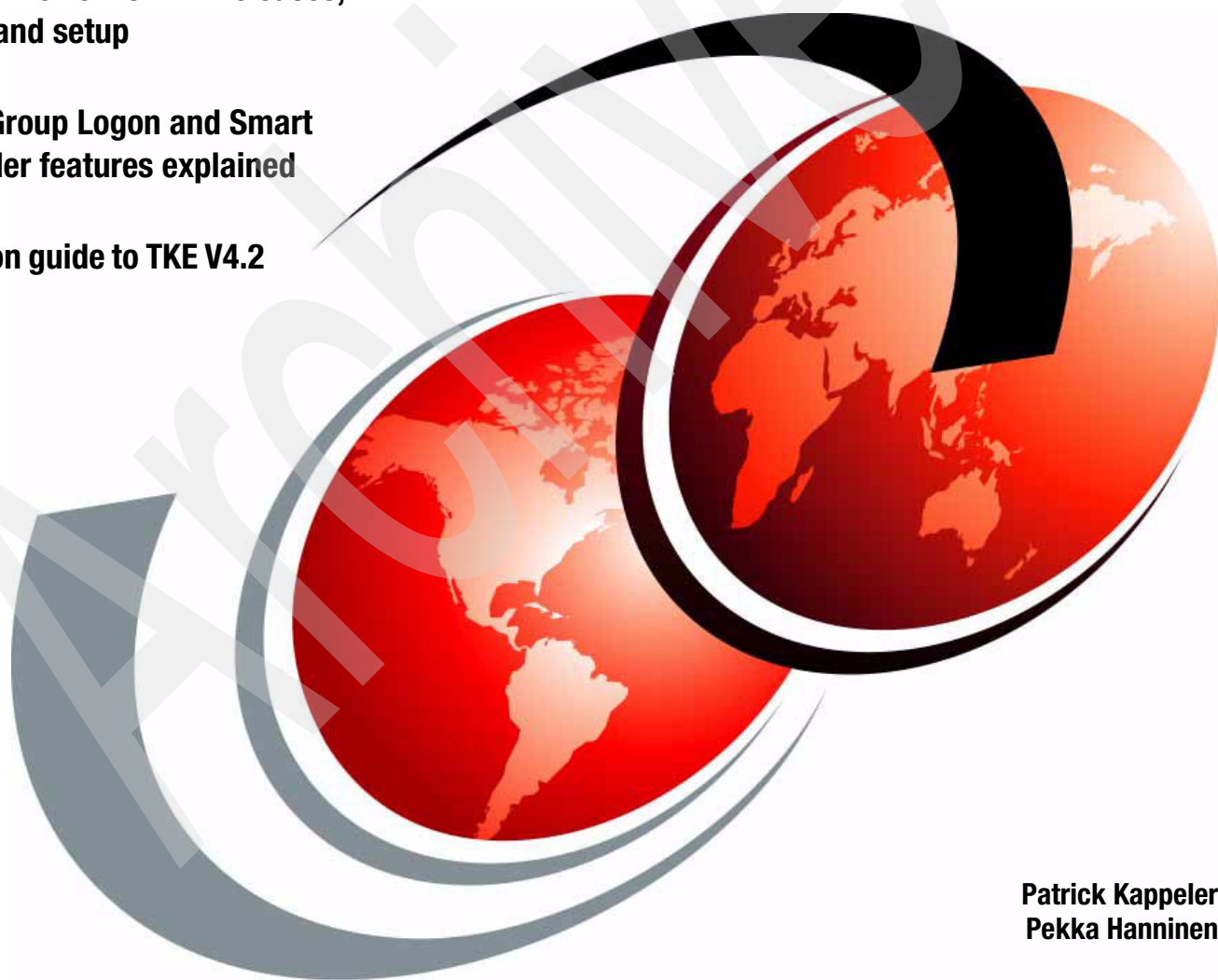


zSeries Trusted Key Entry (TKE) Version 4.2 Update

A technical review of TKE releases, features, and setup

The new Group Logon and Smart Card Reader features explained

A migration guide to TKE V4.2



Patrick Kappeler
Pekka Hanninen

Redbooks



International Technical Support Organization

**zSeries Trusted Key Entry (TKE) V4.2 Installation
Update**

December 2004

Archived

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

Archived

First Edition (December 2004)

This edition applies to zSeries Trusted Key Entry (TKE) Version 4.2.

© Copyright International Business Machines Corporation 2004. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	v
Trademarks	vi
Preface	vii
The team that wrote this redbook.	vii
Become a published author	viii
Comments welcome.	viii
 Chapter 1. A refresher on zSeries Hardware Crypto and the Trusted Key Entry workstation	1
1.1 Background information on the TKE	2
1.1.1 A short history of the Trusted Key Entry workstation	5
1.2 Introduction to the TKE V4 workstation.	6
1.2.1 Reviewing basics of TKE interaction with end users and crypto coprocessors ...	6
1.2.2 Overview of the TKE workstation installation and customization	10
1.2.3 Starting the TKE application	18
1.2.4 Using TKE V4.0 to administer the zSeries secure coprocessors	18
1.3 TKE V4.1	22
1.3.1 TKE enablement for z990 and z890	23
1.4 Overview of the TKE V4.2.	24
1.4.1 z/OS releases	24
1.4.2 TKE hardware	24
1.4.3 TKE software	24
1.4.4 New functions	25
1.4.5 Access control points	26
 Chapter 2. TKE V4.2 Group Logon feature	27
2.1 Group logon feature	28
2.1.1 How to create a group logon environment	28
2.1.2 How to use the Group Logon feature	34
 Chapter 3. Smart Card Support	39
3.1 Smart card feature description	40
3.1.1 Requirements and terminology	40
3.1.2 PKI concepts used in TKE smart card support	41
3.2 How to create the smart card environment	43
3.2.1 Installation of the smart card readers	46
3.2.2 Setting up the zone entities.	46
3.3 Managing changes to the smart card environment	57
3.4 Exploiting the smart card environment	61
3.4.1 Preparing the smart card and 4758 profiles to log on to CNM or the TKE	61
3.4.2 Using the smart card to log on to CNM.	66
3.4.3 Using the smart card to log on to the TKE application	67
3.4.4 Using the smart card to hold a TKE Authority signature key.	68
3.4.5 Using the smart card to store TKE 4758 and zSeries coprocessors keys	72
 Chapter 4. Migrating from previous TKE releases	79
4.1 Migrating from TKE V2 to TKE V4.2	80
4.2 Migrating from TKE Version 3 or higher to TKE Version 4.2.	82

Appendix A. TKE workstation TCP/IP configuration	87
TKE Workstation TCP/IP setup	88
z/OS TCP/IP Host Transaction Program	91
Appendix B. TKE host TCP/IP server setup	93
The main TCP/IP files to check and modify	94
TCPIP.HOSTS.LOCAL	94
TCPIP.DATA	94
TCPIP.PROFILE	94
TKE Host Transaction Program installation	95
CSFTTCP started procedure installation	96
The CSFTTKE module	97
The CSFTHTP3 REXX exec	97
Starting the TKE Host Transaction Program	98
Related publications	99
IBM Redbooks	99
Other publications	99
Online resources	99
How to get IBM Redbooks	99
Help from IBM	100
Abbreviations and acronyms	101
Index	103

Notices

This information was developed for products and services offered in the U.S.A.

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.

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.

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.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.


COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates 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. 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 IBM's application programming interfaces.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM®
OS/2 WARP®
OS/2®
OS/390®

RACF®
Redbooks (logo) ™
Redbooks™
S/390®

VTAM®
z/OS®
zSeries®

The following terms are trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Preface

This IBM® Redbook provides detailed information about the principles of operation and use of new features in the Trusted Key Entry workstation at the Version 4.2 level.

Readers should be familiar with zSeries® hardware cryptography implementation and the purpose and usage of the TKE workstation; however, the first chapter is a refresher of the cryptographic hardware coprocessors that are currently available on the different zSeries models, and the history and setup of the TKE workstation.

New TKE functions such as Smart Card Support and Group Logon are described in terms of implementation and setup, and we give examples of the utilization of these two functions. We also cover the process of migrating from previous TKE releases, and provide examples of TCP/IP setup and configuration for the TKE workstation.

Other redbooks providing more information are:

- ▶ *Exploiting S/390 Hardware Cryptography With Trusted Key Entry*, SG24-5455
- ▶ *S/390 Crypto PCI Implementation Guide*, SG24-5942
- ▶ *zSeries Crypto Guide Update*, SG24-6870
- ▶ *z990 Cryptography Implementation*, SG24-7070

The team that wrote this redbook

This redbook was produced by a team of specialists at the EMEA Products and Solutions Support Center in Montpellier (France).

Patrick Kappeler led this redbook project. He joined IBM in 1970 as a diagnostic programs designer and has held several specialist and management positions as well as international assignments, all dealing with S/390® and zSeries Technical Support. He has been part of the EMEA Products and Solutions Support Center, located in Montpellier (France) since 1996, where his domain of expertise is e-business Security on zSeries. He writes and presents extensively on this topic.

Pekka Hanninen is an IT specialist working with the Integrated Technology Services team in Finland. He has 30 years of experience in IBM Large Systems software. He has worked at IBM for eight years, and his areas of expertise include RACF®, cryptography, and security administration. He holds certificates for CISSP, CISA, and CISM.

Many thanks to the following people for their highly appreciated contributions to this project:

Donyelle Mahler
IBM Poughkeepsie

Victoria Mara
IBM Poughkeepsie

Chris Rayns and Bill White
International Technical Support Organization, Poughkeepsie Center

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions while getting hands-on experience with leading-edge technologies. You will team with IBM technical professionals, Business Partner,s and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us because we want our Redbooks™ to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

ibm.com/redbooks

- Send your comments in an e-mail to:

redbook@us.ibm.com

- Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HYJ Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

A refresher on zSeries Hardware Crypto and the Trusted Key Entry workstation

In this chapter, we provide a short overview of the Trusted Key Entry (TKE), its use, and its evolution since the release of TKE Version 1 in 1997. We then describe the new functions brought by the TKE V4.2 code, which in turn are thoroughly explained in the rest of this paper.

Several redbooks have already addressed, in a broader view, the cryptographic services implementation in the S/390 and zSeries systems and the use of the TKE workstation in this context. Whenever appropriate, we refer to these books in our discussion; however, we expect readers to be familiar, at least at a high level, with the hardware cryptography implementation and management in zSeries and of the z/OS® components that are involved in providing the cryptographic services.

Further information can be found in the TKE utilization reference book *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SA22-7524.

Note: The new zSeries cryptographic coprocessor Crypto Express2 feature (announced October 7, 2004) is internally designated in IBM as *CEX2C*. As this paper is written, it is not clear whether this name will be used in the official IBM documentation. In this paper, we use either *CEX2C* or *Crypto Express2* to designate the same device.

1.1 Background information on the TKE

This section presents an overview of hardware cryptography implementation in the zSeries system. We describe the z/OS components that provide the necessary interfaces to applications to call the cryptographic services, and to security officers to administer the cryptographic coprocessors.

The TKE is one of the options for managing zSeries secure coprocessors in an installation. With secure coprocessors, application keys can be protected when they reside outside of the coprocessor secure enclosure by being encrypted with a master key.

The coprocessors currently in use in zSeries are:

- ▶ The CP Assist for Cryptographic Functions (CPACF) - z990 and z890 only, which is not an actual coprocessor but a hardware facility imbedded in the system's processing units.
- ▶ The PCI Cryptographic Accelerator (PCICA) - all zSeries models - Feature Code 0862. One PCICA feature contains two coprocessors.
- ▶ The PCI Cryptographic Coprocessor (PCICC) - secure coprocessor, on z900 and z800 and 9672 G5/G6 - Feature Code 0860/0861. One PCICC feature on z900 and z800 contains two coprocessors at 16 domains each.
- ▶ The Cryptographic Coprocessor Facility (CCF) - secure coprocessor, on z900 and z800 and 9672 - Feature Code 0800. There are two CCFs available except for uniprocessor models. One CCF has 16 domains.
- ▶ The PCIX Cryptographic Coprocessor (PCIXCC) - secure coprocessor, on z990 and z890 only - Feature Code 0868. One PCIXCC feature contains one coprocessor with 16 domains.
- ▶ The Crypto Express2 coprocessor (CEX2C) - secure coprocessor, z990 and z890 only - Feature Code 0863. (The Crypto Express2 coprocessor will replace the PCIXCC and PCICA coprocessors in the first quarter of 2005.) The Crypto Express2 feature contains two coprocessors at 16 domains each.

The term "*crypto modules*" is also used to designate the coprocessors in the TKE terminology. Figure 1-1 on page 3 gives a high-level description of the z/OS integrated cryptography implementation.

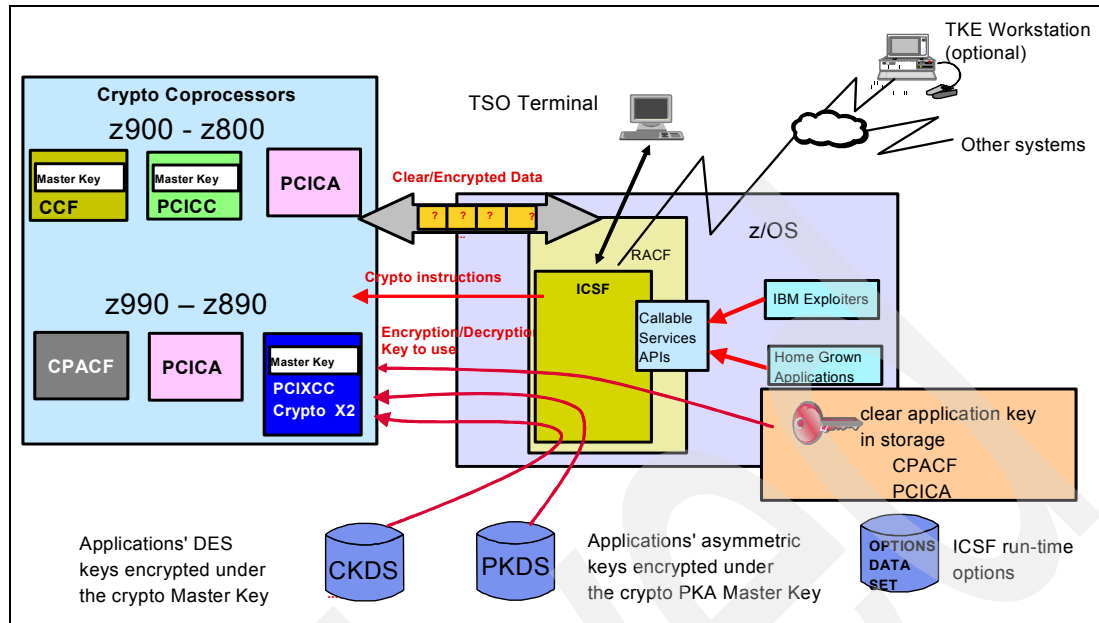


Figure 1-1 Implementation of integrated cryptography in z/OS

- ▶ The exploiters of the cryptographic services call the ICSF (Integrated Cryptographic Services Facility) API. Some functions are performed by the ICSF software without invoking the cryptographic coprocessors; other functions result in ICSF going into routines containing the IBM proprietary crypto machine instructions. Note that the CPACF feature of the z990 or z890 systems can also be accessed directly by applications using problem state instructions that drive the CPACF and have been published in the zSeries Architecture Principle of Operations.
- ▶ These crypto instructions, which are executed by a CPU engine, result in a work request being generated for a cryptographic coprocessor.
- ▶ The crypto coprocessor is provided with the following:
 - Data to encrypt or decrypt from the system memory.
 - The key used to encrypt or decrypt provided by ICSF as per the exploiter's request. Note that these application keys are kept outside the coprocessors encrypted under the master key, except for those functions that are using clear keys. An application key encrypted with the master key is said to be in the "operational" form.
 - Physically, these keys can be stored, encrypted with the master key, in ICSF-managed VSAM data sets and pointed to by the application using the label they are stored under. The Cryptographic Key Data Set (CKDS) is used to store the symmetric keys in their operational form, and the Private Key Data Set (PKDS) is used to store the operational asymmetric keys. The application also has the capability to provide an encrypted encryption key or a clear encryption key directly in memory (that is, to be used *as is*) to the coprocessor.

There is a need to install and maintain the Master keys in the coprocessor, acknowledging that the master key is the installation's most critical secret because it is the ultimate protection for the application keys. Master key management is expected to be done by the installation's Security Officers by using the ISPF administration panels delivered with ICSF, or by using the optional Trusted Key Entry (TKE) workstation to perform with maximum security the highly sensitive processes involved in the installation and maintenance of the master keys and operational keys.

The TKE workstation is an optional, priced feature. It offers a secure, remote, and flexible method of providing master keys and operational keys parts entry and to remotely manage secure cryptographic coprocessors over a non-secure TCP/IP network. The TKE itself has a secure cryptographic coprocessor and utilizes Digital Signature, the Diffie-Hellman key exchange protocol, and Triple-DES functions to provide a highly secure, auditable, and remote method of key entry over a TCP/IP network.

ICSF TKE support is available only if at least one secure coprocessor is enabled on the system. Consequently, ICSF executing on a z990 or a z890 system without at least one PCIXCC or Crypto Express2 feature does not provide any TKE support.

As this book is written, Linux® for zSeries does not provide an API to use the zSeries coprocessors' secure functions. Instead, Linux for zSeries provides access to functions that do not require a master key to be set in the coprocessors. Therefore the use of a TKE is not relevant to Linux for zSeries hardware cryptography.

Refresher on master keys:

- ▶ Master keys are installed in *domains* in the secure coprocessors. There are 16 physical domains per coprocessor, with each domain allocated to a logical partition (LPAR) that runs z/OS. Therefore, up to 16 active LPARs can share a secure coprocessor, with each partition preserving the secrecy of its own master key because it is set in a physically distinct set of registers dedicated to this very partition.
- ▶ There are actually two master keys per domain in a secure coprocessor: the symmetric master key used to encrypt the DES and Triple DES keys, and the asymmetric master key used to encrypt the RSA private key. (Previously, the Digital Signature Standard private key was also included, but DSS support has been dropped with z990 and z890.) A CKDS and PKDS are bound to the value of the master keys in the coprocessor, as all encrypted keys kept in these VSAM datasets can be decrypted only if the coprocessor's current master key is the one that has been used to encrypt the application keys in the CKDS.
- ▶ All of the symmetric master keys must be the same in all of the coprocessors that an instance of ICSF has access to (that is, in the coprocessor domain ICSF is working in). It is the same for all of the asymmetric master keys.
- ▶ A master key is entered in a coprocessor via either the ICSF ISPF panels or TKE in several parts, splitting the master key secret among several security officers who know only their own part of the master key. There must be at least two parts to a master key.

Note: Strictly speaking, although the PCICA coprocessor does not have master keys, it has 16 "domains," which are actually 16 work queues to accommodate requests received from 16 different LPARs.

Enablement of zSeries Integrated Cryptography

By default, hardware cryptography does not come active with the system; it requires ordering a specific Feature Code, which comes as a diskette or CD to install in the system's Support Element to enable the hardware cryptography. Today's orderable Feature Codes also include enablement of the communication between the secure coprocessors and the TKE workstation, if installed. However, since the May 2004 LIC release for z990 and z890, TKE communication with the coprocessors is additionally controlled by a user selection to be made at the system SE/HMC. This is described in 1.3.1, "TKE enablement for z990 and z890" on page 23.

9672, z900, and z800

CCF cryptographic hardware enablement becomes effective after the Power On Reset that follows the installation of FC 0835 for 9672 and FC 0875 for z900 or z800. PCICC enablement requires that CCF be enabled already but is concurrent with system's operations. However, it requires installing an additional diskette FC 0865 with the first PCICC. The PCICC features are hot-pluggable. The PCICA feature is hot-pluggable and only requires CCF to be enabled, without any additional enablement action.

z990 and z890

The complete set of hardware cryptography coprocessors is enabled when the FC 3863 CD has been installed. The Feature Code installation is concurrent with system operations, and the PCICA, PCIXCC, and Crypto Express2 features are all hot-pluggable.

1.1.1 A short history of the Trusted Key Entry workstation

The ancestor of the TKE was the frame-mounted manual-control panel provided with the ICRF (Integrated Cryptographic Facility) feature in the bipolar ES9000 systems. This panel was used by a security officer standing at the system, entering the master key (there was actually only one master key per domain at this time) or operational keys parts. The panel was physically wired to the crypto TCM using a very expensive tamper-resistant cable. The cable consisted of parallel wires and several layers of metal shielding to protect transmission from eavesdropping. The cable was also protected against physical intrusion, such as breaking or cutting the cable, which triggered the tamper indicator when detected. Protection was also provided against attacks utilizing low temperature and ionizing radiation.

With the advent of the hardware cryptography on the 9672 CMOS systems, security officers still had to enter Master keys and operational keys parts, but the concept of the tamper-resistant cable was revisited and it became a cryptographically secured network connection between a special workstation and the cryptographic coprocessors called *PKSC* for Public Key Secure Cable. The network connection was relayed to the coprocessors by only one instance of ICSF in the system (meaning that other instances of ICSF can run in other LPARs, but are not involved in communicating with the TKE).

Note: A single TKE can be used to administer the crypto coprocessors in several physical systems if it has TCP/IP connectivity to these systems, and one instance of ICSF and of the TCP/IP listener is running in each of them. A single TKE can also be used to administer all of the domains in the coprocessors of a single system if one instance of ICSF and of the TCP/IP listener runs in one LPAR.

TKE V1/V2 (1997 to 2000)

The TKE V1 and V2 workstation was OS/2®-based and communicated with ICSF using VTAM® APPC over an SNA network. Two LAN attachments (token-ring or Ethernet) and a Wide Area Connection (a modem attachment) were offered.

The TKE workstation used a 4755 cryptographic adapter internally to sign and encrypt communications with the coprocessors and, optionally, could be attached to an IBM smart card reader attachment, the IBM 4754 Security Interface Unit with IBM proprietary Personal Smart Card (PSC) technology. The TKE was used to administer the CCF, the only coprocessor that was available then.

This TKE version is described in the redbook *Exploiting S/390 Hardware Cryptography With Trusted Key Entry*, SG24-5455.

TKE V3 (2000)

With the introduction of the PCICC card for the 9672 G5/G6 system, the TKE workstation code has been enhanced for remote administration of the PCICC coprocessors along with CCF administration. The TKE also evolved internally:

- ▶ It now uses an IBM 4758-002 cryptographic adapter.

Note: Under special conditions and with proper information given to the users, IBM may provide TKE workstations that contain a 4758-023 Cryptographic Adapter instead of the 4758-002 CA. The 4758-023 is functionally equivalent to the 4758-002 but is certified at FIPS 140-1 level 3 only.

- ▶ There is no more support for smart cards.
- ▶ The only supported network is TCP/IP with a token-ring LAN attachment (FC 0866) or Ethernet attachment (FC 0869). The Wide Area Connection is no longer available.
- ▶ The TKE V3.1 also implemented the concept of hardware access control points in the PCI coprocessors. Access control points are addressed in further detail in Chapter 2, “TKE V4.2 Group Logon feature” on page 27.

This TKE version is described in the redbook *S/390 Crypto PCI Implementation Guide*, SG24-5942.

1.2 Introduction to the TKE V4 workstation

Many features that are described here were already available in TKE V3.x, but we include them for background information.

1.2.1 Reviewing basics of TKE interaction with end users and crypto coprocessors

With the introduction of the PCIXCC card for Z990 at GA 2, a new TKE code level V4.0 was released to support remote administration of PCIXCC. This TKE code release is described in *z990 Cryptography Implementation*, SG24-7070. It presents the following characteristics:

- ▶ The cryptographic functions in the TKE V4.x are performed by an IBM 4758 model 002 or 023 cryptographic coprocessor installed in the workstation (same as TKE 3.X).
- ▶ The graphical interface has also been revised, so users should find the module management panels and menus of the TKE V4.x application friendlier to use.
- ▶ Upgrading 3.X to 4.x is done by updating code in the workstation with the CD FC 0851. Note that old TKE V2.x (based on 4755 cryptographic adapter) hardware cannot be upgraded to TKE 4.x; a new workstation must be shipped.

TKE workstation access control

TKE operations rely on the capability to use the imbedded 4758 cryptographic adapter. The 4758 implements an access control mechanism that uses the *roles* and *profiles* concept (Figure 1-2 on page 7). When necessary, these roles and profiles are defined by the TKE administrator using the Crypto Node Management (CNM) software facility and according to customer security policy. This facility, included in TKE code, is started from an OS/2 window session as shown in Figure 1-6 on page 15, and requires proper user authentication and corresponding privileges to access the administrative functions.

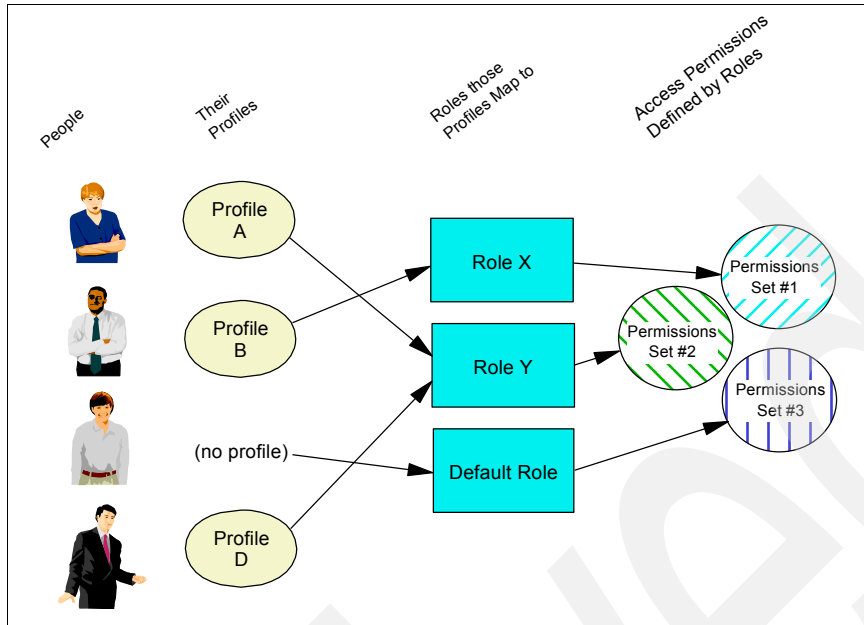


Figure 1-2 Role-based access control

Role

A role defines a class of TKE users who can execute a set of the 4758 cryptographic adapter operations. When creating or changing a role, the TKE administrator will define the TKE 4758 Crypto card commands that will be authorized for users who are mapped to this role.

The TKE 4758 has a DEFAULT role. Use of the DEFAULT role does not require a user profile. Any user can use the services permitted by the DEFAULT role without logging onto or being authenticated by the coprocessor. However, the DEFAULT role is obviously limited in the operations it is allowed to perform.

Note: Predefined roles are set up during TKE initialization, and there is no need to change these roles for normal use of the TKE application, as shown in Figure 1-5 on page 14.

Profile

A profile defines a specific user. It contains a user name and passphrase information and is mapped to only one role, though as many profiles as needed can be created and mapped to the same role.

After logging on under a profile, the TKE user can perform only the commands authorized by the role mapped to the profile. Validity dates may also be defined on a role basis to enforce specific security policies.

Default profiles are set up during TKE initialization and have a default known passphrase. We recommend that you change this passphrase after TKE setup to ensure full access security.

The TKE administrator must create all user profiles required by the security policy in effect (Figure 1-8 on page 16).

Important: The PCI coprocessor in the zSeries systems uses a similar access control concept that also involves roles and authorities. However, these roles and authorities must not be confused with TKE 4758 roles and profiles.

User logon to the TKE

The user logs on to the TKE providing a user ID and a passphrase. The user ID is actually a TKE 4758 user profile, and if the passphrase is correct the TKE user is logged in and can invoke this role's authorized 4758 functions.

An unsuccessful or anonymous logon gives access to the TKE 4758 operations in the DEFAULT role.

A successful logon in the TKEUSER role enables communication with the zSeries system coprocessors for administrative purposes if the correct authority signature key is used.

Security of the communication with the host zSeries system coprocessors

TKE security consists of separate mechanisms to provide integrity and secrecy. At initialization time, security is built up in stages:

1. Integrity of the crypto module
2. Integrity of the authorities
3. These integrity mechanisms used as part of the process to establish secrecy

The authenticity of the commands issued by an authority at the TKE workstation to a crypto module is established by digitally signing the command. The command is signed by the TKE workstation using the secret RSA signature key of the authority. It is verified by the crypto module using the public RSA key of the authority previously loaded into the crypto module. In the same way, the authenticity of the reply from the crypto module to the TKE workstation is digitally signed. The reply is signed by the crypto module using its own secret RSA key and verified by the TKE workstation using the crypto module's public RSA key. To eliminate the possibility of an attacker successfully replaying a previously signed command or reply, a sequence number is included in all signed messages. Sequence numbers are maintained for each crypto module and for each authority communicating with that crypto module.

Additional definitions

Authorities

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

Authority signature key

An authority signs commands by using the secret key of its signature key pair, and the crypto module verifies the signature by using the public key of the same RSA key pair. Before signing and verifying command signatures, the signature key pair must be generated, the secret key must be associated with the authority, and the public key must be sent to the crypto module. All authorities have a public exponent value of 65537.

Authority default signature key

During the crypto module initialization, the public key of a default signature key pair is loaded into the crypto module. The secret key of the default signature key pair is known to the TKE workstation and used until valid authority signature keys are generated and made known to the crypto module. You can reload the public key of a default signature key pair to the crypto module. For CCF, the same default signature key is assigned to authorities 0-13. Authorities 14 and 15 have their own unique default signature keys.

Attention: Authorities 14 and 15 cannot be used for signing CCF commands until their default signature keys have been changed. Either these authority signature keys must be changed or they should not be defined in the Signature Requirements Array as authorized or required to sign commands. For PCICC and PCIXCC/CEX2C, the initialization process creates the authority 00 and assigns the authority default signature key to this authority.

Crypto module signature key

The replies from each crypto module are signed by a crypto module signature key, which is a unique RSA key for each crypto module. The public modulus part of this RSA key is called the crypto module public modulus (CMPM) and can be displayed. The public exponent for all crypto module RSA keys is a fixed value of 65537. The RSA signature key is loaded into the crypto module during the manufacturing and initialization processes. The public part of the RSA key is sent to the TKE workstation at the first communication between the crypto module and the workstation.

Multi-signature commands

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

Cryptographic Coprocessor feature

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

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

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

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

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

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

PCI X Cryptographic Coprocessor and CEX2C Coprocessor feature only

PCIXCC/CEX2C single-signature commands for operational keys (since TKE 4.1):

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

TCP/IP connectivity

The TKE workstation V4.0 communicates with the host system using the TCP/IP network via a token-ring or Ethernet adapter card (Figure 1-3). The TKE z/OS host must run, on top of TCP/IP and ICSF, a TKE Host Transaction Program that listens over a dedicated TCP/IP port and serves the requests issued by connected TKEs.

Refer to “TKE Workstation TCP/IP setup” on page 88 for details about the TCP/IP configuration in OS/2 and the ICSF listener program.

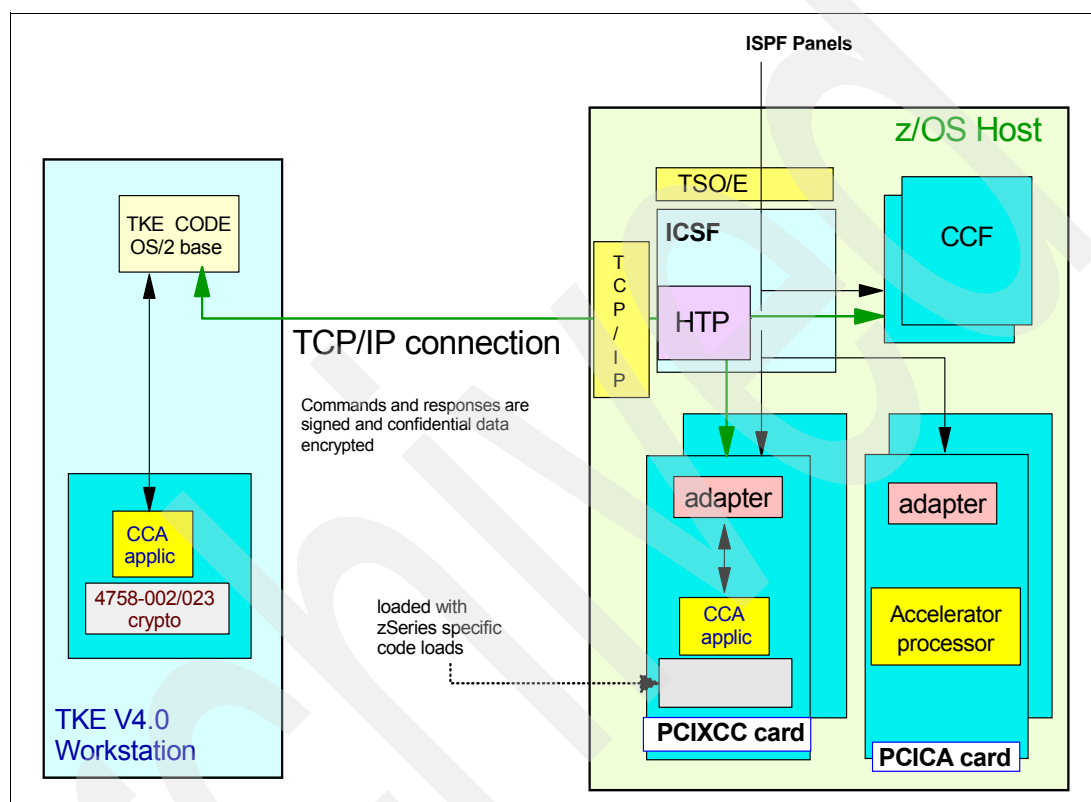


Figure 1-3 TKE workstation in PCIXCC environment before using the new TKE

1.2.2 Overview of the TKE workstation installation and customization

Some definitions first:

CNM (Cryptographic Node Management) utility

A Java™ application that provides a graphical user interface to initialize and manage the TKE 4758 cryptographic adapter.

CNI (Cryptographic Node Initialization) utility

A utility within CNM that automates some of the functions of CNM. It is used to initialize and set up the TKE 4758 cryptographic adapter.

TKE master key

The TKE IBM 4758 card contains one master key (referred to as the DES Master Key) to encrypt the TKE operational DES keys, and one master key (referred to as the PKA Master Key) to encrypt the PKA keys to be stored on the TKE hard disk in the DESSTORE.DAT and PKASTORE.DAT files (also named TKE keystores). The CNM utility is used to set these two master keys.

You enter the DES Master Key in several key parts loaded by different key officers (generally, two officers) through the CNM utility. The entered key parts can be imported from a file, manually keyed, or randomly generated.

After the last master key part is loaded, the officer sets the master key via the CNM utility, which causes both the DES Master Key and the PKA Master Key to be set from these key part values in the TKE 4758. Then the officer uses CNM to encipher or re-encipher the key storages.

TKE workstation key storage

This consists of files on hard disk that store the operational keys encrypted under the TKE IBM 4758 master key. When these keys are needed, they are loaded into the 4758 secure hardware so that they never appear in clear outside of the TKE 4758 secure hardware.

There are two key storage files implemented in the TKE:

- ▶ DES key storage to store symmetric keys (C:\ibm4758\DESSTORE.DAT)
- ▶ PKA key storage to store asymmetric keys (C:\ibm4758\PKASTORE.DAT)

TKE workstation setup

During the manufacturing process, the TKE workstation application is installed onto the PC hard disk. The CCA code segments 1, 2, 3, and FCV (Functions Control Vector) are also loaded into the TKE 4758-002 or 4758-023 cryptographic adapter.

The TKE is then tested. Just before shipment, the cryptographic coprocessor card IBM 4758 is removed from the workstation and shipped in a special thermal-protected container. When received at the customer location, an IBM representative plugs it into the TKE workstation.

Note: When manipulating the 4758 card, *never* remove the batteries; otherwise, the tamper-protection mechanism will definitively disable the card.

The following are shipped along with the workstation:

- ▶ A CD-ROM containing the TKE code
- ▶ A TKE backup diskette
- ▶ A TKE binary diskette
- ▶ *Maintenance Information For Desktop Consoles*, GC38-3115

The TKE workstation application can be reloaded from the TKE CD-ROM and the previously saved backup diskette. When upgrading from TKE3.x to 4.0, customized data is saved on TKE backup diskette and binary backup diskette before installing new code from the CD.

Note: If for any reason the IBM 4758 Crypto card has to be replaced, then the internal CCA code segments 1, 2, and 3 have to be reloaded because new spare 4758 cards only have the minimum code bootstrap loaded at the card manufacturing plant. It will also be necessary to reload the FCV. You can accomplish this using the procedure described in *Maintenance Information for Desktop Consoles*, GC38-3115, to load the code files and FCV file that are kept on the workstation hard disk.

TKE customization

The TKE workstation is shipped from manufacturing with code already loaded and parameters set in default values. Customization has to be performed at the customer's

location to match the production environment requirements and policies. This is schematically described in Figure 1-4.

1. Step one defines TKE authorities (administrator, keymen), sets the TKE Master Key, and defines TKEUSER profiles (people who will manage host cryptographic processors). TCP/IP connection parameters to the host partition must also be entered (see “TKE Workstation TCP/IP setup” on page 88).
2. Step two defines and customizes host names, Host PCIXCC and Crypto Express2 authorities, and access control parameters. If several TKEs access the same cryptographic coprocessors, authorities and access control must be defined only from the first installed TKE.
3. If G5/G6/Z800/Z900 cryptographic coprocessors also have to be controlled from the TKE. (Refer to the redbook *zSeries Crypto Guide Update*, SG24-6870.)

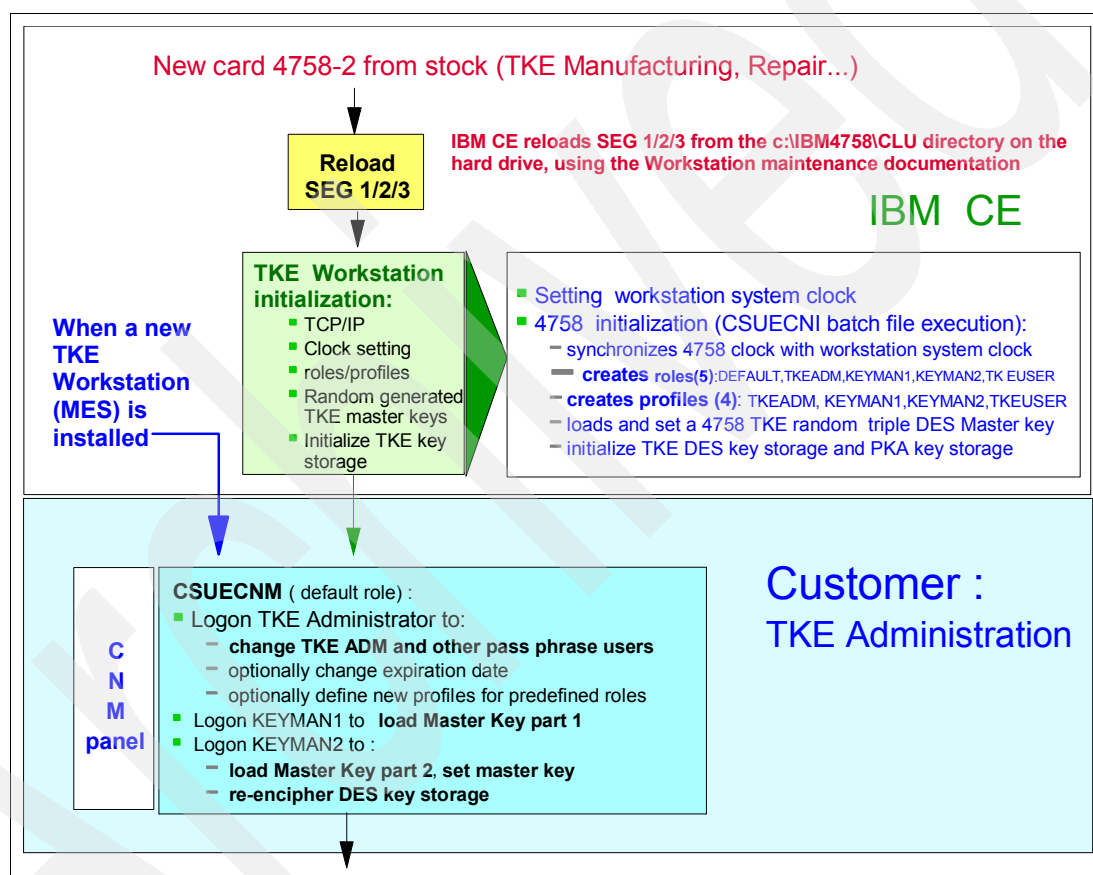


Figure 1-4 TKE V4.0 internal card 4758 setup process data flow, part 1

Details about the TKE workstation 4758 setup

TKE workstation initialization must be done when installing a new TKE or after a TKE misuse, when there is no TKE role or profile available to manage the TKE and no backup diskettes are available.

Normal restoration of a failing TKE must be done using the CD and the backup diskettes.

Important: If the workstation you are working on is already in use, and if some keys are already stored in key storages, then ensure that you have a backup copy of *both* key storage files and the TKE 4758 card master keys parts.

Otherwise, you will not be able to recover the keys in the key storage. Refer to *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SA22-7524, for further information.

TKE workstation initialization

This step is performed at the manufacturing location before the TKE is shipped and does not have to be done again when you receive the TKE. However, it can be re-executed without any problem.

The description of the actual TKE customer.setup begins at “TKE access control administration” on page 14.

To start TKE workstation initialization, enter the following from the OS/2 window:

```
c:\ibm4758\cnm\csuecni c:\tke\4758access\4758initialize.cni
```

This CSUECNI command runs the batch file 4758initialize.cni, which performs the following:

1. Sets the 4758 clock.
2. Creates five TKE predefined roles (shown in Figure 1-5 on page 14).
 - The DEFAULT role enables you to view roles and profiles and to reinitialize the 4758. This is publicly accessible, and no passphrase is needed. (Simply press Cancel when prompted for profile name and passphrase.)

Important: Initializing from the CNM panel (selecting **Crypto node** → **Initialize**) erases all setup done by the 4758initialize.cni batch file. If this option is used, you will have to run the TKE initialization batch file again.

- The TKEADM role is the predefined 4758 administrator role that enables the user to perform security administration for the TKE workstation and to create, change, or delete TKE roles and profiles.
- The KEYMAN1 role enables you to clear the TKE 4758 new master key register and to load the first master key part.
- The KEYMAN2 role enables you to load the middle and last master key parts, to set the master key, and to re-encipher the TKE key storage.
- The TKEUSER role (the TKE general user role) enables communication with and management of the host Crypto modules. This role is also used by the 4753 migration facility.

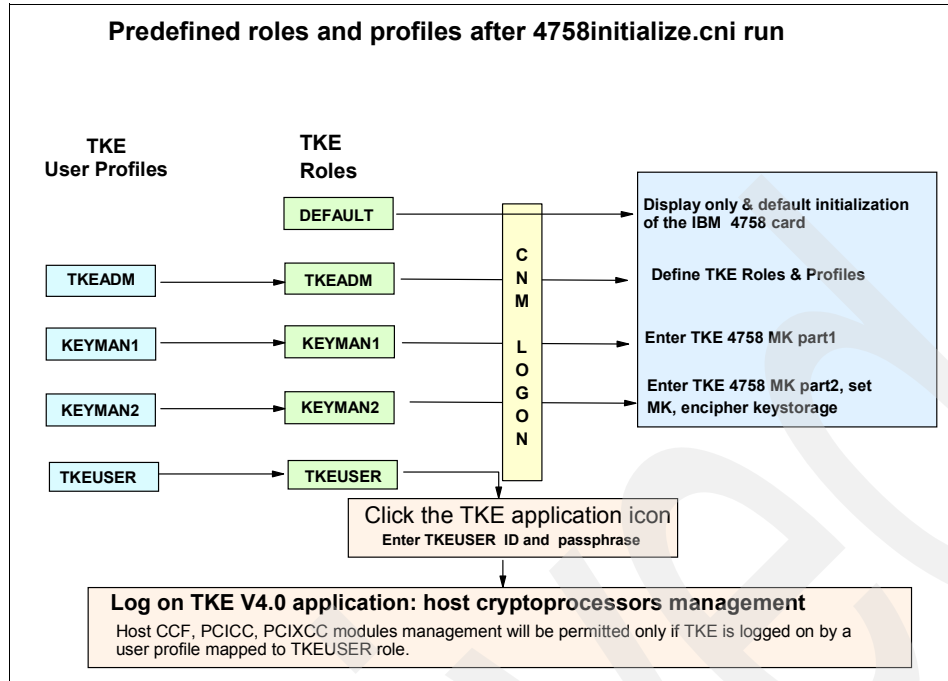


Figure 1-5 TKE workstation predefined roles and profiles

3. Creates four TKE predefined profiles, as shown in Figure 1-5:
 - The TKEADM profile is mapped to the TKEADM role, with the passphrase TKEADM.
 - The KEYMAN1 profile is mapped to the KEYMAN1 role, with the passphrase KEYMAN1.
 - The KEYMAN2 profile is mapped to the KEYMAN2 role, with the passphrase KEYMAN2.
 - The TKEUSER profile is mapped to the TKEUSER role, with the passphrase TKEUSER.
4. Loads and sets a TKE IBM 4758 random DES Master Key.
5. Initializes TKE DES key storage and TKE PKA key storage.

TKE access control administration

This step is used to change the TKE user profiles' default passphrases and replace the IBM 4758 master key that was randomly generated during the TKE initialization process, as no backup is available to recover this key and it is not proper setup for a production environment. These tasks are executed using the Cryptographic Node Management (CNM) utility, a basic application delivered with the IBM 4758 cryptographic coprocessor. Only a subset of the CNM functions is required to customize the TKE and to manage the workstation application.

Note: We strongly recommend that you do *not* use other CNM functions, as this can lead to unpredictable results. In particular, the CNM Initialize function must not be confused with the previously described TKE initialization. Refer to the IBM 4758 PCI Cryptographic Coprocessor CCA Support Program installation manual for additional details on CNM.

To start the CNM utility (Figure 1-6 on page 15), enter the following command from an OS/2 window:

```
C:\ibm4758\cnm\CSUECNM
```


Beginning in TKE V4.2, you can also use the CNM icon in the TKE folder.

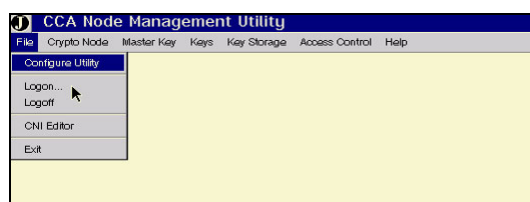


Figure 1-6 TKE workstation CNM utility panel

When the CNM utility is started, only the DEFAULT role commands are permitted. As previously mentioned, the DEFAULT role enables you to display only roles and profiles and to initialize the 4758.

CNM TKE administrator logon

From the menus on the CNM panel, select **File** → **Logon**. Enter the user ID TKEADM and the passphrase TKEADM (these are the default values set at TKE initialization), as shown in Figure 1-7. Note that the user ID and passphrase are case-sensitive.

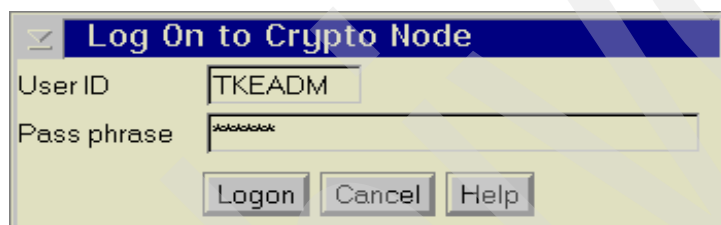


Figure 1-7 CNM utility logon as default TKEADM user with default passphrase

After logon, the TKE administrator should change the passphrase and may also change the activation and expiration dates for the TKEADM profile. For detailed information on how to edit profiles, refer to the IBM 4758 PCI Crypto Coprocessor CCA Support Program manual.

At this time, the administrator should also change the default passphrases in the other predefined profiles and, if needed, create new user profiles mapped to the predefined roles.

To create or change profiles, select **Access Control** → **Profiles** and **New** (to create a new user profile) or **Edit** (to modify a selected existing profile). The administrator must fill in the panel with the information about the new user and the passphrase. (The passphrase may be typed in by the user.) The administrator must also define which role is attributed to this user, as shown in Figure 1-8 on page 16.

Most of the new user profiles will be mapped to the predefined TKEUSER role, as this is the only predefined role permitted for communication with the host Crypto modules.

In our example, we decided to keep the default TKEUSER user ID and passphrase. You may prefer to change this in accordance with the customer security policy at your site.

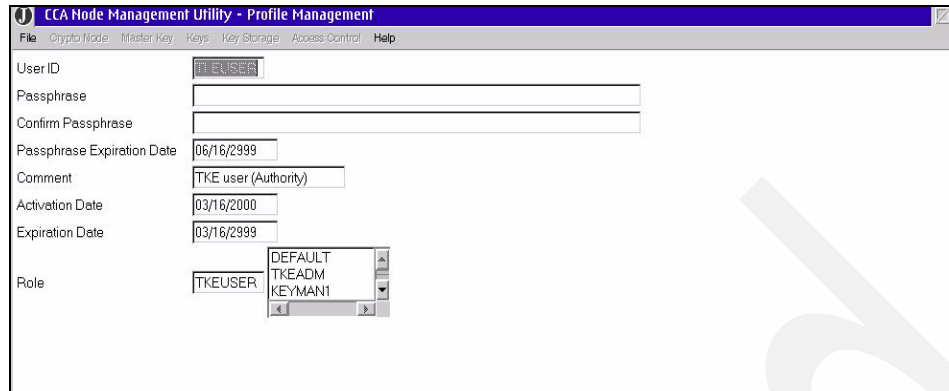


Figure 1-8 TKE workstation profile example: TKEUSER default profile

To create or change roles, select **Access Control** → **Roles** and **New** (to create a role) or **Edit** (to change a selected existing role). Figure 1-9 shows an example.

As explained in “Details about the TKE workstation 4758 setup” on page 12, normally there is no need to change or create roles for the TKE workstation IBM 4758 card because the required functions are already permitted in the predefined roles. However, you can use this as an opportunity to change the validity days specification.

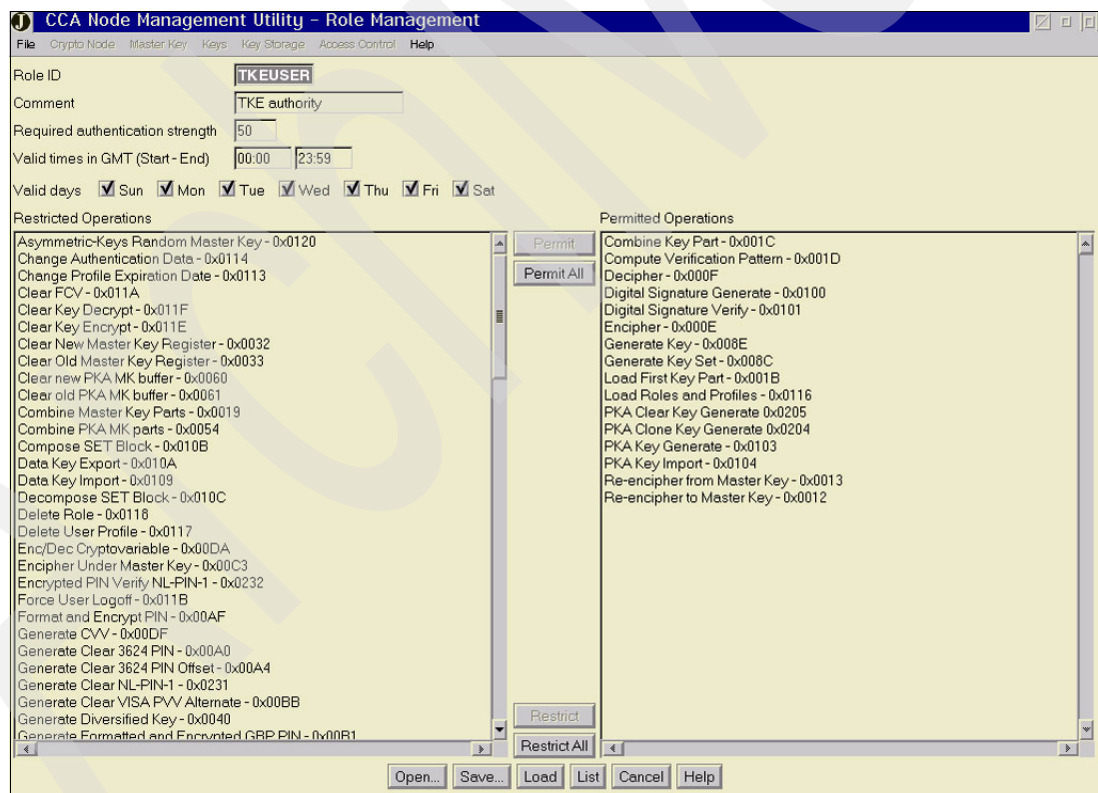


Figure 1-9 TKE workstation role example: TKEUSER default role

As shown in Figure 1-9, the left column of the role panel shows the unauthorized operations and the right column shows the operations that are permitted to the role. You can move operations from one column to the other, according to the specific requirements of your site—but keep in mind that any change in the roles default commands setup may produce

unexpected results when using TKE to manage host crypto modules. Valid days of the week can be also selected.

When the creation or modification of roles, profiles, and passphrases is complete, the TKEADM user ID logs off from the Crypto node using **File** → **Logoff**.

Setting the TKE 4758 master keys

The operating procedure is described in *z990 Cryptography Implementation*, SG24-7070, and in *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SA22-7524.

Customization of the tke.ini parameters

You can customize several parameters by editing the tke.ini file.

1. Issue this command:

```
cd tke\tke
```

2. Using E, edit the tke.ini file:

- Blind key entry option:

This option masks the key parts as they are entered at TKE when working with the host system Crypto modules. If it is required by the security policy, you will have to add the following statement if it does not already exist:

```
BLIND_KEY_ENTRY=TRUE
```

- TRANSPORT_KEY_POLICY (keys used to protect TKE-to-host transactions)

This option selects the default key transport policy. The allowed values are 1, 2, or 3. This value is more convenient to change from the TKE main application panel function (Figure 1-10).

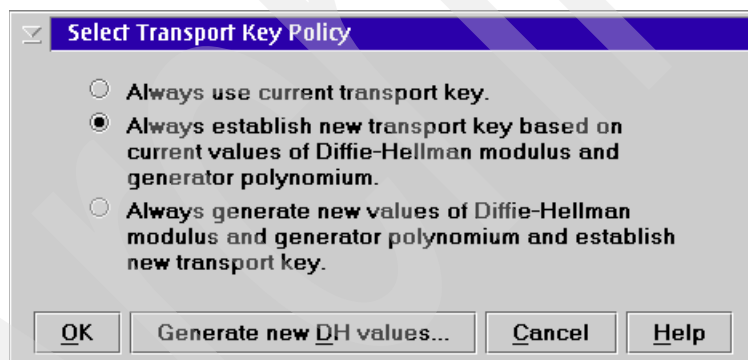


Figure 1-10 Define key policy on main TKE panel

- DEFAULT_DIRECTORY

This option specifies the default directory for saving an authority signature or a key part. Initially this is set to default; it will be changed the first time you save a key to a binary file.

- SERIALIZE_PATH

This option specifies where the TKE saves internal information about hosts and groups. The files HOST.DAT and GROUPS.DAT are saved there.

- MESSAGE_PATH

This option specifies the directory where TKE (on user request) saves the error information in a file named TKE.MSG.

- If your security policy requires that generated keys be saved to diskette and not to the hard drive, you must enable the FLOPPY_DRIVE_ONLY feature.

This function forces generated key parts to be saved on floppy diskettes. Make sure it is set to FLOPPY_DRIVE_ONLY=TRUE.

3. Save the file and close the OS/2 window.

1.2.3 Starting the TKE application

TKE initialization and setup is now complete. You can start the application by opening the TKE folder and double-clicking the TKE V4.0 icon.

Proper TKE 4758 roles must be given to the TKE users who will administer the zSeries systems secure coprocessors (the TKEUSER role or equivalent). The coprocessors have to be set up to authenticate and handle commands arriving from the TKE Authorities. This is explained in *z/OS Cryptographic Services ICSF TKE Workstation User's Guide, SA22-7524*.

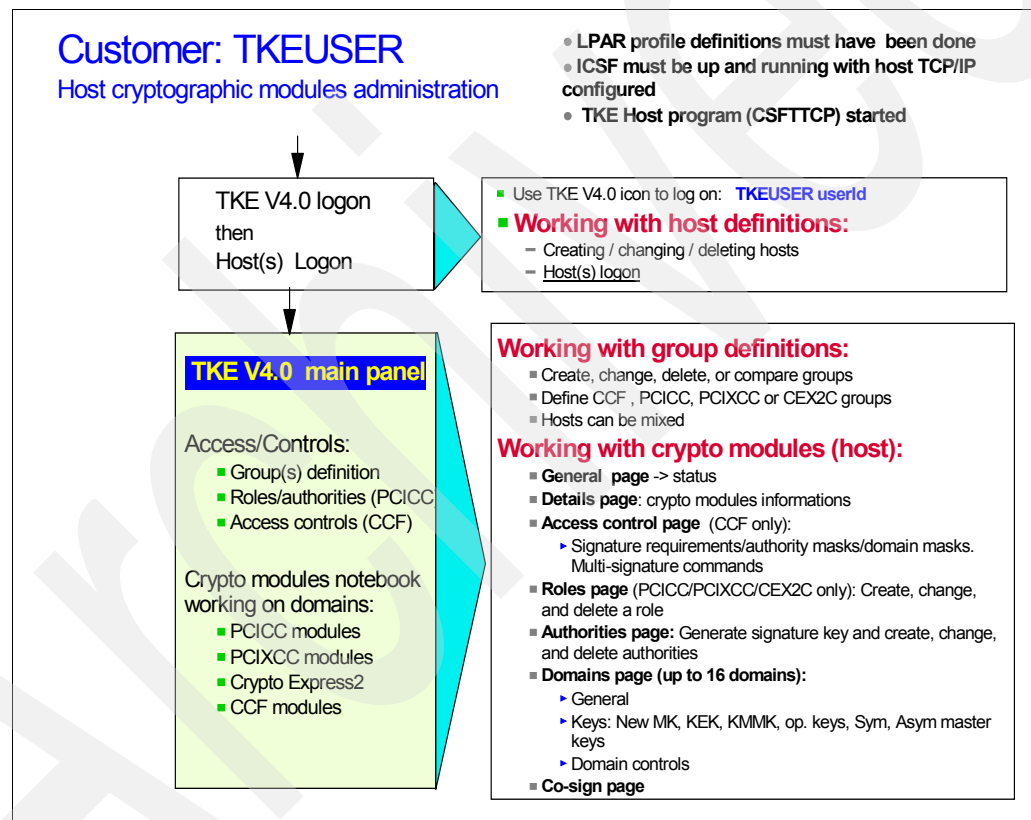


Figure 1-11 Host definitions, host CCFs, PCICC, and PCIXCC/Crypto Express2 customization

1.2.4 Using TKE V4.0 to administer the zSeries secure coprocessors

Refer to *z/OS Cryptographic Services ICSF TKE Workstation User's Guide, SA22-7524*, and redbook *z990 Cryptography Implementation, SG24-7070*.

Important: The TKE V4.0 code does not support entering operational keys in PCIXCC from the TKE, as is possible for other secure coprocessors. This support is added in TKE V4.1, as described in the next chapter.

Access control points

Access to CCA services provided by the PCI coprocessors can be controlled by access control points at TKE code V3.1 and OS/390® V2R9 and above. Note that the availability of access control points is not tied to the TKE release but to the ICSF release; however, you have to be at TKE V4.0 or higher to control the access control points in the PCIXCC or the Crypto Express2 coprocessors.

Access control points are defined in the PCI coprocessor DEFAULT role, the role under which the coprocessor executes the ICSF requests, for each domain. They can be thought of as switches enabling or disabling access to the command processors that provide the requested CCA service, and working inside the coprocessor hardware, as opposed to software-controlled access using the CSFSERV class of profiles in RACF or equivalent.

Switching an access control point between the enabled and disabled state can be done only by using a TKE workstation or in the domain controls panel (Figure 1-12), where all recognized access control points are listed with the related CCA service name.

Note: A non-TKE installation will not acknowledge the access control points that appear as enabled to the PCICCC, PCIXCC, or Crypto Express2 coprocessors, except for the access control point of the DKG-DALL service (Diversified Key Generate for all key types), the DSG Zero-pad Unrestricted Hash Length, and the UDX access control points that come disabled and require a TKE to enable access to the service.

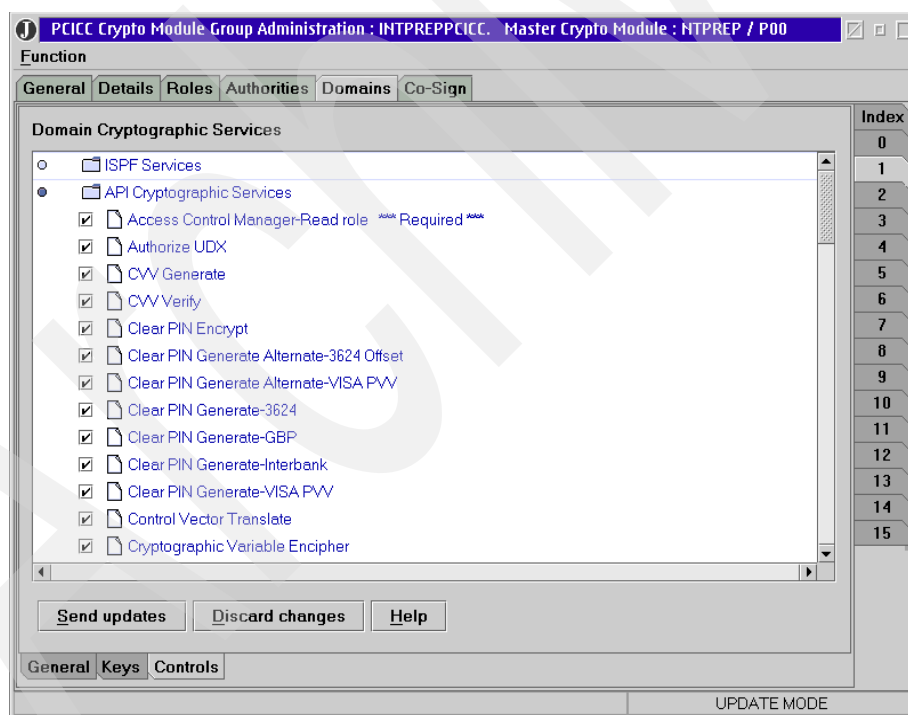


Figure 1-12 Callable services access control points in domain controls

Selecting the individual check box flips the access control point between the enabled or disabled state in the TKE display. The new state is actually recorded into the PCICCC domain with the Send updates button if the authority's role has domain controls and proper domain access permissions.

Figure 1-13 shows the access control point for Symmetric Key Generate PKCS-1.2 in the disabled state. A short test program performing the Symmetric Key Generate ends with an error code, as shown in Example 1-1.

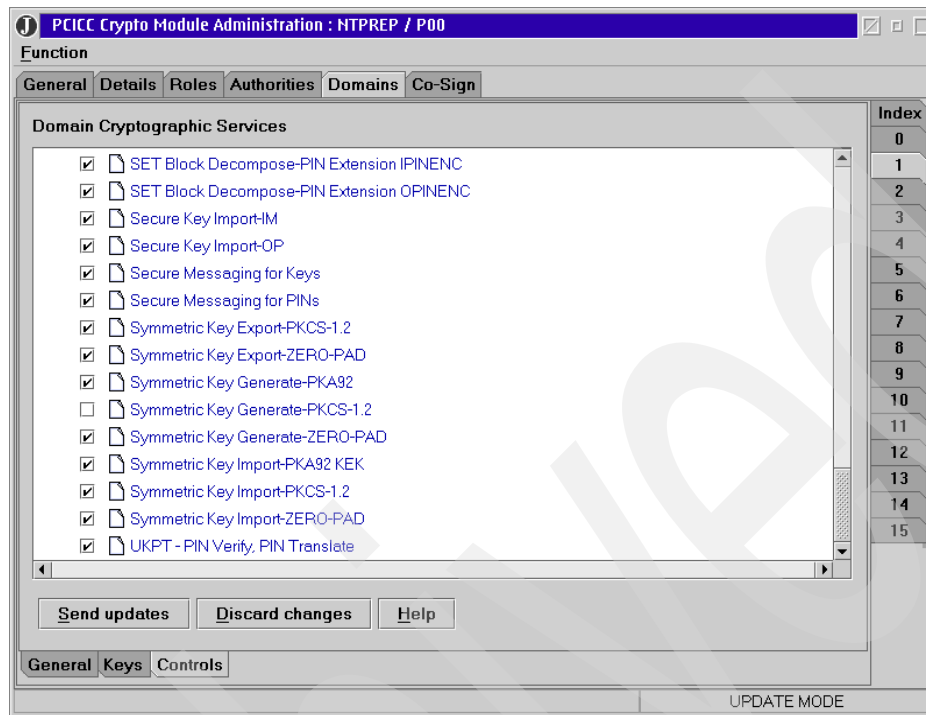


Figure 1-13 Access to Symmetric Key Generate disabled

Example 1-1 Test of a disabled access control point

Normal execution of the test program
 +SYMMETRIC KEY GENERATE - GENERATING
 +KEY GENERATION DONE
 +DES TOKEN WRITTEN
 +RSA ENCIIPHERED KEY WRITTEN

After disabling the access control point:

+SYMMETRIC KEY GENERATE - GENERATING
 +ERROR CODE = 00008, REASON CODE = 00090

Note that some access control points are indicated as *****Required***** in the TKE display. An attempt to modify them opens a pop-up window indicating that required access control points cannot be disabled.

The access control points can also be displayed at the ICSF ISPF panels, by marking a PCICC, PCIXCC or Crypto Express2 in the Coprocessor Management panel with an r (display default role), as shown in for the P00 coprocessor in Example 1-2.

Example 1-2 Selecting the DEFAULT role display in the PCICC

----- ICSF Coprocessor Management ----- Row 1 to 6

Select the coprocessors to be processed and press ENTER.
 Action characters are: A, D, E, R, and S. See the help panel for details.

COPROCESSOR	MODULE ID/SERIAL NUMBER	STATUS
-------------	-------------------------	--------

.	A02		ACTIVE
.	A03		ACTIVE
.	C0	04100000000039C4	04100000000039C4 ACTIVE
.	C1	0410000000003992	0410000000003992 ACTIVE
r	P00	92E01846	ACTIVE
.	P01	92E01983	ACTIVE

Example 1-3 shows all of the access control points that are currently enabled in the DEFAULT role of the selected coprocessor for the pertaining domain.

Example 1-3 ISPF panel showing the enabled access control points

```

----- ICSF - Status Display ----- Row 69 to
COMMAND ==>

Enabled access control points from the default role for P00 domain 1

Secure Messaging for PINs
Set ASYM Master Key
Set SYM Master Key
Symmetric Key Export - PKCS-1.2
Symmetric Key Export - ZERO-PAD
Symmetric Key Generate - PKA92
Symmetric Key Generate - PKCS-1.2
Symmetric Key Generate - ZERO-PAD
Symmetric Key Import - PKA92 KEK
Symmetric Key Import - PKCS-1.2
Symmetric Key Import - ZERO-PAD
SET Block Compose
SET Block Decompose
SET Block Decompose - PIN Extension IPINENC
SET Block Decompose - PIN Extension OPINENC
TKE Authorization for domain 1

```

Access control points can also be defined for UDX services.

New TKE users

For users who have not previously installed a TKE, whose PCICC, PCIXCC, or Crypto Express2 coprocessors never recorded that they were accessed from a TKE, and whose access control points are initially set as if they were non-TKE users: This is all enabled except for the DKG-DALL, DSG Zero-Pad Unrestricted Hash Length, and UDX ones.

TKE users

The PCICC, PCIXCC, or CEX2C coprocessors have recorded that they have been accessed from a TKE once and, when new access control points appear in ICSF, the DEFAULT profile will not be refreshed for the new access control points. Consequently, access control points for existing services will be set to enable (with the exception of DKG-DALL, DSG Zero-Pad Unrestricted Hash Length, and UDX), and access control points for new services will be disabled.

1.3 TKE V4.1

TKE 4.1 code enables the user to generate and load operational keys to be used by the PCIXCC and Crypto Express2, as shown in Table 1-1.

Table 1-1 Operational key types and key lengths

Key type	Possible key lengths
Exporter	16
Importer	16
IPINENC	16
OPINENC	16
PINGEN	16
PINVER	16
IMP-PKA	16
DATA	8, 16, 24
DATAC	16
DATAM	16
DATAMV	16
MAC	16
MACVER	16
User Defined	16
UDATAM	16
UDATAMV	16
IKEYXLAT	16
OKEYXLAT	16

The TKE menu that is used to load the operational key is displayed by clicking the Keys tab in the selected domain. The operational key is stored in the CKDS after its part has been securely sent and assembled into a secure coprocessor.

These keys are defined by their control vector. A control vector is 8 bytes if the key is 8 bytes or 16 bytes if the key is 16 or 24 bytes.

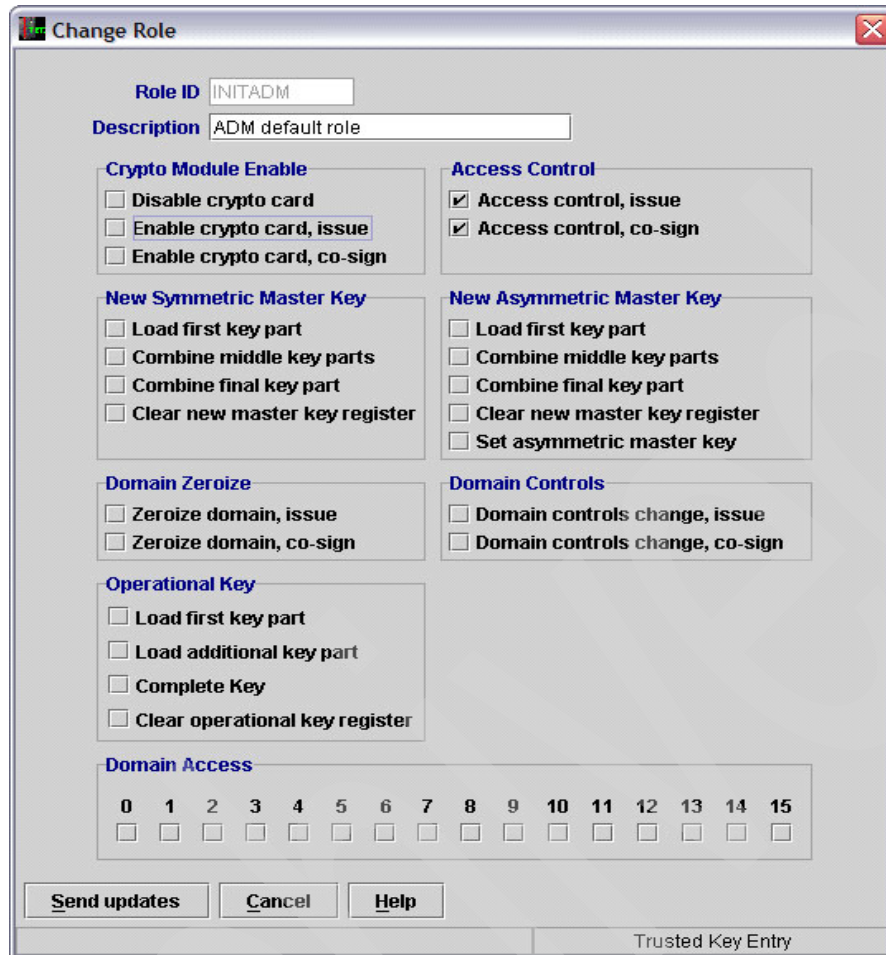


Figure 1-14 Access control points with operational keys load

1.3.1 TKE enablement for z990 and z890

If you have a z890 or z990 with a May 2004 or later version of Licensed Internal Code (LIC) installed, TKE commands must be permitted on the Support Element before any commands issued by the TKE workstation can be executed. (This is a requirement beginning with the May 2004 Licensed Internal Code.) Default setting for TKE commands is Denied. To permit TKE commands on the Support Element, you must perform the following tasks:

1. On the PCI Cryptographic Configuration panel, highlight a PCI Cryptographic number (all PCIXCCs/CEX2Cs available on the server will be displayed) and click **TKE Commands**.
2. On the TKE Command Configuration panel, permit TKE commands by selecting the **Permit TKE Commands** check box, and click **OK**.
3. Repeat steps 1 and 2 for each PCIXCC/CEX2C card.

If TKE commands are not permitted on the Support Element, the following Details error will be displayed on the TKE workstation when an attempt is made to open a Host ID:

Error Message: Program CSFPCIX Interface Error Type 2 Return Code 12 Reason Code 2073
Detail Message iThe PCI X Cryptographic Coprocessor had been disabled on the Support Element. It must be enabled on the Support Element before TKE can access it.

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

1.4 Overview of the TKE V4.2

We now focus more precisely on the TKE workstation features in Version 4.2. Some of these features existed before Version 4.2, as indicated below, but we believed that it was important to be able to clearly position the new functions with respect to the existing implementation.

1.4.1 z/OS releases

This list is provided for reference to the coprocessors support only. None of this release is related directly to the use of the TKE V4.2.

- ▶ For z/OS V1R3 and OS/390 Release 10: Install APAR OW44816 (fix to the APPL permission in RACF) and APAR OW46381 (access control points initial implementation).
- ▶ For z/OS V1R3 and higher and OS/390 Release 10 without the z990 Cryptographic Support Web deliverable: Install APAR OW53666 (additional access control points support).
- ▶ For z990 Cryptographic CP Assist support: ICSF FMID HCR7708 or later.
- ▶ For z990 PCI X Cryptographic Coprocessor support: ICSF FMID HCR770A or later.
- ▶ For z990 and z890 Crypto Express2 Coprocessor support: FMID HCR7720 or toleration APAR OA09157 on FMID HCR770A and HCR770B.

1.4.2 TKE hardware

The TKE workstation is an IBM PCI bus based personal computer. The different feature codes are for your network connection.

- ▶ Display and display driver supporting SVGA with screen resolution 1024 x 768 pixels
- ▶ Minimum 24 MB RAM
- ▶ IBM 4758 Cryptographic Adapter model 002, or model 023 in special situations with proper information from IBM. The cryptographic adapter supports a broad range of DES and public-key cryptographic processes. It is the TKE workstation engine and has key storage for DES keys.

1.4.3 TKE software

The TKE workstation comes with the following software installed:

- ▶ OS/2 WARP® 4.5
- ▶ IBM 4758 PCI Cryptographic Coprocessor Support Program Release 2.41SC for OS/2
- ▶ Trusted Key Entry Version 4.2
- ▶ JAVA runtime environment 1.3.1

The TKE V4.2 code is delivered in CD FC0853.

1.4.4 New functions

The Smart Card Support and Group Logon functions are new with Version 4.2. They are independent from each other but can be exploited concurrently. They are explained in detail in Chapter 2, “TKE V4.2 Group Logon feature” on page 27, and Chapter 3, “Smart Card Support” on page 39.

- ▶ Smart Card Support: The capability of using smart cards and TKE attached smart card readers that can be used for:
 - Generating RSA keys on the smart card for use as 4758 logon user ID and TKE authority command signatures
 - Storing key parts for 4758 Master Keys, CCF Master Keys, PCICC Master Keys, PCIXCC Master Keys, or Crypto Express2 Master Keys
 - Storing operational key parts for PCIXCC, CEX2C, and CCF
 - Ability to log on to workstation 4758 using RSA signature authentication instead of a passphrase

The card operations and contents can be unlocked only through PIN entry at the card reader. A secure session is established between the card reader and the TKE 4758 cryptographic adapter, which results in secrets never being exposed in the clear.

- ▶ Group logon to the TKE workstation: Enables dual and multiple control of workstation commands by requiring a certain number of users to authenticate to the TKE as members of a group. A group can have one to 10 individual users.

More on Smart Card Support

Support for an optional Smart Card Reader attached to the TKE 4.2 workstation enables the use of smart cards, which resemble credit cards in size and shape but contain an embedded microprocessor and associated memory for data storage.

Access to and the use of confidential data on the smart cards are protected by a user-defined personal identification number (PIN). For example, the smart card can store one or more 4758 PCI Cryptographic Coprocessor master key parts. The parts are stored in the clear on the smart card. The master key parts are generated by the 4758 PCI Cryptographic Coprocessor within the TKE workstation and are transferred to the smart card for storage and later read back to the TKE 4758 cryptographic adapter for processing. The master key parts are encrypted, for added security, during transport between the smart card and the 4758.

TKE 4.2 Smart Card Reader support does not remove any of the mechanisms that were available in the previous TKE LIC. That is, with the Smart Card Support, it is still possible to store key parts on diskettes or paper, or to use a TKE authority key stored on a diskette, and to log on to the 4758 using a passphrase.

The following optional features are associated with the TKE 4.2 workstation Smart Card Reader support:

- ▶ TKE 4.2 code (#0853)
- ▶ TKE 4.2 Smart Card Reader (#0887). This feature includes two smart card reader units and 20 smart cards.
- ▶ TKE 4.2 additional smart cards (#0888). This feature contains 10 additional smart cards.

The optional Smart Card Reader, which can be attached to a TKE workstation with the 4.2 level of LIC, is available on S/390 G6 servers as well as zSeries 800, 900, 890, and 990. Currently installed TKE workstations can be upgraded to the TKE 4.2 code to enable use of the Smart Card Reader.

1.4.5 Access control points

At TKE Version 4.x, access to services that are executed on the PCI X Cryptographic Coprocessor or Crypto Express2 Coprocessor is through access control points in the DEFAULT role. To execute callable services on the PCIXCC/CEX2C, access control points must be enabled for each service in the DEFAULT role. All access control points are enabled for new TKE users and non-TKE users. This is also true for brand new TKE V4.2 users.

If you are upgrading from TKE V4.0 or V4.1 to TKE V4.2 and your configuration includes PCIXCCs or CEX2Cs, the settings (enabled-disabled) for existing access control points remain as they were on TKE V4.0 or V 4.1. Depending on the ICSF FMID that is installed, new access control points may have to be enabled.

Note: Access control points DKYGENKY-DALL and DSG ZERO-PAD are always disabled in the DEFAULT role for all customers (TKE and Non-TKE) and require a TKE workstation to enable them. DSG ZERO-PAD is applicable only to the PCIXCC/CEX2C.

Access control points for ICSF FMID HCR770B are:

- ▶ Diversified Key Generate - TDES-XOR
- ▶ Diversified Key Generate - TDESEMV2/TDESEMV4
- ▶ PIN Change/Unblock - change EMV PIN with OPINENC
- ▶ PIN Change/Unblock - change EMV PIN with IPINENC
- ▶ Transaction Validation - Generate
- ▶ Transaction Validation - Verify CSC-3
- ▶ Transaction Validation - Verify CSC-4
- ▶ Transaction Validation - Verify CSC-5
- ▶ Key Part Import - RETRKPR

Access control points for ICSF FMID HCR770A are:

- ▶ CKDS Conversion Program
- ▶ Clear Key Import
- ▶ Decipher
- ▶ Digital Signature Verify
- ▶ DSG ZERO-PAD Unrestricted Hash Length
- ▶ Encipher
- ▶ Key Part Import - ADD-PART keyword
- ▶ Key Part Import - COMPLETE keyword
- ▶ NOCV Exporter
- ▶ NOCV Importer
- ▶ inhibit Export Extended
- ▶ Public Key Encrypt

These access control points are supported only on the PCIXCC/CEX2C.



TKE V4.2 Group Logon feature

In this chapter we explain what a TKE Group Logon is, what its purpose is and how a group of users can be set up and used to log on to the TKE V4.2 workstation.

2.1 Group logon feature

As explained in the previous chapter, access control to the TKE is achieved by defining 4758 user profiles with a user ID and an authentication passphrase. (With TKE V4.2, the passphrase can be replaced by authentication data provided in a smart card.) Logging on is required to administer zSeries system coprocessors or to use TKE utilities such as CNM.

The TKE V4.2 Group Logon feature is the implementation of multiaccess control to get logged on to the TKE 4758 cryptographic adapter. This is based on the use of a group profile, which requires individual authentication of each of the users belonging to the group.

A group profile has the same structure as standard profiles but uses a newly defined authentication mechanism, which is a list of names of other profiles. The Group Logon can be used with the traditional passphrase mechanism or with the newly available smart card feature using public key authentication. The logon request references the group profile, then proceeds with the authentication of the individual members of the group. Figure 2-1 shows a TKE logon menu when groups have been defined.

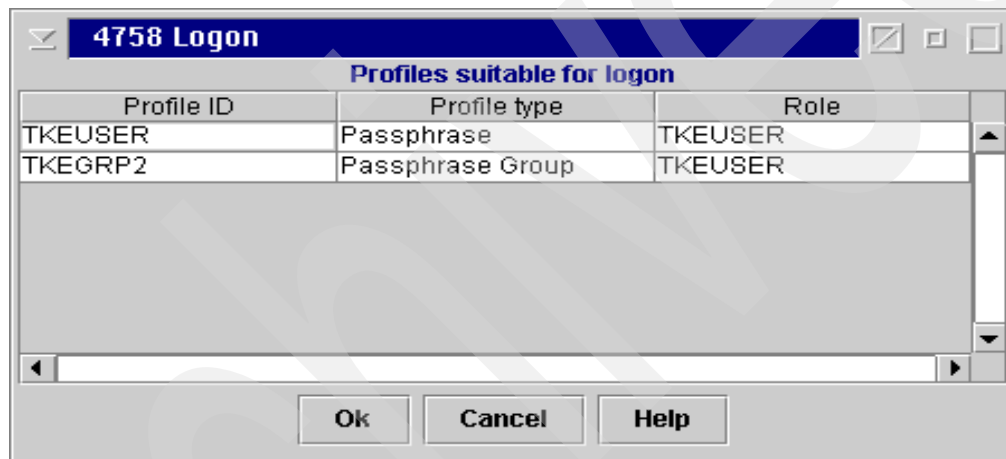


Figure 2-1 Example of the logon prompt when groups have been defined

A group can have from one to 10 members, although not all members have to log on at the same time. All members of a group must use the same authentication mechanism (passphrase or smart card). That is, a group is either:

- ▶ One to 10 users who are authenticated by passphrase
- ▶ One to 10 users who are authenticated by smart card

Note: As we write this document, a group cannot be a member of another group.

Important: It is recommended that when the smart card authentication method is in use users should no longer be authenticated using passphrases, and the profiles specifying passphrase authentication should be deleted.

2.1.1 How to create a group logon environment

In this chapter we describe how to create a group logon environment that uses the passphrase authentication mechanism. Creating a group logon environment using smart cards is almost the same and is briefly described in the smart card chapter.

In this example, we create a group of four users: TKEPH11, TKEPH12, TKEHP21, and TKEHP22.

It is assumed that this is the first group logon profile assigned to a newly installed TKE4.2 workstation. The group logon profiles are created using the CNM utility on the workstation.

1. Start CNM by double-clicking the icon in the Trusted Key Entry folder. To log on to CNM, select **File** → **Passphrase Logon**.



Figure 2-2 Logon to CNM using passphrase

2. Enter the user ID and passphrase in the Passphrase Logon window (Figure 2-3).

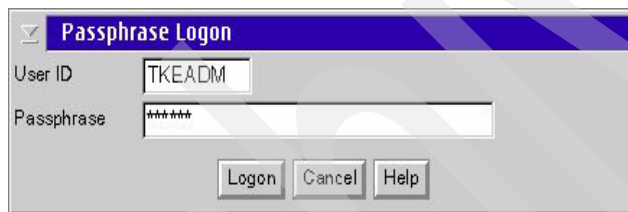


Figure 2-3 Log on using TKEADM user ID

3. After successfully logging on, select **Access Control** → **Profiles** (Figure 2-4).

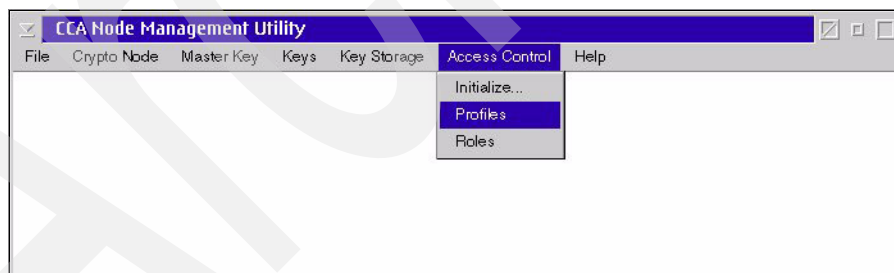


Figure 2-4 Select Access Control → Profiles

4. This displays a list of currently defined profiles in the Profile Management window (Figure 2-5). To create new profiles to be used later in the group profiles, click **New** at the bottom of the window.

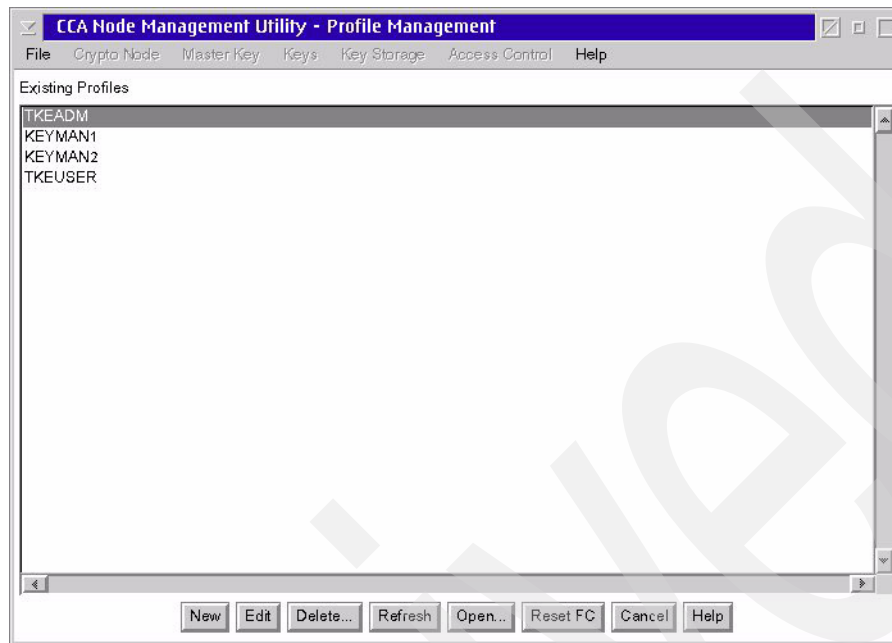


Figure 2-5 CNM Profile Management window

5. This opens a new window for selecting a profile type (Figure 2-6). (Smart card support was already enabled in our test workstation. You may not see the Smart card option if is not yet enabled.) Choose **Passphrase** and click **Continue**.



Figure 2-6 Select profile type Passphrase

6. In the next Profile Management panel, type the profile information as shown in Figure 2-7.

Enter the name of the User ID (the name of this profile) and, optionally, a profile description. The activation date and expiration date designate the validity period of this profile and is examined during the logon process.

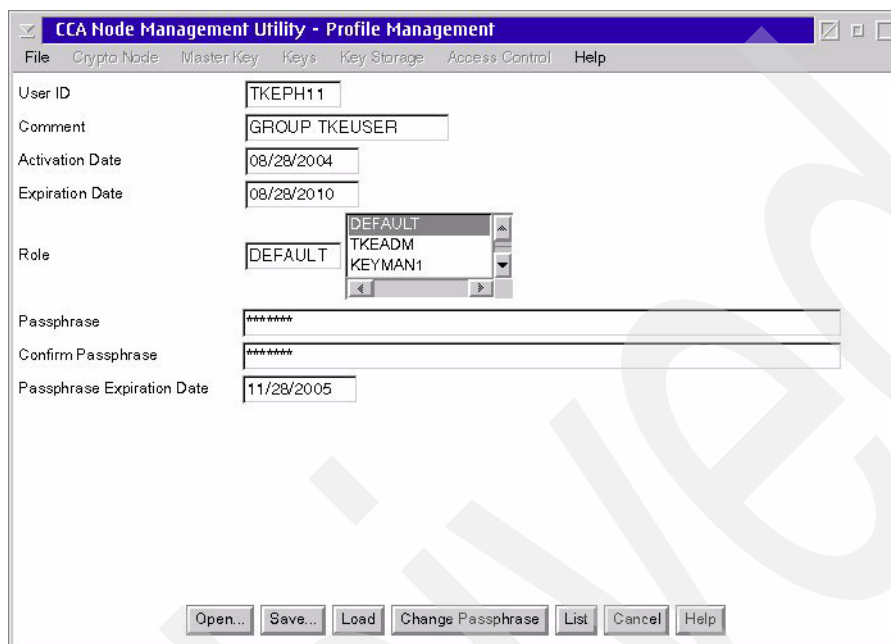


Figure 2-7 Enter profile information

We give the user the **DEFAULT** role, although the user will eventually be in the GROUP role when all required group members have authenticated.

Enter equal values in the passphrase and passphrase confirmation fields, abiding with the installation security rules for the passphrase contents and length (the maximum length is 64 characters). Set the Passphrase expiration date to the desired value.

Important: User ID and Passphrase fields are case-sensitive.

7. You can save the profile on the PC hard disk by clicking **Save** at the bottom of the panel. This opens to the default saving folder, where all other profiles and roles are saved.

To create and load the new profile into the 4758 cryptographic adapter, click **Load**. If all entered information is correct, a success window pops up (Figure 2-8).



Figure 2-8 Successful User ID profile creation

8. Create more user ID profiles the same way to use as members of a group. In our example, we created the four profiles shown in Figure 2-9 on page 32.

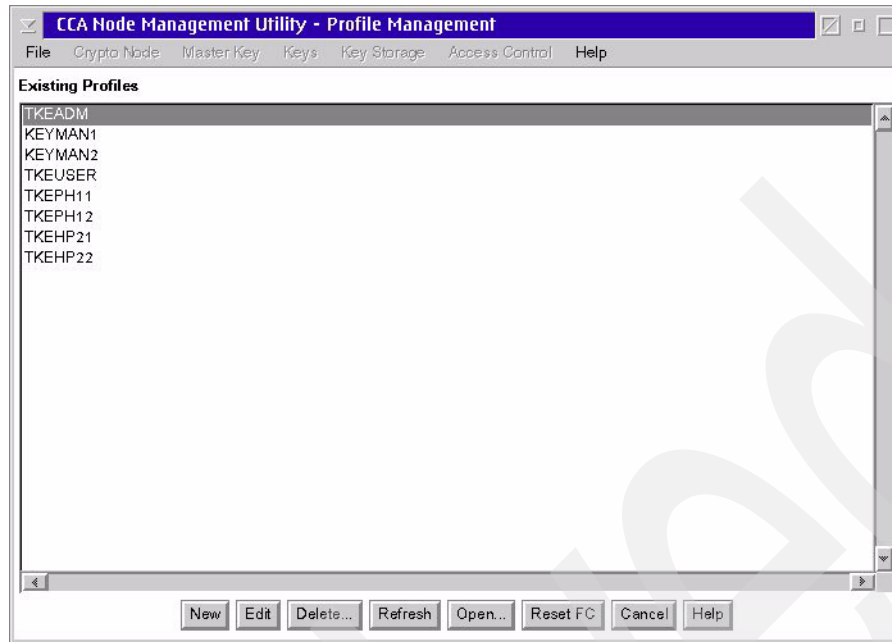


Figure 2-9 Four User ID profiles created and loaded to 4758

9. To create a new group profile, click **New** at the bottom of the panel to open the profile-type window again (Figure 2-10). After selecting the profile type **Group**, click **Continue**.



Figure 2-10 Select profile type Group

10. On the next panel, enter the information to add a new group profile, as indicated in Figure 2-11.

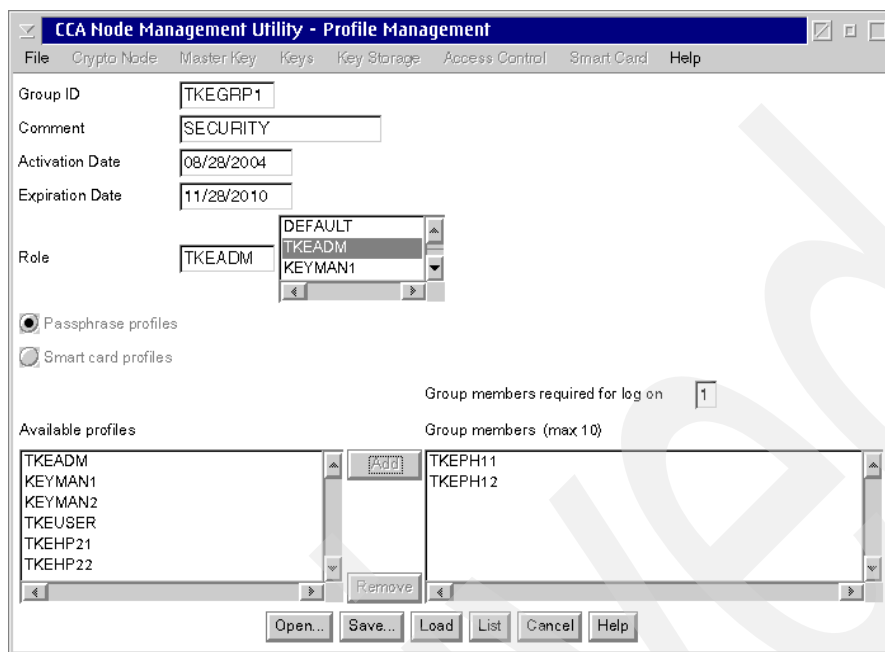


Figure 2-11 Enter Group profile information

Enter the name of the Group ID of this profile and the optional description. This profile is also given an activation date and expiration date.

The role TKEADM is chosen for this group because it is intended to perform a group logon to the CNM utility. If the group were meant to get the privileges needed to administer the zSeries coprocessors, then it would be given the role TKEUSER.

Select the members authentication mechanism desired for this group profile, Passphrase profiles or Smart card profiles. When selecting the desired profile type, the left container shows all possible profiles of the chosen profile type.

Specify the minimum number of group members required for logon. The minimum is one, and the maximum is 10.

Highlight the selected profile in the left container and click **Add** to add it to the group. The right container is updated. The group must have at least the number of members designated in the box above the right container. In our case, two user profiles are defined in the group, and it has been specified that only one out of these two is sufficient to log on.

11. The profile can be saved on the hard disk by clicking **Save** at the bottom of the panel. The default saving folder is where all other profiles and roles are saved.

To load the new group profile into the TKE 4758 cryptographic adapter, click **Load**. If all entered information is correct, a success window pops up (Figure 2-12).



Figure 2-12 Successful Group profile creation

12. We created a second group profile in which the minimum number of group members required to log on is set to two. Then we added three profiles to this group (Figure 2-13). This enables any two of those three members to achieve a successful group logon.

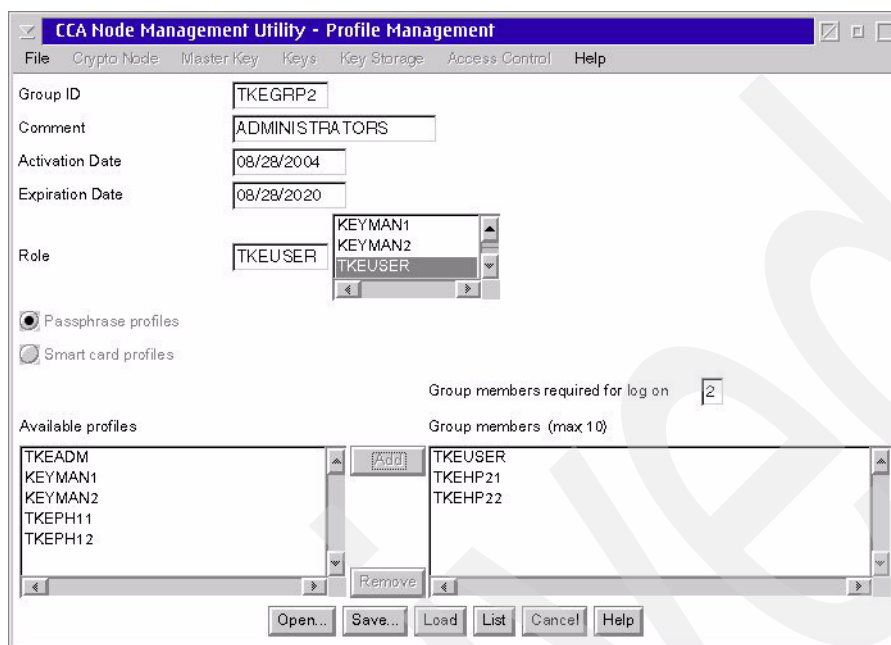


Figure 2-13 Enter the information for the second group profile

Note: When a user logs on as a member of a logon group, his or her individual role will be overridden by the group when the group is successfully logged on.

When the profile is created and loaded into the TKE 4758 cryptographic adapter by clicking **Load**, and a success window pops up, the Profile Management window displays an updated list of existing profiles.

2.1.2 How to use the Group Logon feature

When the group logon environment has been created, the group can log on to the TKE 4758 cryptographic adapter. There are two target applications for the Group Logon option:

- ▶ The CNM 4758 administration program
- ▶ The TKE application itself

Group logon to CNM using a passphrase

Open CNM by double-clicking the CNM icon in the Trusted Key Entry folder at the TKE workstation.

1. When the CNM window opens, select **File** → **Group Logon** (Figure 2-14 on page 35).

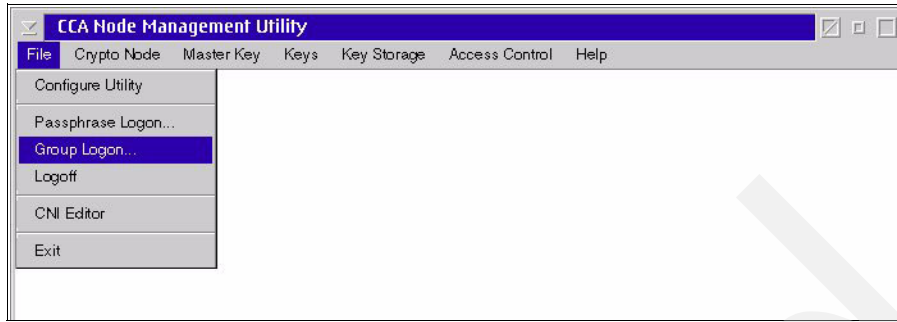


Figure 2-14 File → Group Logon

2. Enter the Group profile ID in the next window (Figure 2-15).

Note: The Group profile ID is case-sensitive and must be entered using the format it was saved in earlier.



Figure 2-15 Window to enter the Group profile ID

3. A window opens, displaying the members of that group, along with the required number of users to be authenticated and the required authentication method (Figure 2-16). To continue the group logon, select one group member who is to authenticate and click **Enter Passphrase**.

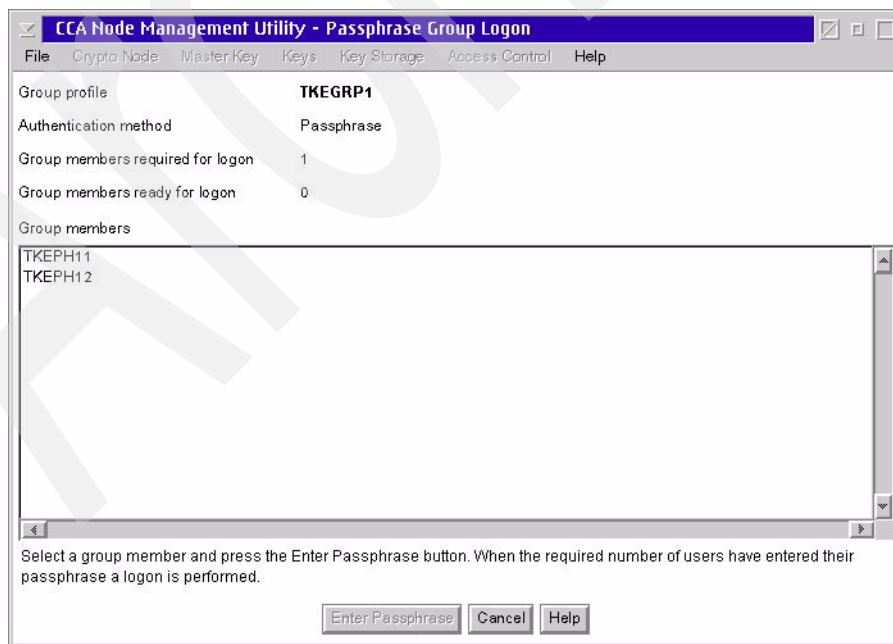


Figure 2-16 The group member selection window

4. A new window opens to enter the passphrase belonging to the selected user profile (Figure 2-17). The passphrase value is case-sensitive and must be entered in the correct format.

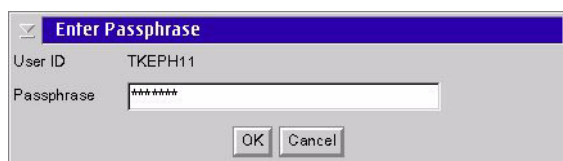


Figure 2-17 Passphrase entered for user TKEPH11

5. When all required members in the group have authenticated successfully, a new window displays that the group logon is accepted. Click **OK** to continue.

If an incorrect passphrase is entered, it will be indicated after all required members in the group have entered their passphrases. This is shown in Figure 2-18, where the group TKEGRP2 requires two group members to log on and member TKEHP22 has entered an incorrect password.

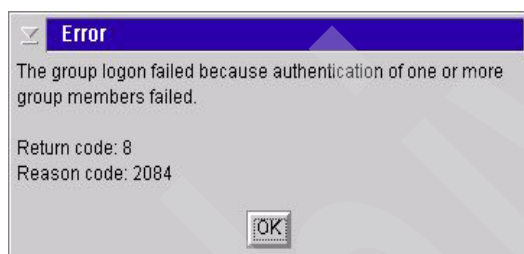


Figure 2-18 One or more invalid passphrases has been entered

6. The group member selection window reopens, showing which passphrases were entered incorrectly (Figure 2-19). All group members must go through the logon process again.

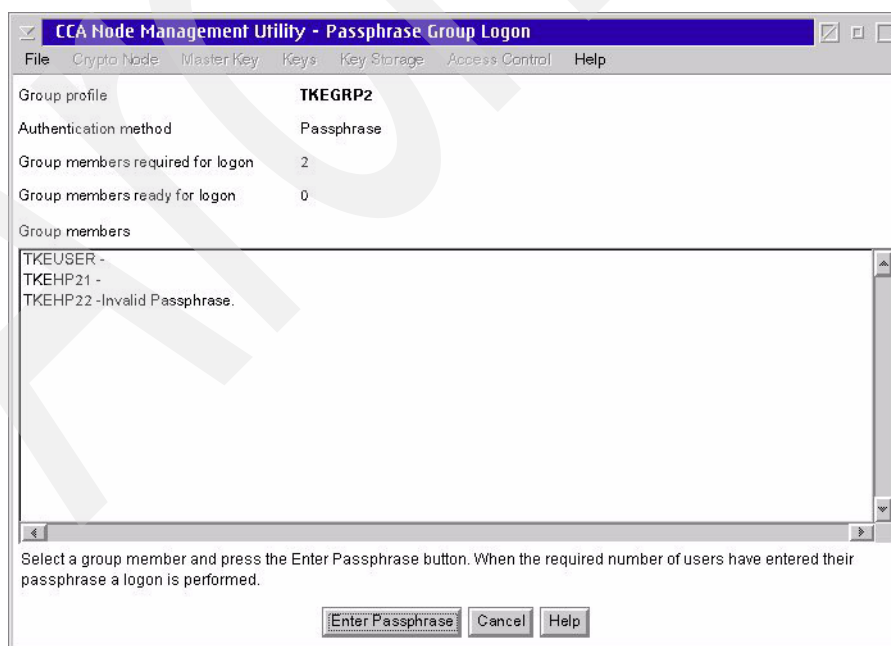


Figure 2-19 Invalid passphrase given by one group member

Group logon to the TKE using a passphrase

Open the TKE application by double-clicking **TKE** in the Trusted Key Entry folder at the TKE workstation main panel.

1. A window opens, showing a list of profiles that are suitable for logon to TKE applications (Figure 2-20). The list comprises both individual user profiles and group profiles that are permitted to the 4758 access control point 0x8002. The TKEUSER role is permitted to this access control point. Select the group profile to be used in the logon process and click **OK**.

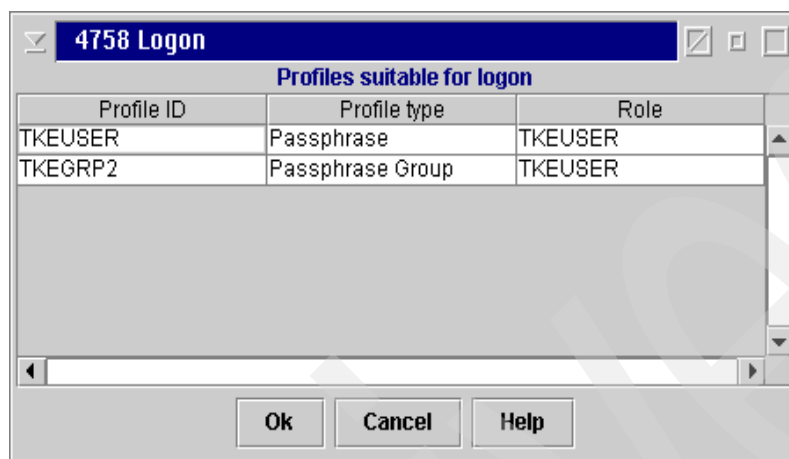


Figure 2-20 List of suitable profiles for TKE logon

2. The next window displays a list of group members and the required minimum number of members to achieve the logon process (Figure 2-21).

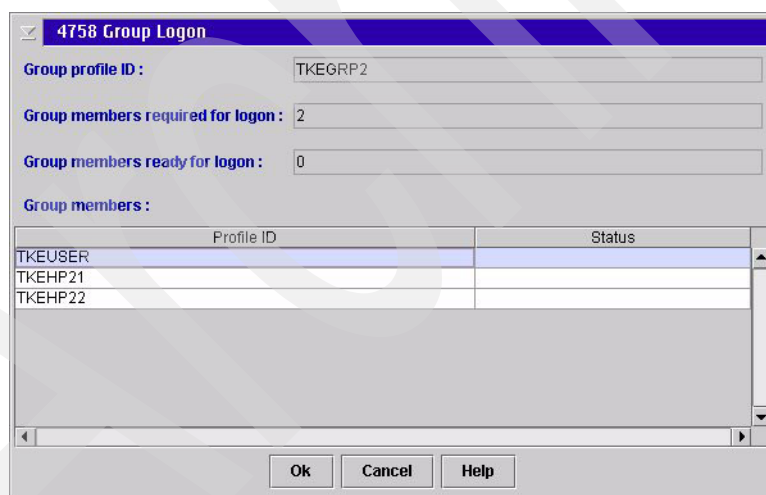
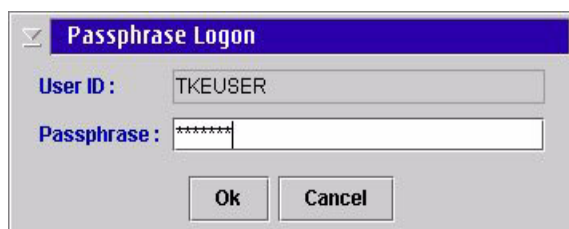


Figure 2-21 Select wanted user id from the group member list

In our example, the group has three members: TKEUSER, TKEHP21, and TKEHP22. Two of those users are required to authenticate to make the group logon successful. Even though TKEUSER could be used as an individual user to make a passphrase logon (see step 1), in the group TKEGRP2 the user in the TKEUSER role can still participate to the group logon as a member of the group.

To log on to the TKE application, highlight one of the members and click **OK**.

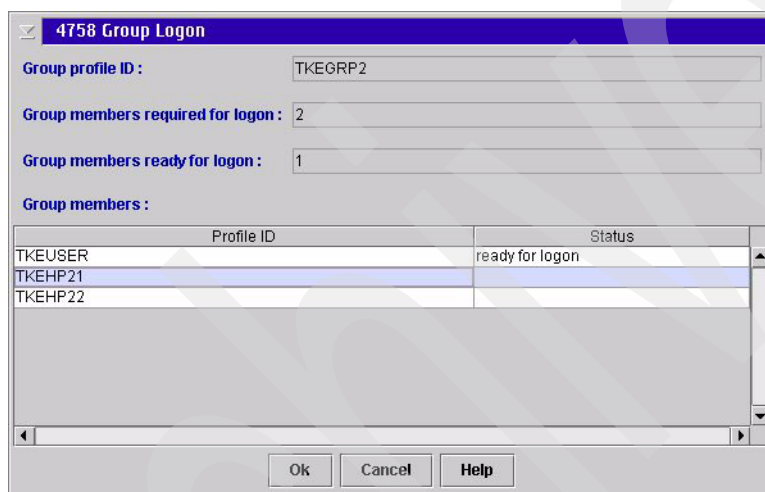
3. Enter the passphrase for the selected group member (Figure 2-22).



A dialog box titled "Passphrase Logon" with a blue header bar. It contains two input fields: "User ID" with the text "TKEUSER" and "Passphrase" with masked characters "*****". Below the fields are "Ok" and "Cancel" buttons.

Figure 2-22 Passphrase entered for user TKEUSER

4. This updates the 4758 Group Logon window to indicate that the member has entered the correct passphrase. The count of group members ready for logon is also updated, as shown in Figure 2-23. Select the next member from the list and click **OK** to enter the passphrase for this member.



A dialog box titled "4758 Group Logon" with a blue header bar. It contains three input fields: "Group profile ID" with "TKEGRP2", "Group members required for logon" with "2", and "Group members ready for logon" with "1". Below these is a table titled "Group members" with two columns: "Profile ID" and "Status". The table lists three members: TKEUSER (status: ready for logon), TKEHP21, and TKEHP22. The TKEHP21 row is highlighted. At the bottom are "Ok", "Cancel", and "Help" buttons.

Profile ID	Status
TKEUSER	ready for logon
TKEHP21	
TKEHP22	

Figure 2-23 The updated group member selection window

When the required number of group members has made a successful logon (in our case, two), the TKE application main window opens.

Note: If any of the members involved in the group logon entered a wrong passphrase, it will be indicated only after *all* participating group members have entered their passphrases. The status column in the 4758 Group Logon window shows any members whose passphrase was incorrect. All passphrases must be entered again for a successful logon.



Smart Card Support

This chapter describes the new Smart Card Support feature of the Trusted Key Entry workstation. The Smart Card Support feature increases operations security when working with TKE giving the possibility to store secret information into the smart cards that never leave the cards in clear. Because TKE users can use their smart cards for authentication to the TKE application, Smart Card Support can also be exploited by the new Group Logon feature as well.

3.1 Smart card feature description

TKE smart cards are intended to be used for:

- ▶ Generating, storing, and use of a 4758 Logon RSA key pair, as an alternative to using a passphrase.
- ▶ Generating, storing, and use of a TKE Authority signature key pair, as an alternative to keeping the authority key pair on the workstation hard disk or on a diskette.
- ▶ Storing ICSF key parts (master key parts and operational key parts), as an alternative to keeping the key parts on the workstation hard disk or on a diskette.
- ▶ Storing the TKE 4758 cryptographic adapter master key parts, as an alternative to keeping the key parts on the workstation hard disk or on a diskette.

Note that the added Smart Card Support does not remove any of the mechanisms available in the previous TKE code. That is, with Smart Card Support it is still possible to store key parts on diskettes or paper, to use a TKE authority signature key stored on a diskette and to log on to the 4758 using a passphrase.

Important: It is recommended that when the smart card setup has proven to be properly working on the TKE workstation, the critical roles and profiles (TKEADM, KEYMAN1, KEYMAN2, and TKEUSER) with passphrase authentication be deleted from the 4758 cryptographic adapter. Those roles and profiles can be loaded back from the disk (folder C:\TKE\4758access) if necessary.

3.1.1 Requirements and terminology

Smart card support requires:

- ▶ TKE 4.2 code, feature code 0853
- ▶ TKE 4.2 Smart Card Reader, feature code 0887. This feature includes two smart card readers and 20 smart cards. Two smart card readers must be attached at all times to each TKE workstation to use smart card functions.
- ▶ TKE workstation with an IBM 4758 PCI Cryptographic Card (the cryptographic adapter). Optional feature code 0888 includes 10 additional smart cards.

Some terminology

Certificate Authority (CA) Smart Card

An entity that establishes a zone using the SCUP. A CA smart card is protected by two six-digit PINs.

Entity

A member of a zone. Entities can be a CA smart card, a TKE smart card, or a 4758 cryptographic adapter.

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 time-out condition occurs.

Note: Think of entering a PIN as “opening” the smart card. As you will see in the rest of this chapter, the smart card also keeps non-secret administrative information in its storage. This information can be displayed without entering a PIN.

PKI Public key infrastructure

SCUP	(Smart Card Utility Program) Performs maintenance operations, such as the creation, initialization, and personalization of CA and TKE smart cards.
Session key	Symmetric key used to protect secret data during transport between entities.
TKE smart card	Used for storing keys and key parts; can hold a maximum of 10 key parts, a 4758 logon key, and a TKE authority key. Protected by a four-digit PIN.
Transport key	Symmetric key used to protect ICSF key parts during transport from the TKE workstation to the zSeries cryptographic coprocessors.
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.

3.1.2 PKI concepts used in TKE smart card support

- ▶ A Certificate Authority delivers digitally signed certificates that certify public keys and the user identities that are bound to these keys. Note that the certificates we are talking about here for the TKE smart card are IBM proprietary format certificates.
- ▶ The CA certifies users operating in its zone. The name of the zone the Certificate Authority covers is specified at Certificate Authority creation.
- ▶ Each entity in the zone has its own RSA key pair, which has been generated inside the entity smart card or in the 4758 itself. The private key is kept and operates always inside the entity secure enclosure (a *retained key* for the 4758 and the equivalent for the smart cards).
- ▶ Entities use their private key to sign messages or decrypt secrets that they receive encrypted with their public key. Entities use other entities' public keys to verify signatures or to encrypt secrets to be sent to these entities.

Note: There is no notion of a validity period in the TKE smart card PKI or certificate revocation; therefore, certificates are not intended to be renewed. However a "blocking" function has been implemented at the smart card level that results from a wrong PIN entered too many times in a row, which requires a CA action to have the card "unblocked." The blocking and unblocking functions are described in "Changing the TKE card PIN" on page 57.

Where does the zone matter?

In this context of the TKE smart card PKI, only entities of the same zone (whose public keys have been certified by the zone CA), can exchange encrypted secrets. In our case:

- ▶ The TKE 4758 or the zSeries coprocessors key parts
- ▶ The smart card secrets that have to be transferred to build smart card backups or copies

This means that being in a different zone from the TKE 4758 entity does not prevent using a smart card to log on to the TKE if the user profile has been set up properly; however, the TKE cannot accept the key parts stored on this smart card that is foreign to the 4758 zone.

Principle of operation of the TKE smart card PKI

Figure 3-1 on page 42 is a schematic overview of the TKE smart card PKI.

- ▶ The zone Certificate Authority, which is actually a smart card. The CA is created by inserting an empty card in one TKE card reader and directing SCUP to initialize a Certificate Authority. This is done by SCUP loading the CA applet into the card, and the CA applet in turn drives the creation of the CA key pair, self-signed certificate, and so on.

The zone that this CA covers will also be indicated. When it is initialized, access to the CA card is controlled using two six-digit PINs.

- ▶ A new TKE user card is initialized and enrolled by inserting the new card into one card reader and the CA card in the other one. SCUP loads a TKE user applet to proceed with initialization, which is mainly creation of the key pair inside the card, and creation of an enrollment certificate request to be signed by the CA smart card. The enrollment is performed by unlocking the CA card so that it can proceed with signing the TKE user card certificate request. The certificate also indicates which zone the TKE user card is operating in.
- ▶ After the TKE user card has been initialized and enrolled, it is personalized (given a four-digit PIN value and some additional administrative information).
- ▶ The TKE 4758 adapter is also one of the entities that are enrolled for the zone.
- ▶ We show here the secret ICSF key parts stored in the TKE user card, which will be sent eventually to the coprocessors via the TKE application. Remember that as a general rule any secret that has to leave the smart card is transmitted encrypted with a dynamically generated symmetric session key. The session key is first sent to the recipient entity encrypted with this entity's public key.

Note: The unlocking of the smart card by the PIN is performed directly at the card reader. The PIN does not leave the card reader and is never presented to the TKE workstation.

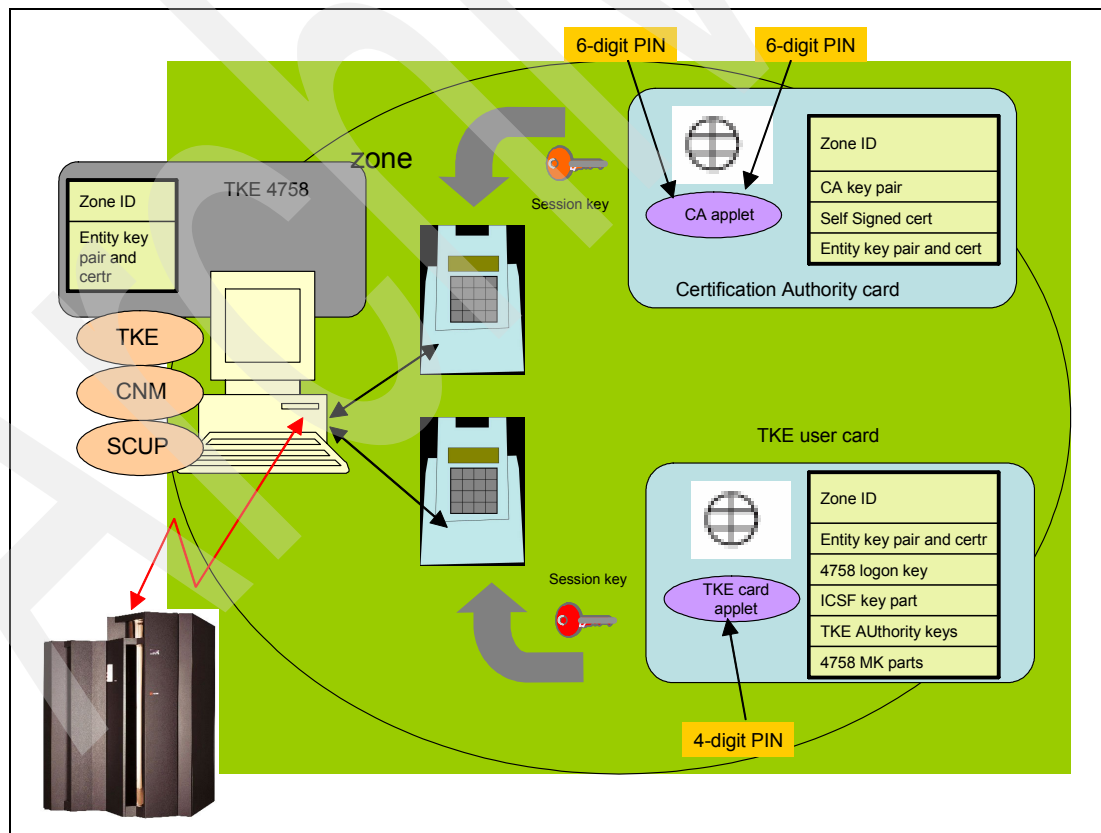


Figure 3-1 Overview of the TKE smart card support implementation

Additional considerations

The CA card is protected by a dual PIN authentication and the card is intended to be initialized and personalized by two persons, proceeding in turn during the personalization process. Due to the importance and sensitivity of this entity, the CA cards must be backed up using the secure process provided by SCUP. This is explained later in this chapter.

Each CA card contains a Zone ID, which is set when the card is created. Each TKE card contains a card description that is chosen by the user when the card is personalized. This description can be used to show the user's current TKE card.

Important: Initializing the 4758 via CNM or CNI deletes the existing enrollment certificate.

3.2 How to create the smart card environment

The smart card feature works with two smart card readers and a set of smart cards. TKE users are expected to use smart cards to authenticate to the CNM utility or the TKE application, so these two programs must be told to support the smart cards. The 4758 must also be initialized via CNI for Smart Card Support with a new .cni file, as indicated below.

CNM utility

To enable the CNM utility to accept smart cards, right-click the CNM icon on the TKE folder, then click **Properties** in the context menu. In the Properties panel, specify /SC in the Parameters field, as shown in Figure 3-2.

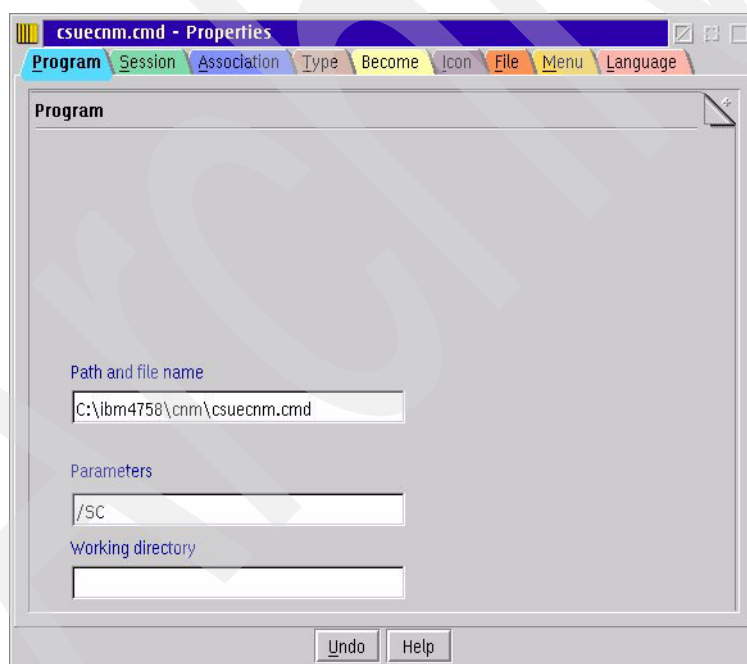


Figure 3-2 Update CNM starting parameter

Close the Properties panel. Smart card support will be activated the next time the CNM utility is started.

4758 initialization for Smart Card Support

The following steps must be performed to initialize the TKE 4758 to support smart cards.

1. Change the working directory:

```
cd ibm4758\cnm
```

2. From the command prompt, type:

```
csuecni c:\tke\4758access\4758SCinitialize.cni
```

3. Run the .cni list, which:

- Initializes the 4758 coprocessor.
- Synchronizes the 4758 clock-calendar with the system clock in the TKE workstation.
- Loads the predefined user role TEMPDEFAULT to the 4758 coprocessor. The TEMPDEFAULT role is a default role that is given any time someone logs on to the TKE 4758 without using an individual profile.

Important: The TEMPDEFAULT role has access control points for all 4758 functions and must be loaded for certain functions to work, such as enrolling the 4758 cryptographic adapters. When the 4758 setup is completed, it should be replaced in the 4758 by the normal DEFAULT role (step 5d on page 45).

- Loads predefined user role SCTKEADM to the 4758 coprocessor. SCTKEADM is a new predefined role for Smart Card Support, equivalent to TKEADM, KEYMAN1, and KEYMAN2 with added access control points, in particular for session keys.
 - Loads predefined user role SCTKEUSR to the 4758 coprocessor. SCTKEUSR is a new predefined role for Smart Card Support, basically equivalent to TKEUSER but with added access control points, in particular for generation and use of session keys.
 - Loads predefined role MIGUSER and user profile MIGUSER to the 4758 coprocessor. The MIGUSER role is used for the 4753 migration utility in the smart card environment.
 - Loads and sets a random master key.
 - Initializes DES key storage.
 - Initializes PKA key storage.
4. SCUP initialization tasks—The following tasks are done using SCUP, and are described in the rest of this chapter:
 - a. Initialize and personalize a CA smart card.
 - b. Back up a CA smart card.
 - c. Enroll local 4758 cryptographic adapter, and remote 4758 cryptographic adapter if applicable.
 - d. Initialize and enroll TKE smart cards.
 - e. Personalize TKE smart cards.Close the SCUP application.
 5. CNM initialization tasks—Open the CNM application. The tasks below are done using CNM, and are described in further details in the rest of this chapter:
 - a. Generate 4758 logon keys to TKE smart cards that will be used to log on to the 4758 cryptographic adapter.
 - b. Define user profiles for the TKE smart cards that have a 4758 logon key.

- c. Define a group profile (optional). Empty predefined group profiles SCTKEADM and SCTKEUSR are provided. A group may contain one to 10 members.
- d. Reload the DEFAULT role from its file backup (c:\tke\4758access\default.rol) using CNM.

Important: Your TKE workstation is not secure until you replace the TEMPDEFAULT role with the regular DEFAULT role. To replace TEMPDEFAULT, you must load the actual DEFAULT role into the 4758 from its disk file.

The rest of the operations below complete the 4758 setup for an actual production environment. We do not discuss this sequence of operations as such in this paper.

6. Log on to the 4758 using a TKE smart card profile or a smart card group profile.
7. Generate a 4758 first key part to a TKE smart card.
8. Load the first key part to the new master key register.

Generating and loading the first and last key parts should be performed by two individuals to set up a dual control security policy: Remove the TKE smart card of individual A and insert a TKE smart card from individual B. We recommend a dual control security policy for key parts. Generate a 4758 last key part to the TKE smart card.

9. Load the last key part to the new master key register. Verify the verification pattern and save it to disk for future reference.
10. Set the master key.
11. Re-encipher DES/PKA key storage.

Smart card utility program (SCUP)

SCUP is already smart-card-enabled and does not need any modification for the use of smart cards. SCUP verifies at startup that both smart card readers are installed. If not, an error message is issued and the program closes down.

Note: Access to SCUP by itself is not protected; however, its security-related functions require users to know the smart cards' PINs and to have the proper 4758 role. Again, the TEMPDEFAULT role has the required privileges for these functions.

TKE application

The TKE application uses Smart Card Support after the TKE initialization file is updated. To do this, edit the tke.ini file in the folder C:\TKE\TKE. This can be done using the edit program called E, as shown in Example 3-1.

Example 3-1 Editing TKE initialization file

```
[C:\tke]cd TKE
```

```
[C:\tke\TKE]DIR
```

```
The volume label in drive C is OS2.
The Volume Serial Number is 6799:C414.
Directory of C:\tke\TKE
```

8-18-04	6:10p	<DIR>	0 .
8-18-04	6:10p	<DIR>	0 ..
8-06-04	12:09p	<DIR>	0 Default
8-06-04	12:09p	<DIR>	0 Definitions
8-06-04	12:09p	<DIR>	0 Message

8-06-04	11:30a	394	0	opencard.properties
8-06-04	11:28a	3066	0	TKE.ico
9-01-04	2:31p	191	35	tke.ini
8-06-04	12:09p	6742668	0	tke42.jar
8-06-04	11:30a	1376	0	tkecard.properties
8-06-04	11:28a	489	0	tkeo.cmd
11 file(s)		6748184 bytes used		
		813870592 bytes free		

[C:\tke\TKE]E TKE.INI

To enable Smart Card Support, set the variable `ENABLE_SMART_CARD_READERS` in the `tke.ini` file to `TRUE`, as shown in Example 3-2.

Example 3-2 Setting the correct smart card variable value

```
SERIALIZE_PATH=Definitions
TRANSPORT_KEY_POLICY=3
FLOPPY_DRIVE_ONLY=false
BLIND_KEY_ENTRY=true
MESSAGE_PATH=Message
ENABLE_SMART_CARD_READERS=TRUE
DEFAULTDIRECTORY=C:\tke\tke\Default
```

Note: The `FLOPPY_DISK_ONLY` variable is relevant only to the storing of secrets on diskette (as opposed to the workstation hard disk). It does not affect storing in the smart card and should be defined according the company security policy.

3.2.1 Installation of the smart card readers



The smart card readers we used in the residency were connected to the TKE workstation with a cable with one connector at the smart card reader and the other end connected in parallel with a twin cable to one of the serial ports and to the mouse port.

The second reader was connected to the other serial port and to the keyboard port. The cables of the mouse and the keyboard could still be plugged in to the workstation on top of the twin cables connectors.

When the card reader receives power, it displays its internal code level. Figure 3-3 shows one of the card reader units that we used for the residency.

Figure 3-3 One of the two Smart Card Readers used in the residency

3.2.2 Setting up the zone entities

Setting up the smart card environment with both smart card readers attached to the TKE workstation uses the Smart Card Utility Program (SCUP) and the CNM utility. The setup

process must be done in a certain order for all entities to be configured correctly. The order of the setup process sequences we ran at the residency is:

1. Initialize a CA card.
2. Back up a CA card (highly recommended).
3. Enroll the local TKE 4758 cryptographic adapter.
4. Enroll the remote TKE 4758 if necessary.
5. Initialize and enroll the TKE cards.
6. Personalize the TKE cards.

Initialization of a CA card

The initialization of the CA card is performed using SCUP.

1. Start SCUP by double-clicking its icon in the TKE folder.
2. Select **CA Smart Card** → **Initialize and personalize CA smart card** (Figure 3-4).

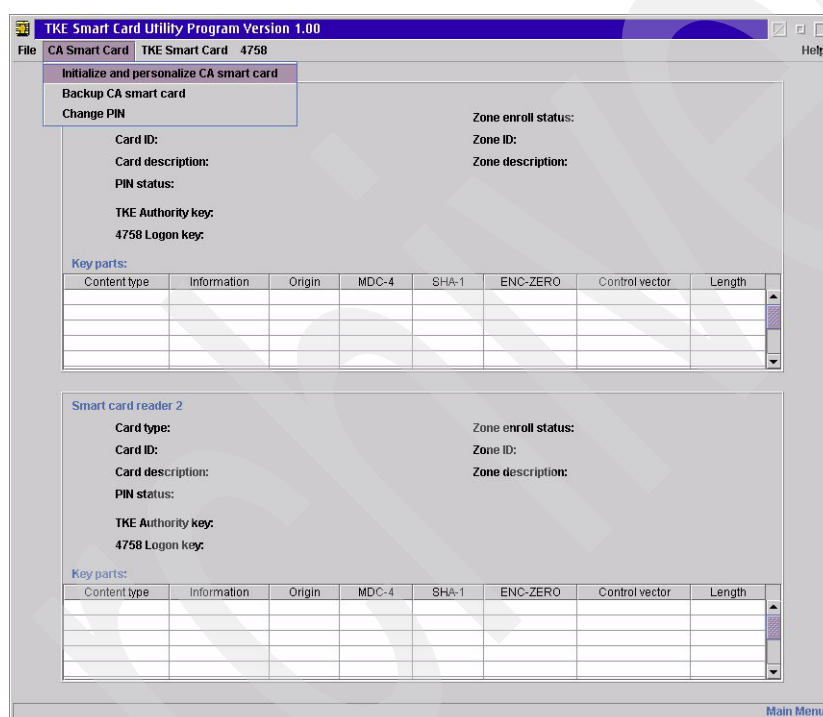


Figure 3-4 Select the initialization and personalization of the CA card

3. You will be prompted to insert the smart card into smart card reader 1. If the smart card to be the new CA card is not empty, the program will prompt you to accept the overwriting of old data. If accepted, the initialization process continues for about one minute, during which the initialization the message in Figure 3-5 is displayed.

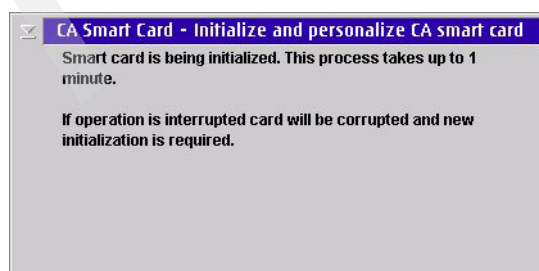


Figure 3-5 Initializing the CA card

- When the initialization is done, the process prompts you to enter the PIN values that are to protect the CA smart card. Enter the CA card's two six-digit PINs, which will be entered twice each at the card reader PIN pad. Figure 3-6 shows the prompt for the first value. After successfully entering the first PIN, the second PIN is prompted in a similar manner.

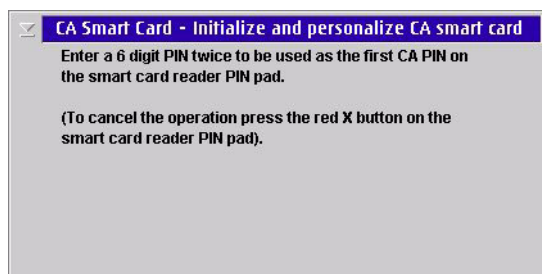


Figure 3-6 CA PINs are six digits long and must entered twice

Important: It is recommended that the first and second CA PINs be entered by different people to have dual custody. Also, the PINs should have different values, but this is not enforced by the code.

If the PIN value is not entered within approximately 30 seconds after the prompt, an error message opens and the CA card initialization process must be restarted.

- After a successful PIN entry, the personalization process carries on by asking for a zone description, as shown in Figure 3-7. This is non-confidential information to be stored on the card; the entities internally use a Zone ID, which is derived from this information. The Zone ID is eventually used to verify whether other entities belong to the same zone and can therefore participate in exchanging secrets.

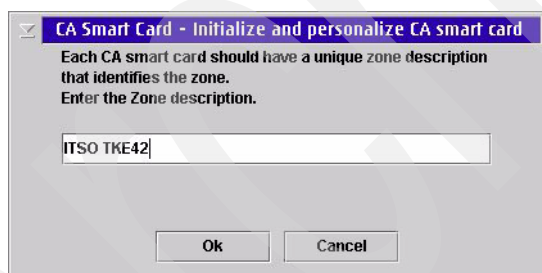


Figure 3-7 Enter the correct zone description

- After the Zone description is entered, you can provide an optional description to be stored in the CA card, as shown in Figure 3-8.

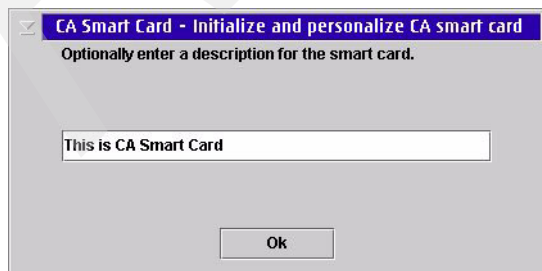


Figure 3-8 Optional description of this CA smart card

- After this data has been provided, the build of the CA smart card completes in about one minute, during which progress messages are displayed. Finally, the SCUP utility reads back the contents of the newly built card and displays the information on the window shown in Figure 3-9.

Remember, if the smart card is removed before completion of the building process, the initialization must be re-started from the beginning.

The screenshot shows the 'TKE Smart Card Utility Program Version 1.00' window. It has a menu bar with 'File', 'CA Smart Card', 'TKE Smart Card', '4758', and 'Help'. The main area is divided into two sections, 'Smart card reader 1' and 'Smart card reader 2'. Each section displays card details and a table of key parts.

Smart card reader 1 details:

- Card type: CA Smart Card v0.3
- Card ID: 607876E3S
- Card description: This is CA Smart Card
- PIN status: Ok
- TKE Authority key: 4758 Logon key:
- Zone enroll status: Enrolled
- Zone ID: 4138C51F
- Zone description: ITSO TKE42

Smart card reader 1 Key parts table:

Content type	Information	Origin	MDC-4	SHA-1	ENC-ZERO	Control vector	Length

Smart card reader 2 details:

- Card type: (empty)
- Card ID: (empty)
- Card description: (empty)
- PIN status: (empty)
- TKE Authority key: 4758 Logon key:
- Zone enroll status: (empty)
- Zone ID: (empty)
- Zone description: (empty)

Smart card reader 2 Key parts table:

Content type	Information	Origin	MDC-4	SHA-1	ENC-ZERO	Control vector	Length

Figure 3-9 The CA smart card content is displayed

Now the CA card can be removed from the reader and kept ready to be used for the other environment setup processes still to perform.

Important: Making one or more backups of the CA card is highly recommended. If the CA card is damaged or blocked (we explain card blocking later), it cannot be recovered or unblocked, no new entities can be enrolled, and existing entities cannot be unblocked or have their PIN reset. Damaging or blocking the CA card results in having to rebuild the complete PKI if no backup is available. There is no mechanism to reset a forgotten PIN in a CA card.

Backup of the CA card

The CA card is backed up using SCUP.

- Double-click the SCUP icon in the TKE folder. In the program window, select **CA Smart Card → Backup CA smart card**. You will be prompted to insert the source CA card into smart card reader 1, as shown in Figure 3-10 on page 50.

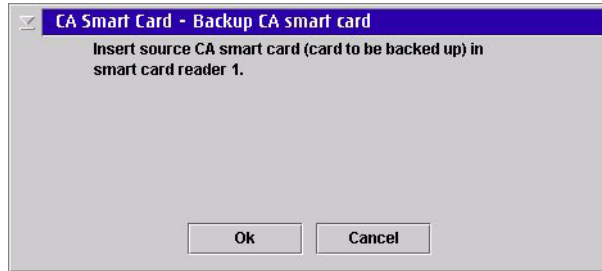


Figure 3-10 Insert the source CA card to reader 1

2. After the SCUP has verified the validity of the CA card in reader 1, the security officers are prompted to enter the first and second PIN of the source CA card.
3. Insert the target CA card into reader 2. The SCUP utility prompts for acceptance of overwriting old data if the target CA card is not empty.
4. When the target CA card initialization is complete, SCUP prompts for the first and second PIN for the new CA card, as shown in Figure 3-11. The PINs entered on the target reader PIN pad *must* be the same as the ones used to protect the source CA card.

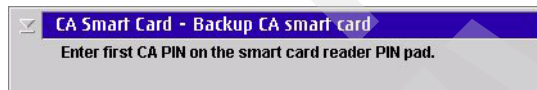


Figure 3-11 Enter the PIN for the target CA card

5. After a successful PIN entry, SCUP builds the backup CA card, which lasts for about one minute. When the backup CA card has been successfully built, SCUP reads the contents of both CA cards and displays the information as shown in Figure 3-12. If any smart card is removed before the completion of the backup process, the process must be re-started from the beginning.



Figure 3-12 Displaying the contents of the source and target CA cards

Enroll a local TKE 4758 Cryptographic Adapter

Important: The operations that we describe here are performed with the TEMPDEFAULT role loaded in the 4758. (The role is available as a result of running the 4758SCinitialize.cni file.) If the enroll is attempted while the normal DEFAULT role is in effect, then the enroll fails with access denied (8/90), and the TEMPDEFAULT has to be loaded from CNM. In any case, when smart card environment initialization is done, ensure that the normal DEFAULT role is reloaded or security will be compromised, as the TEMPDEFAULT role has all privileges.

The local 4758, located inside the TKE workstation, must be enrolled to the zone:

1. Start the SCUP utility by selecting **4758** → **Enroll 4758**, as shown in Figure 3-13.

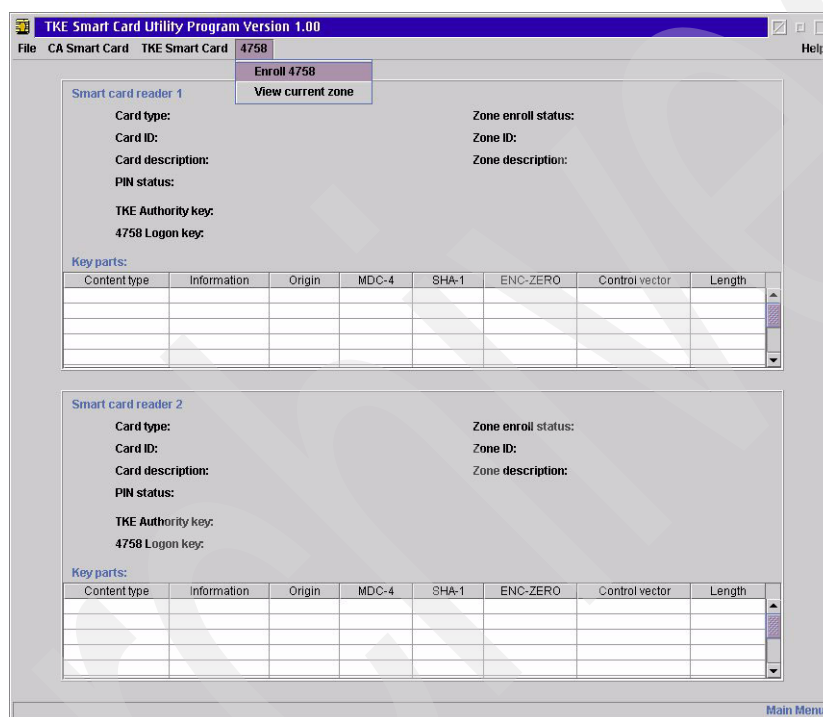


Figure 3-13 Select Enroll 4758

2. Choose whether this process is to enroll a local or remote 4758. We select **Local** and click **OK** (Figure 3-14).

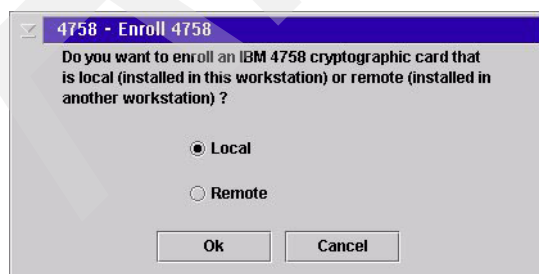


Figure 3-14 Selecting to enroll the local 4758 Crypto card

3. You are prompted to insert the CA card in smart card reader 1 and to enter the CA card PIN values on the reader 1 PIN pad. After the correct CA PINs have been entered, the

4758 generates a retained key pair (that is, the private key will never leave the secure enclosure of the cryptographic adapter), and an enroll request certificate is sent to the CA card to be signed, as shown in Figure 3-15.



Figure 3-15 Generating the enroll request

4. The CA card adds the Zone ID and the Zone description information to the enroll certificate request before signing it and sending it back to the local TKE 4758.

Note: The signature of the enroll certificate request is performed completely inside the smart card itself.

Enroll a Remote TKE 4758 Cryptographic Adapter

The enrollment process is split between the local and remote TKEs. The enrollment certificate request is created at the remote TKE and transmitted to the local TKE using a diskette. The request is then completed and signed by the CA card attached to the local TKE. The signed enrollment certificate is then transferred and installed into the remote TKE. These steps are summarized as:

1. Create the enrollment request at the remote TKE by executing **ENROLL_REQ.CMD** in the c:\TKE\SCUP folder of the remote TKE workstation. Follow the instructions to store the enrollment request on a diskette.
2. On the local TKE workstation start SCUP utility, select **4758 → Enroll 4758**.
3. In the next window, select **Remote** to enroll the remote 4758 and click **OK**. Confirm that the remote enrollment request is available to be processed, as shown in Figure 3-16.

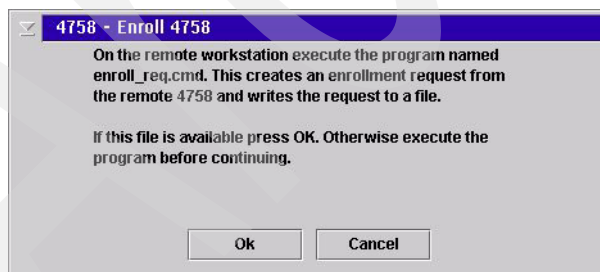


Figure 3-16 The Remote 4758 enrollment request must be available

4. The enrollment process continues at the local TKE by requesting insertion of the CA card in smart card reader 1 and entry of the CA card PIN values at the reader PIN pad. After the correct CA PINs have been entered, designate the remote enrollment request file that is waiting to be processed, as shown in Figure 3-17 on page 53.

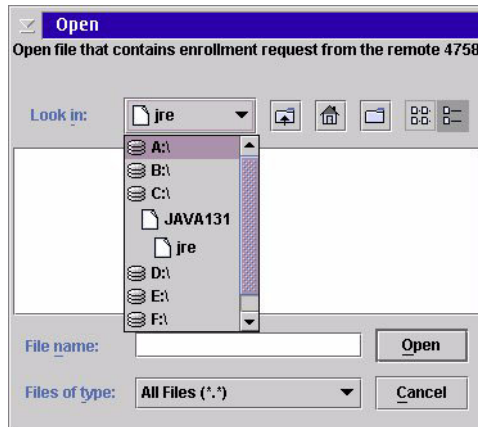


Figure 3-17 Select the Remote 4758 enrollment request file

5. The enrollment certificate request is sent to the local CA card for the certification. After completing the certificate request, the CA card signs the enrollment certificate, which is then stored in a file to be eventually transferred to the remote TKE.
6. To install the certified enrollment request into Remote 4758, execute **ENROLL_INST.CMD** in the c:\TKE\SCUP folder of the remote TKE workstation and follow the instructions.

View zone information

To view the current zone information on the 4758, start the SCUP utility by selecting **4758** → **View current zone**, as shown in Figure 3-18.

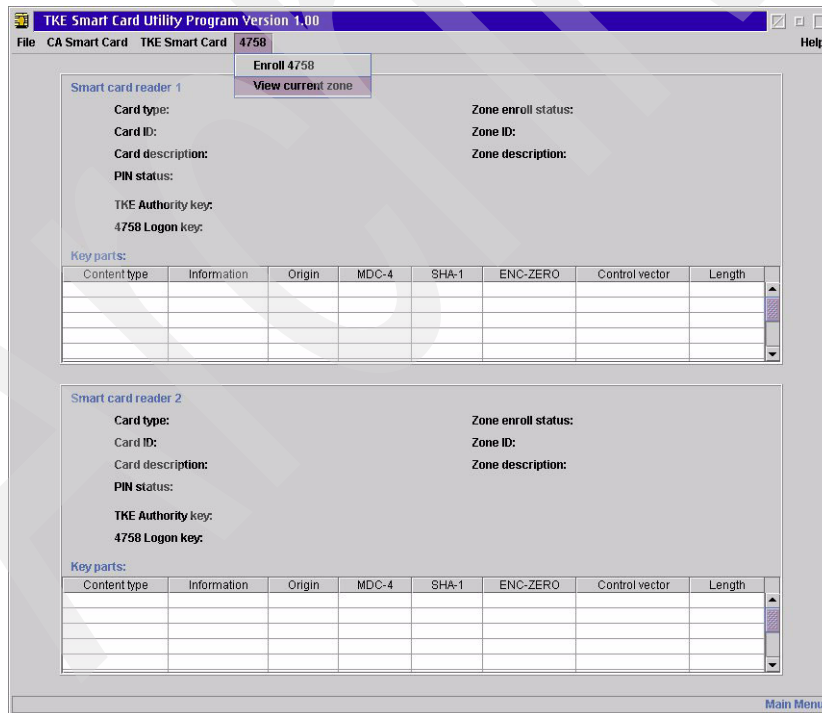


Figure 3-18 Select View current zone from the 4758 menu

The window shown in Figure 3-19 on page 54 opens, displaying the zone ID and the zone description information from the local 4758. To view the zone information in other TKE workstations, you must start SCUP in those TKEs.

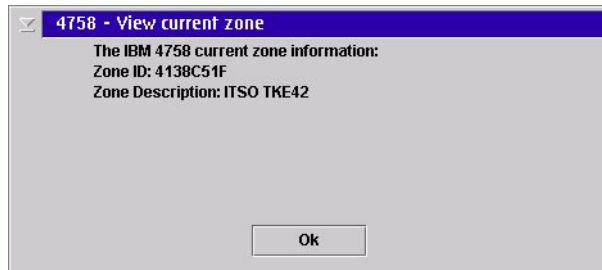


Figure 3-19 Zone information displayed from the 4758

Initialize and enroll the TKE card

The TKE card is initialized by using SCUP:

1. Double-click the SCUP icon in the TKE folder. Select **TKE Smart Card** → **Initialize and enroll TKE smart card**, as shown in Figure 3-20.

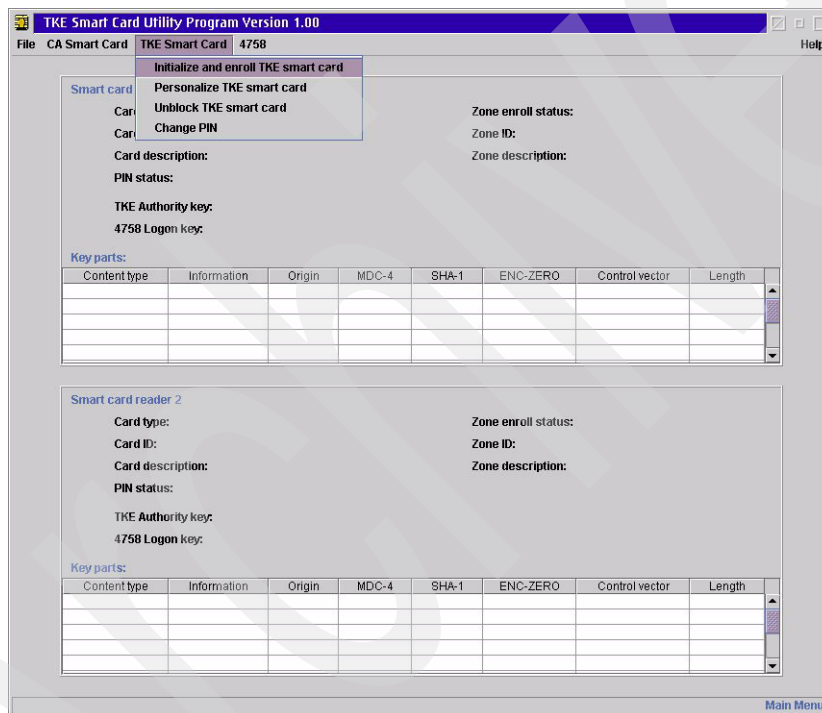


Figure 3-20 Select Initialize and enroll TKE smart card

2. The TKE card enrollment process continues with a request to insert the CA card in smart card reader 1 and to enter both CA card PIN values at the reader PIN pad.
3. After the correct CA PINs have been entered, the TKE card to be initialized has to be inserted into smart card reader 2, as shown in Figure 3-21 on page 55.

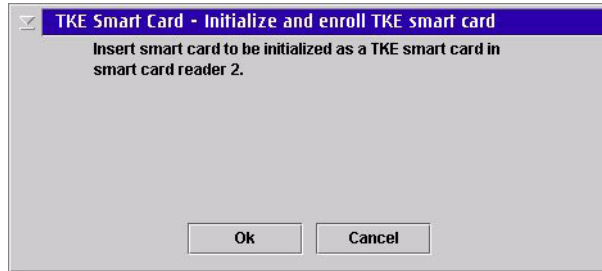


Figure 3-21 Insert the TKE card into smart card reader 2

If the inserted TKE card is not empty, the program will prompt for a confirmation to overwrite the existing data. If confirmed, the initialization process continues for about one minute. It takes another minute to complete the build of the TKE card.

4. When the build process ends successfully, SCUP reads the contents of the cards in the smart card readers and displays the result in the window shown in Figure 3-22.

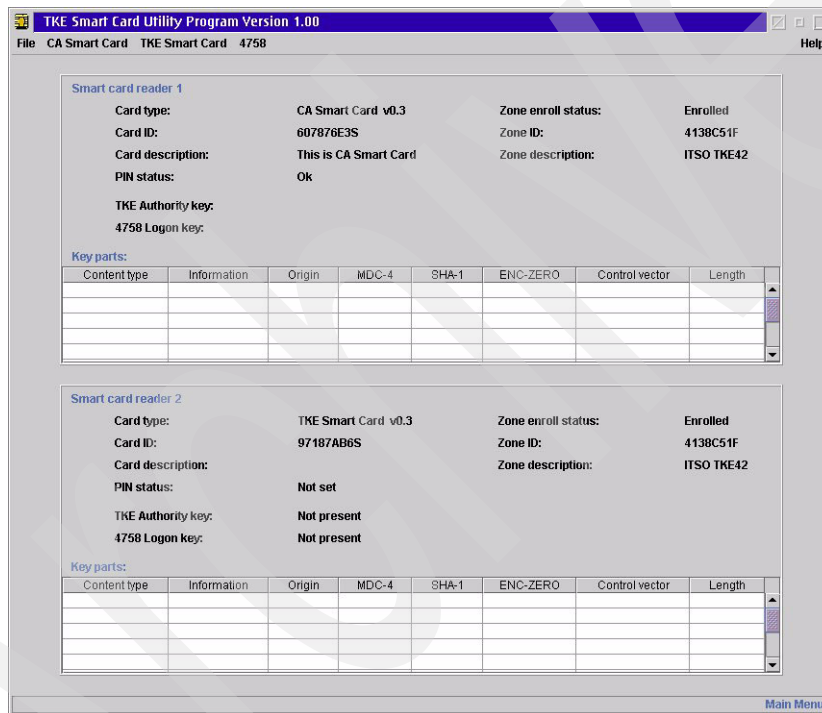


Figure 3-22 Displaying the contents of the CA and TKE cards

Notes:

- During the initialization process, an RSA key pair is generated inside the TKE smart card; the generated private key is never to leave the card.
- At this stage we have completed the initialization and enrollment of the TKE card. The personalization step, where the TKE card PIN will be specified, follows.
The initialization and enrollment process can be performed by somebody other than the final owner of the card. It is expected that the owner of the card will attend the personalization process to specify the PIN to be used to protect the card.

Personalizing the TKE card

The personalization of the TKE card is accomplished with SCUP:

1. Double-click the SCUP icon in the TKE folder. In the program window, select **TKE Smart Card → Personalize TKE smart card**.
2. You are prompted to insert the TKE card into smart card reader 2 and enter a PIN value twice on the reader 2 PIN pad to protect the TKE smart card. This is a four-digit PIN that is used to protect the card.
3. Optionally, after entering the PIN, enter a description of the TKE card to be personalized, as shown in Figure 3-23.

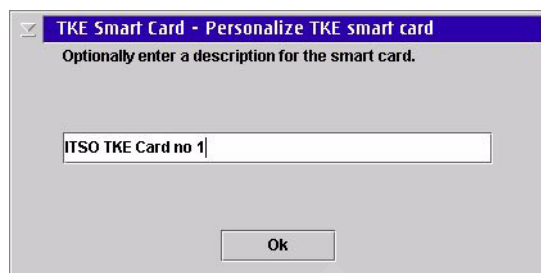


Figure 3-23 Optional description of the TKE smart card

4. When the personalization process ends, SCUP reads the contents of the TKE card in the smart card reader and displays the result in the window shown in Figure 3-24.

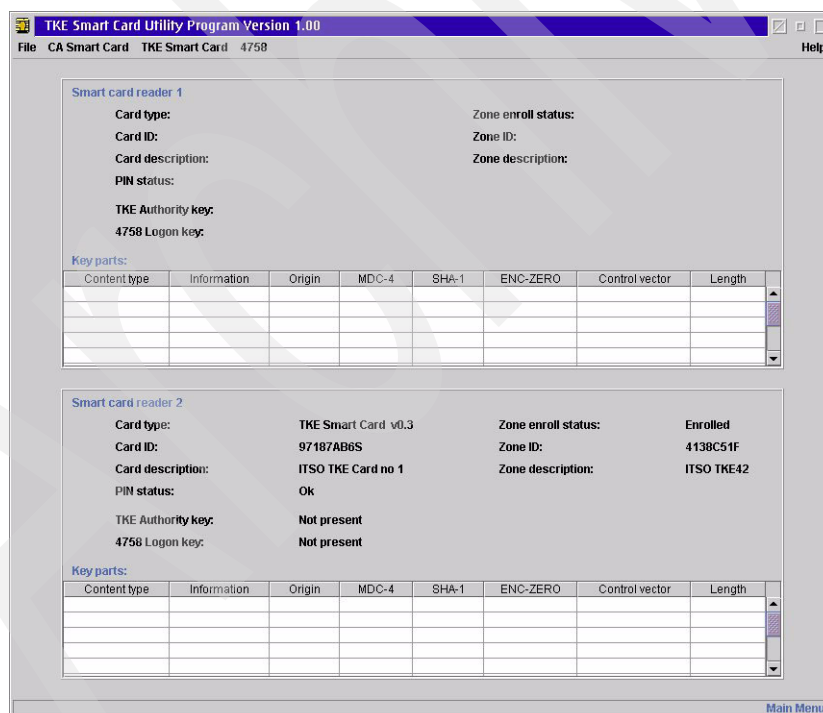


Figure 3-24 Displaying the content of the personalized TKE card

Backing up the TKE card

There is no utility to back up the TKE smart card. However, the Utilities menu in the TKE main window offers a function to copy keys (4758 Logon and Authority Signature) and key parts (operational, ICSF master keys, and 4758 master keys) from one card to another.

3.3 Managing changes to the smart card environment

You may need to change operating conditions while the entities are using their smart cards. The operating environment changes that are supported for TKE smart card are:

- ▶ Changing the PIN of a TKE smart card or a CA card
- ▶ Unblocking a TKE smart card

When a TKE user enters a wrong PIN three times in a row, the TKE smart card becomes blocked, and it cannot be used until it is unblocked with the CA smart card.

Important: A CA smart card can also be blocked after five wrong PINs entered in a row. *There is no process available to unblock a CA smart card.*

Having the CA card blocked implies:

- ▶ Not being able to enroll new entities
- ▶ Not being able to unblock TKE smart cards

This eventually leads to having to rebuild the smart card environment.

Changing the TKE card PIN

This can be done using SCUP or the CNM utility; we demonstrate using SCUP:

1. Double-click the SCUP icon in the TKE folder. In the program window, select **TKE Smart Card** → **Change PIN**, as shown in Figure 3-25.

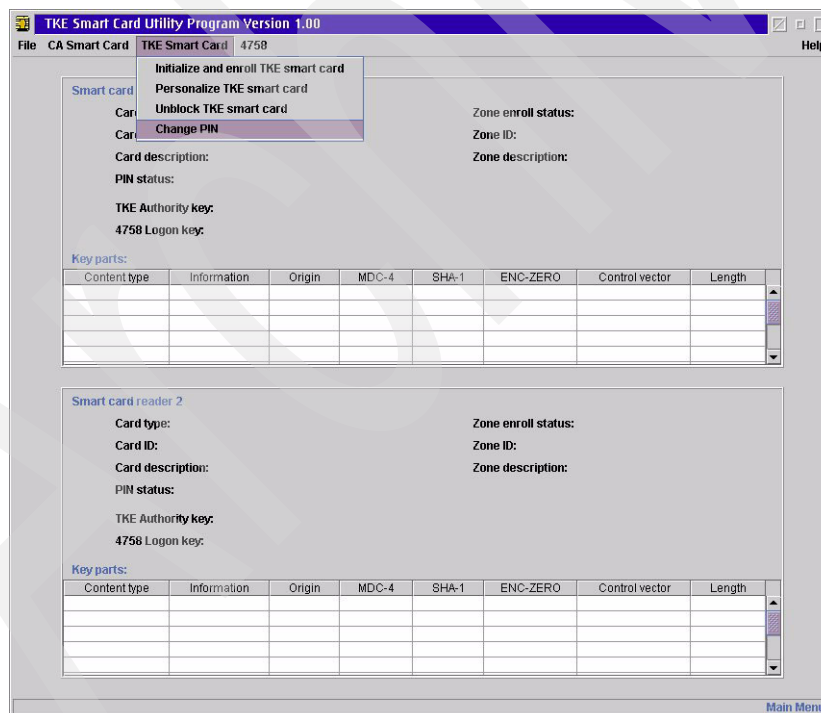


Figure 3-25 Selecting Change PIN for the TKE card

2. You are prompted to insert the TKE card in smart card reader 2 and enter the current PIN value for verification.
3. After the current PIN value has been entered, the PIN change process prompts for the new four-digit PIN value to be entered twice on card reader 2. When the new PIN is stored in the TKE card, a confirmation window pops up.

Changing the CA card PIN

If either of the CA smart card PINs must be changed, this can be done only by using SCUP.

1. Double-click the SCUP icon in the TKE folder. In the program window, select **TKE Smart Card** → **Change PIN**, as shown in Figure 3-26.

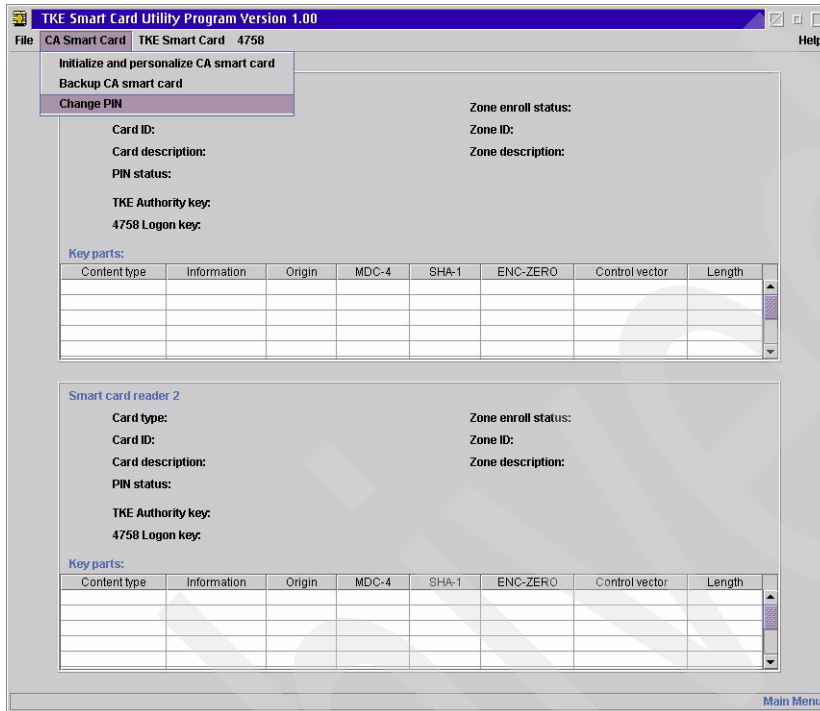


Figure 3-26 Selecting Change PIN for the CA card

2. You are prompted to insert the CA card into smart card reader 1 and asks which of the CA smart card PINs will be changed, as shown in Figure 3-27. If both PINs must be changed, the process must be run independently for each PIN.



Figure 3-27 Select which CA smart card PIN is changed

3. The process prompts for the current value of the selected CA PIN for verification. Then the PIN change process prompts for the new six-digit PIN value to be entered twice on card reader 1. When the new PIN is stored in the CA card, a confirmation window pops up.

Unblocking the TKE smart card

If the TKE smart card PIN is entered incorrectly three times in a row, the smart card reader blocks the TKE card, and it cannot be used until it has been unblocked. Each unsuccessful attempt to enter a correct PIN is indicated in the application window, as shown in Figure 3-28.

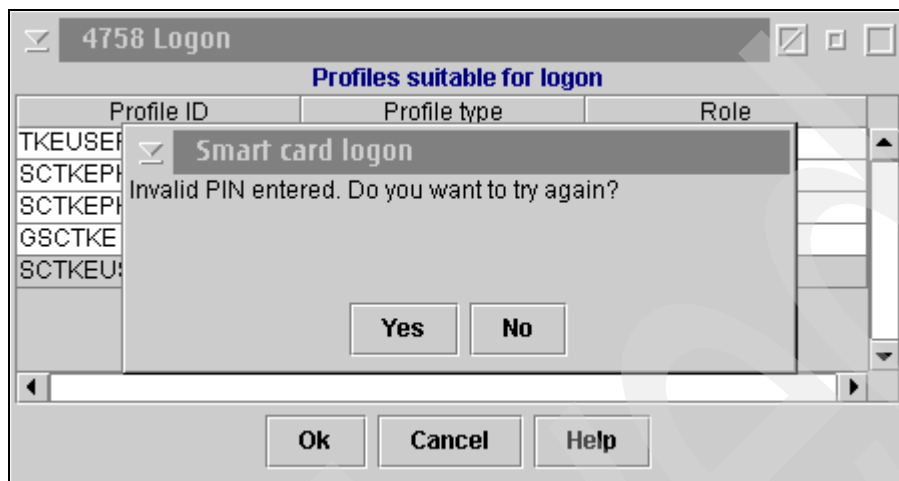


Figure 3-28 Wrong PIN entered

At the third unsuccessful attempt to enter the correct PIN, the card reader blocks the card and the user is informed via the pop-up message shown in Figure 3-29.



Figure 3-29 TKE card blocked pop-up message

This is confirmed by displaying the smart card status in SCUP, as shown in Figure 3-30 on page 60.

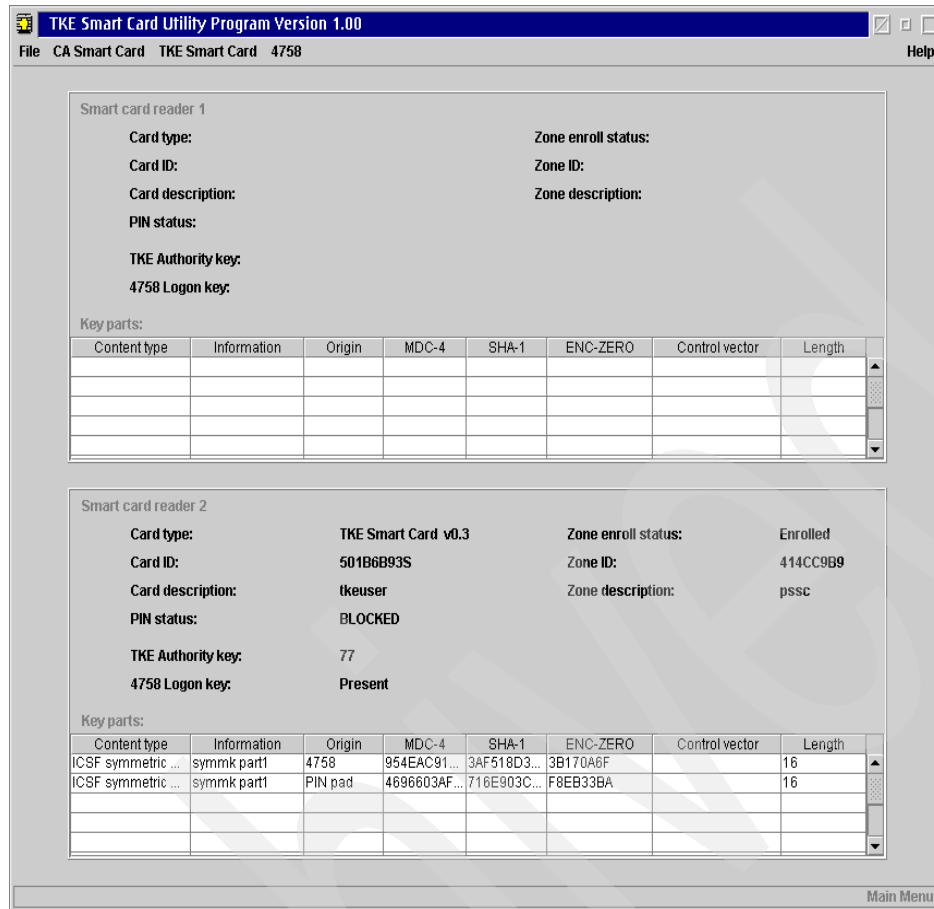


Figure 3-30 The PIN status shows **BLOCKED**

Unlocking of the TKE card can be achieved only by using SCUP.

1. Double-click the SCUP icon in the TKE folder. In the program window, select **TKE Smart Card** → **Unblock TKE smart card**.
2. The TKE card unblock process prompts to insert the CA card into smart card reader 1, as shown in Figure 3-31. The CA smart card must then be opened by entering the CA PINs at on the card reader 1 PIN pad.

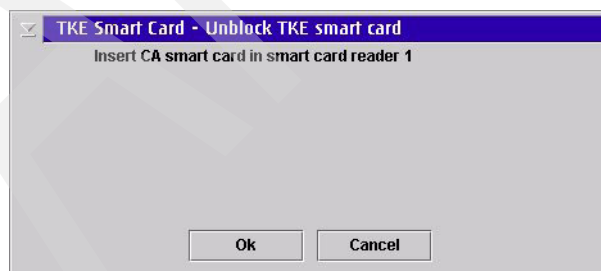


Figure 3-31 Insert the CA card into smart card reader 1

3. You are prompted to insert the blocked TKE card in smart card reader 2, as shown in Figure 3-32.

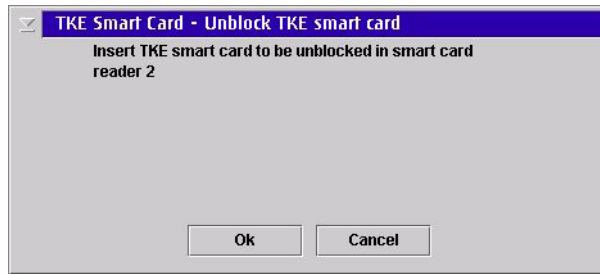


Figure 3-32 Insert the TKE card into smart card reader 2

4. When the TKE smart card PIN is unblocked, a confirmation window pops up.

Note: Unlocking the TKE smart card does not reset or change the PIN value; it simply resets the invalid PIN attempts counter. To resume using the smart card, you still have to enter the specified PIN at card personalization.

3.4 Exploiting the smart card environment

We now provide some examples of the use of the smart card.

3.4.1 Preparing the smart card and 4758 profiles to log on to CNM or the TKE

In this process, we establish the smart card as a means to authenticate to the TKE 4758 Cryptographic Adapter as an alternative to entering an authentication passphrase.

A preliminary step is to provide a 4758 logon key pair to the TKE user smart card. This is described next.

Important: The operations that we describe here are performed with the TEMPDEFAULT role loaded in the 4758 (the role is available as a result of running the .cni file), but it can also be performed with the TKEADM role. Be aware that if you were to reload the TEMPDEFAULT role, you would have to ensure that the normal DEFAULT role is reloaded when complete, or security will be compromised because the TEMPDEFAULT role has all privileges.

Generation of a 4758 logon key

1. Double-click the CNM icon in the TKE folder. In the CNM utility window, select **Smart Card** → **Generate 4758 Logon Key**, as shown in Figure 3-33.

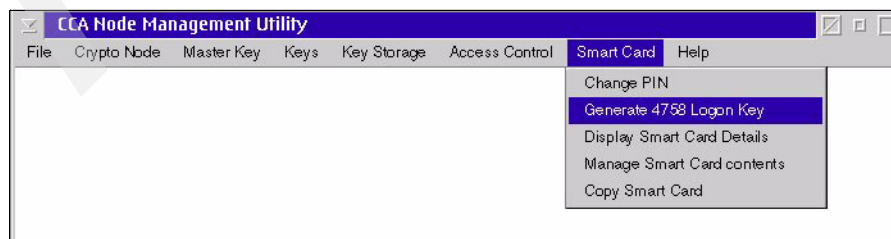


Figure 3-33 Selecting the Generate 4758 Logon Key function in CNM

2. Insert the TKE smart card into card reader 2 (Figure 3-34).



Figure 3-34 Insert a smart card

3. Enter the user ID that will be authenticated with the TKE smart card into the field shown in Figure 3-35.



Figure 3-35 Associating a user ID to the smart card

4. The 4758 Logon Key is generated and confirmed with the message shown in Figure 3-36, which indicates that the smart card can be used to authenticate for the user ID (the 4758 profile) that was entered in the previous step.



Figure 3-36 4758 Logon Key generation complete

Specifying smart card authentication in a TKE 4758 profile

The smart card was given a user ID (a 4758 profile name) in the previous step and an RSA key pair to be used eventually to authenticate against the 4758 profile. The 4758 profile now must be created using smart card authentication.

Note: An existing profile that uses passphrase authentication cannot be updated to operate with smart card authentication. It must be deleted then created again specifying that smart card authentication will be used.

Important: However, we recommend *not* giving the name of the passphrase profile to the smart card profile:

- ▶ Saving these new smart card profiles to the hard disk would overwrite the passphrase profiles, which still might be useful if something goes wrong.
- ▶ Not saving these profiles to disk results in a TKE code upgrade or 4758 replacement to restore the passphrase profiles that have the same names.

To define a new 4758 profile with user authentication by smart card:

1. Click the CNM utility icon in the TKE folder, and select **Access Control** → **Profiles**, as shown in Figure 3-37.

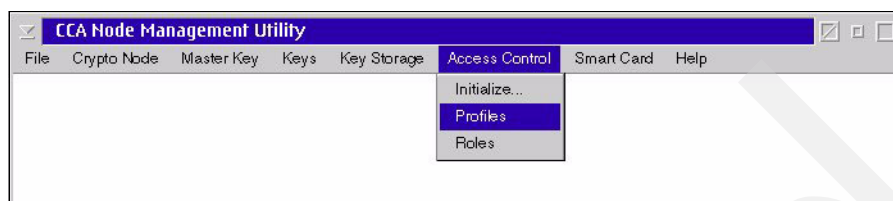


Figure 3-37 Preparing to update the 4758 profiles

2. A list of existing 4758 profiles opens, as shown in Figure 3-38. Click **New** (or **Delete** if the profile already exists and has to be re-created with smart card authentication).

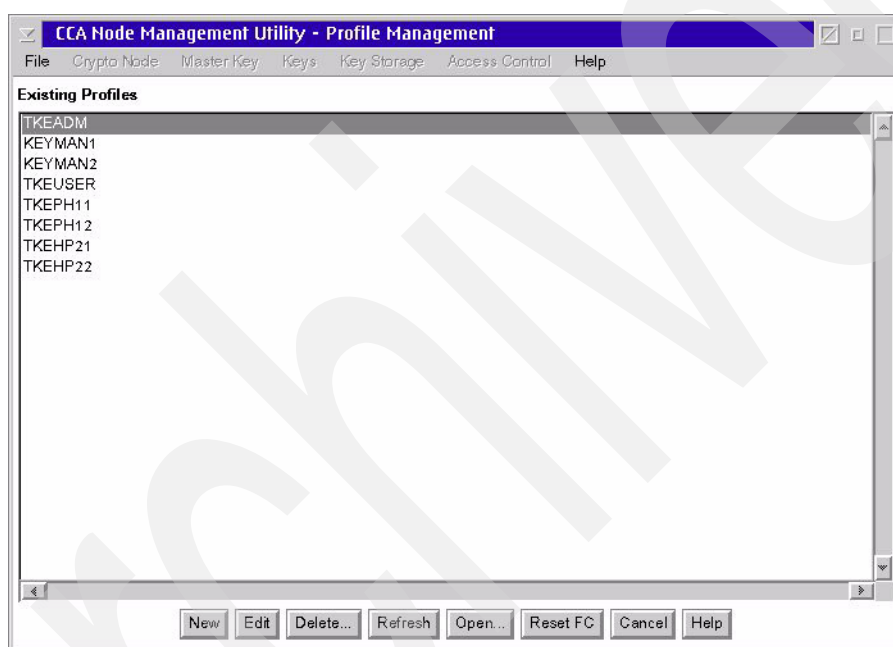


Figure 3-38 List of existing profiles and options

3. Assuming that you have clicked New, select the profile type as shown in Figure 3-39. We choose the **Smart card** type of profile.



Figure 3-39 Choosing the profile type

4. Insert the TKE user smart card into card reader 2 (Figure 3-40 on page 64), which has had a key pair generated and a user ID associated to it.



Figure 3-40 Inserting the smart card for profile creation

5. The CNM utility reads the public information from the card: the user ID that was assigned at 4758 Logon Key generation and the card public modulus, which will be used to check for the card signature during the logon process. This information is displayed in the CNM Profile Management menu, as shown in Figure 3-41.

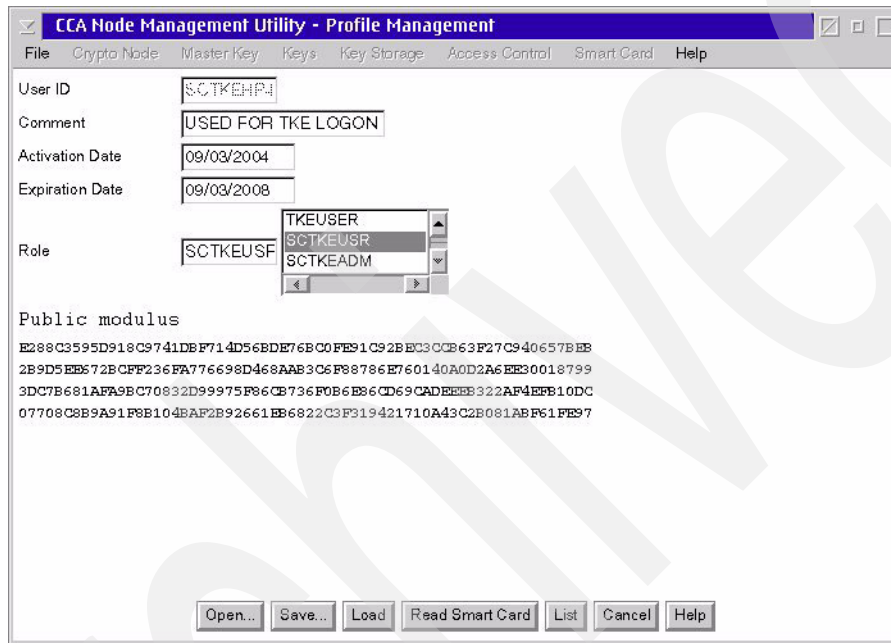


Figure 3-41 User ID and public modulus set in the smart card

This menu is used to complete the profile definition and the new profile must be loaded into the 4758.

Note: Pressing the Read Smart Card button refreshes the value of the public modulus that is kept in the profile, in case the 4758 logon key of the inserted smart card has been changed since the profile was created.

Preparation of a smart card logon group

As noted in Chapter 2, “TKE V4.2 Group Logon feature” on page 27, a logon group has the following characteristics:

- After a successful group logon, the users will be in the group's role. As an example, consider a group in the SCTKEUSR role with each member of the group in the DEFAULT role. After the group logon has been performed successfully, the group members have the privileges of the SCTKEUSR role. This is the typical setup for a TKE users' logon group in which each individual user does not have the proper privilege to use the TKE.
- When defining a logon group, the TKE administrator must specify whether the members of the group will use a passphrase or a smart card to authenticate. Note that all members of

a given logon group must use the same authentication mechanism, because mixing passphrase and smart card authentication in the same group is not permitted.

Definition of the members profiles

Smart cards are prepared as shown in “Generation of a 4758 logon key” on page 61, and group member profiles are defined as indicated in “Specifying smart card authentication in a TKE 4758 profile” on page 62. Figure 3-42 shows an example of a typical member profile, the member being in the DEFAULT role.

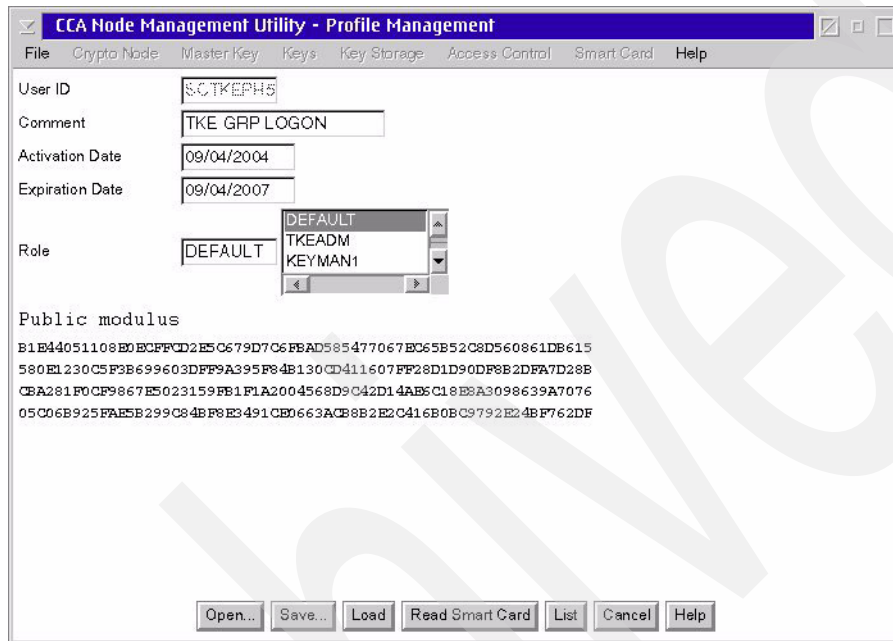


Figure 3-42 typical profile for a smart card group member

To create the new group in the CNM Profiles Management menu, click **New**, and select the **Group** type of profile as shown in Figure 3-43.



Figure 3-43 Specifying the Group type of profile

The logon group profile is specified as shown in Figure 3-44. Here the selected user profiles are picked from smart card profiles, as indicated by the selected radio button on the left. Highlight the member to be added to the group in the available profiles and click **Add**.

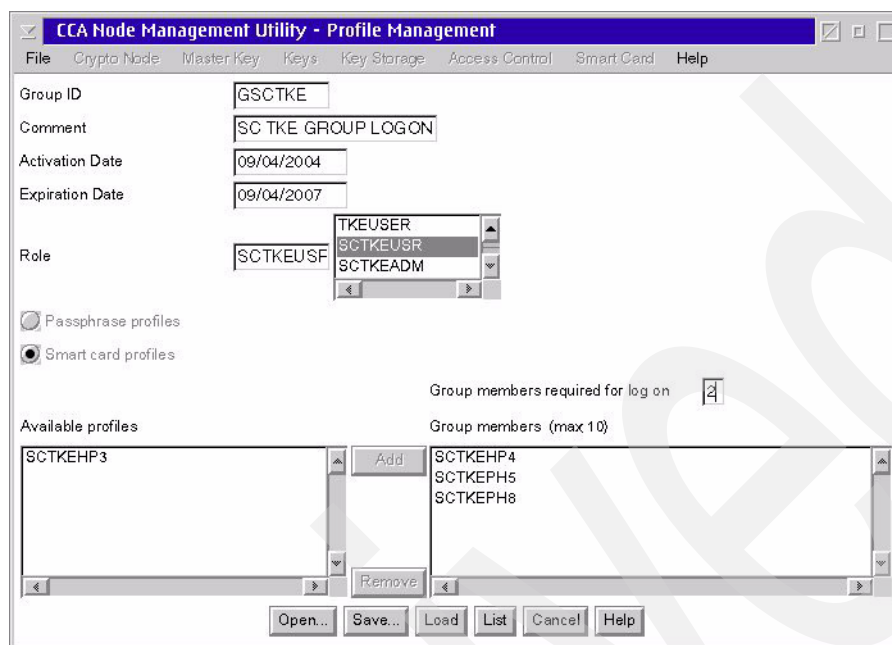


Figure 3-44 Selecting the member of the logon group

3.4.2 Using the smart card to log on to CNM

In the CNM main window, select **File** → **Smart Card Logon**, as shown in Figure 3-45.



Figure 3-45 Starting log on to CNM using the smart card

Insert the smart card into a card reader and enter the PIN, as requested in the message shown in Figure 3-46. The smart card demonstrates to CNM, using digital signature, that it has the private key associated to the user ID bound to the card. This, with the card having been opened with the correct PIN, is a proof of authentication for CNM.

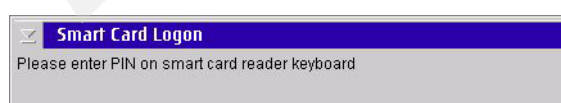


Figure 3-46 Entering the PIN to logon to CNM

3.4.3 Using the smart card to log on to the TKE application

With TKE V4.2, the set of user or group profiles that are displayed as suitable for logon map to roles with permission to access control point 0x8002. If the role does not contain this access control point, the profile cannot be used to log on to the 4758 for the TKE application. Note that the list (Figure 3-47) also indicates whether the user or group profile is using passphrase or smart card authentication.

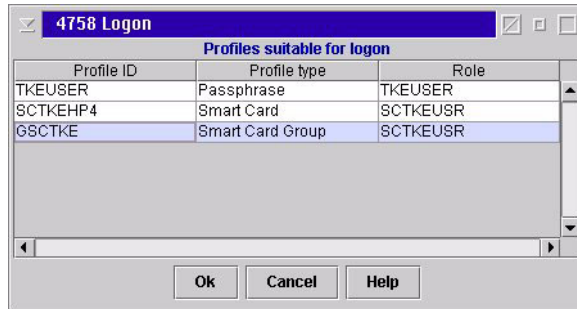


Figure 3-47 Presenting all profiles in the TKEUSER role or equivalent

1. In this example, we log on as group GSCTKE. When the group is selected in the logon profiles above, the window in Figure 3-48 is displayed, indicating how many members are required to log on. Here, two members are required from the group's three members, but none of them have logged on yet.

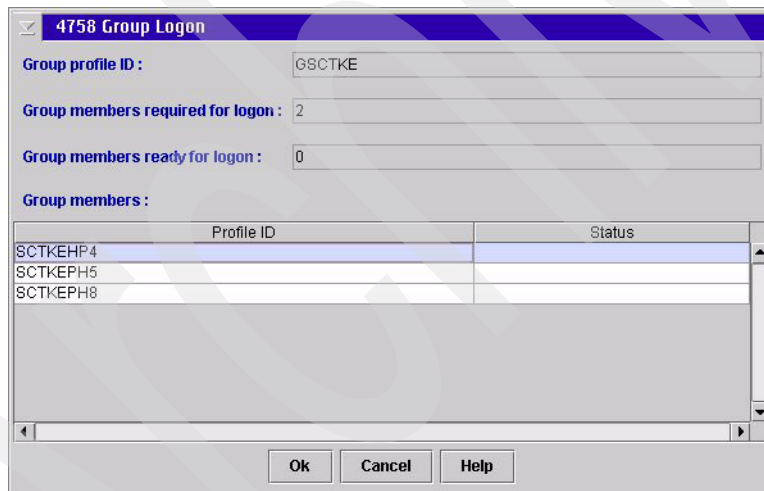


Figure 3-48 smart card logon group

2. After you select the member who will log on next, the prompt in Figure 3-49 appears.



Figure 3-49 Preparing to log on a group member

- After inserting the smart card of user SCTKEHP4 and entering a correct PIN, the authentication process takes place and the group logon panel is updated to indicate that user SCTKEHP4 successfully logged on, as shown in Figure 3-50.

4758 Group Logon

Group profile ID : GSCTKE

Group members required for logon : 2

Group members ready for logon : 1

Group members :

Profile ID	Status
SCTKEHP4	ready for logon
SCTKEPH5	
SCTKEPH8	

Ok Cancel Help

Figure 3-50 The first user of the smart card group has logged on

The 4758 logon is not complete until the required number of logged on members has been met. If authentication fails for any member of the group then the entire group logon must be redone.

3.4.4 Using the smart card to hold a TKE Authority signature key

In this section we describe how the smart card can be used to hold a TKE Authority key pair as an alternative to using a diskette.

Generating the Authority signature key

The process is initiated independently of where the key pair will be kept, be it a smart card or a diskette, using the Authority Administration panel for the target coprocessor or group of coprocessors, as shown in Figure 3-51.

Crypto Coprocessor Module Group Administration : PCIXCC grp. Master Crypto Module : z/OS R6 / X00

Function

General Details Roles Authorities Domains Co-Sign

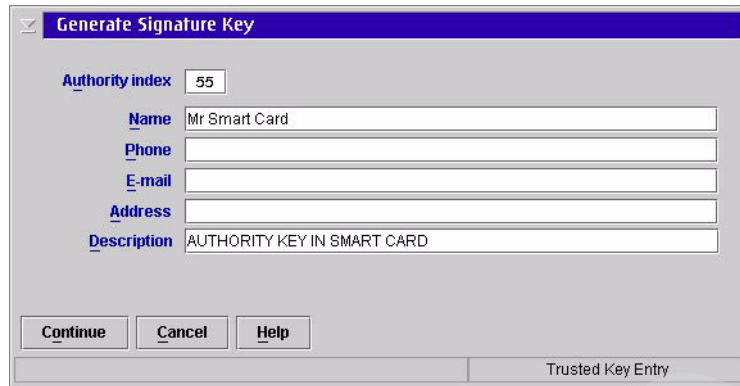
Authorities

Index	Name	Role	Phone	E-mail	Addr	Description
0		INITADM				
11	TOTAL POWER	TOTALADM				

Create Authority
Change Authority
Delete Authority
Generate Signature Key

Figure 3-51 Initiating the TKE Authority key pair generation

1. Enter information about the Authority, still regardless of the key pair storage media, as shown in Figure 3-52. Click **Continue** to complete the key generation process.

A dialog box titled "Generate Signature Key" with a blue header bar. It contains several input fields: "Authority index" with the value "55", "Name" with "Mr Smart Card", "Phone", "E-mail", "Address", and "Description" with "AUTHORITY KEY IN SMART CARD". At the bottom are three buttons: "Continue", "Cancel", and "Help". A "Trusted Key Entry" label is in the bottom right corner.

Generate Signature Key

Authority index 55

Name Mr Smart Card

Phone

E-mail

Address

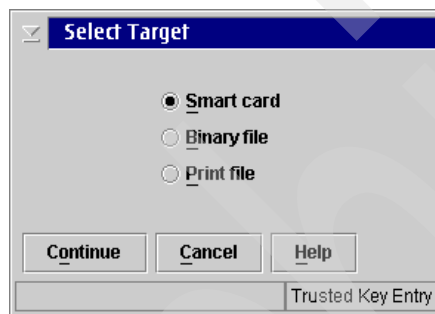
Description AUTHORITY KEY IN SMART CARD

Continue Cancel Help

Trusted Key Entry

Figure 3-52 Providing TKE Authority information

2. Select a target storage device in the pop-up window shown in Figure 3-53. In our case, we select **Smart card**.

A dialog box titled "Select Target" with a blue header bar. It contains three radio button options: "Smart card" (selected), "Binary file", and "Print file". At the bottom are three buttons: "Continue", "Cancel", and "Help". A "Trusted Key Entry" label is in the bottom right corner.

Select Target

☒ Smart card

☐ Binary file

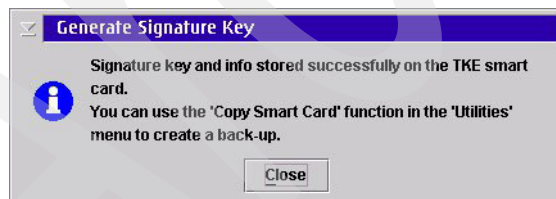
☐ Print file

Continue Cancel Help

Trusted Key Entry

Figure 3-53 Selecting the storage target device

3. Insert the Authority smart card in card reader 2 and enter the PIN. The process completes with the message shown in Figure 3-54.

A dialog box titled "Generate Signature Key" with a blue header bar. It contains an information icon (i) and the following text: "Signature key and info stored successfully on the TKE smart card. You can use the 'Copy Smart Card' function in the 'Utilities' menu to create a back-up." At the bottom is a "Close" button.

Generate Signature Key

Signature key and info stored successfully on the TKE smart card.
You can use the 'Copy Smart Card' function in the 'Utilities' menu to create a back-up.

Close

Figure 3-54 Authority key pair stored onto the smart card

Note: From now on, the private signature key is never to leave the smart card. Any computation involving this key will be performed inside the smart card.

Creating the Authority in the coprocessor

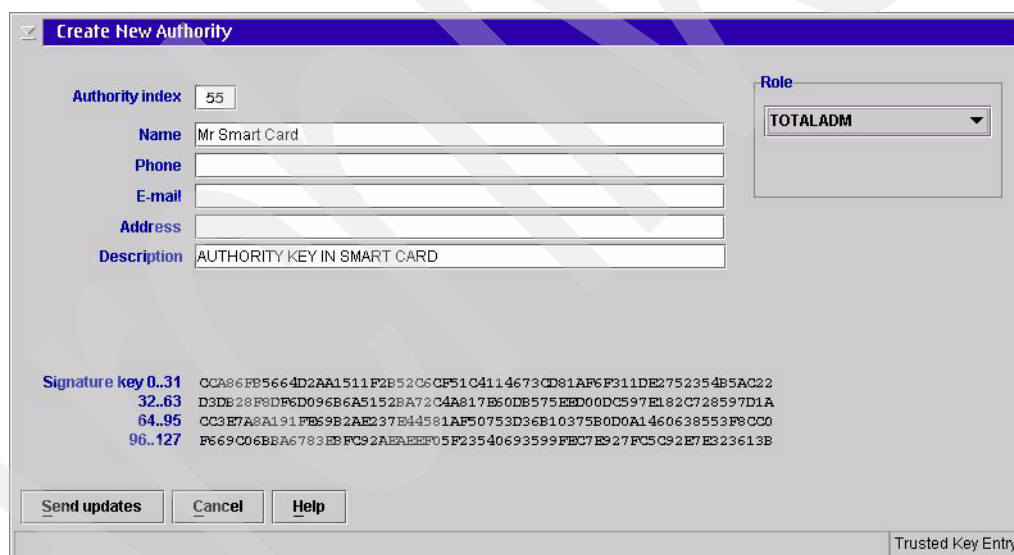
The public modulus of the Authority has to be retrieved and sent to the coprocessor using the Create Authority function at the TKE. Retrieval of the modulus is done using one of several possible storage media. Select the retrieval source in the window shown in Figure 3-55. In our case the retrieval is done from the card in card reader 2.



A dialog box titled "Select Source" with a close button (X) in the top left corner. It contains five radio button options: "Smart card in reader 1", "Smart card in reader 2" (which is selected), "Binary file", "Key storage", and "Default key". At the bottom, there are three buttons: "Continue", "Cancel", and "Help". A status bar at the very bottom reads "Trusted Key Entry".

Figure 3-55 Authority modulus retrieval source

After you enter the correct PIN for the card, the Create Authority menu appears, pre-filled with the information read from the card (Figure 3-56). To create the Authority at the coprocessor, click **Send Updates**.



A dialog box titled "Create New Authority" with a close button (X) in the top left corner. It contains several input fields and a table. On the right, there is a "Role" dropdown menu set to "TOTALADM". At the bottom, there are three buttons: "Send updates", "Cancel", and "Help". A status bar at the very bottom reads "Trusted Key Entry".

Authority index	55
Name	Mr Smart Card
Phone	
E-mail	
Address	
Description	AUTHORITY KEY IN SMART CARD

Signature key 0..31	0CA86FB5664D2AA1511F2B52C6CF51C4114673CD81AF6F311DE2752354B5AC22
32..63	D3DE28F8DF6D096B6A5152BA72C4A817B60DB575EED00DC597E182C728597D1A
64..95	CC3E7A8A191FB69B2AE237E44581AF50753D36B10375B0D0A1460638553F8CC0
96..127	F669C06BBA6783EBFC92A8AEEF05F23540693599FEC7E927FC5C92E7E323613B

Figure 3-56 Authority information read from the smart card and ready to be sent to the coprocessor

Loading a signature key from the smart card

Figure 3-57 shows a request to load a signature key from the TKE coprocessor management window (**Function** → **Load signature key**).

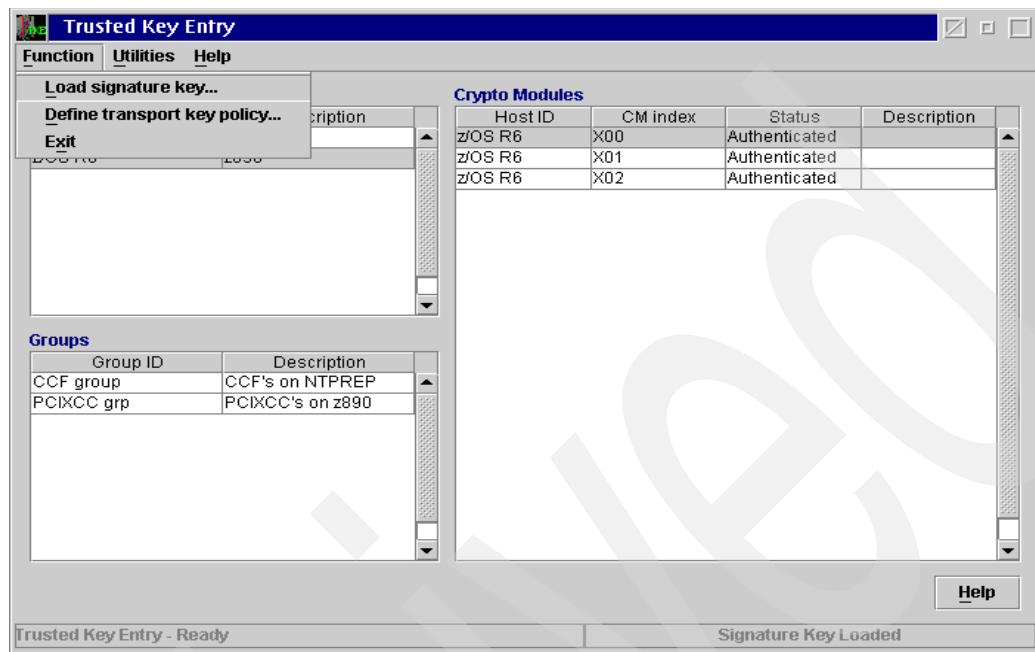


Figure 3-57 Requesting to load a signature key

In the pop-up window shown in Figure 3-58, select the source of the signature key, which in our case is a smart card.



Figure 3-58 Selecting the source of the signature key

We have created an example where the TKE application discovers our mistake, that when the card has been opened with the PIN, that there is no Authority signature key on it. This is reported to the operator in the message shown in Figure 3-59.



Figure 3-59 No Authority signature key in this card!

Assuming that there is a valid Authority signature key in the smart card, then the command to the zSeries coprocessor will be signed *inside* the smart card to preserve the secrecy of the signature key, then sent to the coprocessor by the TKE workstation.

3.4.5 Using the smart card to store TKE 4758 and zSeries coprocessors keys

Note: In the following processes, the secret (the ICSF key part) is actually created in the TKE 4758. A *secure session* is established to transfer these secrets from and to the smart card. A secure session consists of automatically establishing, at both the 4758 and the smart card, a symmetric session key that is used to encrypt the transferred secret with the Triple DES algorithm. The symmetric session key is generated by the 4758 and securely transmitted to the smart card using public key cryptography.

Note: Up to 10 key parts (4758 master key parts, ICSF master key parts, or ICSF operational key parts) can be stored in the smart card.

In this section, we provide some examples of the use of the smart card for some TKE administrative procedures. The full description of all functions that can be performed at the TKE is given in the reference book *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SA22-7524.

Storing TKE 4758 master key parts

TKE 4758 master key parts can be generated and stored into a smart card. Select **Master Key** → **Smart Card Parts** as shown in Figure 3-60.



Figure 3-60 TKE 4758 Master Key management options

Follow the prompt to insert the smart card into the smart card reader. (The PIN is not required at this point.) The smart card description is displayed at the top of the CNM Smart Card Master Key Parts panel; if there were already 4758 master key parts in the smart card their label would be displayed in the container. Figure 3-61 shows no parts already stored in the card. After selecting the key part to be generated, click **Generate & Save** to trigger the key part generation process.

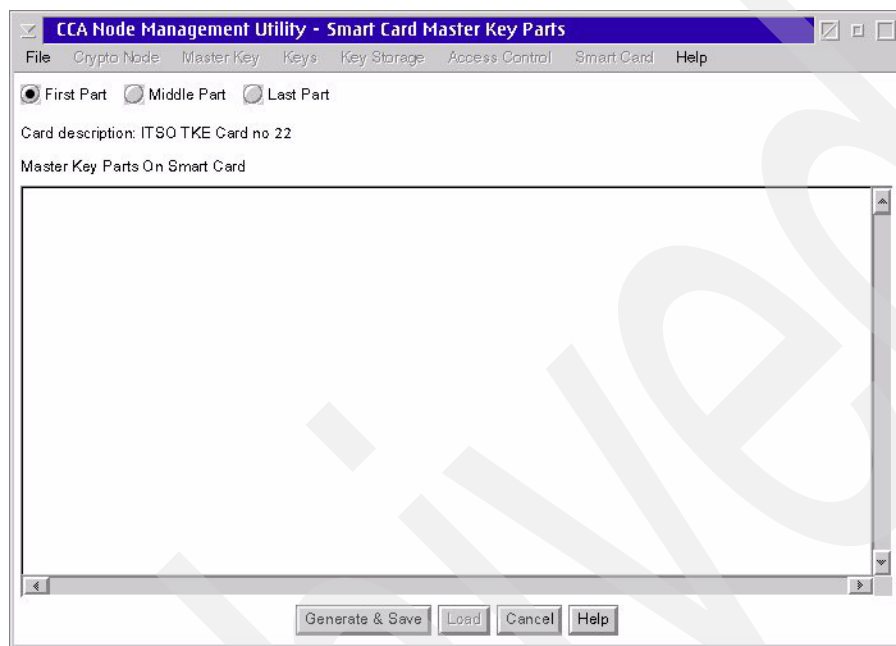


Figure 3-61 TCNM Smart Cards Master Key Parts panel

You are prompted to provide a description for the key part (Figure 3-62), then the process begins.

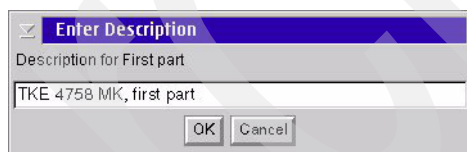


Figure 3-62 Description of the 4758 master key part

The process continues and indication is given that the key pair is being generated.

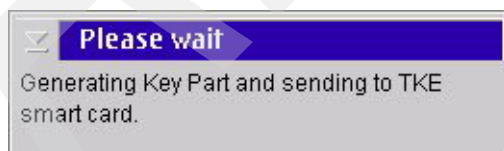


Figure 3-63 Generation of a 4758 key part and store into the smart card

After the key part is generated and saved in to smart card, the smart card contents are read and the 4758 master key parts are displayed.

Storing the ICSF master keys

ICSF master key parts can be generated at the TKE and stored in a smart card for later retrieval. The process is initiated in the coprocessor administration menu after the proper domain is selected, as shown in Figure 3-64.

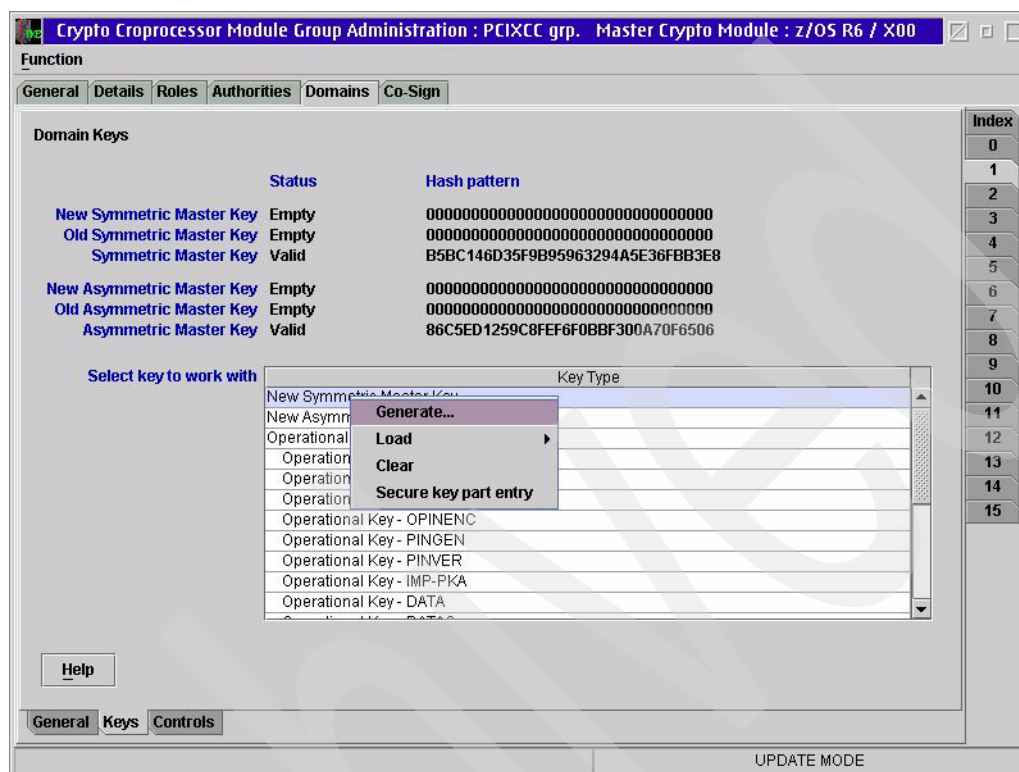


Figure 3-64 Generation of ICSF master key parts

Select **Smart card** as the target when the menu shown in Figure 3-65 appears.

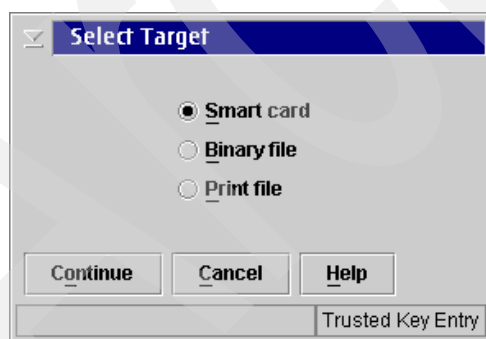


Figure 3-65 Selection of the ICSF master key part target

Insert the target smart card in card reader 2 and enter the PIN. Then enter the key part description as shown in Figure 3-66.

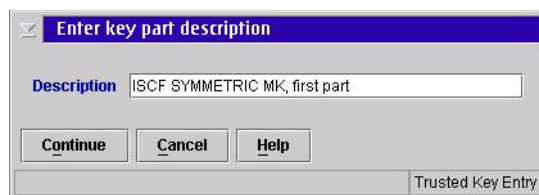


Figure 3-66 Description of the ICSF key part

The key part is then generated and stored in the smart card, as indicated in the message shown in Figure 3-67. Note that the message mentions a Copy Smart Card utility; with this, you can copy the ICSF key parts stored in one smart card to another smart card.

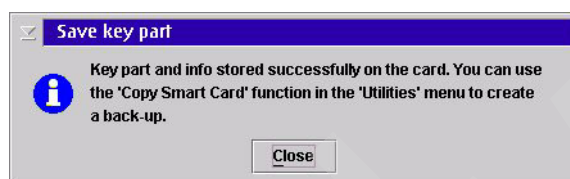


Figure 3-67 Completion of the ICSF key part generation process

From the TKE Main window, you can also invoke Manage smart card contents and Copy smart card contents, as shown in Figure 3-68.

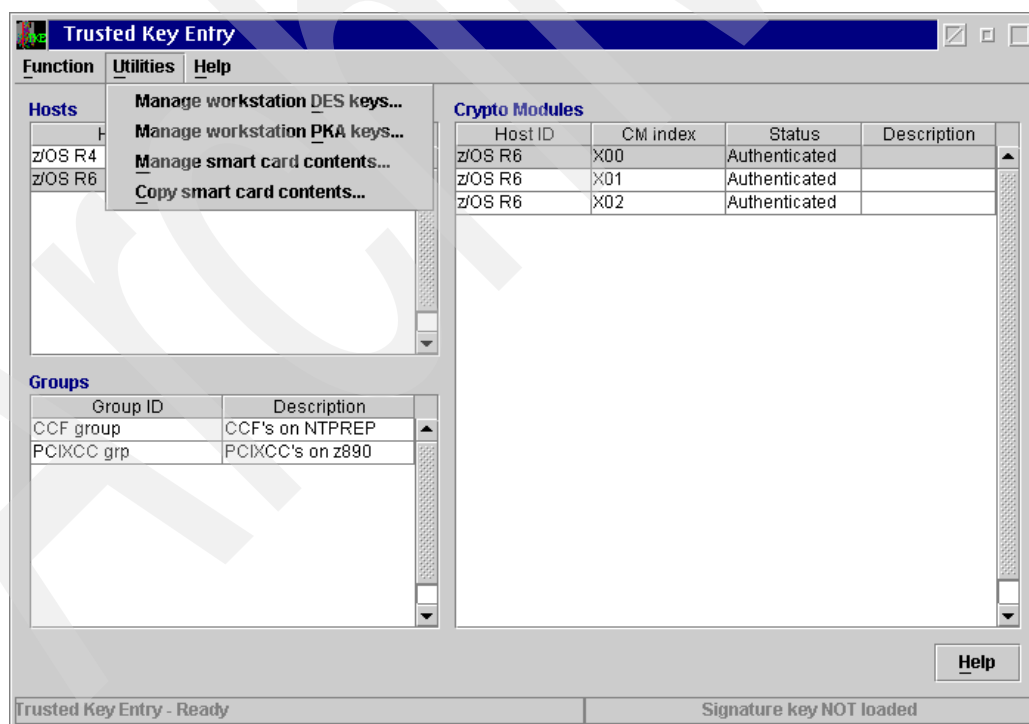


Figure 3-68 Smart card utilities in the TKE coprocessors management panel

Manage Smart Card Contents enables you to delete keys or key parts. Copy Smart Card Contents enables you to copy keys or key parts from one TKE smart card to another. CNM can also be used for both of these functions.

Invoking the Manage Smart Card contents utility provides a view of what ICSF key parts are currently stored on the card, as shown in Figure 3-69. Note that you can access the delete option by right-clicking the key part in the list.

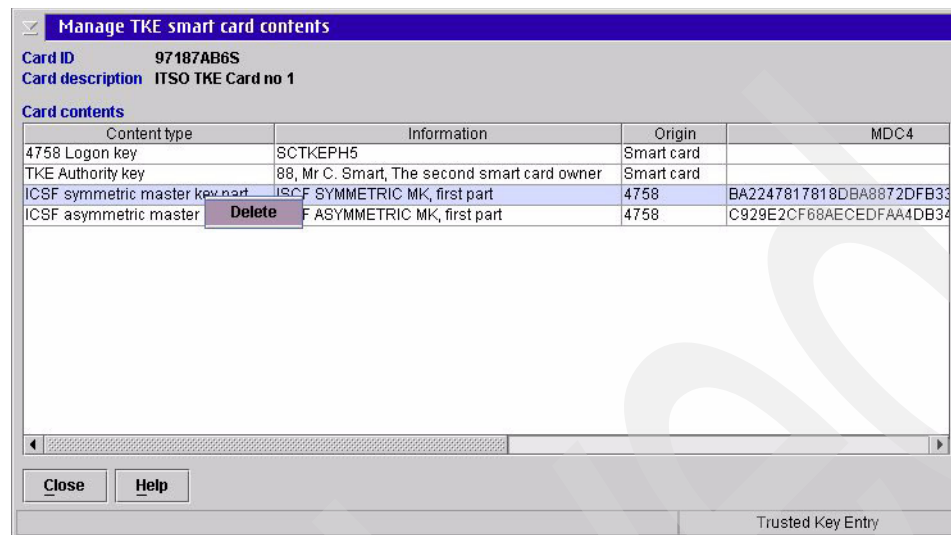


Figure 3-69 Deleting a key part from the smart card

ICSF operational keys

Operational key parts can also be generated at the TKE and stored in a smart card in a similar process to the storing of the master key parts. The process is initiated in the domain page of the target coprocessor.

Loading ICSF key parts from a smart card

We now show an example of loading ICSF operational key parts. This process is started from the coprocessor administration panel, in the selected domain, as shown in Figure 3-70.

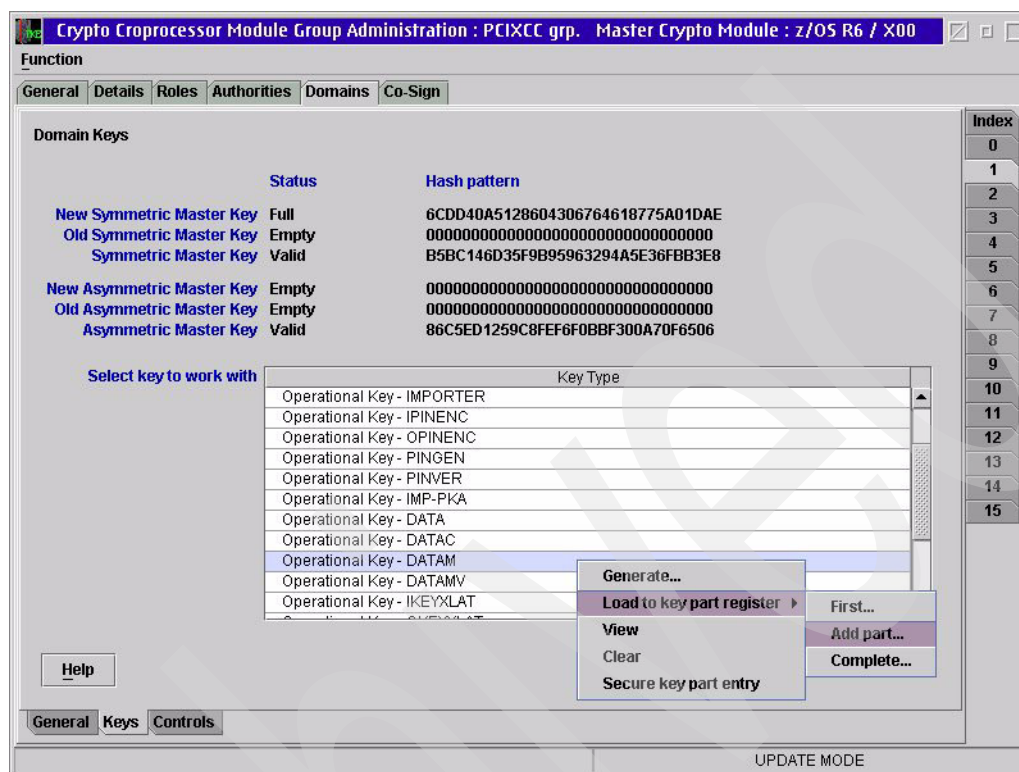


Figure 3-70 Initiating the load of an ICSF operational key part from a smart card

The source is indicated in the pop-up menu shown in Figure 3-71 as being the smart card in card reader 2. There is a prompt for entering the PIN value, not shown here. The key part is then transmitted via a secure session from the smart card to the TKE 4758, which in turn uses the transport key established between the TKE and the zSeries coprocessor to securely send the key part to the coprocessor key part register.



Figure 3-71 Selecting smart card reader 2

Archived



Migrating from previous TKE releases

In this chapter we discuss procedures for migrating from TKE V2 or higher to TKE V4.2. This migration includes both hardware and software.

4.1 Migrating from TKE V2 to TKE V4.2

There are no migration tools provided for migrating to TKE V4.2. Personal Security Cards (PSCs) available with TKE V2.0 *cannot* be used with TKE V4.2. Because of this, you must consider the impact on the following and perform the appropriate actions described:

- ▶ Host Definitions

The TKE V2.0 Host Definitions are APPC connections. You must redefine your existing hosts on TKE V4.2 and define the relevant TCP/IP information.

- ▶ CCF Crypto Modules, Domains, and Authority Definitions

The TKE V2.0 TKECM data set is not compatible with TKE V4.2. You must redefine CCF Crypto Modules, Domains, and Authority definitions. If you plan to use the same data set name for TKE V4.2 that you used for TKE V2.0, you must delete the existing data set or rename it. The TKEFLAGS data set from TKE V2.0 is no longer used in TKE V4.2.

- ▶ Authority Signature Keys on PSCs

Authority signature keys saved on PSCs from TKE V2.0 cannot be used with TKE V4.2. Before operating TKE V4.2, the TKE V2.0 user must do one of the following:

- a. If you will be using binary files for TKE V4.2 authority signature keys

Generate and load new signature keys to the host. From the Authority Administration window, generate a new signature key and save it to a binary file (hard drive or diskette). Read the PM (public modulus). From the authority administration window, create a new authority and choose the signature key you just created to be used with this authority. If this is a CCF crypto module, select **Change authority** and choose the signature key you just created. Send the updated signature key to the host. If saved to a hard drive, copy the binary file to diskette and restore the diskette files to the TKE V4.2 workstation.

- b. If you will be using the TKE V4.2 smart cards for TKE V4.2 authority signature keys

- Change the signature requirements so that signature keys stored on TKE V2.0 PSCs are not required. From the Crypto Module window, update the appropriate commands with the new signature requirements. Remove any authority whose signature key was stored on TKE V2.0 PSCs. If you do not have at least one signature key available that uses either a default key (other than authorities 14 or 15) or a signature key saved to binary file, generate and load a new signature key to the host using a binary file as described above.
 - From TKE V4.2, using a default signature key or a signature key saved to a binary file, generate and load new signature keys to the host. From the Authorities page of the Crypto Module Notebook, generate a new signature key and save it to a TKE V4.2 smart card that has been initialized and personalized. Get the signature key. Send the updated signature key to the host. Repeat for all authorities that will be using signature keys on TKE smart cards.

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

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

► Authority Signature Key in Workstation PKA Key Storage

There is no direct migration for an authority signature key saved in key storage on the TKE V2.0 4755 key storage to key storage on the TKE V4.2 4758 adapter card. You must perform the tasks described above.

► IMP-PKA Keys in Workstation DES Key Storage

There is no direct migration for IMP-PKA keys loaded in the TKE V2.0 workstation key storage to the TKE V4.2 workstation key storage. Depending on how and where the key parts were stored and loaded, the IMP-PKA keys must be reloaded to key storage on the TKE V4.2 workstation. Follow the process below for operational key parts.

► Master and Operational Key Parts

– Key parts saved to binary files on TKE V2.0 hard drive:

- Copy files to diskette.
- Restore diskette files to the hard drive of the new TKE V4.2 workstation.

– Key parts entered via the keyboard:

- Enter the key parts on the TKE V4.2 keyboard.
- If the user wants the known key part values to be saved to a TKE V4.2 TKE smart card, refer to the *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SA22-7524 for details.

– Key parts saved on TKE V2.0 PSCs:

Master and operational key parts stored on TKE V2.0 PSCs cannot be used on TKE V4.2. The data blocks on the PSCs must be copied to binary files using the TSS HIKM utility. The utility is executed on the TKE V2.0 workstation as follows:

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

```
CD WCS10\UTIL  
HIKM
```

The WCS utilities are installed on the C: drive.

ii. Press Enter. On panel CSUCM22, press PF2 (to log on with the public profile).

iii. On panel CSUCM20, select option 9 and press Enter.

iv. On panel CSUCZ20, select option 3 and press Enter.

v. On panel CSUCZ01, select option 4 and press Enter.

vi. On panel CSUCZ07, select option 2 and press Enter.

vii. On panel CSUCR88, insert the PSC card.

viii. On panel CSUCR86, select the desired data block ID and press Enter.

ix. On panel CSUCZ10, select the desired profile and press Enter.

x. On panel CSUCD03, follow the instructions to Enter the PIN on the security interface unit, then press E on the security interface unit.

xi. On panel CSUCZ03, enter Type Block Token and press Enter.

xii. On panel CSUCZ09, select option 1 and press Enter.

xiii. On panel CSUCR33, enter the Path for the Data File and press Enter. Message CSUC0356I will be displayed on the screen. Press Enter.

xiv. Copy the file from the hard drive to diskette.

xv. Restore the diskette files to the hard drive of new TKE workstation.

4.2 Migrating from TKE Version 3 or higher to TKE Version 4.2

TKE Version 4 and higher enables you to manage crypto modules on your legacy machines and any PCIXCCs/CEX2Cs inside your z990 or z890. To migrate to TKE V4.2, you must update both the TKE workstation code and the 4758 cryptographic adapter code. Both of these steps should have been completed as part of the MES instruction. In addition, the following tasks should have been performed as part of the MES upgrade:

1. If your Host system is being converted from a z900 to a z990 or from a z800 to a z890, the TKE V3.0, V3.1, V4.0, and V4.1 CM data set is not compatible with TKE V4.2. If you plan to use the same data set name for TKE V4.2 that you used for your current TKE, you must delete the existing data set or rename it.
2. You must update the TKE.INI file for FLOPPY_DRIVE_ONLY, ENABLE_SMART_CARD_READERS, and TRANSPORT_KEY_POLICY.
3. TKE Enablement permitted for z990 and z890 systems.

With the upgrade to TKE V4.2, both Passphrase and Smart Card Support are now available. While it is not mandatory, it is recommended that one method be chosen and used, and a mixture of methods avoided.

Passphrase setup

Several new access control points were added to the TKEUSER and TKEADM predefined roles. These changes require the user to load the new roles before passphrase logon can occur or certain functions may be used.

All predefined roles and profiles are in directory c:\tke\4758access.

- ▶ Use the CNM utility:
Open the TKE folder on the desktop/
- ▶ Double-click on the CNM utility.
- ▶ Log on to the 4758 using passphrase logon and the predefined TKEADM profile (or an equivalent passphrase profile/role).
- ▶ Load the new TKEUSER role using TKEUSR42.rol (Select **Access Control** → **Roles** → **Open** → tkeusr42.rol → **Load** → **OK** → **Cancel**.)
- ▶ Load the new TKEADM role using TKEADM42.rol.
- ▶ If you have any user profiles other than the predefined TKE user profiles, and you want to continue to be able to use them to log on to the 4758 to use TKE, you must add several new access control points to the roles that the profiles are mapped to. The new access control points needed are:

X'8002'	TKE logon
X'0250'	Load Diffie-Hellman key mod/gen
X'0251'	Combine Diffie-Hellman key parts
X'0252'	Clear Diffie-Hellman key values
X'027A'	Unrestrict Combine key parts

(Select **Access Control** → **Roles**. Highlight the applicable role and select **Edit**. Add required access control points to the Permitted Operations and **Save** (if desired) → **Load** → **OK** → **Cancel**.)

- ▶ If you have defined roles for TKE administrator functions, you must add new access control point X'030B' - Reset battery low indicator.
- ▶ If you will be creating Group Logon Passphrase Profiles, proceed to the next section. Otherwise, LOGOFF CNM.

Passphrase Group Logon setup

If you want to require that multiple users logon to the 4758 cryptographic adapter before either TKE or CNM can be used, define a group profile.

- ▶ Select: **Access Control** → **Profiles** → **New**. From the Profile Management pop-up, select **Group**.
- ▶ Enter the Group ID, update the Expiration Date. Select the role for the group profile, select passphrase profiles.
- ▶ Update the number of Group members required for Logon (minimum is 1, maximum is 10).
- ▶ Highlight the profiles from the Available profiles list that you want added to the group and select **Add**.
- ▶ When complete, select **Load** to load the group profile into the 4758 cryptographic adapter. If you also want to save the profile to the hard drive, select **Save**.

Note: The Role of the Group overrides the roles of the individual user profiles in the Group. Members in the group should have their individual user profiles mapped to the DEFAULT role to limit the access the user profiles have outside of the Group.

Smart card setup

If you will be using smart cards, several setup tasks must be completed, including:

- ▶ Activating Smart Card Support in CNM
- ▶ Loading smart card roles to the 4758 cryptographic adapter
- ▶ Initializing and personalizing a CA smart card
- ▶ Backing up a CA smart card
- ▶ Enrolling the local 4758 cryptographic adapter
- ▶ Enrolling the remote 4758 cryptographic adapter, if applicable
- ▶ Initializing and enrolling TKE smart cards
- ▶ Personalizing TKE smart cards
- ▶ Generating 4758 logon keys
- ▶ Defining smart card user profiles
- ▶ Defining smart card group profiles, if applicable
- ▶ Resetting the DEFAULT role
- ▶ Updating the TKE.INI file
- ▶ Generating new authority signature keys and saving them to TKE smart cards
- ▶ Uploading the new signature keys to the host

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

Steps for smart card setup

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

1. Activate Smart Card Support in CNM. Right-click the CNM icon in the TKE folder, and click **Properties** in the pop-up menu.
2. In the Properties panel, specify /SC in the Parameters field. Close the Properties panel. Smart Card Support will be activated the next time you double-click the icon to start CNM.

Use CNM for the following tasks (Double-click the CNM icon in the TKE folder):

- a. Log on to the 4758 cryptographic adapter using Passphrase Logon and TKEADM (or an equivalent passphrase profile).
 - b. Load the TEMPDEFAULT.rol: **Access Control** → **Roles** → **Open** → **tempdefault.rol** → **Load** → **OK** → **Cancel**.
 - c. Load the SCTKEUSR role: **Access Control** → **Roles** → **Open** → **sctkeusr.rol** → **Load** → **OK** → **Cancel**.
 - d. Load the SCTKEADM role: **Access Control** → **Roles** → **Open** → **sctkeadm.rol** → **Load** → **OK** → **Cancel**.
 - e. Load the MIGUSER role: **Access Control** → **Roles** → **Open** → **miguser.rol** → **Load** → **OK** → **Cancel**.
 - f. Log off TKEADM.
 - g. Exit CNM.
3. SCUP initialization tasks

Label the smart card readers 1 and 2 (for usability purposes). The following tasks are performed using SCUP:

- a. Initialize and personalize a CA smart card. The first and second CA PINs should be entered by different administrators and have different values: **CA Smart Card** → **Initialize and Personalize CA Smart Card** and follow the prompts.
- b. Back up the CA smart card: **CA Smart Card** → **Backup CA Smart Card** and follow the prompts.
- c. Enroll local 4758 cryptographic adapter: **4758** → **Enroll 4758** → **Local** and follow the prompts.
- d. Enroll remote 4758 cryptographic adapter if applicable:
 - On the remote TKE, open an OS/2 window; enter `cd tke\scup` and issue `enroll_req.cmd` and follow the prompts.
 - On local TKE from SCUP, select: **4758** → **Enroll 4758** → **Remote** and follow the prompts.
 - On the remote TKE, from `c: tke\scup`: issue `enroll_inst.cmd` and follow the prompts.
- e. Initialize and enroll TKE smart cards: **TKE Smart Card** → **Initialize and Enroll TKE Smart Card** and follow the prompts.
- f. Personalize TKE smart cards: **TKE Smart Card** → **Personalize TKE Smart Card** and follow the prompts.
- g. Close the SCUP application.

4. CNM initialization tasks

Open the CNM application. It is not necessary to log on to the 4758 cryptographic adapter because the TEMPDEFAULT role is still active. The following tasks are done using CNM:

- a. It is not necessary to create any new 4758 roles because SCTKEUSR, SCTKEADM, and MIGUSER are supplied with the code and provide all the required access controls for logging onto the 4758 for TKE, CNM, and the Migration Utility, respectively. However, you can create new roles as appropriate for your installation. If you do create new roles and want the user profiles that will be mapped to the roles to be suitable for 4758 logon for TKE, you must permit access control point x'8002' for TKE USER. If the role does not contain this access control point, the user profile will not be displayed for logon for TKE.
- b. Generate a 4758 logon key to a TKE smart card that will be used for logon to the 4758 cryptographic adapter. You will have to generate a 4758 logon key for each user logging on: **Smart Card** → **Generate 4758 Logon key** and follow the prompts.
- c. Define user profiles for the TKE smart cards that have a 4758 logon key: **Access Control** → **Profiles** → **New** → **Smart Card** and fill in the fields; map to SCTKEUSR or SCTKEADM roles → **Load**.

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

- d. Load user profile for MIGUSER: **Access Control** → **Profiles** → **Open (miguser.pro)** → **Save** → **Load**.
- e. Define a group profile (optional). Empty group profiles SCTKEADM and SCTKEUSR are provided. A group may contain 1 to 10 members. Select **Access Control** → **Profiles** → **Open (sctkeusr.pro or sctkeadm.pro)** and add profiles you want to the group, req # for logon → **Save** → **Load**

or

Select **Access Control** → **Profiles** → **New** → **Group** → **Smart Card** and add profiles you want to the group, req # for logon → **Save** → **Load**.)

Note: The role of the group overrides the roles of the individual profiles in the group.

- f. Reset the DEFAULT role. Your TKE workstation is not secure until the DEFAULT role is reset: **Access Control** → **Roles** → **Open** → **default.rol** → **Load** → **OK** → **Cancel**.
- g. Close the CNM application.
- h. Ensure that the TKE.INI file has been updated for ENABLE_SMART_CARD_READERS=TRUE
- i. Have each authority log on to TKE and generate a new authority signature key. Save the signature key to a TKE smart card and upload the new signature to the Host.

Note: Each TKE smart card can hold only one authority signature key. When you are confident the new roles and profiles on the 4758 for smart card use are correct, the existing passphrase roles and profiles should be deleted (TKEADM, TKEUSER, KEYMAN1, and KEYMAN2).

Archived



TKE workstation TCP/IP configuration

This appendix explains how to configure the TCP/IP service in the OS/2 of the TKE workstation.

TKE Workstation TCP/IP setup

The TKE administrator must configure the workstation for access via a TCP/IP network.

1. To start this configuration, from the TKE OS/2 desktop, double-click the TCP/IP icon to open the Configuration Notebook, as shown in Figure A-1.

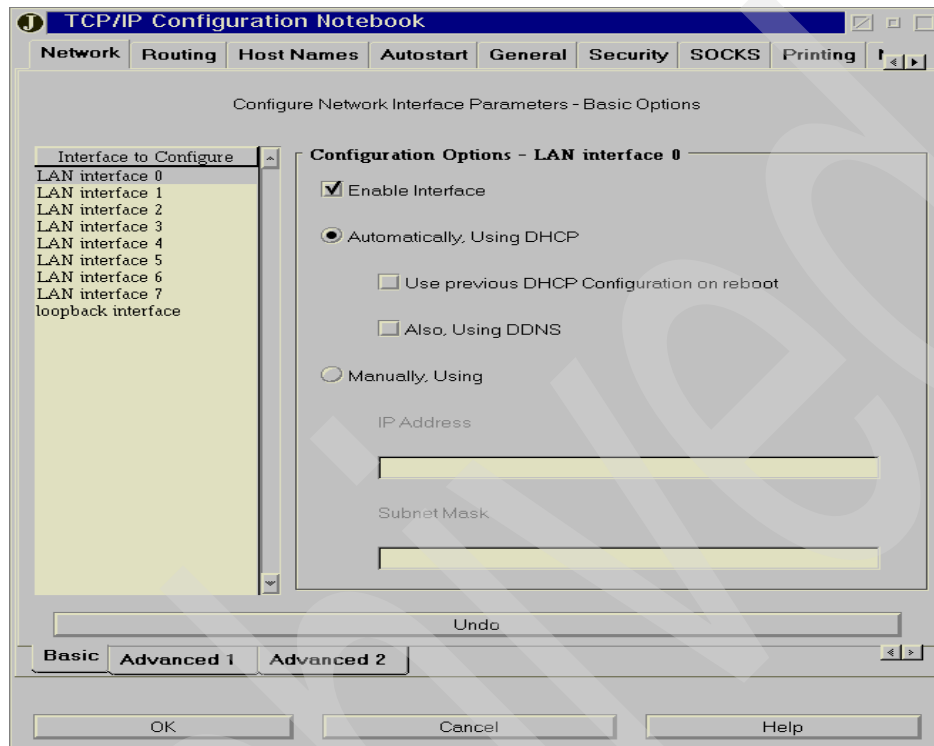


Figure A-1 TCP/IP Configuration Notebook

2. Fill in the basic options page of the Network tab for at least one adapter, typically **LAN interface 0**.
3. In our example, the option **Automatically using DHCP** was used. This setup is dependent on the specific network implementation, and has to be performed with the assistance of the customer network support personnel.

4. Read the Configure Routing Information online help to determine whether any special situations apply to the computer you are configuring. If so, you may need to complete the field on the Routing tab. (However, this was not needed in the case of our DHCP network.) Refer to Figure A-2.

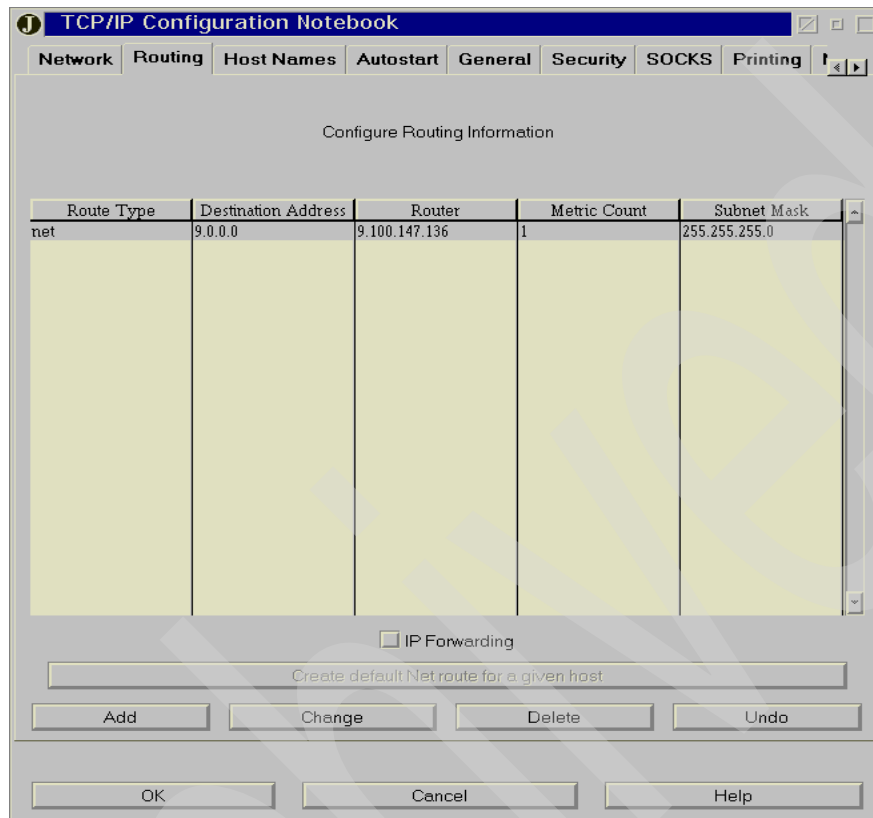


Figure A-2 TCP/IP routing tab

5. Click the **Autostart** tab in the Configure Automatic Starting of Services page. Select **routed** from the Autostarted Services list, check the **Autostart Service** box, and click **OK**.

We started the routed daemon in our configuration. This is shown in Figure A-3.

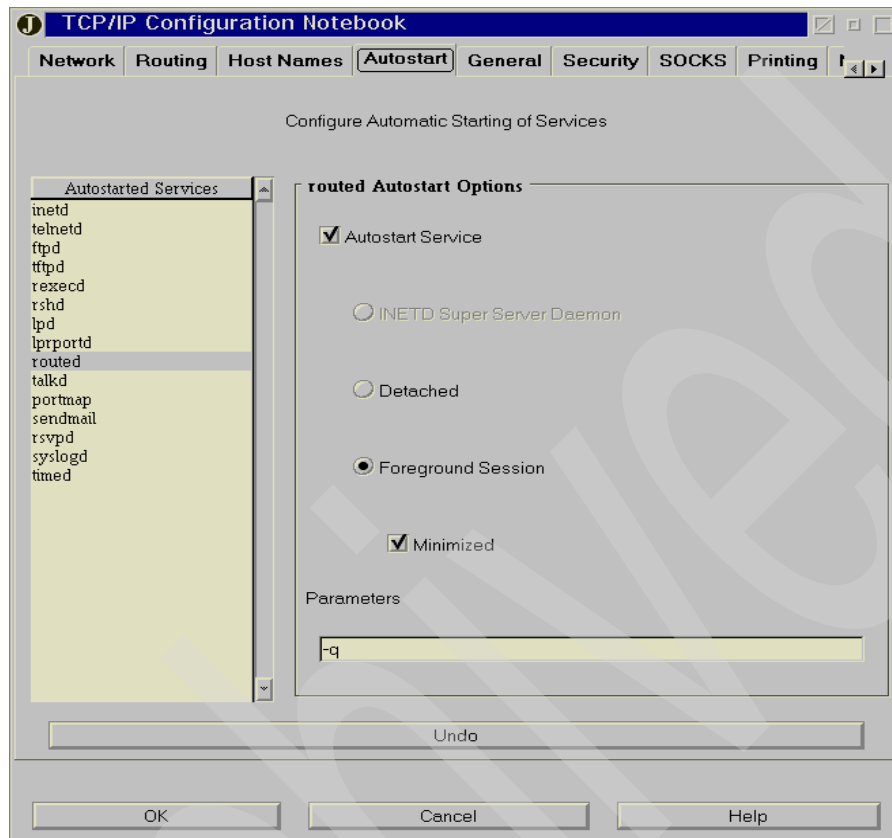


Figure A-3 Autostart tab

6. On the Configure Name Resolution Services pages, select the **Host Names** tab and provide the host name, local domain, and name service addresses as shown in Figure A-4. (This is not needed with a DHCP network.)

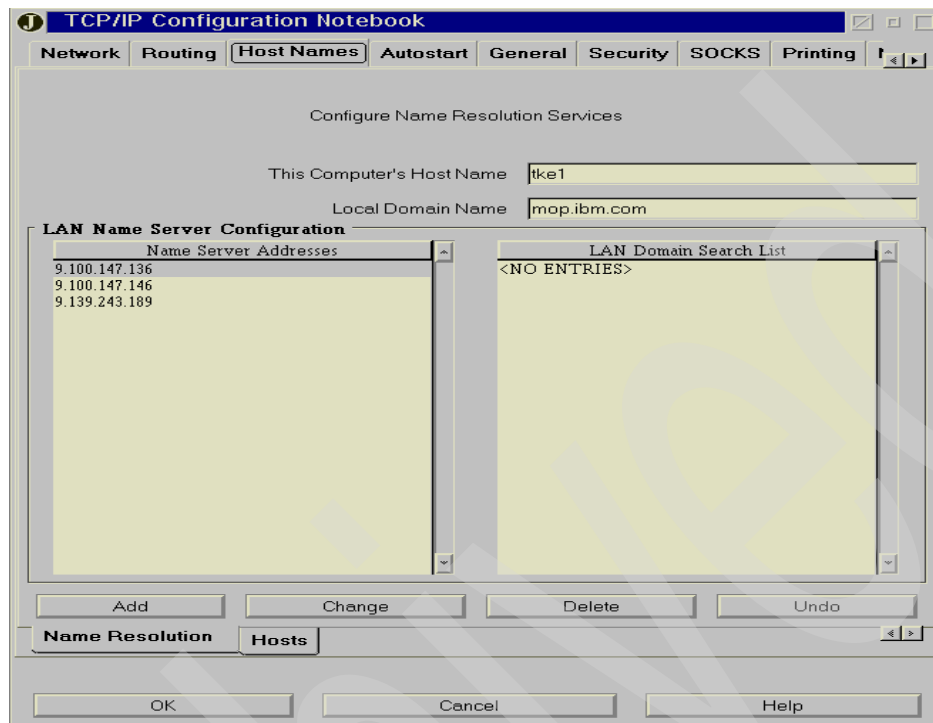


Figure A-4 Host Names tab

z/OS TCP/IP Host Transaction Program

The setup of the Host Transaction Program is explained in Appendix B, "TKE host TCP/IP server setup" on page 93.

Archived



TKE host TCP/IP server setup

This appendix describes the TCP/IP setup and customization required for proper TKE and TKE host communication.

The main TCP/IP files to check and modify

At this point, we assume that your TCP/IP stack has already been installed and configured. This section discusses the parameters of interest for TKE communications.

Note: In the following examples, TCPIP has to be replaced by the high-level qualifier that you defined to your installation with the DATASETPREFIX statement in TCPI.DATA.

TCPIP.HOSTS.LOCAL

This file contains TCP/IP hosts IP addresses and their corresponding domain names. This is the Site Table, which is intended to replace or to complement the services provided by the Domain Name Server from which you are requesting IP address resolution. Note that this information is exploited by the TKE TCP/IP server for informational purposes only; messages in the server print file may be issued that mention the local host name and IP address.

As an example, here is the entry from our TCPIP.HOSTS.LOCAL file. Our TKE host is named MVN9 and has IP address is 9.100.203.111.

```
HOST : 9.100.203.111 : MVN9 :::
```

TCPIP.DATA

For standard servers and clients, the anchor configuration data set is the TCPIP.DATA data set. This is the main resolver configuration data set, with information on host name, domain origin, and so on.

In addition, it holds the TCPIPJOBNAME parameter (which identifies the TCP/IP stack to use) and the DATASETPREFIX parameter (which is used by the resolver code when allocating the other configuration data sets).

In our configuration, TCPIP.DATA contains these entries:

- ▶ HOSTNAME MVN9
- ▶ DATASETPREFIX TCPIP.OMVS
- ▶ TCPIPJOBNAME TCPIPOE

TCPIP.PROFILE

The PORT statement in the TCPIP.PROFILE file is used to declare reserved ports (ports that cannot be attributed as a result of a port request by any application). Only the application that runs with the jobname specifically indicated in the PORT statement can get access to the designated port.

In our configuration, we had the following entries in our TCPIP.PROFILE:

```
50003 TCP CSFTTCP ; TKE server
```

This entry indicates that port 50003 is reserved for the exclusive use of job CSFTTCP, which starts the TKE TCP/IP server in the TKE host system. It also indicates that port 50003 will be used for communications via the TCP transport layer.

The modifications made in the TCPIP.PROFILE are taken into account by stopping and restarting the related TCP/IP stack, or are made dynamically by using the VARY

TCPIP,OBEYFILE command. In order to bring a new PORT dynamically, we entered the port statement to be dynamically executed in TCPIP.TCPPARMS(OBEYTKE), as shown in Example B-1.

Example B-1 OBEYTKE job

```

BROWSE      TCPIP.TCPPARMS(OBEYTKE) - 01.02                Line 00000000 Col 001 080
***** Top of Data *****
; -----
; Reserve ports for the following servers.
PORT
  50003 TCP CSFTTCP      ; crypto TKE server
***** Bottom of Data *****

```

Then we issued the VARY TCPIP command followed by a D TCPIP,NETSTAT to check that the CSFTTCP port was actually dynamically reserved. (We had only one TCP/IP instance running in the system, so we did not enter the TCP/IP task name in the commands; see Example B-2.)

Example B-2 Vary TCP/IP command

```

TCPIP,,OBEYFILE,TCPIP.TCPPARMS(OBEYTKE)
EZZ0060I PROCESSING COMMAND: VARY TCPIP,,OBEYFILE,TCPIP.TCPPARMS(OBE
YTKE)
EZZ0300I OPENED OBEYFILE FILE 'TCPIP.TCPPARMS(OBEYTKE)'
EZZ0309I PROFILE PROCESSING BEGINNING FOR 'TCPIP.TCPPARMS(OBEYTKE)'
EZZ0316I PROFILE PROCESSING COMPLETE FOR FILE 'TCPIP.TCPPARMS(OBEYTK
E)'
EZZ0053I COMMAND VARY OBEY COMPLETED SUCCESSFULLY
D TCPIP,,N,PORTL
EZZ2500I NETSTAT CS V2R8 TCPIP0E 637
PORT# PROT USER      FLAGS RANGE
00020 TCP  OMVS      D
00021 TCP  OMVS      DA
00023 TCP  OMVS      DA
00080 TCP  OMVS      DA
00111 TCP  OMVS      DA
50003 TCP  CSFTTCP   DA

```

Note: The change resulting from the OBEYFILE command is not carried across stopping and starting of the TCP/IP instance; therefore, you must edit the TCPIP.PROFILE in order to permanently install the change.

TKE Host Transaction Program installation

The Host Transaction Program is the interface between the TKE workstation and the crypto coprocessors. It includes the following software components:

- ▶ The CSFTTCP started procedure, which invokes the Terminal Monitor Program, which in turn executes the CSFTHTTP3 REXX exec.
- ▶ The CSFTHTTP3 REXX exec, which is a member of CSF.SCSFCLIO (where CSF can be another high-level qualifier specific to your installation).
- ▶ A parameter file CSFTPRM, used by the CSFTHTTP3 exec.
- ▶ The CSFTTKE module in the CSF.SCSFMOD0 library.

- The Crypto Module (CM) Data Set, which is used to maintain information about the crypto coprocessors in the configuration

CSFTTCP started procedure installation

CSFTTCP can be copied from SYS1.SAMPLIB into the procedure library of the installation and customized according to your installation requirements. In our installation we decided to implement the parameter file CSFTPRM as a member of our SYS1.PARMLIB.MVN9 data set.

Example B-3 CSFTTCP procedure

```
CSFTTCP PROC LEVEL=SYS1, MEMBER=CSFTHTP3,
//          CPARM=''
//CLIST    EXEC PGM=IKJEFT01,
//          TIME=1440,
//          PARM='EX ''&LEVEL..SCSFCLIO(&MEMBER)'' ''&CPARM'' EXEC'
//SYSPRINT DD SYSOUT=*
//SYSEXEC  DD DSN=&LEVEL..SCSFCLIO, DISP=SHR
//SYSPROC  DD DSN=&LEVEL..SCSFCLIO, DISP=SHR
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD DUMMY
//TKEPARMS DD DSN=&LEVEL..PARMLIB.&SYSNAME.(CSFTPRM), DISP=SHR
//*
/* CUSTOMIZE THE DSN TO BE TCPIP DATASET ON YOUR SYSTEM
//SYSTCPD  DD DISP=SHR, DSN=TCPIP.TCPPARMS(TCPDATOE)
```

Execution of the TKE Host Transaction Program must occur under External Security Manager control (in our case, RACF). A new facility profile, CSFTTKE, must be defined, and the user ID given to the started task must be permitted to the profile.

We created a user ID TKEUSER with a TSO segment but, for security purposes, with the NOPASSWORD attribute; that is, it is a *protected* user. (Note that we do not show the creation of the user catalog or any other specific user-related facilities that may be required by your installation policy.)

In our case, we also had to permit TKEUSER to SYS1.PARMLIB to enable the task to read the CSFTPRM file (Example B-4).

Example B-4 Listing of TKEUSER

```
TKEUSER NOPASSWORD TSO(ACCTNUM(AX0000) PROC(IKJSYS) UNIT(SYSDA))
ADDSD 'TKEUSER.**' OWNER(SYS1) UACC(NONE)
PE 'SYS1.**' ACC(READ) ID(TKEUSER)
RDEFINE STARTED CSFTTCP.* STDATA(USER(TKEUSER))
SETROPTS RACLIST(STARTED) REFRESH
RDEFINE FACILITY CSFTTKE UACC(NONE) OWNER(SYS1)
PERMIT CSFTTKE CLASS(FACILITY) ID(TKEUSER)
SETROPTS CLASSACT(FACILITY)
SETROPTS RACLIST(FACILITY) REFRESH
```

An additional level of security can be implemented by defining the APPL class profile CSFTTKE in RACF, and by permitting to this profile only the approved TKE users (as individual RACF user IDs or as an RACF group).

Example B-5 RACF APPL class list

```
SETROPTS CLASSACT(APPL)
SETROPTS RACLIST(APPL)
```

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

Note that if the RACF CSFSERV general resource class is active, the CSFTTCP user ID (TKEUSER, in our case) has to be permitted to CSFPCI and CSFPKCS.

Example B-6 CSFSERV class active

```
IT CSFPKSC CLASS(CSFSERV) ACC(READ) ID(TKEUSER)
PERMIT CSFPCI CLASS(CSFSERV) ACC(READ) ID(TKEUSER)
SETOPTS RACLIST(CSFSERV) REFRESH
```

Information about these profiles can be found in the *z/OS V1R6.0 ICSF Administrator's Guide*, SA22-7521.

The CSFTTKE module

The CSFTTKE command must be authorized in member IKJTSoxx of SYS1.PARMLIB. (The CSFTTKE module resides in CSF.SCSFMODE0.) The change to IKJTSoxx can be made dynamically by using the PARMLIB UPDATE(xx) command, where xx is the suffix of the modified IKJTSo member.

Example B-7 CSFTTKE command authorized

```
HCMD NAMES(          /***** AUTHORIZED COMMANDS *****/ +
CSFTTKE              /* AUTHORIZE TKE SERVER                */ +
```

The CSFTHTTP3 REXX exec

This exec resides in the CSF.SCSFCLIO library. It is invoked by the CSFTTCP procedure and goes through an initialization phase before listening to the TKE request over the TCP/IP socket. During its initialization, CSFTHTTP3 reads the parameter file designated in the TKEPARMS DD card of CSFTTCP; that is, SYS1.PARMLIB(CSFTPRM).

CSFTPRM has to be edited to indicate what CM data set to use and which TCP/IP port to connect to. The default values are, respectively, &SYSNAME.TKECM and 50003. Our edited CSFTPRM is shown in Example B-8.

Example B-8 Section of Port and CM dataset in CSFTPRM

```
BROWSE    SYS1.PARMLIB.MVN9(CSFTPRM) - 01.08          Line 00000000 Col 001 080
***** Top of Data *****
SET THE TKE DATA SETS;'TKEUSER.TKECM'
PORT;50003
SET DISPLAY LEVEL;TRACE ALL
***** Bottom of Data *****
```

Notes:

- ▶ We selected the TRACE ALL options. Other options are TRACE NON-ZERO, which traces non-zero return codes obtained during the transactions, and TRANSACTION TRACE, which traces transactions inputs and outputs. TRACE NON-ZERO is the default when no display level option is specified.
- ▶ We found that CSFTTCP fails if CSFTPRM contains sequence numbers in columns 73 to 80. When editing CSFTPRM, ensure that you have the sequence numbering on UNNUM.

Starting the TKE Host Transaction Program

We recommend that you perform a preliminary check of TCP/IP connectivity using a simple PING command from any workstation that can reach the TKE host TCP/IP stack.

When you issue the START CSFTTCP command, CSFTTHTTP3 is started and then listens for any incoming TCP/IP request.

Miscellaneous information, complemented with trace entries if tracing is active, is found in the SYSTSPRT DD data set, as shown in Example B-9.

Example B-9 CSFTTCP startup

```
THTP3 started at 19 Apr 2000, 09:50:54.
Generic user id.:      TKEUSER
CM  dataset:          'TKEUSER.TKECM'
RACF environment:     "Cipher"
TCP/IP port:          50003
Display level         "Trace all"
=====
19 Apr 2000 09:50:55 SocketSetList: ReturnCode=0, SocketSetList: ''
Misc. host info:
REXX/SOCKETS version  = REXX/SOCKETS CS V2R6 APR 17,1998
Domain name            =
Host Id (ipaddress)    = 9.100.203.111
Host Name              = MVN9
Fully qual. host name  = MVN9
Job id.                = CSFTTCP syslog start csfttcp
```

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information on ordering these publications, see “How to get IBM Redbooks” on page 99. Note that some of the documents referenced here may be available in softcopy only.

- ▶ *Exploiting S/390 Hardware Cryptography With Trusted Key Entry*, SG24-5455
- ▶ *S/390 Crypto PCI Implementation Guide*, SG24-5942
- ▶ *zSeries Crypto Guide Update*, SG24-6870
- ▶ *z990 Cryptography Implementation*, SG24-7070

Other publications

These publications are also relevant as further information sources:

- ▶ *z/OS ICSF Overview*, SA22-7519
- ▶ *z/OS ICSF System programmer's Guide*, SA22-7520
- ▶ *z/OS ICSF Administrator's Guide*, SA22-7521
- ▶ *z/OS ICSF Application programmer's Guide*, SA22-7522
- ▶ *z/OS Cryptographic Services ICSF TKE Workstation User's Guide*, SA22-7524

Online resources

These Web sites and URLs are also relevant as further information sources:

- ▶ IBM Systems Journal article

<http://domino.research.ibm.com/tchjr/journalindex.nsf/a3807c5b4823c53f85256561006324be/fc9c727abee8d3f985256eb500713360>

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Abbreviations and acronyms

ACP	access control point	PSC	personal security card
APPC	Advanced Program-to-Program Communication	RSA	register save area
CA	Certificate Authority	SCUP	Smart Card Utility Program
CCF	Cryptographic Coprocessor Feature	SE	support element
CEX2C	Crypto Express2 coprocessor	SNA	Systems Network Architecture
CKDS	Cryptographic Key Data Set	TKE	Trusted Key Entry
CMOS	complementary metal-oxide semiconductor	VTAM	Virtual Telecommunications Access Method
CNI	Cryptographic Node Initialization	ZD	zeroize domain
CNM	Cryptographic Node Management		
CPMP	crypto module public modulus		
DES	Data Encryption Standard		
DHCP	Dynamic Host Configuration Protocol		
DSS	decision support system		
FCV	Functions Control Vector		
HMC	Hardware Management Console		
IBM	International Business Machines Corporation		
ICRF	Integrated Cryptographic Facility		
ICSF	Integrated Cryptographic Services Facility		
ITSO	International Technical Support Organization		
LAN	local area network		
LAP	load authorization public modulus		
LCB	load PKSC Control Block		
LCS/LCR	load and combine PKA master keys		
LDAP	Lightweight Directory Access Protocol		
LEC	load environmental control mask		
LIC	licensed internal code		
LKP	load key part		
PCICA	PCI Cryptographic Accelerator		
PCIXCC	PCI Cryptographic Coprocessor		
PKA	public key algorithm		
PKDS	Private Key Data Set		
PKI	public key infrastructure		
PM	public modulus		
PSC	Personal Smart Card		

Archived

Index

Numerics

4755 Cryptographic Adapter 5
4758-023 6
4758initialize.cni 13

A

access control points
 TKE V3.1 6
APAR OA09157 24
APAR OW44816 24
APAR OW46381 24
APAR OW53666 24
Authority 8
 authority index 8
 Default signature key 8
 public exponent 8
 Signature key 8
 signature key
 loading from smart card 71
 on smart card 68

C

CA applet 41
CA smart card 42
CCF 2
CKDS 3
CNI 10
CNM 10, 14
 Group logon
 passphrase 34
 icon 15
 logon 15
 Smart card logon 66
 preparation 61
Code segments 11
Coproductors enablement
 CCF 5
 CPACF 5
 Crypto Express2 5
 PCICA 5
 PCICC 5
 PCIXCC 5
CPACF 2
Crypto Express2 2
 Enablement 5
Crypto modules 2
 Public exponent 9
Cryptographic coprocessors 2
CSFSERV class of RACF profiles 19
CSFTHTP3 REXX exec 97
CSFTPRM 96
CSFTTCP 95
 port 95

 started procedure 96
CSFTTKE
 module 97
CSUECNI 13

D

DEFAULT
 role 7, 31
DEFAULT role 8
DES 4
Diffie-Hellman 4
digital signature 4
DKG_DALL 19
DKYGENK-DALL 26
Domain 4
DSG ZERO-PAD 26
DSG Zero-Pad Unrestricted 21
DSS support 4

F

FC0800 2
FC0835 5
FC0853 24–25
FC0860 2
FC0861 2
FC0863 2
FC0865 5
FC0868 2
FC0875 5
FC0887 25
FC0888 25
FC3863 5
FCV 11
FMID
 HCR770A 24
 HCR770B 24
 HCR7720 24

G

Group Logon feature
 failure to logon 38
 Group creation 28
 Group profile 32
 Overview 28
 Passphrase profile 30
 smart card logon 64

I

IBM 4754 Security Interface Unit 5
IBM 4758-002 Cryptographic Adapter 6
IBM Personal Smart Card
 migration to TKE V4.2 80

- TKE V2 5
- ICSF 3
 - ICSF-managed VSAM data sets 3
 - ICSF-owned data space 3
 - key parts
 - loading from smart card 77
 - Master keys
 - storing on smart card 74
- ISPF panels 4, 20

K

- KEYMAN1 13
- KEYMAN1 role 13
- KEYMAN2 13

L

- Linux for zSeries 4

M

- Manual-control panel 5
- Master Keys
 - ICSF 3
- May 2004 LIC 23
- Migration
 - TKE V2 to TKE V4.2 80
 - TKE V3 to TKE V4.2 82
- MIGUSER role 44
- Multi-signature command 9

O

- OBEYTKE 95
- Operational keys 22
- operational keys
 - access control points 23

P

- PCICA 2, 101
 - Enablement 5
 - Queues 4
- PCICC
 - enablement 5
 - Multi-signature commands 9
- PCIXCC 2
 - Enablement 5
 - Multi-Signature commands 9
- PIN
 - CA card 48
 - CA smart card 42
 - changing smart card PIN 57
 - Dual authentication 43
 - prompt 40
 - TKE smart card 42
- PKDS 3
- PKSC 5
- Profile 7
 - KEYMAN1 14
 - KEYMAN2 14

- TEMPDEFAULT 44
- TKEADM 14
- TKEUSER 12
- Profiles
 - creation 15

R

- RACF Facility profile
 - CSFTTKE 96
- Redbooks Web site 99
 - Contact us viii
- Role 13
 - DEFAULT 13, 44
 - KEYMAN1 13
 - KEYMAN2 13
 - SCTKEADM 44
 - SCTKEUSR 44
- Roles
 - creation 16
- RSA key 8
- RSA key pair 55

S

- Save profile 31
- SCUP 41, 45
- Signature key
 - Cryptomodule signature key 9
- Smart Card Readers
 - installation 46
- Smart Card Support
 - 4758 key generation 61
 - blocked card 59
 - CA card 41
 - CA card backup 48
 - CA smart card 40
 - CNM 43
 - ENROLL_INST.CMD 53
 - entity 40
 - group logon 64
 - initialization
 - CA card 47
 - overview 40
 - PIN change 57
 - PKI concepts 41
 - requirements 40
 - session key 41
 - setup
 - zone entities 46
 - smart card profile 62
 - TKE 4758 enrollment
 - local TKE 51
 - remote TKE 52
 - TKE 4758 initialization 44
 - TKE smart card 41
 - backup 56
 - enrollment 54
 - initialization 54
 - personalization 56
 - tke.ini 46

- transport key 41
- unblock card 59
- zone 41
- zone ID 43

T

- TCP/IP 93, 98
 - connectivity 10
 - socket 97
- TCP/IP file
 - TCPIP.HOSTS.LOCAL 94
- TCP/IP files 94
 - TCPIP.DATA 94
 - TCPIP.PROFILE 94
- TCPIP.PROFILE
 - CSFTTCP PORT 94
- TEMPDEFAULT role 44, 51
- TKE
 - 4758 key parts 45
 - storing on smart card 72
 - 4758 Master key 10, 14
 - 4758 user profile 8
 - Customization 11
 - definitions 12
 - Domains 5
 - Group logon
 - passphrase 37
 - Host Transaction Program 95–96
 - Introduction to the TKE V3.1 workstation 6
 - Loading the first part of the TKE Master Key 17
 - Master key 8, 17, 45
 - OS/2 desktop 88
 - shipping 11
 - Starting the Application 18
 - the TKE application 45
 - TKE Workstation access control 12
 - tke.ini parameters 17
 - workstation installation 10
 - Workstation key storage 11
 - workstation TCP/IP setup 88
- TKE application
 - smart card logon 67
- TKE enablement
 - for z990 and z890 23
- TKE smart card 42
- TKE user applet 42
- TKE V4.2
 - access control points 26
 - Group logon 25
 - Smart Card Support 25
- TKE V4.x
 - upgrading to 4.x 6
- TKE Workstation 4
- tke.ini
 - BLIND_KEY_ENTRY 17
 - DEFAULT_DIRECTORY 17
 - ENABLE_SMART_CARD_READERS 45
 - FLOPPY_DISK_ONLY 46
 - FLOPPY_DRIVE_ONLY 18
 - MESSAGE_PATH 17

- SERIALIZE_PATH 17
- TRANSPORT_KEY_POLICY 17

- TKEADM 13
 - Role 13
- TKEUSER
 - profile 14
 - role 8, 16
 - TSO userID 96

V

- VTAM APPC 5

Z

- Zone 41
- Zone description 48
- Zone information 53

Archived



Redbooks

zSeries Trusted Key Entry (TKE) Version 4.2 Update

A technical review of TKE releases, features, and setup

The new Group Logon and Smart Card Reader features explained

A migration guide to TKE V4.2

This IBM Redbook provides detailed information about the principles of operation and use of new features in the Trusted Key Entry workstation at the Version 4.2 level.

Readers should be familiar with zSeries hardware cryptography implementation and the purpose and usage of the TKE workstation; however, the first chapter is a refresher of the cryptographic hardware coprocessors that are currently available on the different zSeries models, and the history and setup of the TKE workstation.

New TKE functions such as Smart Card Support and Group Logon are described in terms of implementation and setup, and we give examples of the utilization of these two functions. We also cover the process of migrating from previous TKE releases, and provide examples of TCP/IP setup and configuration for the TKE workstation.

**INTERNATIONAL
TECHNICAL
SUPPORT
ORGANIZATION**

**BUILDING TECHNICAL
INFORMATION BASED ON
PRACTICAL EXPERIENCE**

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks