feature to generate a user specified number of master key parts and store them on TKE smart cards or save them to binary or print files. **Note:** You can use the same smart card or switch smart cards between key part generations.
	Generate a set of master key parts		Run a wizard-like feature to generate a set of master key parts (AES, DES, RSA or ECC (APKA)).
	Load single key part	First Intermediate Last	Load one key part into the appropriate "new" master key register. **Notes:** 1. To load a first part, the "new" master register status must be "empty". 2. To load an intermediate or last part, the "new" master register status must be "part full" (partially full).
	Load all key parts from	Smart card Binary file Print file	Run a wizard-like feature to load an entire "new" master key register. At the beginning of the process, you specify the total number of key parts and have the option of clearing the "new" master key register. **Note:** No new security controls are introduced by this feature. ALL authority and dual control requirements you put in place remain in effect. It takes the same number of people to load an entire key using this procedure as it does loading an entire key one part at a time.
	Load all new master keys		Run a wizard-like feature to load one or more new master key registers -- first, middle (optional), and last key parts. At the beginning of the process, you have the option of clearing one or more master key registers. Note: No new security controls are introduced by this feature. ALL authority and dual control requirements you put in place remain in effect. It takes the same number of people to load an entire key using this procedure as it does loading an entire key one part at a time.
	Clear	New Master Key Register Old Master Key Register	Clear the new or old master key register. The status of the register will be "empty" when the operation is complete.

Table 20. Key types and actions for the supported crypto modules (continued)

Key type	Popup	Sub-popup	Action description
	Set (Option only shown on RSA master key)		Sets the RSA master key. **Notes:** 1. Beginning with HCR7790, ICSF blocks the use of the Set RSA Master Key command from TKE if any online host crypto modules are found with the September 2011 LIC or later (CEX3C or later). The set must be done from ICSF. 2. The current RSA master key is transferred to the old RSA master key register. 3. The new RSA master key register is transferred to the current RSA master key register. 4. The new RSA master key register is reset to zeros.
AES master key ECC (APKA) master key DES master key RSA master key (continued)	Set, immediate		Sets the master key. Transfers the value in the current master key register to the old master key register, transfers the value in the new master key register to the current master key register, and clears the new master key register. Under normal circumstances, set master keys using ICSF procedures or services that coordinate setting the master key with initializing or re-enciphering key storage. This option sets the master key but does not change the associated key storage. If used inappropriately, this command causes the keys in key storage to become unusable when accessed by ICSF in the domain. Use this option only when key storage does not need to be initialized or re-enciphered when the master key is set. For example, this command can be used to reload previous master key values if a host crypto module has been inadvertently zeroized.
	Secure key part entry		Enter known key part value to a TKE smart card; see Appendix A, “Secure key part entry,” on page 303.
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.

Table 20. Key types and actions for the supported crypto modules (continued)

Key type	Popup	Sub-popup	Action description
	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 are only shown on Operational Keys - AES key types other than DATA.	Load one key part into a key part register. **Note:** 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 type IMP-PKA and AES operational key type IMPORTER.	First Intermediate Last	Load a key part to the TKE workstation's DES or AES 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 303.
RSA keys	Generate single key part		Generate an RSA key and encrypt it under a DES IMP-PKA key or AES IMPORTER key.
	Encipher		Encipher an unencrypted RSA key under an IMP-PKA key.
	Load to PKDS		Load an RSA key to the PKDS active in the logical partition where the Host Transaction Program is started.
	Load to dataset		Load an RSA key to the host data set

Master keys - AES, ECC (APKA), DES, or RSA

Generate single key part: The generate action for a new AES, ECC (APKA), DES, or RSA Master Key type generates 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, prompting you to specify the target.

Figure 79. Select Target

Select the target: TKE smart card, binary file or print file. If you are working with a host crypto module that has CCA 4.3 or later installed and you are generating a DES master key part, a window opens prompting you to specify the key part length.

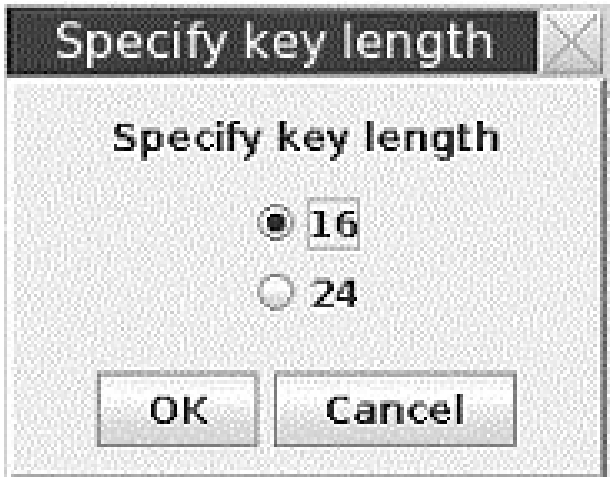


Figure 80. Specify key part length

Save the key part. If you are 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 workstation crypto adapter and the TKE smart cards are in the same zone. To display the zone of a TKE smart card, exit TKE and use either the Cryptographic Node Management Utility or the Smart Card Utility Program under Trusted Key Entry Applications. See “Display smart card details” on page 269 or “Display smart card information” on page 281.

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

If you are saving to a TKE smart card, a message window prompts you to insert the smart card into the smart card reader.

Figure 81. Save key part to smart card

After you insert the TKE smart card, click OK. Then enter the PIN onto the smart card reader PIN pad.

A window opens prompting you for a key part description.

Figure 82. Enter key part description

Enter a description for the key part, and click **Continue**.

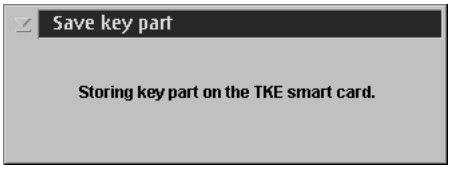


Figure 83. Save key part

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

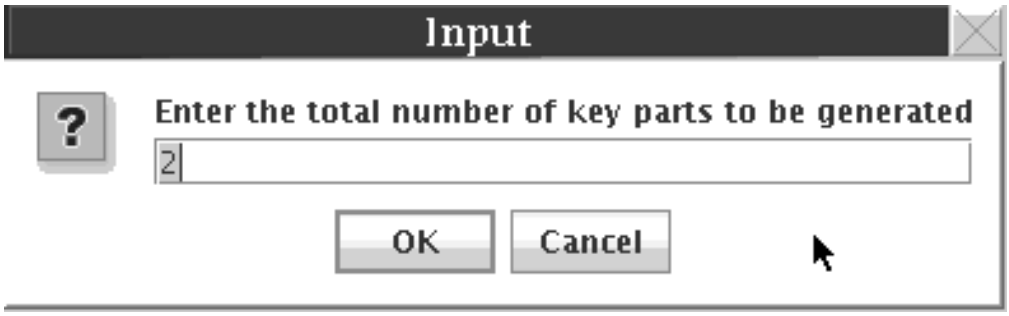


Figure 84. Enter number of keys to be generated

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

Generate a set of master key parts: To create a set of master key parts of different types, use the 'generate a set of master key parts' feature. The feature helps you through the process of generating the set of master key parts.

Load single key part: The load action from the New AES, DES, ECC (APKA), or RSA 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.

After you select **Load single key part**, a new menu pops up from which you can select the key part to load:
- First
- Intermediate
- Last

If a TKE 7.2 or later workstation is connected to a host system that has ICSF HCR77A0 or later installed and is managing a host crypto module that has CCA 4.3 or greater installed, you can load either a 16-byte or 24-byte DES master key on the host crypto module. A 24-byte DES master key provides improved protection of DES operational keys stored in the CKDS on the host.

The length of the DES master key is controlled by a domain control setting. The domain control is "DES master key - 24-byte key" and it is found under the "ISPF Services" domain controls that appear on the domain **Controls** tab in the crypto module notebook. If this domain control is enabled, all DES master key parts that are loaded to the new DES master key register must be 24 bytes in length. If this domain control is disabled, all DES master key parts that are loaded to the new DES master key register must be 16 bytes in length. The setting of this domain control at the time the first DES master key part is loaded is used to determine the length of all DES master key parts.

Two other domain control settings that are found in ICSF HCR77A0 and CCA 4.3 are also used when you load either a new 24-byte DES master key or new RSA master key. The "Warn when weak wrap - Master keys" domain control (found under the "Coprocessor Configuration" domain controls on the domain **Controls** tab) is used to warn of a "weak" master key at the time the last master key part is loaded. If this domain control is enabled, a warning message is displayed after the last master key part is loaded indicating that the key is "weak". A master key is considered "weak" if two or more 8-byte pieces of the master key are identical. For

example, if A, B, and C represent the 8-byte pieces of the master key, an A-B-C key would be considered a "strong" key, but an A-B-A key would be considered "weak".

The other domain control setting that is used when you load either a new 24-byte DES master key or new RSA master key is the "Prohibit weak wrapping - Master keys" control (also found under "Coprocessor Configuration"). If this domain control is enabled and a "weak" master key is detected at the time the last master key part is loaded, an error message is displayed and the load of the last master key part fails.

Input from TKE smart card: Follow these steps:

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

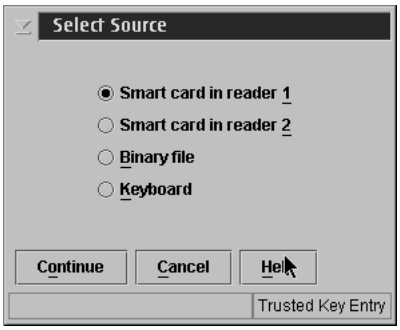


Figure 85. Select key source - smart card

   Make your selection and click **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 workstation crypto 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 269 or “Display smart card information” on page 281.
3. The smart card contents are read and displayed in the Select key part from TKE smart card window:

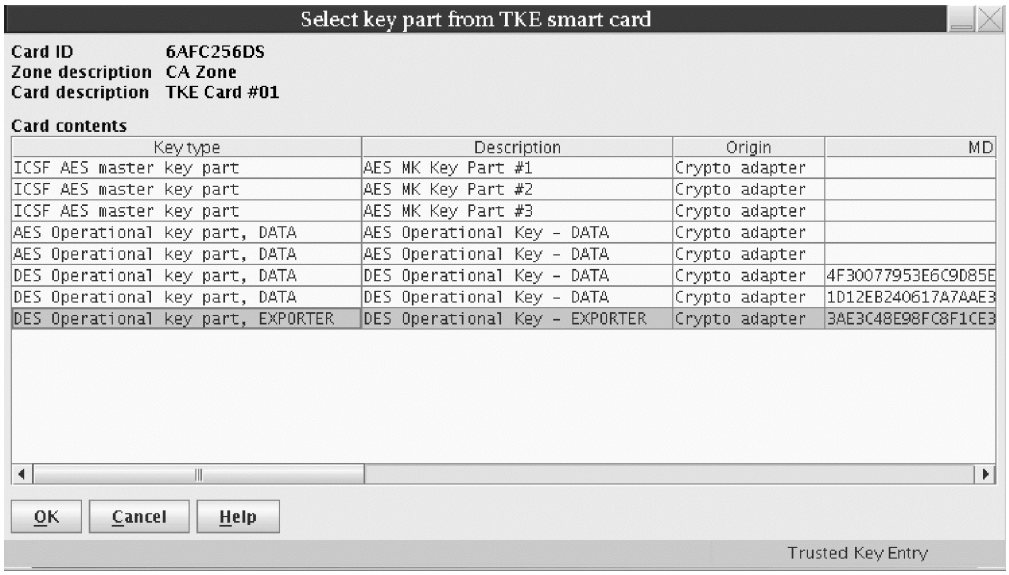


Figure 86. Select key part from TKE smart card

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 RSA 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 (APKA) 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** push button.

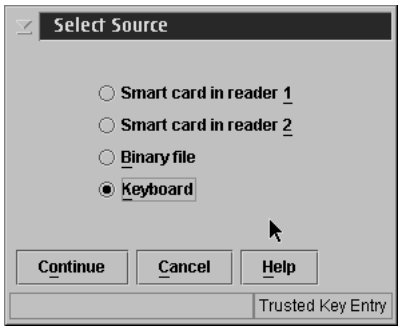


Figure 87. Select key source - keyboard

If keyboard is selected as the input source an input dialog box is displayed with input fields for either a 16-byte key, a 24-byte key or a 32-byte key depending on the key type. The dialog box displayed for entering the key values depends on the installation's Blind Key Entry selection. Blind Key Entry masks the key values being entered by representing the values as asterisks.

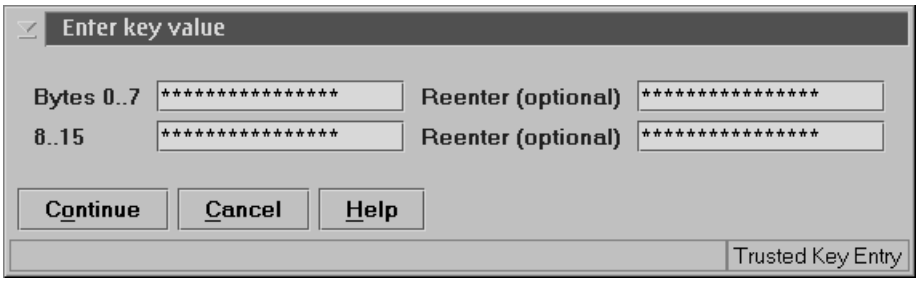


Figure 88. Enter Key Value - Blind Key Entry

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 128.

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** push button.

Figure 89. Enter Key Value

- For the DES and RSA master keys, when the user presses **Continue**, the MDC-4 (and Encipher Zero for a 16-byte DES Master Key) are calculated and displayed, providing the user with the opportunity to visually verify the MDC-4 and ENC-ZERO values. When **Load Key** is pressed, the user is asked if he or she would like to save the key part. If the user selects **Yes** to save the key part, a file chooser window is opened for the user to specify the file location (CD/DVD drive, USB flash memory drive, or TKE Data Directory) and file name for saving the key part. Then the key part is loaded. If the user selects **No**, the key part is not saved and the key part is loaded.

Figure 90. Key Part Information Window

Press **Load key**.

- For an AES or ECC (APKA) master key, when the user presses **Continue**, the AES-VP is calculated and displayed, providing the user with the opportunity to visually verify the AES-VP value. When **Load key** is pressed, the user is asked if he or she would like to save the key part. If yes, a file chooser window is opened for the user to specify the file location (CD/DVD drive, USB flash memory drive, or TKE Data Directory) and file name for saving the key part. Then the key part is loaded. If no, the key part is not saved and the key part is loaded.

Figure 91. 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** push button.

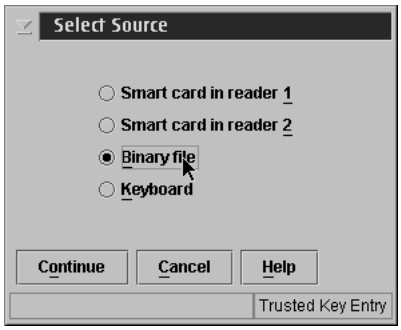


Figure 92. Select key source - binary file

The Specify key file window is displayed.

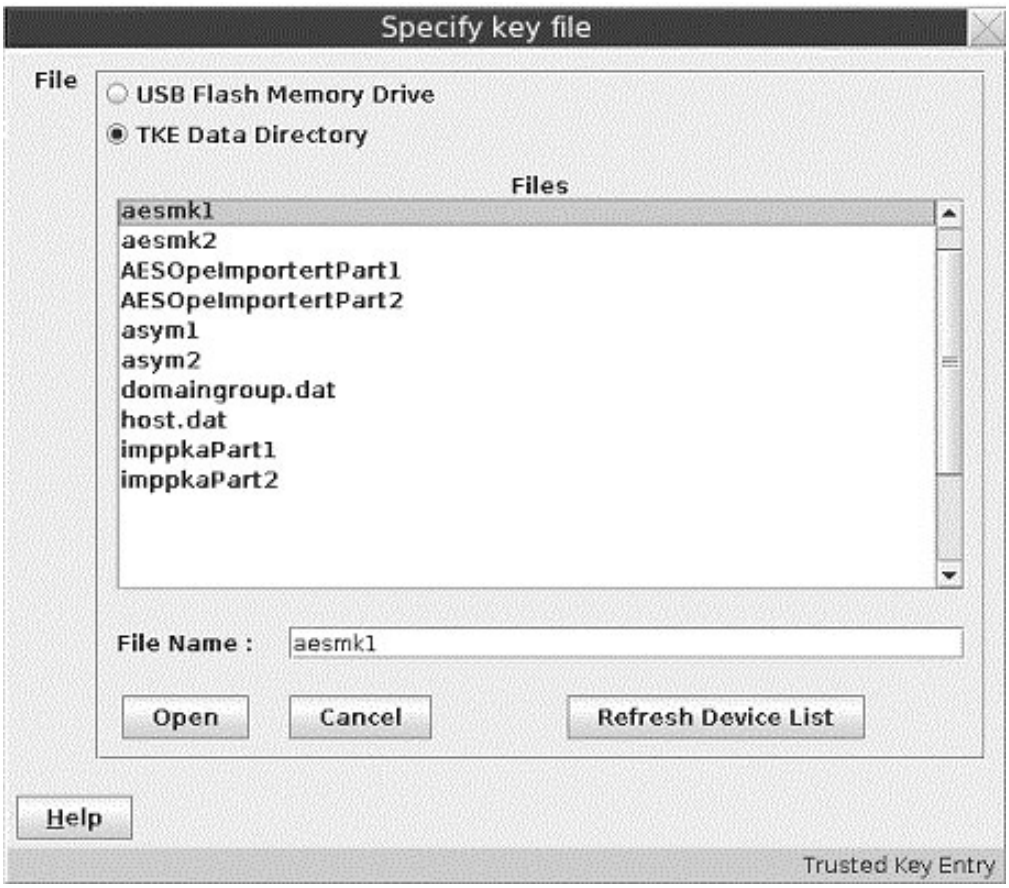


Figure 93. Specify Key File

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

The Key Part Information window is displayed.

- For a DES or RSA master key, the MDC-4 is calculated and displayed, providing the user with the opportunity to visually verify the value.
- For a 16-byte DES master key, when loading from a binary file, the Encipher Zero hash is calculated and displayed. This display provides the user with the opportunity to visually verify the value.
- For AES and ECC (APKA) master keys, the AES-VP is calculated and displayed, providing the user with the opportunity to visually verify the AES-VP value.

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

Figure 94. Key Part Information window

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

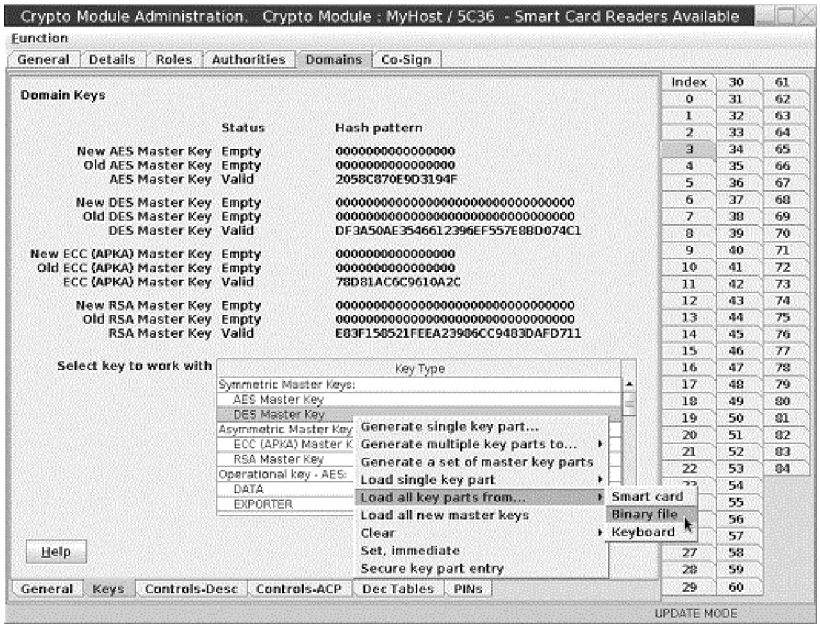


Figure 95. Load all key parts from

2. A window opens prompting you for the number of key parts to be loaded. In the text entry field of this window, enter the number of key parts to be loaded and click **OK**. In this example, there are two key parts.

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

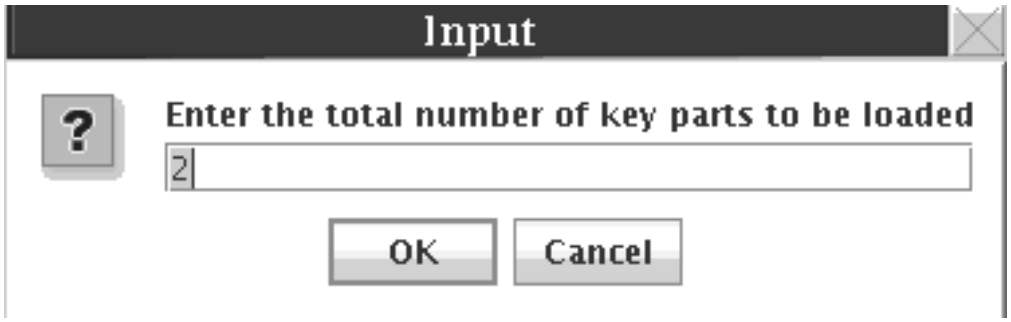


Figure 96. Enter the total number of key parts

3. A window opens asking if you want to clear the key register. In this example, we click **Yes** to clear the key register before loading the key parts from the binary file.

Figure 97. 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 command 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 window opens 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 window opens with the message `Command was executed successfully`. Click **Close** to continue the process.

4. A window opens with the message `Select first key part`. Click **OK** 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" window opens. 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 click **Open**.

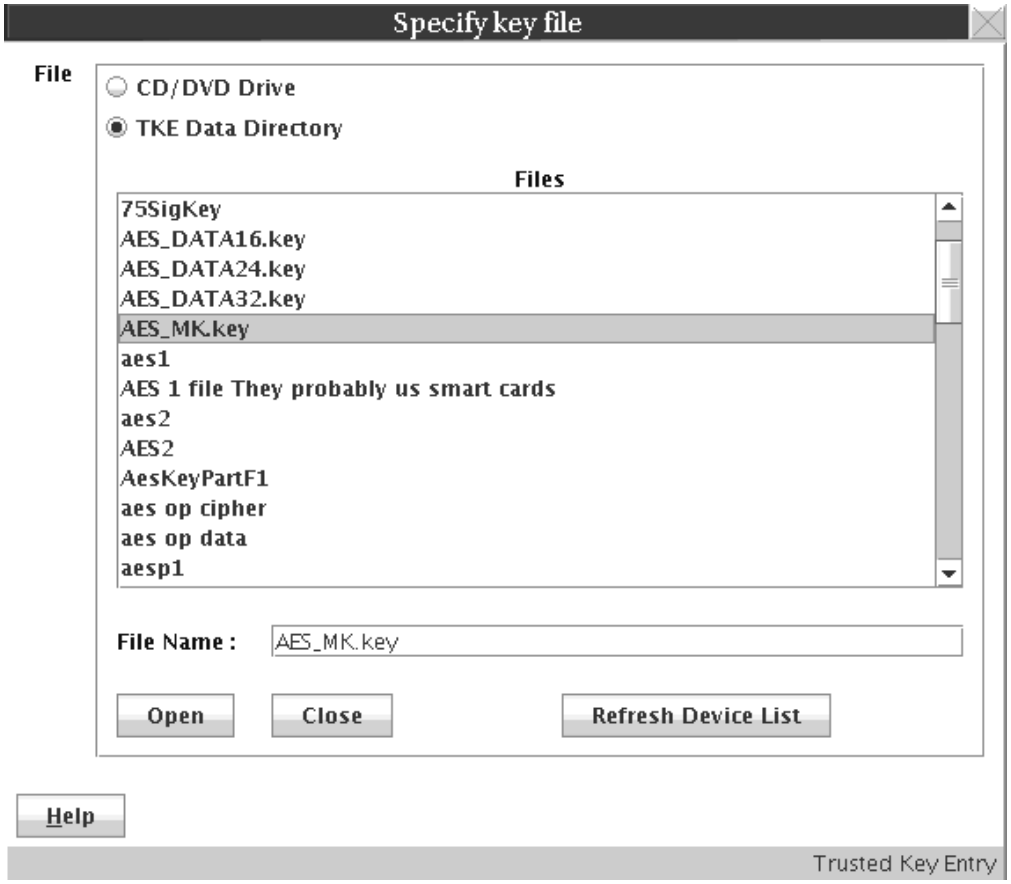


Figure 98. Specify key file (first key part)

6. A window opens displaying the key part information contained in the binary file. To load the key material, click **Load key**.

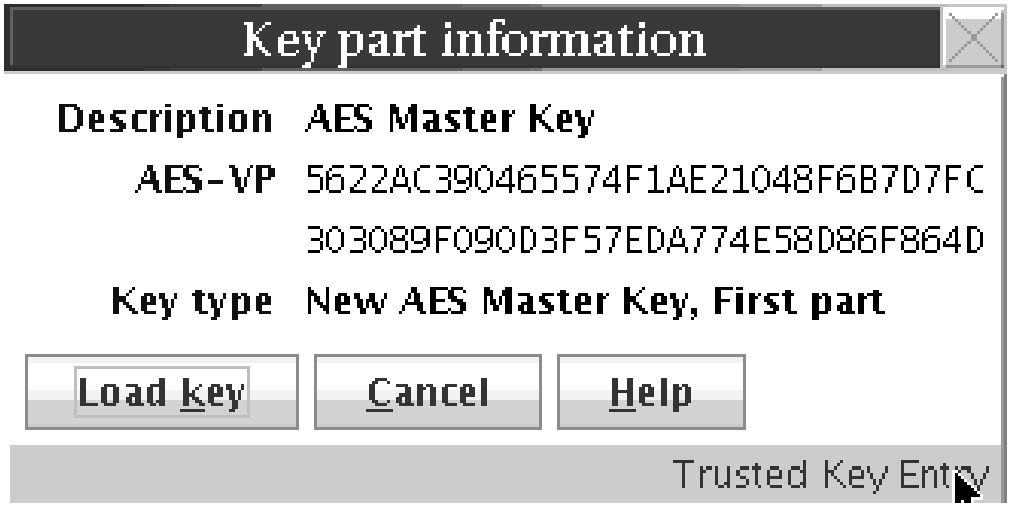


Figure 99. Key part information (first key part)

When load of the key part completes, a window opens with a `Command was executed successfully` message. Click **Close** to continue the process.

7. In our example, we are loading two key parts. A window opens with a message `Select last key part`. Click **OK** to continue to select this key part.
8. A "Specify key file" window opens. Select the appropriate file for this key part, and click **Open**.

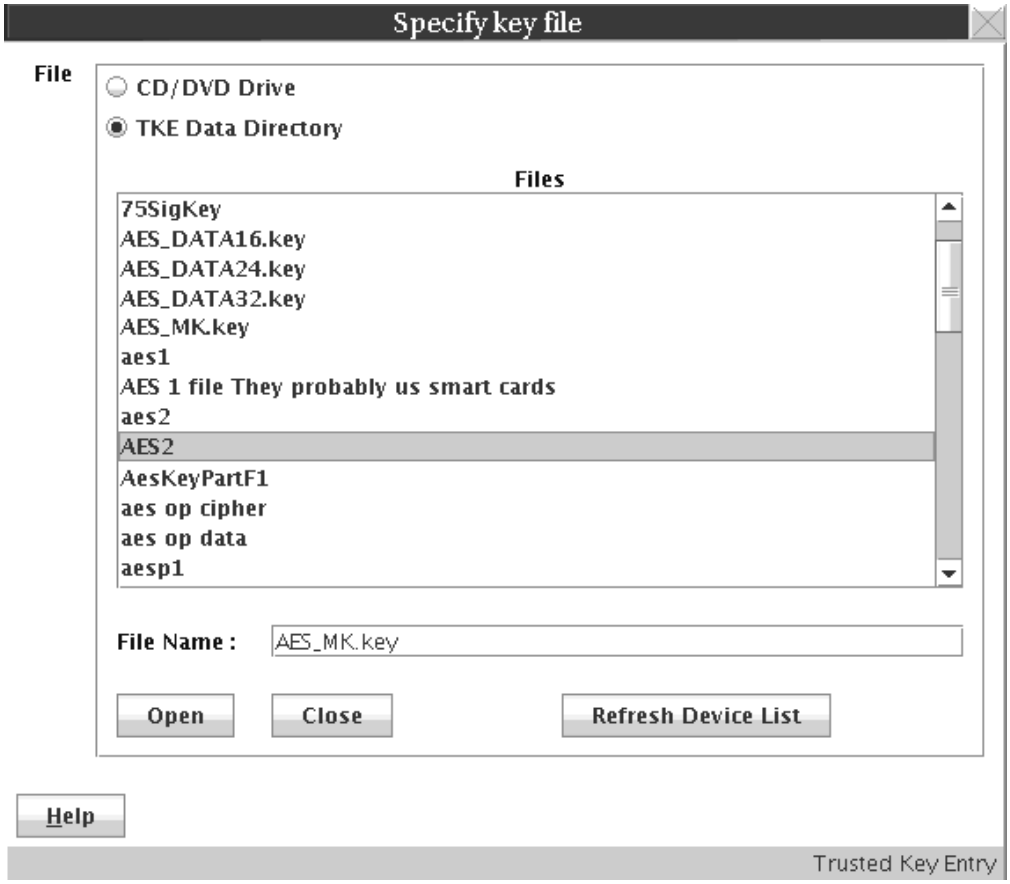


Figure 100. Specify key file (second key part)

9. A window opens that displays the key part information contained in the binary file. To load the key material, click **Load key**.

Figure 101. Key part information (second key part)

When load of the key part completes, a window opens with a message `Command was executed successfully`. Click **Close**. The process is complete.

Load all new master keys: To load all new master key registers at once, use the 'load all new master keys' feature. The feature helps you through the process of loading the new master key registers.

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 message window opens, prompting you to verify that you want to clear the key register.

Figure 102. Clear new or old master key register validation message

If you click **Yes**, but an authority signature key has not been loaded, you are prompted to load an authority signature key.

If you click **Yes** and the command executes successfully, a message window opens informing you of the success.

Figure 103. Clear new or old new master key successful message

Set: This option is available only for RSA master keys. PKA Callable Services must be disabled on ICSF before you use this option.

This option transfers the value in the current RSA master key register to the old RSA master key register, transfers the value in the new RSA master key register to the current RSA master key register, and clears the new RSA master key register.

Note: Beginning with HCR7790, ICSF blocks the use of the Set RSA Master Key command from TKE if any online host crypto modules are found with the September 2011 LIC or later (CEX3C or later). ICSF signals an error in this case. You can use the Set RSA Master Key command with earlier versions of ICSF, or if all online host crypto modules are at earlier CCA levels.

Set, immediate: This option is available for all master key types (AES, ECC (APKA), DES, and RSA). It transfers the value in the current master key register to the old master key register, transfers the value in the new master key register to the current master key register, and clears the new master key register.

Under normal circumstances, set master keys by using ICSF procedures or services that coordinate setting the master key with initializing or re-enciphering key storage. This option sets the master key but does not change the associated key storage. If used inappropriately, this option causes the keys in key storage to become unusable when accessed by ICSF in the domain.

Use this option only when key storage does not need to be initialized or re-enciphered when the master key is set. For example, this command can be used to reload previous master key values if a host crypto module was inadvertently zeroized.

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.
After 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 231) or using an option on Key Generator Utility Processes (KGUP) Job Control Language (JCL) (see *z/OS Cryptographic Services ICSF Administrator’s Guide*).

CEX2C, CEX3C, and CEX4C host crypto modules support a maximum of 100 key part registers distributed across all domains. On the CEX5C, 512 key part registers are supported and distributed across all domains.

An AES key part register that has a type other than DATA 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 keys other than AES DATA 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 (APKA) master keys and for DES operational keys, AES DATA operational keys, and all other AES operational 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 conform to the rules of a valid control vector. For more details on control vectors, see Appendix C in *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

Instead of a control vector, AES keys other than AES DATA 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 *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 opens showing the key type, key length, description, and control vector. Only the description field can 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 (DES MAC, MACVER and DATA, and all AES key types) then the key length field can also be updated.

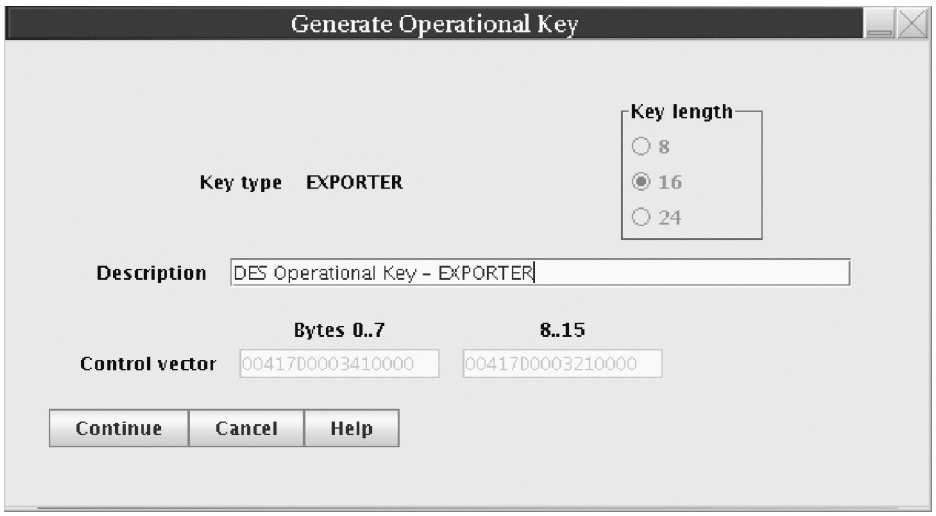


Figure 104. Generate Operational Key - predefined EXPORTER Key Type

When Generate is selected for a `USER DEFINED` key, the Generate Operational Key window opens showing the key type, key length, description, and blank control vector fields. All but the key type can be updated. The control vector entered must conform to the rules for a valid control vector.

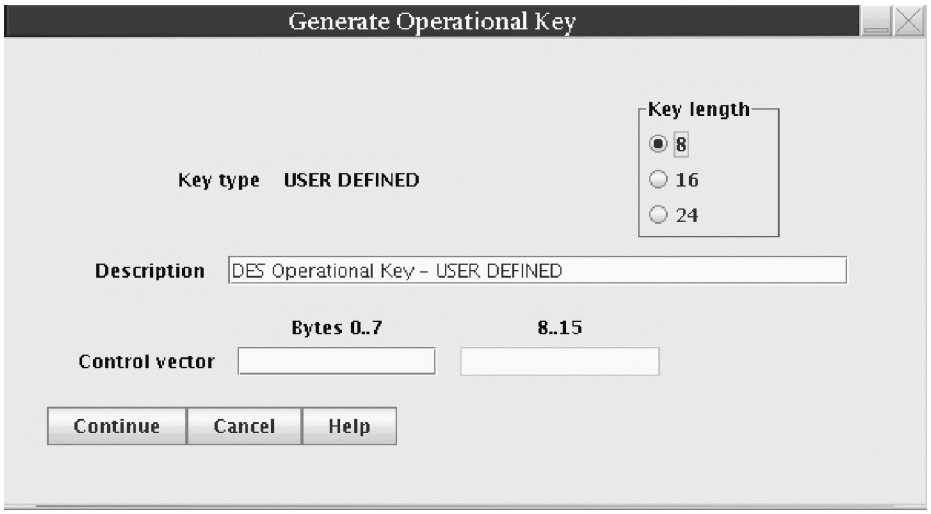


Figure 105. Generate Operational Key - USER DEFINED

When Generate is selected for an AES key other than AES DATA, the Generate Operational Key window opens 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 can be changed by pressing the **Change key attributes** push button.

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

Figure 106. 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** push button.

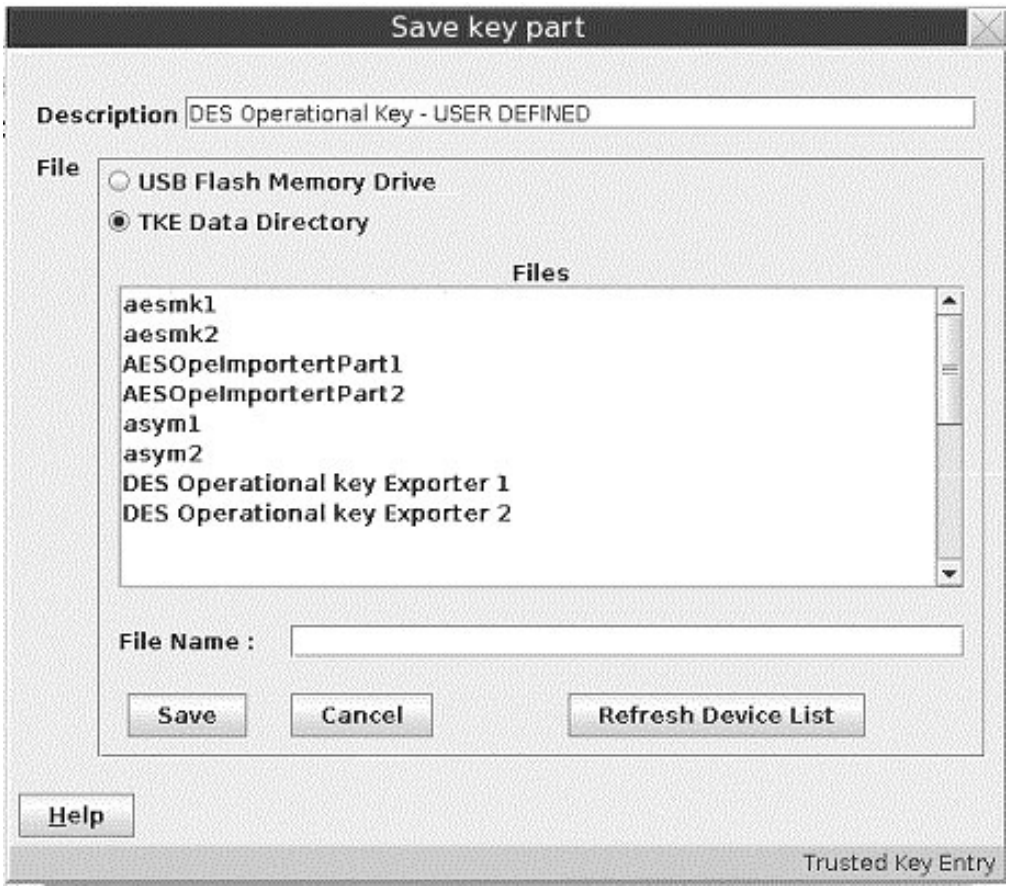


Figure 107. Save key part

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

Figure 108. Save key again

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

Save key to Smart Card

Note: The TKE workstation crypto 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 workstation crypto adapter; otherwise the Generate fails. 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 269, "Display smart card information" on page 281 or "View current zone" on page 301.

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 message indicates 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 127.

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 opens, prompting you to select the source for the key part.

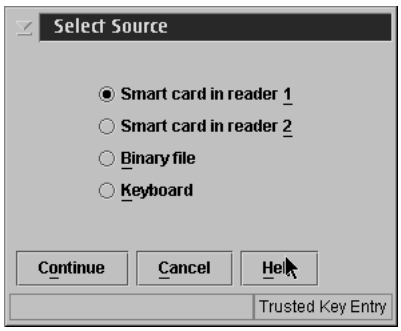


Figure 109. Select Source

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

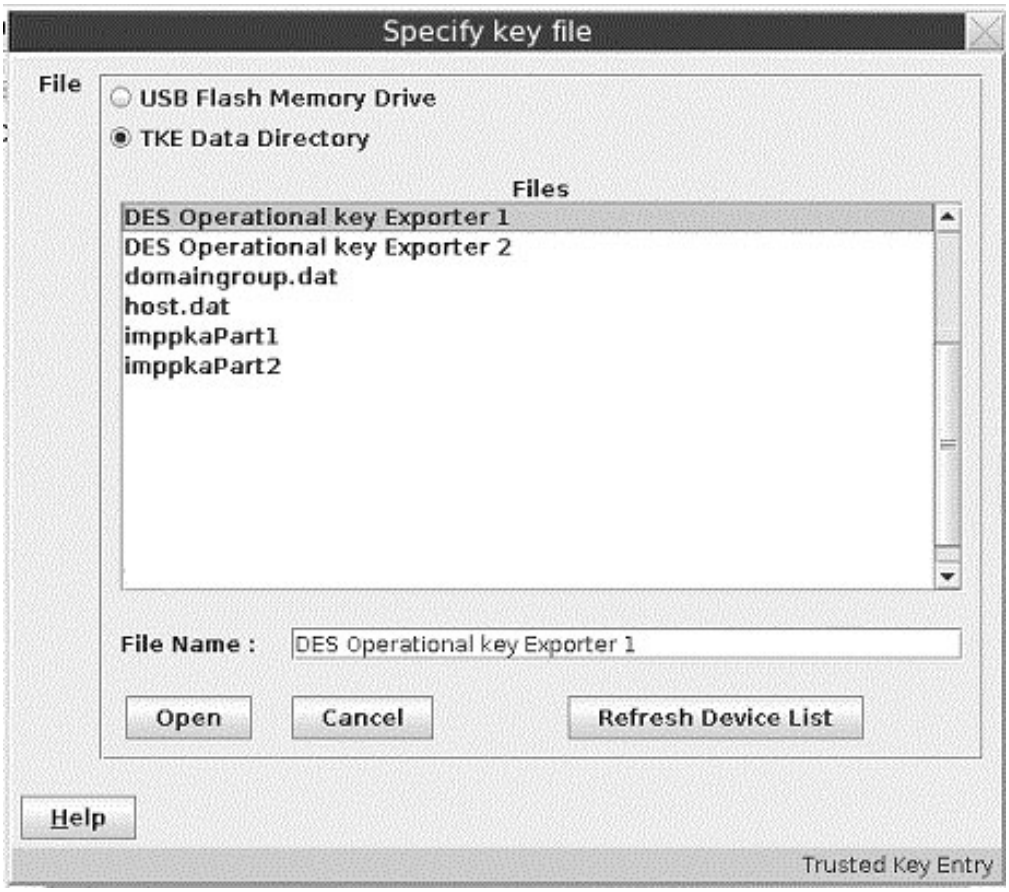


Figure 110. Specify key file for binary file source

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.

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

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.

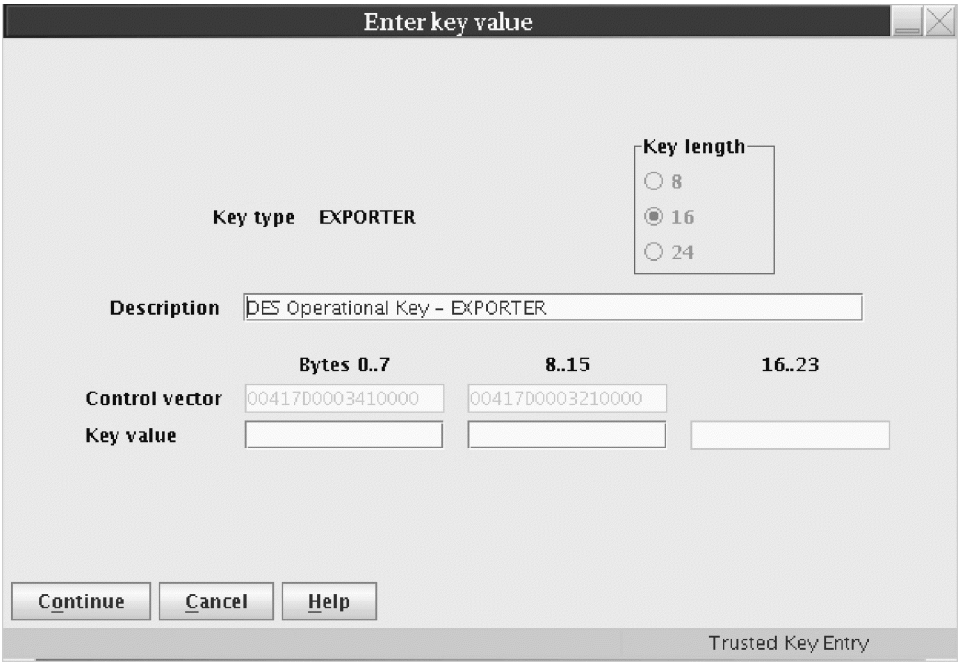


Figure 111. Enter key value - keyboard source for predefined EXPORTER key type

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*.

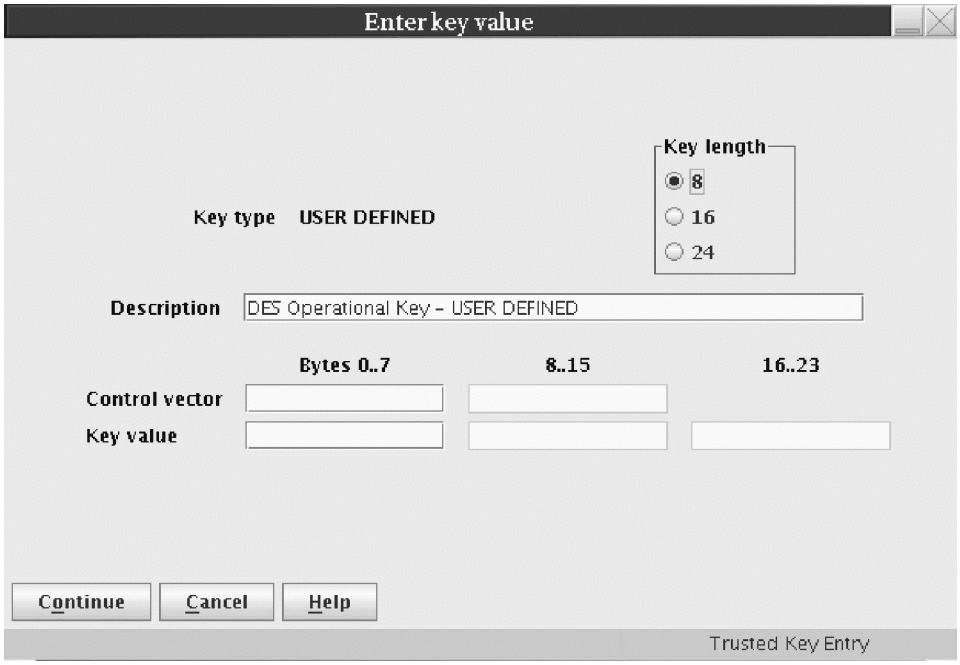


Figure 112. Enter key value - keyboard source for USER DEFINED key type

When the key type is an AES type other than DATA, the **Key value** fields can be updated and the **Change key attributes** push 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**.

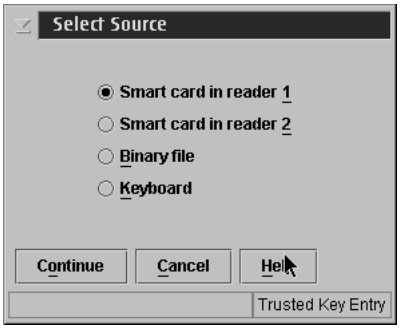


Figure 113. Select Source

2. In the Select key part from TKE smart card window, highlight the key part, right click, and either choose **Select** or press **OK**.

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

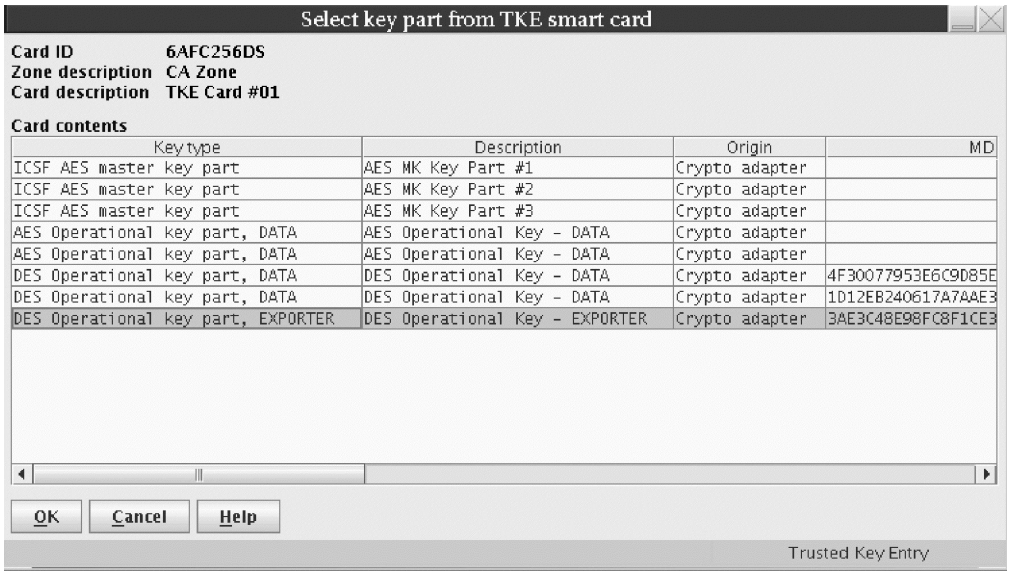


Figure 114. Select key part from TKE smart card

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 all other AES keys, 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** push 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 is converted to uppercase.

Figure 115. 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 opens. 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 is adjusted to odd.

Figure 116. DES key part register information

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

Load to Key Part Register - Add Part: A **Load to key part register Add Part** can be performed multiple times, but must be performed at least once. The process for loading additional parts is similar to loading the first key part.

If **Binary file** is selected, the user chooses the file to load. If **Smart card in reader 1** or **Smart card in reader 2** is selected, the user chooses the key part to load. If **Keyboard** is selected and the key type is a predefined operational key, the **Enter Key Value** window is displayed. If the key type is `USER DEFINED`, then the **Load Operational Key Part Register** window is displayed with a drop down menu of

available control vectors.

Figure 117. 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 118, which displays the available control vectors, the key part bit (bit 44) is turned on indicating that the key in the key part register is a partial key and is not yet complete. This bit will be turned on automatically when the first key part is loaded regardless of whether or not the user turned it on when the control vector was defined.

Figure 118. 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.

Figure 119. 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.

Figure 120. 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:

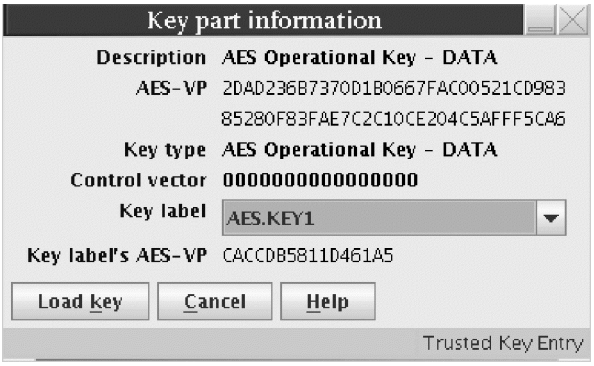


Figure 121. AES key part information - add part

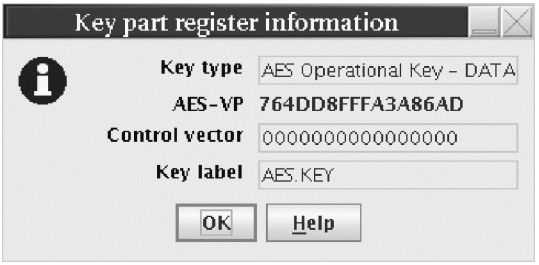


Figure 122. AES key part register information

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.

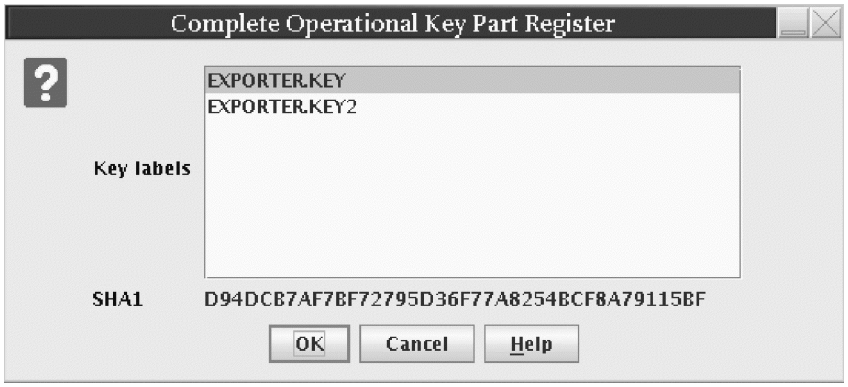


Figure 123. Complete DES Operational Key Part Register - predefined EXPORTER key type

To select one key label, highlight the label using the left mouse button. To select more than one key label, highlight the label using the left mouse button, then hold down the Control key and highlight additional key labels using the button. To select a range of key labels, highlight the first key label using the left mouse button, then hold down the Shift key and highlight the last key label. All key labels between the two selected labels will be selected. To select all the key labels, hold down the Control key and type an 'a'. When only one key label is selected for a DES key, the SHA-1 hash of the accumulated key in the key part register is displayed. If more than one key label is selected then the SHA-1 field on the window contains a '-'.

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

Figure 124. Complete DES Operational Key Part Register - USER DEFINED key type

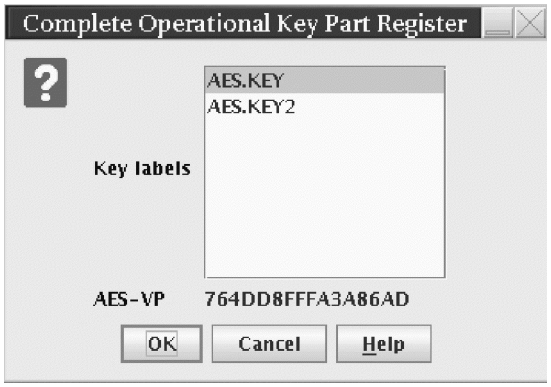


Figure 125. Complete AES Operational Key Part Register

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 '-'.

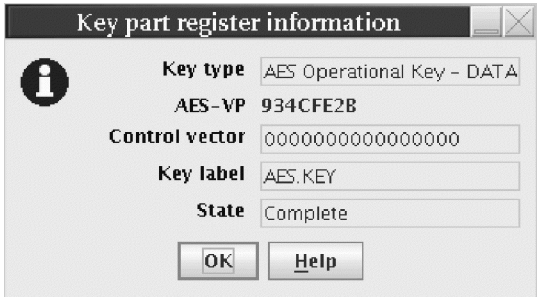


Figure 126. AES Key part register information - predefined DATA key type in Complete state

After the key labels have been selected, the **Key part register information** window is displayed for each label that was selected. The ENC-ZERO value is shown for completed DES keys and the AES-VP is shown for completed AES keys.

Figure 127. DES Key part register information - predefined EXPORTER key type in Complete state

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

View

Operational Key View is used to display key part register information. When **View** is selected for a predefined operational key, the **View Operational Key Part**

Register window is displayed. Only key part register labels that contain keys of the same operational key type are displayed for selection.

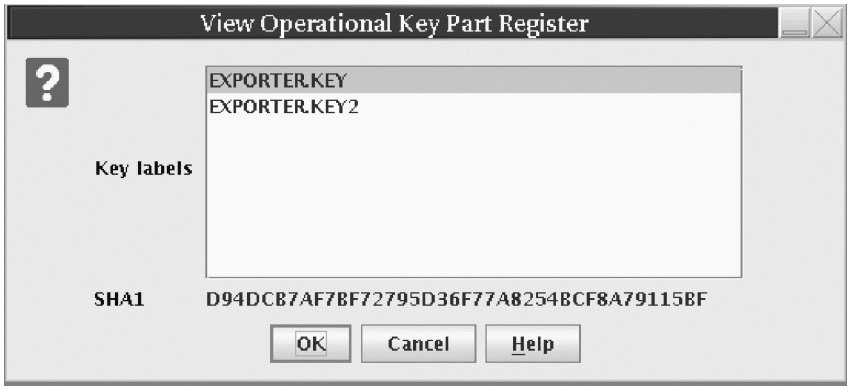


Figure 128. View DES Operational Key Part Register - EXPORTER, one key label selected

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

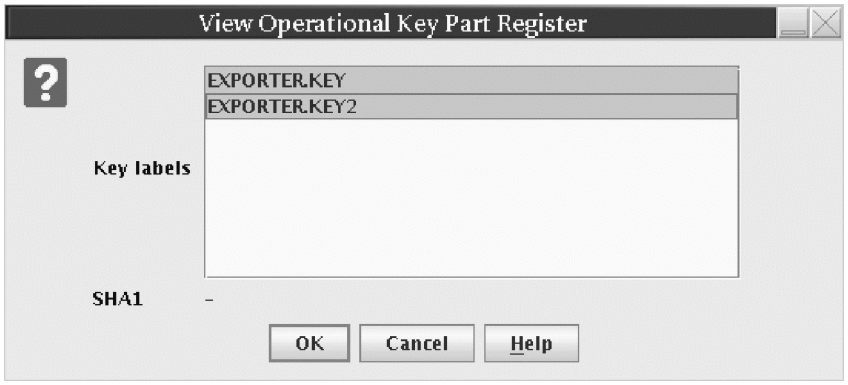


Figure 129. View DES Operational Key Part Register - EXPORTER, all key labels selected

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

Figure 130. View DES Operational Key Part Register - USER DEFINED

After the key labels have been selected, the **Key part register information** window is displayed for each label that was selected. For keys that are in the First part entered or Intermediate part entered state, the SHA-1 value is displayed for the accumulated partial key value. Since the key contained in the key part register is a partial key, the key part bit (bit 44) of the control vector (CV) will be turned on. This is true for predefined and `USER DEFINED` key types.

Figure 131. View DES key part register information - key part bit on in CV

If the key is in the Complete state, the ENC-ZERO value of the completed key is displayed for DES keys, and the AES-VP value of the completed key is displayed for AES keys. The control vector for the completed key will have the key part bit turned off.

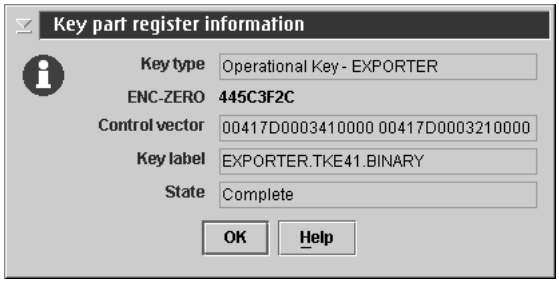


Figure 132. View DES key part register information - complete key

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

Figure 133. View key register successful message

Clear

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

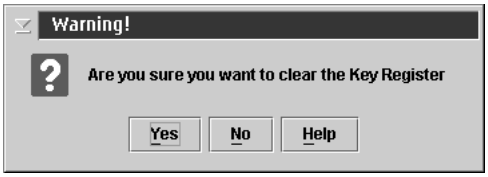


Figure 134. Warning! message for clear operational key part register

When clear is selected for a predefined operational key, the **Clear Operational Key Part Register** window is displayed. Only key part register labels that contain keys of the same operational key type are displayed for selection. If the key type supports different key lengths, then all key part registers of the key type selected will be displayed regardless of key length.

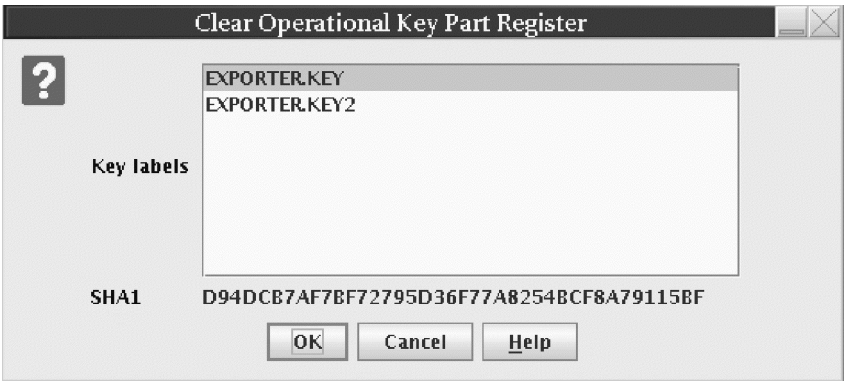


Figure 135. Clear Operational Key Part Register - EXPORTER key type, one key label selected

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 '-'.

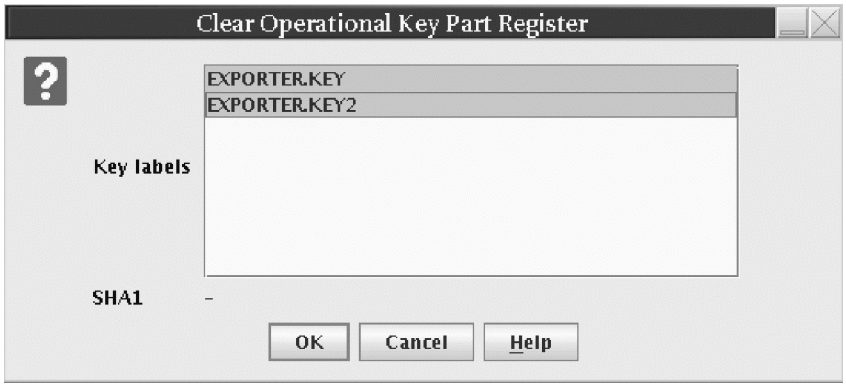


Figure 136. Clear DES Operational Key Part Register - EXPORTER key type, all key labels selected

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

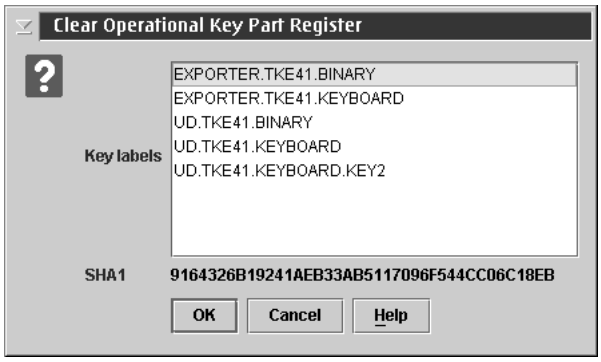


Figure 137. Clear DES Operational Key Part Register - USER DEFINED, one key label selected

When you press the **OK** push button on the **Clear Operational Key Part Register** window, the selected key labels are processed, and a message is displayed indicating that the command was executed successfully.

Figure 138. Clear Key Register successful message

DES operational key: Load to Key Storage

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

- **First**
- **Intermediate**
- **Last**

The contents of the container depend upon the user's selection.

If the user selected **First**, the container shows all keys in the workstation key storage usable as IMP-PKA key encrypting keys. The user can utilize these as skeletons for composing the new key label.

If the user selected **Intermediate** or **Last**, the container shows all keys in the workstation key storage that have been installed with the first key part. It also shows any optional intermediate key parts that have been installed. The user must select one of these as the key label.

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

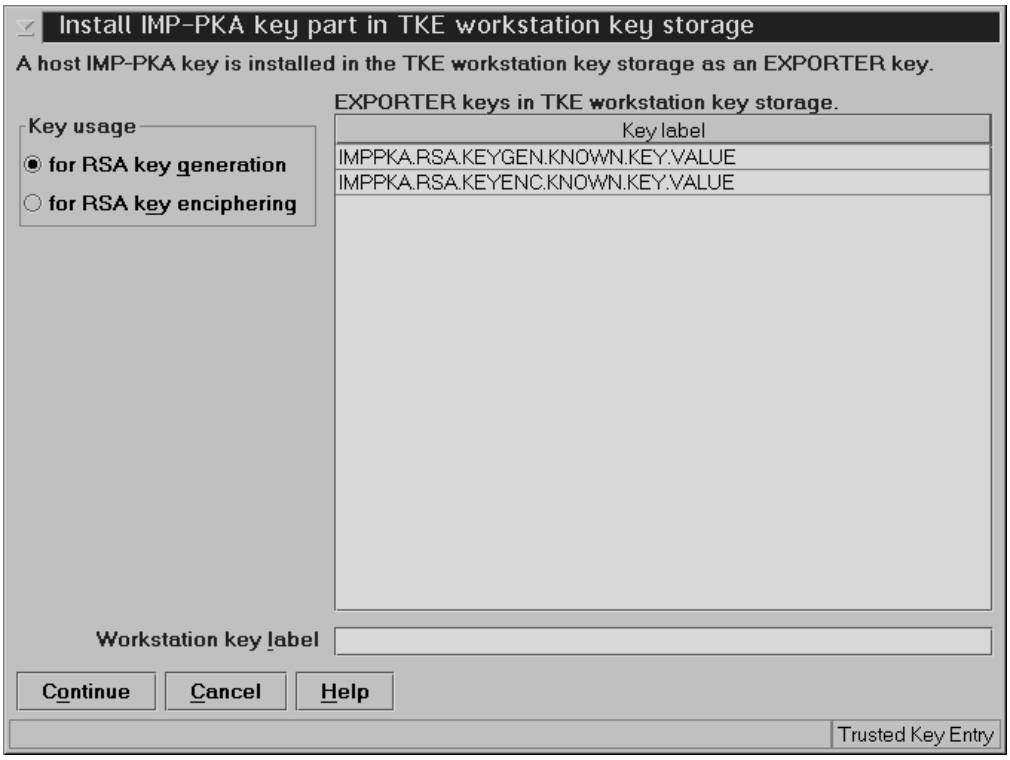


Figure 139. Install IMP-PKA Key Part in Key Storage

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 170.

AES operational key: Load to Key Storage

This selection is only possible for AES IMPORTER keys. An AES IMPORTER key can be used to protect RSA keys during transport from the workstation to ICSF as long as the 'Key can be used for IMPORT', 'Key can be used for GENERATE-PUB' and 'Key can wrap RSA keys' attributes are set to 'Yes' in the key's attributes. After selecting **Load to Key Storage**, the user chooses one of the following key parts to load to the workstation key storage:

- First...
- Intermediate...
- Last...

The contents of the container depend upon the user's selection.

If the user selected **First**, the container shows all keys in the workstation key storage usable as AES IMPORTER key encrypting keys. The user can utilize these as skeletons for composing the new key label.

If the user selected **Intermediate** or **Last**, the container shows all keys in the workstation key storage that have been installed with the first key part. It also shows any optional intermediate key parts that have been installed. The user must select one of these as the key label.

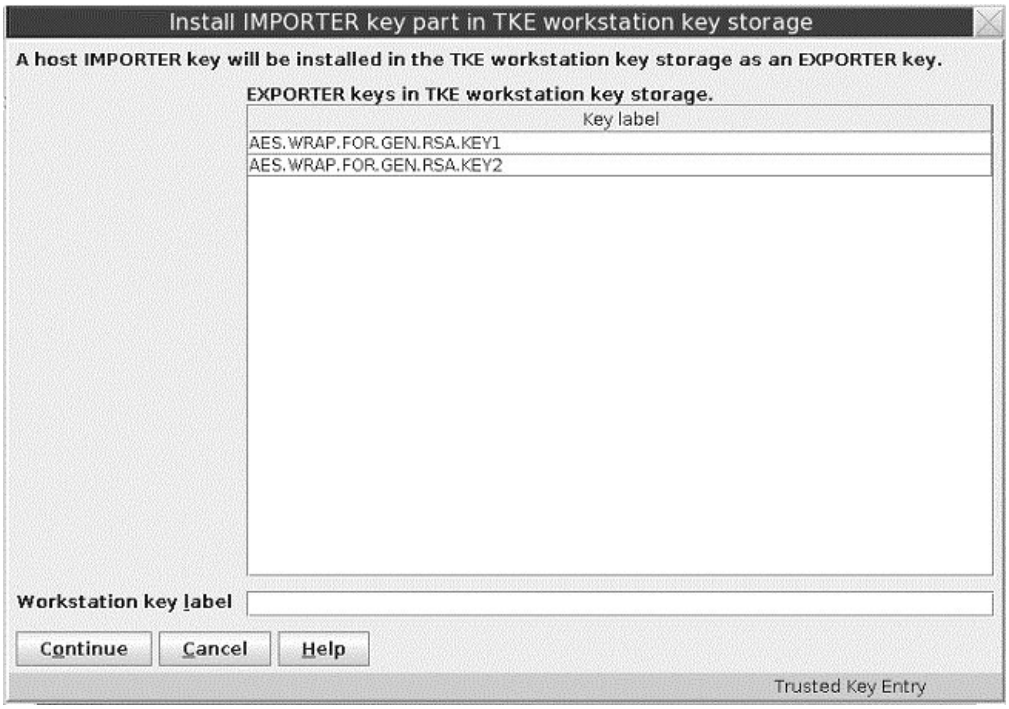


Figure 140. Install AES IMPORTER Key Part in Key Storage

Note: For the RSA key to be loaded into the PKDS, the AES IMPORTER key value must be stored in the CKDS. See "Load to Key Part Register First" on page 170.

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 303 for details on using this function.

RSA keys

Generate RSA Key

This selection initiates RSA key generation at the workstation. The generated RSA key is protected with a previously generated DES IMP-PKA or AES IMPORTER key, and the encrypted RSA key is saved in a file.

Notes:

- RSA keys can also be generated and saved in the host PKDS using ICSF panels and services (CSNDPKG for generate, and CSNDKRC or CSNDKRW to write to the host PKDS.) For more information, see *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

- An RSA key with a length of 1024 or less can be wrapped with a DES IMP-PKA or AES IMPORTER key.
- An RSA key with a length greater than 1024 must be wrapped with an AES IMPORTER key.

From the Domain Keys page, right-click **RSA key** in the **Key Types** container and select **Generate**. The Generate RSA Key window opens.

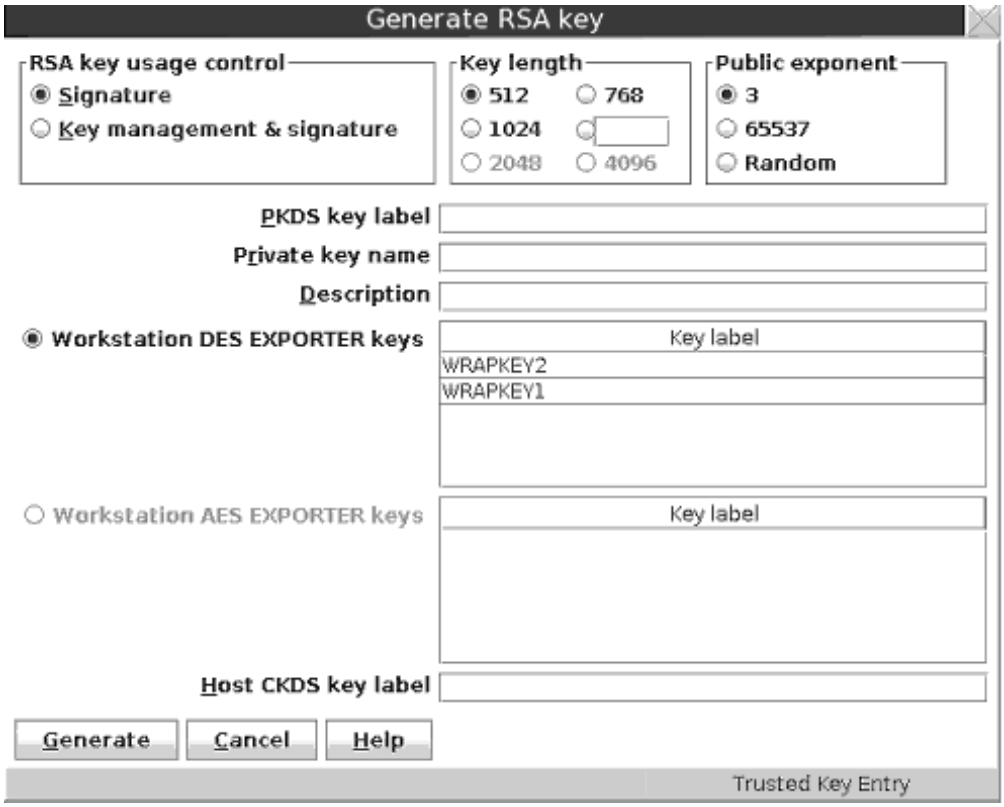


Figure 141. Generate RSA Key

In the Generate RSA key window, specify the following information:

RSA key usage control
Specifies whether or not the RSA key can be used for key management purposes (encryption of DES keys). All RSA keys can be used for signature generation and verification.

Key length
Length of the modulus of the RSA key in bits. For RSA keys protected by a DES EXPORTER key, any length between 512 and 1024 is allowed. For RSA keys protected by an AES EXPORTER key, any length between 512 and 1024, and lengths of 2048 and 4096 are allowed. When a length of 2048 or 4096 is selected, the AES EXPORTER key should be at least 24 bytes long. If not, a message is displayed.

Public exponent
Value of the public exponent of the RSA key.

PKDS key label
Label to be given the imported RSA key at the host. The information provided in this field can be changed when you load the RSA key to the host.

Private key name
Text string that is included in the RSA key token and cryptographically related to the key. The private key name can be used for access control for the key. The information you entered in the PKDS key label field is copied to this field and can be edited.

Description
Optional free text that is saved with the RSA key and displayed when you retrieve the key.

Workstation DES EXPORTER keys
This container displays the labels of the DES EXPORTER keys currently in TKE workstation DES key storage that can be used to protect RSA keys generated at the TKE workstation. When these keys were loaded into TKE DES key storage, key usage of "for RSA key generation" was specified. To select one of these keys, click **Workstation DES EXPORTER keys** and select a key label.

Workstation AES EXPORTER keys
This container displays the labels of the AES EXPORTER keys currently in TKE workstation AES key storage that can be used to protect RSA keys generated at the TKE workstation. Only keys with set attributes including "Key can be used for IMPORT", "Key can be used for GENERATE-PUB", and "Key can wrap RSA keys" are listed. To select one of these keys, click **Workstation AES EXPORTER keys** and select a key label.

Host CKDS key label
The CKDS key label at the host used to import the RSA key. The selected workstation DES EXPORTER or AES EXPORTER key label is copied to this field and can be edited. This information can be changed when you load the RSA key to the host.

When the key is generated, a window opens that prompts the user to specify the file location (USB flash memory drive or TKE Data Directory) and file name for saving the generated RSA key.

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

Encipher RSA Key

This selection allows an RSA key to be read from a clear key file, encrypted with a previously generated IMP-PKA key encrypting key, and saved in a file. The format of the clear key file is described in Appendix D, "Clear RSA key format," on page 323.

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

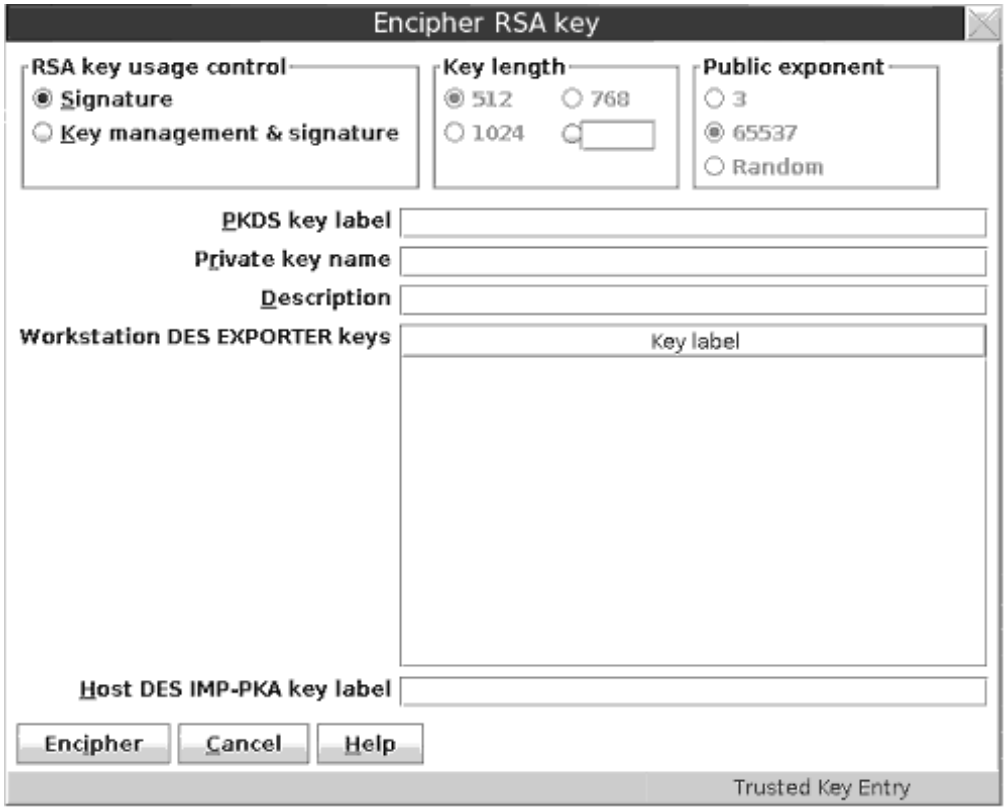


Figure 142. Encipher RSA Key

In the Encipher RSA key window, specify the following information:

- **RSA key usage control** — Specifies whether the RSA key can be used for key management purposes (encryption of DES keys). All RSA keys can be used for signature generation and verification.
- **PKDS key label** — Label to be given the imported RSA key at the host. The information provided in this field can be changed when you load the RSA key to the host.
- **Private key name** — Text string that is included in the RSA key token and cryptographically related to the key. The private key name can be used for access control for the key. The information you entered in the PKDS key label field is copied to this field and can be edited.
- **Description** — Optional free text that is saved with the RSA key and displayed when you retrieve the key.
- **Workstation DES EXPORTER keys** — This container displays the labels of the DES EXPORTER keys currently in TKE workstation DES key storage that can be used to protect RSA keys entered from a clear key file. When these keys were loaded into TKE DES key storage, key usage of "for RSA key enciphering" was specified. AES EXPORTER keys in TKE workstation AES key storage cannot be used to encipher an RSA key. Select a key label by clicking it.
- **Host DES IMP_PKA key label** — The CKDS key label at the host used to import the RSA key. The selected workstation DES EXPORTER key label is copied to this field and can be edited. This information can be changed when you load the RSA key to the host.

When the key is enciphered, a file chooser window is displayed for the user to specify the file location (USB flash memory drive or TKE Data Directory) and file name for saving the encrypted RSA key.

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

Load RSA Key to PKDS

This selection allows the user to load an RSA key to the host and install it in the PKDS. Using this function, it is only possible to load the RSA key to the PKDS in the TKE Host logical partition (LPAR). For loading RSA keys to TKE target LPARs, see "Load RSA key to host dataset" on page 189.

Having selected **Load to PKDS**, a dialog box is displayed for selecting the input file holding the encrypted RSA key. When completed, the **Load RSA key to PKDS** window is displayed.

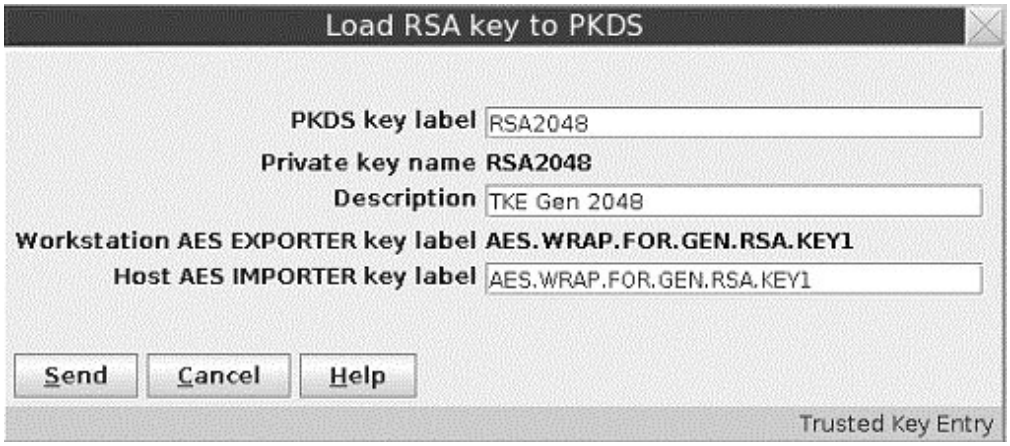


Figure 143. Load RSA Key to PKDS

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

- **PKDS key label** — Label to be given the imported RSA key at the host. Change this field as needed.
- **Private key name** — Text string that is included in the RSA key token and cryptographically related to the key. The private key name can be used for access control for the key. The information you entered in the PKDS key label field is copied to this field and can be edited.
- **Description** — Optional free text that was saved with the RSA key.
- **Workstation DES EXPORTER key label** — Label of the workstation DES IMP-PKA key that protects the RSA key. Displayed when the key-encrypting key is a DES IMP-PKA key.
- **Workstation AES EXPORTER key label** — Label of the workstation AES IMPORTER key that protects the RSA key. Displayed when the key-encrypting key is an AES IMPORTER key.
- **Host DES IMP-PKA key label** — Label of the DES IMP-PKA key stored in the host CKDS that will be used to import the RSA key. Displayed when the key-encrypting key is a DES IMP-PKA key. Change this field as needed.

- **Host AES IMPORTER key label** — Label of the AES IMPORTER key stored in the host CKDS that will be used to import the RSA key. Displayed when the key-encrypting key is an AES IMPORTER key. Change this field as needed.

Load RSA key to host dataset

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

The host data set must be defined in advance. If a workstation DES EXPORTER key was used to protect the RSA key at the time the RSA key was generated or enciphered, the host data set must have the following attributes:

```
recfm fixed, lrecl=1500, partitioned
```

If a workstation AES EXPORTER key was used to protect the RSA key at the time the key was generated, the host data set must have the following attributes:

```
recfm fixed, lrecl=3000, partitioned
```

Using this installation method, it is possible to load RSA keys into any PKDS in any LPAR. For information about the TSO/E ICSF interface, "Installing RSA keys in the PKDS from a data set" on page 234.

The steps are the same as for loading an RSA key to PKDS (see "Load RSA Key to PKDS" on page 188), except that the user has to specify the full data set and member name. If you don't specify the data set and member name in quotes, the high level qualifier for the data set is the TSO/E logon of the administrator/host user ID.

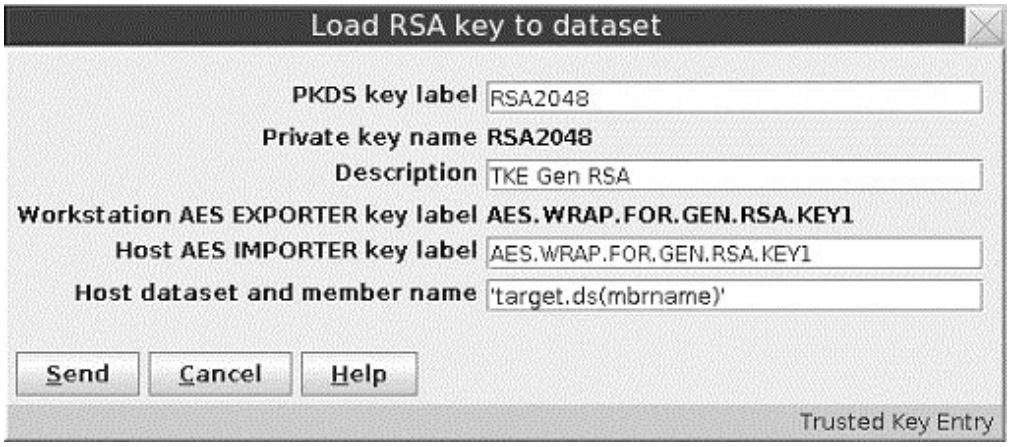


Figure 144. Load RSA Key to Dataset

Domain Controls pages

The Domain Controls pages display the cryptographic functions that are in effect for the domain and allows you to make changes to them. The 'Controls-Desc' page displays the domain controls sorted by description, and the 'Controls-ACP' page displays the domain controls sorted by ACP value.

- To change a setting, click on it. Changing a setting on one domain controls page changes the corresponding setting on the other domain controls page.
- To upload the controls settings to the crypto module, click **Send updates**.

- To leave the controls settings unaltered after you have made changes to the page, click **Discard changes**.
- To save the displayed domain control settings to a file, click **Save to file**.
- To load the domain control settings from a previously saved file, click **Load from file**. This option changes the displayed control settings. Click **Send updates** to upload the displayed settings to the crypto module.

The last two options cause a window to open that allows you to select the file to use.

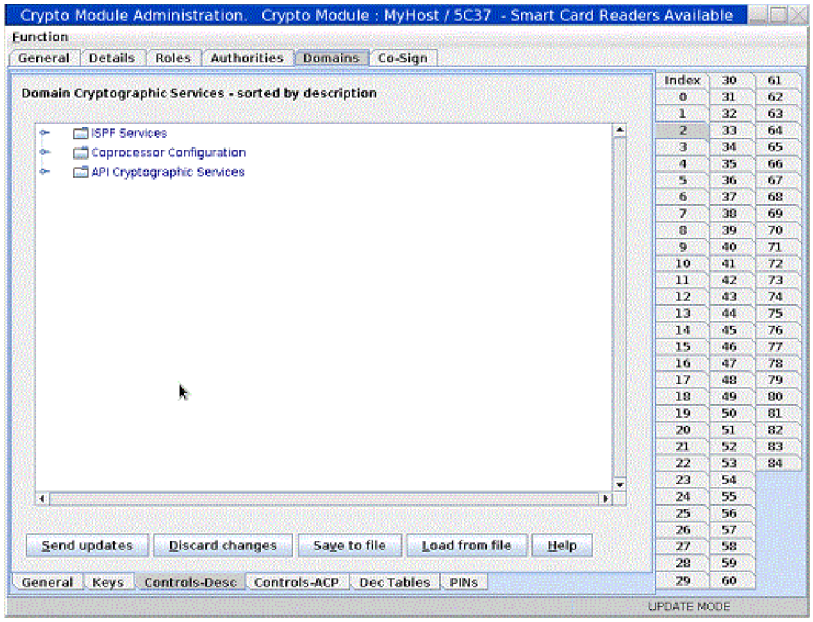


Figure 145. Domain Controls page

Note: When managing domain controls through a TKE workstation, services displayed on the Domain Controls panel might not be available on the host crypto module. Enabling a service on this panel that is not supported by the host crypto module does not make this service available.

Working with Domain Controls settings

You are able to administer access control points to ISPF Services, API Cryptographic Services and User Defined Extensions (UDX) from these pages.

There are expandable folders for the Domain Cryptographic services. Some services cannot be disabled because they are “required”. This is indicated on the panel. You can enable or disable services within the following folders:

- ISPF Services
- Coprocessor Configuration
- API Cryptographic Services
- UDXs (appears only if you have created UDXs on your system)

The access control points displayed on the Domain Controls pages depend on the level of ICSF used to communicate with the host crypto module. Later versions of ICSF may support additional access control points not supported on earlier versions.

Some access control points displayed on the Domain Controls pages may not be implemented on the host crypto module. You can change the value of these access control points, but they do not affect the operation of the host crypto module.

When moving to a later version of ICSF, you may need to manually set or reset the new access control points that are displayed.

ISPF Services: Under the ISPF Services folder, there are check boxes for the services that you can enable or disable. These services are for loading and setting the DES, AES, ECC (APKA), and RSA master keys on supported host crypto modules through the ICSF panel interface.

Coprocessor Configuration: Under the Coprocessor Configuration folder are all of the controls that govern the key wrapping behavior of ICSF callable services. For more information, see *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

API Cryptographic Services: Under the API Cryptographic Services folder are all the ICSF services that can be enabled or disabled from the TKE workstation. See *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.

Domain Decimalization Tables page

Decimalization tables map hexadecimal digits to decimal digits, and are used in certain host crypto module operations that process Personal Identification Numbers (PINs). By selecting **Use Only Valid Decimalization Table** in the domain controls for a domain, you can restrict the set of allowed decimalization tables for the domain. Only decimalization tables with a status of Active in the Decimalization Tables page are allowed to be used.

Decimalization tables can contain only decimal digits ('0' through '9') and must be exactly 16 digits long. Every domain has slots for 100 decimalization tables. These tables can be managed only from a TKE workstation. You can load, activate, or delete tables from this page. The Decimalization Tables page is displayed only for host crypto modules that support decimalization tables.

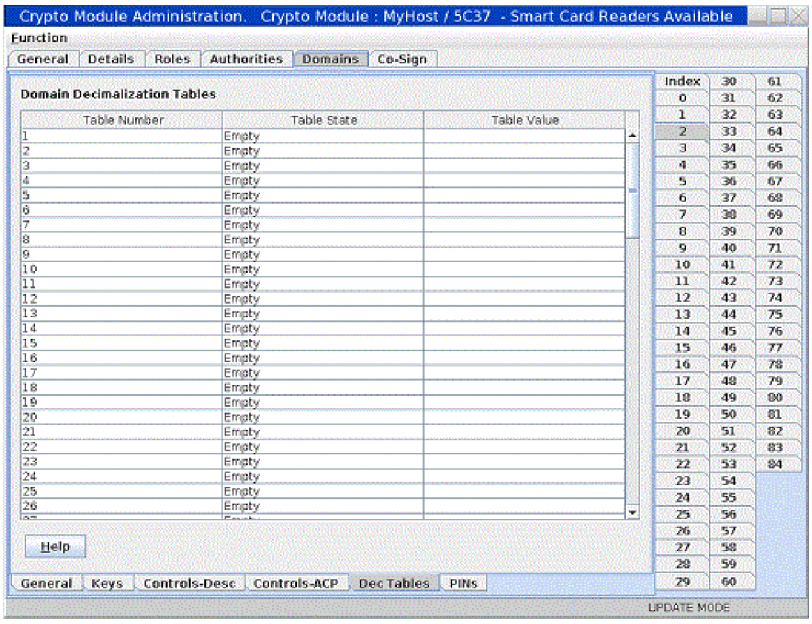


Figure 146. Decimalization tables page

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**

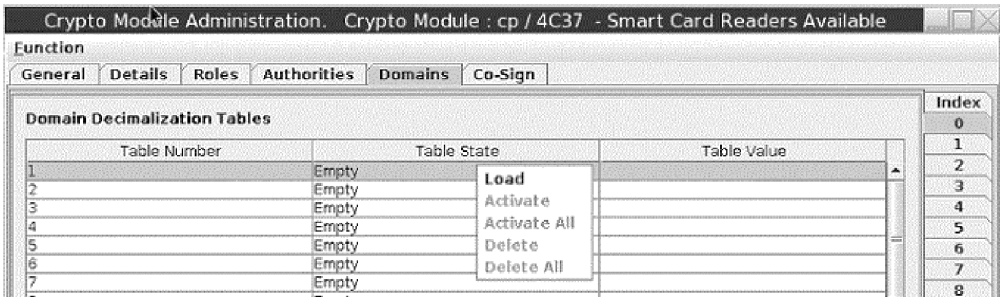


Figure 147. Table entry options

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** push button to create the table entry.

Figure 148. 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** push 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** push button in the information message box.

Note:

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.

Domain Restricted PINs page

You can restrict the use of weak or trivial Personal Identification Numbers (PINs) in a domain by using the Domain Restricted PINs page. You can specify up to 20 PIN values to be disallowed. Disallowing a PIN value prevents users from changing a PIN to the disallowed value, and prevents CCA verbs from ever

generating the disallowed PIN value. Disallowing a PIN value on the Domain Restricted PINs page does not affect the use of existing PINs, however, even if they have the disallowed value.

The PINs to be disallowed can be 4 - 12 digits long, and can contain only decimal digits ('0' through '9'). The Domain Restricted PINs page is displayed only for host crypto modules that support restricting weak or trivial PINs.

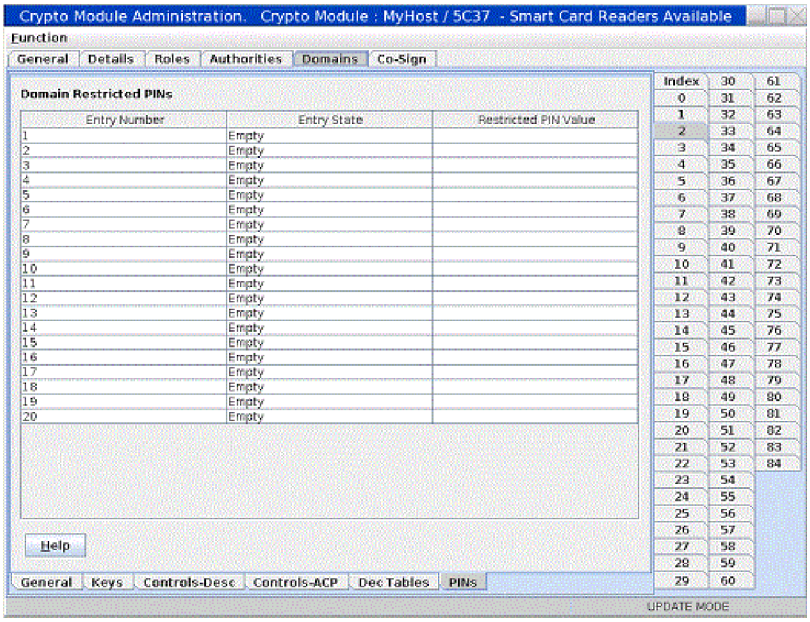


Figure 149. Domain Restricted PINs page

To manage an entry, left-click to select the entry and then right-click to display command options. The available options are:

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

Options that are not valid are disabled. An option might be invalid because of the state of the selected entry (you cannot delete an empty entry, for example), or because the role of the current authority does not allow the option.

There are three access control points in roles that control the ability to manage what PINs are restricted:

- Load Restricted PIN
- Activate Restricted PIN
- Delete Restricted PIN

When you select the **Load** option, a window opens in which you can enter the value of the PIN to be restricted. You can enter 4 - 12 decimal digits. If the role of the current authority has both the load and the activate ACPs selected, the entry goes to the Active state. If the role of the current authority has only the load but not the activate ACP selected, the entry goes to the Loaded state. Separate ACPs for the load and activate options supports dual control of adding a PIN to the restricted PINs list, for users who require dual control.

You can load an entry that is already in the Loaded or Active state, if the role of the current authority has the Delete Restricted PIN ACP. This ACP is required because reloading an entry effectively deletes the current entry.

The **Activate** option changes the state of the entry from Loaded to Active.

The **Delete** option removes the PIN and changes the state of the entry to Empty.

The **Activate All** option activates all entries that are in the Loaded state.

The **Delete All** option deletes all entries in the 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 a host crypto module, exactly two signatures are required for a dual-signature command. The authority index and name of each authority allowed to sign the pending command are displayed.

Authorities who have already signed the command are indicated by a **Yes** in the column labeled ***Signed***.

Pressing the **Co-sign** push button initiates the signing of the pending command. It opens windows in which you can choose the source of the authority signature key and then choose the authority index associated with that key. The possible authority signature key sources are as follows:

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

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

Host crypto module index values

After a host or domain group is opened, a list of cryptographic modules is displayed. Table 21 on page 196 shows the crypto module index value that is displayed based on the type of module and the mode it is running.

Notes:

- A host cryptographic coprocessor running IBM Common Cryptographic Architecture (CCA) code is running in CCA mode.

- A host cryptographic coprocessor running IBM Enterprise PKCS #11 (EP11) code is running in EP11 mode.

Table 21. Module index type displayed on the TKE

Host cryptographic coprocessor type and mode	**Module index type displayed on the TKE**	
	TKE 8.0	**Prior to TKE 8.0**
Crypto Express5S running in EP11 mode	5P*xx*	N/A
Crypto Express5S running in CAA mode	5C*xx*	N/A
Crypto Express4S running in EP11 mode	4P*xx*	SP*xx*
Crypto Express4S running in CAA mode	4C*xx*	SC*xx*
Crypto Express3 running in CAA mode	3C*xx*	G*xx*
Crypto Express2 running in CAA mode	2P*xx*	E*xx*

Chapter 8. Using the Crypto Module Notebook to administer EP11 crypto modules

The Crypto Module Notebook is the central point for displaying and changing all information related to a crypto module. It is used for single crypto modules as well as for domain groups. The contents of some pages vary depending on whether you selected a single crypto module or a domain group.

The TKE Main Window lists the crypto modules available on each host machine to which the TKE Workstation is connected, and also lists any crypto module groups and domain groups you created. Double-click on a crypto module or domain group in the TKE Main Window to open the Crypto Module Notebook and work with the selected crypto module or domain group. There are two versions of the Crypto Module Notebook — one for CCA crypto modules (CEX2C, CEX3C, CEX4C, and CEX5C) and one for EP11 crypto modules (CEX4P and CEX5P).

This topic describes how to use the Crypto Module Notebook for EP11 crypto modules. For information about how to use the Crypto Module Notebook for CCA crypto modules, see Chapter 7, “Using the Crypto Module Notebook to administer CCA crypto modules,” on page 131.

In the main TKE window, when you open an EP11 host crypto module or a domain group made up of EP11 host crypto modules, the Crypto Module Notebook for EP11 crypto modules is displayed. The Crypto Module Notebook opens on the Module General tab.

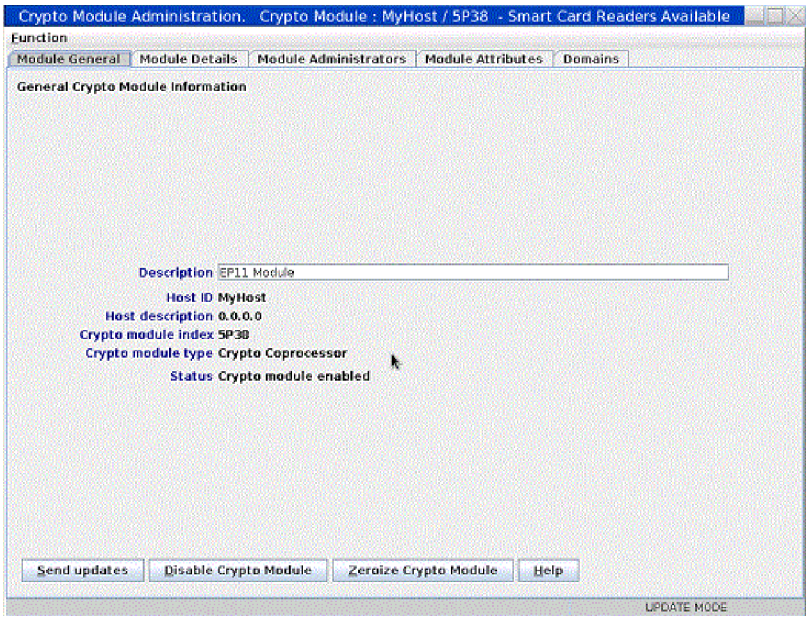


Figure 150. Crypto Module Notebook for EP11 - Module General page

The Crypto Module Notebook is the central point for displaying and changing all information related to a crypto module or a domain group. Most panels are the same when referencing a single host crypto module versus a domain group, but there are minor differences on some panels for the two cases.

Note: Master key parts for EP11 host crypto modules and administrator signature keys are held exclusively on smart cards. Smart card readers must be enabled to perform most administrative tasks. To enable smart card readers, check the Enable Smart Card Readers option on the Preferences pull-down menu on the TKE main window. The main TKE application needs to be restarted for this option to take effect.

Notebook mode

The notebook is opened in one of three possible modes:

- **UPDATE MODE**
- **READ-ONLY MODE**
- **LOCKED READ-ONLY MODE** - domain group notebooks only

The mode is displayed in the lower-right corner on all crypto module notebook pages.

In **UPDATE MODE**, you are able to display crypto module information and to perform updates to the crypto module.

In **READ-ONLY MODE**, you are able to display crypto module information but not update it.

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

Imprint mode

Imprint mode is a temporary operational mode for EP11 crypto modules and domains and is intended for initial setup only. A crypto module and all domains are placed in imprint mode when:

- Segments 2 and 3 of an EP11 crypto module are loaded for the first time
- Ownership of segments 2 and 3 is surrendered and segments 2 and 3 are reloaded
- An EP11 crypto module is zeroized

A domain reenters imprint mode when it is zeroized.

In imprint mode, most commands are executed without requiring command signatures. Administrators can be added and removed, attributes can be changed, the crypto module can be enabled and disabled, and the domain or crypto module in imprint mode can be zeroized. But other commands are not allowed. Imprint mode is used for initial crypto module setup, before master keys can be loaded and control points can be reset to restrict domain functionality.

The concept of "imprint mode" exists at both the crypto module level and the domain level. You must exit imprint mode at the crypto module level before you are allowed to exit imprint mode in any domain on the crypto module.

When a crypto module or its domains are placed in imprint mode, the signature threshold and revocation signature threshold values are set to zero. The crypto module threshold values are shown on the Module Attributes tab. Domain

threshold values are shown on the Domain Attributes tabs. To exit imprint mode, the signature threshold and revocation signature threshold must be changed to nonzero values. The command to change the signature threshold value to a nonzero value must be signed, with the number of required signatures equal to the new signature threshold value. If you try to set the signature threshold or revocation signature threshold to a number larger than the number of administrators that are installed in the crypto module or domain, an error is signaled.

Crypto Module Notebook Function menu

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

- **Refresh Notebook**. This option refreshes the notebook by reading information from the host. Performing a refresh might change the mode of the notebook.
- **Manage Signature Keys**. Use this option to predefine the smart card readers that are checked for administrator signature keys when signatures are needed for administrative commands to the host crypto module. If no smart card readers are selected using this option, you are prompted to insert a smart card with an administrator signature key in smart card reader 1 for each required signature. The result can be frequent prompts to insert or replace a smart card in smart card reader 1.

  If this option predefines smart card readers as the source of signature keys, commands that require administrator signatures automatically use the smart cards in those readers to generate signatures whenever signatures are needed. If the smart card reader does not initially contain a smart card, you are prompted to insert a smart card and enter the PIN. After a valid smart card is inserted in the reader and the PIN is entered, the card can be used to generate additional signatures without further user action.

  All smart card readers are automatically selected as sources of administrator signature keys under this option when the TKE workstation crypto adapter is initialized for smart card use.
- **Release Crypto Module**. An update lock maintained by ICSF prevents attempts to update a host crypto module by more than one TKE workstation at a time. If communication between TKE and a host crypto module is abnormally terminated, the update lock might not be released. If the TKE attempts to reconnect to the host crypto module, it is not able to obtain the update lock and displays a warning indicating the user ID that currently owns the update lock. Selecting the **Release Crypto Module** option releases the update lock and reassigns it to the current user. Be aware, however, that releasing a crypto module can damage an on-going operation initiated by another user. Use this option only if you are certain that the crypto module must be released.

  A dialog prompts you to confirm that you want to release the crypto module.

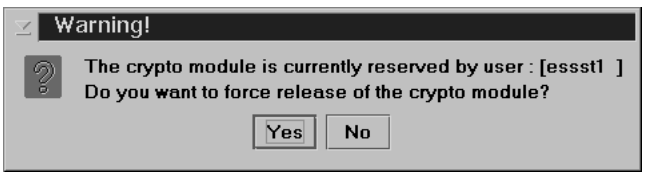


Figure 151. Window to release crypto module

  You can confirm release of the crypto module by clicking **Yes**.
- **Compare Group**. This option is displayed only when working with a domain group. It compares members of the group and identifies any differences between

them. Group members should be configured the same (for example, all member domains should have the same set of installed administrators and the same signature threshold) in order for group operations to complete successfully on all group members.

- **Close**. This option closes the crypto module notebook.

Tabular pages

Tabular pages available in the crypto module notebook for EP11 are:

- **Module General**: see "Crypto Module Notebook Module General tab."
- **Module Details**: see "Crypto Module Notebook Module Details tab" on page 202.
- **Module Administrators**: see "Crypto Module Notebook Module Administrators tab" on page 203.
- **Module Attributes**: see "Crypto Module Notebook Module Attributes tab" on page 205.
- **Domains**: see "Crypto Module Notebook Domains tab" on page 207.

The notebook opens to the Module General tab.

Crypto Module Notebook Module General tab

The contents of this page are:

- **Description**. This field is an optional free text description for the crypto module. For a domain group, this field is an optional description for the crypto module that contains the master domain for the group. You can change the description by typing the new description in the text box and clicking **Send updates**.
- **Host ID**. This field is the ID of the host that contains the crypto module, or, in the case of a domain group, that contains the crypto module with the master domain for the domain group.
- **Host Description**. This field is the description of the host that contains the crypto module, or, in the case of a domain group, that contains the crypto module with the master domain for the domain group.
- **Crypto Module Index**. This field is the index of the crypto module or of the crypto module with the master domain for the domain group. Together with the crypto module type, the index uniquely identifies a crypto module within a host. The index value is 00 through 63.
- **Crypto Module Type**. For the crypto modules that TKE currently supports, this field is always set to *Crypto Coprocessor*.
- **Status**. A crypto module is either enabled or disabled. When a crypto module is enabled, it is available for processing. You can change the status of the module by clicking **Enable Crypto Module** or **Disable Crypto Module**.

When the crypto module is enabled, **Disable Crypto Module** is displayed at the bottom of the page. When the crypto module is disabled, **Enable Crypto Module** is displayed.

If you click **Disable Crypto Module** in a domain group notebook, all crypto modules with at least one domain in the domain group are disabled. This action disables the crypto module for the entire system, not just the LPAR that issued the disable. You are asked to confirm this choice.

Similarly, if you click **Zeroize Crypto Module** in a domain group, all crypto modules with at least one domain in the domain group are zeroized. You are asked to confirm this choice.

Zeroizing a crypto module has the following effects:

- The signature threshold and revocation signature threshold for the crypto module are set to zero, and the crypto module reenters imprint mode. See "Imprint mode" on page 198.
- The crypto module permissions, attribute controls, and operational mode bits are set to their default values.
- All crypto module administrators are removed.
- All domains on the crypto module are zeroized. Zeroizing a domain makes the following changes to the domain:
  - Sets the domain signature threshold and revocation signature threshold to zero, and causes the domain to re-enter imprint mode.
  - Sets the domain permissions, attribute controls, and operational mode bits to their default values.
  - Removes all domain administrators.
  - Clears the new and current master keys in the domain.
  - Re-enables all domain control points.

Intrusion latch

Under normal operation, the intrusion latch of a cryptographic card is tripped when the card is removed. This trip causes all master keys to be erased, all administrators to be removed, and all other configuration settings to revert to their default values. The card and all domains reenter imprint mode. See "Imprint mode" on page 198.

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

1. Open an emulator session on the TKE workstation and log on to your TSO/E user ID on the host system where the card will be removed.
2. From the ICSF Primary Option Menu, select Option 1 for Coprocessor Management.
3. Leave the Coprocessor Management panel displayed during the rest of this procedure. You will be required to press Enter on the Coprocessor Management panel at different times.

   Important: Do not exit this panel.
4. Open the TKE Host where the card will be removed. Open the crypto module notebook for the host crypto module. Click **Disable Crypto Module**.
5. After the crypto module is disabled within TKE, press the Enter key on the ICSF Coprocessor Management panel. The status should change to DISABLED.

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

6. **Configure Off** the card from the Support Element. The Support Element is a dedicated workstation used for monitoring and operating IBM System z hardware. A user authorized to perform actions on the Support Element must complete this step.
7. After the card is Offline, press the Enter key on the Coprocessor Management panel. The status should change to OFFLINE.
8. Remove the card. Perform whatever operation needs to be done. Replace the card.
9. **Configure On** the card from the Support Element. The Support Element is a dedicated workstation used for monitoring and operating 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, press the Enter key on the Coprocessor Management panel. The status should change to DISABLED.
11. From the TKE Workstation Crypto Module General page, click **Enable Crypto Module**.
12. After the card is enabled from TKE, press the Enter key on the Coprocessor Management panel. The Status should return to its original state. If the Status was ACTIVE in step 2, when the card is enabled it should return to ACTIVE.

All master keys, administrators, and other configuration data should still be available. The data was not cleared with the card removal because it was DISABLED first using the TKE workstation.

Crypto Module Notebook Module Details tab

The Module Details tab contains three pages, which can be selected by clicking the tabs on the right side of the window. The pages and their contents are:

- **Crypto Module** - Shows basic information needed to recognize a host crypto module. Different information is displayed, depending on the crypto module type. The following fields may be displayed on this page:
  - **Crypto Module ID** - Unique identifier burned into the crypto module during the manufacturing process.
  - **Public Modulus** - For crypto modules with an RSA device key, the modulus of the key. TKE uses the public key to verify signed replies from the host crypto module.
  - **Modulus Length** - For crypto modules with an RSA device key, the length of the modulus, in bits.
  - **ECC Public Key** - For crypto modules with an ECC device key, the ECC public key.
  - **Key Identifier** - The SHA-256 hash over the public part of the device key. For RSA keys, the hash is over the DER-encoded modulus and public exponent. For ECC keys, the hash is over the ECC public key.
- **Crypto Services (Function Control Vector Values)**
  - CDMF availability
  - 56-bit DES availability
  - Triple DES availability
  - 128-bit AES availability
  - 192-bit AES availability
  - 256-bit AES availability
  - SET services

  - Maximum modulus for key management
  - Maximum elliptic curve field size in bits for key management
- **Other CM Info**
  - API Ordinal Number
  - Firmware Identifier
  - API Version
  - CSP Version
  - Firmware Configuration ID
  - API Configuration ID
  - CSP Configuration ID

Crypto Module Notebook Module Administrators tab

An administrator controls a signature key that allows him or her to sign commands to a host crypto module. Administrator signature keys are stored on smart cards. The administrator has physical possession of the smart card and knows the smart card Personal Identification Number (PIN).

Up to eight administrators can be defined for each domain on a host crypto module, and eight additional administrators can be defined for the host crypto module as a whole. Domain-level administrators are allowed to sign commands to that domain. Crypto-module-level administrators can sign commands to any domain on the crypto module and to the crypto module as a whole.

The signature threshold and revocation signature threshold values on the **Module Attributes** tab determine how many administrators are required to sign commands to the crypto module. Some commands require only a single signature, regardless of how the signature threshold is set. The signature threshold and revocation signature threshold values on the **Domain Attributes** tab determine how many administrators are required to sign commands to that domain.

Administrators are allowed to sign any command. For EP11 crypto modules, there is no concept of "role" (in which the role associated with an administrator defines the set of commands the administrator is allowed to sign).

To work with the crypto-module-level administrators, click the **Module Administrators** tab on the main crypto module notebook page. To work with domain-level administrators, click the **Domains** tab on the main crypto module notebook page, select a domain, and then click the **Domain Administrators** tab for that domain. Right clicking in these pages displays a pop-up menu with options to add or remove an administrator, or generate an administrator signature key and store it on a smart card.

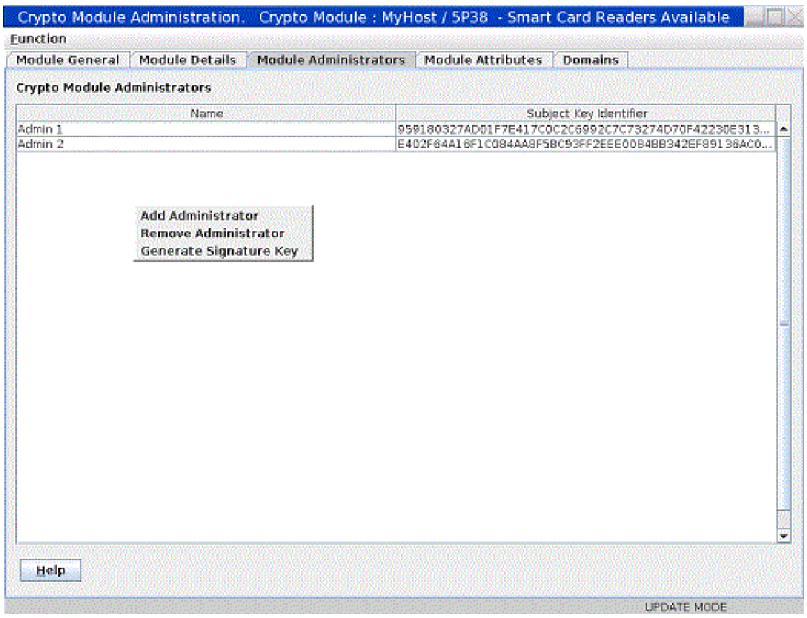


Figure 152. Module Administrators page

EP11 crypto modules identify administrators by using a 32-byte **Subject Key Identifier**, which is a hash of the signature key. The TKE workstation allows users to associate a name of up to 30 characters with each administrator. Users are encouraged to assign unique, meaningful names for each administrator signature key created. The administrator name and subject key identifier are displayed in the administrators list on the Module Administrators page. Both the name and the subject key identifier are written to audit records when commands are signed.

Generate signature key

To generate an administrator signature key and save it on a smart card, right click in the **Module Administrators** page to display the pop-up menu. From the pop-up menu, select the **Generate Signature Key** option.

You are asked to enter an administrator name. Users are encouraged to select unique, meaningful names for each signature key created. After entering the administrator name, you are prompted to insert a smart card in a reader and enter the PIN to complete the operation. The generated key is a 320-bit Brainpool ECC key.

Add administrator

To add an administrator, right click in the **Module Administrators** page to display the pop-up menu. From the pop-up menu, select the **Add Administrator** option.

You are asked to insert a smart card that contains an administrator signature key in a smart card reader and enter the PIN. The public key and administrator name are read from the smart card and used to define an administrator to the EP11 crypto module. Up to eight administrators can be defined.

Remove administrator

To remove an administrator, select the administrator to be removed by left-clicking it in the list of administrators. Then right-click to display the pop-up menu and click **Remove Administrator**. You are not allowed to remove an administrator if

removing it would reduce the number of administrators below the signature threshold value or revocation signature threshold value.

Crypto Module Notebook Module Attributes tab

Use the Module Attributes tab to display a set of attributes associated with the crypto module and change them.

To change the crypto module attributes, type new values in the **Signature Threshold** and **Revocation Signature Threshold** fields and select or clear check boxes in the attributes trees. Then click **Send updates**. If you change your mind you can click **Discard changes**. Your changes are discarded and the page is refreshed with attributes reread from the crypto module.

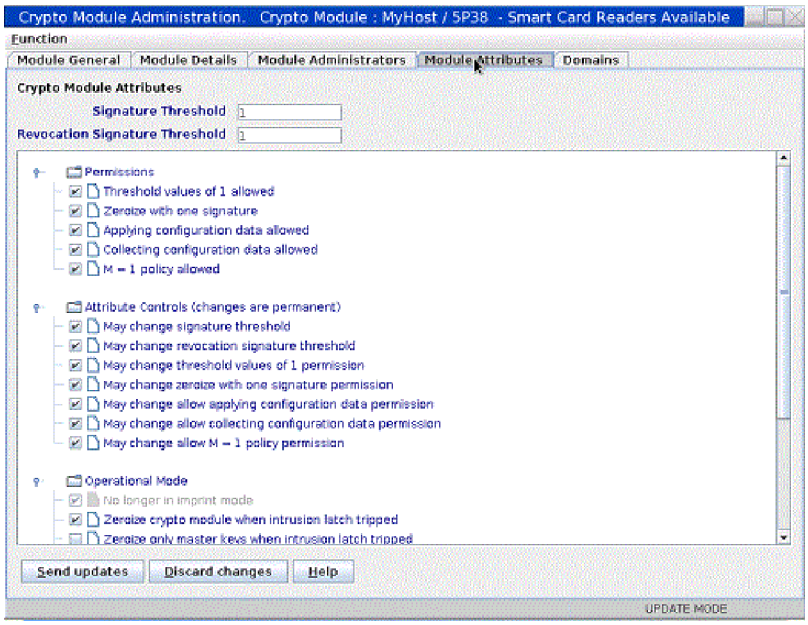


Figure 153. Module Attributes page

Using the Crypto Module Notebook Module Attributes Tab, you can set the following attributes:

- **Signature Threshold** and **Revocation Signature Threshold**.

  The signature threshold controls the number of signatures needed to execute most commands to the crypto module. Some commands require a single signature, regardless of how this attribute is set. Each domain on the crypto module has its own signature threshold attribute, which controls the number of signatures required for most commands sent to that domain. The maximum signature threshold value that can be set is 8.

  The revocation signature threshold controls the number of signatures required to remove a crypto module administrator. The maximum revocation signature threshold value that can be set is 8.

  When the crypto module is zeroized, the signature threshold and revocation signature threshold are set to 0 and the crypto module is put in imprint mode. In imprint mode commands to the crypto module do not require administrator signatures. Imprint mode is intended for initial crypto module setup, before the crypto module is used to manage master keys. To exit imprint mode, set the signature threshold and revocation signature threshold to nonzero values. You

must exit imprint mode at the crypto module level before you can exit imprint mode in any domain on the crypto module.

- **Permissions**.
  - **Threshold values of 1 allowed** - When checked, the signature threshold and revocation signature threshold can be set to 1. If not checked, the signature threshold and revocation signature threshold must be set to values greater than 1.
  - **Zeroize with one signature** - When checked, zeroizing the crypto module requires just one signature, regardless of the signature threshold value. When not checked, the signature threshold value specifies the number of signatures required to zeroize the crypto module.
- **Attribute Controls**

  These check boxes restrict changes to other fields on the panel. After the crypto module is zeroized, these check boxes are all selected and any attribute on the panel can be changed. If you clear one of these check boxes and click **Send updates**, the corresponding attribute is frozen and you are not allowed to change it. You can clear these fields, but you cannot select them again. The crypto module must be zeroized to select them again. You are asked to confirm your choice if you clear one of these fields and click **Send updates**. The attributes controls are:
  - **May change signature threshold** This control allows the crypto module signature threshold value to be changed.
  - **May change revocation signature threshold** This control allows the crypto module revocation signature threshold to be changed.
  - **May change threshold values of 1 permission** This control allows the **Threshold values of 1 allowed** permission to be changed.
  - **May change zeroize with one signature permission** This control allows the **Zeroize with one signature** permission to be changed.
- **Operational Mode**. The operational mode bits are:
  - **No longer in imprint mode**. This bit is read-only and indicates whether the crypto module is in imprint mode. Imprint mode is a temporary condition used for initial setup. Setting the signature threshold and revocation signature threshold to nonzero values exits imprint mode.
  - **Zeroize crypto module when intrusion latch tripped**. When checked this bit specifies that the entire crypto module is to be zeroized when the intrusion latch is set. Physically removing a crypto module from a host system sets the intrusion latch.
  - **Zeroize only master keys when intrusion latch tripped**. When checked, this bit specifies that only the master keys on the crypto module are to be zeroized when the intrusion latch is set. Physically removing a crypto module from a host system sets the intrusion latch. This bit is ignored when the **Zeroize crypto module when intrusion latch tripped** bit is set.
  - **Battery is low**. This bit is read-only and indicates the battery on the EP11 crypto module needs to be replaced.
  - **Crypto module is enabled**. This bit is read-only and indicates whether the crypto module is enabled or disabled. The crypto module can be enabled and disabled by clicking **Enable Crypto Module** and **Disable Crypto Module** on the Module General page.

    Clicking **Enable Crypto Module** and **Disable Crypto Module** on the Module General tab changes the state of the **Crypto module is enabled** bit, the **Zeroize crypto module when intrusion latch tripped** bit, and the **Zeroize only master keys when intrusion latch tripped** bit. When **Disable Crypto**

Module is clicked on the Module General tab, all 3 bits are cleared. This allows the crypto module to be physically removed from the host system without losing configuration data. See "Intrusion latch" on page 201 for the procedure to follow when moving a host crypto module. When the crypto module is enabled by clicking **Enable Crypto Module**, this bit and the **Zeroize crypto module when intrusion latch tripped** bits are checked, but the **Zeroize only master keys when intrusion latch tripped** bit remains unchecked.

- **Standards Compliance Settings**. These bits indicate whether all domains on the crypto module are configured to conform to the indicated industry standard. Domains conform to a standard based on their control point settings. Each domain has its own Standards Compliance Settings attribute. If one or more domains does not conform to a standard, the crypto module as a whole is shown to not conform to the standard. The EP11 crypto module is always compliant with the FIPS 2009 standard, so that **Standards Compliance Settings** attribute is always set. These bits are read-only.

Crypto Module Notebook Domains tab

To manage the administrators, attributes, master keys, and control points for the domains on an EP11 crypto module, click the **Domains** tab in the crypto module notebook. Use the set of tabs on the right side of this page to select a domain to manage. Tabs are present only for those domains configured using the Support Element as control domains for the TKE workstation. Select a domain by clicking it. A set of tabs is displayed at the bottom of the page with functions to manage domain facilities: **Domain General**, **Domain Administrators**, **Domain Attributes**, **Domain Keys**, and **Domain Control Points**.

In a domain group notebook, the **Domains** tab is replaced by a **Domain** tab, and there is no list of control domains on the right side of the page. In a domain group notebook, the displayed attributes, administrators, keys, and control points are from the master domain of the group. Updates made in a domain group notebook are made to all member domains of the group, or to all crypto modules with at least one domain in the domain group.

Domain General page

The domain general page displays the domain index and domain description for the domain, and contains a **Zeroize domain** push button that allows the domain to be zeroized. For domain groups, the index and description of the master domain are displayed, and a **Zeroize domain group** push button replaces the **Zeroize domain** push button. Clicking **Zeroize domain group** causes all member domains to be zeroized.

You can change the domain description by typing a new description in the text box and clicking **Send updates**. If you change your mind after entering a new description, you can click **Discard changes**. Your changes are discarded and the existing domain description is refetched from ICSF. Updating the description in a domain group notebook causes the description of all member domains to be updated.

Zeroizing a domain has the following effects:

- The signature threshold and revocation signature threshold are set to zero, and the domain re-enters imprint mode. See "Imprint mode" on page 198.
- The domain permissions, attribute controls, and operational mode bits are set to their default values.

- All domain administrators are removed.
- The domain new master key and current master key are erased. Any data in the ICSF PKCS #11 token data set (TKDS) encrypted by the current master key becomes unrecoverable.
- All domain control points are set.

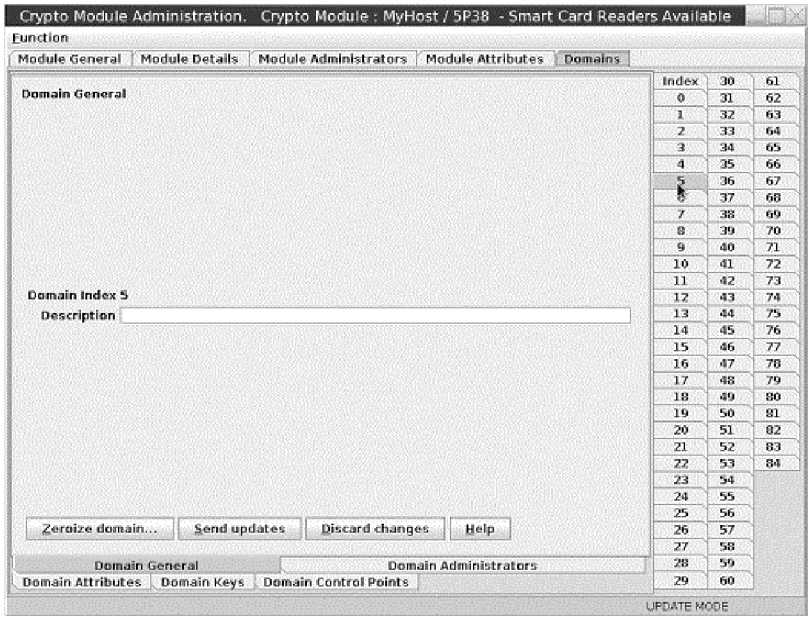


Figure 154. Domain General page

Domain Administrators page

The domain administrators page is identical to the module administrators page, but manages the domain administrators rather than the crypto module administrators. See "Crypto Module Notebook Module Administrators tab" on page 203 for a description of this page.

Domain Attributes page

Use the Domain Attributes tab to display a set of attributes associated with the domain and change them. The attributes displayed are:

- Signature Threshold
- Revocation Signature Threshold
- Permissions
- Attribute Controls
- Operational Mode
- Standards Compliance Settings

To change the domain attributes, type new signature thresholds in the text fields or select or clear check boxes in the attributes trees. Then click **Send updates**. If you change your mind, you can click **Discard changes**. Your changes are discarded and the page is refreshed with domain attributes reread from the crypto module.

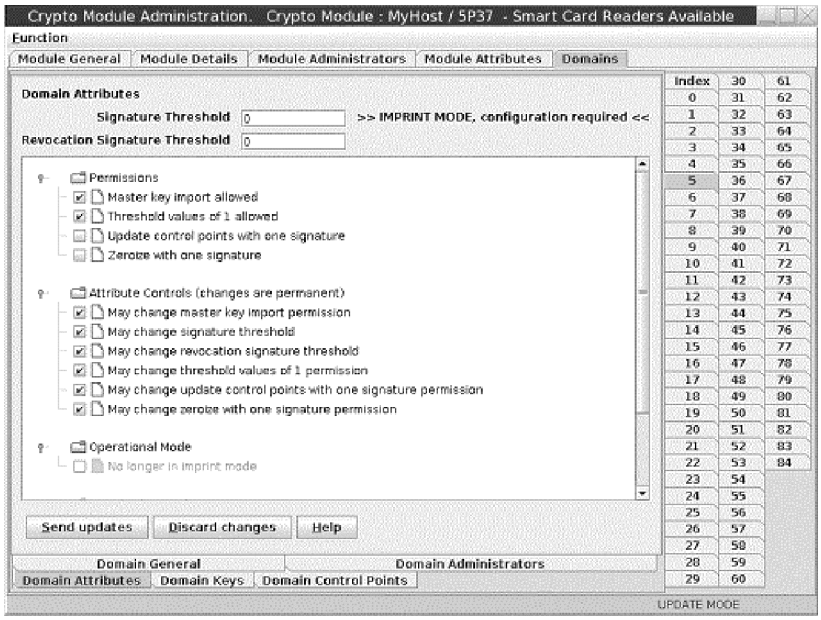


Figure 155. Domain Attributes page

Using the Domain Attributes tab, you can set the following attributes:

- **Signature Threshold** and **Revocation Signature Threshold**.

  The signature threshold controls the number of signatures needed to execute most commands to the domain. Some commands require a single signature, regardless of how this attribute is set. The maximum signature threshold value that can be set is 8.

  The revocation signature threshold controls the number of signatures required to remove a domain administrator. The maximum revocation signature threshold value that can be set is 8.

  When the domain is zeroized, the signature threshold and revocation signature threshold are set to 0 and the domain is put in imprint mode. In imprint mode you can add and remove administrators, zeroize the domain, and change attributes, but you are not allowed to load or clear the master keys or change the domain control points. Imprint mode is a temporary condition intended for initial setup. To exit imprint mode, set the signature threshold and revocation signature threshold to nonzero values. You must exit imprint mode at the crypto module level before you can exit imprint mode in the domain.
- **Permissions**. When a permissions bit is checked, the operation is allowed. When the permissions bit is unchecked, the operation is prohibited.
  - **Master key import allowed** - allows the new master key register in the domain to be loaded.
  - **Threshold values of 1 allowed** - When selected, the signature threshold and revocation signature threshold can be set to 1. If not selected, the signature threshold and revocation signature threshold must be set to values greater than 1.
  - **Update control points with one signature** - When selected, updating the control points requires a single signature. When not selected, the signature threshold specifies the number of signatures needed to update the control points.

  - **Zeroize with one signature**- When selected, zeroizing the domain requires just one signature, regardless of the signature threshold value. When not selected, the signature threshold value specifies the number of signatures required to zeroize the domain.
- **Attribute Controls**. Use these check boxes to restrict changes to other fields on the panel. After the domain is zeroized, these check boxes are all selected and any attribute on the panel can be changed. If you clear one of these check boxes and click **Send updates**, the corresponding attribute is frozen and you are not allowed to change it. You can clear these checkboxes, but you cannot reselect them. The domain must be zeroized to select them again. You are asked to confirm your choice if you clear one of these check boxes and click **Send updates**.
  - **May change master key import permission** - controls whether the **Master key import allowed** permission can be changed.
  - **May change signature threshold** - controls whether the domain signature threshold value can be changed.
  - **May change revocation signature threshold** - controls whether the domain revocation signature threshold value may be changed.
  - **May change threshold values of 1 permission** - controls whether the **Threshold values of 1 allowed** permission can be changed.
  - **May change update control points with one signature permission** - controls whether the **Update control points with one signature permission** can be changed.
  - **May change zeroize with one signature permission** - controls whether the **Zeroize with one signature** permission can be changed.
- **Operational Mode**. The operational mode bits are:
  - **No longer in imprint mode**. This bit is read-only and indicates whether the domain is in imprint mode. Imprint mode is a temporary condition used for initial setup. Setting the signature threshold and revocation signature threshold to nonzero values exits imprint mode.
- **Standards Compliance Settings**. These bits indicate whether the domain is configured to conform to the indicated industry standard. Domains conform to a standard based on their control point settings. These bits are read-only.

Domain Keys page

The domain keys page displays the status and verification pattern of the new master key register and current master key register for the domain.

The current master key encrypts all data stored for the domain in the ICSF PKCS #11 token data set (TKDS). To change the current master key, first the new master key register must be loaded, using two or more key parts stored on smart cards.

Right clicking in the page causes a pop-up menu to be displayed. From this menu you can select the following operations:

- **Generate key part** - Generate a random master key part value and save it on a smart card.
- **Load new master key** - Load the new master key register on the host crypto module using two or more key parts previously saved on smart cards.
- **Commit new master key** - Commit the value in the new master key register. The value in the new master key register must be committed before ICSF can use it to re-encrypt data in the TKDS for the domain.

- **Set, immediate** - Sets the new master key, but without re-encrypting the data in the TKDS for the domain.

  Normally, use ICSF procedures or services that coordinate setting the master key with initializing or re-encrypting TKDS. This option sets the master key but does not change TKDS. If used inappropriately, this option causes the data in the TKDS to become unusable when accessed by ICSF in the domain.

  Use this option only when the TKDS does not need to be initialized or re-encrypted when the master key is set. For example, this option can be used to reload the previous master key value if a host crypto module has been inadvertently zeroized.
- **Clear new master key** - Clear the new master key register.
- **Clear current master key** - Clear the current master key register. Use this option with caution. Any data stored in the ICSF TKDS for the domain becomes unusable. You are asked to confirm this choice
- **Secure key part entry** - Use the PIN pad on the smart card reader to enter a known key part value and save it on a smart card.

After the new master key register is loaded and its value is committed, ICSF can re-encrypt data in the TKDS for the domain. After all data is re-encrypted, ICSF can finalize the new master key. Finalizing moves the value in the new master key register to the current master key register and changes the state of the new master key register to *Empty*.

The domain keys panel in a domain group notebook shows the status and verification patterns of the master key registers in the master domain. When load, commit, and clear options are executed in a domain group, commands are sent to each member domain of the domain group.

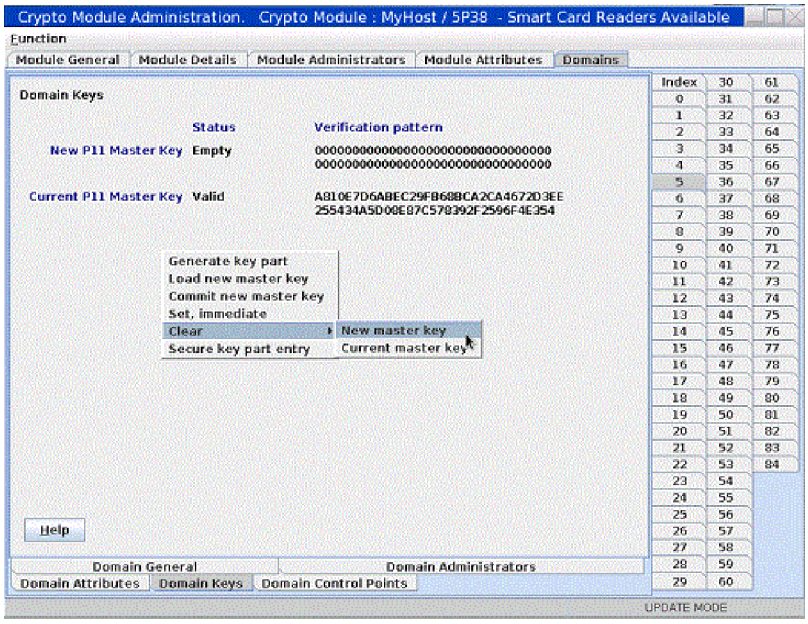


Figure 156. Domain Keys page

Generate key part

To generate one or more EP11 master key parts and save them on smart cards, right click in the Domain Keys page to display the pop-up menu. From the pop-up menu, select the **Generate key part** option.

You are asked to enter the number of key parts you want to generate. For each key part, you are guided through the process of selecting a smart card reader to use, inserting a smart card in the reader, entering the PIN, and entering a description to associate with the key part. You can cancel at any time.

Load new master key

To load the new master key register for the domain, right click in the Domain Keys page to display the pop-up menu. From the pop-up menu, select the **Load new master key** option.

You are asked to enter the total number of key parts to be loaded. For each key part, you are guided through the process of selecting a smart card reader to use, inserting a smart card in the reader, entering the PIN, and selecting the key part on the smart card to be loaded. You can cancel at any time.

Key parts on the smart card are encrypted for transport to the host crypto module using Elliptic Curve Diffie-Hellman (ECDH). The first step in ECDH is to generate an IMPORTER key on the crypto module. Generating the key requires a signed command. Therefore, signatures are collected twice when you run the Load New Master Key option – once to generate an IMPORTER key and once to do the final load. Both commands require only a single signature, regardless of how the domain signature threshold is set.

Secure key part entry

To enter a known value for an EP11 master key part onto a smart card, right click in the Domain Keys page to display the pop-up menu. From the pop-up menu, select the **Secure key part entry** option.

The same process is followed for secure key part entry of EP11 master key parts as for secure key part entry of other key types. See Appendix A, “Secure key part entry,” on page 303 for details on this process.

Domain Control Points page

Use the Domain control points page to display the set of control points that are currently active for the domain and change them. When selected, a control point permits an operation in the domain. When not selected, the operation is not allowed.

To change control points, select or clear check boxes to select or deselect individual control points. Then click **Send updates** to send the changes to the host crypto module. If you change your mind, you can click **Discard changes**. Any changes you made are discarded and the page is refreshed with the current control points for the domain.

You can save the displayed control points to a file by clicking **Save to file**. You can load the control points from a previously saved file by clicking **Load from file**. In both cases, a window opens in which you can select the file to use. After loading the control points from a file, click **Send updates** to send the changes to the host crypto module.

Right click in an open area of the page to display a pop-up menu. From this menu you can reset collections of control points to ensure conformity with an operating standard such as FIPS or BSI. After selecting the wanted standard, click **Send updates** to send the updates to the host crypto module.

Use care when deselecting control points in the Control Point Management category. These control points can be used to prevent further updates to the control points for the domain. After these control points are turned off, further updates to the control points are not permitted. The domain must be zeroized before the control points can be changed again. You are asked to confirm your choice when turning off these control points.

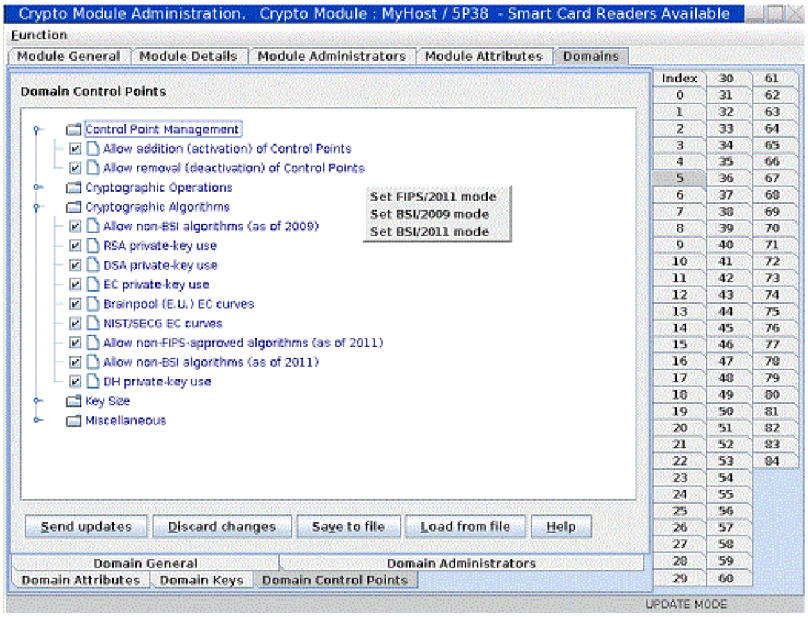


Figure 157. Domain Control Points page

Chapter 9. Auditing

TKE implements logging of security relevant operations that occur on the TKE workstation. TKE provides auditors with a trail of activities on the TKE workstation that are not currently tracked. Security actions 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 data set.

ICSF also uses SMF record type 82 to record certain ICSF events. ICSF writes to subtype 16 whenever a TKE workstation either issues a command request to, or receives a reply response from, a CCA or EP11 crypto module. In addition to the subtype 16 records, you can use the TKE Audit Record Upload Configuration Utility to send Trusted Key Entry workstation security audit records to a System z host. These security audit records are stored in the SMF data set as a type 82 subtype 29 record.

TKE Audit Configuration utility

To configure auditing, log on with the AUDITOR user name, select **Trusted Key Entry** and then select the **Audit Configuration Utility**.

The TKE Audit Configuration Utility is displayed.

By default, all available auditing is enabled.

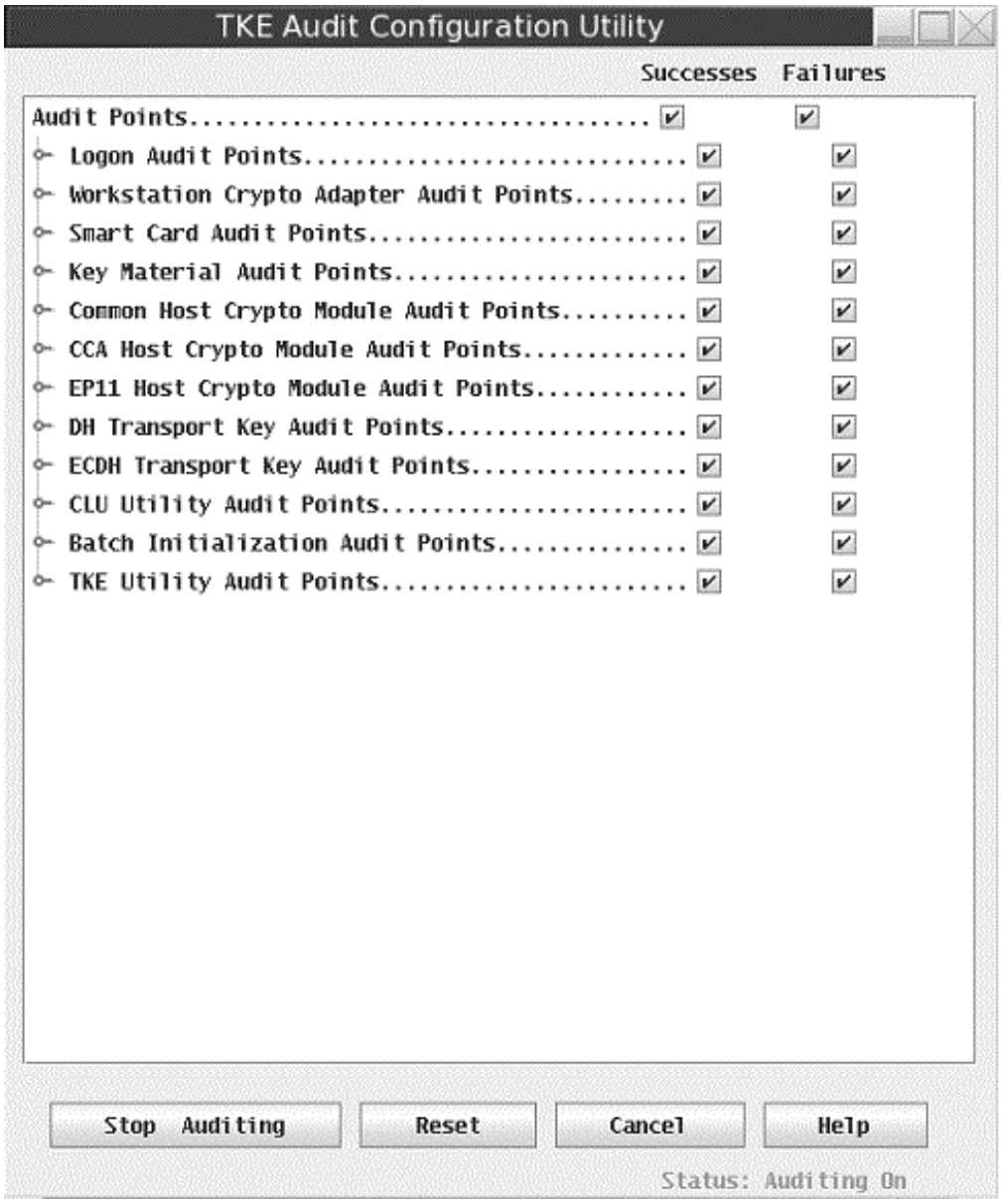


Figure 158. Default settings for auditing

You can customize the auditing utility to your desired preference. To turn off auditing, click on **Stop Auditing** to change the status to **Auditing Off**.

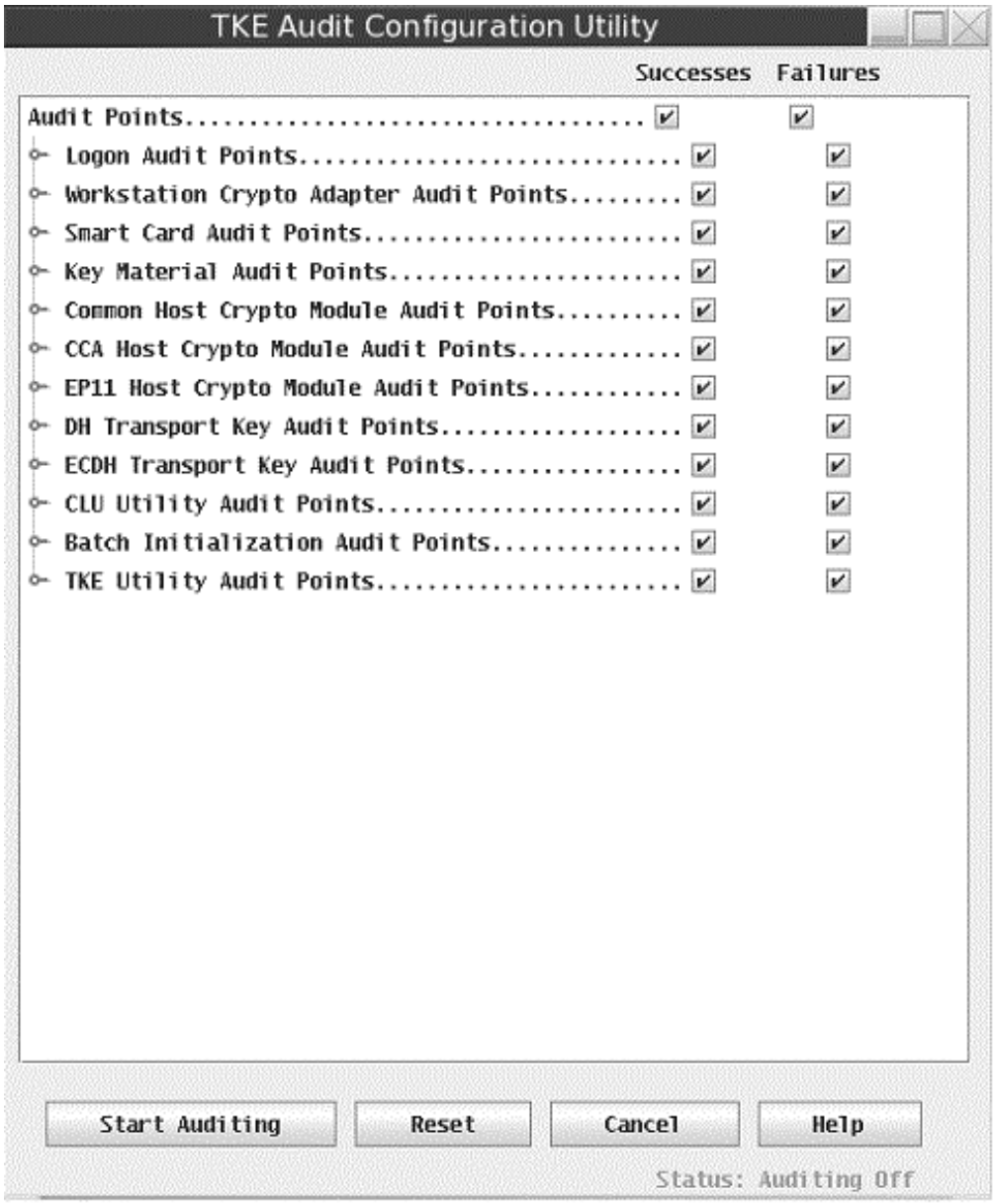


Figure 159. Auditing is off

If you wish to enable and disable specific audit records (both successes and failures) you can expand each audit point to see the individual audit records associated with the group by clicking on the symbol to the left of the audit point.

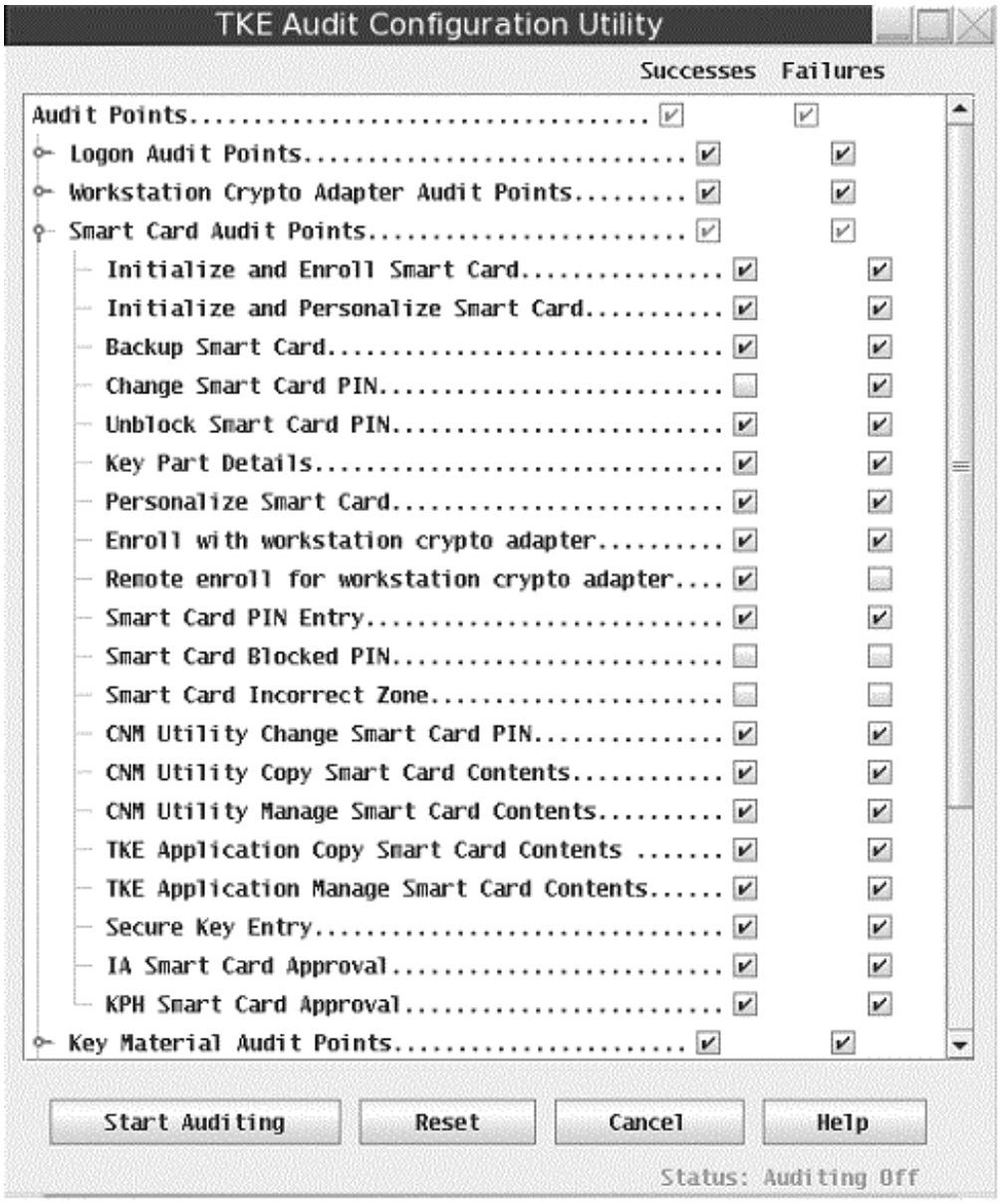


Figure 160. Example of expanded auditing points

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 maximum size of 30 MB.

When the security log reaches 75% full, a hardware message alerts the user on the TKE console. The View Security Logs task determines whether the message displays. By default, the message displays.

When the security log reaches 100% capacity, the oldest third of the audit records are deleted.

In order to avoid deleting records you can archive the security logs (see "Archive security logs" on page 223).

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

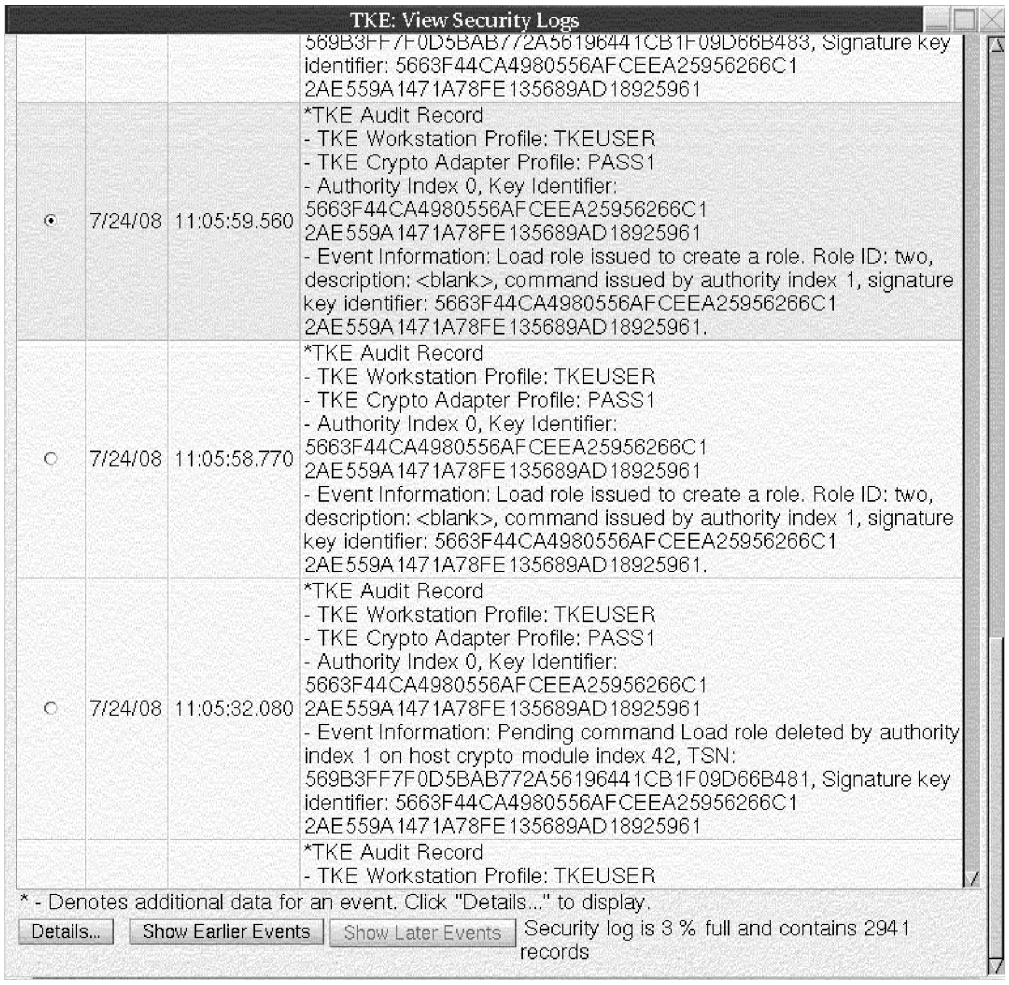


Figure 161. Viewing the security logs

This log displays 1000 records per page. The 1000 record pages can be navigated by clicking on **Show Earlier Events** and **Show Later Events**.

If the audit record contains an asterisk (*) next to the line saying 'TKE Audit Record', this means that there are further details available to view. You can view

the details by selecting the radio button corresponding to the desired audit record and clicking **Details**.

Figure 162. Viewing additional details of the security logs

Audit and log management

Audit and log management copies the console events log, security log, and tasks performed log to a USB flash memory drive. Select **Service Management** and, from the service management window, select **Audit and Log Management**.

The Audit and Log Management dialog box is displayed.

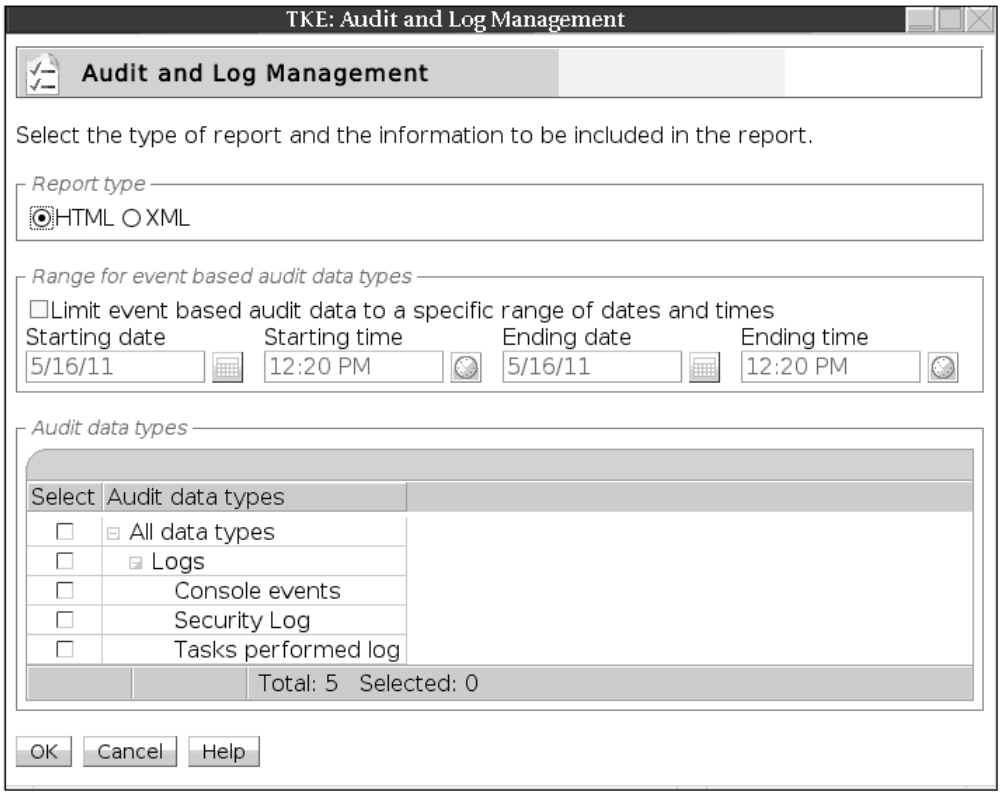


Figure 163. Audit and Log Management dialog

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

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

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

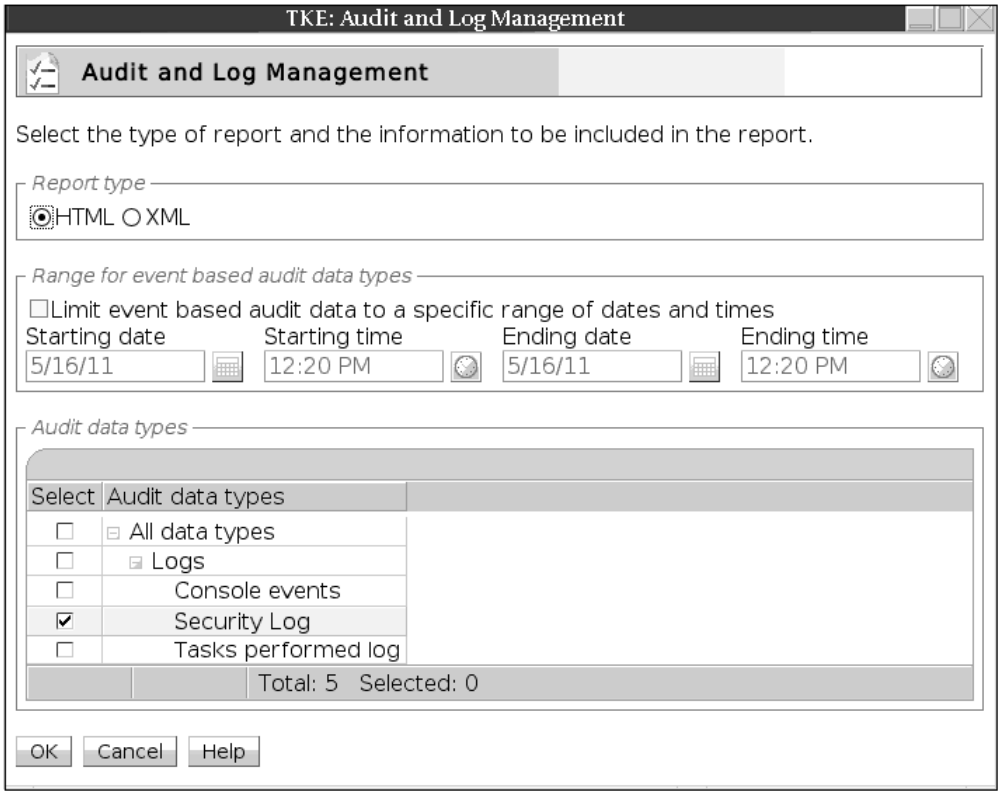


Figure 164. Audit and Log Management dialog (security log data selected)

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

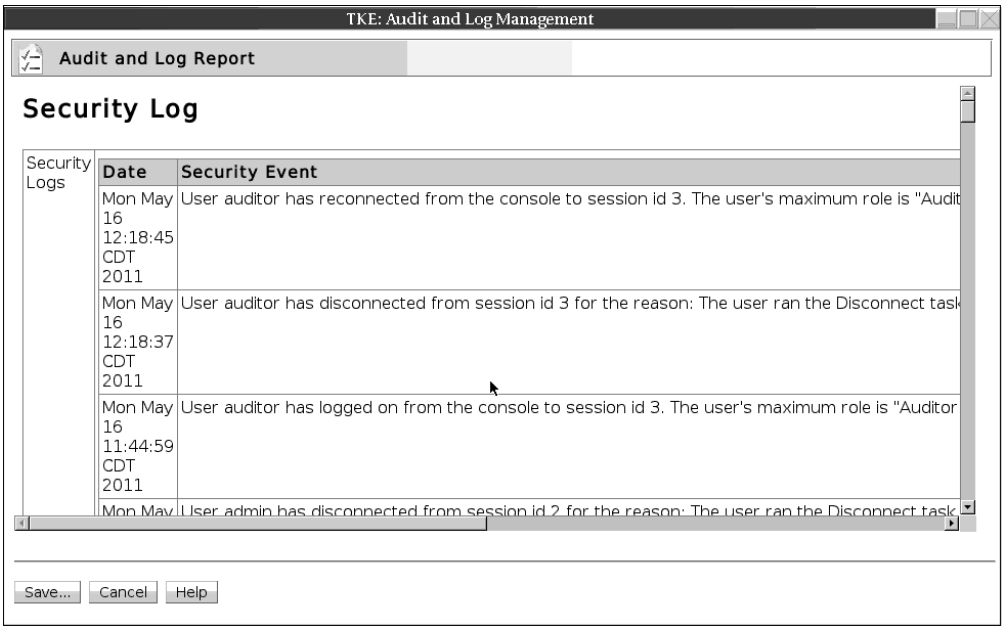


Figure 165. Security Log

This window contains the report produced from the log data. To save the report to a USB flash memory drive, click **Save**. The Export Data window opens.

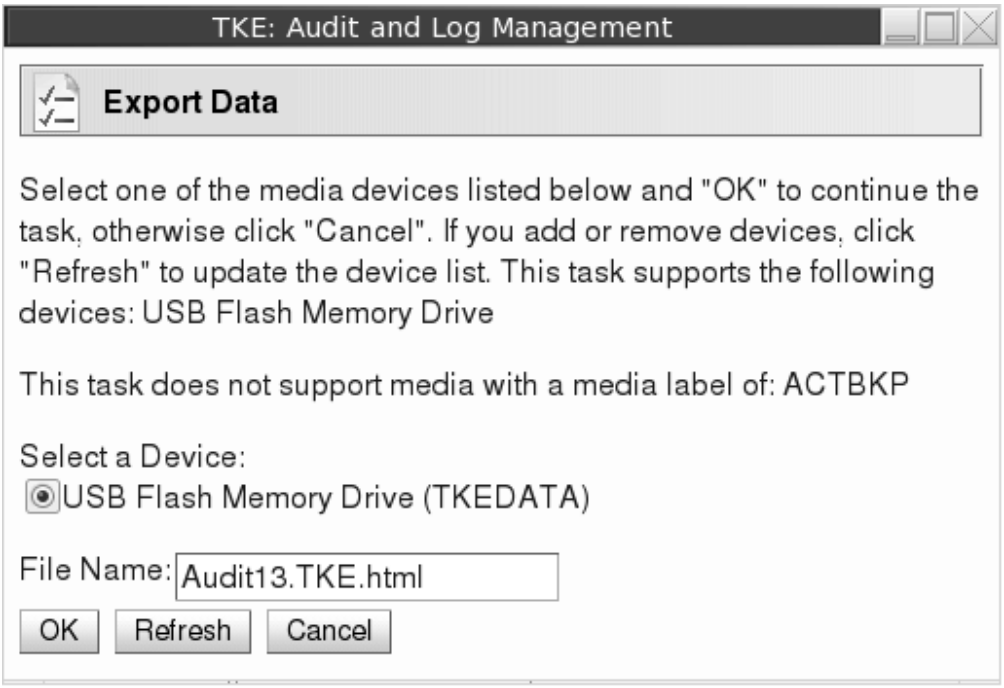


Figure 166. Export Data

Note: If a USB flash memory drive is not currently present, nothing is listed under **Select a Device**. To write to a USB flash memory, drive insert the drive, wait for the USB Device Status window to appear, and then click **Refresh**. When **OK** is clicked, the report is saved with the specified file name to the USB flash memory drive.

A 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 USB flash memory drive, and then erases enough events from the security log to reduce its size to 20% of its maximum capacity.

In order to Archive the Security log, log in as the AUDITOR user and select **Service Management**. From the service management window select **Archive Security Logs**.

Note: You must have a USB flash memory drive that is formatted with no volume label or a volume label of ACTSECLG. Use the Format Media utility to format the flash memory drive (see "Format media" on page 351).

Figure 167. Archiving the security logs

With a valid USB flash memory drive inserted, click **Archive**.

While the security log is being archived, an "Archiving Security Log..." message box displays. After the archiving is completed, a message box displays indicating that the archive operation has completed.

TKE Audit Record Upload Configuration utility

ICSF uses SMF record type 82 to record certain ICSF events. ICSF writes to subtype 16 whenever a TKE workstation either issues a command request to, or receives a reply response from, a CCA or EP11 crypto module. In addition to the subtype 16 records, you can use the TKE Audit Record Upload Configuration Utility to send Trusted Key Entry workstation security audit records to a 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 the TKE Audit Record Upload Configuration utility

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

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

To start the TKE Audit Record Upload Configuration utility, go to the Trusted Key Entry Console Workplace window and select *TKE Audit Record Upload Utility*.

The TKE Audit Record Upload Configuration Utility window is displayed.

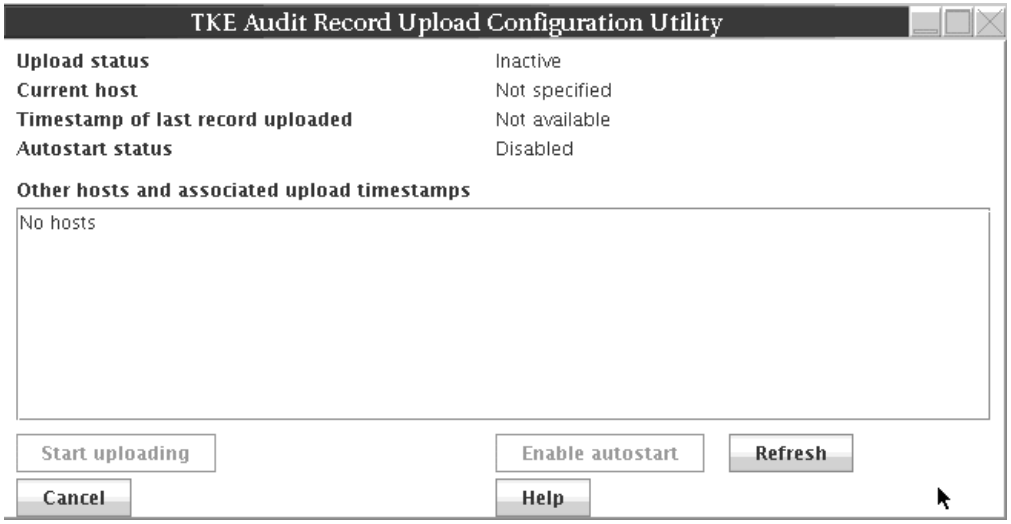


Figure 168. TKE Audit Record Upload Configuration utility

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 226 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 227 for more information.

Configure TKE for audit data upload

To upload audit data to a host system, you need to add the target host to the TKE Audit Record Upload utility's host list, and make the target host the current host. To do this:

1. Add the target host to the TKE Audit Record Upload utility's host list. To do this:

a. In the TKE Audit Record Upload Configuration Utility window, right click to display a popup menu, and select the **Add Host** menu item.

   The Specify Host Information dialog is displayed.

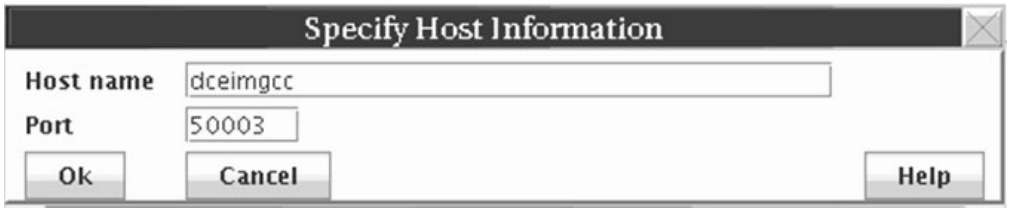


Figure 169. Specify Host Information dialog

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** push button.

   The Specify Host Information dialog closes and the host name is added to the TKE Audit Record Upload Configuration Utility's host list. The host name will appear in the *Other hosts and associated timestamps* area of the window.

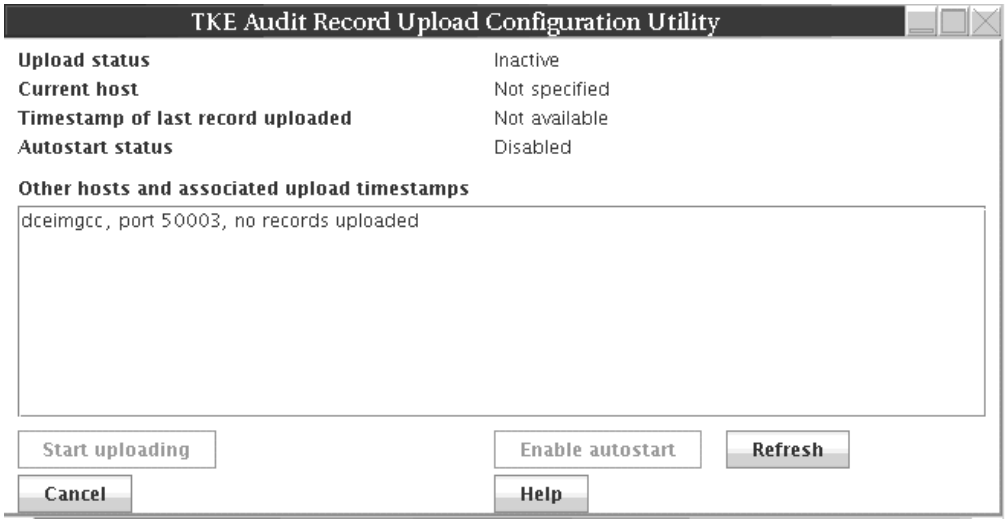


Figure 170. Other hosts and associated timestamps

2. Make the target host the current host. To complete this step, you must have a user ID and password for the target host.

   a. In the TKE Audit Record Upload utility window's *Other hosts and associated timestamps* area, click on the target host name to highlight it.

   b. In the TKE Audit Record Upload utility window's *Other hosts and associated timestamps* area, right click on the target host name to display a popup menu, and select the **Specify current host** menu item.

      The Specify Host Login Information dialog is displayed.

Figure 171. Specify Host Login Information

c. In the Specify Host Login Information dialog, enter the user ID and password, and click the **Ok** push 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" on page 227 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 224), you can upload audit records to the target host. If you have not already logged onto the host system during this session, the Specify Host Logon Information dialog will prompt you for a user ID and password before the audit records will be uploaded. To complete this task, you must have a user ID and password for the target host.

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

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

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

- Pressing the **Refresh** push button will refresh the TKE Audit Record Upload Utility window. In particular, the Timestamp of last record uploaded field will be updated.
- Pressing the **Stop uploading** push button will stop the audit record upload.

You can also enable automatic audit record upload. When enabled, audit records will be uploaded every time the workstation is rebooted. See "Enabling and disabling automatic audit record upload" on page 227 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 224), you can enable automatic audit record upload. This is called autostart mode. In autostart mode, audit records will be uploaded every time the workstation is rebooted. If you have not already logged on to the host system during this session, the Specify Host Logon Information dialog will prompt you for a user ID and password before autostart mode will be enabled. To complete this task, you must have a user ID and password for the target host.

In the TKE Audit Record Upload Utility window, click the **Enable autostart** push button.

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

The TKE Audit Record Upload Configuration Utility will enable autostart mode, and will upload audit records every time the workstation is rebooted. The TKE Audit Record Upload Configuration Utility window's Autostart status field will indicate that autostart is enabled.

To disable automatic audit record upload, click the **Disable autostart** push button.

Chapter 10. Managing keys using TKE and ICSF

Master keys are used to protect all cryptographic keys that are active on your system.

Because master key protection is essential to the security of the other keys, ICSF stores the master keys within the secure hardware of the cryptographic feature. This nonvolatile key storage area is unaffected by system power outages, because it has a battery backup. The values of the master keys never appear in the clear outside the cryptographic feature.

Requirements: ICSF is required to complete some operations initiated from TKE:

- For CCA host crypto modules, operations that require ICSF include setting the master keys, loading operational keys into the CKDS, and loading RSA keys from a host data set to the PKDS.
- For CCA host crypto modules, ICSF is also required for initializing or refreshing the CKDS, disabling and enabling PKA services, PKDS initialization, PKDS reencipher, and PKDS activate.
- For EP11 host crypto modules, operations that require ICSF include first time setting of the P11 master key, any subsequent P11 master key change, initializing or updating the TKDS, and reenciphering the TKDS.

For more information about these ICSF procedures, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

Attention: Be prepared to switch between your TKE workstation and your ICSF host session.

Note: Under normal circumstances, set master keys using ICSF services that coordinate setting the master key with initializing or re-enciphering key storage. Failure to do this can cause the keys or tokens in key storage to become unusable when accessed by ICSF. There are some exceptions.

- ICSF prior to HCR7790 allows the RSA master key to be set from TKE using the **Set** option, but PKA Callable Services must be disabled first. If no online host crypto modules are at the September 2011 LIC level or later, ICSF at HCR7790 or later also allows the RSA master key to be set from TKE using the **Set** option.
- Beginning with TKE V7.30, the **Set, immediate** option allows any master key to be set from TKE. Use this option only when key storage does not need to be initialized or re-enciphered when the master key is set. For example, this option can be used to reload a previous master key value if a host crypto module has been inadvertently zeroized.

Changing master keys

For security reasons your installation should change the master keys periodically. In addition, if the master keys have been cleared, you might want to change the master keys after you reenter the cleared master keys.

For CCA host crypto modules, the DES and AES master keys protect the Cryptographic Key Data Set (CKDS). There are three main steps involved in changing the DES or AES master key:

1. Load the DES or AES master key parts into the new master key register.
2. Reencipher the CKDS under the new DES or AES master key.
3. Change the new DES or AES master key and activate the reenciphered CKDS.

In the first step, DES and AES master key parts can be loaded using TKE, or from ICSF panels. The second and third steps are performed using ICSF, or can be done using the Coordinated KDS Change Master Key utility (HCR7790 or higher). For information about this utility, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

For CCA host crypto modules, the RSA and ECC (APKA) master keys protect the Public Key Data Set (PKDS). There are six main steps involved in changing the RSA or ECC (APKA) master key:

1. Disable PKA Services (required to load the RSA master key).
2. Enter the RSA or ECC (APKA) master key parts into the new master key register.
3. Reencipher the PKDS under the new RSA or ECC (APKA) master key.
4. Change the new master keys and activate the reenciphered PKDS.
5. Enable PKA Services.
6. Enable Dynamic PKDS Access.

RSA and ECC (APKA) master key parts can be loaded using TKE or from ICSF panels. The other steps are performed using ICSF, or can be done using the Coordinated KDS Change Master Key utility (HCR77A0 or higher). For information about this utility, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

Notes:

1. On older versions of ICSF, the RSA master key is called the asymmetric master key.
2. ICSF uses the term 'ECC master key'. CCA calls it the 'APKA master key'. On TKE, it is referred to as the 'ECC (APKA) master key'.
3. Steps 1, 5, and 6 are not required on z196/z114 and newer systems.

For EP11 host crypto modules, the P11 master keys protect the PKCS #11 token key data set (TKDS).

If multiple instances of ICSF share the same TKDS in a sysplex environment, the P11 master key must be set to the same value for each instance. All instances must be at HCR77A0 or higher, even if they do not use secure PKCS #11 services. A TKE domain group can be used to manage the multiple domains of the ICSF instances so that all receive the same new P11 master key value.

There are three main steps involved in changing the P11 master key:

1. Load the P11 master key parts into the new master key register.
2. Create a VSAM data set to hold the reenciphered keys.
3. Do a coordinated TKDS master key change.

In the first step, P11 master key parts must be loaded using TKE. There is no ICSF option to load P11 master key parts. ICSF is required to perform the other steps.

For step-by-step ICSF procedures for changing master keys, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

Adding host crypto modules after ICSF initialization

You might want to add additional host crypto modules to your system. After the new crypto modules have been installed and configured by the appropriate hardware personnel, make them known to the TKE workstation by following the appropriate procedure.

1. Open the Host where the crypto module or modules were added. You will be prompted to authenticate the crypto module.
2. Open the new crypto module or modules.
3. Use the authority 0 default signature key to administer access control (create the same roles and authorities for the new crypto module to match the crypto modules currently on the host). Load the authority signature keys to match the other crypto modules.
4. Load a new signature key for an authority that can load master keys. If one authority does not have the ability to load all the master key parts for each master key, you may need to load additional authority signature keys.
5. Load the master keys.

   Note: The keys should be the same keys that you loaded to the other crypto modules. If you are adding more than one crypto module, load the keys in all crypto modules before setting the master key.
6. Set the DES or AES master key on the crypto module from ICSF when everything is the same (roles, authorities, controls, master keys).
7. If desired, add the new crypto module to the group by doing a group change.

Loading operational keys to the CKDS

You can load operational key parts into 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. Domain controls X'029E' - Operational Key Load - Variable-Length Tokens and X'0309' - Operational Key Load 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

```
HCR77A0  -------------- 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, KDS Processing
  3  OPSTAT           -  Installation options
  4  ADMINCNTL        -  Administrative Control Functions
  5  UTILITY          -  ICSF Utilities
  6  PPINIT           -  Pass Phrase Master Key/KDS Initialization
  7  TKE              -  TKE Master and Operational Key processing
  8  KGUP             -  Key Generator Utility processes
  9  UDX MGMT         -  Management of User Defined Extensions
```

Figure 172. ICSF primary menu panel

2. The Coprocessor Management panel appears. Put a 'K' by the coprocessor that contains the key part register to load.

```
------------------------ ICSF Coprocessor Management -------- Row 1 to 1 of 1
COMMAND ===>                                                 SCROLL ===> PAGE

 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            AES   DES   ECC   RSA   P11
  -----------   -------------    ------            ---   ---   ---   ---   ---
K   G41         99001193         ACTIVE             A     A     U     U
.   SP45        97006046         ONLINE                                     U
****************************** Bottom of data ********************************
```

Figure 173. Coprocessor Management panel

3. The Operational Key Load panel appears. The coprocessor previously selected and the active CKDS are displayed at the top of the panel.

```
------------------------ ICSF - Operational Key Load -------------------------
COMMAND ===>

Coprocessor selected for new key:  G41
CKDS Name:  SUIMGCD.PRIVATE.CRP230.SCSFCKDS

Enter the key label.

Key label
===> DES.IMPPKA.0305

Control Vector ===> YES  YES or NO
```

Figure 174. Operational Key Load panel

   a. In the key label field, enter the CKDS entry label for the key. The label must match the key label specified on the key part information window on TKE when the First key part was loaded to the key part register. Otherwise, a `KEY NOT FOUND` message is displayed. See "Load to Key Part Register First" on page 170.
   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.

```
---------------------- ICSF - DES Operational Key Load --- CKDS RECORD EXISTS
COMMAND ===>

A record with the following specifications has been found in the CKDS:

Key label: DES.IMPPKA.0305
Key type : IMP-PKA
```

Figure 175. Operational Key Load panel

When a DES operational key is successfully loaded, the ENC-ZERO value and control vector are displayed for the user. When an AES operational key is successfully loaded, the AES-VP is displayed.

```
------------------------ ICSF - Operational Key Load ------ KEY LOAD COMPLETE
COMMAND ===>

Coprocessor selected for new key:  G41
CKDS Name:  SUIMGCD.PRIVATE.CRP230.SCSFCKDS

Enter the key label.

Key label
===> DES.IMPPKA.0305

Vector ===> YES  YES or NO
ENC-ZERO VP:         77C92984

Control vector:      0042050003410000    0042050003210000
```

Figure 176. Operational Key Load Panel - ENC-ZERO and CV values displayed

```
------------------------- ICSF - Operational Key Load ------ KEY LOAD COMPLETE
COMMAND ===>

Coprocessor selected for new key:  G41
CKDS Name:  SUIMGCD.PRIVATE.CRP230.SCSFCKDS

Enter the key label.

Key label
===> AES.IMPORTER.0305

Control Vector ===> YES  YES or NO

AES-VP:              8B0CEDFD74D1CC3E
```

Figure 177. Operational Key Load Panel - AES -VP displayed

Installing RSA keys in the PKDS from a data set

If you used TKE to load an RSA key into a host data set member, you load it from the data set to the PKDS by this method.

1. Select Option 7, TKE, on the ICSF Primary Option Menu.

```
HCR77A0  -------------- 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, KDS Processing
  3  OPSTAT           -  Installation options
  4  ADMINCNTL        -  Administrative Control Functions
  5  UTILITY          -  ICSF Utilities
  6  PPINIT           -  Pass Phrase Master Key/KDS Initialization
  7  TKE              -  TKE Master and Operational Key processing
  8  KGUP             -  Key Generator Utility processes
  9  UDX MGMT         -  Management of User Defined Extensions
```

Figure 178. Selecting the TKE option on the ICSF Primary Menu panel

2. The TKE Processing Selection panel appears. Select option 3.

```
----------------------- 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 179. 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.

```
------------------------- ICSF - PKA Direct Key Load -------------------------
COMMAND ===>

 Enter the data set name and the key specifications.

 Key Data Set
  Name   ===> 'SUIMGCD.PRIVATE.RSAKEYS.AES(R0525A)'
```

Figure 180. PKA Direct Key Load

If the RSA key is loaded successfully into the PKDS, a **LOAD COMPLETED** message is displayed in the upper right corner. If an error occurs during the load process, an applicable error message is displayed in the upper right corner with detailed error information displayed in the middle of the display for selected errors. You may also press the PF1 key for more information.

Chapter 11. Cryptographic Node Management utility (CNM)

The Cryptographic Node Management (CNM) utility is a Java application that provides a graphical user interface to initialize and manage the TKE workstation crypto adapter. It is part of the IBM Cryptographic Coprocessor CCA Support Program.

This topic describes the functions of CNM that are used for initializing and managing the TKE workstation crypto adapter.

Note: Smart Card and Smart Card Group options within the CNM panels will only be available if CNM is enabled to support Smart Cards. See “Initializing the TKE workstation crypto adapter for use with smart card profiles” on page 77.

To start CNM, click with the left mouse button on the "Trusted Key Entry" link in the left panel of the main Trusted Key Entry Console page. Then, under the "Applications" section displayed in the right panel, click with the left mouse button on "Cryptographic Node Management Utility".

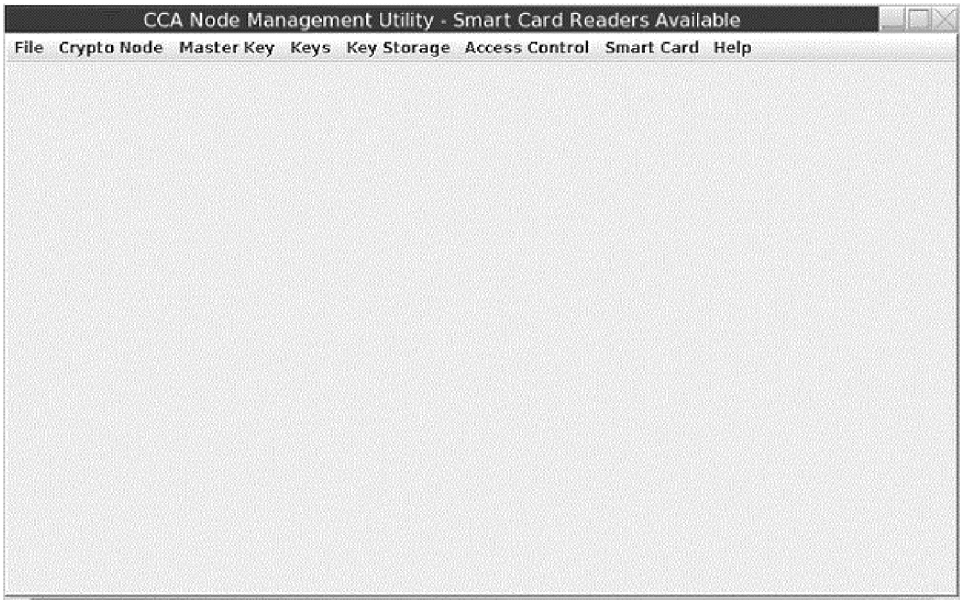


Figure 181. CNM main window

Crypto adapter logon

To run the Cryptographic Node Management utility (CNM), you must log on to the TKE workstation crypto adapter. If you start CNM and are not already logged on to the TKE workstation crypto adapter, you will be prompted to select a user profile and log on (as described in “Crypto adapter logon: passphrase or smart card” on page 93).

Only profiles authorized to run CNM will be displayed. If, when you start CNM, you are logged on to the TKE workstation crypto adapter with a profile that is not

authorized to run CNM, a warning will be displayed and you will be asked if you want to log off and log on with a different user profile.

File menu

From the **File** pull-down, you can choose the following actions:

CNI editor
The CNI editor is a utility within the CNM utility that is used to create CNI scripts to automate some of the functions of CNM.

Enable smart card readers
This option enables smart card readers for CNM and for other TKE applications.

Note: When the TKE workstation crypto adapter is initialized for smart card use, this option is automatically selected.

Exit Exit the CNM application.

Exit and logoff
Exit the CNM application and log off from the TKE workstation crypto adapter.

Select **Yes** to confirm logoff. A successful message is displayed.

Crypto Node menu

TKE crypto adapter clock-calendar

The TKE workstation crypto adapter uses its clock-calendar to record time and date and to prevent replay attacks in passphrase logon.

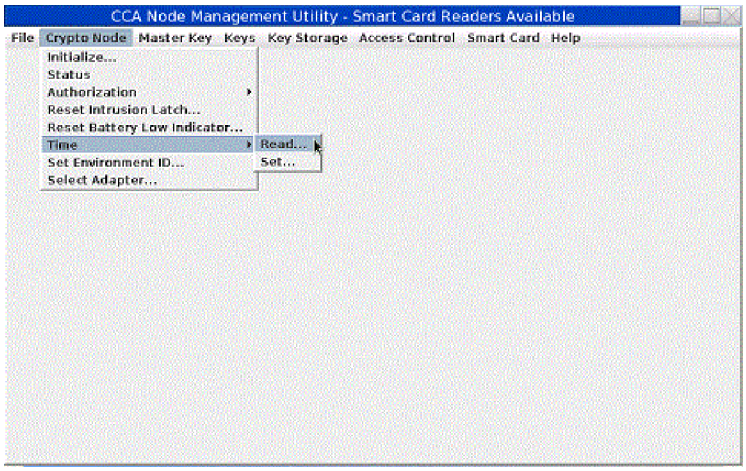


Figure 182. CNM main window — Crypto Node Time sub-menu

Read clock-calendar

To read the TKE workstation crypto adapter clock-calendar:

1. From the **Crypto Node** pull-down menu, select **Time**. A sub-menu is displayed.
2. From the sub-menu, select **Read**; the current date and time is displayed. The time is displayed in Greenwich Mean Time (GMT).

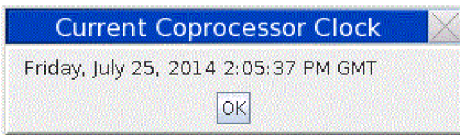


Figure 183. Current Coprocessor Clock

3. Finish the task by selecting **OK**.

Synchronize clock-calendar

To synchronize the TKE workstation crypto adapter clock-calendar with the TKE workstation clock:

Note: You must be logged on to the TKE workstation crypto adapter using TKEADM or an equivalent profile.

1. From the **Crypto Node** pull-down menu, select **Time**. A sub-menu is displayed.
2. From the sub-menu, select **Set**; a confirmation dialog is displayed.

Figure 184. 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 workstation crypto adapter using a unique user profile. Each user profile is associated with a role. Multiple profiles can use the same role. The TKE workstation crypto adapter authenticates logons using the passphrase or crypto adapter logon key contained on a TKE or EP11 smart card and protected by the smart card PIN that identifies the user.

A TKE administrator can manage roles and profiles using windows that can be opened from the CNM utility Access Control pull-down menu.

The Load User Roles and Profiles and Save User Roles and Profiles menu items contain the same respective functions as found in the TKE Workstation Setup utility.

Managing roles

When you initialize the TKE workstation crypto adapter, a set of IBM-supplied roles are loaded on the adapter. You can use the CCA Node Management Utility's Role Management window to modify the IBM-supplied roles on the adapter, or to define and load your own roles on the adapter.

Each of the IBM-supplied roles is created from a corresponding IBM-supplied role definition file that is stored on the TKE workstation's hard drive. You can also define your own role definition files. The role definition files you create can be stored on the TKE workstations's hard drive or on removable media. A role definition file describes the attributes of a role, and are important for migration between versions of TKE and for recovery. We recommend that you:

- Create role definition files for any new roles you create. This will help during migration to a new TKE workstation or for recovery of the TKE workstation crypto adapter data. If you later modify the role loaded on the TKE workstation crypto adapter, you should also modify the corresponding role definition file.

  When creating role definition files, we recommend using the naming convention *role-name*.rol.
- Do not edit the IBM-supplied role definition files. By leaving the IBM-supplied role definition files unedited, you preserve the ability to restore IBM-supplied roles to their default settings, including the default passwords. If you edit the IBM-supplied roles, we recommend you save the modified settings to a new role definition file instead of editing the original role definition file supplied by IBM.

To open the CCA Node Management Utility's Role Management window:

1. Go to the CCA Node Management Utility main window.
2. From the **Access Control** pull-down menu, select **Roles**.

The CCA Node Management Utility's Role Management window is displayed. Initially, this window lists the roles currently loaded on the TKE workstation crypto adapter.

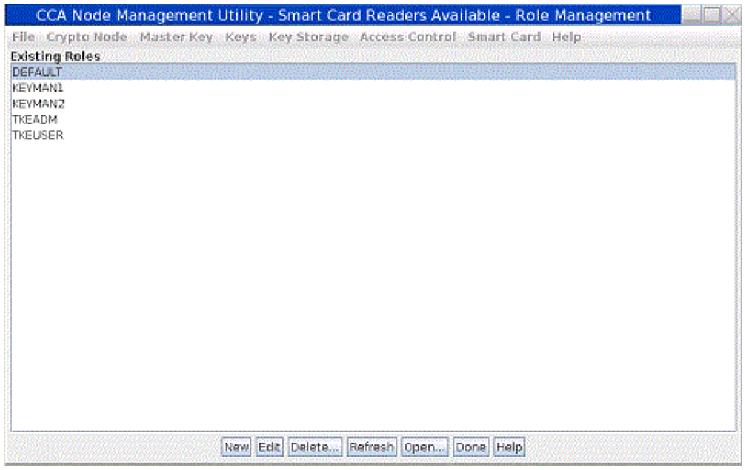


Figure 185. Role Management window listing the roles on the TKE workstation crypto adapter

You can use the Role Management window to manage the roles on the TKE workstation crypto adapter and to manage any associated role definition files. You can use:

- **New** to create a new role.
- **Edit** to edit a role on the TKE workstation crypto adapter.
- **Delete** to delete a role. To do this, you first select the role in the window and then click **Delete**.
- **Refresh** to refresh the list in the window.
- **Open** to open a role definition file.
- **Done** to close the window.

Clicking **New**, **Edit**, or **Open** all eventually open a window for modifying role settings and then either loading those settings as a role on the TKE workstation crypto adapter or saving those settings in a role definition file. It helps to think of **New**, **Edit**, and **Open** as different ways of populating that window with initial values for editing.

- Clicking **New** opens the window and populates it with default attributes for a new role.
- Clicking **Edit** opens the window and populates it with the attributes of the selected role.
- Clicking **Open** opens the window and populates it with the attributes of the selected role definition file.

From that point, however, you'll be able to modify any of the attributes (including the name) and load it as a role on the adapter or save it as a role definition file on the TKE workstation's hard drive or on removable media.

If you are creating a new role or role definition file, for example, you could open either an existing role or role definition file that has settings similar to the ones you want for the new role or role definition file. You would then only have to modify the name and any settings you want changed before loading it as a new role or saving it as a new role definition file.

Creating a new role or role definition

From the CCA Node Management Utility main window, you can select **Access Control –> Roles** off the menu bar to display the CCA Node Management Utility's Role Management window. Initially, this window lists the roles currently loaded on the TKE workstation crypto adapter.

To create a new role or role definition file, it does not matter if a role name is highlighted in the CCA Node Role Management window, or if the list is empty. To create a new role or role definition file:

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

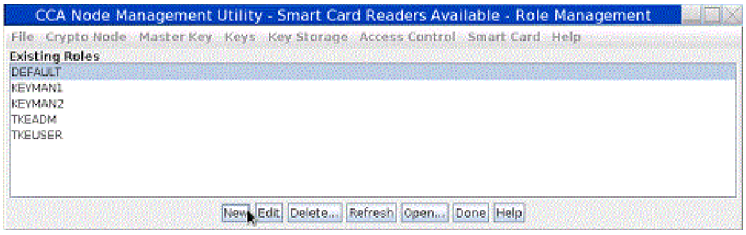


Figure 186. From the CCA Node Management Utility's Role Management window, click on the New push button

A secondary window opens for modifying role settings and then either loading those settings as a role on the TKE workstation crypto adapter or saving those settings in a role definition file. Because you selected the **New** push button, this secondary window is populated with the default attributes and settings for a new role.

Editing a role on the TKE workstation crypto adapter

From the CCA Node Management Utility main window, you can select **Access Control –> Roles** off the menu bar to display the CCA Node Management Utility's Role Management window. Initially, this window lists the roles currently loaded on the TKE workstation crypto adapter.

To edit a role that is currently loaded on the TKE workstation crypto adapter:

1. In the list of roles, click on the name of the role you want to edit.

   The role name is reverse highlighted (white on black) to show that it is selected.
2. Click on the **Edit** push button.

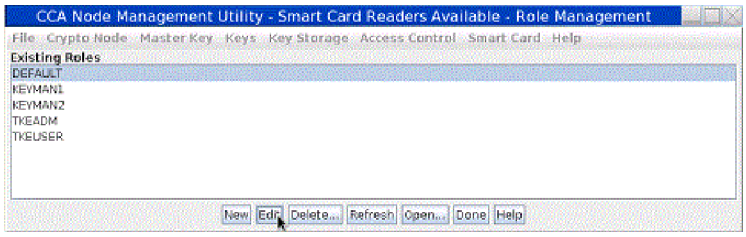


Figure 187. Select role and click Edit

A secondary window opens for modifying role settings and then either loading those settings as a role on the TKE workstation crypto adapter or saving those settings in a role definition file. This secondary window is populated with the attributes of the selected role.

Opening a role definition file

Role definition files have all the attributes and settings necessary to create or update a role on the TKE workstation crypto adapter. Unlike a role, a role definition file is not loaded onto the TKE workstation crypto adapter, but is instead stored on the TKE workstation's hard drive or on removable media. Keep in mind that:

- You can have a role definition file for a role that is not currently loaded on the TKE workstation crypto adapter.
- It is possible that the settings in a role definition file do not currently match the settings of the actual role on the TKE workstation crypto adapter.

From the CCA Node Management Utility main window, you can select **Access Control –> Roles** off the menu bar to display the CCA Node Management Utility's Role Management window. Initially, this window lists the roles currently loaded on the TKE workstation crypto adapter.

To open a role definition file, it does not matter if a role name is highlighted in the CCA Node Role Management window, or if the list is empty. This is because you are not opening a role on the TKE workstation crypto adapter. Instead, you are opening a file on the TKE workstation's hard drive or on removable media.

To open a role definition file:

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

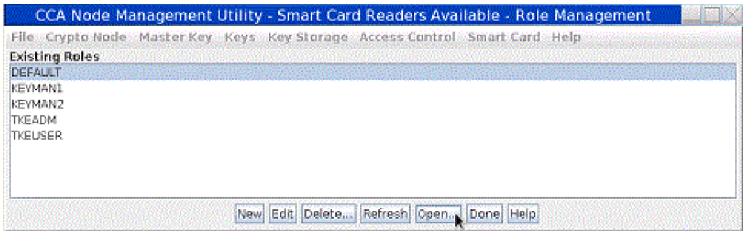


Figure 188. From the CCA Node Management Utility's Role Management window, click on the Open push button

The **Specify file to open** dialog is displayed.

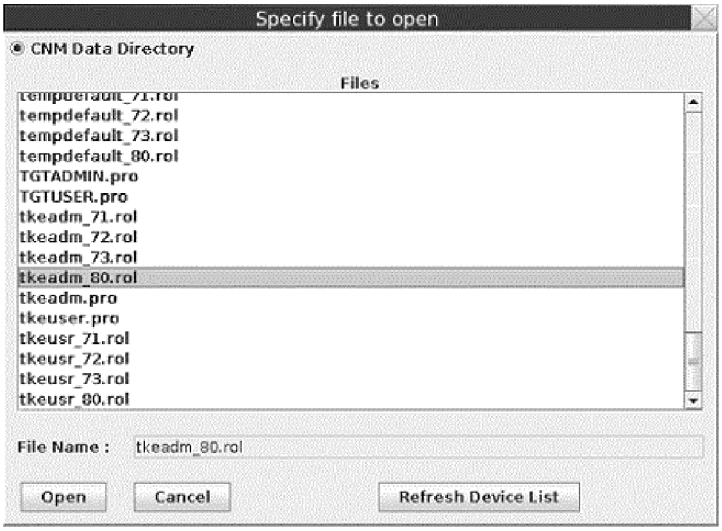


Figure 189. Specify file to open dialog

2. In the **Specify file to open** dialog:
   a. In the list of files, click on the name of the role definition file you want to open. Role definition files typically follow the naming convention *role_name*.rol.

      The role name is reverse highlighted (white on black) to show that it is selected.

   b. Click the **Open** push button.

      A secondary window opens for modifying role settings and then either loading those settings as a role on the TKE workstation crypto adapter or saving those settings in a role definition file. This secondary window is populated with the attributes of the selected role definition file.

Making changes to a role or role definition file

From the CCA Node Management Utility main window, you can select **Access Control –> Roles** off the menu bar to display the CCA Node Management Utility's Role Management window. Initially, this window lists the roles currently loaded on the TKE workstation crypto adapter. When you click the **New**, **Edit**, or **Open** push button on the initial window, a secondary window opens for modifying role settings and then either loading those settings as a role on the TKE workstation crypto adapter or saving those settings in a role definition file.

- The **New** push button will open the window and populate it with default attributes for a new role.

- The **Edit** push button will open the window and populate it with the attributes of the selected role.
- The **Open** push button will open the window and populate it with the attributes of the selected role definition file.

Regardless of how the window was opened and populated with attributes, you can use the window to modify any of the attributes. By changing the Role ID, in fact, you can create a new role or role definition file. Once you have modified the attributes as desired, you can load the role on the TKE workstation crytpo adapter, or save the settings as a role definition file on the TKE workstations's hard drive or on removable media. When making changes to a role you have created, in fact, you will likely want to also create or modify an associated role definition file for migration or recovery purposes.

Note: Do not edit the IBM-supplied role definition files. By leaving the IBM-supplied role definition files unedited, you preserve the ability to restore IBM-supplied profiles to their default settings, including the default passwords. If you edit the IBM-supplied roles, we recommend you save the modified settings to a new role definition file instead of editing the original role definition file supplied by IBM.

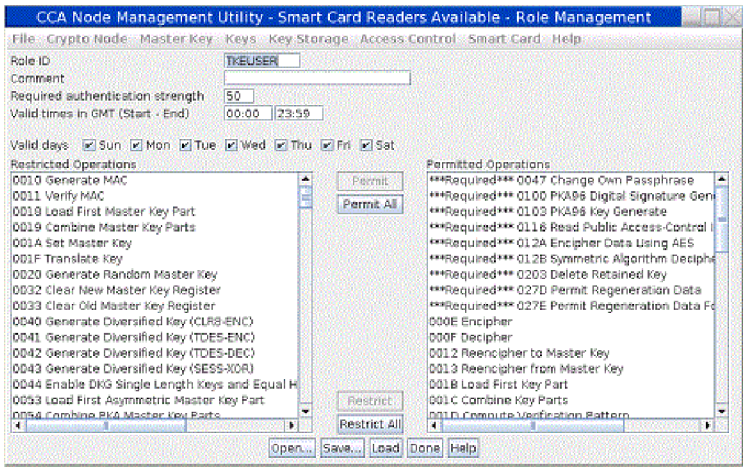


Figure 190. Role Management window modifying role attributes

To make changes to a role or role definition file:

1. Edit the text entry fields and use the window's controls to modify the displayed attributes as desired.
   - The **Role ID** field shows the name of the role. It is a case-sensitive character string with a maximum length of 8 characters.
   - The **Required authentication strength** field shows the level of authentication required to log on to user profiles with this role. Passphrase profiles created on the TKE have passphrases which have strength of 50. For a new role, this field defaults to 0.
   - **Valid times in GMT (Start – End)** fields show the range of hours during the valid days that the user is allowed to log on. For a new role, these fields default to the entire day.
   - The **Valid days** check boxes identify the days of the week that the user is allowed to log on. By default, none of the days are selected for a new role.

- The **Restricted operations** area list of functions the role is not allowed to use, while the **Permitted operations** area lists the functions the role is allowed to use.
  - To permit the role to use a particular function:
    a. In the list of **Restricted Operations**, click on the name of the function.

       The function name is reverse highlighted (white on black) to show that it is selected.
    b. Click the **Permit** push button.

       The function name appears in the **Permitted Operations** list to show the role can use that function.
  - To restrict the role from using a particular function:
    a. In the list of **Permitted Operations**, click on the name of the function.

       The function name is reverse highlighted (white on black) to show that it is selected.
    b. Click the **Restrict** push button.

       The function name appears in the **Restricted Operations** list to show the role is not allowed to use that function.
  - To permit the role to use all functions, click on the **Permit All** push button.
  - To restrict the role from using any function, click on the **Restict All** push button.

2. Load the settings as a role on the TKE workstation crypto adapter or save the settings in a role definition file.

   Note: If you want to both save the settings as a role definition file, and also load the role on the TKE workstation crypto adapter, save the role definition file first. When you load a role, the CCA Node Management Utility's Role Management window closes. If you try to save load the role first, the window will close before you have a chance to save the role definition file.

   - To save a role definition file:
     a. Click the **Save** push button.

        A standard save file dialog is displayed. We recommend you use the naming convention *role_name*.rol.
     b. If you do not want to also load the role on the TKE workstation crypto adapter, you can click the **Done** push button. Clicking the **Done** push button closes the window.
   - To load the role on the TKE workstation crypto adapter:
     a. Click the **Load** push button.

        The role is loaded on the TKE workstation crypto adapter, and the window is closed.

Notes:

1. You can click the **Done** push button to close this window at any time. Any changes you made that were not loaded or saved prior to pressing the **Done** push button will be lost.
2. You can click the **Open** push button at any time to select a new role definition file to edit. Any changes you made that were not loaded or saved will be lost when the window is populated with the attributes of the new role definition file.

Managing profiles

When you initialize the TKE workstation crypto adapter, a set of IBM-supplied profiles are loaded on the adapter. You can use the CCA Node Management Utility's Profile Management window to modify the IBM-supplied profiles on the adapter, or to define and load your own profiles on the adapter.

Each of the IBM-supplied profiles is created from a corresponding IBM-supplied profile definition file that is stored on the TKE workstation's hard drive. You can also define your own profile definition files. The profile definition files you create can be stored on the TKE workstation's hard drive or on removable media. A profile definition file describes the attributes of a profile, and are important for migration between versions of TKE and for recovery. We recommend that you:

- Create profile definition files for any new profiles you create. This will help during migration to a new TKE workstation or for recovery of the TKE workstation crypto adapter data. If you later modify the profile loaded on the TKE workstation crypto adapter, you should also modify the corresponding profile definition file.

  When creating profile definition files, we further recommend:

  – using the naming convention *profile-name*.pro.

  – using the IBM-supplied roles (such as TKEUSER, SCTKEADM) whenever possible.
- Do not edit the IBM-supplied profile definition files. By leaving the IBM-supplied profile definition files unedited, you preserve the ability to restore IBM-supplied profiles to their default settings, including the default passwords. If you edit the IBM-supplied profiles, we recommend you save the modified settings to a new profile definition file instead of editing the original profile definition file supplied by IBM.

To open the CCA Node Management Utility's Profile Management window:

1. Go to the CCA Node Management Utility main window.
2. From the **Access Control** pull-down menu, select **Profiles**.

   The CCA Node Management Utility's Profile Management window is displayed. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter.

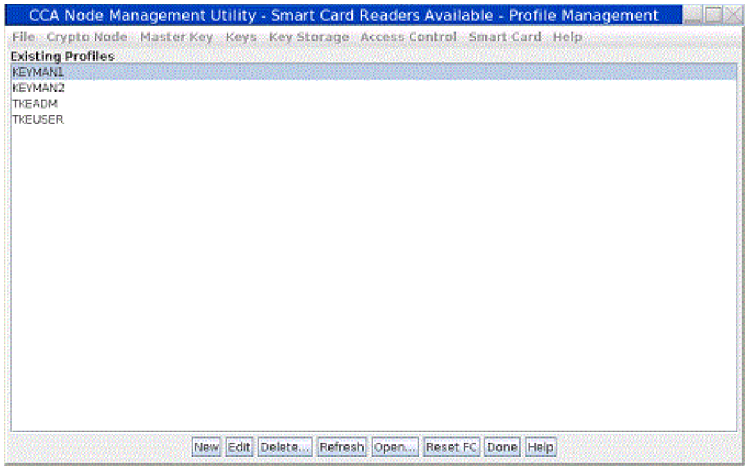


Figure 191. Profile Management window listing the profiles on the TKE's local crypto adapter

You can use the Profile Management window to manage the profiles on the TKE workstation crypto adapter and to manage any associated profile definition files. You can use:

- the **New** push button to create a new smart card, passphrase, or group profile.
- the **Edit** push button to edit a profile on the TKE workstation crypto adapter.
- the **Delete** push button to delete a profile by highlighting it and pressing the Delete button. To do this, you first select the profile in the window and then click the **Delete** button.
- the **Refresh** push button refresh the list in the window.
- the **Open** push button to open a profile definition file.
- the **Done** push button to close the window.

Clicking the **New**, **Edit**, or **Open** push buttons will all eventually open a window for modifying profile settings. The window will differ slightly depending on the type of profile – either a passphrase profile, a smart card profile, or a group profile. From this window, you will be able to load the settings as a profile on the TKE workstation crypto adapter (provided a profile of the same name is not already loaded on the adapter), or save the settings as a profile definition file on the TKE workstation's hard drive or on removable media.

To replace a profile that is already loaded on the TKE workstation crypto adapter, you will always want to use the **Edit** push button. Only by clicking the **Edit** push button will you be able to replace an already-loaded profile.

Creating a new profile or profile definition

From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter.

To create a new profile or profile definition file, it does not matter if a profile name is highlighted in the CCA Node Management window, or if the list is empty. To create a new profile or profile definition file:

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

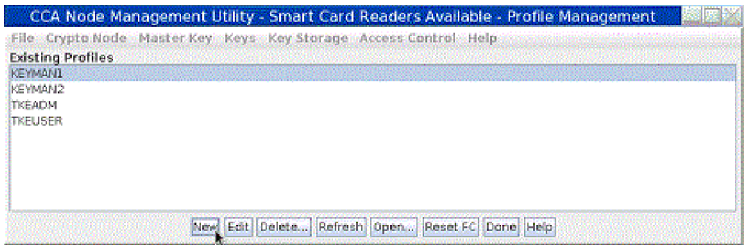


Figure 192. From the CCA Node Management Utility's Profile Management window, click on the New push button

A dialog window opens, prompting you for the type of profile you want to create.

Figure 193. Select profile type

2. In the dialog window, select the type of profile you want to create and click the **Continue** push button.

   A secondary window opens for modifying profile settings and then either loading those settings as a profile on the TKE workstation crypto adapter (provided a profile of the same name is not already loaded on the adapter) or saving those settings in a profile definition file. The window is populated with the default attributes and settings for a new passphrase profile, smart card profile, or group profile.

Editing a profile on the TKE workstation crypto adapter

From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter.

To edit a profile that is currently loaded on the TKE workstation crypto adapter:

1. In the list of profiles, click on the name of the profile you want to edit.

   The profile name is reverse highlighted (white on black) to show that it is selected.

2. Click on the **Edit** push button.

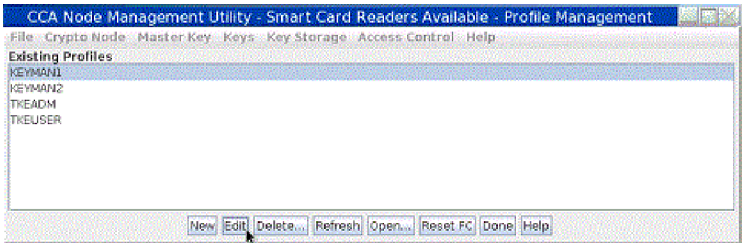


Figure 194. Select profile and click Edit

A secondary window opens for modifying profile settings and then either replacing profile on the TKE workstation crypto adapter or saving those settings in a profile definition file. This secondary window is populated with the attributes of the selected profile.

Opening a profile definition file

Profile definition files have all the attributes and settings necessary to create or update a profile on the TKE workstation crypto adapter. Unlike a profile, a profile definition file is not loaded onto the TKE workstation crypto adapter, but is instead stored on the TKE workstation's hard drive or on removable media. Keep in mind that:

- You can have a profile definition file for a profile that is not currently loaded on the TKE workstation crypto adapter.
- It is possible that the settings in a profile definition file do not currently match the settings of the actual profile on the TKE workstation crypto adapter.

From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter.

To open a profile definition file, it does not matter if a profile name is highlighted in the CCA Node Profile Management window, or if the list is empty. This is because you are not opening a profile on the TKE workstation crypto adapter. Instead, you are opening a file on the TKE workstation's hard drive or on removable media.

To open a profile definition file:

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

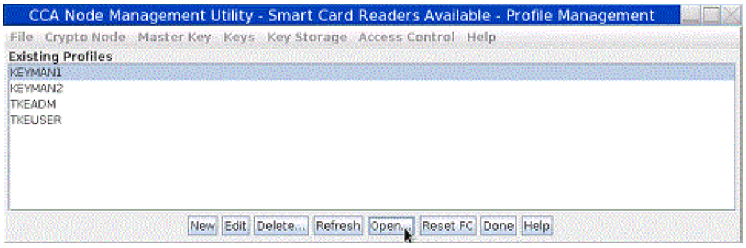


Figure 195. From the CCA Node Management Utility's Profile Management window, click on the Open push button

The **Specify file to open** dialog is displayed.

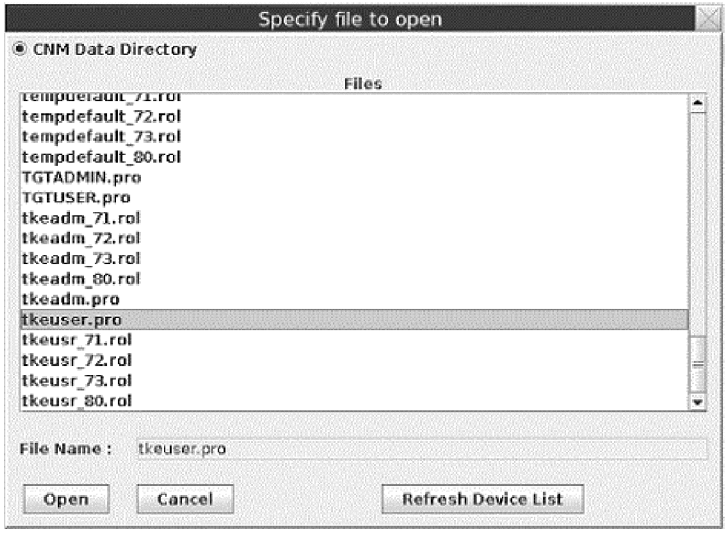


Figure 196. Specify file to open dialog

2. In the **Specify file to open** dialog:
   a. In the list of files, click on the name of the profile definition file you want to open. Profile definition files typically follow the naming convention *profile_name*.pro.

      The profile name is reverse highlighted (white on black) to show that it is selected.

   b. Click the **Open** push button.

      A secondary window opens for modifying profile settings and then either loading those settings as a profile on the TKE workstation crypto adapter (provided a profile of the same name is not already loaded on the adapter) or saving those settings in a profile definition file. This secondary window is populated with the attributes of the selected profile definition file.

Making changes to a profile or profile definition file

From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter. When you click the **New**, **Edit**, or **Open** push button on the initial window, a secondary window opens for modifying profile settings and then either loading those settings as a profile on the TKE workstation crypto adapter or saving those settings in a profile definition file.

- The **New** push button will first prompt you for the type of profile and then will open the window and populate it with default attributes for that profile type.
- The **Edit** push button will open the window and populate it with the attributes of the selected profile.
- The **Open** push button will open the window and populate it with the attributes of the selected profile definition file.

The window will differ slightly depending on the type of profile you are modifying – either a passphrase profile, a smart card profile, or a group profile.

Making changes to a passphrase profile or passphrase profile definition file:
From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles

currently loaded on the TKE workstation crypto adapter. When you click the **New**, **Edit**, or **Open** push button on the initial window, a secondary window opens for modifying profile settings and then either loading those settings as a profile on the TKE workstation crypto adapter or saving those settings in a profile definition file.

If the profile or profile definition file is for a passphrase profile, a window is displayed for making changes to a passphrase profile. In particular, fields are presented for entering the passphrase and passphrase expiration date.

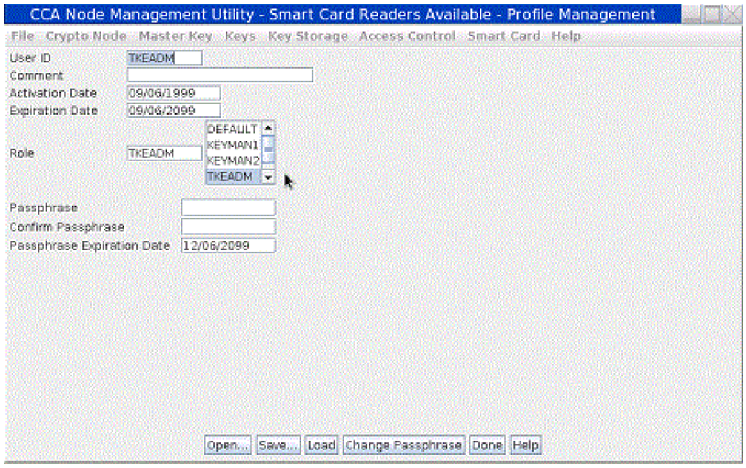


Figure 197. Profile Management window for passphrase profiles

To make changes to a passphrase profile or a passphrase profile definition file:

1. Edit the text entry fields and use the window's controls to modify the displayed attributes as desired.
   - The **User ID** field shows the name of the profile. It is a case-sensitive character string with a maximum length of 8 characters.
   - The **Comment** field shows an optional character string with a maximum length of 20 characters.
   - The **Activation Date** field determines the first date the user can log on. This field defaults to the current date.
   - The **Expiration Date** field determines the last date the user can log on. When a new profile is being created, the date will default to the current date. Remember to adjust this date.
   - The **Role** field shows the name of the role that defines the permissions granted to the profile. Select a role from the list.

     Note: Individual profiles that are intended to be used only as group members should be given a role that has very few or no permitted operations (such as the DEFAULT role). This is done to ensure the profile has very little authority outside the group.
   - The **Passphrase** field contains the case-sensitive character string that the user must enter to log on to the TKE workstation crypto adapter. The passphrase must:
     - Have a length between 8 and 64 characters.
     - Contain at least 2 letters and at least 2 numbers.
     - Must not contain the user ID.
   - The **Confirm Passphrase** field must contain the same case-sensitive character string as the **Passphrase** field.

- The **Passphrase Expiration Date** contains the expiration date for the passphrase. When a new profile is created, the date defaults to three months after the current date. Remember to adjust this date.

2. Load the settings as a profile on the TKE workstation crypto adapter, save the settings in the profile definition file, or change just the passphrase for the profile.

   Note: If you want to save the settings as a profile definition file, and also either change the passphrase for the profile or load the profile on the TKE workstation crypto adapter, save the profile definition file first. When you change the passphrase for a profile or load a profile, the CCA Node Management Utility's Profile Management window closes. If you try to change the passphrase or load the profile first, the window will close before you have a chance to save the profile definition file.

   - To save a profile definition file:
     a. Click the **Save** push button.

        A standard save file dialog is displayed. We recommend you use the naming convention *profile_name*.pro.

     b. If you do not want to also change the passphrase or load the profile on the TKE workstation crypto adapter, you can click the **Done** push button. Clicking the **Done** push button closes the window.
   - To load the profile on the TKE workstation crypto adapter:
     a. Click the **Load** push button.

        The profile is loaded on the TKE workstation crypto adapter, and the window is closed.
   - To change the passphrase for the profile:
     a. Click the **Change Passphrase** push button. The passphrase profile on the TKE workstation crypto adapter is updated with the new passphrase and passphrase expiration date. No other changes will be make to the passphrase profile.

Notes:

1. You can click the **Done** push button to close this window at any time. Any changes you made that were not loaded or saved prior to pressing the **Done** push button will be lost.
2. You can click the **Open** push button at any time to select a new profile definition file to edit. Any changes you made that were not loaded or saved will be lost when the window is populated with the attributes of the new profile definition file.

Making changes to a smartcard profile or smartcard profile definition file: From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter. When you click the **New**, **Edit**, or **Open** push button on the initial window, a secondary window opens for modifying profile settings and then either loading those settings as a profile on the TKE workstation crypto adapter or saving those settings in a profile definition file.

If the profile or profile definition file is for a smartcard profile, a window is displayed for making changes to a smart card profile. In particular, the public modulus and key identifier for the TKE workstation crypto adapter logon key is

displayed.

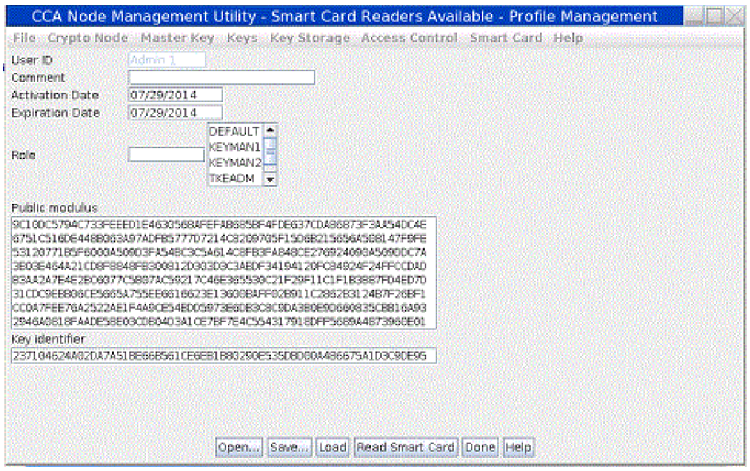


Figure 198. Profile Management window for smart card profiles

To make changes to a smartcard profile or a smartcard profile definition file:

1. Edit the text entry fields and use the window's controls to modify the displayed attributes as desired. Some of the fields are informational, and cannot be edited.
   - The **User ID** field shows the name of the profile. The name of the profile is obtained from the profile, the smart card, or a profile definition file. This value cannot my changed.
   - The **Comment** field shows an optional character string with a maximum length of 20 characters.
   - The **Activation Date** field determines the first date the user can log on. This field defaults to the current date.
   - The **Expiration Date** field determines the last date the user can log on. When a new profile is being created, the date will default to the current date. Remember to adjust this date.
   - The **Role** field shows the name of the role that defines the permissions granted to the profile. Select a role from the list.

     Note: Individual profiles that are intended to be used only as group members should be given a role that has very few or no permitted operations (such as the DEFAULT role). This is done to ensure the profile has very little authority outside the group.
   - The **Public Modulus** fields shows the public modulus of the TKE workstation crypto adapter logon key. This value is read from the profile, profile definition file, or smart card. This value cannot be changed.
   - The **Key Identifier** field shows a SHA-256 hash of the DER-encoded public modulus and public exponent of the TKE workstation crypto adapter logon key for this profile. This field cannot be changed.
2. Load the settings as a profile on the TKE workstation crypto adapter or save the settings in the profile definition file.

   Note: If you want to both save the settings as a profile definition file, and also load the profile on the TKE workstation crypto adapter, save the profile definition file first. When you load a profile, the CCA Node Management

Utility's Profile Management window closes. If you try to save load the profile first, the window will close before you have a chance to save the profile definition file.

- To save a profile definition file:
  a. Click the **Save** push button.

     A standard save file dialog is displayed. We recommend you use the naming convention *profile_name*.pro.

  b. If you do not want to also load the profile on the TKE workstation crypto adapter, you can click the **Done** push button. Clicking the **Done** push button closes the window.
- To load the profile on the TKE workstation crypto adapter:
  a. Click either the **Load** or **Replace** push button. (If, from the initial Profile Management window, you selected the **New** push button to create a new profile, or the **Open** push button to open a profile definition file, this secondary window will contain a **Load** push button. If, from the initial Profile Management window, you selected the **Edit** push button to edit a profile already loaded on the TKE workstation crypto adapter, this secondary window will contain a **Replace** push button.)

     The profile is loaded on the TKE workstation crypto adapter, and the window is closed.

     If the profile is already loaded on the TKE workstation crypto adapter, and you click the **Load** push button, the load operation will fail. Go back to the initial Profile Management window and select the **Edit** push button to edit the profile. This window will then contain a **Replace** push button for replacing the already-loaded profile.

Notes:

1. You can click the **Done** push button to close this window at any time. Any changes you made that were not loaded or saved prior to pressing the **Done** push button will be lost.
2. You can click the **Open** push button at any time to select a new profile definition file to edit. Any changes you made that were not loaded or saved will be lost when the window is populated with the attributes of the new profile definition file.

Making changes to a group profile or group profile definition file: From the CCA Node Management Utility main window, you can select **Access Control –> Profiles** off the menu bar to display the CCA Node Management Utility's Profile Management window. Initially, this window lists the profiles currently loaded on the TKE workstation crypto adapter. When you click the **New**, **Edit**, or **Open** push button on the initial window, a secondary window opens for modifying profile settings and then either loading those settings as a profile on the TKE workstation crypto adapter or saving those settings in a profile definition file.

If the profile or profile definition file is for a group profile, a window is displayed for making changes to a group profile. In particular, group member information is displayed.

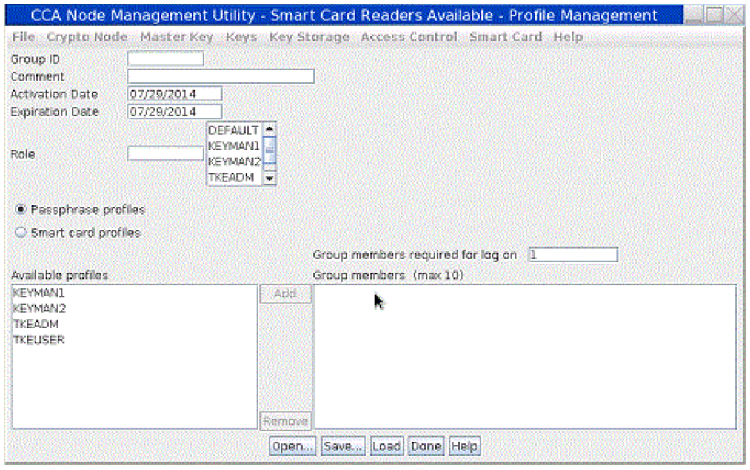


Figure 199. Profile Management window for group profiles

To make changes to a group profile or a group profile definition file:

1. Edit the text entry fields and use the window's controls to modify the displayed attributes as desired.
   - The **Group ID** field shows the name of the profile. It is a case-sensitive character string with a maximum length of 8 characters.
   - The **Comment** field shows an optional character string with a maximum length of 20 characters.
   - The **Activation Date** field determines the first date the user can log on. This field defaults to the current date.
   - The **Expiration Date** field determines the last date the user can log on. When a new profile is being created, the date will default to the current date. Remember to adjust this date.
   - The **Role** field shows the name of the role that defines the permissions granted to the profile. Select a role from the list.

     Note: The role of the group will override the roles of the individual users.
   - The **Passphrase profiles** and **Smart card profiles** radio buttons determine the type or profiles that can be members of the group. All the profiles in a group must be the same type.
   - The **Group members required for log on:** field shows the number of users that must sign on to complete the group sign on. The value must be between 1 and the number of profiles in the group. A group cannot contain more than 10 profiles.
   - The **Available profiles** area lists the profiles the selected type (passphrase profiles or smart card profiles) that are not currently members of the group, while the **Group members** area lists the profiles that are members of the group.
     – To add a profile to the group:
       a. In the list of **Available profiles**, click on the name of the profile you want to add to the group.

          The profile name is reverse highlighted (white on black) to show that it is selected.
       b. Click the **Add** push button.

          The profile name appears in the **Group members** list to show that it is now a member of the group.

– To remove a profile from the group:
  a. In the list of **Group members**, click on the name of the profile you want to remove from the group.

     The profile name is reverse highlighted (white on black) to show that it is selected.
  b. Click the **Remove** push button.

     The profile name is removed from the **Group Members** list to show that it is no longer a member of the group.

2. Load the settings as a profile on the TKE workstation crypto adapter or save the settings in the profile definition file.

   Note: If you want to both save the settings as a profile definition file, and also load the profile on the TKE workstation crypto adapter, save the profile definition file first. When you load a profile, the CCA Node Management Utility's Profile Management window closes. If you try to save load the profile first, the window will close before you have a chance to save the profile definition file.

   - To save a profile definition file:
     a. Click the **Save** push button.

        A standard save file dialog is displayed. We recommend you use the naming convention *profile_name*.pro.
     b. If you do not want to also load the profile on the TKE workstation crypto adapter, you can click the **Done** push button. Clicking the **Done** push button closes the window.
   - To load the profile on the TKE workstation crypto adapter:
     a. Click either the **Load** or **Replace** push button. (If, from the initial Profile Management window, you selected the **New** push button to create a new profile, or the **Open** push button to open a profile definition file, this secondary window will contain a **Load** push button. If, from the initial Profile Management window, you selected the **Edit** push button to edit a profile already loaded on the TKE workstation crypto adapter, this secondary window will contain a **Replace** push button.)

        The profile is loaded on the TKE workstation crypto adapter, and the window is closed.

        If the profile is already loaded on the TKE workstation crypto adapter, and you click the **Load** push button, the load operation will fail. Go back to the initial Profile Management window and select the **Edit** push button to edit the profile. This window will then contain a **Replace** push button for replacing the already-loaded profile.

Notes:

1. You can click the **Done** push button to close this window at any time. Any changes you made that were not loaded or saved prior to pressing the **Done** push button will be lost.
2. You can click the **Open** push button at any time to select a new profile definition file to edit. Any changes you made that were not loaded or saved will be lost when the window is populated with the attributes of the new profile definition file.

Master Key menu

The Master Key pull-down menu has menu items for the following key stores you can manage:

- DES/PKA Master Key
- AES Master Key

These menu items have additional items for the following tasks you can perform:

- Auto set...
- Create Random Master Key... (Only available for DES/PKA master key)
- Clear New ...
- Parts
- Smart Card Parts (TKE must be enabled for use with smart cards)
- Set...
- Verify

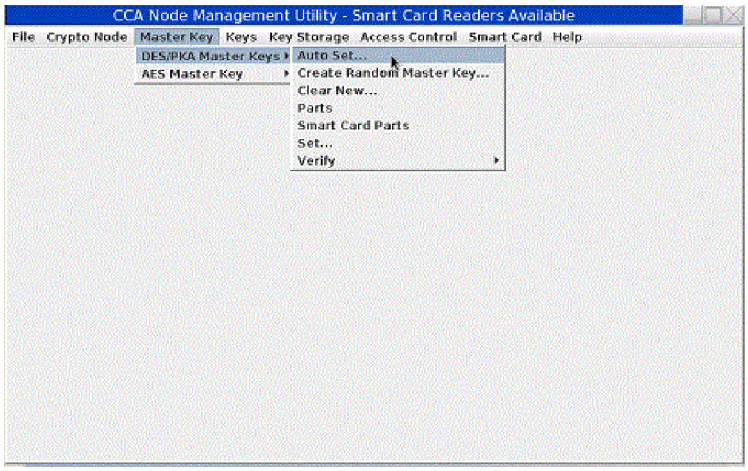


Figure 200. CNM main window — Master Key pull-down menu

The master keys are stored in the tamper-resistant TKE workstation crypto adapter.

The DES/PKA master keys are used to encipher other keys. Each master key is a 24 byte DES key (192 bits). However, because DES keys contain 1 parity bit per byte, it has an effective length of 168 bits of "real" key material. Random master keys are generated and set when the TKE workstation crypto adapter is initialized. If a master key of unknown value is lost, you cannot recover the keys enciphered under it. We recommend that you load a new master key by entering clear key parts or by loading key parts that are stored on smart cards.

The AES master key is used to encipher other keys.

Each master key on the TKE workstation crypto adapter has three registers:

- **Current Master Key Register.** The active master key is stored in the current master key register.
- **Old Master Key Register.** The previous master key is stored in the old master key register.
- **New Master Key Register.** The new master key register is an interim location used to combine master key parts to form a new master key

Auto Set and Create Random Master Key

The Auto Set and Create Random Master Key pull-down menu options use different methods to generate and set new master key values.

The Create Random Master Key option is only available for DES/PKA master keys pull down.

Note: If a master key of unknown value is lost, you cannot recover the keys enciphered under it. We recommend that you load a new master key by entering clear key parts or by entering key parts generated to TKE smart cards.

Clear new

The Clear New pull-down menu option allows you to clear the new master key registers. If a new master key register has a value in it, you must clear it before you can do load a first key part. To clear the new master key register:

1. From the Master Key pull-down menu, select **Clear New...**

   A confirmation dialog displays, prompting you to verify that you want to clear the new master key register.

Figure 201. Clear New Master Key Register — confirm clearing

2. If you are certain you want to clear the new master key register, click the confirmation dialog's **Yes** push button.

   An information box informs you that the new master key register is cleared. Select **OK** to finish.

Figure 202. Clear New Master Key Register — register cleared

Parts — Loading a new master key from clear key parts

To load new master key parts into the TKE workstation crypto adapter, load the first key part, any middle key parts, and the last key part into the new master key register, and then load the new master key. The first and last key parts are required. Middle key parts are optional; you can load multiple middle key parts.

1. From the **Master Key –> DES/PKA Master Key** or **Master Key –> AES Master Key** pull-down menu items, select the **Parts** menu option.

   The Load Master Key panel is displayed.

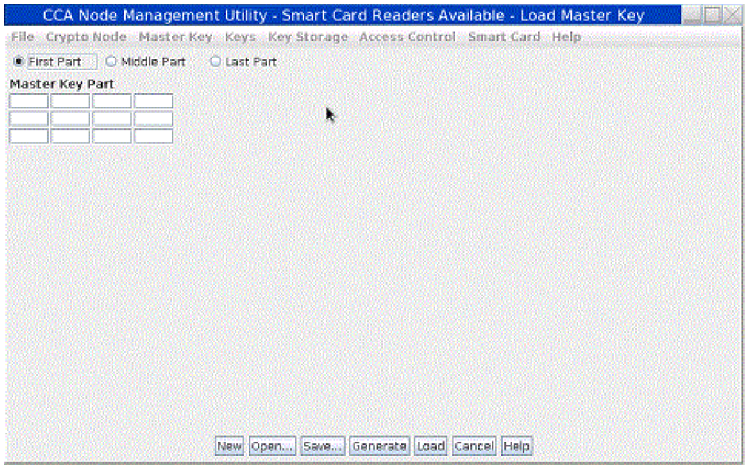


Figure 203. Load Master Key from Clear Parts

2. Select the radio button corresponding to the key part you are loading (First Part, Middle Part or Last Part).
3. Enter the clear key part by doing one of the following:
   - Select **New** to clear data entered in error.
   - Select **Open**... to retrieve key parts saved to disk.
   - Select **Generate** to have the TKE workstation crypto adapter randomly generate a key part.
   - Manually enter a key value into the "Master Key Part" fields. Each field accepts four hexadecimal digits.

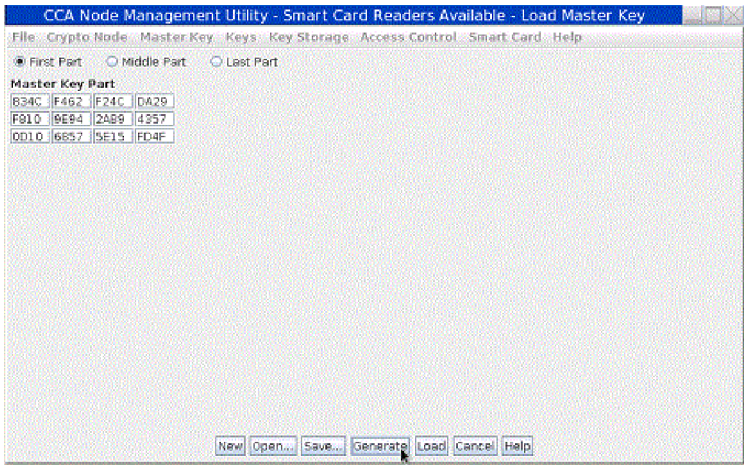


Figure 204. Load Master Key from Clear Parts — key part randomly generated

4. Select **Load** to load the key part into the new master key register, and select **Save** to save the key part to disk.

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

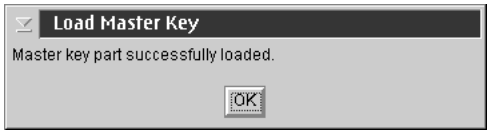


Figure 205. Load Master Key from Clear Parts — key part successfully loaded

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 266.)

We recommend a dual control security policy. With a dual control security policy, the first and last key parts are loaded by different people.

Smart card parts — generating master key parts to a smart card

Steps for generating master key parts and saving them on a TKE or EP11 smart card are as follows:

1. From the **Master Key** pull-down menu, select **DES/PKA Master Keys** or **AES Master Key** and then select **Smart Card Parts**. You will be prompted to insert a TKE or EP11 smart card into smart card reader 2. A Smart Card Master Key Parts panel is displayed. Any TKE workstation crypto adapter master key parts stored on the smart card are listed in the container. The smart card description is displayed. Ensure this is the correct smart card you want to save the key part on.

   Note: Make sure that the TKE workstation crypto adapter and the smart card are in the same zone. To determine the zone for a smart card, use CNM, see "Display smart card details" on page 269 or SCUP "Display smart card information" on page 281. To determine the zone of the TKE workstation crypto adapter, use SCUP "View current zone" on page 301. To use SCUP, you must first exit from CNM.

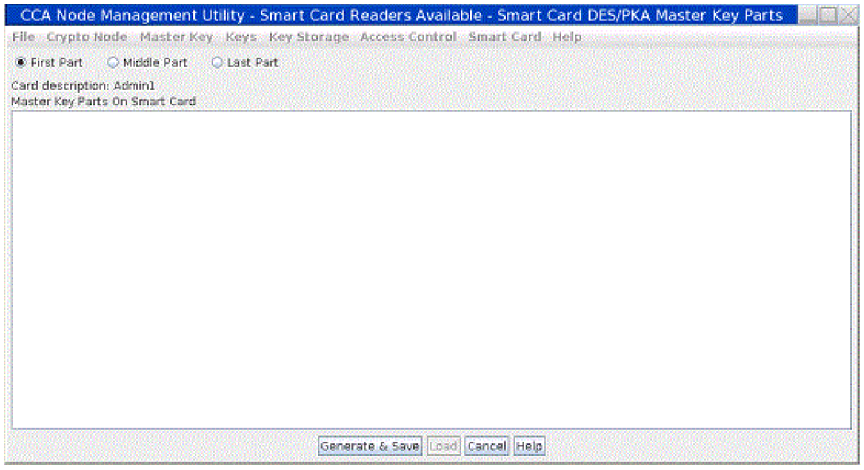


Figure 206. Smart Card Master Key Parts panel

2. Select the radio button for the key part you are generating (First Part, Middle Part, or Last Part).
3. Press the **Generate & Save** push button. You will be prompted for an optional description for the key part you are generating. A maximum of 32 characters may be specified.

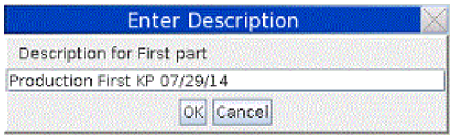


Figure 207. Smart Card Master Key Parts panel — key part description prompt

4. You will be prompted for the PIN of the smart card inserted in smart card reader 2.

A secure session is established between the TKE workstation crypto adapter and the smart card. The key part is generated to the smart card. The key part list is refreshed.

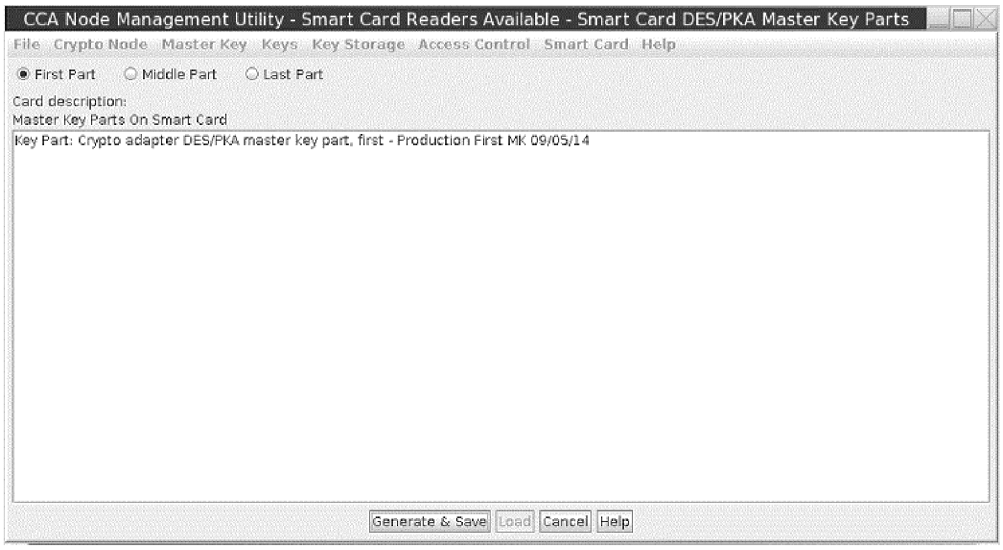


Figure 208. Smart Card Master Key Parts panel — key part generated

Note: The key parts in the list are prefixed as follows:

- Key Part: Crypto Adapter master key part, first - <optional description follows>
- Key Part: Crypto Adapter master key part, middle - <optional description follows>
- Key Part: Crypto Adapter master key part, last - <optional description follows>

A First and Last key part is required. Middle key parts are optional. We recommend a dual control security policy. With a dual control security policy, the first and last key parts are generated to different smart cards so that no one person has access to the complete key. At this point, we recommend that you insert a different smart card in smart card reader 2 to generate middle or last key parts. Repeat the preceding steps to generate any middle or last key parts.

Smart card parts — loading master key parts from a smart card

Steps for loading TKE workstation crypto adapter master key parts from a TKE or EP11 smart card are as follows:

1. From the **Master Key** pull-down menu, select **DES/PKA Master Keys** or **AES Master Key**, and then select **Smart Card Parts**. You are prompted to insert a TKE or EP11 smart card into smart card reader 2. A Smart Card Master Key Parts panel is displayed. Any TKE workstation crypto adapter master key parts stored on the smart card are listed in the container. The smart card description is displayed. Ensure that this is the correct smart card you want to work with.
2. Highlight the key part you want to load into the selected TKE workstation crypto adapter new master key register. Click **Load**. You are prompted for the PIN of the smart card inserted in smart card reader 2.

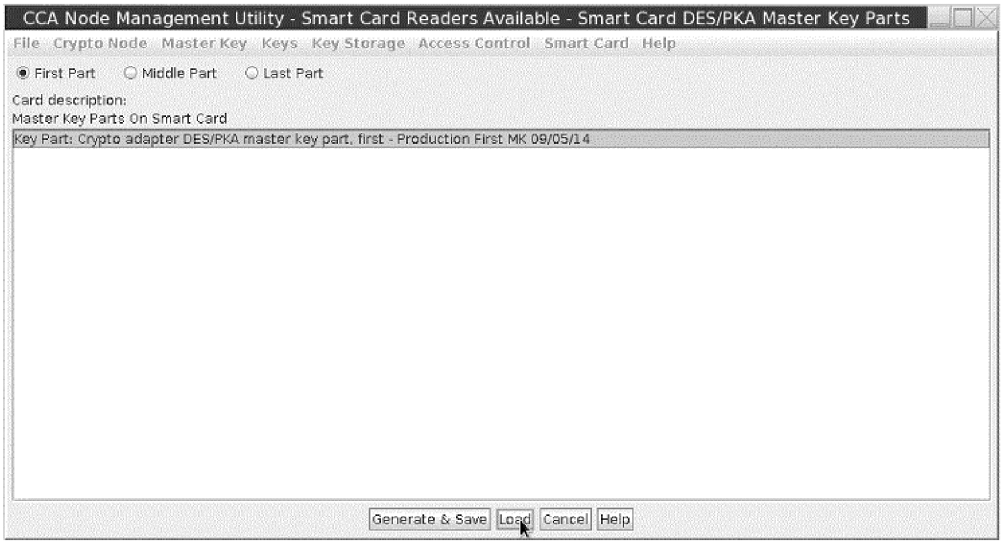


Figure 209. Master Key Part Smart Card panel — loading a Crypto Adapter key part from a smart card

3. A secure session is established between the TKE workstation crypto adapter and the smart card. A pop-up message displays, indicating that the key part was successfully loaded.

Figure 210. Master key part successfully loaded

4. Repeat steps 1 on page 262 through 3 to load additional key parts into the TKE workstation crypto adapter new master key register. If the key parts are on different smart cards, remove the smart card from smart card reader 2 and insert the smart card that contains the next key part to load.

   Note: Key parts must be loaded in order. Specifically, a first key part must be loaded first (Key Part: Crypto Adapter master key part, first) and the last key part (Key Part: Crypto Adapter master key part, last) must be loaded last.

Set — setting the master key value

To set the master key value:

1. From the **Master Key** pull-down menu, select **DES/PKA Master Keys** or **AES Master Key**, and then select **Set...** This will do the following:
   - Transfer the key in the current master key register to the old master key register and delete the former old master key.
   - Transfer the key in the new master key register to the current master key register.
2. After setting a new master key, reencipher the keys currently in key storage. See “Reenciphering key storage” on page 266.

Verify — verifying the master key

A verification pattern (VP) is generated for each master key stored in the master-key registers (new, current and old). The VP can be used to verify that the correct key part was entered, for instance, when you have many key parts stored to disk or smart cards. It can also be used to verify that the key part was entered correctly, particularly when key parts are entered manually. The VP is zero when the register is empty. After each key part is entered, the key part is combined with the existing key in the register and the VP is updated. The VP does not reveal information about the clear key value.

The VP can be saved to disk for future reference. For example, in the event the TKE workstation crypto adapter is initialized, the master key registers are cleared. When the master key is reloaded, you can compare the VP of the master key register to the VP saved to disk. If they are identical, it indicates that the correct master key parts were loaded. Then you can set the master key. If they are different, you can clear the new master key register and load the correct key parts.

To verify a master key, do the following:

1. From the **Master Key** pull-down menu, select **Verify**. A sub-menu is displayed.

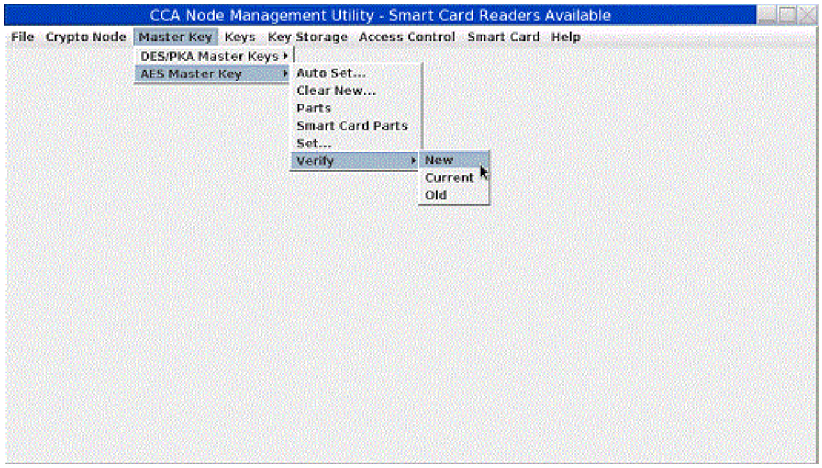


Figure 211. Master Key Verify sub-menu

2. From the submenu, select the master key register you wish to verify - **New**, **Current** or **Old**. Typically, you will choose **New**. You cannot change the current or old master key.
3. The VP is displayed in the Master Key Register Verification panel.

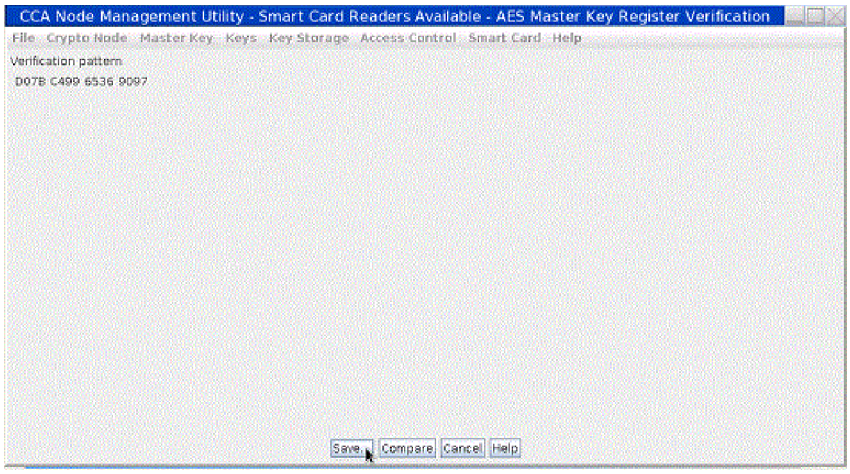


Figure 212. Master Key Register Verification panel - verification pattern is displayed

4. Select **Save** to save the VP to a file. A file chooser will be displayed for the user to specify both a file name, and where to save the file (USB flash memory drive or CNM Data Directory).

   Attention: Do not remove a USB flash memory drive from the USB port before you complete the operation that is using the drive, or before you respond to a message related to the operation that is using the drive. If you do remove a drive before the operation is complete, hardware messages might be generated on the TKE workstation.
5. Select **Compare** to compare the VP to a VP previously saved to disk. A file chooser will be displayed for the user to specify the location and filename of the saved VP.

Figure 213. Master Key Register VP compare successful

Key Storage menu

The Key Storage pull-down menu of the CNM main window contains menu items to manage or initialize DES, PKA, or AES key storage.

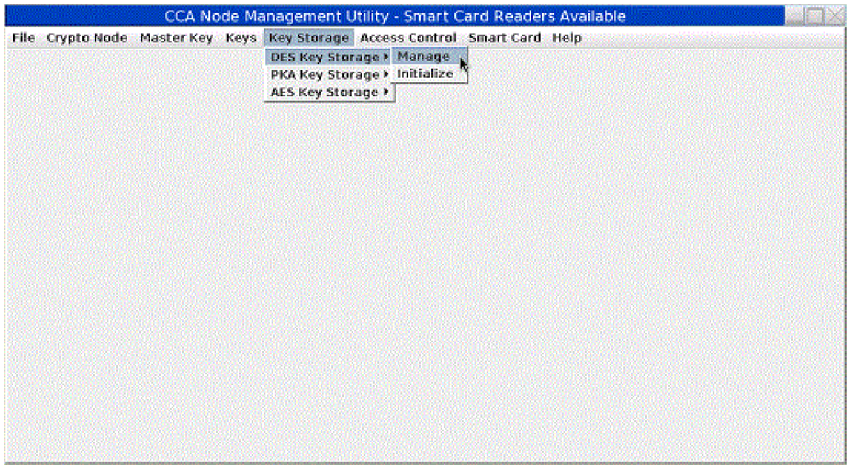


Figure 214. CNM main window — Key Storage pull-down menu

Reenciphering key storage

Key storage is a repository of keys that you access by key label. DES keys, PKA (RSA) keys, and AES keys are held in separate storage systems. The keys in key storage are enciphered under the current TKE workstation crypto adapter master key. When a new master key is set, thereby becoming the current master key, the keys must be reenciphered to the current master key.

To reencipher the keys in storage, do the following:

1. From the **Key Storage** pull-down menu, select **DES Key Storage**, **PKA Key Storage**, or **AES Key Storage**. A sub-menu is displayed.
2. From the sub-menu, select **Manage**. A Key Storage Management panel is displayed. The panel lists the labels of the keys in key storage.

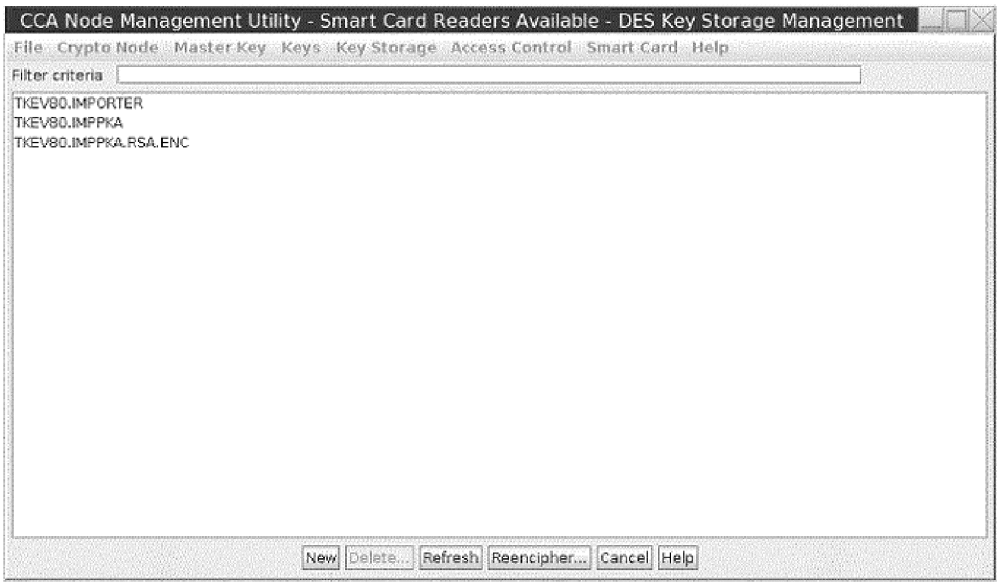


Figure 215. Key Storage Management Panel – key labels list

3. Select **Reencipher...**; the keys are reenciphered using the key in the current master key register.

Smart card menu

The Smart Card pull-down menu of the CNM main window contains the following menu items.

- Change PIN
- Generate Crypto Adapter Logon Key
- Display Smart Card Details
- Manage Smart Card contents
- Copy Smart Card

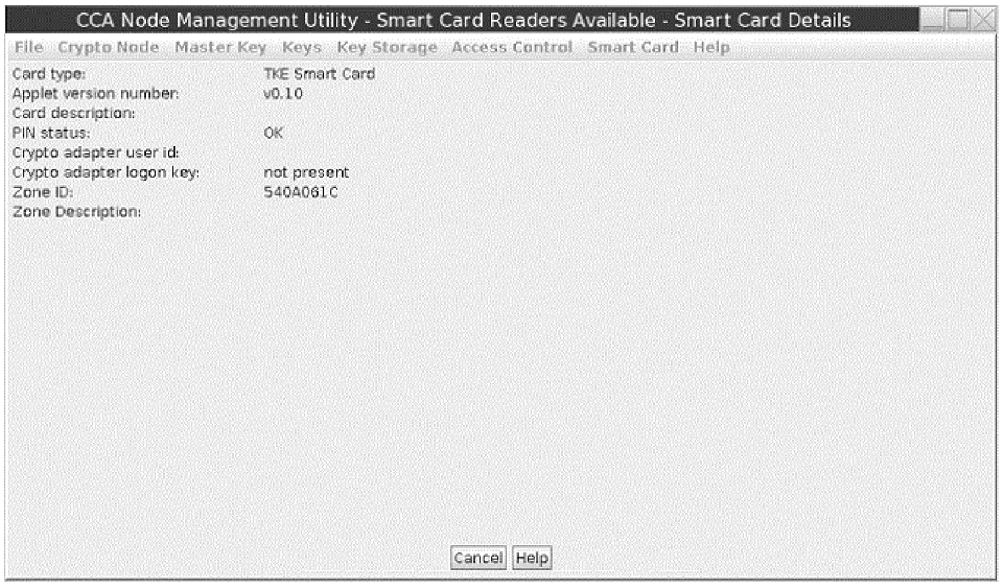


Figure 216. CNM main menu — Smart Card pull-down menu

Change PIN

TKE and EP11 smart cards are secured with a PIN. You can change your PIN using this function. You must know your current PIN. If your smart card is blocked due to too many incorrect PIN attempts, this function will fail.

To change the PIN, perform the following steps:

1. From the **Smart Card** pull-down menu, select **Change PIN**. An informational window will prompt you to insert your smart card into smart card reader 2. Insert your smart card and press **OK** to continue.

Figure 217. Change PIN — insert smart card prompt

2. You will be prompted for your current PIN. Enter your current PIN on the smart card reader 2 PIN pad.

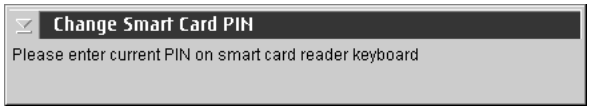


Figure 218. Change PIN — enter current PIN prompt

3. You will be prompted for your new PIN. The new PIN must be entered twice and both PINs must match.

Figure 219. Change PIN — enter new PIN prompt

4. The PIN is successfully changed on the smart card.

Generate TKE crypto adapter logon key

A Crypto Adapter logon key allows a user to log on to the TKE workstation crypto adapter using a TKE or EP11 smart card to access functions not allowed in the default role. A Crypto Adapter logon key is an RSA public/private key pair generated within the smart card. The private key never leaves the smart card. The public key is read from the smart card and loaded to the TKE workstation crypto adapter when a user profile is defined.

To generate a Crypto Adapter logon key, do the following:

1. From the Smart Card pull-down menu, select Generate Crypto Adapter Logon Key. You will be prompted for a TKE or EP11 smart card. Insert the smart card into smart card reader 2.

Figure 220. Generate Crypto Adapter Logon Key — insert smart card

2. You will be prompted for a PIN. Enter the PIN on the smart card reader 2 PIN pad.

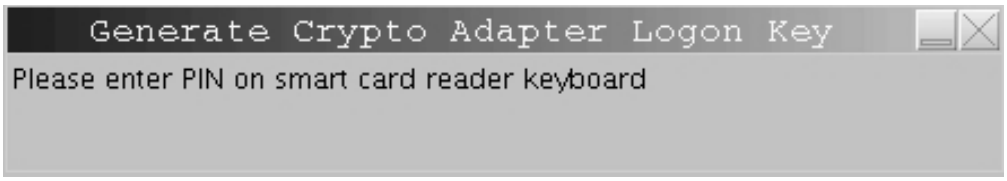


Figure 221. Generate Crypto Adapter Logon Key — PIN prompt

3. You will be prompted for a user ID for the smart card. This user ID will be read from the smart card when defining a smart card user profile.

Figure 222. Generate Crypto Adapter Logon Key — User ID prompt

4. The Crypto Adapter logon key is generated.

Figure 223. Generate Crypto Adapter Logon Key — key generated

Display smart card details

Use this function to display public information about a TKE or EP11 smart card.

1. From the **Smart Card** pull-down menu, select **Display Smart Card Details**. You will be prompted for a TKE or EP11 smart card. Insert the smart card into smart card reader 2.

Figure 224. Display Smart Card Details — insert smart card prompt

The smart card is read and the public information is displayed.

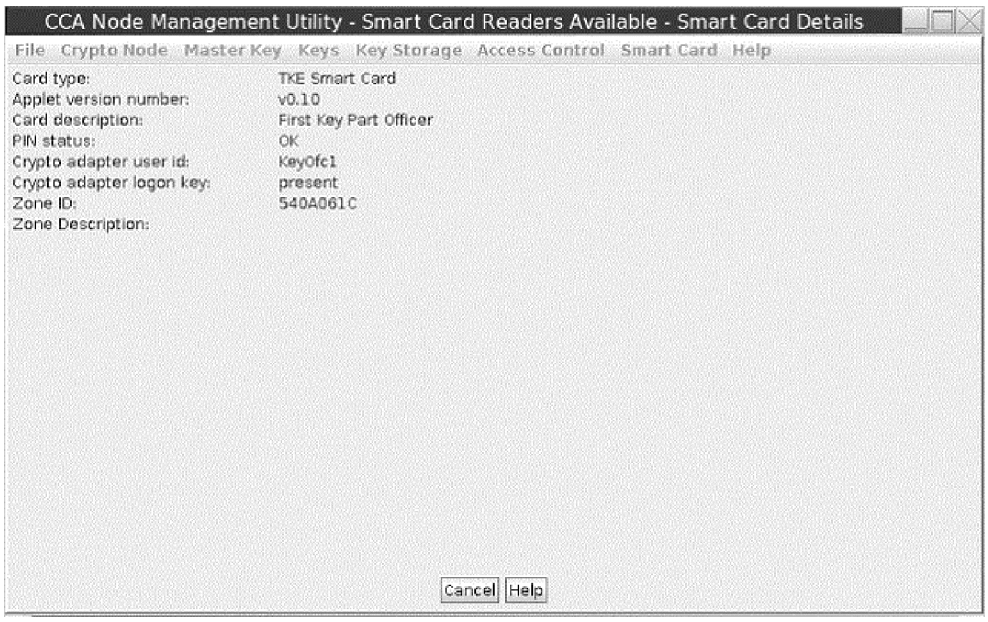


Figure 225. Display Smart Card Details — public information displayed

The following information is displayed for a TKE or EP11 smart card:

Card type
TKE smart card or EP11 smart card

Applet version number
Version number of applet loaded on smart card

Card description
Description of the smart card. The smart card description was entered when the smart card was personalized

PIN status
The PIN status can be OK/blocked/not set. The PIN is set when the smart card is personalized

Crypto Adapter User ID
User ID entered when a Crypto Adapter logon key is generated. The User ID may be blank if the smart card does not have a Crypto Adapter logon key

Crypto Adapter Logon Key
Status can be present/not present

Zone ID
Set when the smart card is initialized

Zone Description
Set when the smart card is initialized

Manage smart card contents

Use this function to delete keys or key parts from a TKE or EP11 smart card. A TKE or EP11 smart card can hold up to 50 key parts, a TKE authority signature key or EP11 administrator signature key, and a crypto adapter logon key. To display the smart card contents using the Manage Smart Card Contents function, do the following:

1. From the **Smart Card** pull-down menu, select **Manage Smart Card contents**. You will be prompted for a TKE or EP11 smart card. Insert the source smart card into smart card reader 2.

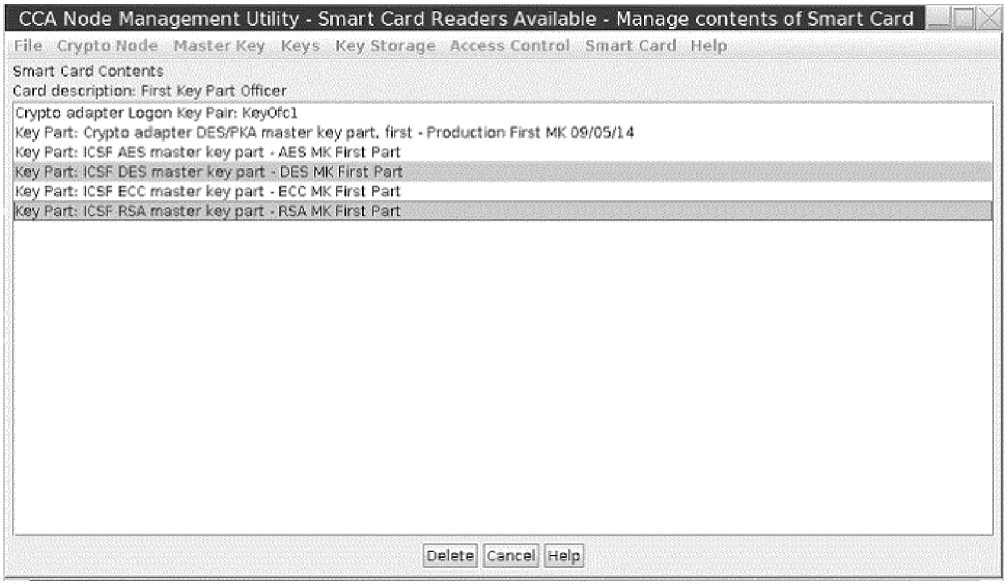


Figure 226. Manage Smart Card contents — contents of smart card are displayed

2. The smart card description is displayed. Ensure this is the correct smart card you want to work with. Highlight the keys and/or key parts you want to delete. Press the **Delete** push button.
3. You will be prompted for your PIN. Enter your PIN on the smart card reader 2 PIN pad.
4. You will be asked to confirm the deletion of the selected objects. Press **OK** to continue.

Figure 227. Manage Smart Card contents — confirm delete prompt

5. The objects are deleted and the list is refreshed.

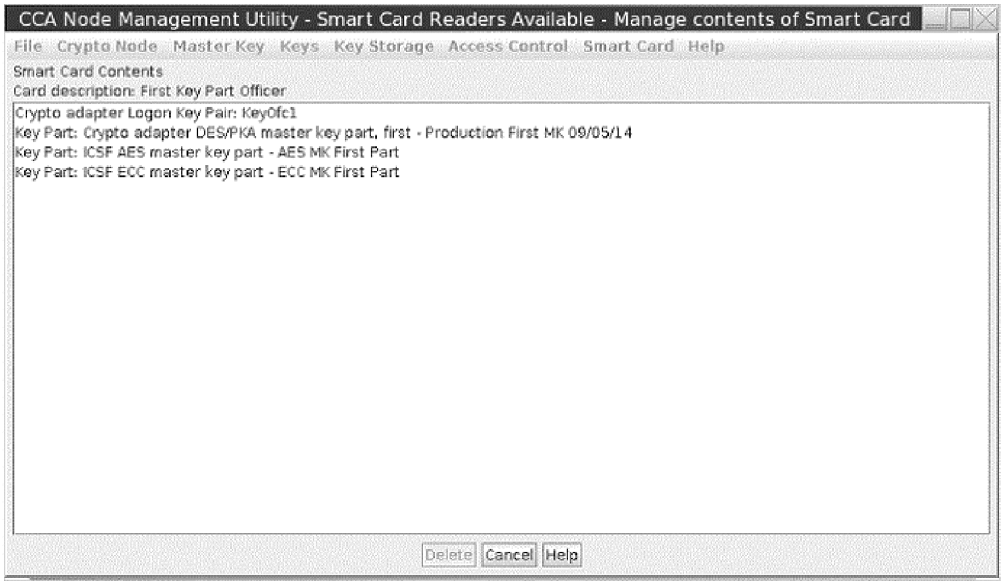


Figure 228. Manage Smart Card contents

Attention: If you delete a crypto adapter logon key, you will not be able to log on to the TKE workstation crypto adapter until you generate a new crypto adapter logon key and the administrator updates your crypto adapter user profile.

If you delete a TKE authority signature key, you will not be able to sign a TKE command until the administrator generates a new authority signature key and uploads it to the host.

Copy smart card

Use this function to copy a key or key part or parts from one TKE smart card to another TKE smart card, or from one EP11 smart card to another EP11 smart card. The two smart cards must belong to the same zone. Specifically, the two smart cards must have the same Zone ID. Use **Display Smart Card Details** to verify the Zone ID of the smart cards.

Notes:

1. AES key parts cannot be copied to a TKE smart card that does not have the TKE applet version 0.4 or later. ECC (APKA) key parts cannot be copied to a TKE smart card that does not have the TKE applet version 0.6 or later.
2. ECC authority signature keys cannot be copied to a TKE smart card that does not have the TKE applet version 0.10 or later.
3. Smart card copy does not overwrite the target smart card. If there is not enough room on the target smart card, you will get an error message. You can either delete some of the keys on the target smart card (see "Manage smart card contents" on page 271) or use a different smart card.
4. TKE Version 6.0 was the final release that supported DataKey smart cards. Copying a DataKey smart card is the only 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 are prompted for a source TKE or EP11 smart card. This is the smart card you

want to copy from. Insert the source smart card into smart card reader 1. The contents of the smart card are displayed in the source container on the top.

Figure 229. Copy Smart Card — insert source smart card

2. You are prompted for a target smart card. This is the smart card you want to receive the data. The target smart card must be the same type (TKE or EP11) as the source smart card. Insert the target smart card into smart card reader 2. The contents of the smart card are displayed in the target container on the bottom. The contents of this container are greyed out.

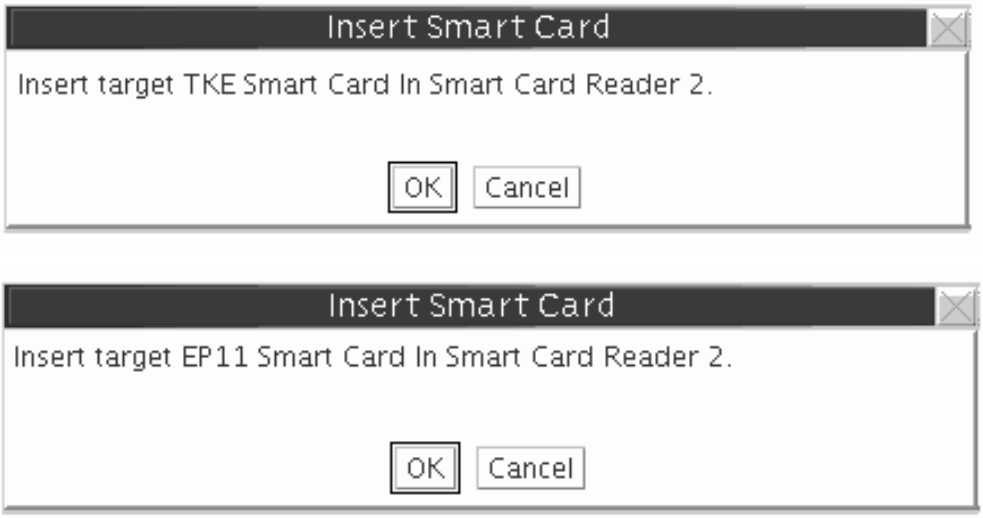


Figure 230. Copy Smart Card — asked for the TKE or EP11 smart card

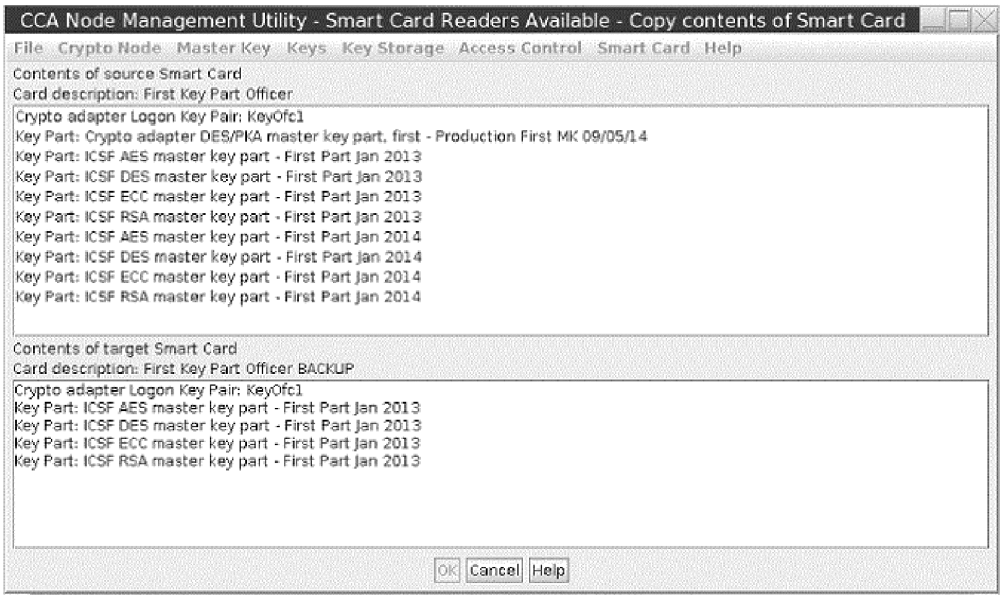


Figure 231. Copy Smart Card — smart card contents are displayed

3. Highlight the objects in the source container to copy to the target container. Press **OK** to continue.

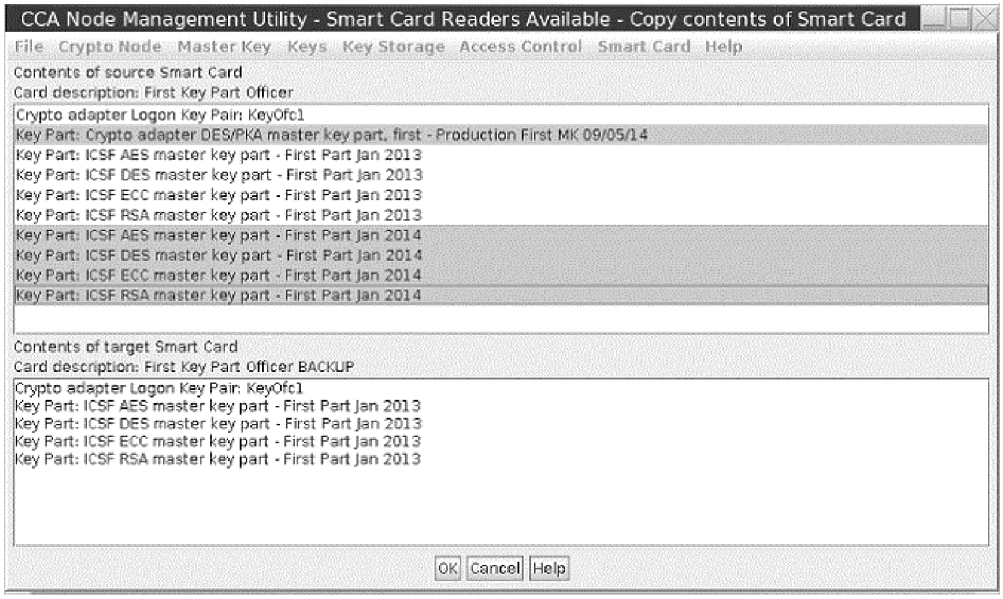


Figure 232. Copy Smart Card — highlight source objects to copy to target

4. You are prompted for the PIN of the source smart card in smart card reader 1. Enter the PIN on the smart card reader 1 PIN pad.

Figure 233. Copy Smart Card — source smart card PIN prompt

5. You are prompted for the PIN of the target smart card in smart card reader 2. Enter the PIN on the smart card reader 2 PIN pad. A secure session is established between the two smart cards and the selected object or objects are copied. The contents of the target container is refreshed.

Figure 234. Copy Smart Card — target smart card PIN prompt

Figure 235. Establishing a secure session between source and target smart cards

Figure 236. Objects are copied to the target smart card

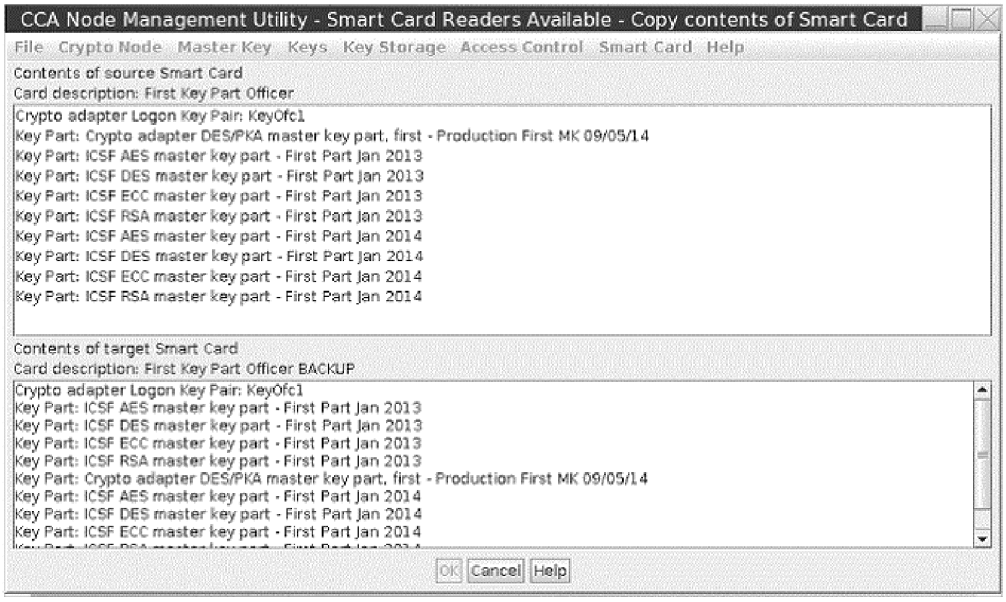


Figure 237. Copy Smart Card — objects are copied to the target container

TKE and EP11 smart cards can hold a maximum of 50 key parts, in addition to a crypto adapter logon key and a TKE authority signature key or an EP11 administrator signature key.

CNM common errors

Message: "Incorrect passphrase"
Return Code: 4
Reason Code: 2042
Explanation: Check that you typed in the passphrase correctly. The passphrase is case sensitive.

Message: "Access is denied for this function"
Return Code: 8
Reason Code: 90
Explanation: The role associated with your profile does not allow you to perform this function. Log off the crypto module and log on using a profile associated with a role that allows this function.

Message: "Your user profile has expired"
Return Code: 8
Reason Code: 92
Explanation: The TKE administrator must reset the expiration date on the user profile.

Message: "Your authentication data (for example, passphrase) has expired."
Return Code: 8
Reason Code: 94
Explanation: The TKE administrator must change the passphrase and reset the passphrase expiration date on the user profile. Then, select **Replace** to load the profile into the workstation coprocessor.

Message: "The user profile does not exist"
Return Code: 8
Reason Code: 773
Explanation: Make sure you typed in the user ID correctly. The user ID is case sensitive.

Message: "The group logon failed because authentication of one or more group members failed."
Return Code: 8
Reason Code: 2084
Explanation: One or more user profiles in the group failed authentication (for example, passphrase expired or profile expired) causing the group logon to fail. The group logon window will indicate which user failed and the reason for the logon failure. Correct the user profile or attempt group logon again and select a different member in the group members list for logon.

Message: "The profile is included in one or more groups"
Return Code: 8
Reason Code: 2085
Explanation: You attempted to delete a user profile that is currently a member of a group profile. You must remove the user profile from the group member list before deleting the profile.

Message: "The group role does not exist."
Return Code: 8
Reason Code: 2086
Explanation: You attempted group logon using a group profile that is associated with a role that does not exist. The TKE administrator must define the role and load it to the TKE workstation crypto adapter before the group profile may be used.

Message: "Your group profile has not yet reached its activation date"
Return Code : 8
Reason Code: 2087
Explanation: The group profile has an activation date that is later than the

current date. The TKE administrator must change the activation date before the group profile may be used or wait until the activation date arrives.

Message: "Your group profile has expired."
Return Code: 8
Reason Code: 2088
Explanation: The group profile has surpassed its expiration date.
The TKE administrator must change the expiration date before the group profile may be used.

Chapter 12. Smart Card Utility Program (SCUP)

The TKE Smart Card Utility Program (SCUP) supports the smart card system with the following functions:

General information

When entering PINs, the PIN prompt appears on both the TKE workstation screen as well as on the smart card reader. When certain tasks will take over one minute for SCUP to execute, information messages are returned. Be patient so that you do not have to restart the task.

Beginning in TKE 7.2, TKE supports 2, 3, or 4 smart card readers. The additional readers were added to reduce the amount of smart card swapping needed during the command signature phase for PKCS #11 (EP11) functions. However, the additional readers can be used in other operations too. Some screens in SCUP look different when more than 2 readers are present.

Note: There are 6 USB ports on a TKE workstation. This is enough ports for the mouse, keyboard, and 4 smart card readers. However, this configuration does not leave any USB ports for removable media. If you want to have 4 smart card readers and have ports available for USB flash memory, we recommend the purchase of an unpowered 2 or 4 slot USB hub. Plug the smart card readers into the hub which will leave other USB ports available for USB flash memory drivers.

The utility is capable of overwriting your smart cards. You will be prompted to reply **OK** before the card is overwritten.

To start SCUP, click on **Trusted Key Entry** in the main workstation screen. This will display various workstation functions.

Note: You can use the Smart Card Utility Program if you are logged on at the console as ADMIN or TKEUSER. In addition, you must be logged onto the TKE workstation crypto adapter with a profile defined when you configured the TKE

workstation from CNM. You are prompted to logon to the TKE workstation crypto adapter if you are not currently logged on.

Click on **Applications**. Under Applications, click on **Smart Card Utility Program**. The Smart Card Utility Program screen appears.

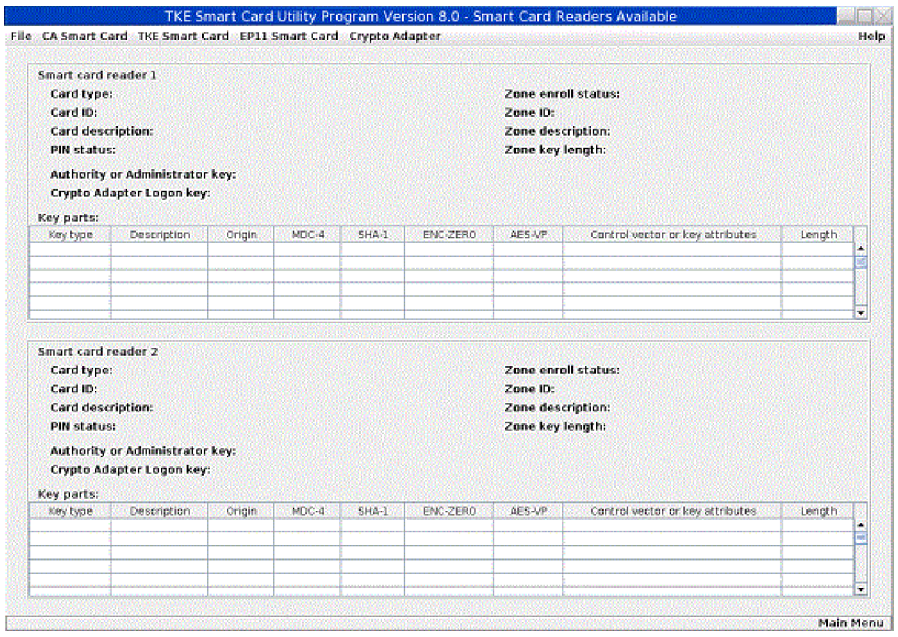


Figure 238. First screen of TKE Smart Card Utility Program (SCUP) with 2 readers

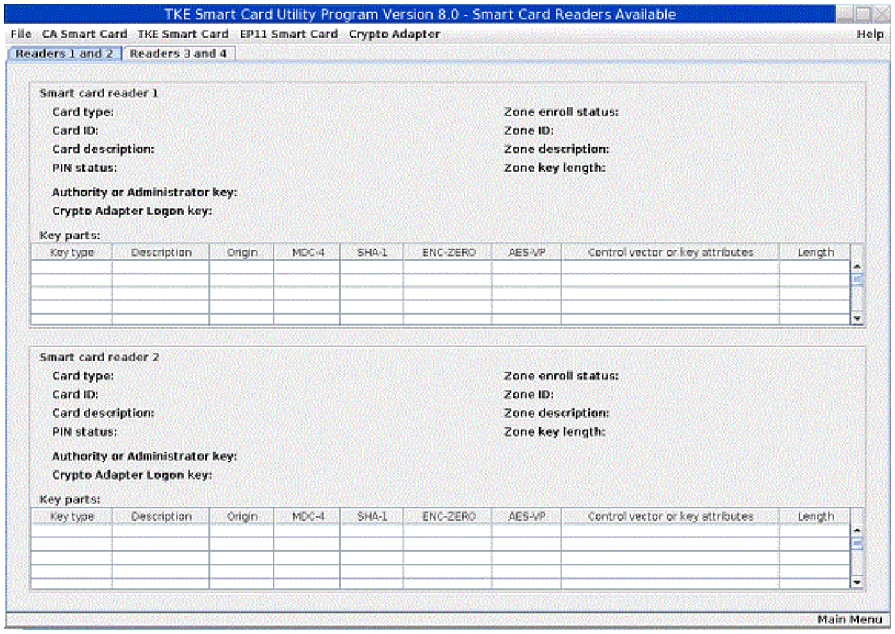


Figure 239. First screen of TKE Smart Card Utility Program (SCUP) with more than 2 readers

Drop down menus exist for these tabs on the top of the screen:
- **File**
- **CA Smart Card**
- **TKE Smart Card**
- **EP11 Smart Card**

- **Crypto Adapter**

Tasks associated with the drop down menu for **File** are:
- "Display smart card information."
- "Display smart card key identifiers" on page 283
- 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 284.
- "Back up a CA smart card" on page 287.
- "Change PIN of a CA smart card" on page 289.

Tasks associated with the drop down menu for **TKE Smart Card** are:
- "Initialize and enroll a TKE smart card" on page 289.
- "Personalize a TKE smart card" on page 291.
- "Unblock PIN on a TKE smart card" on page 291.
- "Change PIN of a TKE smart card" on page 291..

Tasks associated with the drop down menu for **EP11 Smart Card** are:
- "Initialize and enroll an EP11 smart card" on page 292
- "Personalize an EP11 smart card" on page 293
- "Unblock PIN on an EP11 smart card" on page 294
- "Change PIN of an EP11 smart card" on page 294

Tasks associated with the drop down menu for **Crypto Adapter** are:
- "Enroll a TKE cryptographic adapter" on page 294.
- "View current zone" on page 301.

File menu functions

Display smart card information

After you have created a smart card, you are advised to check the results. If you are copying keys from one smart card to another, you might also want to verify that all of the keys were correctly copied to the other smart card.

1. Insert the smart cards to be displayed in the smart card readers. From the **File** menu, click **Display smart card information**.

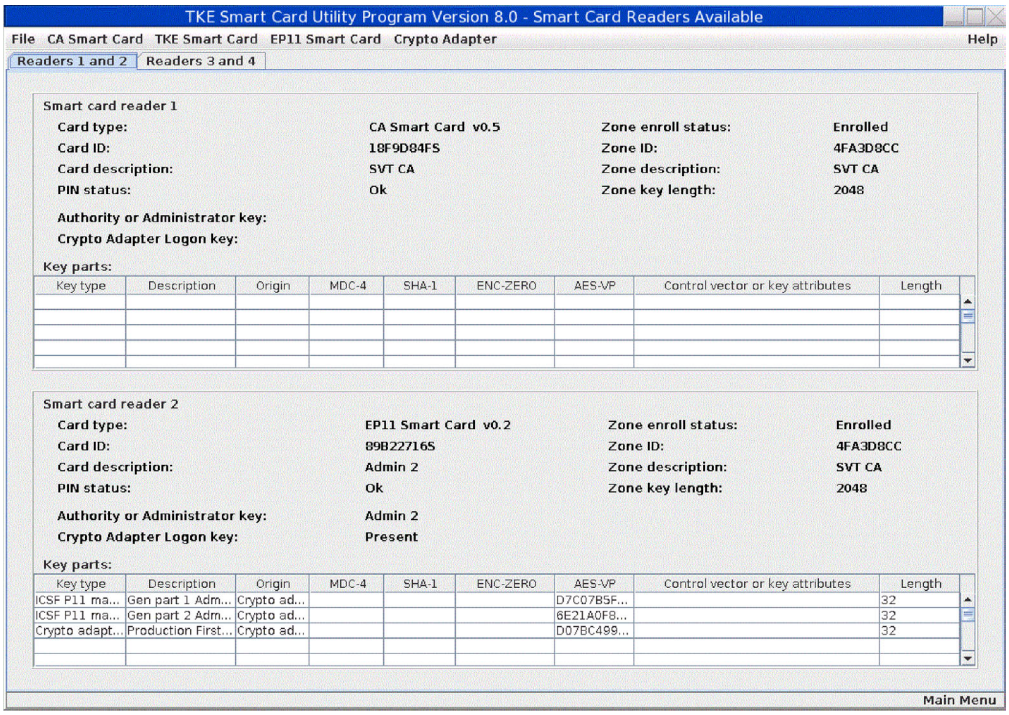


Figure 240. Display smart card information

The panel provides the following information about the smart card:

- **Card type**: Identifies the type and applet version of the smart card in the reader. TKE supports CA, TKE, EP11, MCA, IA, and KPH smart cards.
- **Card ID**: A 9-digit identifier generated when the smart card is initialized.
- **Card description**: This is the description you entered when creating the smart card. Can be 30 characters in length.
- **PIN status**: OK, Blocked or Not set
- **Authority or Administrator key**: For TKE smart cards, displays the authority index and name. For EP11 smart cards, displays the administrator name.
- **Crypto Adapter Logon Key**: For TKE and EP11 smart cards, 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 generates 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 and EP11 smart cards store key parts, so fields in the **Key parts** table are filled in only for these smart card types.

- **Key type**: operational key parts, TKE crypto adapter master key parts, or ICSF master key parts
- **Description**: description of key part (optional)
- **Origin**: Crypto Adapter or PIN-PAD
- **MDC-4**: MDC-4 hash value of the key part
- **SHA-1**: SHA-1 hash value of the key part

- **ENC-ZERO**: ENC-ZERO hash value of the key part
- **AES-VP**: AES verification pattern of the key part
- **Control vector or key attributes**: For DES operational key parts and AES DATA operational key parts, contains the control vector. For AES non-DATA operational key parts, indicates whether the key part uses the default key attributes or custom key attributes. Blank for master key parts.
- **Length**: 8, 16, 24 or 32 bytes

Display smart card key identifiers

This function displays the key identifiers and key lengths for the TKE Authority Key or EP11 Administrator Key, and the Crypto Adapter Logon Key, on a TKE or EP11 smart card. Some information from the Display smart card information panel is repeated to provide context.

1. Insert smart card or cards to be displayed in smart card reader 1 or 2. From the **File** menu, click **Display smart card key identifiers**.

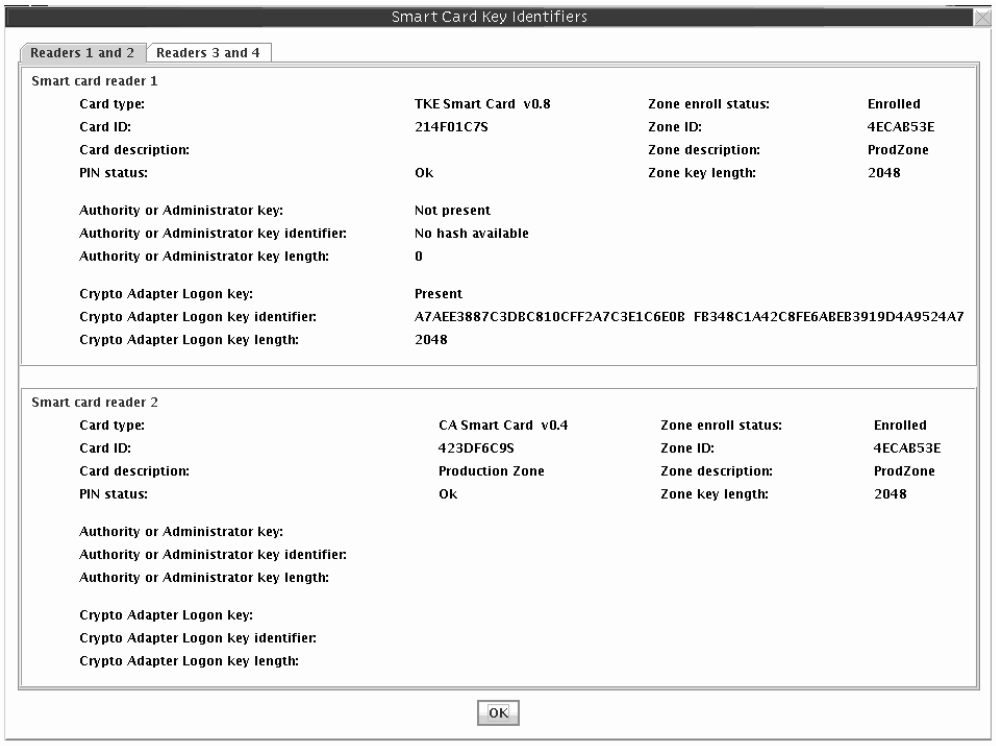


Figure 241. Display of smart card key identifiers

The panel provides this information about the smart card:

- **Card type**: Identifies the type and applet version of the smart card in the reader. TKE supports CA, TKE, EP11, MCA, IA, and KPH smart cards.
- **Card ID**: A 9-digit identifier generated when the smart card is initialized.
- **Card description**: This is the description you entered when creating the smart card. Can be 30 characters in length.
- **PIN status**: OK, Blocked or Not set
- **Authority or Administrator key**: For TKE smart cards, displays the authority index and name. For EP11 smart cards, displays the administrator name.

- **Authority or Administrator key identifier**: For TKE and EP11 smart cards, identifies the authority or administrator key. The key identifier is the SHA-256 hash of the public part of the signature key.
- **Authority or Administrator key length:** The type of the authority or administrator signature key, if present. The type (either RSA or ECC) is indicated along with either the key size in bits (RSA) or curve size in bits (ECC).
- **Crypto Adapter Logon Key**: For TKE and EP11 smart cards, the value can be Present or Not Present.
- **Crypto Adapter Logon Key Identifier**: For TKE and EP11 cards, identifies the crypto adapter logon key. The key identifier is the SHA-256 hash of the DER-encoded public modulus and public exponent of the RSA key pair.
- **Crypto Adapter Logon key length**: The length of the RSA key (in bits) on the smart card used to log on to the TKE workstation crypto adapter.
- **Zone enroll status**: The Zone enroll status is the status of the card. It is either Enrolled or Not enrolled.
- **Zone ID**: When a CA or MCA smart card is created, the system will generate an 8-digit zone number.
- **Zone Description**: This is the description you entered when creating the CA or MCA smart card. Can be 12 characters in length.
- **Zone key length**: The length of the zone certificate public modulus in bits.

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 36 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.

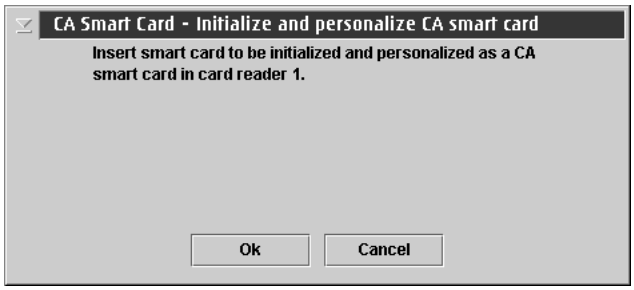


Figure 242. First step for initialization and personalization of the CA smart card

3. A dialog box displays, prompting you to select the zone key length. The zone key length can be either 1024 bit or 2048 bit.

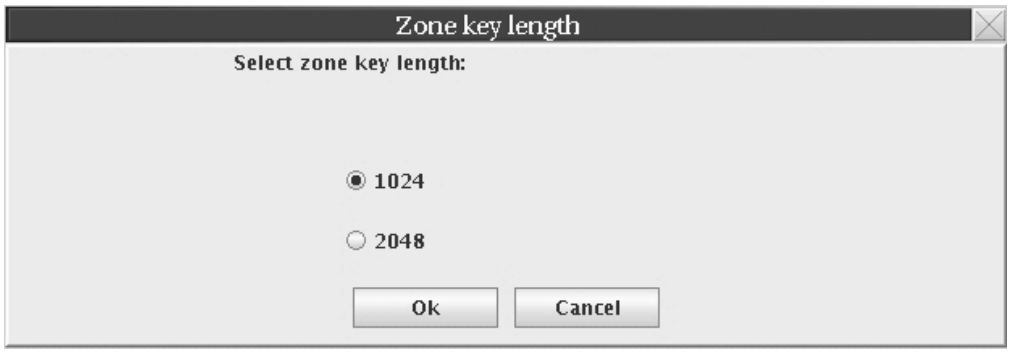


Figure 243. Zone key length window

4. If the smart card is not empty, a message is displayed indicating that the smart card is not empty and all data will be overwritten. If this is acceptable click **OK**.

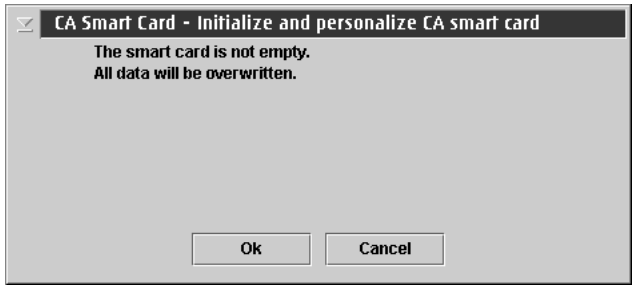


Figure 244. Message if card is not empty

5. The smart card will now be initialized.

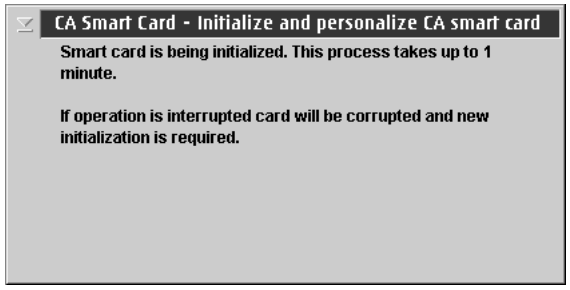


Figure 245. Initialization message for CA smart card

6. At the next prompt, enter a 6-digit PIN number twice. This is the first CA smart card PIN.

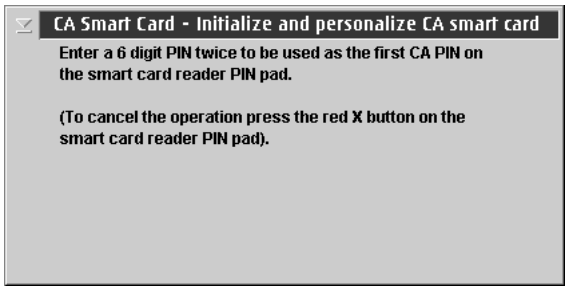


Figure 246. Enter first PIN for CA smart card

7. At the next prompt, enter a 6-digit PIN number twice. This is the second CA smart card PIN. For dual control it is recommended that different administrators enter the first and second CA smart card PIN and the PINs should not be the same.

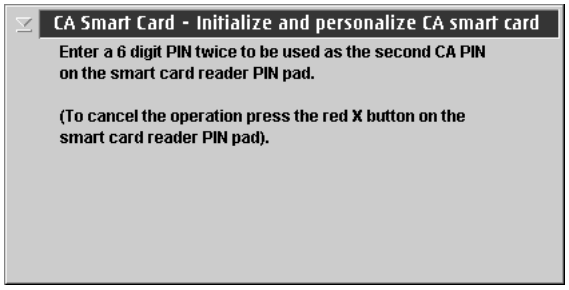


Figure 247. Enter second PIN twice for CA smart card

8. A dialog displays, prompting you to enter a zone description. Although a zone description is optional, it is recommended that you specify one.

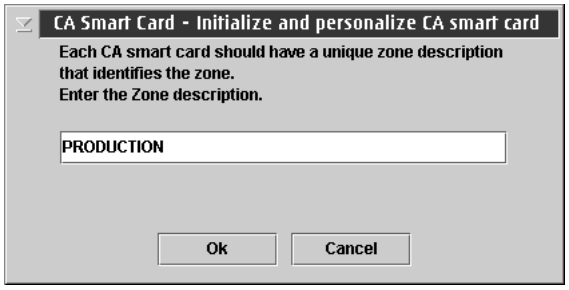


Figure 248. Enter zone description for CA smart card

9. A dialog displays, prompting you to enter a CA smart card description. Although a smart card description is optional, it is recommended that you specify one. After the description is entered the CA Smart Card will be built.

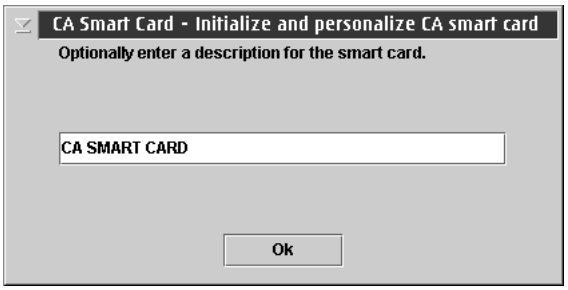


Figure 249. Enter card description for CA smart card

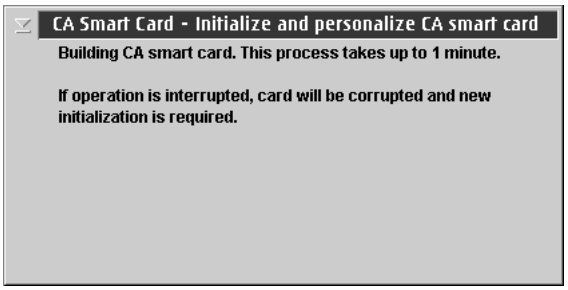


Figure 250. Building a CA smart card

10. You will get a message that a CA Smart Card was successfully created.

Back up 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 workstation crypto 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 or later, you can still backup CA smart cards to IBM part number 45D3398, 74Y0551, or 00JA710 smart cards.

To back up a CA smart card, follow these steps:

1. From the *CA Smart Card* drop down menu, select the *Backup CA smart card* option.
2. When prompted, insert the CA smart card to be backed up into smart card reader 1.

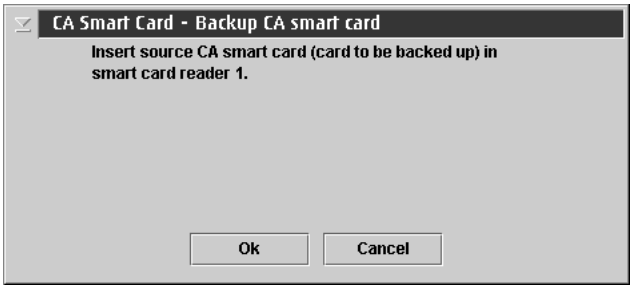


Figure 251. Begin creation of backup CA smart card

3. Enter the first CA smart card PIN.
4. Enter the second CA smart card PIN.
5. Insert the target CA smart card in smart card reader 2.
6. If the target smart card is not empty, you will be asked to overwrite all of the data on the smart card.
7. The target smart card is initialized.

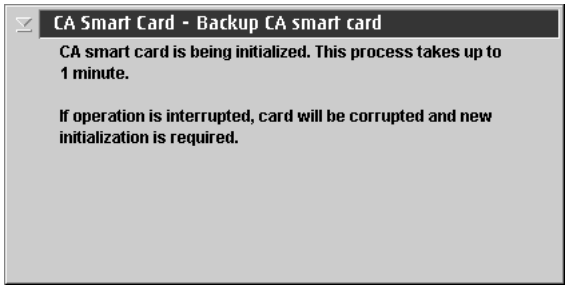


Figure 252. Initialization of backup CA smart card

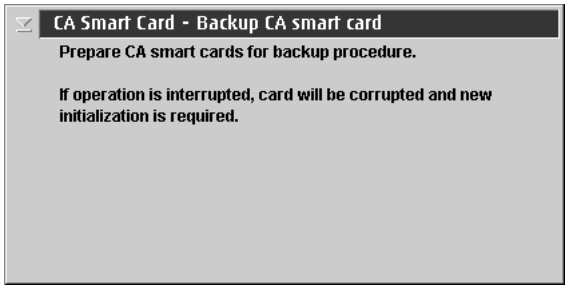


Figure 253. Continue creation of backup CA smart card

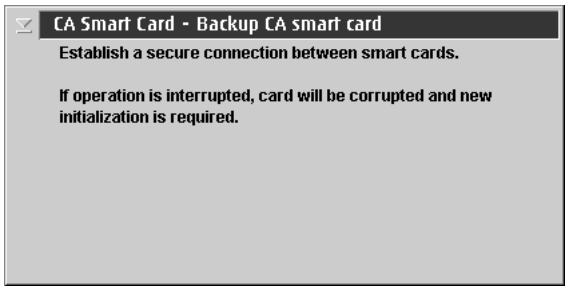


Figure 254. Establish secure connection for backup CA smart card

8. At the prompts, enter the first and second CA PINs of the original CA smart card on the smart card reader 2.

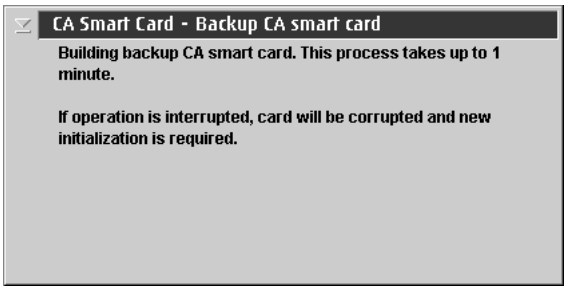


Figure 255. Building backup CA smart card

9. You will get a message that a CA Smart Card was successfully copied.

Change PIN of a CA smart card

To change the PIN of a CA smart card, follow these steps:

1. From the *CA Smart Card* drop down menu, select *Change PIN* option.
2. Insert the CA smart card in smart card reader 1.
3. A dialog displays, prompting you to select either first CA PIN or second CA PIN.

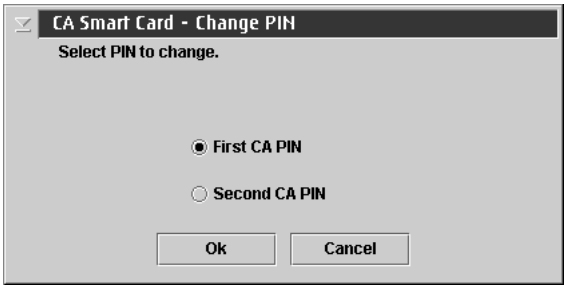


Figure 256. Select first CA PIN

4. Enter the current 6-digit PIN once.
5. Enter the new PIN twice — when prompted.
6. You will get a message that the PIN was successfully changed.

TKE smart card menu functions

The purpose of a TKE smart card is to hold key material for CCA host crypto modules (CEX2C, CEX3C, CEX4C, and CEX5C crypto modules). Before the TKE smart card can hold key material, however, it must be initialized and personalized. The TKE Smart Card menu contains options for initializing and personalizing a TKE smart card. Menu options are also available to unblock and change the smart card's PIN.

Initialize and enroll a 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 36 for more information.

To initialize a TKE smart card, follow these steps:

1. From the *TKE Smart Card* drop down menu, select *Initialize and enroll TKE smart card* option.

2. At the prompt, insert a CA smart card (into smart card reader 1) belonging to the zone you want to enroll the TKE smart card in.
3. Enter the first CA PIN on the PIN pad of smart card reader 1.
4. Enter the second CA PIN on the PIN pad of smart card reader 1.

   Note: If you have entered the two PINs for the CA card, have not restarted SCUP, and have not removed the CA card, the two PINs (of the CA smart card) may not require reentry when you are initializing TKE smart cards. This feature is only used when initializing TKE smart cards. All other functions that require the CA PINs will require reentry every time.
5. At the prompt, insert in smart card reader 2 a smart card to be initialized as a TKE smart card.

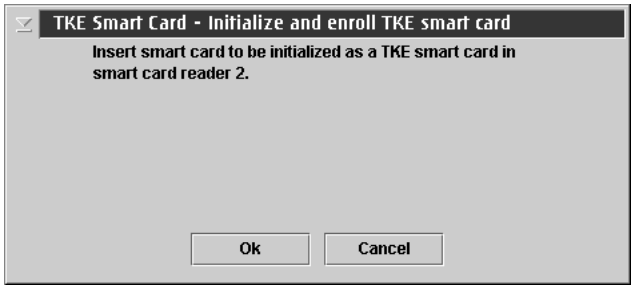


Figure 257. Initialize and enroll TKE smart card

6. If the card is not empty, you will be asked to overwrite all of the data on the smart card.
7. You will see screens indicating that the smart card is being initialized and then the TKE smart card is being built.

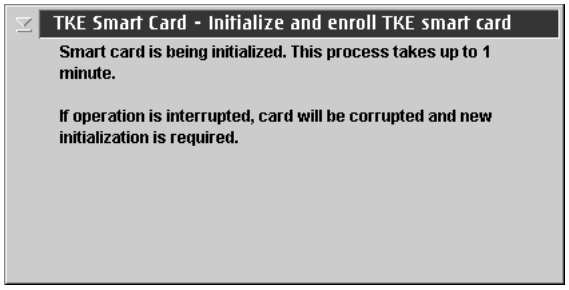


Figure 258. Initializing TKE smart card

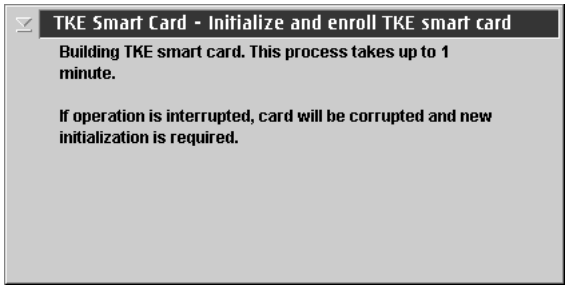


Figure 259. Building TKE smart card

8. When complete, you will get a message that the TKE smart card was successfully created. The TKE smart card must be personalized before it can be used for storing keys and key parts.

Personalize a TKE smart card

To personalize a TKE smart card, follow these steps:

1. From the *TKE Smart Card* drop down menu, select the *Personalize TKE smart card* option.
2. You will be prompted to insert an initialized TKE smart card in smart card reader 2.

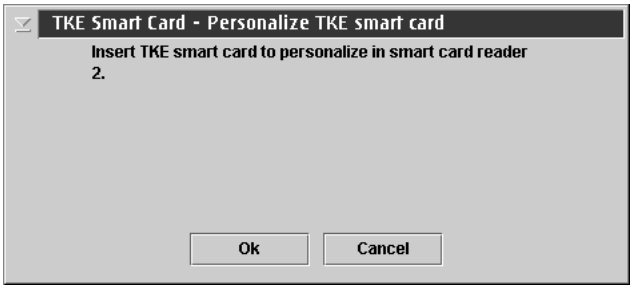


Figure 260. Personalizing TKE smart card

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.

EP11 smart card menu functions

The purpose of an EP11 smart card is to hold key material for EP11 host crypto modules (CEX4P and CEX5P crypto modules). This key material can include EP11 master key parts, key parts for TKE workstation crypto adapter master key registers, a TKE crypto adapter logon key, and an EP11 administrator signature key.

The EP11 Smart Card menu contains options for initializing and enrolling an EP11 smart card in a zone, for personalizing an EP11 smart card, for unblocking an EP11 smart card, and for changing the PIN on an EP11 smart card. The function and flow of these options is the same as for TKE smart cards, with an EP11 smart card being used in place of the TKE smart card.

Initialize and enroll an EP11 smart card

To initialize an EP11 smart card, follow these steps:

1. From the *EP11 Smart Card* drop down menu, select *Initialize and enroll EP11 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 EP11 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 EP11 smart cards. This feature is only used when initializing EP11 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 EP11 smart card.

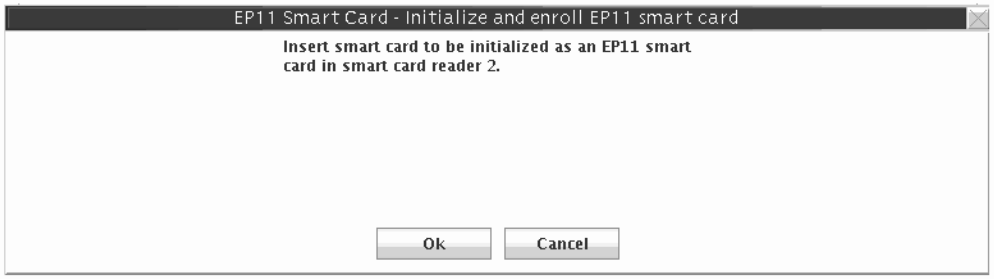


Figure 261. Initialize and enroll EP11 smart card

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 EP11 smart card is being built.

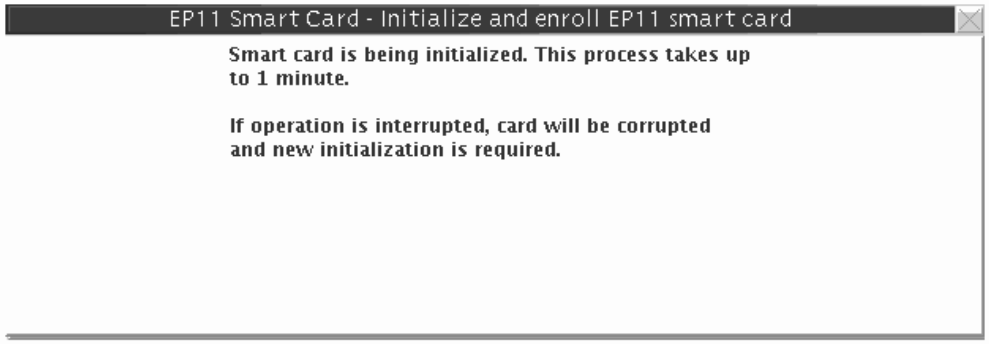


Figure 262. Initializing EP11 smart card

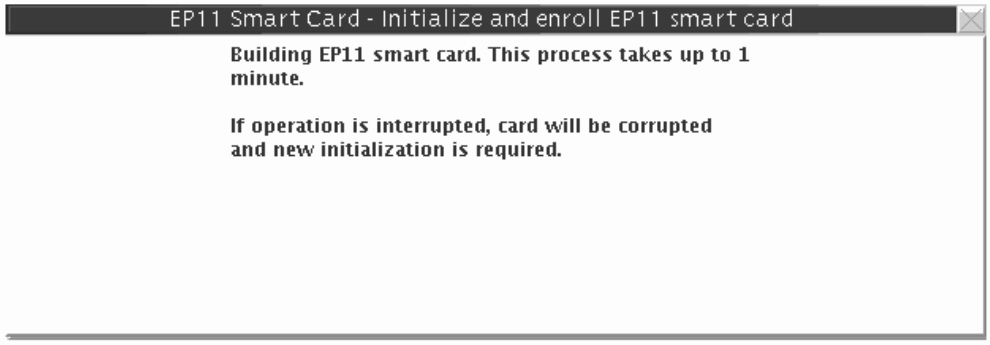


Figure 263. Building EP11 smart card

8. When complete, you will get a message that the EP11 smart card was successfully created. The EP11 smart card must be personalized before it can be used for storing keys and key parts.

Personalize an EP11 smart card

To personalize an EP11 smart card, follow these steps:

1. From the *EP11 Smart Card* drop down menu, select the *Personalize EP11 smart card* option.
2. You will be prompted to insert an initialized EP11 smart card in smart card reader 2.

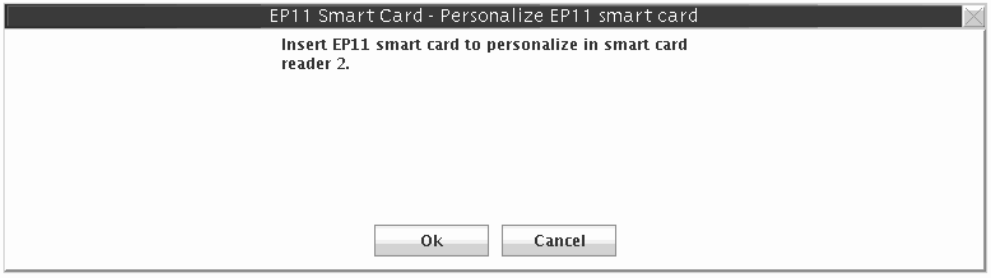


Figure 264. Personalizing EP11 smart card

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 EP11 smart card (optional).
5. When complete, you will get a message that the EP11 smart card personalization was successful.

Unblock PIN on an EP11 smart card

If an EP11 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 an EP11 smart card, follow these steps:

1. From the *EP11 Smart Card* drop down menu, select *Unblock EP11 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 EP11 smart card to be unblocked in smart card reader 2.
6. You will get a message that the EP11 smart card was successfully unblocked.

Change PIN of an EP11 smart card

To change the PIN of an EP11 smart card, follow these steps:

1. From the *EP11 Smart Card* drop down menu, select *Change PIN* option.
2. Insert the EP11 smart card in smart card reader 2.
3. Enter the current PIN once. This is a 6-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 crypto adapter can be enrolled locally or remotely.

Note: Enrolling of the TKE workstation crypto adapter must be done before loading key parts from TKE or EP11 smart cards.

You can check if the TKE workstation crypto adapter is enrolled in a zone from the Crypto Adapter drop down menu: select *View current zone* option. If it is not, a message window will indicate that the crypto adapter is not enrolled in a zone.

Figure 265. View current zone for a TKE cryptographic adapter

Local TKE workstations that have access to the CA Card may be enrolled locally. If you have offsite TKE workstations without access to the CA card, you may use the remote enroll application to enroll these workstations in the same zone.

If the enroll does not occur as part of the initialization, the current DEFAULT role will not have the necessary ACPs to perform the enroll. You can log on with a profile using SCTKEADM or equivalent authority, or you can reload the TEMPDEFAULT role (see "Managing roles" on page 239). If the TEMPDEFAULT role is used, then, once the enroll is complete, it is critical that the TEMPDEFAULT role be returned to the normal DEFAULT role. The TEMPDEFAULT role cannot be allowed to stay loaded as this role has ACPs for all functions.

Local crypto adapter enrollment

1. From the Crypto Adapter drop down menu, select Enroll Crypto Adapter option.
2. Select *local* when prompted for enrollment type.

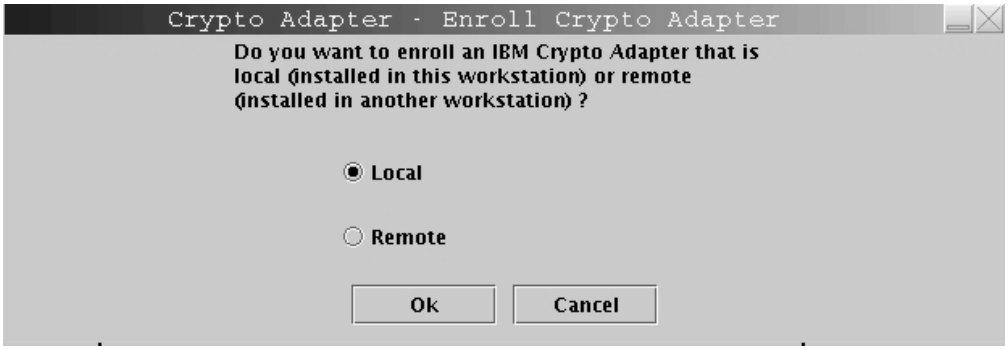


Figure 266. Select local zone

3. At the prompt, insert the CA smart card in smart card reader 1.
4. At the prompt, enter the first CA PIN on the PIN pad of smart card reader 1.
5. At the prompt, enter the second CA PIN on the PIN pad of smart card reader 1.
6. You will get a message that the enrollment for the crypto adapter was successful.

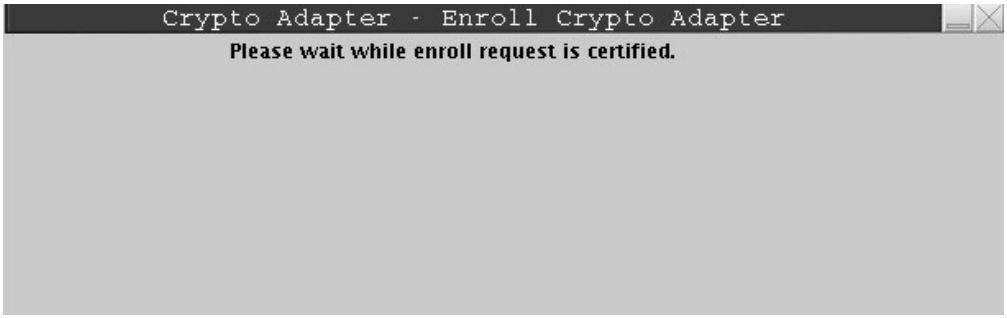


Figure 267. Certifying request for local Crypto Adapter enrollment

Figure 268. Message for successful Crypto Adapter enrollment

7. View the zone information after the crypto adapter is enrolled by selecting *View current zone* from the Crypto Adapter drop down menu.

Figure 269. View current zone after Crypto Adapter enrollment

Remote crypto adapter enrollment

The "Begin zone remote enroll process" and the "Complete zone remote enroll process" applications work together. You can use them to enroll a TKE workstation in the same zone as another TKE workstation at a remote site when you do not have the CA smart card at the site where the TKE workstation to be enrolled is located. Use remote enrollment only under the following conditions:

- The TKE workstation that is to be enrolled in the zone is not at the same location as the TKE that is enrolled in the zone.
- The CA smart card is not available (and will never be available) at the site where the TKE workstation that must be enrolled is located.

Guideline: It is highly preferable that CA smart cards be available at both locations and that you use local zone enrollment in place of remote enrollment.

Note: Without a CA smart card, you cannot create any TKE or EP11 smart cards. Instead, you must create TKE and EP11 smart cards at the location with the CA smart card, and send them to the location without the CA smart card.

The following tasks are required to complete the remote zone enrollment on a TKE:

1. Task 1: If necessary, format a USB flash memory drive for Trusted Key Entry data. For more information, see "Formatting a USB flash memory drive for Trusted Key data (task 1)."
2. Task 2: Create a remote zone enrollment request.

   From the TKE workstation that is to be enrolled, use the "Begin zone remote enroll process" application to create an enrollment request file. After the request file is created, it must be taken to the TKE that is enrolled in the zone. For more information, see "Creating a remote zone enrollment request (task 2)" on page 298.
3. Task 3: Process the remote zone enrollment request.

   From the TKE workstation that is enrolled in the zone, use the "remote enrollment" function of the smart card utility program (SCUP) to process the request. This function produces an enrollment certificate file. After the certificate file is created, it must be taken back to the TKE that is to be enrolled in the zone. For more information, see "Processing the remote zone enrollment request (task 3)" on page 299

   Requirement: The SCUP remote enroll operation requires a CA smart card.
4. Task 4: Complete the remote zone enrollment.

   From the TKE workstation that is to be enrolled, use the "Complete zone remote enroll process" application to finish the zone enrollment. For more information, see "Completing the remote zone enrollment (task 4)" on page 300.

Formatting a USB flash memory drive for Trusted Key data (task 1):

This task is the first task in the remote zone enrollment process. You can use a USB flash memory drive to move files between the TKE workstation that is going to be enrolled and the TKE workstation that is already enrolled in the zone. The USB flash memory drive must be formatted for Trusted Key Entry data.

About this task

If your USB flash memory drive is not formatted for Trusted Key Entry data, follow these instructions. Otherwise, skip to the next task, "Creating a remote zone enrollment request (task 2)" on page 298

Procedure

1. Install the USB flash memory drive in any open USB port and wait for the device to report in. It can take up to 30 seconds.
2. From the Trusted Key Entry console, click **Service Management**.
3. Open the **Format Media** application.
4. Click **Trusted Key Entry data**.
5. Click **Format**.
6. Click the choice for your USB flash memory device.
7. Click **OK** The format process starts.
8. Click **Format**. Do not change the file system format.

9. Click **Yes** to allow the media to be overwritten. A window with a completion message opens when the format process is complete.
10. Click **OK** to close the message window.

Results

The USB flash memory drive is formatted for Trusted Key Entry data. Continue to the next task, "Creating a remote zone enrollment request (task 2)."

Creating a remote zone enrollment request (task 2):

This task is the second task in the remote zone enrollment process.

Before you begin

- You must have a USB flash memory drive that is formatted for Trusted Key Entry data. For more information, see "Formatting a USB flash memory drive for Trusted Key data (task 1)" on page 297.
- You must know the strength of the zone in which you are enrolling. It is either 1024 or 2048.

About this task

Perform this task on the TKE workstation that is to be enrolled in the remote zone.

Attention: After you complete this task, you must not reset the device key on this TKE workstation before you complete the zone enrollment. If you do, the remote zone enrollment fails and you must restart the remote zone enrollment process. Specifically, you must not take any of the following actions:

- Use the Cryptographic Node Management utility to initialize the TKE workstation's local crypto adapter.
- Use the TKE workstation's "IBM Crypto Adapter initialization" application to initialize the TKE's local crypto adapter.
- Locally enroll the TKE in a zone.

If you take any of these actions, the error `exception during application install` is issued at the end of task 4.

Procedure

1. Install the USB flash memory drive that is formatted for Trusted Key Entry data.
2. From the Trusted Key Entry console, click **Trusted Key Entry**.
3. Open the "Begin zone remote enroll process" application.
4. If necessary, log on to the crypto adapter.
5. Click **Yes** when you see the message `Begin remote enroll`.
6. Respond to the message about the remote zone key length:
   - Click **Yes** if the strength of the zone is 1024.
   - Click **No** if the strength of the zone is 2048.
7. If you are prompted to confirm the 2048 zone strength, click **Yes**.
8. If you are prompted to confirm that the existing enrollment is to be replaced, click **Yes**.

   Note: This step removes the TKE workstation from its current zone. The TKE workstation is not enrolled in a zone until the entire remote crypto adapter

enrollment process is complete. If you cancel the process after this point, you must restart and complete the remote crypto adapter enrollment process or perform a local "enroll crypto adapter" operation from the Smart Card Utility program.

9. When the "save the enrollment request file" window opens, respond:
   - Click **USB Flash Memory drive**
   - Enter a file name. For example, `MyEnrollmentRequestForTKExxxx`
   - Click **Save**.
10. When a window opens with a completion message, click **OK** to close the window.
11. When a window opens with a logoff message, click **OK**. Either logoff option is acceptable.
12. Remove the USB flash memory drive and send it to the remote location of the TKE that is enrolled in the zone.

Results

You created a remote zone enrollment request, saved the request to a USB flash memory drive, and sent the drive to the remote location. Continue to the next task, "Processing the remote zone enrollment request (task 3)."

Processing the remote zone enrollment request (task 3):

This task is the third task in the remote zone enrollment process.

Before you begin

- You must have the CA smart card.
- You must have the USB flash memory drive that has the enrollment request file. This file was created in task 2 ("Creating a remote zone enrollment request (task 2)" on page 298.

About this task

Perform this task on the TKE workstation that is enrolled in the zone.

Procedure

1. Install the USB flash memory drive that has the enrollment request file on the TKE workstation.
2. From the Trusted Key Entry console, click **Trusted Key Entry**.
3. Open the Smart Card Utility Program (SCUP).
4. If necessary, log on to the crypto adapter. You must log on with a profile that has TKEADM, SCTKEADM, or equivalent authority.
5. Click **Crypto Adapter > Enroll Crypto Adapter**.
6. Click **Remote**.
7. Click **OK**. A window opens with a message that asks if the file is available.
8. Click **OK**.
9. Insert the CA smart card in reader 1 and press the **OK** button.
10. Enter the PINs when you are prompted. The "open file that contains enrollment request" window opens.
11. Open the enrollment request file.
    a. Select **USB Flash Memory drive**.

b. Select the enrollment request file that was created in task 2.
c. Click **Open**.

A window with the message `do you want to enroll this adapter` opens.

12. Click **OK.** An enrollment certificate chain is created. A window with the message `enrollment has been granted` opens.
13. Save the enrollment certificate chain on the USB flash memory drive.
    a. Click **USB Flash Memory drive**.
    b. Enter a file name. For example, `EnrollmentCertForTKExxxx`.
    a. Click **Save**.
14. Click **OK** on the informational message.
15. Click **File > Exit and Logoff** to close the SCUP application.
16. Remove the USB flash memory drive and send it to the location of the TKE workstation that is to be enrolled in the zone.

Results

An enrollment certificate was created and saved to the USB flash memory drive. Continue to the next task, "Completing the remote zone enrollment (task 4)."

Completing the remote zone enrollment (task 4):

This task is the fourth and last task in the remote zone enrollment process.

Before you begin

You must have the USB flash memory drive that contains the enrollment certificate file that was created in task 3 ("Processing the remote zone enrollment request (task 3)" on page 299).

About this task

Perform this task on the TKE workstation that is to be enrolled in the remote zone.

If you receive the error `exception during application install` during this task, you probably reset the device key before you completed the zone enrollment. You must restart the remote zone enrollment process. For more information, see "Creating a remote zone enrollment request (task 2)" on page 298.

Procedure

1. Install the USB flash memory drive that contains the enrollment certificate file on the TKE workstation.
2. From the Trusted Key Entry console, click **Trusted Key Entry**.
3. Open the application "Complete zone remote enroll process for an IBM crypto adapter".
4. If necessary, log on to the crypto adapter.
5. Click **Yes** on the "Complete remote enroll" window.
6. If necessary, click **Yes** to allow the enrollment to replace an existing enrollment.
7. Open the enrollment request certificate.
   a. On the "open the enrollment request certificate" window, select **USB Flash Memory drive**.

b. Select the enrollment certificate that you created in task 3.
c. Click **Open**.

A window opens with the message `Crypto adapter has been enrolled`.

8. Click **Yes**. A window opens with a logoff message.
9. Click **Yes**. Either logoff option is acceptable.

Results

The remote zone enrollment is complete.

View current zone

Use the View current zone function to determine the current zone of the TKE workstation crypto adapter. You may want to compare it to the zone of a TKE or EP11 smart card when working with key parts.

To view the current zone of the TKE workstation crypto adapter, follow these steps:

1. From the *Crypto Adapter* drop down menu, select *View current zone* option.

Figure 270. 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 or EP11 smart card. A known key part will have been saved on paper or in a binary file.

Secure Key Part Entry allows migration of existing key parts to TKE or EP11 smart cards and provides an additional mechanism for key part entry. Using the PIN pad on the smart card reader, the key part can be stored on a smart card. You must enter the key part hexadecimal digits on the smart card reader key pad. See "Entering a key part on the smart card reader" on page 311.

By entering the key part on the PIN pad, the key part can be stored securely and any clear copies of the key part can be destroyed. Once stored on the smart card, the user should use the TKE to securely copy the key part to another smart card that is enrolled in the same zone for a backup. The user can then load the key part into key storage or onto the host.

Key parts for CCA host crypto modules (CEX2C, CEX3C, CEX4C, and CEX5C) are saved on TKE smart cards. Key parts for EP11 host crypto modules (CEX4P and CEX5P) are saved on EP11 smart cards.

Steps for secure key part entry

The steps you need to follow for secure key part entry differ depending on whether you are entering the key parts on a TKE or an EP11 smart card.

Steps for secure key part entry for a TKE smart card

For CCA host crypto modules, secure key part entry begins from the Crypto Module Notebook Domains tab's Keys tab by right-clicking the desired key type for entry. Right-clicking the desired key type reveals a menu with an entry for secure key part.

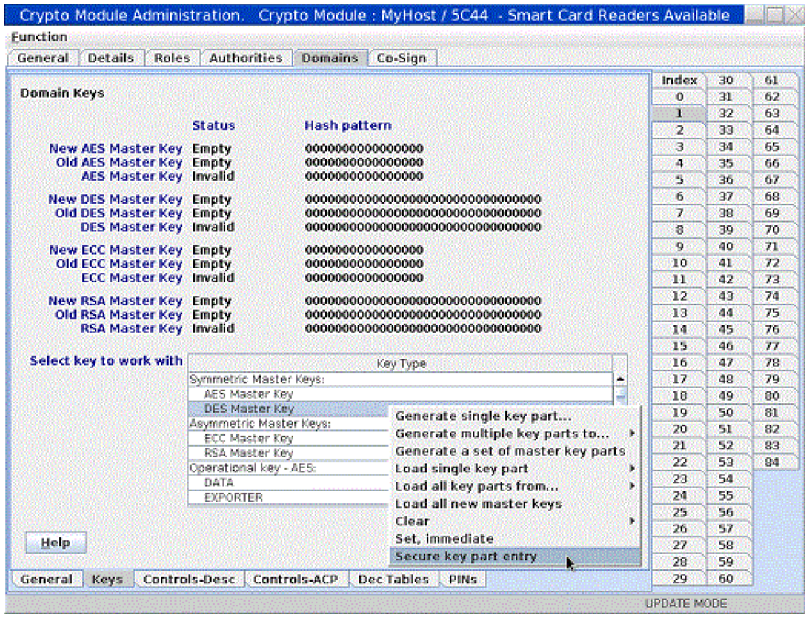


Figure 271. Choosing secure key part entry from the domains keys panel

This menu entry is available for all supported crypto module types.

1. Select **Secure key part entry**.

   For master keys on all host crypto modules, a panel for entering a key part description displays.

Figure 272. Enter description panel for secure key part entry

For DES operational keys, the Secure Key Part Entry window opens.

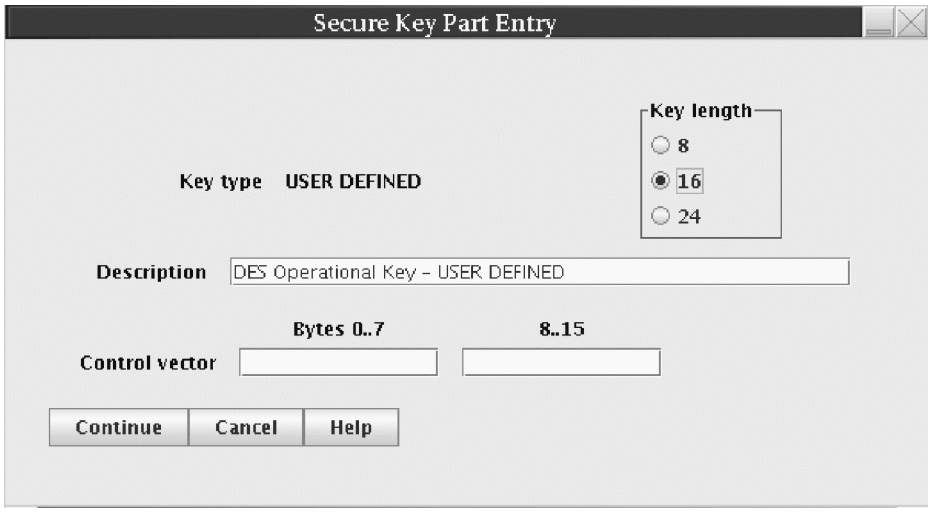


Figure 273. DES USER DEFINED operational key for secure key part entry

For a DES USER DEFINED operational key, the user is allowed to update the description, the key length, and the control vector.

For a predefined DES operational key or AES DATA operational key, only the description can be updated, unless the key type supports multiple key lengths. In that case, the key length field can also be updated. For a predefined DES operational key or AES DATA operational key, the control vector cannot be updated.

For AES operational keys other than DATA, the following Secure Key Part Entry window opens.

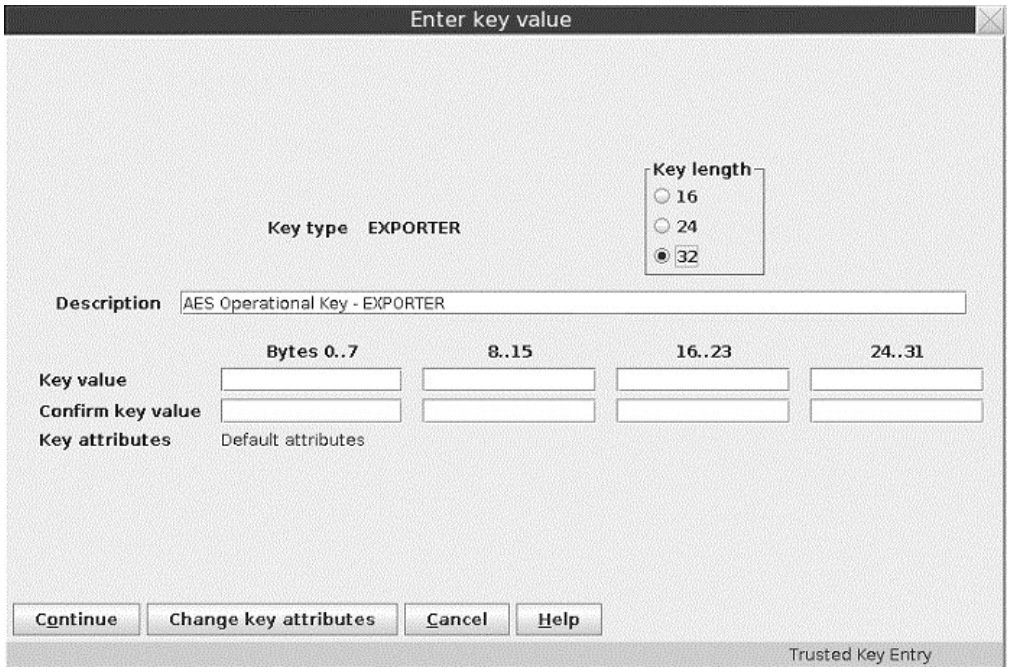


Figure 274. AES non-DATA operational key for secure key part entry

The key part description can be updated. Click **Change key attributes** to modify the key attributes.

2. After all the appropriate information has been entered for master and operational keys, the user is prompted to insert a TKE smart card into reader 2.

Figure 275. Secure key part entry — insert TKE smart card into reader

3. Enter the PIN on the smart card reader PIN pad when prompted.

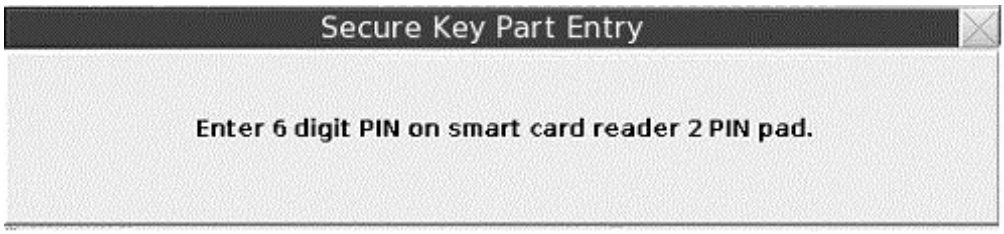


Figure 276. Secure key part entry — enter key part digits

A dialog displays information about the TKE smart card.

4. If the TKE smart card information is correct, press **Yes** to continue.

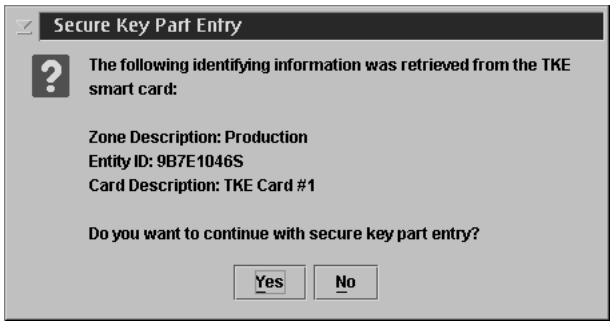


Figure 277. Secure key part entry card identification

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 311.

Note: Make sure that the TKE workstation crypto adapter and the TKE smart cards are in the same zone. To display the zone of a TKE smart card, exit TKE and use either the Cryptographic Node Management Utility or the Smart Card Utility Program under Trusted Key Entry Applications. See "Display smart card information" on page 281 or "Display smart card key identifiers" on page 283.

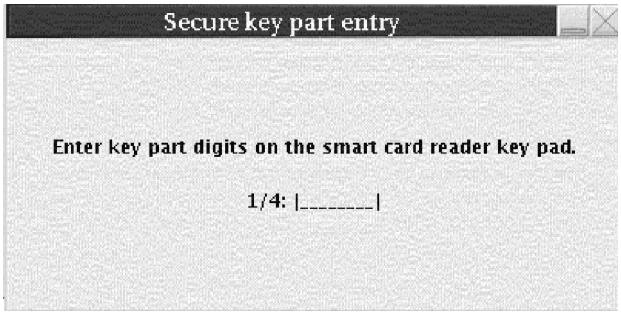


Figure 278. Secure key part entry — enter key part digits

The dialog shows the progress of each hexadecimal digit entered with an asterisk (*).

6. After the key part value has been successfully entered on the PIN pad, a window opens showing information about the key part just entered. Verify that you entered the information correctly.
   - For a DES key part, the ENC-ZERO, MDC-4, and SHA1 values are shown.
   - For an AES or ECC (APKA) key part, the AES-VP value is shown.
   - For a DES or AES DATA operational key, the control vector (CV) is also displayed.
   - For an AES non-DATA operational key, the window allows you to display key attributes.

   Click **OK** to continue.

Figure 279. Secure key part entry — DES key part information for a master key

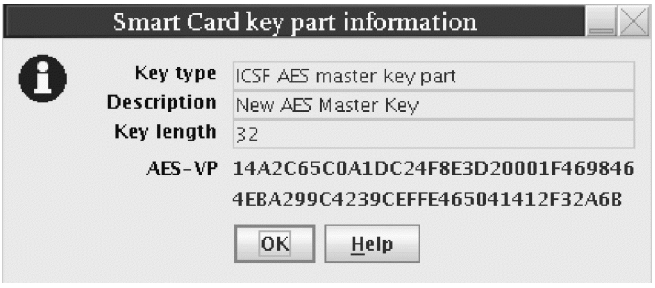


Figure 280. Secure key part entry — AES key part information for a master key

Figure 281. Secure key part entry — DES key part information for operational key

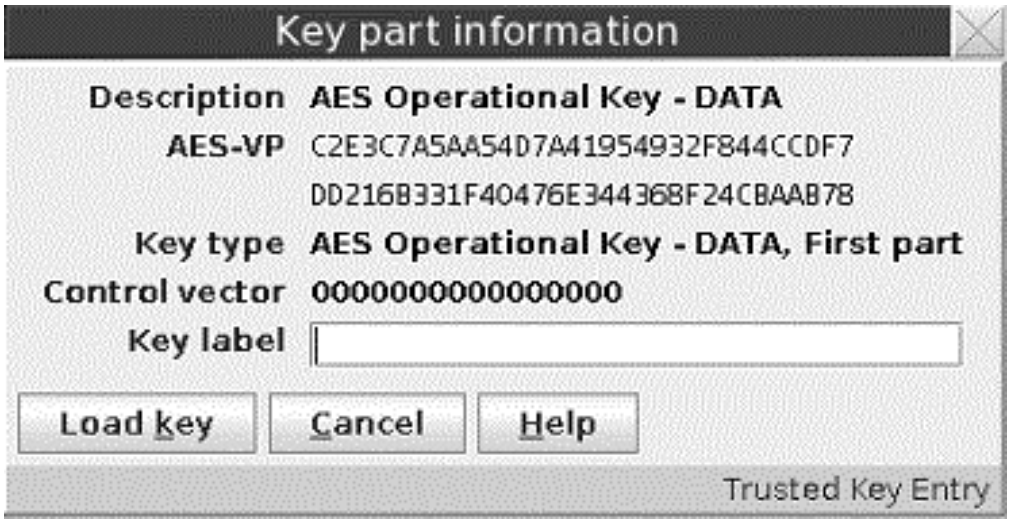


Figure 282. Secure key part entry — AES DATA operational key

Figure 283. Secure key part entry — AES non-DATA key

7. A message is displayed if the command executed successfully.

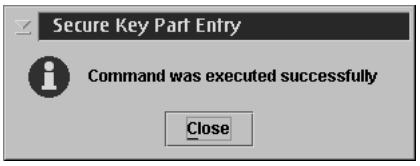


Figure 284. Secure key part entry — message for successful execution

Steps for secure key part entry for a EP11 smart card

For EP11 host crypto modules, secure key part entry begins from the **Keys** tab for a domain in the Crypto Module Notebook. Right-click in the domain keys window to display a menu, and click **Secure key part entry**.

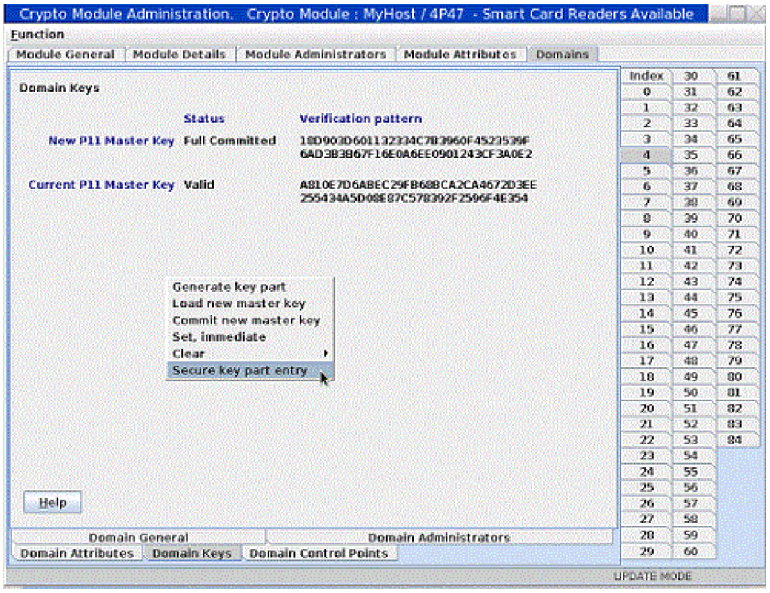


Figure 285. Choosing secure key part entry from the domain keys window

You are prompted to enter a description for the key part. After entering the description, you are prompted to select the smart card reader to use, to insert an EP11 smart card in the reader, and to enter the PIN. After the PIN is entered, a confirmation window opens showing the smart card's zone description, entity ID, and card description.

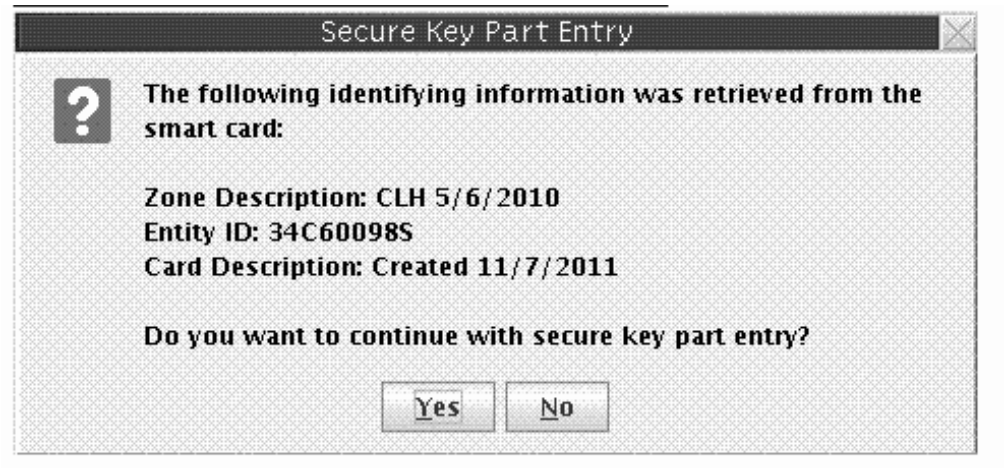


Figure 286. Secure key part entry card identification

Note: The smart card must be in the same zone as the TKE workstation crypto adapter in order for secure key part entry to be successful.

If you accept this smart card, you are prompted to enter the hexadecimal digits for the key part on the smart card reader PIN pad. To enter each hexadecimal digit, you must press two buttons on the PIN pad. For example, press "0" and "2" for the hexadecimal digit 2, or "1" and "4" for the hexadecimal digit E. After each hexadecimal digit is entered, an asterisk (*) is displayed on the panel to show how many hexadecimal digits have been entered.

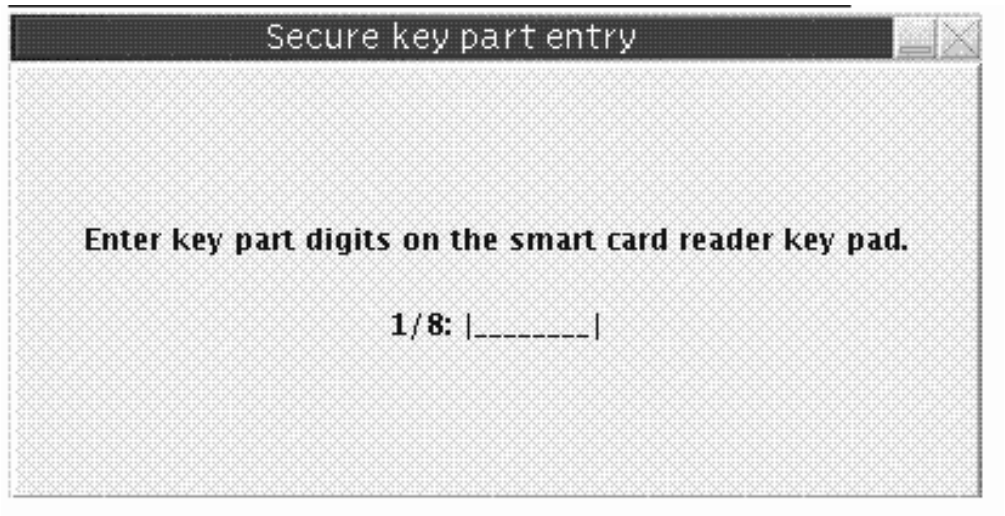


Figure 287. Secure key part entry -- enter key part digits

After all hexadecimal digits for the key part have been entered, a Smart Card key part information window opens showing the AES-VP for the key part that was entered.

Figure 288. Secure key part entry -- key part information window

Entering a key part on the smart card reader

A key part is hexadecimal. The PIN pad on the smart card reader does not provide hexadecimal digits, so you must enter two digits that represent the decimal equivalent of a hexadecimal digit. The valid range of decimal digit input is 00–15. This range is equivalent to the hexadecimal digit input range of 0–F. A conversion table is provided (Table 22 on page 312).

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 22. Decimal to Hexadecimal Conversion Table

Hexadecimal Digit	Decimal Digits Entered on PIN PAD
0	00
1	01
2	02
3	03
4	04
5	05
6	06
7	07
8	08
9	09
A	10
B	11
C	12
D	13
E	14
F	15

Appendix B. LPAR considerations

Host image profiles for logical partitions must be correctly configured in order to use the TKE workstation to manage keys and perform other operations. The host support element is used to set and change the configuration.

When customizing an image profile using the support element, four fields are specified:

- **Usage domain index** – The domain associated with the logical partition.
- **Control domain index** – The set of domains that can be managed from this logical partition. It must include the usage domain index value for this logical partition. A logical partition used as the TKE host includes the usage domain index values for all logical partitions the TKE workstation may manage.
- **Cryptographic Candidate List** – The set of cryptographic coprocessors that the logical partition may access.
- **Cryptographic Online List** – The set of cryptographic coprocessors that will be brought online when the logical partition is activated.

If a command is sent to a domain that is not in a logical partition's control domain index, ICSF returns an error (return code 12, reason code 2015).

There is no specific field to identify a logical partition as a TKE host when you are customizing image profiles. You must decide which logical partition will be the TKE host and set up the control domain index and Cryptographic Candidate List appropriately. The control domain index for this partition must include the usage domain index values for all logical partitions that the TKE workstation will control, and the Cryptographic Candidate List for this partition must include all entries in the Cryptographic Candidate Lists for the logical partitions that the TKE workstation will control. The control domain index must also include the usage domain index value for the TKE host partition itself.

Multiple logical partitions can specify the same usage domain index, provided there are no common entries on their Cryptographic Candidate Lists. (Logical partitions may not share the same domain on the same cryptographic coprocessor, but can use the same domain index value on different cryptographic coprocessors.) In order to control these partitions, however, the TKE host partition must have a unique usage domain index, because its Cryptographic Candidate List must include all coprocessors of the logical partitions being controlled.

The example in Figure 289 on page 314 has 3 LPARs and 4 cryptographic coprocessors: 00, 01, 02, 03. There is no domain sharing. In this case, all the cryptographic coprocessors can be specified in the Candidate List for each LPAR.

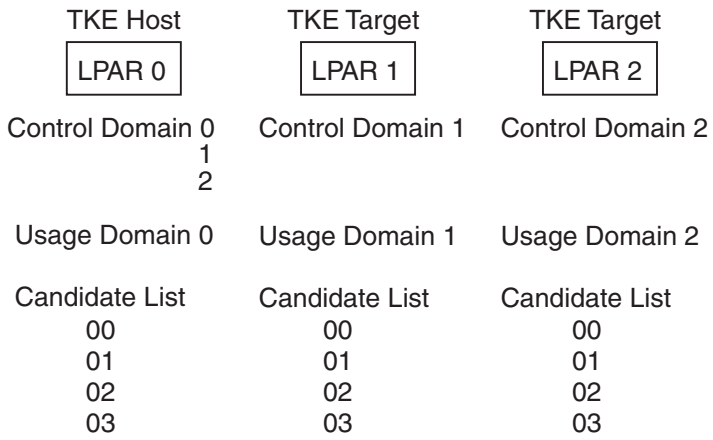


Figure 289. An example of TKE host and TKE target LPARs without domain sharing

The example in Figure 290 has 4 LPARs, 2 sharing the same domain and 4 cryptographic coprocessors: 00, 01, 02, 03. In this case, LPAR 1 and LPAR 2 share the same domain, but the Candidate List does not share any of the same cryptographic coprocessors.

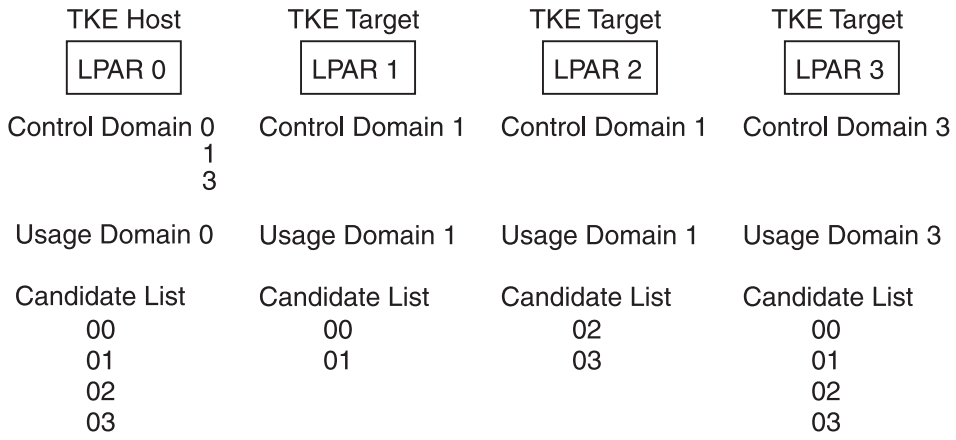


Figure 290. An example of TKE host and TKE target LPARs with domain sharing

If the same domain is specified by more than one LPAR and the Candidate List has any of the same cryptographic coprocessors, the first LPAR that is activated will IPL without error, but the other LPARs with the same domain will fail activation.

Appendix C. Trusted Key Entry - workstation crypto adapter initialization

Cryptographic Node Management Batch Initialization

The Cryptographic Node Management Batch Initialization task allows the user to execute user-created scripts.

User-defined scripts can be created using the CNI editor in the Cryptographic Node Management utility. Open the Cryptographic Node Management utility. Click **File** and select **CNI Editor**.

All scripts must be run from a USB flash memory drive or CNM data directory. User-created scripts can be used to further initialize the TKE workstation crypto adapter after passphrase or smart card initialization has been done. For details on initializing the TKE workstation crypto adapter for passphrase or smart card use, see “Initializing the TKE workstation crypto adapter for use with passphrase profiles” on page 77 and “Initializing the TKE workstation crypto adapter for use with smart card profiles” on page 77.

To execute a user-defined CNI script, click **Trusted Key Entry**, and then **Cryptographic Node Management Batch Initialization**. You must be logged onto the console as ADMIN to access this task. The Select CNI file to Run window opens. Select the location (USB flash memory drive or CNM data directory) and the file name of the CNI to execute. Click **Open**.

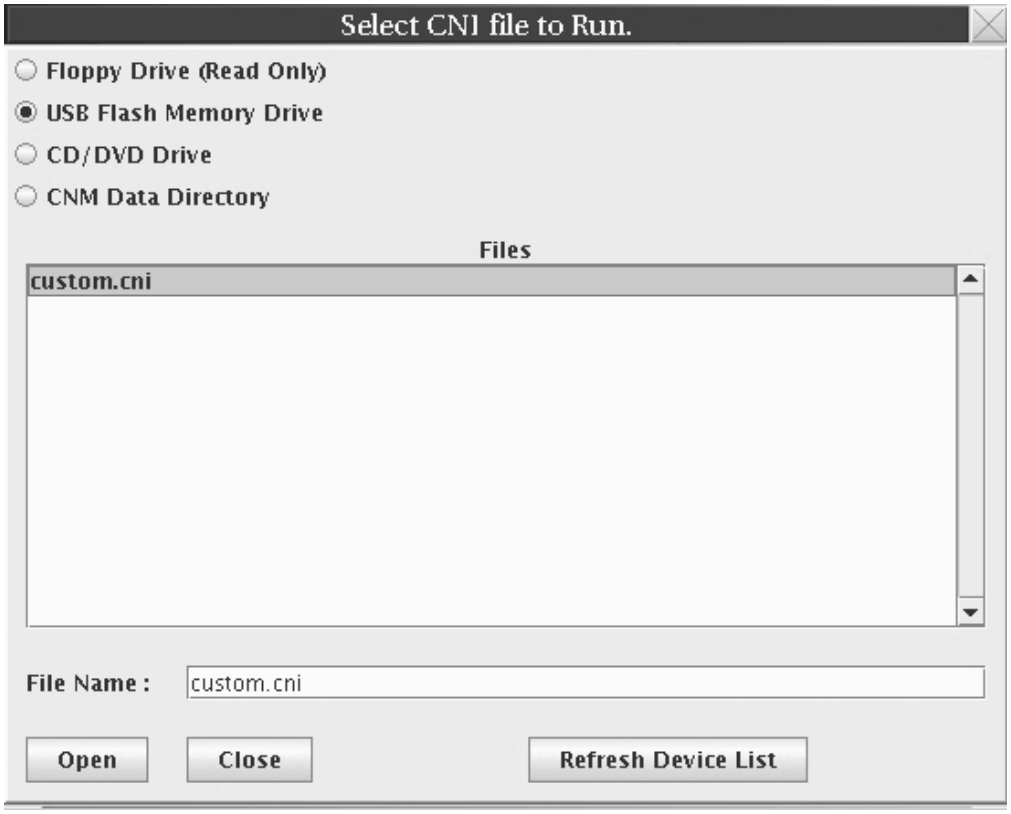


Figure 291. Cryptographic Node Management Batch Initialization task window

The output window shows the operations performed. Click **OK** to exit this task.

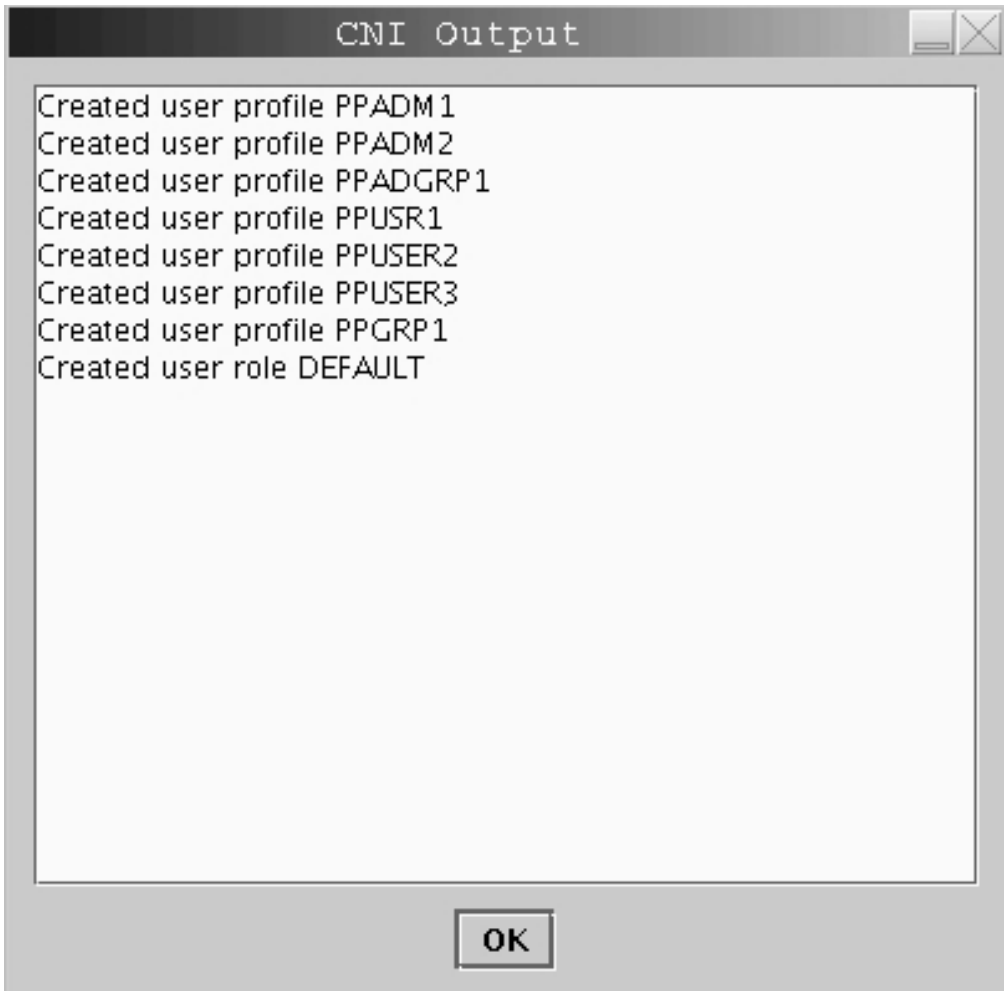


Figure 292. Cryptographic Node Management Batch Initialization task output window

CCA CLU (Code Load utility)

The CCA CLU task is used for loading and checking code on the TKE workstation crypto adapter.

CLU requires exclusive access to the TKE workstation crypto adapter. No other TKE applications can use the TKE crypto adapter while CLU is active, and no TKE crypto adapter user can be logged on. If TKE audit record upload is active at the time CLU is started, audit records are not uploaded to the host system until CLU is ended.

Note: CLU should be executed only when directed by IBM support. CLU functions can take several minutes to execute.

To invoke the CLU utility, click **Trusted Key Entry**, then select **CCA CLU**. You must be logged on as ADMIN to access this task.

CLU processing

When CLU is invoked, the Non-Factory Mode is displayed. You can select any combination of CLU command check boxes.

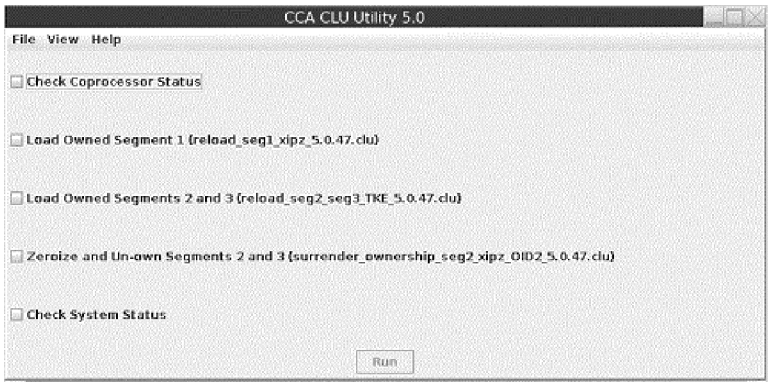


Figure 293. CLU command check boxes

When you click **RUN**, the commands execute in the order they appear on the application window.

If a command fails, the commands checked after the failing command do not execute and remain checked.

After clicking **Run**, view the Output Log or the Command History to check the output from the CLU commands. Both can be viewed by clicking **View** and then clicking **Output Log** or **Command History**.

Figure 294. CLU View menu

Figure 295. Output log file

The CLU output log file is available to the user in the CNM Data Directory.

Figure 296. CLU command history

If all CLU commands complete without error, a message indicating that all CLU commands completed successfully is displayed.

Figure 297. Successful completion of CLU commands

Checking coprocessor status

Before loading code you should check the coprocessor status. To use the CLU utility check status command (ST), you must select the **Check Coprocessor Status** check box and then click **Run**.

View the results in the Output Log or Command History.

Loading coprocessor code

IBM 4767 crypto adapters are supported.

1. Change segment 1:

a. If the segment 1 image name indicates ... Factory ..., set the application to Factory Mode (**File > Factory Mode**). The Factory Mode CLU window opens.

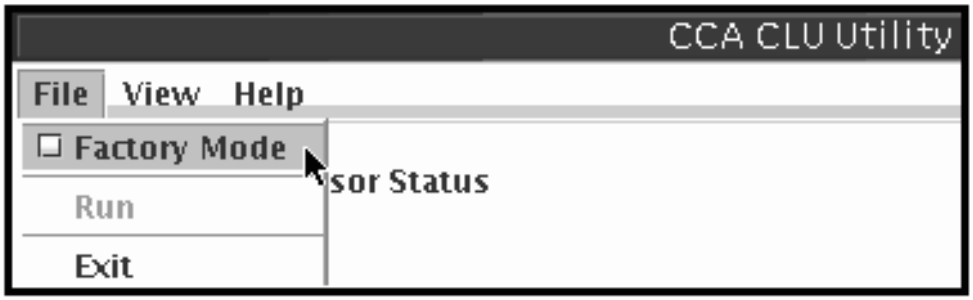


Figure 298. CLU File menu

Reload segment 1 with the CCA segment 1 file by selecting **Load Factory Segment 1** and clicking **Run**.

b. If the segment 1 image name does not indicate ... Factory ..., and the segment 1 revision level is less than 50000, reload segment 1 with the CCA segment 1.

Note: This choice is only available when the application is not in Factory Mode (**File > Factory Mode**).

2. Change segments 2 and 3:
   a. If segment 2 ROM status indicates Unowned... Set the application to Factory Mode (**File > Factory Mode**). Select **Load Factory Segments 2 and 3 (establish_ownership_then_emergency_reload_seg2_seg3_TKE_5.0.*xx*.clu)** and click **Run**.
   b. If segment 2 and 3 ROM status both indicate owner 02... Select **Load Owned Segments 2 and 3 (reload_seg2_seg3_TKE_5.0.*xx*.clu)** and click **Run**.

   Note: This choice is only available when the application is not in Factory Mode (**File > Factory Mode**).
3. When you have successfully completed this process, a check of the coprocessor status or validate of the coprocessor code indicates that the segments contain:

   Segment 1 Image: 5.0.*xx* P*xx*
   Segment 2 Image: 5.0.*xx* 1*xx*
   Segment 3 Image: 5.0.*xx* CCA TKE

   where the *xx* values are dependent on the maintenance level of the TKE. View the results in the Output Log or Command History.

Validating coprocessor code

If you want to validate the code loaded on the crypto adapter use the CLU utility validate command (VA). Select the appropriate check box for your TKE workstation crypto adapter and click **Run**.

View the results in the Output Log or Command History.

Checking system status

If you want to check the system status of your TKE workstation crypto adapter, use the CLU utility check system status command (SS). Select the **Check System Status** check box and click **Run**.

View the results in the Output Log or Command History.

Resetting coprocessor

If you need to reset the TKE workstation crypto adapter use the CLU utility reset coprocessor command (RS). You must enter Factory mode by clicking **Factory Mode** under the **File** menu. Then select the **Reset Coprocessor** check box and click **Run**.

View the results in the Output Log or Command History.

Removing coprocessor CCA code and zeroizing CCA

To Zeroize the CCA node and remove the CCA Coprocessor Code from segments 2 and 3, select the **Zeroize and Unown Segments 2 and 3** check box and click **Run**. This should result in the segment 2 and 3 ROM Status indicated Unowned.

View the results in the Output Log or Command History.

Help menu

The CLU Utility has a help page. To view the help, click **Contents** from the **Help** menu.

Appendix D. Clear RSA key format

An RSA key can be imported from a file holding the unencrypted RSA key. The file must be an ASCII text file. CR/LF can be inserted at any place for enhanced readability of the file.

The contents of the file are:

Description	Length (characters)
Key modulus length in bits (hex value)	4
Length of Modulus field in bytes (hex value)	4
Length of Public exponent field in bytes (hex value)	4
Length of Private exponent field in bytes (hex value)	4
Modulus (hex value)	-
Public exponent (hex value)	-
Private exponent (hex value)	-

The format follows the key_value_structure format defined for the PKA Key token Build (CSNDPKB) callable service.

These are examples of two file contents for the same clear RSA key. The key length is 512 bits and the public exponent is 65537.

Example 1:

```
0200
0080
0003
0080
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
80000000000000001AE28DA4606D885EB7E0340D6BAAC51991C0CD0EAE835AF
D9CFF3CD7E7EA74141DADD24A6331BEDF41A6626522CCF15767D167D01A16F97
010001
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0252BDAD4252BDAD425A8C6045D41AFAF746BEBD5F085D574FCD9C07F0B38C2C
45017C2A1AB919ED2551350A76606BFA6AF2F1609A00A0A48DD719A55E9CA801
```

Example 2:

```
0200004000030040
80000000000000001AE28DA4606D885EB7E0340D6BAAC51991C0CD0EAE835AF
D9CFF3CD7E7EA74141DADD24A6331BEDF41A6626522CCF15767D167D01A16F97
010001
0252BDAD4252BDAD425A8C6045D41AFAF746BEBD5F085D574FCD9C07F0B38C2C
45017C2A1AB919ED2551350A76606BFA6AF2F1609A00A0A48DD719A55E9CA801
```

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 10 for more information.

Table 23. Tasks, applications and utilities accessible by console user name

Navigation	Task	Privileged mode access ID - None	Privileged mode access ID - ADMIN	Privileged mode access ID - AUDITOR	Privileged mode access ID - SERVICE
Trusted Key Entry					
Applications	Begin Zone Remote Enroll Process for 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		
	Migrate IBM Host Crypto Module Public Configuration Data	X	X		
	Configuration Migration Tasks	X	X		
	TKE Workstation Setup		X		
	Migrate Roles Utility		X		X
	Smart Card Utility Program	X	X		
	TKE's IBM Crypto Adapter Initialization		X		
	Trusted Key Entry	X	X		
Utilities	Edit TKE Files	X	X		
	TKE File Management Utility	X	X	X	X
	TKE Workstation Code Information	X	X		
	Configure Displayed Hash Size		X		
	Configure Printers		X		
	TKE Audit Configuration Utility			X	
	TKE Audit Record Upload Utility			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

Table 23. Tasks, applications and utilities accessible by console user name (continued)

Navigation	Task	Privileged mode access ID - None	Privileged mode access ID - ADMIN	Privileged mode access ID - AUDITOR	Privileged mode access ID - SERVICE
	Users and Tasks	X	X	X	X
	View Console Information	X	X	X	X
	View Console Service History				X
	View Licenses	X	X	X	X
	Format Media	X	X	X	X
	Backup Critical Console Data		X		X
	Offload Virtual RETAIN® Data to Removable Media				X
	Rebuild Vital Product Data				X
	Save Upgrade Data		X		X
	Transmit Console Service Data				X
	Manage Print Screen Files	X	X	X	X
Console Logs	View Console Events	X	X	X	X
	View Console Tasks Performed			X	X
	Audit and Log Management	X	X	X	X
	View Security Logs			X	
	Archive Security Logs			X	
Console Internal Code	Analyze Console Internal Code				X
	Authorize Internal Code Changes				X
	Change Console Internal Code				X
Configuration	Configure 3270 Emulators	X	X	X	X
	Customize Console Date/Time		X		X
	Customize Network Settings		X		X
	Customize Scheduled Operations		X		X
	Reassign Hardware Management Console				X
	Change Password		X	X	X
	Certificate Management		X		X

Using USB flash memory drives with TKE applications and utilities

Trusted Key Entry applications and utilities tasks recognize a USB flash memory drive and allow you to use the drive (if applicable for the task) only if the IBM-supported drive meets these requirements:

- It is plugged into a USB port on the TKE.
- It is 1 GB or larger in size.
- It has been formatted with the appropriate data label and format type for the application or utility. For a list of supported format types and labels and the applications that use them, see Table 24 on page 352.

Otherwise, Trusted Key Entry Applications and Utilities tasks do not recognize the drive and you are not able to use it.

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

Begin zone remote enroll process

This task is for an IBM Crypto Adapter. It is for use on the Remote TKE to begin the zone enrollment process.

See “Remote crypto adapter enrollment” on page 296.

CCA CLU

This task is for loading code onto the TKE workstation crypto adapter.

See “CCA CLU (Code Load utility)” on page 317.

Complete zone remote enroll process

This task is for an IBM Crypto Adapter. It is for use on the Remote TKE to complete the zone enrollment process.

See “Remote crypto adapter enrollment” on page 296

Configure Displayed Hash Size

The Configure Displayed Hash Size utility allows you to set the maximum display length of hash values in TKE applications. The maximum display length can be set to 1 to 64 characters. Hash types that can be affected by this function are: MDC-4, SHA-1, SHA-256 and ENC-ZERO.

Figure 299. Configure Displayed Hash Size task window

To use the Configure Displayed Hash Size utility:

- Select the 'Truncate displayed hash characters' check-box if you want to enable the truncation of displayed hash data. To disable the truncation of displayed hash data, unselect the 'Truncate displayed hash characters' check-box.
- Enter the maximum number of hash characters to display (1-64) in the text field. This value must be an integer between 1 and 64.
- Click the Update button to save the changes entered on the panel.

Note: Hash data written to logs or files is only affected by the state of the Configure Displayed Hash Size settings at the time the data is output.

Configure Printers

This is the Common Unix Printing System (CUPS) configuration tool that is used to configure printers used by the TKE workstation.

Cryptographic Node Management batch initialization

This task is for using a batch interface to execute a user-created CNI file. A user-created CNI file can be used to initialize a TKE workstation crypto adapter differently than the TKE 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 11, "Cryptographic Node Management utility (CNM)," on page 237.

Edit TKE files

The Edit TKE Files task provides a way to edit and browse files on a USB flash memory drive or within the four allowed TKE-related data directories on the hard drive:

- TKE Data Directory
- Migration Backup Data Directory
- CNM Data Directory
- SCUP Data Directory

Files in the Configuration Data Directory cannot be accessed by the Edit TKE Files task and should be reviewed using the review functions in the configuration migration applications.

To open the Edit TKE Files task, click **Trusted Key Entry** and then click **Edit TKE Files**.

You must be logged on to the TKE workstation crypto adapter for this task. If you are not currently logged onto the adapter, a logon window is displayed. You will need to select a profile to log on to the adapter. If you are already logged onto the adapter, no logon window will be displayed (the current logon will be used).

In the Open Text Editor window, select a file from the displayed list or manually enter a file name. If you manually enter a file name that does not exist, a new file by that name will be created in the location specified.

If the crypto adapter profile currently being used is authorized to print files, the Print button is shown in the Open Text Editor window.

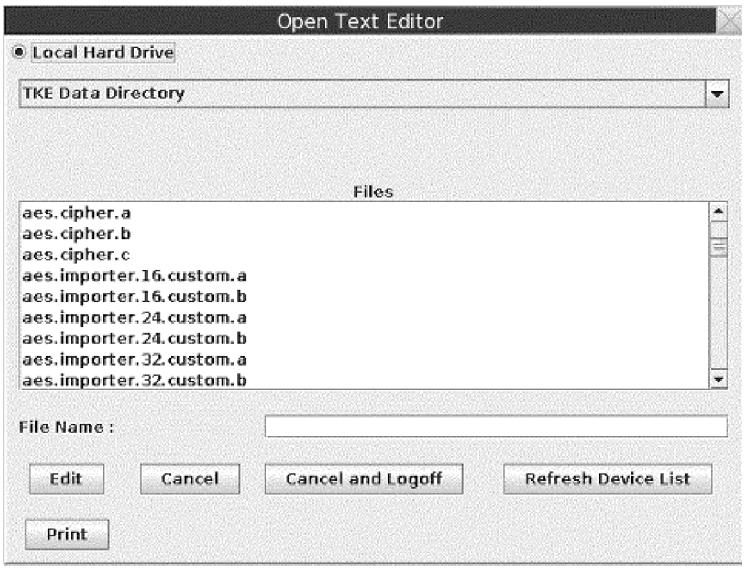


Figure 300. Edit TKE Files task window

You can edit the file within the edit text box and use File -> Save menu item to save the file.

Figure 301. Editor - File menu items

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

The editor provides options for Undo, Cut, Copy, Paste, along with Line Selection and Search/Replace.

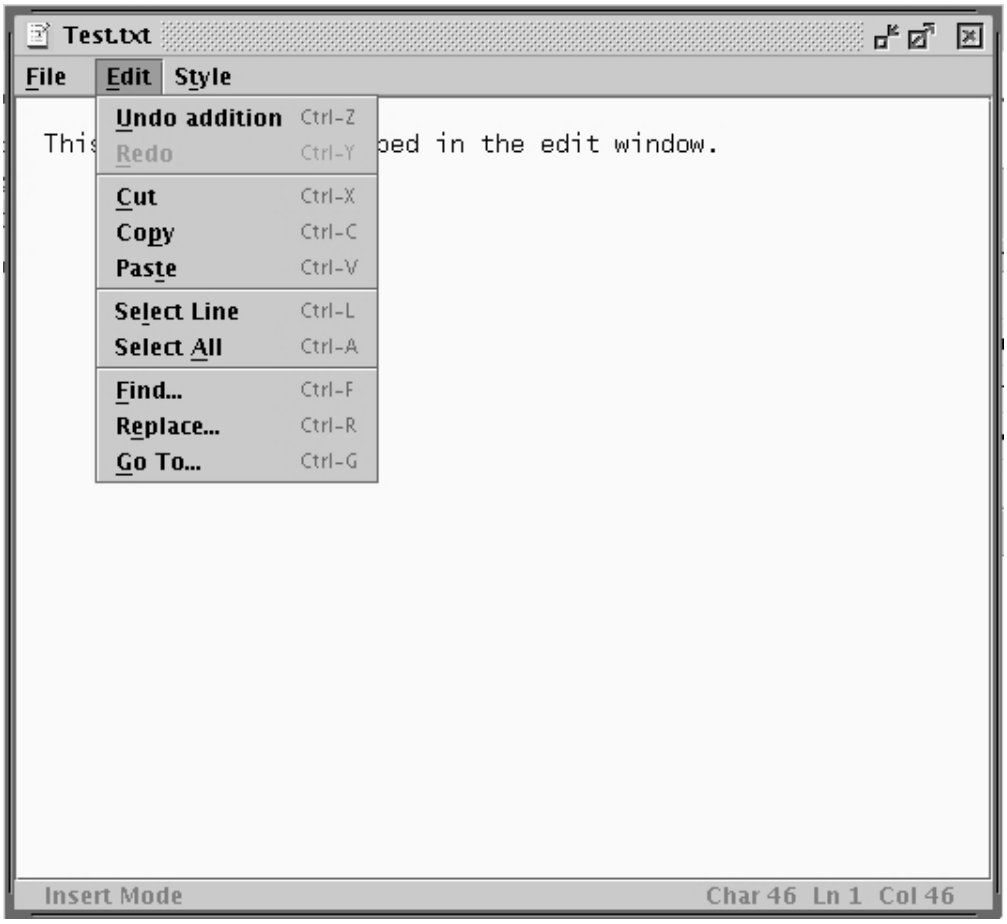


Figure 302. Editor - Edit menu items

In addition, there are options for Fonts, line wrap, and background.

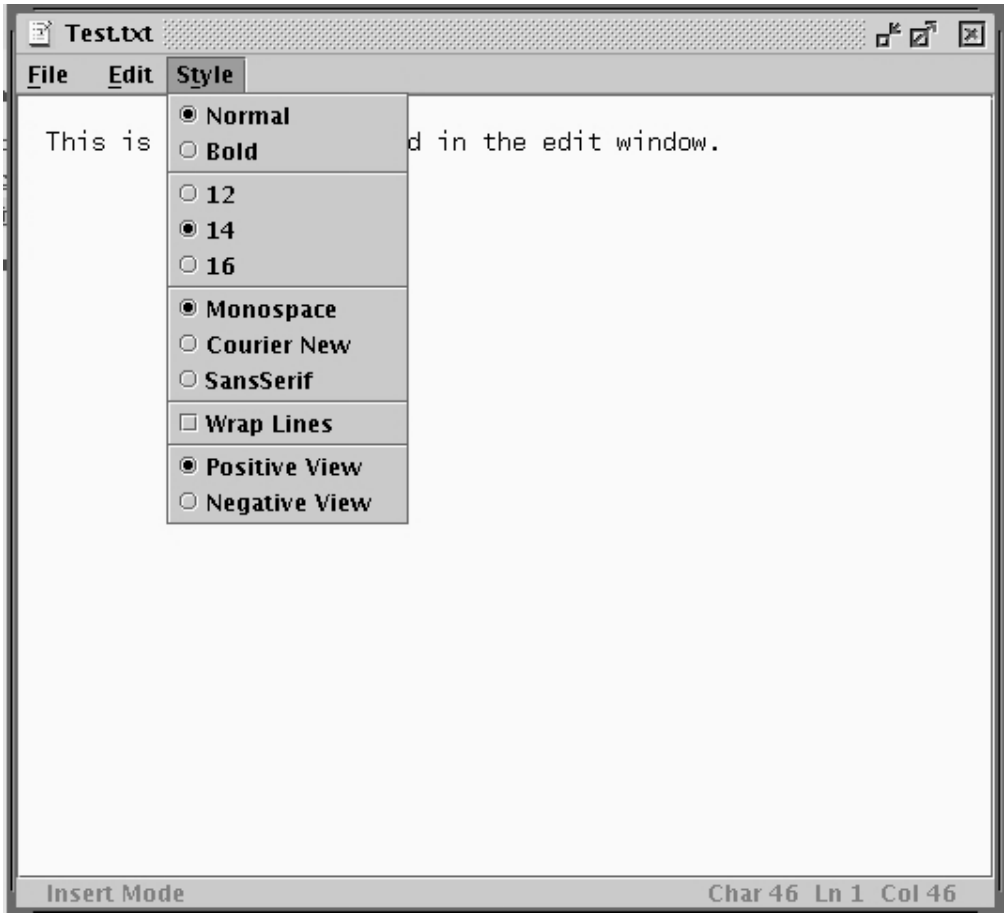


Figure 303. Editor - Style Menu Items

Migrate Roles utility

This utility, introduced in TKE 7.1, simplifies the process of adding new ACPs to existing roles on your TKE workstation crypto adapter. This is useful during migration, because new ACPs are not automatically added to existing roles during the migration process.

See “Adding new ACPs to existing roles using the Migrate Roles utility” on page 81 for more information.

Smart Card Utility Program

This task is used for initializing smart cards, enrolling smart cards in a zone, and enrolling TKE workstations in a zone.

See Chapter 12, “Smart Card Utility Program (SCUP),” on page 279.

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 215 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) data set. Each TKE security audit record is stored in the SMF dataset as a type 82 subtype 29 record. This allows you to place TKE security audit records from 1 or more TKE Workstations into a single SMF data set on a target host. From the host, a security officer can use SMF features to analyze and archive the TKE security audit data.

See “TKE Audit Record Upload Configuration utility” on page 223 for more information

TKE File Management utility

Attention: DVD-RAM is not supported on TKE 7.2 or later systems. If you have a DVD-RAM that is formatted for TKEDATA (TKEDATA DVD-RAM) and you want to use the files from the TKEDATA DVD-RAM on a TKE 7.2 or later system, see “Using files from a TKEDATA DVD-RAM on a TKE 7.2 or later system” on page 45 for additional information.

The TKE File Management Utility task allows you to manage files on a USB flash memory drive, or within supported data directories on the local hard drive. It provides the ability to delete, rename, and copy files.

To invoke this task, click on **Trusted Key Entry** and then click on the **TKE File Management Utility**.

You must be logged on to the TKE workstation crypto adapter for this task. If you are not currently logged on to the adapter, a logon window is displayed. You will need to select a profile to log on to the adapter. If you are already logged onto the adapter, no logon window will be displayed (the current logon will be used).

When the TKE File Management Utility is opened the user is presented with the following task window.

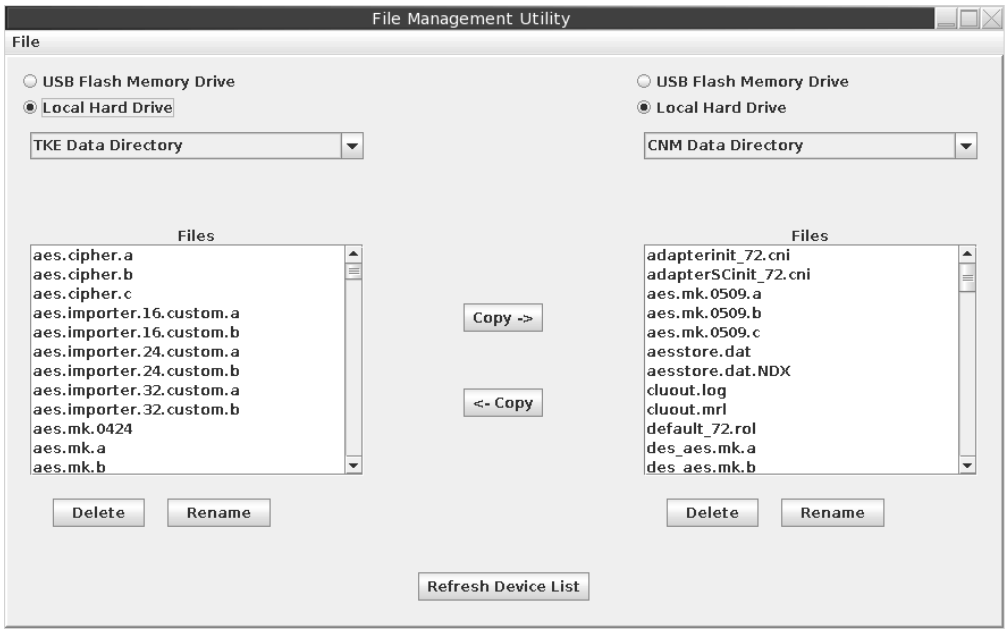


Figure 304. TKE File Management Utility task window

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

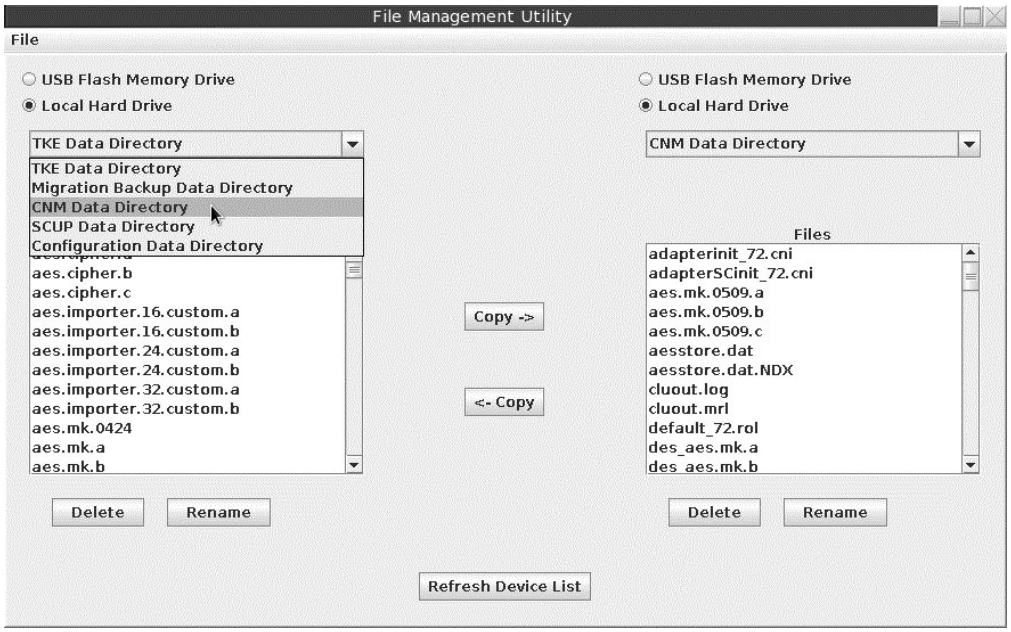


Figure 305. TKE File Management - directory options

From the displayed list you can select a single file, numerous files, blocks of files, or the entire display.

- For a single file, just click on the desired file.
- To select more than one file click on the first file, hold down the Ctrl key and click on each additional file.
- To select a block of files, click on the first file, hold down the Shift key and click on the last file. All files between the two selected files will be selected.
- To select all the files, hold down the Ctrl key and type an 'a'.

Clicking on **Delete** will display a confirmation window.

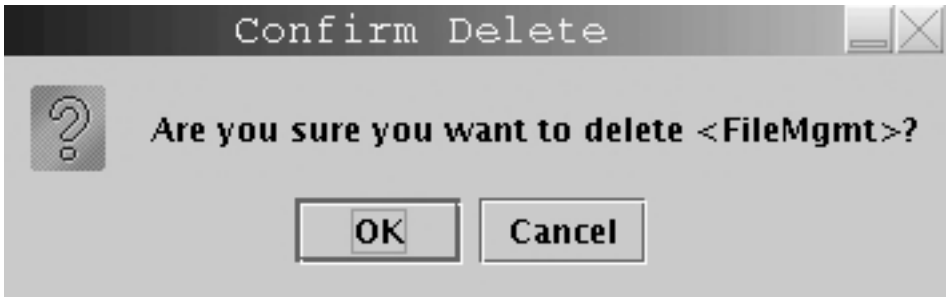


Figure 306. Delete confirmation window

Clicking on **Rename** will present a window for inputting a filename.

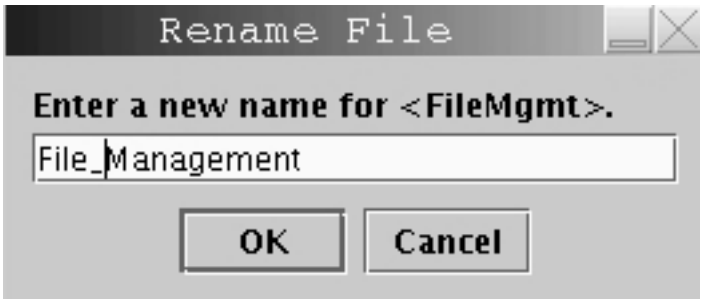


Figure 307. Window for inputting a filename

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

TKE workstation code information

The TKE Workstation Code Information window shows information about the code used by the TKE applications. The information can be useful in problem determination. Updates to TKE application code are reflected in this window. This task does not give information about the code on the TKE workstation crypto adapter.

To invoke this task, click **Trusted Key Entry** and then click **TKE Workstation Code Information**.

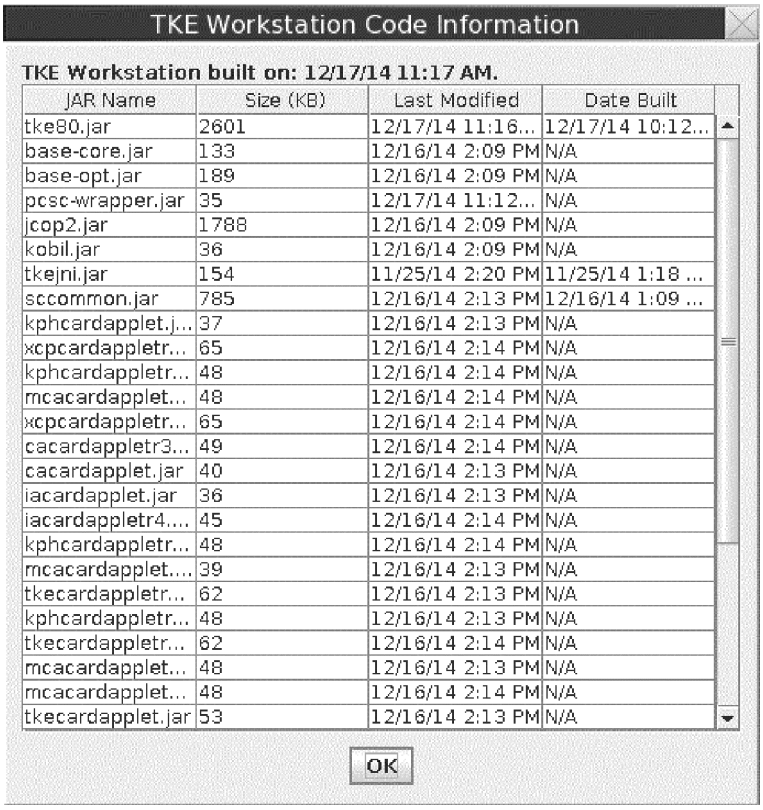


Figure 308. TKE Workstation Code Information window

Configuration migration

The TKE workstation provides tools to securely capture host crypto module configuration data to a file, and then apply this data to another host crypto module. Tools are provided for both CCA and EP11 host crypto modules. These tools simplify the task of installing new or replacement host crypto modules, and can be used for backup and disaster recovery.

For CCA crypto modules, two tools are provided:

- One tool migrates only public configuration data (roles, authorities, and domain control settings).
- One tool migrates all configuration data, including secret data such as master key values. The protocol for migrating secret data is more complex than the protocol for migrating only public data, and requires the participation of several smart card holders.

For EP11 crypto modules, only the tool that migrates all configuration data (including master keys) is supported.

To migrate only public configuration data, click **Migrate IBM Host Crypto Module Public Configuration Data** on the **Trusted Key Entry** menu. To migrate all configuration data, click **Configuration Migration Tasks** on the **Trusted Key Entry** menu.

Migrate IBM Host Crypto Module Public Configuration Data

Use this utility to save host crypto module configuration data (such as roles, authorities, and domain control settings) to a file on the TKE workstation, and to load a host crypto module with configuration data that was previously saved to a file. The utility simplifies the task of restoring the configuration when a host crypto module is replaced. This utility supports only CCA crypto modules and CCA domain groups.

The utility saves and loads only public configuration data. Private data, such as the value of master key registers, is not accessed.

The utility supports the following four tasks:

- Collecting configuration data from a host crypto module and saving it in a file.
- Applying previously saved configuration data to a host crypto module.
- Collecting configuration data from one host crypto module and applying it to a different host crypto module in one operation.
- Reviewing previously saved configuration information in a file.

The source and target can be either a single host crypto module or a domain group. When the source is a domain group, the crypto module containing the master domain of the group is located and used as the source crypto module. When the target is a domain group, all crypto modules with at least one domain in the domain group are updated with the configuration data read from a file.

To apply configuration data to a target host crypto module, you must use an authority that allows roles and authorities to be created on the target, such an authority with the predefined INITADM role. When the utility applies configuration data to a domain group, the current authority signature key is checked before each crypto module in the group is updated. If it does not have the required authority, you can load a different authority signature key.

The apply task creates and uses a temporary role and authority, which it removes when finished. In some cases, the temporary role cannot be removed. Because a temporary authority is used, 99 authorities are the most that can be migrated by the utility. If 100 authorities are defined in the source configuration, the authority at index 99 must be created on the target manually. A warning is displayed for these special cases.

Target crypto modules must support all cryptographic services of the source configuration. To ensure that this requirement is met, the utility checks that the CCA version on the target module is at a higher level than the source configuration. If it is not, migration is not allowed.

In the apply task, existing roles, authorities, and domain control settings on target crypto modules are removed and replaced with the configuration data from the file. Domains optionally can be zeroized before you apply configuration data. This action clears the master key registers. Only control domains can be zeroized. For more information about control domains, see Appendix B, “LPAR considerations,” on page 313.

Files that are used by the configuration migration utility are created in, and read from, the Configuration Data Directory. The TKE File Management utility can copy, rename, and delete files in this directory.

Note: The apply task reserves target host crypto modules for update. If a target host crypto module is already reserved for update by another application, the apply task fails with an error message. The other application must be closed before the apply task can be run. In abnormal situations, it might be necessary to take the following steps to force release of the target host crypto module:

1. Start the main TKE application.
2. Open a crypto module notebook for the reserved host crypto module.
3. Select **Release Crypto Module** from the **Function** menu of the crypto module notebook. This function forcibly releases the host crypto module from the application that was holding it and reserves it for the crypto module notebook.
4. Close the crypto module notebook to release the host crypto module.

Configuration migration tasks

This application provides access to utilities used to securely migrate configuration data, including secret data such as master key values, from one crypto module to another. This application can be used for both CCA crypto modules and EP11 crypto modules. When you select this application, the Configuration Migration Tasks panel is displayed.

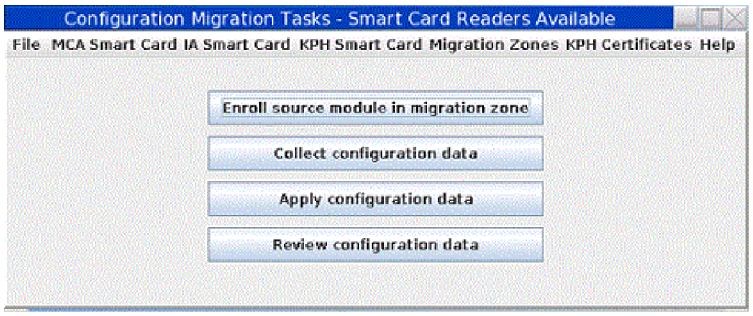


Figure 309. Configuration Migration Tasks panel

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 domain group.

The KPH smart card authorizes reconstruction of the transport key.

For CCA crypto modules, before configuration data can be collected from a source host crypto module, the source host crypto module must be enrolled in the migration zone using the **Enroll source module in migration zone** task. EP11 crypto modules do not need to be enrolled in the migration zone.

During the **Collect configuration data** task, the source host crypto module generates a transport key and splits it into "N" parts. (The key splitting algorithm allows the key to be recovered with only "M" of the original "N" parts. It does not matter which "M" parts are provided.) Each key part is encrypted using the public key from one of the "N" KPH smart cards. The source host crypto module captures the configuration data and encrypts it using the transport key. The encrypted configuration data and "N" encrypted key parts are returned.

During the **Apply configuration data** task, the target crypto module generates and returns a target decryption public key. It also returns an Outbound Authentication (OA) signature over the target decryption public key and the target host crypto module OA certificate chain.

"K" IA smart cards approve the target crypto module and target decryption public key, with help from the OA proxy (see “OA proxy” on page 341).

"M" KPH smart cards approve reconstructing the transport key, with help from the OA proxy (see “OA proxy” on page 341). KPH smart cards receive the transport key part that was encrypted with their public key, decrypt it using their private key, re-encrypt it using the target decryption public key, and return the result.

The target crypto module receives the encrypted configuration data and the "M" rewrapped key parts. It decrypts the rewrapped key parts using its private key, reconstructs the transport key, and decrypts and applies the configuration data.

The target of the apply task can be either a single crypto module or a domain group. When the target is a domain group, the configuration data is applied to each crypto module with at least one domain in the group.

Signature collection

CCA and EP11 crypto modules have different command authentication architectures. CCA is role-based. Commands are signed by authorities whose roles allow the action. EP11 uses a signature threshold approach, where all administrators have equal authority to issue commands but must be installed on the target domain or crypto module. Each target domain and crypto module independently specifies the number of administrator signatures that are required to issue commands (the *signature threshold*).

Because of the different architectures, signature collection for configuration migration commands is different. For CCA, the role of the current authority is

checked before each command is issued. You can load a different signature key if the authority is not authorized to issue the command.

For EP11, for each required signature you are prompted to insert a smart card with an administrator signature key in smart card reader 1. If that signature key does not match one of the installed administrators on the target crypto module or domain, you are prompted to insert a different smart card. This prompting continues until a valid signature key is found or until you cancel.

For EP11, you can bypass the prompting for each signature by predefining smart card readers as a source for signatures. After a smart card is inserted in the reader and the PIN is entered, signatures are collected automatically as needed, without further prompting. You can predefine signature key sources by using the **Manage EP11 Signature Keys** option on the **Function** menu.

Window actions

Function menu
This menu includes options to exit the Configuration Migration Tasks application, and to predefine smart card readers as the source of signatures for commands to EP11 crypto modules.

MCA Smart Card menu
This menu includes options to display the contents of an MCA smart card, initialize and personalize an MCA smart card, back up an MCA smart card, or change the PIN on an MCA smart card.

IA Smart Card menu
This menu includes options to display the contents of an IA smart card, initialize and enroll an IA smart card in a migration zone, personalize an IA smart card (set the PIN and description), unblock an IA smart card, or change the PIN on an IA smart card.

KPH Smart Card menu
This menu includes options to display the contents of a KPH smart card, initialize and enroll a KPH smart card in a migration zone, personalize a KPH smart card (set the PIN and description), unblock a KPH smart card, or change the PIN on a KPH smart card.

Migration Zones menu
Use the **Work with migration zones** function on this menu to display the list of migration zones that are known to the TKE workstation, and add or delete entries.

To minimize the number of times an MCA smart card must be inserted in a card reader during migration tasks, the TKE workstation maintains a list of known migration zones. The list is updated automatically when a new MCA smart card is created. If you must add or remove migration zones from this list, you can use this function. To add a migration zone to the list, you must insert the MCA smart card for the zone in the smart card reader and enter the PINs.

KPH Certificates menu
Use the **Work with KPH certificates** function on this menu to display the list of KPH smart cards that are known to the TKE workstation, and add or delete entries.

To minimize the number of times KPH smart cards must be inserted in a card reader during migration tasks, the TKE workstation maintains a list of known KPH certificates. The list is updated automatically when a new

KPH smart card is created. If you must add or remove a KPH certificate from this list, you can use this function. To add a KPH certificate to the list, you must insert the KPH smart card in the smart card reader.

Enroll source module in migration zone
This option starts a wizard that takes you through the steps to enroll a source host crypto module in a migration zone. The source crypto module must be enrolled in a migration zone before configuration data can be collected from it. This action is needed only for CCA crypto modules.

You need to know what migration zone you will use before you run this wizard. If you must define a new migration zone, you can use the **MCA Smart Card** menu to create a new MCA smart card. If you define a new migration zone, you also must create IA and KPH smart cards to use in the zone.

To run this wizard, you must load a signature key that permits the Certificate Insert operation on the source crypto module. If the signature key has insufficient authority, you can load a different signature key.

Collect configuration data
This option starts a wizard that takes you through the steps to collect configuration data from a source host crypto module and save it in a file. Before you run this wizard on a CCA host crypto module, you must enroll the host crypto module in the migration zone.

You must know what migration zone and what KPH smart cards you will use before you run this wizard. Only KPH smart cards for the selected migration zone can be used.

In this wizard, you indicate the set of domains that you want to collect configuration data from. Configuration data for only those domains is saved in the configuration data file. During the apply task, configuration data for domains that are not saved in the configuration data file is set to the default value.

To run this wizard on a CCA crypto module, you must load a signature key that permits the Crypto Data Extract operation on the source host crypto module. If the signature key has insufficient authority, you can load a different signature key.

Apply configuration data
This option starts a wizard that takes you through the steps to apply configuration data to a target host crypto module or target domain group.

The wizard prompts you to insert IA smart cards in the smart card reader and enter the PIN. The "K" policy for the migration zone specifies the required number of IA smart cards.

The wizard prompts you to insert KPH smart cards in the smart card reader and enter the PIN. "M" of the "M-of-N" policy for the migration zone is the required number of KPH smart cards.

To run this wizard on a CCA crypto module, you must load a signature key that permits the Target Prepare and Crypto Target Inject operations on the target host crypto module or target group. If the signature key has insufficient authority, you can load a different signature key. The default role and authority that is created when a host crypto module is initialized allow you to run these operations.

Review Configuration Data

This option starts a wizard that displays the non-secret contents of a configuration data file that you select.

Different data is saved in the configuration data file for CCA and EP11 host crypto modules. For both crypto module types, the saved data includes the serial number and code level of the source crypto module, the date and time that the configuration data was collected, the migration zone and KPH certificates used, and what domains were collected. For CCA it includes a list of the roles and authorities collected, the domain controls for collected domains, and key register status and key hashes for collected domains. For EP11 it includes the crypto module administrators and attributes, and the domain administrators, attributes, control points, and key status and hash values for collected domains.

Instructions for migrating key material

If you want to migrate configuration data that includes master key values, follow these steps:

1. Decide what migration zone you are using. If you are not using an existing migration zone, create an MCA smart card that defines the new zone. You must define the M-of-N and K policies. "N" is the number of parts the transport key is split into and must be 1 - 10. "M" is the number of key parts that are required to reconstruct the transport key and must be between 1 and "N". "K" is the number of Injection Authorities that are required to approve applying configuration data on the target host crypto module and must be 1 - 10.

   Guideline: Create a backup whenever you create a new MCA smart card.
2. Use the **Migration Zones** menu to check that the migration zone you want to use is listed. If it is not listed, add it.
3. If you are using a new migration zone, create IA and KPH smart cards. You must create at least "K" IA smart cards and "N" KPH smart cards for the migration zone, but you can create more.
4. Decide what KPH smart cards you are using. Use the **KPH Certificates** menu to check that the KPH smart cards you want to use are listed. If they are not listed, add them.
5. Run the “Enroll source module in migration zone” wizard to enroll the source host crypto module in the migration zone. This step is needed only for CCA crypto modules.
6. Run the “Collect configuration data” wizard to collect configuration data on the source host crypto module. The wizard prompts you to enter the media type and a file name for storing the encrypted configuration data.
7. Run the “Apply configuration data” wizard to apply configuration data on the target host crypto module. As the wizard runs, the IA and KPH smart card holders are prompted to insert their smart cards in a smart card reader and enter their PINs.

OA proxy

When migrating configuration data from one host crypto module to another, the Injection Authority (IA) and Key Part Holder (KPH) smart cards verify outputs from the source and target host crypto modules. These outputs are signed by the host crypto modules' private keys, as part of a process called Outbound Authentication. In addition to the OA signature, the source and target host crypto modules provide their OA certificate chain, which terminates in an IBM root certificate.

Some IBM host crypto modules use key sizes for their OA signatures and certificate chains that are larger than what is supported by currently available smart cards. To handle these host crypto modules, the TKE workstation crypto adapter acts as an OA proxy for the smart cards. The TKE workstation crypto adapter verifies the OA signature and certificate chain and signs the output data using a specially-generated OA proxy signing key.

Each migration zone on the workstation needs to create an OA proxy certificate for this OA proxy signing key. The OA proxy certificate is created automatically when Migration Certificate Authority (MCA) smart cards are created, and when the migration zone is added or updated using the **Migration Zones** pull-down menu on the **Configuration Migration Tasks** panel.

If the TKE workstation crypto adapter is replaced or re-initialized, these OA proxy certificates are no longer valid. The migration zones listed under the **Migration Zones** pull-down menu will be removed automatically and must be re-registered using the MCA smart cards. Users who wish to change the OA proxy signing key can do so by manually deleting all migration zones found using the **Migration Zones** pull-down menu and then re-adding them.

Smart card applet level for configuration migration

Beginning with the CEX5C and CEX5P host crypto modules, OA signatures are based on ECC keys rather than RSA keys. In order to migrate configuration data to these host crypto modules, IA and KPH smart cards supporting ECC signatures must be used.

IA and KPH smart cards with these expanded capabilities can be created starting with TKE 8.0. IA and KPH smart cards created on previous versions of TKE cannot be used to apply configuration data to host crypto modules that use ECC keys for outbound authentication. The expanded capabilities are present on IA and KPH smart cards with applet version 0.3 or greater.

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 366
- "Rebuild vital product data" on page 356

The following tasks are displayed if you are logged in as **Auditor**:

- "Archive security logs" on page 343
- "View security logs" on page 370

The following tasks are displayed for multiple user names:

- "Audit and log management" on page 354

- "Backup critical console data"
- "Change password" on page 345
- "Configure 3270 emulators" on page 85
- "Customize console date/time" on page 74
- "Customize network settings" on page 70
- "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 364
- "View console tasks performed" on page 368
- "View licenses" on page 368

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 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 223 for more information.

Authorize internal code changes

This task is used to verify or change the setting that allows using this TKE workstation to perform installation and activation of internal code changes and other subsequent operations. This task should only be invoked by your IBM Customer Engineer or when directed by IBM Product Engineering. You must log on with a console name of SERVICE to use this task.

For details, refer to *System z Service Guide for Trusted Key Entry Workstations*, GC28-6901.

Backup critical console data

This task performs the same function as the Customize Scheduled Operations for Backup Critical Hard Disk Information. Rather than executing it as a scheduled operation, this task will execute the backup immediately. The backup critical

console data operation copies critical files from the Trusted Key Entry workstation to the Backup DVD-RAM or USB flash memory drive.

To invoke this task, log on as either ADMIN or SERVICE, click on Service Management and then click on Backup Critical Console Data.

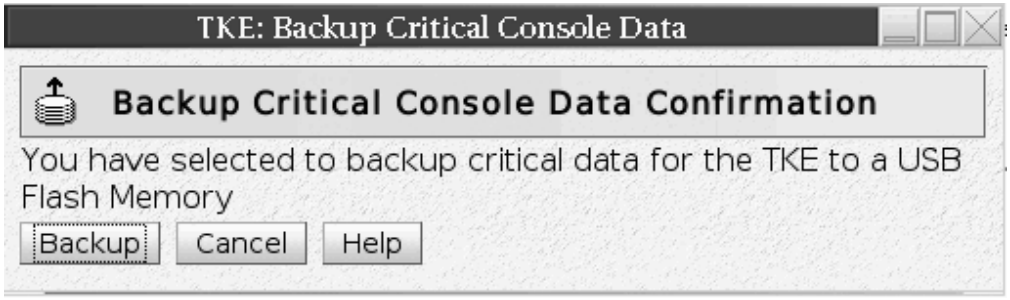


Figure 310. Backup Critical Console Data window

The DVD-RAM or USB flash memory drive for the Backup Critical Console Data task must be formatted with a volume identification of ACTBKP, using the Format Media task.

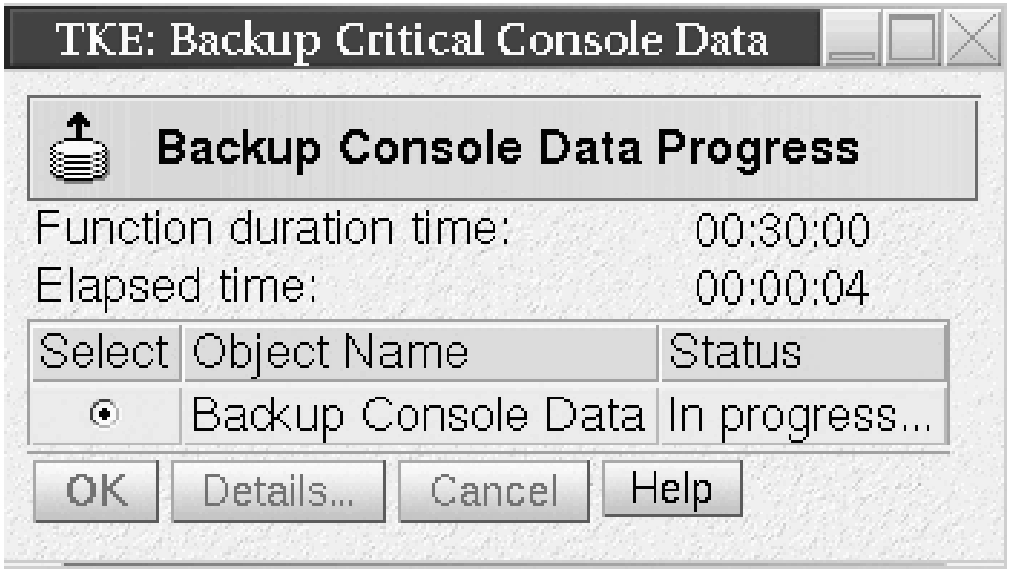


Figure 311. Backup Console Data Progress window - in progress

When the operation is complete the Status field of the Backup Critical Console Data window will be updated to indicate Success.

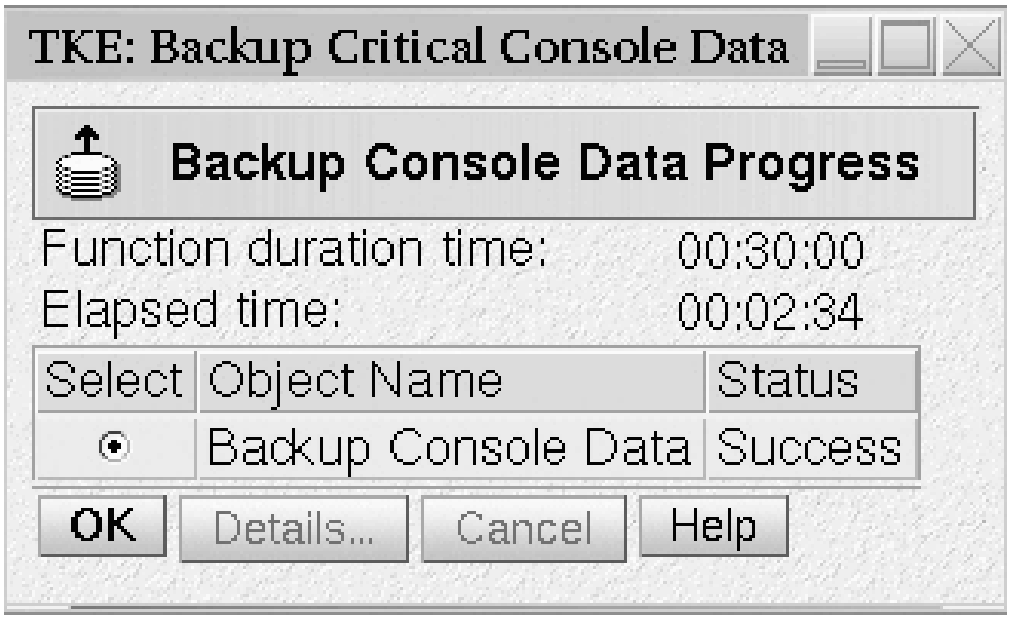


Figure 312. Backup Console Data Progress window - success

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**.

If you are logged on as ADMIN, you can change the ADMIN, AUDITOR, and SERVICE passwords. If you are logged on as AUDITOR or SERVICE, you can change only your own password.

When the task is executed, the user is required to enter the current password and then the new password twice. When done successfully, and if the new password conforms to the password rules, the task ends.

Note: When the TKE workstation is migrated to a new version, the password values are preserved. They do not revert to the default values.

Password requirements

Password requirements for the user's password are as follows:

- Password must be between 4 and 8 characters.
- The password may be alphanumeric but may not contain any special characters.

No other restrictions, such as password history rules or repeating characters, apply.

Customize scheduled operations

Use this task to customize a schedule for backing up critical hard disk information to USB flash memory drive. You must log on with a console user name of SERVICE or ADMIN to use this task.

It is important to back up critical console data regularly so that the latest system changes and updates are available for recovery situations.

Note: The USB flash memory drive that is used for the backup must be formatted with the label ACTBKP. See "Format media" on page 351 for details.

Figure 313. Customize Scheduled Operations task window

The backup USB flash memory drive is intended for use only during a hard disk restore operation, which completely replaces the contents of the hard disk drive. The hard disk restore operation loads the system image from the installation DVD (shipped with your TKE workstation) and then restores the data from the backup USB flash memory drive.

The backup USB flash memory drive includes any microcode fixes (MCFs) and microcode loads (MCLs) that were applied to the system. Also included is TKE-related data. After the restore/reload operation the system is back to the service level and TKE level of the last backup.

Scheduled operations are helpful for situations where automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance. A schedule can be set for one operation or repeated many times.

To open this task, click **Service Management** and then click **Customize Scheduled Operations**.

The Customize Scheduled Operations window opens.

Click **Options** on the menu bar to select:

New
To create a new scheduled operation

Delete
To remove a scheduled operation

Refresh
To update the current list of scheduled operations

Select All
To choose all scheduled operations that are currently displayed

Deselect All
To clear all scheduled operations that were currently selected

Exit
To exit this task

When **New** is selected from the **Options** menu, the Add a Scheduled Operation window opens.

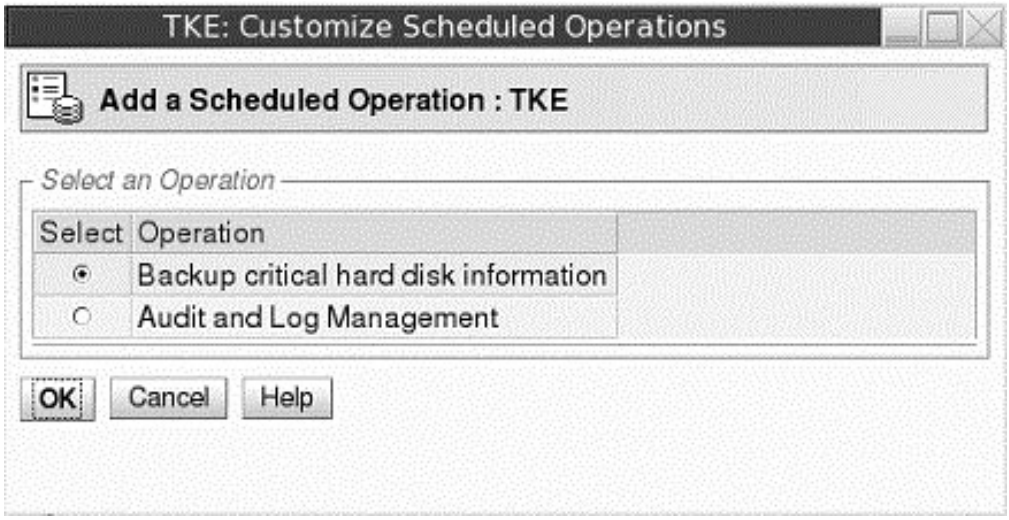


Figure 314. Customize Scheduled Operations - Add a Scheduled Operation window

Clicking **OK** opens a window in which the time, date, and repetition rate of the operation can be specified.

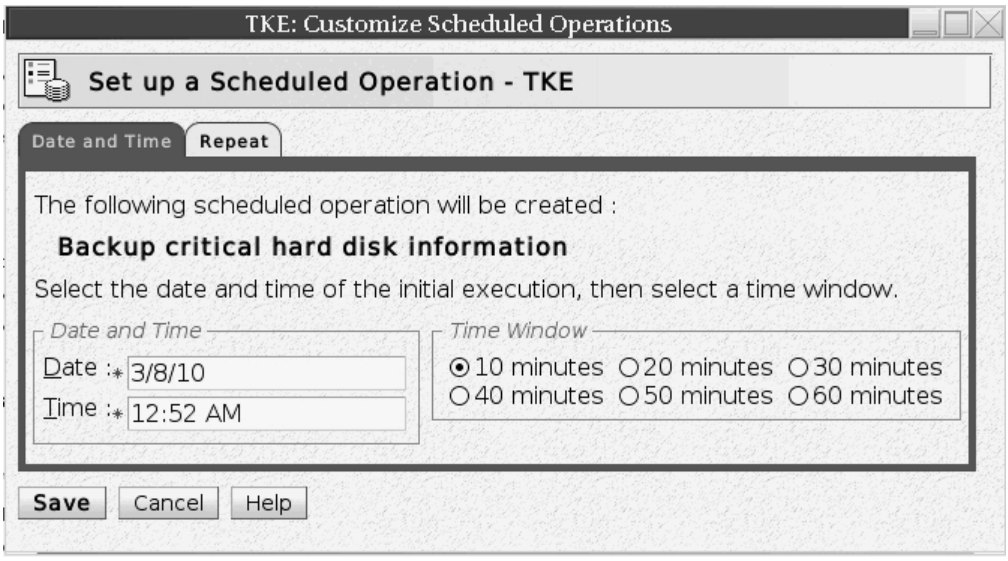


Figure 315. Customize Scheduled Operations - Set Date and Time window

Enter the date and time for a scheduled operation in the **Date and Time** area. The **Time Window** area defines the time frame in which the scheduled operation must start.

After you specify the date, time, and time window, click the **Repeat** tab.

Select whether the operation is a single occurrence or repeats. Select the days of the week you want to perform the operation. The **Interval** field specifies the number of weeks to elapse before the scheduled operation is performed again. The **Repetitions** field specifies the number of times you want the scheduled operations to be performed.

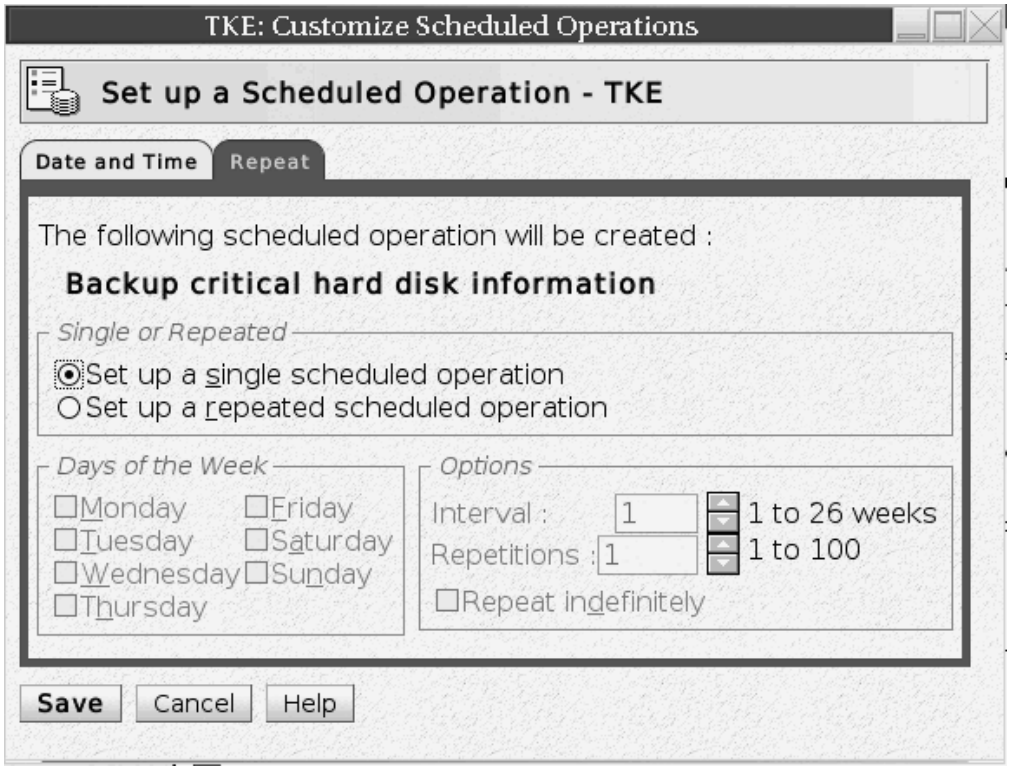


Figure 316. Customize Scheduled Operations - Set repetition of operation

After all the information is selected, click **Save** to complete the scheduling of the operation.

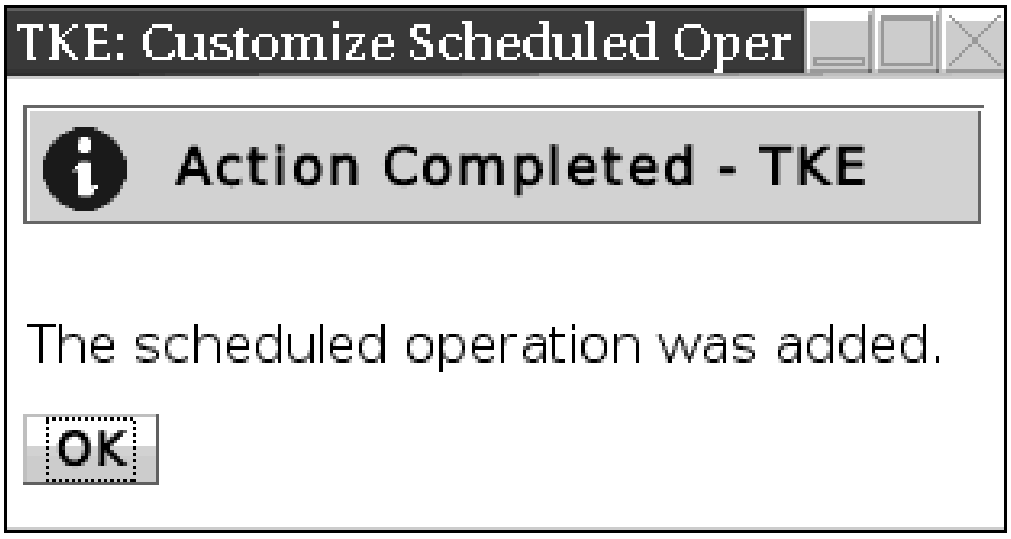


Figure 317. Completion window for Adding Scheduled Operation

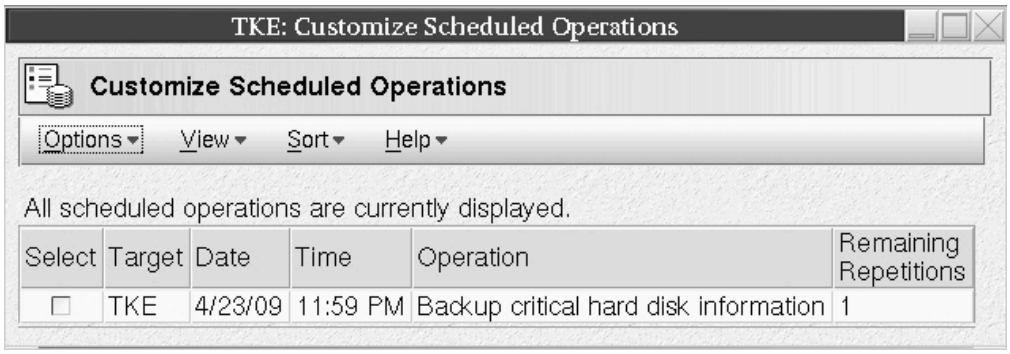


Figure 318. Customize Scheduled Operations

Click **Sort** on the menu bar to specify how you want to view the list of scheduled operations: by date and time, by object, or by operation. The **Date and time** option sorts the list according to date in descending order with the most recent operation at the top. The **By Object** and **By Operation** options have no meaning for TKE. The only object is TKE and the only operation is Backup Critical Console Data.

Click **View** on the menu bar to select:

`Schedule Details`
Used to display schedule information for the selected scheduled operation. For TKE, Object and Operation are not relevant.

`New Time Range`
Used to specify a definite time range (days, weeks, months, or displayed scheduled operations) for the selected operation.

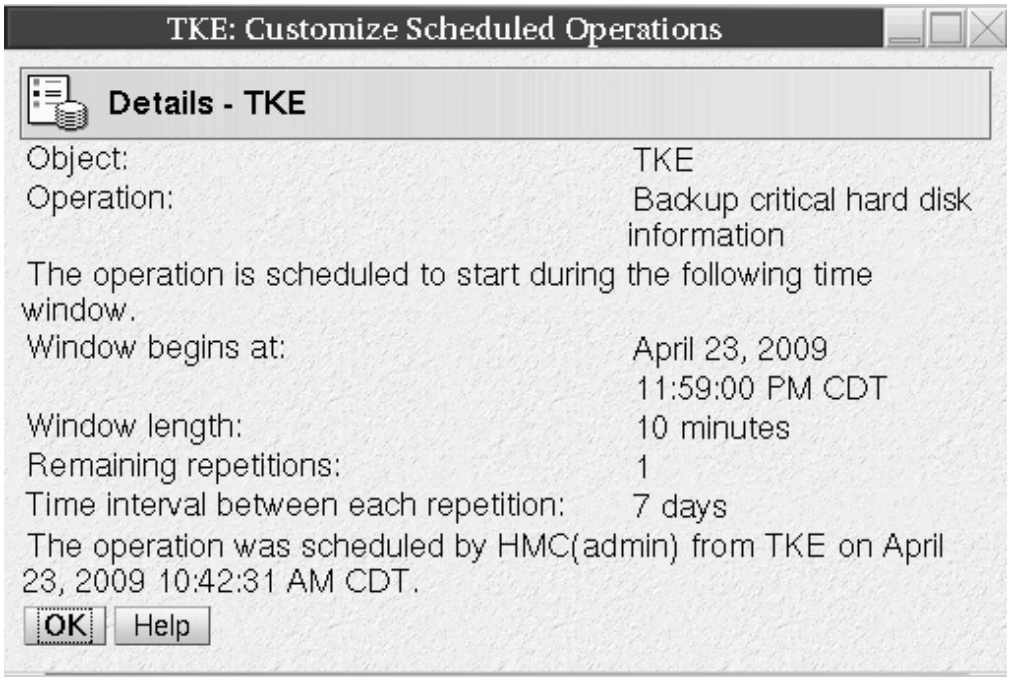


Figure 319. Details view of scheduled operation

Figure 320. New time range window for scheduled operation

Format media

The Format Media task is used to format USB flash memory drives.

1. To invoke this task, click on **Service Management** and then click on **Format Media**.

   The Format Media dialog is displayed.

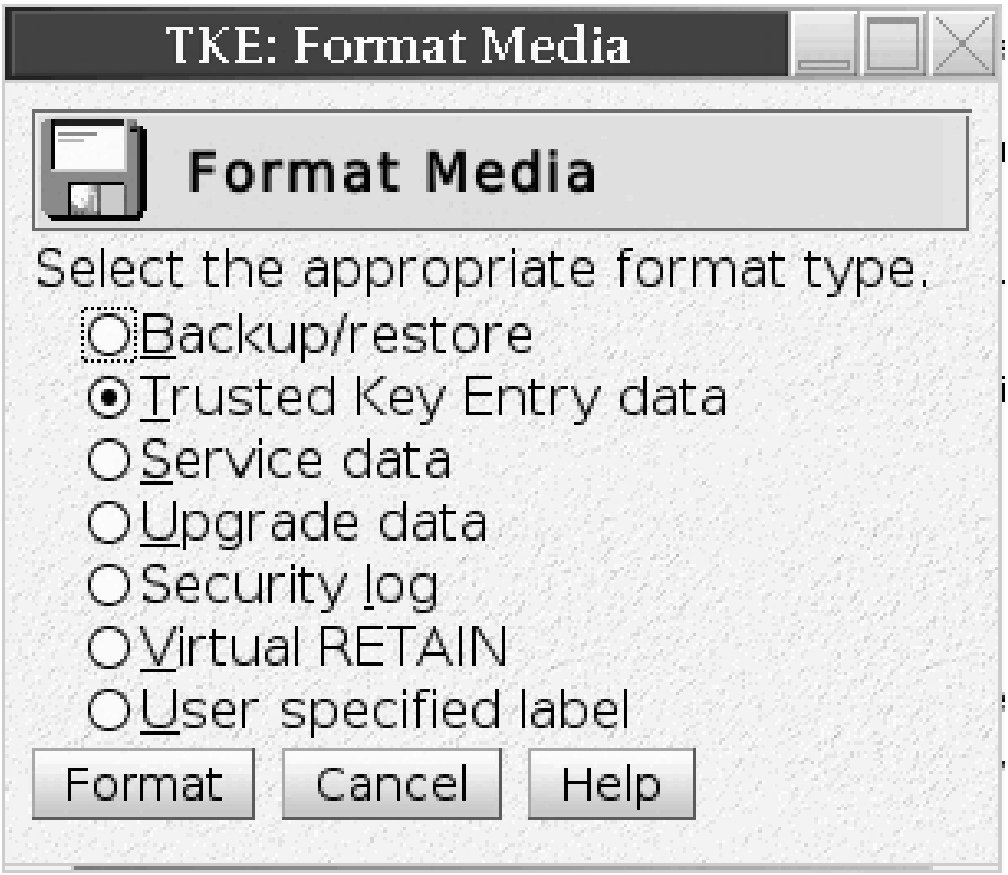


Figure 321. Format Media dialog

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 24. Allowable labels when formatting USB flash memory

Format	Label	Description:
Backup/restore	ACTBKP	This formatted media is used in the Backup Critical Console Data task and the Customize Scheduled Operations task. To choose this format type, select Backup/restore.
Trusted Key Entry data	TKEDATA	This formatted media is used in the TKE applications and tasks. TKE data can be related to TKE, SCUP, CNM, the Migration utility, or user defined. To choose this format type, select Trusted Key Entry data.
Service data	SRVDAT	This formatted media is used in the Transmit Console Service Data task. To choose this format type, select Service data.

Table 24. Allowable labels when formatting USB flash memory (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 Removable Media task. To choose this format type, select Virtual RETAIN.
User-specified label		

3. In the Format Media dialog, click the **Format** push button. If you selected "User specified label", a dialog will prompt you for a label name. Type in the name, and click the **Format** push button.

   The Select Media Device dialog is displayed.

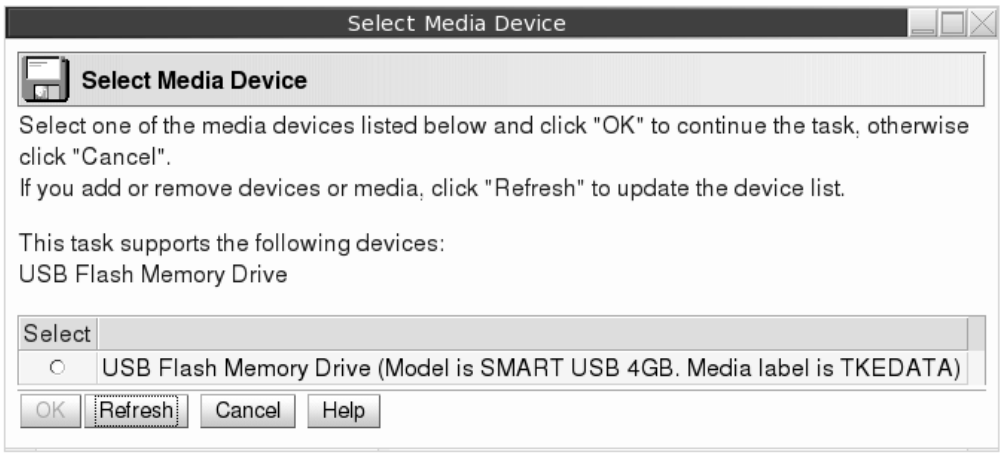


Figure 322. Select Media Device

4. In the Select Media Device dialog, select the radio button for the desired device, and click the **OK** push button.

   A confirmation dialog displays a warning that the format media action will remove all data on the removable media selected.

5. If you wish to continue the format media action, click the confirmation dialog's **Yes** push button.

   An informational window will display when the Format Media action has completed.

Audit and log management

This task copies the TKE console's default security log to an ASCII format file on a USB flash memory drive. The default security log on the TKE console is not changed. You must logon with a console user name of AUDITOR to use this task. See “Audit and log management” on page 220 for more information.

Hardware messages

This task displays messages about hardware activity on the Trusted Key Entry workstation.

When the green 'Status OK' icon (lower left corner of the TKE Console), changes to the blue 'Status Messages' icon it indicates that a Hardware Message is pending. The message can be viewed by clicking on the Status icon or by invoking this task.

To invoke the Hardware Messages task, click on Service Management and then click on Hardware Messages.

Messages are listed from the oldest to the newest message, with the oldest message displayed at the top of the list.

Date
Displays the date the message was sent.

Time
Displays the time the message was sent.

Message Text
Displays the message.

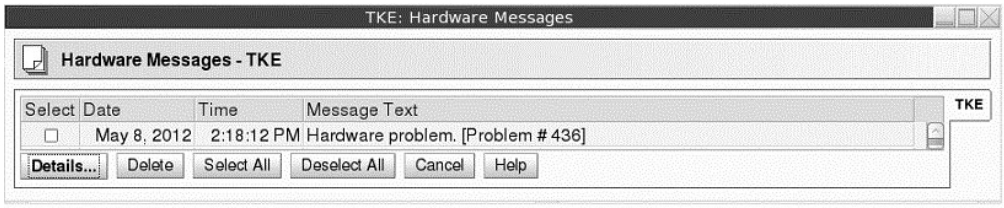


Figure 323. Hardware Messages window

Hardware messages notify you of events that involve or affect the TKE workstation hardware or internal code.

To promptly view, act on, or delete messages:

1. Select a message, then click Details to display details.

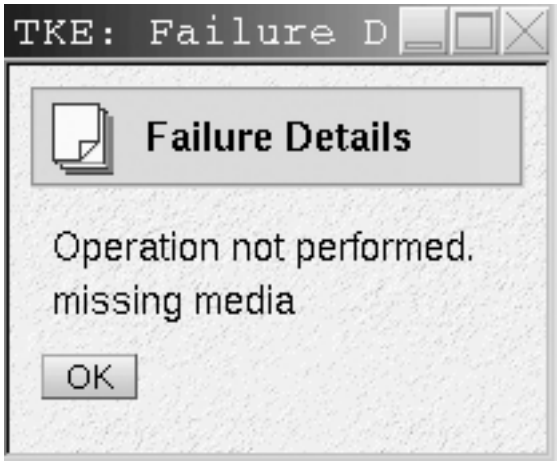


Figure 324. Hardware Messages - details window

2. If messages details are available and intervention is required, perform the action recommended in the details.
3. To delete the selected message, click Delete.

A message is displayed until an action causes it to be deleted.

Some messages are deleted automatically after the message or its details are displayed, if available. These messages generally provide information only, and are deleted automatically because no further action is required.

Messages that require further action provide message details that include a recommended action. The message and its details remain available until it is deleted manually. This allows reviewing the message details to assist intervention. But the message must be deleted when its information is no longer required.

Deleting messages provides greater assurance that new messages will be displayed as they are received.

Lock console

This task is used to allow customers to lock the TKE console. The Lock Console task appears in the Service Management tree when you are logged in as ADMIN, SERVICE, AUDITOR, or TKEUSER.

To invoke this task, click on Service Management and then click on Lock Console.

This task prompts the user for a password in order to lock the TKE console. Passwords can be up to any 12 characters except a space, backspace (\), *, and -. If any of these characters are entered you will receive an error message.

Figure 325. Prompt for password

The user must enter a password and confirm it.

Once you have entered a password value, confirmed it, and selected **OK**, a screen saver will lock the TKE Console. To unlock the console, move the mouse or touch the keyboard and you will be prompted for the password.

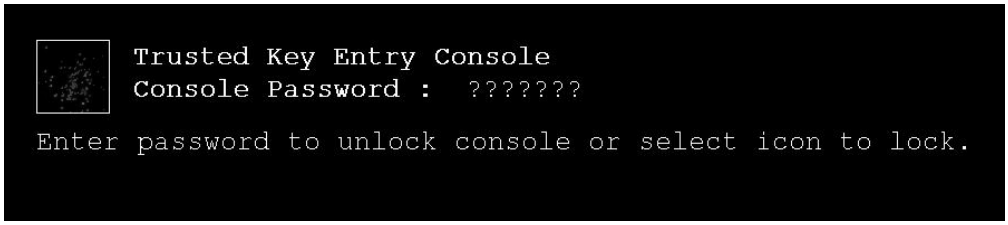


Figure 326. Prompt to unlock console

At the Console Password prompt, each keystroke appears as a question mark on the password prompt. If the correct password is entered, the user returns to the TKE console. If an incorrect password is entered, an error message will be displayed informing the user.

Manage print screen files

The Manage Print Screen Files task can be used to print individual windows on the TKE console to a file or to print the entire screen. Print screen files can be viewed, copied to a USB flash memory drive, and deleted using this task.

Network diagnostic information

The Network Diagnostic Information task displays network information such as TCP/IP addresses and Ethernet settings. It can test network connections by sending an echo request (ping) to a remote host.

Rebuild vital product data

This task is used to rebuild the Vital Product Data for the TKE machine.

Note: This task will only be displayed when logged on with the SERVICE user name.

Offload virtual RETAIN data to removable media

Note: This task will only be displayed when logged on as the SERVICE ID.

This task is used to select, by problem number, specific virtual RETAIN data to offload to a USB flash memory drive.

To invoke this task, click on Service Management and then click on Offload Virtual RETAIN Data to removable media.

Note: The removable media must be formatted with volume identification label VIRTRET, using the Format Media task.

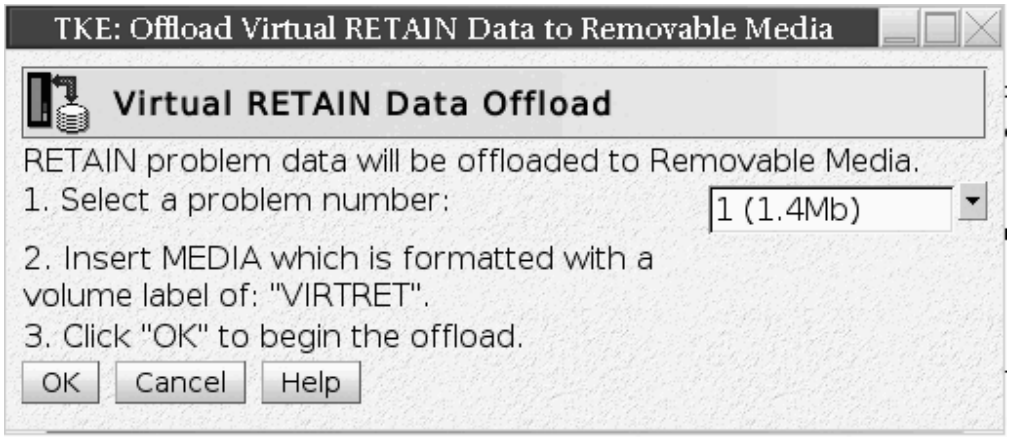


Figure 327. Virtual RETAIN Data Offload window

In the Virtual RETAIN Data Offload window, select the Problem Number and click OK. The selected virtual RETAIN data is off-loaded to the removable media.

When the virtual RETAIN data is offloaded successfully, a message is displayed indicating the offload was successful.

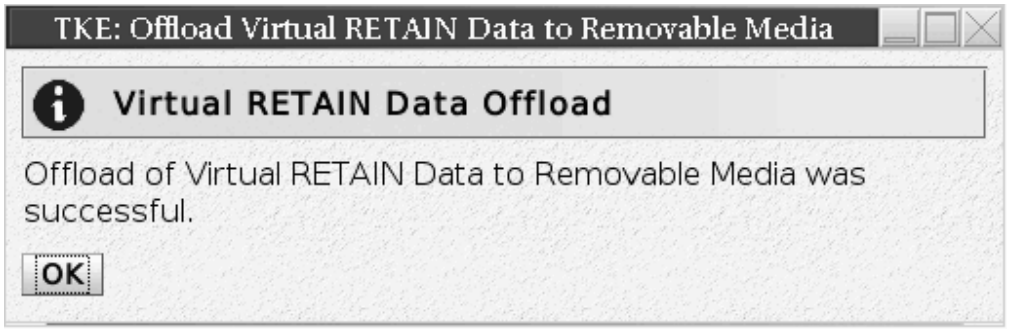


Figure 328. Successful offload of data

If you insert removable media that has not been formatted or that has the wrong label, an error message is displayed.

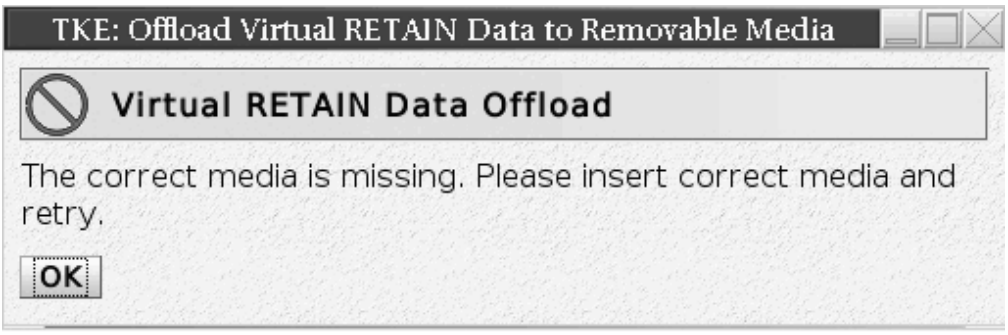


Figure 329. Virtual RETAIN Data Offload incorrect media error

Save upgrade data

The Save Upgrade Data task is used when a customer is upgrading to a new TKE image. The task should only be executed when an engineering change (EC) upgrade or miscellaneous equipment specification (MES) instructs you to save the Trusted Key Entry workstation's upgrade data. You must log on with a console user name of ADMIN or SERVICE to use this task.

All data pertinent to the TKE workstation (for example, TKE-related data directories, emulator sessions, and TCP/IP information) will be saved. Upgrading the Trusted Key Entry workstation requires saving its upgrade data before installing new EC or MES code, then restoring the upgrade data afterwards.

To invoke this task, click on Service Management and then click on Save Upgrade Data.

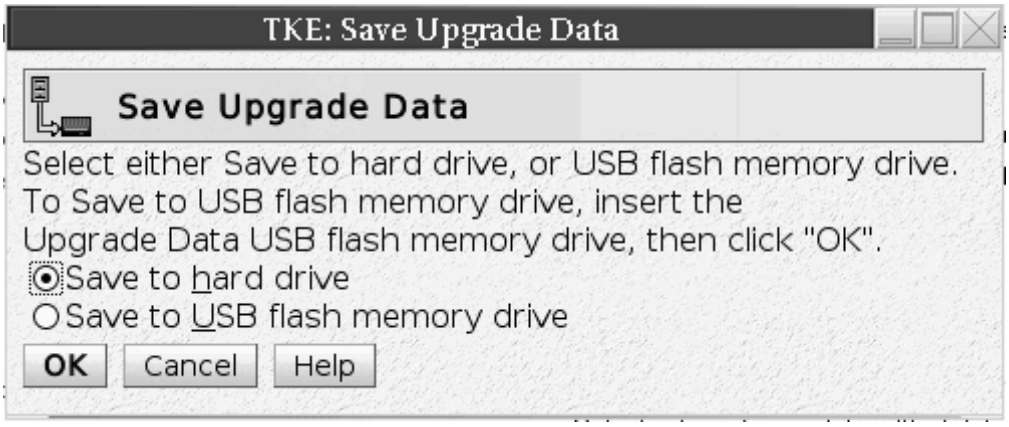


Figure 330. Save Upgrade window

Some upgrade procedures save and restore the Trusted Key Entry workstation's upgrade data automatically, and there is no need to use this console action. Otherwise, if you are following an upgrade procedure that instructs you to save the Trusted Key Entry workstation's upgrade data, you must use this console action to save it manually.

Note: The USB flash memory drive for this task must be formatted with a volume identification label of ACTUPG, using the Format Media task.

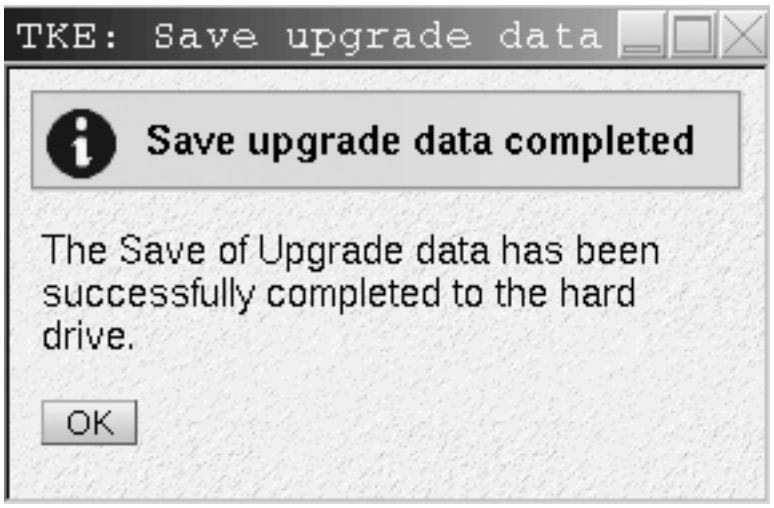


Figure 331. Save upgrade success window

Shutdown or restart

This task allows you to restart the application/console or power off.

To invoke this task, click on Service Management and then click on Shutdown or Restart.

The Shutdown or Restart dialog displays.

Figure 332. Shutdown or Restart task window

Select one of the following options from the dialog and press **OK**.

Restart Application
To close the Trusted Key Entry workstation and restart the application, select Restart application.

Restart Console
To close the Trusted Key Entry workstation, perform a system power-on reset, and restart the console, select Restart console.

Power-off console
To close the Trusted Key Entry workstation, shut down the operating system, and power-off the hardware, select Power-off console.

Selecting any option will present you with a confirmation window. Press **Yes** to continue.

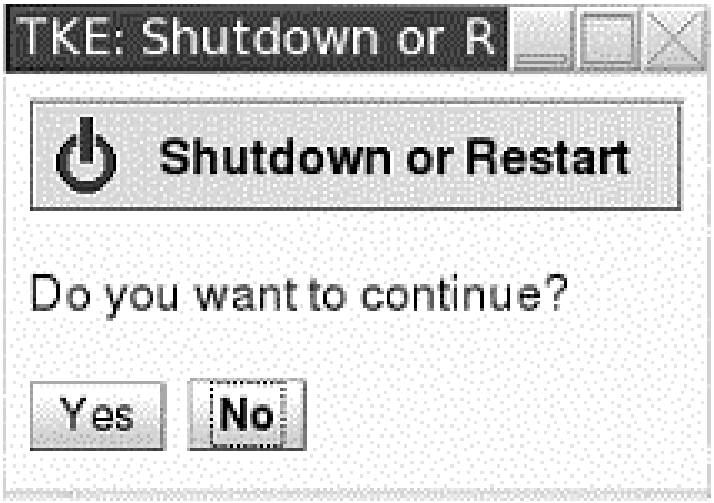


Figure 333. Confirmation window

Transmit console service data

This task is used to select the types of service data and the method to send the data to aid in the problem determination. You must log on with a console user name of SERVICE to use this task.

To invoke this task, click on Service Management and then click on Transmit Console Service Data.

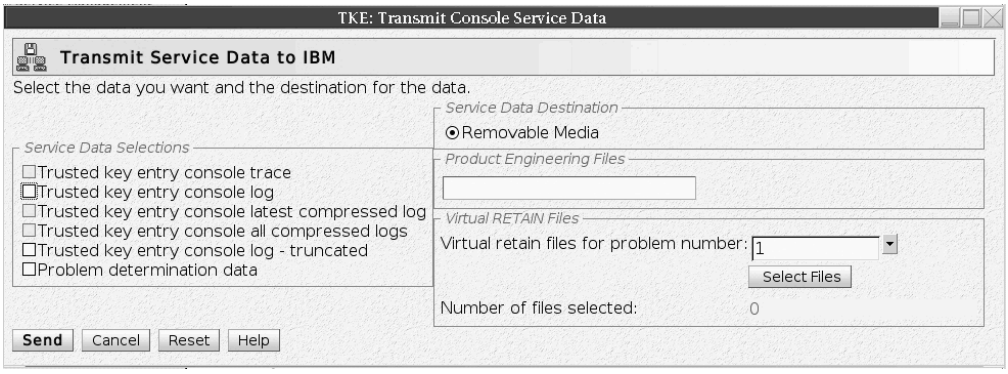


Figure 334. Transmit Console Service Data

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 a USB flash memory drive selected virtual RETAIN files for the specified problem number.

Note: You can select and copy virtual RETAIN files to a USB flash memory drive for only a single problem number at a time.

Note: When using a USB flash memory drive for service data it must first be formatted specifically for Service Data. See "Format media" on page 351 for details.

Successful completion will present the following window.

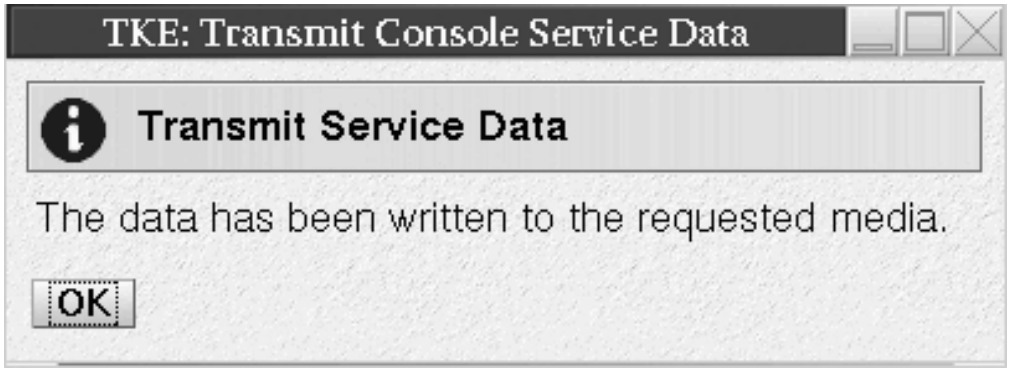


Figure 335. Transmit Console Service Data - successful completion

For Virtual RETAIN Files, enter the problem number in the Virtual RETAIN Files for Problem Number field and click on Select Files.

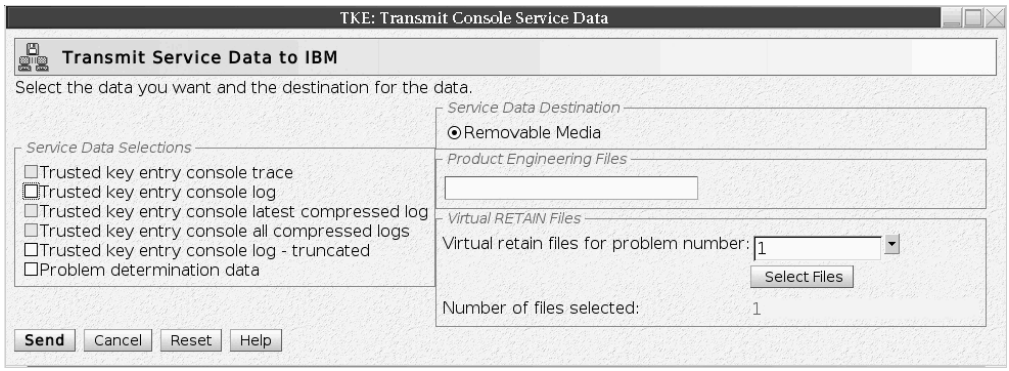


Figure 336. Update problem number for virtual RETAIN file

Select the applicable Virtual RETAIN Files and click OK.

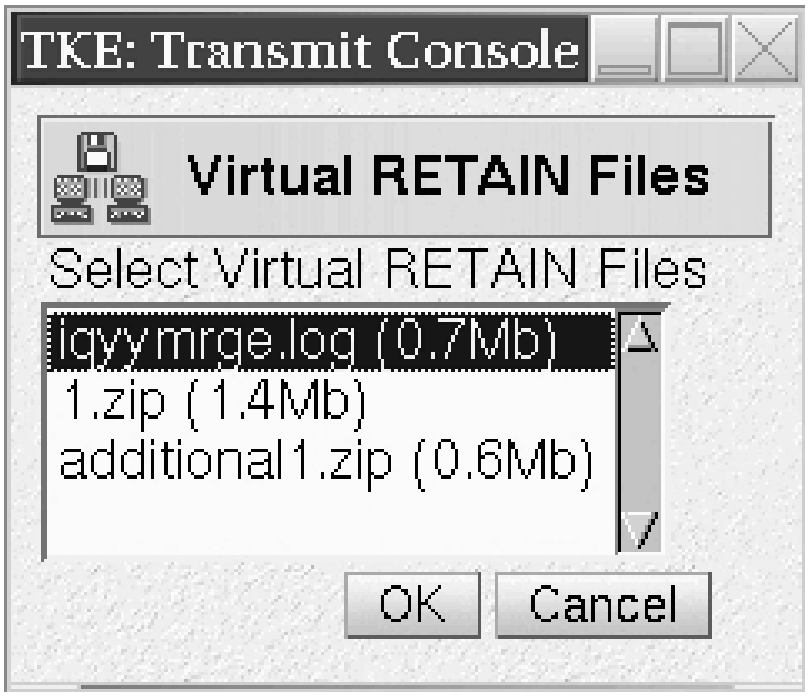


Figure 337. Select the virtual RETAIN files

Click on Send to transmit the selected Virtual RETAIN files to Media.

Insert the selected media when prompted.

Figure 338. 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.'

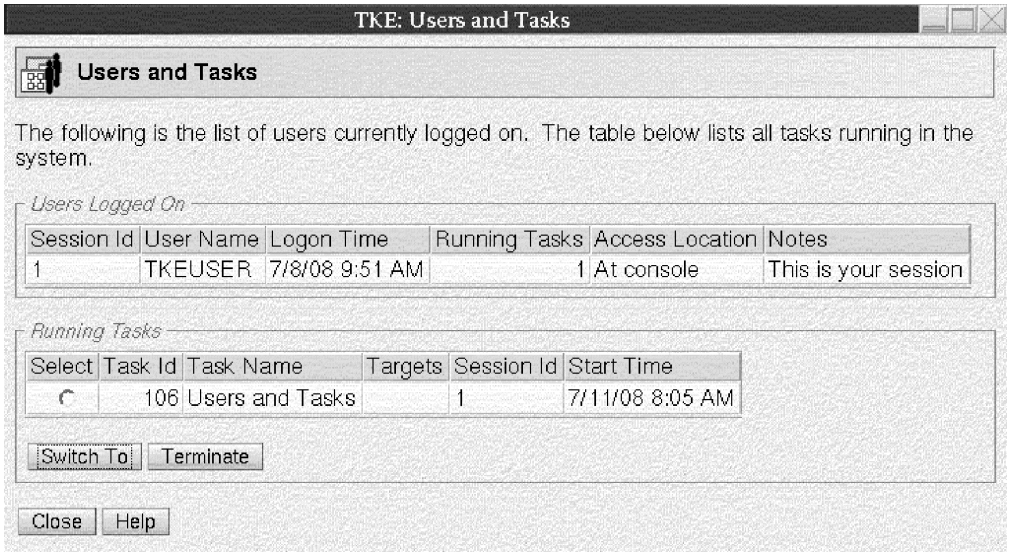


Figure 339. Users and Tasks window

View console events

This task displays console events logged by the Trusted Key Entry workstation.

To invoke this task, click on Service Management and then click View Console Events.

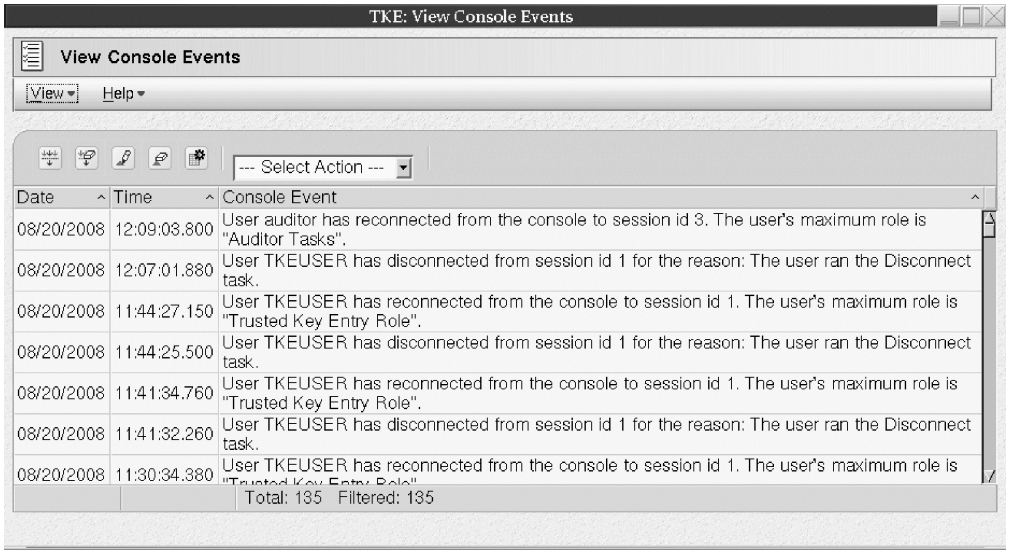


Figure 340. View Console Events window

The Trusted Key Entry workstation automatically keeps a log of significant operations and activities, referred to as console events, that occur while the application is running.

This window displays all console events currently logged and lists them in reverse order of occurrence, from the most recent event to the oldest event. You can select a different time and date range for the events displayed using an option on the View pull-down menu.

View console information

This task shows the Machine Information (Type, Model Number, and Serial Number) and the Internal Code Change History. The information contained here may be useful for problem determination.

To invoke this task, click on Service Management and then click on View Console Information.

The View Console Information window is displayed.

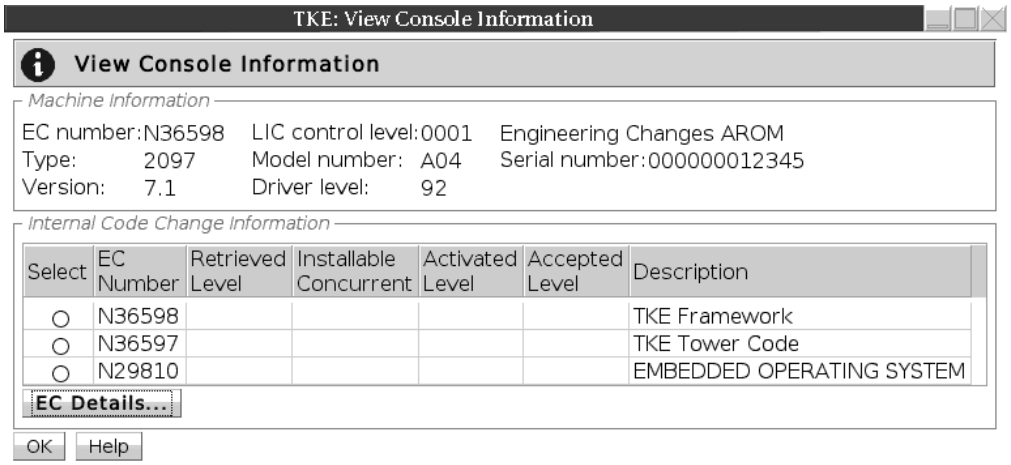


Figure 341. View Console Information window

For additional information about an internal code change, select an EC number, then click **EC Details**.

The Internal Code Change Details window is displayed.

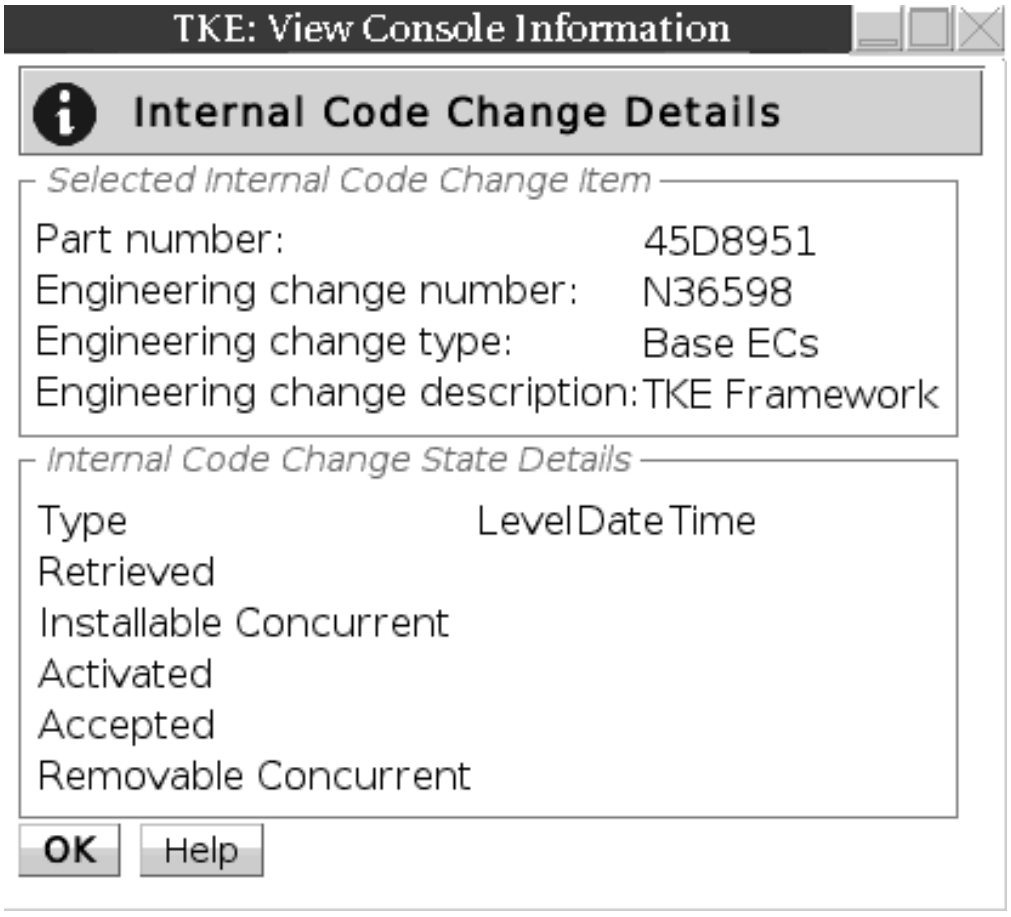


Figure 342. Internal Code Change Details window

The View Console Information window contains the following information.

EC Number
Displays the engineering change (EC) number of the internal code change.

Retrieved Level
Displays the internal code change level that was most recently copied to the console, making it available for installation.

Installable Concurrent
Displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for this console, from the current installed level up to and including the installable concurrent level, without disrupting the operations of this console.

Activated Level
Displays the internal code change level that was most recently activated as a working part of the licensed internal code of the console.

Accepted Level
Displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the console.

Removable Concurrent
Displays the lowest installed internal code change level that can be removed such that the remaining installed change level can be activated concurrently. That is, you can remove all change levels installed for this console, from the current installed level down to and including the removable concurrent level, without disrupting the operations of this console.

View console service history

The View Console Service History is used to review or close problems that are discovered by Problem Analysis. A problem is opened when Problem Analysis determines service is required to correct a problem.

To invoke this task, click on Service Management and then click on View Console Service History.

The View Console Service History window is displayed.

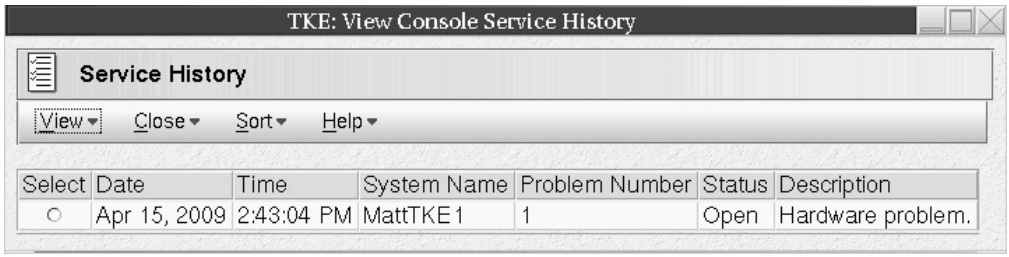


Figure 343. View Console Service History window

Each record of a problem includes detailed information about the problem and indicates whether the service required to correct the problem is still pending (Open), is already completed (Closed), or no longer needed (Closed).

View on the menu bar:

- **Problem summary** lists information about the problem and what actions are needed to diagnose and correct it.

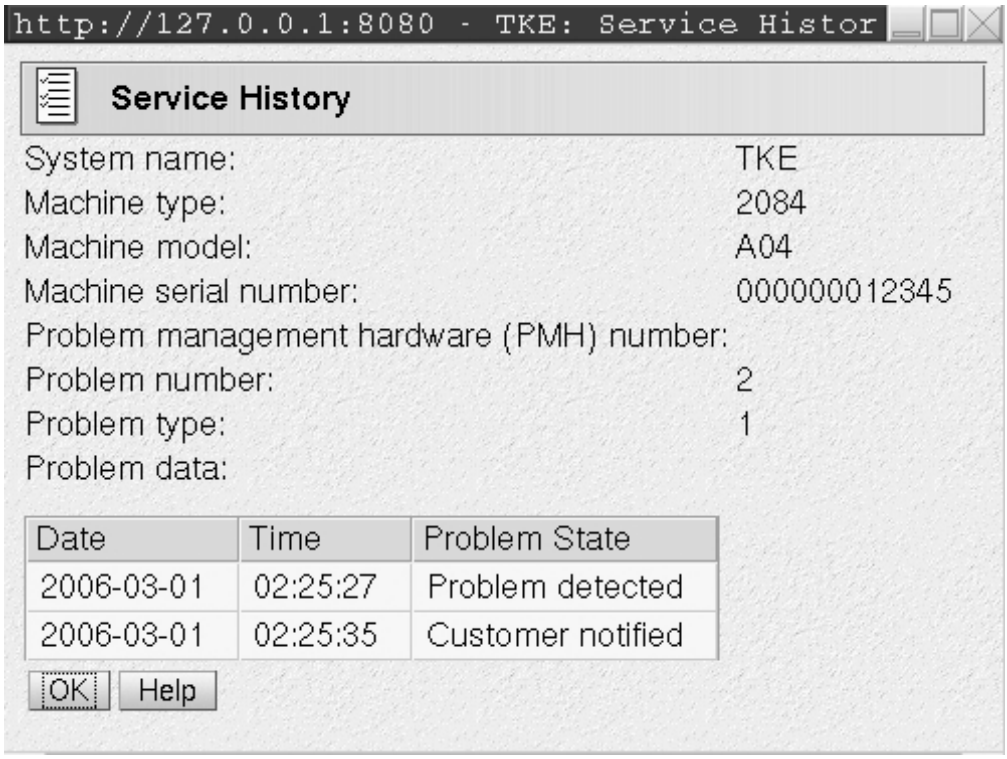


Figure 344. Problem summary

- The **Problem Analysis Panels** show System name, Date, Time, Problem Description, and Corrective Actions that a user can take.

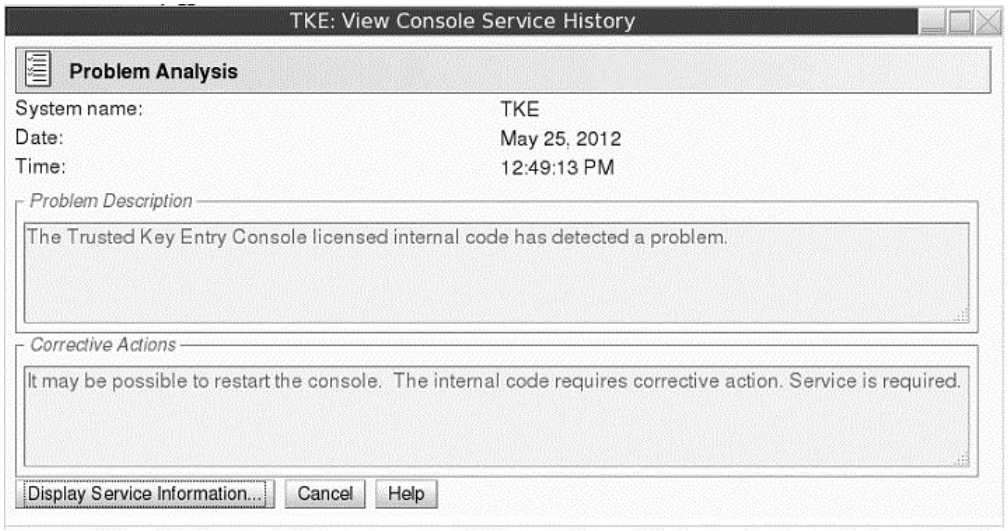


Figure 345. Problem Analysis

- **Cancel** exits this task and returns to the Trusted Key Entry Console.

Clicking **Close** on the menu bar brings up two options:

- **Selected Problem** changes the status of the selected problem to Closed.
- **All Problems** changes the status of all open problems to Closed.

View console tasks performed

The View Console Tasks Performed task window shows a summary of the console tasks performed with the date and time associated with each task. The most recent tasks invoked are appended to the bottom of the list. This information is useful in determining past activity performed on the TKE Workstation for auditing or problem determination.

To invoke this task, click on Service Management and then click on View Console Tasks Performed. The View Console Tasks Performed window is displayed.

You must scroll the display to the right until you see the inner right scroll bar for moving the display up and down.

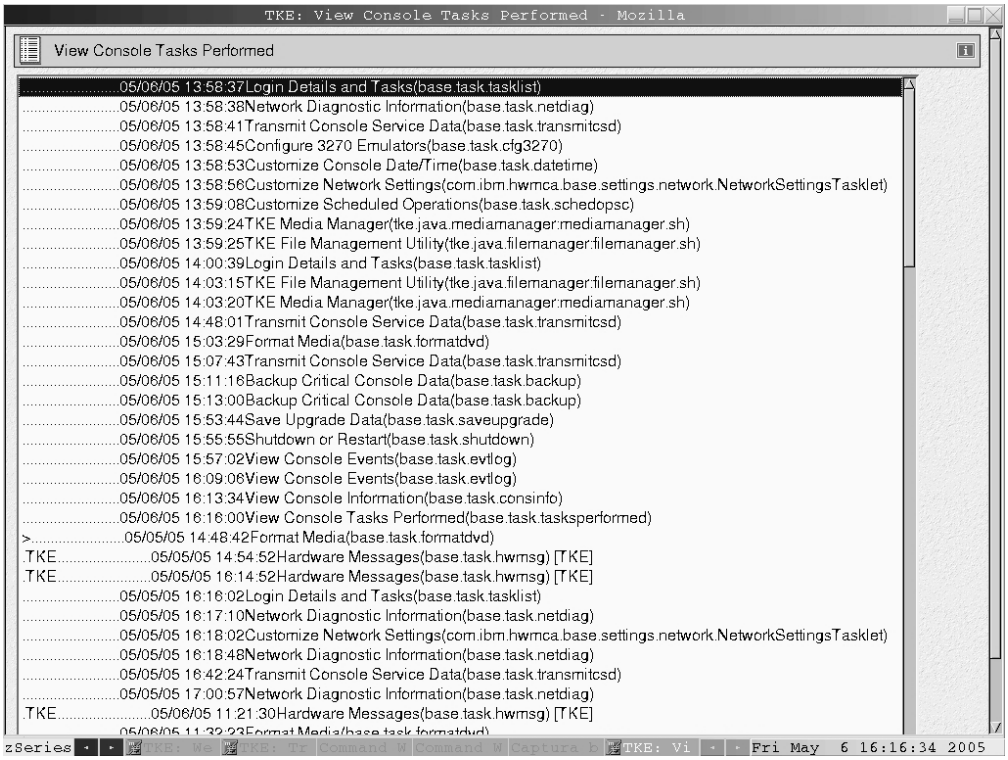


Figure 346. View Console Tasks Performed window

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
- IBM CCA 5.0 Embedded Operating System
- Addendum for Elliptical Curve Cryptography
- Mozilla Firefox Browser License
- Apache Tomcat License Information
- Boost License Information
- Java License Information
- Apache BeanUtils License Information

- Apache Digester License Information
- Apache Collections License Information
- Apache Logging License Information
- Help System License Information
- ActiveMQ-CPP License Information
- ACE+TAO License Information
- ACE+TAO IIOP License Information

To view a specific license, click on it. When you are done viewing the license information click on **OK** to exit.

If you have not viewed any license information through this task, the first TKE related task that you invoke will display the license information. This will only be done once.

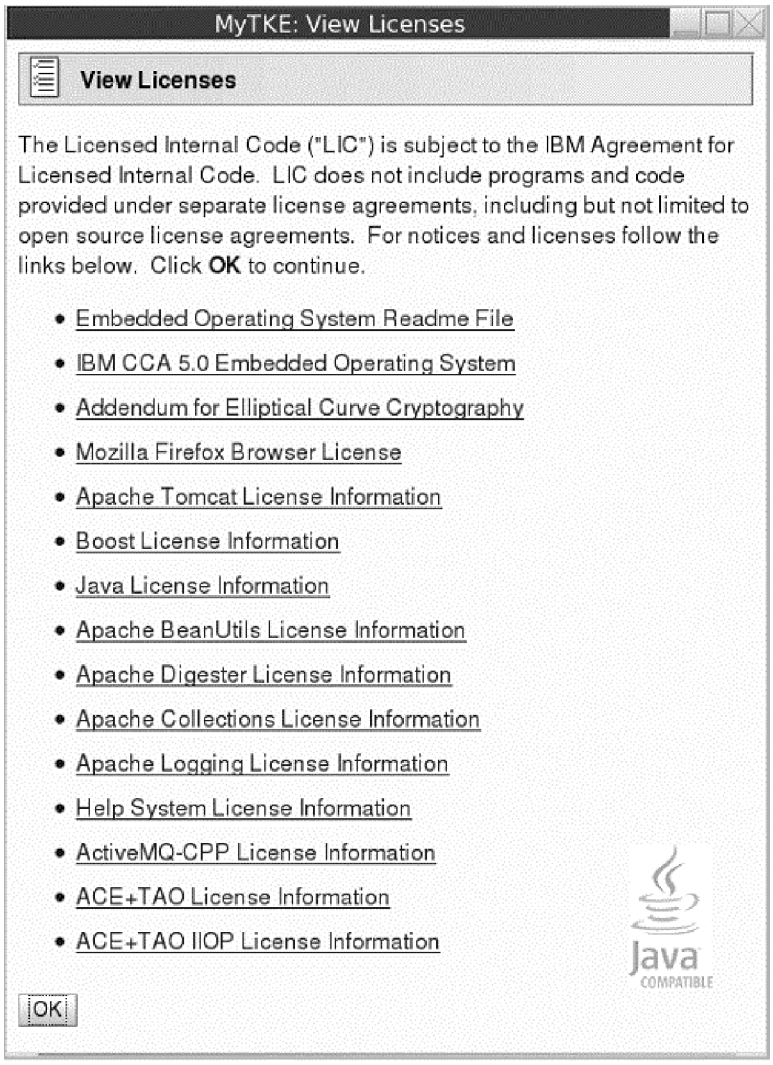


Figure 347. View Licenses window

View security logs

This task displays the TKE console's default security log. The security log is a record of the security-relevant events that have occurred on or have been initiated by the TKE workstation. You must log on with a console user name of AUDITOR to use this task.

See “View security logs” on page 219 for more information.

Appendix F. TKE best practices

This information describes the setup required for TKE to manage host crypto modules, and a set of setup steps to perform on the TKE workstation. TKE workstations initialized for passphrase and initialized for smart card use are considered separately.

Checklist for loading a TKE machine - passphrase

Expectations

- You are working with CCA host crypto modules
- The support element has enabled TKE on these host crypto modules
- LPARs are established
- TKE licensed internal code (LIC) is loaded on the TKE workstation
- Segments 1, 2, and 3 have been loaded on the TKE workstation crypto adapter
- The TKE host transaction program has been configured and started in the host TKE LPAR
- ICSF is started in each LPAR

Setup

- 2 TKEs both running the same level of software
  - One for production
  - One for backup
- 2 Central electronic complex (CEC) cards being shared
  - One Test LPARs (Domain 0)
  - Three Production LPARs (Domain 1, 2, 3)

  TKE can load the master key in a group of domains as defined by a domain group.
- Host TKE LPAR 1

  When defining the LPAR activation profile, the usage domain will be 1 and the control domain will be 0, 1, 2, 3.

The following User IDs are used to restrict access to the TKE workstation crypto adapter:

- TKEUSER - can run the main TKE application
- TKEADM - can create and update TKE roles and profiles
- KEYMAN1 - can clear TKE new master keys and load first master key parts
- KEYMAN2 - can load TKE middle and last key parts and reencipher TKE workstation key storage

Authorities are used to restrict access to the CCA crypto modules on the host machine.

One way to control access to CCA host crypto modules is with a minimum of seven host authorities.

- ISSUER
  - Disable host crypto module

  - Enable host crypto module issue
  - Access control issue
  - Zeroize domain issue
  - Domain control change issue
- COSIGN
  - Access control co-sign
  - Enable host crypto module co-sign
  - Zeroize domain co-sign
  - Domain control change co-sign
- MKFIRST
  - AES, DES, ECC (APKA), or RSA load first master key part
  - Clear new master key register
  - Clear old master key register
- MKMIDDLE
  - AES, DES, ECC (APKA), or RSA combine middle master key parts
- MKLAST
  - AES, DES, ECC (APKA), or RSA combine final master key part
  - Set RSA master key
- FIRSTCLEAR
  - Load first operational key part
  - Clear operational key register
- ADDCOMP
  - Load additional operational key part
  - Complete key

The following tasks should be run using the TKE workstation to set up the TKE workstation and the host crypto modules for use. Be aware that the Service Management tasks available to you will vary depending on the console user name you used to log on. Refer to "Service Management tasks" on page 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 keys are set and TKE key storages are initialized.
4. Logon to CNM with KEYMAN1 - OPTIONAL
   a. Clear the new DES/PKA and AES master key registers
   b. Enter known first master key parts for the DES/PKA and AES master keys.
   c. Logoff
5. Logon to CNM with KEYMAN2 - OPTIONAL
   a. Enter known middle and last master key parts for the DES/PKA and AES master keys.
   b. Reencipher DES, PKA, and AES key storage
   c. Logoff
6. Logon to CNM with TKEADM

a. Create user defined roles - OPTIONAL
b. Create user defined profiles - OPTIONAL
c. Create groups and add users - OPTIONAL

   Note: Group members should already be defined.
d. Change the passphrases for all of the predefined profiles - TKEADM, TKEUSER, KEYMAN1, and KEYMAN2

7. Log on to the main TKE application with TKEUSER profile or another profile with the same authority
   a. Load the default authority key for key index 0
   b. Change these options of your security policy via the TKE preferences menu
      - Blind Key Entry
      - Removable media only
   c. Create a Host
   d. Create domain groups - OPTIONAL
   e. Open a host or a domain group (requires host logon)
   f. Open a crypto module notebook or domain group notebook
   g. Create role or roles
   h. Generate authority key or keys and save them to binary file or files
   i. Create different authorities using the different authority key or keys that were just generated.
   j. Delete the authority 00 or change the authority key to a key that is not the default key. If you delete authority 00 make sure that you have 2 other known authority keys that have the Domain control change issue and co-sign.
8. Configure 3270 Emulators
9. Backup Critical Console Data onto a USB flash memory drive.
10. Customize Scheduled Operations to schedule the backup critical console data task

Checklist for loading a TKE machine - smart card

Expectations:

- You are working with CCA or EP11 host crypto modules.
- The support element has enabled TKE on these host crypto modules.
- LPARs are established (set up and predefined).
- TKE licensed internal code (LIC) is loaded on the TKE workstation.
- Segments 1, 2, and 3 have been loaded on the TKE workstation crypto adapter.
- The TKE host transaction program has been configured and started in the host TKE LPAR.
- ICSF is started in each LPAR.
- Smart card readers are attached.

Setup

- 2 TKEs both running the same level of software
  - One for production
  - One for backup

- 2 CECs cards being shared
  - One Test LPARs (Domain 0)
  - Three Production LPARs (Domain 1, 2, 3)

  TKE can load the master key in a group of domains as defined by a domain group.
- Host TKE LPAR 1

  When defining the LPAR activation profile, the usage domain will be 1 and the control domain will be 0, 1, 2, 3.

Profiles and roles are used to restrict access to the TKE workstation crypto adapter. There are two roles, listed below, that are needed to use the TKE and CNM applications. Profiles are created by first generating a crypto adapter logon key and then creating a profile using the crypto adapter logon key.

- SCTKEUSR - can run the main TKE application
- SCTKEADM - can run CNM to create and update TKE roles and profiles

Authorities are used to restrict access to the CCA crypto modules on the host machine.

Administrators are used to restrict access to the EP11 crypto modules on the host machine.

One way to control access to the CCA host crypto modules is with a minimum of seven host authorities.

- ISSUER
  - Disable host crypto module
  - Enable host crypto module issue
  - Access control issue
  - Zeroize domain issue
  - Domain control change issue
- COSIGN
  - Access control co-sign
  - Enable host crypto module co-sign
  - Zeroize domain co-sign
  - Domain control change co-sign
- MKFIRST
  - AES, DES, ECC (APKA), or RSA load first master key part
  - Clear new master key register
  - Clear old master key register
- MKMIDDLE
  - AES, DES, ECC (APKA), or RSA combine middle master key parts
- MKLAST
  - AES, DES, ECC (APKA), or RSA combine final master key part
  - Set RSA master key
- FIRSTCLEAR
  - Load first operational key part
  - Clear operational key register
- ADDCOMP

– Load additional operational key part
– Complete key

The steps to set up the TKE workstation for smart card use are as follows. Be aware that the Service Management tasks available to you will vary depending on the console user name you used to log on. Refer to “Service Management tasks” on page 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 keys are set and TKE key storages are initialized.
4. Open the SCUP application.
   a. Create a CA smart card.
   b. Backup CA smart cards.
   c. Create TKE smart cards.

      Note: In general, smart cards created on a particular TKE release cannot be used on TKE workstations that are at prior release levels. There are exceptions. See “Smart card usage” on page 36.
   d. Create EP11 smart cards.
   e. Enroll the TKE workstation crypto adapter with the CA card.
5. Open CNM.

   Note: Choose the "Default Logon". The temp default role will be used, and has full access to do everything on the crypto adapter.
   a. Enter known DES/PKA and AES master keys. (Optional)
      • Do this only if you want to have known master keys to use again.
   b. Reencipher DES, PKA, and AES key storage. (Optional)
      • Do this only if you entered your own master keys.
   c. Generate TKE workstation crypto adapter logon keys for each smart card that will be logging on to the TKE or CNM applications.
   d. Create new profile or profiles for the smart cards under the Access Control menu. The roles for these profiles are loaded in the crypto adapter when TKE's IBM Crypto Adapter Initialization task is run.
   e. Create group or groups and add users.

      Note: Group members should already be defined.
   f. Load the default role.
      • When the TKE workstation crypto adapter is initialized the TEMPDEFAULT role is loaded. You need to load the DEFAULT role to secure the TKE workstation.
6. Log on to the main TKE application with the SCTKEUSR profile or another profile with the same authority.
   a. Load the default authority key for key index 0.
   b. Change these options of your security policy via the TKE preferences menu
      • Blind Key Entry
      • Removable media only

c. Create a Host.
d. Create domain groups. (Optional)
e. Open a host or a domain group (requires host logon).
f. Open a crypto module notebook or domain group notebook.
g. For CCA host crypto modules:
    1) Create roles.
    2) Generate authority keys and save them to TKE smart cards.

       Note: You can generate and save 1024-bit and 2048-bit RSA keys and BP-320 ECC keys on TKE smart cards. Authorities with 2048-bit RSA keys are supported starting with the CEX3C. Authorities with BP-320 ECC keys are supported starting with the CEX5C.
    3) Create different authorities using the different authority keys that were just generated.
    4) Delete the authority 00 or change the authority key to a key that is not the default key. If you delete authority 00 make sure that you have 2 other known authority keys that have the Domain control change issue and cosign.
h. For EP11 host crypto modules:
    1) Generate administrator keys and save them to EP11 smart cards.
    2) Zeroize the host crypto module or the set of domains you want to administer. Zeroizing a host crypto module or domain puts it in "imprint mode", where administrators can be added without using signed commands.
    3) Add crypto module and domain administrators.
    4) Set the signature threshold and revocation signature threshold on each crypto module and domain. This ends imprint mode.

7. Configure 3270 Emulators.
8. Backup Critical Console Data.
9. Customize Scheduled Operations to schedule the backup critical console data task.
10. If using the same set of smart cards on another TKE, you need to use the Remote Enroll feature for TKE.

Appendix G. TKE hardware support and migration information

This information includes the following topics:

- "TKE release and feature codes available by CEC levels"
- "Smart card readers and smart cards orderable by TKE release"
- "TKE (LIC) upgrade paths" on page 379
- "Host cryptographic modules managed by TKE" on page 379

TKE release and feature codes available by CEC levels

Table 25 shows the TKE licensed internal code (LIC) that is orderable based on the date and type of your CEC.

Most of the time, a new version of the TKE workstation is released at the same time as a new CEC. When you order a new TKE workstation, you receive the latest TKE hardware with the latest TKE licensed internal code (LIC) installed on it. For example, if you had placed an order for a new TKE workstation between September of 2012 and September of 2013, you would have received TKE 7.2 (or, in order words, hardware feature code 0841 with LIC feature code 0850).

Table 25. TKE release and feature codes available by CEC level

	Feature codes			CEC information										
TKE release (LIC)	**Hardware**	**LIC**	**Initial release date**	**z9-109 z9EC 2094**	**z9BC 2096**	**z10 EC 2097**	**z10 BC 2098**	**z10 EC GA3 z10 BC GA2**	**z196**	**z114**	**zEC12**	**zBC12**	**z13**
TKE 5.3	0839	0854	Oct 2008	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A
TKE 6.0	0840	0858	Nov 2009	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A
TKE 7.0	0841	0860	Sept 2010	N/A	N/A	Yes	Yes	Yes	Yes	Yes	N/A	N/A	N/A
TKE 7.1	0841	0867	Sept 2011	N/A	N/A	Yes	Yes	Yes	Yes	Yes	N/A	N/A	N/A
TKE 7.2	0841	0850	Sept 2012	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	N/A	N/A
TKE 7.3	0842	0872	Sept 2013	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes	N/A
TKE 8.0	0847	0877	Feb 2015	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes

Your host cryptographic environment determines the level of TKE LIC that you can use. To determine which host cryptographic modules are supported by your TKE, see Table 28 on page 380.

Smart card readers and smart cards orderable by TKE release

Table 26 shows the smart card readers and smart cards that can be ordered for each TKE release.

Table 26. Smart card readers and smart cards orderable by TKE release

TKE release (LIC)	**Smart card reader**		**Smart card**	
	Feature code	**Type**	**Feature code**	**Part number**
TKE 5.3	0885	Omnikey/HID	0884	45D3398

Table 26. Smart card readers and smart cards orderable by TKE release (continued)

TKE release (LIC)	Smart card reader		Smart card	
	Feature code	**Type**	**Feature code**	**Part number**
TKE 6.0	0885	Omnikey/HID	0884	45D3398
				74Y0551* #
TKE 7.0	0885	Omnikey/HID	0884	45D3398
				74Y0551* #
TKE 7.1	0885	Omnikey/HID	0884	45D3398
				74Y0551*
TKE 7.2	0885	Omnikey/HID	0884	74Y0551*
TKE 7.3	0885	Omnikey/HID	0884	74Y0551*
TKE 8.0	00JJ019	Omnikey/HID	00JJ020	00JA710

* Part number 74Y0551 replaced part number 45D3398 in feature code 0884.

\# An MCL is required in order to support part number 74Y0551 on TKE 6.0 and TKE 7.0.

There are restrictions on what smart card part numbers can be used to create different smart card types. See “Smart card compatibility issues” on page 35 for more information.

DATAKEY smart cards are not supported on TKE 7.0 or later. If you are upgrading from TKE 6.0 to TKE 7.0 or later and have DATAKEY smart cards, you need to backup your CA smart cards using a more current smart card part number and copy keys and key parts from your TKE smart cards onto TKE smart cards created from a more current smart card part number. See “Datakey card usage” on page 38 for information on migrating data to a new smart card.

To identify the part number of your smart card, look for the following:

DATAKEY
Has blue and orange art work and DATAKEY printed on them.

45D3398
Are white and do not have any part number printed on them.

74Y0551
Has part number 74Y0551 printed on them.

00JA710
Has part number 00JA710 printed on them.

TKE (LIC) upgrade paths

Table 27 shows which TKE licensed internal code (LIC) can be upgraded to a new LIC level.

Table 27. Summary of when a TKE workstation can be upgraded

Starting point			Upgradable to TKE LIC level					
TKE release (LIC)	**Hardware feature code**	**TKE crypto adapter type**	**TKE 6.0 (FC 0858)**	**TKE 7.0 (FC 0860)**	**TKE 7.1 (FC 0867)**	**TKE 7.2 (FC 0850)**	**TKE 7.3 (FC 0872)**	**TKE 8.0 (FC 0877)**
TKE 5.3	0839	4764	Yes	No	No	No	No	No
TKE 6.0	0839	4764	**Base***	No	No	No	No	No
	0840							
TKE 7.0	0841	4765	N/A	**Base***	Yes	Yes	Yes	No
TKE 7.1	0841	4765	N/A	N/A	**Base***	Yes	Yes	No
TKE 7.2	0841	4765	N/A	N/A	N/A	**Base***	Yes	No
TKE 7.3	0841	4765	N/A	N/A	N/A	N/A	**Base***	No
	0842	4765	N/A	N/A	N/A	N/A	**Base***	Yes
TKE 8.0	0847	4767	N/A	N/A	N/A	N/A	N/A	**Base***

Base* The initial TKE LIC level installed on the TKE workstation before it was shipped.

Note: In general, you cannot upgrade your TKE's LIC if the new level LIC requires a new TKE crypto adapter type. For example, in Table 27, TKE 5.3 and TKE 6.0 require a 4764 crypto adapter and TKE 7.*x* workstations require a 4765 crypto adapter. Therefore, TKE workstation feature codes 0839 and 0840 (TKE 5.3 and TKE 6.0) cannot be upgraded to a TKE 7.*x* LIC because TKE 7.*x* workstations required a different TKE crypto adapter type (4764 versus 4765). Upgrades from TKE 7.3 with hardware feature code 0842 to TKE 8.0 are permitted, but the TKE crypto adapter must be replaced.

When you upgrade the TKE LIC level of an existing TKE workstation, you can keep your user data. If you have an older TKE and want to introduce a TKE 7.*x* to your complex, see Chapter 3, “TKE migration and recovery installation,” on page 45 for information on moving user data to your TKE 7.*x* workstation.

Host cryptographic modules managed by TKE

TKE manages host cryptographic modules on any CEC where that particular host cryptographic module is supported. In other words, for example, TKE is unaware whether a CEX3C module is running on an IBM System z10, IBM zEnterprise 196, IBM zEnterprise 114, IBM zEnterprise EC12, IBM zEnterprise BC12, or an IBM z13.

Table 28 on page 380 identifies the host cryptographic modules that each TKE release can manage.

Table 28. Host cryptographic modules managed by TKE LIC

TKE release (LIC)	Host cryptographic modules supported by TKE release					
	CEX2C	**CEX3C**	**CEX4C**	**CEX4P**	**CEX5C**	**CEX5P**
TKE 5.2	Yes	No	No	No	No	No
TKE 5.3	Yes	Yes	No	No	No	No
TKE 6.0	Yes	Yes	Sometimes*	No	No	No
TKE 7.0	Yes	Yes	Sometimes*	No	No	No
TKE 7.1	Yes	Yes	Sometimes*	No	No	No
TKE 7.2	Yes	Yes	Yes	Yes#	No	No
TKE 7.3	Yes	Yes	Yes	Yes#	No	No
TKE 8.0	Yes	Yes	Yes	Yes#	Yes@	Yes#, @

* A Crypto Express4 that is running in Common Cryptographic Architecture (CCA) mode as a CEX4C is only supported when running ICSF HCR7790 or lower with the toleration APAR OA39075 that allows the CEX4C to report in as a CEX3C. In this case, ICSF sees the module as a CEX3C and manages it as a CEX3C.

CEX4P and CEX5P crypto modules require smart cards to hold administrator certificates and master key material. Smart card readers must be attached to the TKE to administer these host crypto module types.

@ A minimum level of ICSF HCR77B0 is required when managing Crypto Express5S coprocessors. Older releases of ICSF, even in toleration mode, will not return the list of Crypto Express5S coprocessors to the TKE.

Some host cryptographic configurations (in other words, specific cryptographic features or combinations of the CEC, host cryptographic module, CCA or EP11 level, and ICSF) require minimum levels of TKE to support the environment.

Appendix H. Accessibility

Accessible publications for this product are offered through IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSLTBW/welcome).

If you experience difficulty with the accessibility of any z/OS information, send a detailed message to the "Contact us" web page for z/OS (http://www.ibm.com/systems/z/os/zos/webqs.html) or use the following mailing address.

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
United States

Accessibility features

Accessibility features help users who have physical disabilities such as restricted mobility or limited vision use software products successfully. The accessibility features in z/OS can help users do the following tasks:

- Run assistive technology such as screen readers and screen magnifier software.
- Operate specific or equivalent features by using the keyboard.
- Customize display attributes such as color, contrast, and font size.

Consult assistive technologies

Assistive technology products such as screen readers function with the user interfaces found in z/OS. Consult the product information for the specific assistive technology product that is used to access z/OS interfaces.

Keyboard navigation of the user interface

You can access z/OS user interfaces with TSO/E or ISPF. The following information describes how to use TSO/E and ISPF, including the use of keyboard shortcuts and function keys (PF keys). Each guide includes the default settings for the PF keys.

- *z/OS TSO/E Primer*
- *z/OS TSO/E User's Guide*
- *z/OS V2R2 ISPF User's Guide Vol I*

Dotted decimal syntax diagrams

Syntax diagrams are provided in dotted decimal format for users who access IBM Knowledge Center with a screen reader. In dotted decimal format, each syntax element is written on a separate line. If two or more syntax elements are always present together (or always absent together), they can appear on the same line because they are considered a single compound syntax element.

Each line starts with a dotted decimal number; for example, 3 or 3.1 or 3.1.1. To hear these numbers correctly, make sure that the screen reader is set to read out

punctuation. All the syntax elements that have the same dotted decimal number (for example, all the syntax elements that have the number 3.1) are mutually exclusive alternatives. If you hear the lines 3.1 USERID and 3.1 SYSTEMID, your syntax can include either USERID or SYSTEMID, but not both.

The dotted decimal numbering level denotes the level of nesting. For example, if a syntax element with dotted decimal number 3 is followed by a series of syntax elements with dotted decimal number 3.1, all the syntax elements numbered 3.1 are subordinate to the syntax element numbered 3.

Certain words and symbols are used next to the dotted decimal numbers to add information about the syntax elements. Occasionally, these words and symbols might occur at the beginning of the element itself. For ease of identification, if the word or symbol is a part of the syntax element, it is preceded by the backslash (\) character. The * symbol is placed next to a dotted decimal number to indicate that the syntax element repeats. For example, syntax element *FILE with dotted decimal number 3 is given the format 3 * FILE. Format 3* FILE indicates that syntax element FILE repeats. Format 3* * FILE indicates that syntax element * FILE repeats.

Characters such as commas, which are used to separate a string of syntax elements, are shown in the syntax just before the items they separate. These characters can appear on the same line as each item, or on a separate line with the same dotted decimal number as the relevant items. The line can also show another symbol to provide information about the syntax elements. For example, the lines 5.1*, 5.1 LASTRUN, and 5.1 DELETE mean that if you use more than one of the LASTRUN and DELETE syntax elements, the elements must be separated by a comma. If no separator is given, assume that you use a blank to separate each syntax element.

If a syntax element is preceded by the % symbol, it indicates a reference that is defined elsewhere. The string that follows the % symbol is the name of a syntax fragment rather than a literal. For example, the line 2.1 %OP1 means that you must refer to separate syntax fragment OP1.

The following symbols are used next to the dotted decimal numbers.

? indicates an optional syntax element
The question mark (?) symbol indicates an optional syntax element. A dotted decimal number followed by the question mark symbol (?) indicates that all the syntax elements with a corresponding dotted decimal number, and any subordinate syntax elements, are optional. If there is only one syntax element with a dotted decimal number, the ? symbol is displayed on the same line as the syntax element, (for example 5? NOTIFY). If there is more than one syntax element with a dotted decimal number, the ? symbol is displayed on a line by itself, followed by the syntax elements that are optional. For example, if you hear the lines 5 ?, 5 NOTIFY, and 5 UPDATE, you know that the syntax elements NOTIFY and UPDATE are optional. That is, you can choose one or none of them. The ? symbol is equivalent to a bypass line in a railroad diagram.

! indicates a default syntax element
The exclamation mark (!) symbol indicates a default syntax element. A dotted decimal number followed by the ! symbol and a syntax element indicate that the syntax element is the default option for all syntax elements that share the same dotted decimal number. Only one of the syntax elements that share the dotted decimal number can specify the ! symbol. For example, if you hear the lines 2? FILE, 2.1! (KEEP), and 2.1 (DELETE), you know that (KEEP) is the

default option for the FILE keyword. In the example, if you include the FILE keyword, but do not specify an option, the default option KEEP is applied. A default option also applies to the next higher dotted decimal number. In this example, if the FILE keyword is omitted, the default FILE(KEEP) is used. However, if you hear the lines 2? FILE, 2.1, 2.1.1! (KEEP), and 2.1.1 (DELETE), the default option KEEP applies only to the next higher dotted decimal number, 2.1 (which does not have an associated keyword), and does not apply to 2? FILE. Nothing is used if the keyword FILE is omitted.

*** indicates an optional syntax element that is repeatable**

The asterisk or glyph (*) symbol indicates a syntax element that can be repeated zero or more times. A dotted decimal number followed by the * symbol indicates that this syntax element can be used zero or more times; that is, it is optional and can be repeated. For example, if you hear the line 5.1* data area, you know that you can include one data area, more than one data area, or no data area. If you hear the lines 3* , 3 HOST, 3 STATE, you know that you can include HOST, STATE, both together, or nothing.

Notes:

1. If a dotted decimal number has an asterisk (*) next to it and there is only one item with that dotted decimal number, you can repeat that same item more than once.
2. If a dotted decimal number has an asterisk next to it and several items have that dotted decimal number, you can use more than one item from the list, but you cannot use the items more than once each. In the previous example, you can write HOST STATE, but you cannot write HOST HOST.
3. The * symbol is equivalent to a loopback line in a railroad syntax diagram.

+ indicates a syntax element that must be included

The plus (+) symbol indicates a syntax element that must be included at least once. A dotted decimal number followed by the + symbol indicates that the syntax element must be included one or more times. That is, it must be included at least once and can be repeated. For example, if you hear the line 6.1+ data area, you must include at least one data area. If you hear the lines 2+, 2 HOST, and 2 STATE, you know that you must include HOST, STATE, or both. Similar to the * symbol, the + symbol can repeat a particular item if it is the only item with that dotted decimal number. The + symbol, like the * symbol, is equivalent to a loopback line in a railroad syntax diagram.

Notices

This information was developed for products and services offered in the U.S.A. or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not 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
U.S.A

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

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:

Site Counsel
IBM Corporation
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.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

COPYRIGHT LICENSE:

This information might contain sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS™, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted

for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (http://www.ibm.com/software/support/systemsz/lifecycle/)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe is either a registered trademark or trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z

Printed in USA

SC14-7511-04