z/OS
2.5

Getting started with TKE at your enterprise

Note

Before using this information and the product it supports, read the information in “Notices” on page 35.

This edition applies to Version 2 Release 5 of z/OS® (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

Last updated: 2021-09-30

Contents

Tables

How to send your comments to IBM

We appreciate your input on this information. Please provide us with any feedback that you have, including comments on the clarity, accuracy, or completeness.

Use one of the following methods to send your comments:

Important: If your comment regards a technical problem, see instead "If you have a technical problem" on page vii.

- Send an email to mhvrcfs@us.ibm.com.
- Send an email from the Contact the z/OS team web page (www.ibm.com/systems/campaignmail/z/zos/contact_z).

Include the following information:

- Your name and address
- Your email address
- Your phone or fax number
- The title:

  Getting started with TKE at your enterprise
- The topic and page number or URL of the specific information to which your comment relates
- The text of your comment.

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

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

If you have a technical problem

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

- Visit the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

Chapter 1. What is TKE?

The Trusted Key Entry (TKE) feature is an integrated solution that manages cryptographic keys in a secure environment. The TKE workstation enables basic local and remote key management and is an optional hardware feature of IBM Z that provides a management tool for Z host cryptographic coprocessors. The TKE contains a combination of hardware, firmware, and software. An optional smart card reader can be added to the TKE workstation.

TKE workstation and the most recent TKE 9.2 LIC are optional features of the z15.

Requirements: For information about the conditions you must meet before you can use TKE, see Chapter 2, “Requirements for TKE,” on page 3.

Chapter 2. Requirements for TKE

This topic describes the requirements for TKE.

Identifying the console

For information about identifying the TKE console, see

- Service Guide for Trusted Key Entry Workstations (www.ibm.com/servers/resourcelink/lib03010.nsf/pagesByDocid/BE66F954000C29758525817900600DB2?OpenDocument)

  Note: You need an IBM id for Resource Link to view and download this publication.

Trusted Key Entry components

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

TKE hardware

- TKE Workstation.
- IBM 4768 Cryptographic adapter.

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

Available with a TKE 9.2 workstation is:

- Feature 0900: 10 IBM part number 00RY790 smart cards.
- Feature 0891: 2 smart card readers and 20 IBM part number 00RY790 smart cards.

Notes:

1. You can carry your smart card readers from feature code 0885 or 0891 forward. Existing smart cards can be used on TKE 9.2 with these readers.
2. With Gemalto smart card readers, you must press the green Enter button after you enter the PIN or a character during the secure key entry process.
3. IDENTIV smart card readers do not have a display window. When you press on the pad, a tone comes from the reader that indicates that the pad was pressed. When the PIN is fully entered, a different pitched tone plays, signaling that the PIN is complete.
4. To manage EP11 host crypto modules, EP11 smart cards are required. Only IBM part numbers 74Y0551 and 00JA710 can be used to create EP11 smart cards.
5. Kobil smart card readers are not supported and not usable with TKE 7.0 or later.
6. DataKey smart cards are no longer usable with TKE 7.0 or later.
7. Older smart cards must be reinitialized on TKE 7.0 or later to be able to store ECC (APKA) master keys.

Two USB flash memory drives are shipped with TKE:

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

TKE software

The following software is preinstalled on the TKE workstation:

- IBM Cryptographic Coprocessor Support Program Release 6.0.

- Trusted Key Entry Version 9.2 - FC 0879.

Notes:

1. TKE software should not be changed without instructions from IBM Service.
2. TKE 6.0 software, FC 0858, can be installed only on TKE workstations FC 0859, FC 0839, or FC 0840.
3. TKE 7.0 software, FC 0860, can be installed only on a TKE 7.0 workstation, FC 0841.
4. TKE 7.1 software, FC 0867, can be installed only on a TKE 7.0 workstation, FC 0841.
5. TKE 7.2 software, FC 0850, can be installed only on a TKE 7.0 workstation, FC 0841.
6. TKE 7.3 software, FC 0872, can be installed only on a TKE 7.0 workstation, FC 0841 or FC 0842.
7. TKE 8.0 software, FC 0877, can be installed only on a TKE 8.0 workstation, FC 0847.
8. TKE 8.1 software, FC 0878, can be installed only on a TKE 8.0 workstation, FC 0847 or FC 0097.
9. TKE 9.0 software, FC 0879, can be installed on a TKE workstation, FC 0842, FC 0847, FC 0097, FC 0098, FC 0849, FC 0080, FC 0081, FC 0085, or FC 0086.

   Note:

   - When TKE 9.0 is installed on FC 0842 or FC 0847, the workstation feature code becomes 0849.
   - When TKE 9.0 is installed on FC 0097, the workstation becomes feature code becomes 0080.
   - When TKE 9.0 is installed on FC 0098, the workstation becomes feature code becomes 0081.
10. You can only upgrade your TKE workstation to TKE 9.1 software, FC 0880, if your workstation is assigned to a z13 or later.
11. You can only upgrade your TKE workstation to TKE 9.2 software, FC0881, if your workstation is assigned to a z14 or later.

Supported host cryptographic adapters

The host cryptographic adapters supported by TKE 9.2 are:

- Crypto Express2 adapter (CEX2C).
- Crypto Express3 adapter (CEX3C).
- Crypto Express4 CCA adapter (CEX4C).
- Crypto Express4 PKCS #11 adapter (CEX4P).
- Crypto Express5S CCA adapter (CEX5C).
- Crypto Express5S PKCS #11 adapter (CEX5P).
- Crypto Express6S CCA adapter (CEX6C).
- Crypto Express6S PKCS #11 adapter (CEX6P).
- Crypto Express7S CCA adapter (CEX7C).
- Crypto Express7S PKCS #11 adapter (CEX7P).

These host cryptographic adapters:

- Provide a secure processing environment with hardware to provide DES, AES, TDES, RSA, SHA-1, and SHA-256 cryptographic services with secure key management and finance-industry special function support.
- Perform random number generation and modular math functions for RSA and similar public-key cryptographic algorithms.
- Include sensors to protect against attacks that involve probe penetration, power sequencing, radiation, and temperature manipulation.

CEX2C, CEX3C, CEX4C, CEX5C, CEX6C, and CEX7C adapters implement the IBM Common Cryptographic Architecture and are referred to as CCA coprocessors.

CEX4P, CEX5P, CEX6P, and CEX7P adapters implement the IBM Enterprise PKCS #11 architecture and are referred to as EP11 coprocessors.

Host crypto module

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

When a host crypto module is manufactured, a unique 8-byte Crypto-Module ID (CMID) is generated and permanently stored on the crypto module. The CMID is returned in all reply messages sent from the host crypto module to the TKE workstation.

TKE release and feature codes available by CEC levels

Table 1 on page 5 shows the TKE licensed internal code (LIC) that is orderable based on the date and type of your CEC.

Most of the time, a new version of the TKE workstation is released at the same time as a new CEC. When you order a new TKE workstation, you receive the latest TKE hardware with the latest TKE licensed internal code (LIC) installed on it. For example, if you had placed an order for a new TKE workstation between September of 2012 and September of 2013, you would have received TKE 7.2 (or, in order words, hardware feature code 0841 with LIC feature code 0850).

Table 1. TKE release and feature codes available by CEC level

TKE release (LIC)	Feature codes			CEC information												
	Hardware	LIC	Initial release date	z9-109 z9EC 2094	z9BC 2096	z10 EC 2097	z10 BC 2098	z10 EC GA3 z10 BC GA2	z196	z114	zEC12	zBC12	z13	z13s	z14	z15
TKE 5.3	0839	0854	Oct 2008	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
TKE 6.0	0840	0858	Nov 2009	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
TKE 7.0	0841	0860	Sept 2010	N/A	N/A	Yes	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A
TKE 7.1	0841	0867	Sept 2011	N/A	N/A	Yes	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A
TKE 7.2	0841	0850	Sept 2012	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A
TKE 7.3	0842	0872	Sept 2013	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
TKE 8.0	0847	0877	Feb 2015	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes	Yes	Yes
TKE 8.1	0847 or 0097	0878	Feb 2016	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes	Yes	Yes
TKE 9.0	0085 or 0086	0879	Sept 2017	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes	Yes
TKE 9.1	0085 or 0086	0880	Nov 2018	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes
TKE 9.2	0085 or 0086	0881	Sept 2019	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes

Your host cryptographic environment determines the level of TKE LIC that you can use. To determine which host cryptographic modules are supported by your TKE, see Table 7 on page 12.

Smart card readers and smart cards orderable by TKE release

Table 2 on page 6 shows the smart card readers and smart cards that can be ordered for each TKE release.

Table 2. Smart card readers and smart cards orderable by TKE release				
TKE release (LIC)	**Smart card reader**		**Smart card**	
	Feature code	**Type**	**Feature code**	**Part number**
TKE 5.3	0885	Omnikey/HID	0884	45D3398
TKE 6.0	0885	Omnikey/HID	0884	45D3398
				74Y0551* #
TKE 7.0	0885	Omnikey/HID	0884	45D3398
				74Y0551* #
TKE 7.1	0885	Omnikey/HID	0884	45D3398
				74Y0551*
TKE 7.2	0885	Omnikey/HID	0884	74Y0551*
TKE 7.3	0885	Omnikey/HID	0884	74Y0551*
TKE 8.0	0885 or 0891	Omnikey/HID	0884 or 0892	00JA710
TKE 8.1	0885 or 0891 @	Omnikey/HID/ Gemalto	0884 or 0892	00JA710
TKE 9.0	0885 or 0891 @	Omnikey/HID/ Gemalto/IDENTIV	0892	00JA710
TKE 9.1	0891	IDENTIV	0900	00RY790
TKE 9.2	0891	IDENTIV	0900	00RY790

*****
Part number 74Y0551 replaced part number 45D3398 in feature code 0884.

#
An MCL is required to support part number 74Y0551 on TKE 6.0 and TKE 7.0.

@

- Clients in the United States, Canada, and European Union (EU) might receive Gemalto CT700 readers.
- With Gemalto smart card readers, you must press the green Enter button after you enter the PIN or a character during the secure key entry process.

There are restrictions on what smart card part numbers can be used to create different smart card types. For more information, see “Smart card compatibility issues” on page 7.

DATAKEY smart cards are not supported on TKE 7.0 or later. If you are upgrading from TKE 6.0 to TKE 7.0 or later and have DATAKEY smart cards, you need to back up your CA smart cards by using a more current smart card part number and copy keys and key parts from your TKE smart cards onto TKE smart cards that are created from a more current smart card part number. See “Datakey card usage” on page 11 for information on migrating data to a new smart card.

To identify the part number of your smart card, look for the following:

DATAKEY
Has blue and orange art work and DATAKEY printed on them.

45D3398
Are white and do not have any part number printed on them.

74Y0551
Has part number 74Y0551 printed on them.

00JA710
Has part number 00JA710 printed on them.

Smart card compatibility issues

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

Applet version

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

Table 3. Applet version by TKE release

	CA smart card	**TKE smart card**	**EP11 smart card**	**Smart card part**
TKE 5.2 or earlier	applet version = 0.3	applet version = 0.3	Not supported	Any supported card
TKE 5.3	applet version = 0.3	applet version = 0.4	Not supported	Any supported card
TKE 6.0	applet version = 0.4	applet version = 0.5	Not supported	Any supported card
TKE 7.0	applet version = 0.4	applet version = 0.6	Not supported	Any supported card
TKE 7.1	applet version = 0.4	applet version = 0.7	Not supported	Any supported card
TKE 7.2	applet version = 0.4	applet version = 0.8	Not supported	45D3398
TKE 7.2	applet version = 0.4	applet version = 0.8	applet version = 0.1	74Y0551
TKE 7.3	applet version = 0.4	applet version = 0.8	Not supported	45D3398
TKE 7.3	applet version = 0.5	applet version = 0.9	applet version = 0.2	74Y0551
TKE 8.0	applet version = 0.4	applet version = 0.8	Not supported	45D3398
TKE 8.0	applet version = 0.5	applet version = 0.10	applet version = 0.2	74Y0551
TKE 8.0	applet version = 0.5	applet version = 0.10	applet version = 0.2	00JA710
TKE 8.1	applet version = 0.6	applet version = 0.11 [1]	Not supported	45D3398
TKE 8.1	applet version = 0.7	applet version = 0.12 [2]	applet version = 0.3[3]	74Y0551
TKE 8.1	applet version = 0.7	applet version = 0.12[2]	applet version = 0.3[3]	00JA710

Table 3. Applet version by TKE release (continued)				
	CA smart card	**TKE smart card**	**EP11 smart card**	**Smart card part**
TKE 9.0	applet version = 0.6	applet version = 0.15[4]	Not supported	45D3398
TKE 9.0	applet version = 0.7	applet version = 0.16[5]	applet version = 0.4[6]	74Y0551
TKE 9.0	applet version = 0.7	applet version = 0.16[5]	applet version = 0.4[6]	00JA710
TKE 9.1 and TKE 9.2	applet version = 0.6	applet version = 0.17	Not supported	45D3398
TKE 9.1 and TKE 9.2	applet version = 0.7	applet version = 0.18	applet version = 0.5	74Y0551
TKE 9.1 and TKE 9.2	applet version = 0.7	applet version = 0.18	applet version = 0.5	00JA710
TKE 9.1	applet version = 0.8	applet version = 0.19	applet version = 0.6	00RY790
TKE 9.2	applet version = 0.8	applet version = 0.20	applet version = 0.7	00RY790

Notes:

1. A PTF available on TKE 8.1 changes the applet version to 0.13. The PTF adds support for an alternate zone when copying smart card contents.
2. A PTF available on TKE 8.1 changes the applet version to 0.14. The PTF adds support for an alternate zone when copying smart card contents.
3. A PTF available on TKE 8.1 changes the applet version to 0.4. The PTF adds support for an alternate zone when copying smart card contents.
4. A PTF available on TKE 9.0 changes the applet version to 0.17. The PTF modifies support for using an alternate zone when copying smart card contents.
5. A PTF available on TKE 9.0 changes the applet version to 0.18. The PTF modifies support for using an alternate zone when copying smart card contents.
6. A PTF available on TKE 9.0 changes the applet version to 0.5. The PTF modifies support for using an alternate zone when copying smart card contents.

Table 4. Applet version by TKE release				
	MCA smart card	**IA smart card**	**KPH smart card**	**Smart card part**
TKE 7.0 to TKE 7.2	applet version = 0.1	applet version = 0.1	applet version = 0.1	Any supported card
TKE 7.3	applet version = 0.1	applet version = 0.1	applet version = 0.1	45D3398
TKE 7.3	applet version = 0.2	applet version = 0.2	applet version = 0.2	74Y0551
TKE 8.0	applet version = 0.1	Not supported	Not supported	45D3398
TKE 8.0	applet version = 0.2	applet version = 0.3	applet version = 0.3	74Y0551

Table 4. Applet version by TKE release (continued)				
	MCA smart card	**IA smart card**	**KPH smart card**	**Smart card part**
TKE 8.0	applet version = 0.2	applet version = 0.3	applet version = 0.3	00JA710
TKE 8.1, TKE 9.0, TKE 9.1, and TKE 9.2	applet version = 0.3	Not supported	Not supported	45D3398
TKE 8.1, TKE 9.0, TKE 9.1, and TKE 9.2	applet version = 0.4	applet version = 0.4	applet version = 0.4	74Y0551
TKE 8.1, TKE 9.0, TKE 9.1, and TKE 9.2	applet version = 0.4	applet version = 0.4	applet version = 0.4	00JA710
TKE 9.1 and TKE 9.2	applet version = 0.5	applet version = 0.5	applet version = 0.5	00RY790

Notes:

1. In general, smart cards that are created on a particular TKE release cannot be used on TKE workstations that are at prior release levels. TKE 5.2 applets are not usable on TKE 7.1 and later because they can only be installed on DataKey smart cards, and DataKey smart cards are not supported.
2. If you are collecting data that will be applied to a Crypto Express 5 or later:
   - The KPH certificates must come from smart cards at the minimum applet version 0.3. This applet version was first available in TKE 8.0.
   - The collect must be done from a TKE 8.0 or later.
3. If you are applying data to a Crypto Express 5 or later, you must use IA smart cards that are at applet version 0.3 or later. This applet version was first available in TKE 8.0.
4. If you are using Gemalto CT700 smart card readers:
   - MCA smart cards must be at the minimum applet version 0.4. This applet version was first available in TKE 8.1.
   - IA smart cards must be at the minimum applet version of 0.4. This applet version was first available in TKE 8.1.
   - KPH smart cards must be at the minimum applet version of 0.4. This applet version was first available in TKE 8.1.
5. If you want to collect data from a Common Cryptographic Architecture (CCA) module that has domains configured to run in PCI-compliant mode, all of your smart cards (the MCA, IA, and KPH smart cards):
   - Must be initialized and personalized on TKE 9.1 or later.
   - Must be the minimum part number of 00RY790 (the blue smart card).
   - The Migration Zone (MCA smart card) must have EC-521 strength zones.

Zone key type and length

TKE uses smart cards and establishes zones for two categories of operations: normal crypto module administration, which includes loading keys and key parts and signing commands to a crypto module, and configuration migration. CA, TKE, and EP11 smart cards are created for normal crypto module administration, and MCA, IA, and KPH smart cards are created for configuration migration. Support for configuration migration was added in TKE 7.0.

Zone keys establish secure communication between entities in a zone. Entities include smart cards and the TKE workstation crypto adapter.

Prior to TKE 6.0, zones for normal crypto module administration use 1024-bit RSA keys. Beginning in TKE 6.0, customers can select either 1024-bit RSA keys or 2048-bit RSA keys as the zone key type.

When support for configuration migration was added in TKE 7.0, the zone key type for configuration migration was restricted to 2048-bit RSA keys. Similarly, when support for EP11 crypto modules was added in TKE 7.2, a zone key type of 2048-bit RSA keys was required to create an EP11 smart card.

Beginning in TKE 9.1, zones based on P521 ECC keys are supported for both normal crypto module administration and configuration migration. You must use 00RY790 smart cards for this zone type. The zone key type and size is selected when initializing and personalizing a CA or an MCA smart card.

Smart card usage

Table 5 on page 10 indicates in more detail where CA smart cards created in different releases can be used. Usage means employing a CA smart card to create TKE smart cards, creating a backup CA smart card, or enrolling a TKE workstation cryptographic adapter in the zone. OmniKey smart card readers are required to use CA smart cards with a zone key length of 2048-bits.

Table 5. CA smart card usage

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

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

Table 6 on page 10 indicates in more detail where TKE smart cards created in different releases can be used. Usage means employing a TKE smart card to store or load key parts or to generate and retain an authority signature key or a crypto adapter logon key, to copy keys and key parts from one smart card to another, to log on to the TKE workstation crypto adapter, or to create a profile for the TKE workstation crypto adapter. The TKE smart card must be enrolled in the zone where it is used, although this is not required to use the authority signature key or crypto adapter logon key on the smart card. The authority signature key and the crypto adapter logon key are not subject to zone constraints.

Table 6. TKE smart card usage

	Use on TKE 5.2 or before	**Use on TKE 5.3**	**Use on TKE 6.0**	**Use on TKE 7.0 and above**
Created on TKE 5.2 or before	Yes	Yes	Yes	No
Created on TKE 5.3	No	Yes	Yes	Yes[2]

Table 6. TKE smart card usage (continued)				
	Use on TKE 5.2 or before	**Use on TKE 5.3**	**Use on TKE 6.0**	**Use on TKE 7.0 and above**
Created on TKE 6.0, 1024-bit zone key	No	Yes[1]	Yes	Yes[2]
Created on TKE 6.0, 2048-bit zone key	No	No	Yes	Yes
Created on TKE 7.0 and above	No	No	No	Yes

[1] This smart card could contain:

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

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

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

When creating an EP11 smart card on TKE 8.1, you must use a smart card associated with part numbers 74Y0551 or 00JA710.

Datakey card usage

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

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

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

Host cryptographic modules managed by TKE

TKE manages host cryptographic modules on any CEC where that particular host cryptographic module is supported. In other words, for example, TKE is unaware whether a CEX3C module is running on an IBM System z10, IBM zEnterprise 196, IBM zEnterprise 114, IBM zEnterprise EC12, IBM zEnterprise BC12, IBM z13, IBM z13s, IBM z14, or IBM z15.

Table 7 on page 12 identifies the host cryptographic modules that each TKE release can manage.

Table 7. Host cryptographic modules managed by TKE LIC								
TKE release (LIC)	**Host cryptographic modules supported by TKE release**							
	CEX2C	**CEX3C**	**CEX4C**	**CEX4P**	**CEX5C**	**CEX5P**	**CEX6C**	**CEX6P**
TKE 5.2	Yes	No	No	No	No	No	No	No
TKE 5.3	Yes	Yes	No	No	No	No	No	No
TKE 6.0	Yes	Yes	Sometimes*	No	No	No	No	No
TKE 7.0	Yes	Yes	Sometimes*	No	No	No	No	No
TKE 7.1	Yes	Yes	Sometimes*	No	No	No	No	No
TKE 7.2	Yes	Yes	Yes	Yes#	No	No	No	No
TKE 7.3	Yes	Yes	Yes	Yes#	No	No	No	No
TKE 8.0	Yes	Yes	Yes	Yes#	Yes@,+	Yes#, $	No	No
TKE 8.1	Yes	Yes	Yes	Yes#	Yes@,+	Yes#, $	No	No
TKE 9.0	Yes	Yes	Yes	Yes#	Yes@,+	Yes#, $	Yes	Yes#
TKE 9.1	Yes	Yes	Yes	Yes#	Yes@,+	Yes#, $	Yes	Yes#
TKE 9.2	Yes	Yes	Yes	Yes#	Yes@,+	Yes#, $	Yes	Yes#

+

TKE 8.1 with the TKE Tower Code level of 3 or higher is required to manage a CEX5C at level CCA 5.3. The TKE Tower Code is include in TKE LIC Control Level 004 and beyond.

*****

A Crypto Express4 that is running in Common Cryptographic Architecture (CCA) mode as a CEX4C is only supported when running ICSF FMID HCR7790 or lower with the toleration APAR OA39075 that allows the CEX4C to report in as a CEX3C. In this case, ICSF sees the module as a CEX3C and manages it as a CEX3C.

#

Modules running in EP11 mode require smart cards to hold administrator certificates and master key material. Smart card readers must be attached to the TKE workstation to administer these host crypto module types.

@

You must be using one of the following levels of ICSF:

- ICSF FMID HCR77B0.
- ICSF FMID HCR77A1, HCR77A0, HCR7790, or HCR7780 in toleration mode (APAR OA45547) and also have the new function APAR OA44910.

$

You must be using one of the following levels of ICSF:

- ICSF FMID HCR77B0.
- ICSF FMID HCR77A1 in toleration mode (APAR OA45547) and also have the new function APAR OA44910.

Some host cryptographic configurations (in other words, specific cryptographic features or combinations of the CEC, host cryptographic module, CCA or EP11 level, and ICSF) require minimum levels of TKE to support the environment.

TKE hardware support and migration information

For information about TKE hardware support and migration, see the following:

- TKE Hardware Support and Migration Information (www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/TD106231)

Chapter 3. Planning for TKE

This topic describes the installation, configuration, and migration actions you need to consider for TKE.

Installation

For information about installing the TKE console, see:

- Service Guide for Trusted Key Entry Workstations (www.ibm.com/servers/resourcelink/lib03010.nsf/pagesByDocid/BE66F954000C29758525817900600DB2?OpenDocument)

  Note: You need an IBM id for Resource Link to view and download this publication.

This information applies to the following:

- TKE installation - 7327
- TKE installation - 7382
- TKE installation - 2461 TKE (FC 0097/0085)
- TKE installation - 2461 TKE (FC 0098/0086)

Configuring the TKE Cryptographic Coprocessor Adapter

For information about configuring the TKE Cryptographic Coprocessor Adapter, see:

- Service Guide for Trusted Key Entry Workstations (www.ibm.com/servers/resourcelink/lib03010.nsf/pagesByDocid/BE66F954000C29758525817900600DB2?OpenDocument)

  Note: You need an IBM id for Resource Link to view and download this publication.

TKE upgrade considerations

Considerations before upgrading a TKE or copying data from an existing TKE

- "DVD-RAM is not supported on a TKE 7.2 or later system" on page 13
- "Copying files to the TKE 7.0 or TKE 7.1 hard drive" on page 14
- "Copying files to a USB flash memory drive while on a TKE 7.0 or TKE 7.1 system" on page 14
- "Preparing for a new TKE local crypto adapter" on page 16

DVD-RAM is not supported on a TKE 7.2 or later system

Important: If you are still using DVD-RAM on a pre-TKE 7.2 system, DVD-RAM is not supported on TKE 7.2 or later systems. If you want to continue to use files that are on your DVD-RAM on a TKE 7.2 or later, you must remove the data from the DVD-RAM before your move to the TKE 7.2 or later system.

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

- Copy the files from the TKEDATA DVD-RAM to the TKE's hard drive before upgrading the TKE to version 7.2 or later. For more information, see "Copying files to the TKE 7.0 or TKE 7.1 hard drive" on page 14.
- Copy the files from the TKEDATA DVD-RAM to a USB flash memory drive that is formatted for TKEDATA from a TKE 7.0 or TKE 7.1 system. For more information, see "Copying files to a USB flash memory drive while on a TKE 7.0 or TKE 7.1 system" on page 14.

Copying files to the TKE 7.0 or TKE 7.1 hard drive

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

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

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

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

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

      Note: In general, store each file from the TKEDATA DVD-RAM into the directory that the file originally came from. General information about the three most common types of files that are saved on TKEDATA DVD-RAM include:

      - Key part files should be stored in the TKE Data Directory.
      - Profile and role definition files should be stored in the CNM Directory.
      - Data from either of the host migration wizards should be stored in the Configuration Data Directory.

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

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

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

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

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

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

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

      Note:

      - It can take up to 1 minute for the message to appear.
      - You can press OK to close the "USB Device Status" message or wait for it to close in 10 seconds.
   b. Perform the following steps only if you want to format the USB flash memory drive. Proceed to Step "4" on page 15 if you do not want to format the USB flash memory drive.

      The USB flash memory drive must be formatted if:

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

      You can use a USB flash memory drive that was formatted for TKEDATA on a TKE 7.2 or later system. To format the USB flash memory drive:

      i) From the Trusted Key Entry Console on your TKE 7.0 or TKE 7.1 system, open the Service Management window pane.
      ii) Open the Format Media application.
      iii) Select the "Trusted Key Entry Data" radio button and press the FORMAT button.
      iv) Select the radio button for the USB flash memory drive device you want to format and press OK.
      v) You might receive the "file system setting" window before the confirm format message. If you do, take the default setting and press the FORMAT button.
      vi) Press YES to confirm that you want to format the media.
      vii) Press OK to close the completion message.
4. Perform the following steps to copy the files from the TKEDATA DVD-RAM to the USB flash memory drive:
   a. From the Trusted Key Entry Console on your TKE 7.0 or TKE 7.1 system, open the Trusted Key Entry window pane.
   b. Open the TKE File Management Utility.

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

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

Note: After all the files are stored on the USB flash memory drive:

- The USB flash memory drive can be used as removable media on any TKE 7.0 or later system.
- You can remove the USB flash memory drive at any time.

5. Perform the following clean-up steps:
   a. Close the File Management Utility by selecting either “Exit” or “Exit and logoff” to close the TKE application window.
   b. Open the TKE Media Manager utility.

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

Preparing for a new TKE local crypto adapter

All TKEs have a local crypto adapter. After a TKE has been configured according to your TKE security policy, the TKE local crypto adapter will contain user-defined profiles and sometimes user-defined roles. You might want to configure a new TKE local crypto adapter with an existing set of user-defined roles and user-defined profiles if:

- Your TKE is given a new TKE local crypto adapter as part of an upgrade. For example, an upgrade from TKE 8.*x* to TKE 9.0 requires the 4767 TKE crypto adapter to be replaced with the 4768 TKE local crypto adapter.
- You want to configure a new TKE workstation local crypto adapter with the same user-defined roles and user-defined profiles found on an existing TKE local crypto adapter.

You might prefer to manually configure the new TKE local crypto adapter, but there are three methods for creating files with user-defined role and user-defined profile definitions that can be copied and later used to load the roles and profiles onto a new TKE local crypto adapter. The different methods for creating role and profile definition files that can be used to load the roles and profiles onto a TKE local crypto adapter are:

- “Method 1: Creating TKESavedRoles.dat and TKESavedProfiles.dat files from CNM” on page 16
- “Method 2: Creating TKESavedRoles.dat and TKESavedProfiles.dat files from the TKE Workstation Setup wizard” on page 16
- “Method 3: Creating individual user-defined role and user-defined profile definition files” on page 17

Method 1: Creating TKESavedRoles.dat and TKESavedProfiles.dat files from CNM

Beginning in TKE 8.0, the Crypto Node Management utility provides a feature that allows you to collect all the user-defined role and user-defined profile definitions in one operation. If any user-defined roles are found, the definitions are placed in the TKESavedRoles.dat file. If any user-defined profiles are found, the definitions are placed in the TKESavedProfiles.dat file. The following steps can be used to create these files:

1. From the Trusted Key Entry Console, select **Cryptographic Node Management Utility**.
2. Select **Access Control > Save User Roles and Profiles**.

Method 2: Creating TKESavedRoles.dat and TKESavedProfiles.dat files from the TKE Workstation Setup wizard

Beginning in TKE 7.3, the TKESavedRoles.dat and TKESavedProfiles.dat files can be created by a step inside the TKE Workstation Setup wizard. In TKE 7.3, only the tasks in the TKE Workstation setup wizard can use these files. The following steps can be used to create these files:

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

Method 3: Creating individual user-defined role and user-defined profile definition files

In all releases of the TKE, you can use a feature in the Cryptographic Node Management (CNM) utility to create individual role and profile definition files for each of your user-defined roles and profiles on the TKE's local crypto adapter. The files contain all the information that is required to load the roles and profiles onto a TKE's local crypto adapter. You can use the following steps to create individual role and profile definition files. **Note**: Use this method only if you are not on TKE 7.3 or later.

Procedure

1. On the source TKE workstation, from the Trusted Key Entry Console, select **Trusted Key Entry.**
2. Open the **Cryptographic Node Management** utility.
3. Sign on to the TKE crypto adapter if you are prompted to do so.
4. If you do not have customer-defined roles for which you need to create files, skip to step "7" on page 17.
5. **Select Access Control > Roles**.
   For each user-defined role:
   a) Highlight the user-defined role.
   b) Click **Edit**.
   c) Click **Save**.
   d) Enter a file name.
      File naming suggestion: Use *role name*.rol.
   e) Click **Save**.
      A message window opens confirming that the role has been saved.
   f) Click **OK** to close the message window.
   g) Click **Done** to end the edit session.
6. After the last user-defined role is saved, click **Done.**
7. If you do not have user-defined profiles, skip to step "10" on page 18
8. For each user-defined profile:
   a) Select **Access Controls > Profiles**.
   b) Highlight the user-defined profile.
   c) Click **Edit**.
   d) For passphrase profiles, enter a password.
      The password does not have to match the password that the profile has on the crypto adapter.

e) Click **Save**.

f) Enter a file name.

File naming suggestion: Use *profile name*.pro.

g) Click **Save**.

A message window opens confirming that the profile has been saved.

h) Click **OK** to close the message window.

i) Click **Done** to end the edit session.

9. After the last user-defined profile is saved, click **Done**.
10. Select **File > Exit** to exit the utility.

TKE (LIC) upgrade paths

Table 8 on page 18 shows which TKE licensed internal code (LIC) can be upgraded to a new LIC level.

Table 8. Summary of when a TKE workstation can be upgraded

Starting point			**Upgradable to TKE LIC level**									
TKE release (LIC)	**Hard-ware feature code**	**TKE crypto adapte r type**	**TKE 6.0 (FC 0858)**	**TKE 7.0 (FC 0860)**	**TKE 7.1 (FC 0867)**	**TKE 7.2 (FC 0850)**	**TKE 7.3 (FC 0872)**	**TKE 8.0 (FC 0877)**	**TKE 8.1 (FC 0878)**	**TKE 9.0 (FC 0879)**	**TKE 9.1 (FC 0880)**	**TKE 9.2 (FC 0881)**
TKE 5.3	0839	4764	Yes	No	No	No	No	No	No	No	No	No
TKE 6.0	0839	4764	**Base***	No	No	No	No	No	No	No	No	No
	0840											
TKE 7.0	0841	4765	N/A	**Base***	Yes	Yes	Yes	No	No	No	No	No
TKE 7.1	0841	4765	N/A	N/A	**Base***	Yes	Yes	No	No	No	No	No
TKE 7.2	0841	4765	N/A	N/A	N/A	**Base***	Yes	No	No	No	No	No
TKE 7.3	0841	4765	N/A	N/A	N/A	N/A	**Base***	No	No	No	No	No
	0842	4765	N/A	N/A	N/A	N/A	**Base***	Yes	Yes	Yes	Yes	Yes
TKE 8.0	0847	4767	N/A	N/A	N/A	N/A	N/A	**Base***	Yes	Yes	Yes	Yes
TKE 8.1	0847	4767	N/A	N/A	N/A	N/A	N/A	N/A	**Base***	Yes	Yes	Yes
	0097											
TKE 9.0	0085	4768	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**Base***	Yes	Yes
	0086											
TKE 9.1	0085	4768	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**Base***	Yes
	0086											
TKE 9.2	0085	4768	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**Base***
	0086											

Base*

The initial TKE LIC level installed on the TKE workstation before it was shipped.

Note: In general, you cannot upgrade the LIC level of your TKE workstation if the new LIC level requires a new TKE crypto adapter type. An exception is that upgrades from TKE 7.3 with hardware feature code 0842 to TKE 8.0 or TKE 8.1 are permitted, but the TKE crypto adapter must be replaced.

Notes about upgrading to TKE 9.0

- When TKE workstation feature 0842 or 0847 is upgraded to TKE 9.0, it becomes workstation feature 0849.
- When TKE workstation feature 0097 is upgraded to TKE 9.0, it becomes workstation feature 0080.
- When TKE workstation feature 0098 is upgraded to TKE 9.0, it becomes workstation feature 0081,

The upgrade to TKE 9.0 does not include the new secure workstation features of TKE. You must purchase a new TKE 9.0 workstation to obtain the new capability.

When you upgrade the LIC level of your TKE workstation, you can keep your user data.

TKE migration actions

Upgrading an existing TKE workstation to TKE 9.2

Notes:

- A TKE can only be upgraded to TKE 9.2 if the TKE feature is assigned to z14 or later.
- Only TRENTON workstations can be upgraded to TKE 9.2.
- If your TKE is currently at TKE 8.1 or older and you can upgrade it to TKE 9.2, you must purchase a 4768 crypto card with your upgrade.
- TKE 9.2 firmware is only available on USB media or through a network install.

When you upgrade an existing workstation to TKE 9.2, the TKE licensed internal code (LIC) is updated and a new TKE local crypto adapter is installed in the workstation. Both of these actions are completed by an IBM Customer Engineer (CE). At the end of the process, when the CE runs the TKE Workstation Setup wizard, you need to make the necessary customer-based decisions. The following steps are an overview of the entire upgrade process:

1. You need to create the **TKESavedRoles.dat** and **TKESavedProfiles.dat** files that are used to load your roles and profiles onto the new 4768 TKE local crypto adapter that the TKE workstation receives. For instructions on how to create these files, see “Preparing for a new TKE local crypto adapter” on page 16. These files are included in the data that is collected during the save upgrade data.
2. Before the CE starts the firmware upgrade, the CE collects customer data on the workstation by using the **Save Upgrade Data** utility. The data is placed on a USB flash memory drive.
3. The CE powers down the TKE workstation and replaces the 4767 crypto adapter with the 4768 crypto adapter.

   Notes:

   - When the 4767 crypto adapter is replaced with the 4768 crypto adapter, the TKE workstation's feature code also changes.

     Table 9. TKE feature code changes

Starting TKE workstation feature code	New TKE workstation feature code
0097	0080
0098	0081

   - Code is not placed on the new 4768 crypto adapter until the TKE Workstation Setup wizard is run.
4. The CE installs the new TKE firmware on the TKE workstation by using the Install/Recovery procedure.
5. The CE reapplies the customer data onto the TKE workstation by using the frame roll installation procedure. The USB flash memory drive with the **saved upgrade data** is used during this procedure. This step also restores the network settings.
6. The CE runs the TKE Workstation Setup wizard to complete the workstation setup process. The wizard includes a step for updating the code on the new TKE workstation’s local crypto adapter.
7. During a TKE workstation upgrade, you need to make the following customer configuration decisions. If you are not present when the CE runs the TKE Workstation Setup wizard, you can run the TKE Workstation Setup wizard on your own. The following are a list of wizard steps that require your attention:

Initialize TKE crypto adapter
The new 4768 TKE local crypto adapter must be initialized. You need to decide whether the TKE local crypto adapter is to be initialized for use with passphrase or smart card profiles.

Note that initializing the TKE local adapter zeroizes the adapter. Initialize the TKE local crypto adapter only one time or when you want to return to a known starting point.

Hints:

- If your user-defined TKE local adapter profiles use the system-supplied roles of TKEUSER or TKEADM, you want to initialize your adapter for use with Passphrase profiles.
- If your user-defined TKE local adapter profiles use the system-supplied roles of SCTKEUSR or SCTKADM, you want to initialize your adapter for use with smart card profiles.

Enable smart card readers
If you use smart cards, select **Yes**.

Customize displayed hash size
If you are subject to any regulations or policies that require you to limit the length of your displayed key verification patterns, you can select a reduced display length.

Load user roles and profiles
In the TKE 9.2 upgrade, the TKE workstation received a new TKE local crypto adapter. Your user-defined roles and profiles need to be loaded onto this new adapter. If you created and saved the **TKESavedRoles.dat** and **TKESavedProfiles.dat** files, as mentioned in step 1, the wizard finds the files and reloads your roles and profiles.

Note: You must set the passphrase for any passphrase profile you load onto the new TKE crypto adapter.

Add new access control points to your user roles
If you have any user-defined roles, you might need to add new access control points to the roles.

Check TKE crypto adapter group profiles
In the past, it was recommended that members of a TKE local crypto adapter group profile be assigned the role of DEFAULT. TKE now contains the system-supplied role of TKEGRPMB (TKE group member role). The TKEGRPMB role contains only the required ACPs. Checking TKE crypto adapter group profiles determines whether you have any TKE local adapter group profile members with the role of DEFAULT. If you do, the wizard offers you the option to change the member's role to TKEGRPMB.

Save user roles and profiles
If you changed any group member profiles, you might want to save your updated user-defined roles and profiles.

Convert crypto module groups to domain groups
If you have any crypto module groups from a pre-TKE 8.0 system, you can use this utility to created new domain groups based on the existing group definition.

Note: You can do this process only when you are willing and able to open the hosts included in the group. You might want to do the conversion later.

Enroll TKE crypto adapter in a zone
If your TKE was enrolled in a zone before the upgrade, you need to enroll your new 4768 TKE local crypto adapter in your zone. The CA smart card with the zone is required for this operation.

Add migration zone
If you use the Configuration Migration Tasks application, the list of known MCAs was cleared when the new 4768 crypto module was initialized. You need to add your MCAs to your MCA zone list. The MCA smart card or cards are required for this operation.

Add key part holder certificates
The upgrade operation saved and restored customer data. The list of known key part holders (KPHs) is restored. You do not need to add your KPH certificates again.

Change enhanced password encryption policy

The TKE always uses the best available method for protecting the host password during a sign-on operation. When ICSF is at FMID HCR77B0 or later, enhanced password protection is used. You can select a policy that only allows a host sign-on attempt if enhanced password protection is used. IBM recommends that you move to the minimum ICSF level of FMID HCR77B0 and that you select the TKE policy that only allows a sign-on to systems that support enhanced password protection.

Your TKE 9.2 is ready for use when all preceding steps are completed.

TKE host crypto module migration

See Overview of the IBM TKE host crypto module migration feature (mediacenter.ibm.com/media/Host+Crypto+Module+Migration+Video+1+-+Overview+of+the+IBM+TKE+Host+Module+Migration+Feature/1_xd0juqn1) for information on host crypto module migration.

Chapter 4. Setting up TKE

Use the following sections to set up a TKE workstation:

TKE workstation setup and customization

For information about setting up and customizing the TKE workstation, see

- Service Guide for Trusted Key Entry Workstations (www.ibm.com/servers/resourcelink/lib03010.nsf/pagesByDocid/BE66F954000C29758525817900600DB2?OpenDocument)

  Note: You need an IBM id for Resource Link to view and download this publication.

TKE workstation setup wizard

See Initialize your new Trusted Key Entry (TKE) using the TKE Workstation Setup wizard (mediacenter.ibm.com/media/Initialize+Your+New+Trusted+Key+Entry+(TKE),+Using+the+TKE+Workstation+Setup+Wizard/1_5vrbxdo1) for information about the TKE workstation setup wizard.

TKE best practices

This information describes the setup required for TKE to manage host crypto modules, and a set of setup steps to perform on the TKE workstation. TKE workstations initialized for passphrase and initialized for smart card use are considered separately.

Checklist for loading a TKE machine - passphrase

Expectations

- You are working with CCA host crypto modules
- The support element has enabled TKE on these host crypto modules
- LPARs are established
- TKE licensed internal code (LIC) is loaded on the TKE workstation
- Segments 1, 2, and 3 have been loaded on the TKE workstation crypto adapter
- The TKE host transaction program has been configured and started in the host TKE LPAR
- ICSF is started in each LPAR

Setup

- 2 TKEs both running the same level of software
  - One for production
  - One for backup
- 2 Central electronic complex (CEC) cards being shared
  - One Test LPARs (Domain 0)
  - Three Production LPARs (Domain 1, 2, 3)

TKE can load the master key in a group of domains as defined by a domain group.

- Host TKE LPAR 1

  When defining the LPAR activation profile, the usage domain will be 1 and the control domain will be 0, 1, 2, 3.

The following User IDs are used to restrict access to the TKE workstation crypto adapter:

- TKEUSER - can run the main TKE application
- TKEADM - can create and update TKE roles and profiles
- KEYMAN1 - can clear TKE new master keys and load first master key parts
- KEYMAN2 - can load TKE middle and last key parts and reencipher TKE workstation key storage

Authorities are used to restrict access to the CCA crypto modules on the host machine.

One way to control access to CCA host crypto modules is with a minimum of seven host authorities.

- ISSUER
  - Disable host crypto module
  - Enable host crypto module issue
  - Access control issue
  - Zeroize domain issue
  - Domain control change issue
- COSIGN
  - Access control co-sign
  - Enable host crypto module co-sign
  - Zeroize domain co-sign
  - Domain control change co-sign
- MKFIRST
  - AES, DES, ECC (APKA), or RSA load first master key part
  - Clear new master key register
  - Clear old master key register
- MKMIDDLE
  - AES, DES, ECC (APKA), or RSA combine middle master key parts
- MKLAST
  - AES, DES, ECC (APKA), or RSA combine final master key part
  - Set RSA master key
- FIRSTCLEAR
  - Load first operational key part
  - Clear operational key register
- ADDCOMP
  - Load additional operational key part
  - Complete key

The following tasks should be run using the TKE workstation to set up the TKE workstation and the host crypto modules for use. Be aware that the Service Management tasks available to you will vary depending on the console user name you used to log on.

1. Customize Network Settings
2. Customize Console Date/Time

3. Initialize the TKE workstation crypto adapter for passphrase use
    a. Predefined TKE roles and profiles are loaded.
    b. The TKE master keys are set and TKE key storages are initialized.
4. Logon to CNM with KEYMAN1 - OPTIONAL
    a. Clear the new DES/PKA and AES master key registers
    b. Enter known first master key parts for the DES/PKA and AES master keys.
    c. Logoff
5. Logon to CNM with KEYMAN2 - OPTIONAL
    a. Enter known middle and last master key parts for the DES/PKA and AES master keys.
    b. Reencipher DES, PKA, and AES key storage
    c. Logoff
6. Logon to CNM with TKEADM
    a. Create user defined roles - OPTIONAL
    b. Create user defined profiles - OPTIONAL
    c. Create groups and add users - OPTIONAL

        Note: Group members should already be defined.
    d. Change the passphrases for all of the predefined profiles - TKEADM, TKEUSER, KEYMAN1, and KEYMAN2
7. Log on to the main TKE application with TKEUSER profile or another profile with the same authority
    a. Load the default authority key for key index 0
    b. Change these options of your security policy via the TKE preferences menu
        - Blind Key Entry
        - Removable media only
    c. Create a Host
    d. Create domain groups - OPTIONAL
    e. Open a host or a domain group (requires host logon)
    f. Open a crypto module notebook or domain group notebook
    g. Create role or roles
    h. Generate authority key or keys and save them to binary file or files
    i. Create different authorities using the different authority key or keys that were just generated.
    j. Delete the authority 00 or change the authority key to a key that is not the default key. If you delete authority 00 make sure that you have 2 other known authority keys that have the Domain control change issue and co-sign.
8. Configure 3270 Emulators
9. Backup Critical Console Data onto a USB flash memory drive.
10. Customize Scheduled Operations to schedule the backup critical console data task

Checklist for loading a TKE machine - smart card

Expectations:

- You are working with CCA or EP11 host crypto modules.
- The support element has enabled TKE on these host crypto modules.
- LPARs are established (set up and predefined).
- TKE licensed internal code (LIC) is loaded on the TKE workstation.

- Segments 1, 2, and 3 have been loaded on the TKE workstation crypto adapter.
- The TKE host transaction program has been configured and started in the host TKE LPAR.
- ICSF is started in each LPAR.
- Smart card readers are attached.

Setup

- 2 TKEs both running the same level of software
  - One for production
  - One for backup
- 2 CECs cards being shared
  - One Test LPARs (Domain 0)
  - Three Production LPARs (Domain 1, 2, 3)

  TKE can load the master key in a group of domains as defined by a domain group.
- Host TKE LPAR 1

  When defining the LPAR activation profile, the usage domain will be 1 and the control domain will be 0, 1, 2, 3.

Profiles and roles are used to restrict access to the TKE workstation crypto adapter. There are two roles, listed below, that are needed to use the TKE and CNM applications. Profiles are created by first generating a crypto adapter logon key and then creating a profile using the crypto adapter logon key.

- SCTKEUSR - can run the main TKE application
- SCTKEADM - can run CNM to create and update TKE roles and profiles

Authorities are used to restrict access to the CCA crypto modules on the host machine.

Administrators are used to restrict access to the EP11 crypto modules on the host machine.

One way to control access to the CCA host crypto modules is with a minimum of seven host authorities.

- ISSUER
  - Disable host crypto module
  - Enable host crypto module issue
  - Access control issue
  - Zeroize domain issue
  - Domain control change issue
- COSIGN
  - Access control co-sign
  - Enable host crypto module co-sign
  - Zeroize domain co-sign
  - Domain control change co-sign
- MKFIRST
  - AES, DES, ECC (APKA), or RSA load first master key part
  - Clear new master key register
  - Clear old master key register
- MKMIDDLE
  - AES, DES, ECC (APKA), or RSA combine middle master key parts
- MKLAST
  - AES, DES, ECC (APKA), or RSA combine final master key part

  - Set RSA master key
- FIRSTCLEAR
  - Load first operational key part
  - Clear operational key register
- ADDCOMP
  - Load additional operational key part
  - Complete key

The steps to set up the TKE workstation for smart card use are as follows. Be aware that the Service Management tasks available to you will vary depending on the console user name you used to log on.

1. Customize Network Settings.
2. Customize Console Date/Time.
3. Initialize the TKE workstation crypto adapter for smart card use:
   a. Predefined TKE roles and profiles are loaded.
   b. The TKE master keys are set and TKE key storages are initialized.
4. Open the SCUP application.
   a. Create a CA smart card.
   b. Backup CA smart cards.
   c. Create TKE smart cards.

      Note: In general, smart cards created on a particular TKE release cannot be used on TKE workstations that are at prior release levels. There are exceptions. See “Smart card usage” on page 10.
   d. Create EP11 smart cards.
   e. Enroll the TKE workstation crypto adapter with the CA card.
5. Open CNM.

   Note: Choose the "Default Logon". The temp default role will be used, and has full access to do everything on the crypto adapter.
   a. Enter known DES/PKA and AES master keys. (Optional)
      - Do this only if you want to have known master keys to use again.
   b. Reencipher DES, PKA, and AES key storage. (Optional)
      - Do this only if you entered your own master keys.
   c. Generate TKE workstation crypto adapter logon keys for each smart card that will be logging on to the TKE or CNM applications.
   d. Create new profile or profiles for the smart cards under the Access Control menu. The roles for these profiles are loaded in the crypto adapter when TKE's Crypto Adapter Initialization task is run.
   e. Create group or groups and add users.

      Note: Group members should already be defined.
   f. Load the default role.
      - When the TKE workstation crypto adapter is initialized the TEMPDEFAULT role is loaded. You need to load the DEFAULT role to secure the TKE workstation.
6. Log on to the main TKE application with the SCTKEUSR profile or another profile with the same authority.
   a. Load the default authority key for key index 0.
   b. Change these options of your security policy via the TKE preferences menu

- Blind Key Entry
- Removable media only

c. Create a Host.

d. Create domain groups. (Optional)

e. Open a host or a domain group (requires host logon).

f. Open a crypto module notebook or domain group notebook.

g. For CCA host crypto modules:

i) Create roles.

ii) Generate authority keys and save them to TKE smart cards.

Note: You can generate and save 1024-bit and 2048-bit RSA keys and BP-320 ECC keys on TKE smart cards. Authorities with 2048-bit RSA keys are supported starting with the CEX3C. Authorities with BP-320 ECC keys are supported starting with the CEX5C.

iii) Create different authorities using the different authority keys that were just generated.

iv) Delete the authority 00 or change the authority key to a key that is not the default key. If you delete authority 00 make sure that you have 2 other known authority keys that have the Domain control change issue and cosign.

h. For EP11 host crypto modules:

i) Generate administrator keys and save them to EP11 smart cards.

ii) Zeroize the host crypto module or the set of domains you want to administer. Zeroizing a host crypto module or domain puts it in "imprint mode", where administrators can be added without using signed commands.

iii) Add crypto module and domain administrators.

iv) Set the signature threshold and revocation signature threshold on each crypto module and domain. This ends imprint mode.

7. Configure 3270 Emulators.
8. Backup Critical Console Data.
9. Customize Scheduled Operations to schedule the backup critical console data task.
10. If using the same set of smart cards on another TKE, you need to use the Remote Enroll feature for TKE.

Appendix A. Other resources

Here are other resources that will help you learn more about TKE.

Initialize your new Trusted Key Entry (TKE) using the TKE Workstation Setup wizard (mediacenter.ibm.com/media/Initialize+Your+New+Trusted+Key+Entry+(TKE),+Using+the+TKE+Workstation+Setup+Wizard/1_5vrbxdo1): This video shows you how to setup your TKE workstation using the Trusted Key Entry Workstation Setup Wizard.

IBM TKE easy way to migrate or clone a TKE workstation (mediacenter.ibm.com/media/IBM+TKE+Easy+Way+to+Migrate+or+Clone+a+TKE+Workstation/1_5ihmp5sq): This video shows you how to migrate or clone a TKE workstation.

Trusted Key Entry (TKE) CCA Playlist (mediacenter.ibm.com/media/1_tcn7d7qj): An 8-video series that shows you everything you need to do in order to load master keys from the TKE product.

Overview of the IBM TKE host crypto module migration feature (mediacenter.ibm.com/media/Host+Crypto+Module+Migration+Video+1+-+Overview+of+the+IBM+TKE+Host+Module+Migration+Feature/1_xd0juqn1): This video provides an introduction to the host crypto module migration feature of the IBM Trusted Key Entry (TKE).

Using Trusted Key Entry (TKE) to initialize smart cards (mediacenter.ibm.com/media/Using+Trusted+Key+Entry+(TKE)+to+Initialize+Smart+Cards+for+TKE+Workstation+and+CCA+Normal-Mode+Module+Management/1_tq4cfu63): This video shows you how to initialize all the smart card you will need to access your TKE workstation and manage CCA host crypto module and domains.

Create TKE local crypto adapter profiles using the TKE Workstation Logon Profile wizard (mediacenter.ibm.com/media/Create+TKE+Local+Crypto+Adapter+Profiles+Using+the+TKE+Workstation+Logon+Profile+Wizard/1_btlonb4g): This video shows you how to create the profiles you need to access your TKE workstation. These profiles are used when you open TKE applications and utilities.

Create and open Trusted Key Entry (TKE) host definitions (mediacenter.ibm.com/media/Create+and+Open+Trusted+Key+Entry+(TKE)+Host+Definitions/1_l0yq9j7n)

Create and open Trusted Key Entry (TKE) CCA domain groups (mediacenter.ibm.com/media/Create+and+Open+Trusted+Key+Entry+(TKE)+CCA+Domain+Groups/1_3eujuv5g)

Creating roles and profiles for managing CCA modules using the Trusted Key Entry (TKE) Setup Module Policy wizard (mediacenter.ibm.com/media/Creating+Roles+and+Profiles+for+Managing+CCA+Modules+Using+the+Trusted+Key+Entry+(TKE)+Setup+Module+Policy+Wizard/1_igid8h1r)

Creating CCA master key parts using the 'Generate a Set of Master Key Parts' feature of Trusted Key Entry (TKE) (mediacenter.ibm.com/media/Creating+CCA+Master+Key+Parts+Using+the+%201CGenerate+a+Set+of+Master+Key+Parts%201D+Feature+of+Trusted+Key+Entry+(TKE)/1_2q4wytv4)

Loading CCA master key parts using the “Load All New Master Keys” feature of Trusted Key Entry (TKE) (mediacenter.ibm.com/media/Loading+CCA+Master+Key+Parts+Using+the+%201CLoad+All+New+Master+Keys%201D+Feature+of+Trusted+Key+Entry+(TKE)/1_zo63p677)

IBM techdoc on TKE hardware support and migration:

- TKE Hardware Support and Migration Information (www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/TD106231)

z/OS publications updated in support of TKE:

- z/OS Cryptographic Services publications for ICSF FMID HCR77D1 (www.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSICSFFmidHCR77D1Publications?OpenDocument)

- z/OS Cryptographic Services publications for ICSF FMID HCR77D0 (www.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSICSFFmidHCR77D0Publications?OpenDocument)
- z Systems Processor Resource/Systems Manager Planning Guide (www.ibm.com/support/docview.wss?uid=isg22dec9fb95bdff17385257dc4007a164f&aid=1)

Appendix B. Accessibility

Accessible publications for this product are offered through IBM Documentation (www.ibm.com/docs/en/zos).

If you experience difficulty with the accessibility of any z/OS information, send a detailed message to the Contact the z/OS team web page (www.ibm.com/systems/campaignmail/z/zos/contact_z) or use the following mailing address.

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
United States

Accessibility features

Accessibility features help users who have physical disabilities such as restricted mobility or limited vision use software products successfully. The accessibility features in z/OS can help users do the following tasks:

- Run assistive technology such as screen readers and screen magnifier software.
- Operate specific or equivalent features by using the keyboard.
- Customize display attributes such as color, contrast, and font size.

Consult assistive technologies

Assistive technology products such as screen readers function with the user interfaces found in z/OS. Consult the product information for the specific assistive technology product that is used to access z/OS interfaces.

Keyboard navigation of the user interface

You can access z/OS user interfaces with TSO/E or ISPF. The following information describes how to use TSO/E and ISPF, including the use of keyboard shortcuts and function keys (PF keys). Each guide includes the default settings for the PF keys.

- *z/OS TSO/E Primer*
- *z/OS TSO/E User's Guide*
- *z/OS ISPF User's Guide Vol I*

Dotted decimal syntax diagrams

Syntax diagrams are provided in dotted decimal format for users who access IBM Documentation with a screen reader. In dotted decimal format, each syntax element is written on a separate line. If two or more syntax elements are always present together (or always absent together), they can appear on the same line because they are considered a single compound syntax element.

Each line starts with a dotted decimal number; for example, 3 or 3.1 or 3.1.1. To hear these numbers correctly, make sure that the screen reader is set to read out punctuation. All the syntax elements that have the same dotted decimal number (for example, all the syntax elements that have the number 3.1)

are mutually exclusive alternatives. If you hear the lines `3.1 USERID` and `3.1 SYSTEMID`, your syntax can include either `USERID` or `SYSTEMID`, but not both.

The dotted decimal numbering level denotes the level of nesting. For example, if a syntax element with dotted decimal number 3 is followed by a series of syntax elements with dotted decimal number 3.1, all the syntax elements numbered 3.1 are subordinate to the syntax element numbered 3.

Certain words and symbols are used next to the dotted decimal numbers to add information about the syntax elements. Occasionally, these words and symbols might occur at the beginning of the element itself. For ease of identification, if the word or symbol is a part of the syntax element, it is preceded by the backslash (\) character. The `*` symbol is placed next to a dotted decimal number to indicate that the syntax element repeats. For example, syntax element `*FILE` with dotted decimal number 3 is given the format `3 \* FILE`. Format `3* FILE` indicates that syntax element `FILE` repeats. Format `3* \* FILE` indicates that syntax element `* FILE` repeats.

Characters such as commas, which are used to separate a string of syntax elements, are shown in the syntax just before the items they separate. These characters can appear on the same line as each item, or on a separate line with the same dotted decimal number as the relevant items. The line can also show another symbol to provide information about the syntax elements. For example, the lines `5.1*, 5.1 LASTRUN, and 5.1 DELETE` mean that if you use more than one of the `LASTRUN` and `DELETE` syntax elements, the elements must be separated by a comma. If no separator is given, assume that you use a blank to separate each syntax element.

If a syntax element is preceded by the % symbol, it indicates a reference that is defined elsewhere. The string that follows the % symbol is the name of a syntax fragment rather than a literal. For example, the line `2.1 %OP1` means that you must refer to separate syntax fragment `OP1`.

The following symbols are used next to the dotted decimal numbers.

? indicates an optional syntax element
The question mark (?) symbol indicates an optional syntax element. A dotted decimal number followed by the question mark symbol (?) indicates that all the syntax elements with a corresponding dotted decimal number, and any subordinate syntax elements, are optional. If there is only one syntax element with a dotted decimal number, the ? symbol is displayed on the same line as the syntax element, (for example `5? NOTIFY`). If there is more than one syntax element with a dotted decimal number, the ? symbol is displayed on a line by itself, followed by the syntax elements that are optional. For example, if you hear the lines `5 ?, 5 NOTIFY`, and `5 UPDATE`, you know that the syntax elements `NOTIFY` and `UPDATE` are optional. That is, you can choose one or none of them. The ? symbol is equivalent to a bypass line in a railroad diagram.

! indicates a default syntax element
The exclamation mark (!) symbol indicates a default syntax element. A dotted decimal number followed by the `!` symbol and a syntax element indicate that the syntax element is the default option for all syntax elements that share the same dotted decimal number. Only one of the syntax elements that share the dotted decimal number can specify the ! symbol. For example, if you hear the lines `2? FILE, 2.1! (KEEP), and 2.1 (DELETE)`, you know that `(KEEP)` is the default option for the `FILE` keyword. In the example, if you include the `FILE` keyword, but do not specify an option, the default option KEEP is applied. A default option also applies to the next higher dotted decimal number. In this example, if the `FILE` keyword is omitted, the default `FILE(KEEP)` is used. However, if you hear the lines `2? FILE, 2.1, 2.1.1! (KEEP)`, and `2.1.1 (DELETE)`, the default option KEEP applies only to the next higher dotted decimal number, `2.1` (which does not have an associated keyword), and does not apply to `2? FILE`. Nothing is used if the keyword `FILE` is omitted.

*** indicates an optional syntax element that is repeatable**
The asterisk or glyph (*) symbol indicates a syntax element that can be repeated zero or more times. A dotted decimal number followed by the * symbol indicates that this syntax element can be used zero or more times; that is, it is optional and can be repeated. For example, if you hear the line `5.1* data area`, you know that you can include one data area, more than one data area, or no data area. If you hear the lines `3* , 3 HOST, 3 STATE`, you know that you can include `HOST, STATE`, both together, or nothing.

Notes:

1. If a dotted decimal number has an asterisk (*) next to it and there is only one item with that dotted decimal number, you can repeat that same item more than once.
2. If a dotted decimal number has an asterisk next to it and several items have that dotted decimal number, you can use more than one item from the list, but you cannot use the items more than once each. In the previous example, you can write `HOST STATE`, but you cannot write `HOST HOST`.
3. The * symbol is equivalent to a loopback line in a railroad syntax diagram.

+ indicates a syntax element that must be included

The plus (+) symbol indicates a syntax element that must be included at least once. A dotted decimal number followed by the + symbol indicates that the syntax element must be included one or more times. That is, it must be included at least once and can be repeated. For example, if you hear the line `6.1+ data area`, you must include at least one data area. If you hear the lines `2+, 2 HOST,` and `2 STATE`, you know that you must include `HOST, STATE,` or both. Similar to the * symbol, the + symbol can repeat a particular item if it is the only item with that dotted decimal number. The + symbol, like the * symbol, is equivalent to a loopback line in a railroad syntax diagram.

Notices

This information was developed for products and services that are offered in the USA or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

This information could include missing, incorrect, or broken hyperlinks. Hyperlinks are maintained in only the HTML plug-in output for IBM Documentation. Use of hyperlinks in other output formats of this information is at your own risk.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Site Counsel
2455 South Road

Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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 illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or

reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's name, email address, phone number, or other personally identifiable information for purposes of enhanced user usability and single sign-on configuration. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at ibm.com®/privacy and IBM's Online Privacy Statement at ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at ibm.com/software/info/product-privacy.

Policy for unsupported hardware

Various z/OS elements, such as DFSMSdfp, JES2, JES3, and MVS™, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those

products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (www.ibm.com/software/support/systemsz/lifecycle)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and Trademark information (www.ibm.com/legal/copytrade.shtml).

Index

Product Number: 5650-ZOS