Linux on Z and LinuxONE Trusted Key Entry 9.1

How to set an AES master key



This edition applies to the TKE version 9.1 and to all subsequent versions and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 2019. US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this document	V
Chapter 1. Getting started	
Scenario	
Prerequisites	
Starting the TKE console	3
Chapter 2. Establishing the security environment	
Enabling the TKE smart card support	5
Creating and connecting a host	
Creating the required roles and authorities	15
Chapter 3. Setting an AES master key on a CCA coprocessor	25
Generating key parts	25
Loading key parts	
Activating the master key	
More information	
· · · · · · ·	
ACCESSIDIUTY	
Notices	41
Trademarks	

About this document

This publication outlines a procedure how to create an AES master key on a cryptographic coprocessor configured in CCA coprocessor mode (shortly referred to as CCA coprocessor) using the Trusted Key Entry (TKE) workstation. The cryptographic coprocessor is connected to an IBM Z[®] mainframe that runs an instance of Linux on Z.

What this document describes

There are multiple master key types and different methods how to create and set these keys using TKE capabilities. This document focuses on the creation and setting of an AES master key on a CCA coprocessor.

What this document does not describe

This document does not describe the complete process of setting up a comprehensive security concept, nor does it demonstrate all security features available from the TKE workstation.

Further information

For information about sophisticated features, for example, for using TKE domain groups, refer to the *Trusted Key Entry Workstation User's Guide* (SC14-7511) from the <u>IBM Resource Link</u> or from the <u>IBM</u> Knowledge Center.

Terminology

A cryptographic coprocessor is also called a cryptographic adapter. The TKE graphical user interface uses the term *crypto module* for a cryptographic coprocessor.

vi Linux on Z and LinuxONE: How to set an AES master key

Chapter 1. Getting started

As a single point of control, you require a Trusted Key Entry workstation (TKE) to securely manage multiple cryptographic coprocessors with their domains, master keys and operational keys stored inside.

The TKE provides the following secure services:

- Loading and maintaining master and operational keys into the host cryptographic hardware.
- Configuring and managing the cryptographic coprocessors in the host, for example, configure a coprocessor for running in CCA coprocessor mode.
- Providing a host cryptographic hardware migration feature. The TKE allows you to collect data from one host cryptographic coprocessor and apply the data to another host cryptographic coprocessor.
- Managing the involved smart cards.

A TKE comprises the following components:

- the hardware: a workstation with a cryptographic coprocessor which is used for secure communication with connected hosts
- the LIC (Licensed Internal Code) which includes an embedded operating system which supports one single application. No other applications or products can be installed on the TKE.
- smart card readers and smart cards.

Each TKE version is closely associated with the host platforms that it supports.

The TKE implementation uses a zone concept to ensure the secure transfer of key parts. After a short introduction of this concept, this document outlines the process how to initialize a certificate authority smart card (CA smart card) and the required TKE smart cards within a zone. Following this, you are guided through a scenario how to set a master key on a CCA coprocessor.

Note: The Trusted Key Entry workstation is a powerful appliance used to manage IBM Z cryptographic coprocessors. It provides hardware-based key management services with proper encryption strength, dual controls, and security-relevant auditing.

There are multiple ways and methods for setting master keys on a cryptographic adapter (coprocessor). New users of the TKE services may be overwhelmed by all the offered features and functions.

Therefore, the illustrated scenario presents one quick and easy path, but nevertheless a valid real-life approach, to generate and activate an AES master key on a domain of a cryptographic adapter configured in CCA coprocessor mode. This master key is composed from two key parts, which are individually generated and owned by two persons in a Linux on Z installation.

Figure 1 on page 2 depicts the environment in which the TKE workstation applications work. In Linux on Z, the TKE communicates with the host coprocessors using a TKE daemon called catcher.exe. This daemon is listening on a certain port for TKE commands.

In addition, a support element (SE) is required for cryptographic configuration. This is a dedicated workstation used for monitoring and operating IBM Z hardware. TKE commands must be permitted on the SE before any commands issued by the TKE workstation can be processed.

A master key is finally set within one or more domains of the attached coprocessors.



Figure 1. The TKE workstation environment

Scenario

An AES master key, which is composed from two key parts, is created and activated.

In the scenario described in this document, a security environment is established with two authorities for module administrators who manage the cryptographic coprocessor, and another two authorities for key administrators who create and activate a new master key. Only if both authorities work together, the required tasks can be completed. This approach is called dual control security.

The key parts are generated on two separate smart cards by two key administrators with different privileges. The key parts are loaded from the smart cards onto the cryptographic coprocessor.

The first key administrator is authorized to create and load the first key part. The second key administrator is authorized to create and load the second key part. Loading the second key part will automatically create the final master key. Both key administrators will be authorized to activate the new master key.

Prerequisites

On your Linux host system, you must install the CCA RPM or DEB package, which contains a Linux TKE daemon. This daemon must be running and ready to receive TKE requests. Also, you must enable the involved coprocessor to perform TKE commands.

You need to start the catcher.exe program, which is the Linux TKE daemon to handle administrative commands between the TKE and the cryptographic coprocessors. You can use the CSUTKEcat system initialization script to handle the daemon via systemctl. The catcher.exe daemon is automatically started by the CSUTKEcat system initialization script when Linux starts. You can also use this script to start or stop the catcher.exe from the command line. To start the catcher.exe, use the command:

systemctl start CSUTKEcat.service

You must ensure that the firewall of your Linux system allows to access the catcher.exe via port 50003, because this daemon listens for TKE commands on this port. These commands are translated into **ioctl** commands which communicate with the zcrypt device driver.

To verify whether the catcher.exe daemon is running on your system, enter the following command and look for the daemon in the output list:

# ps ax		
 9689 ? 	Ss	0:11 /opt/IBM/CCA/bin/catcher.exe

This description shows how to set a master key on a cryptographic coprocessor that is running in CCA mode. From the support element (SE), you must at first enable such coprocessors to perform TKE commands.

Therefore, logon to the appropriate support element. Open **Systems Management**, then select the system with the attached cryptographic coprocessor. In the list of **Tasks**, navigate to **Configuration** and open the **Cryptographic Configuration** dialog (Figure 2 on page 3). Select the appropriate cryptographic coprocessor and press the **TKE Commands...** button. In the upcoming dialog, select the **Permit TKE commands** check box and confirm your request when prompted. This action changes the text entry in the **TKE commands** column in Figure 2 on page 3 from **Denied** to **Permitted**.

Fast path: Logon SE → System Management → Tasks → Configuration → Cryptographic Configuration

<mark>∰</mark> ? c	ryptogra	phic Config	uration - M35						
- Crypto	graphic Inf	ormation —							
Select	Number	Status	Crypto Serial	Number	Туре		Operating mode	TKE Commands	
0	00	Configured	YH10DV62P3	68	CEX5S Accelera	itor	Default	Not supported	
0	03	Configured	YH10DV5763	38	CEX5S EP11 Co	processor	Default	Permitted	
0	04	Configured	YH10DV7313	24	CEX6S Accelera	itor	Default	Not supported	
۲	05	Configured	YH10DV7313	08	CEX6S CCA Co	processor	Default	Denied	
0	06	Configured	YH10DV7313	14	CEX6S EP11 Co	processor	Default	Permitted	
Select	a Cryptog	raphic num	per and then cl	ick the t	ask push button.		1		
View I	Details	Test RNG/C	Zeroize	Doma	in Management	TKE Com	mands Crypt	o Type Configuratio	n
Zeroize	All Te:	st RNG/CIS o	n All UDX Co	onfigurati	on Refresh	Cancel	Help		

Figure 2. Permit TKE commands

Starting the TKE console

You can perform all tasks required for configuring your smart cards and for setting a new master key on attached cryptographic coprocessors from the TKE console on the TKE workstation.

You can configure that the Trusted Key Entry welcome dialog automatically loads on start-up. Click on **Launch the Trusted Key Entry web application**. Then the initial **Trusted Key Entry Console** (Figure 3 on page 4) opens and offers access to a set of commonly used applications and utilities available on the TKE workstation.



Figure 3. TKE Console - starting the Trusted Key Entry program

What to do next

Before you can create and load a master key, you must have completed all sub-tasks described in <u>Chapter</u> 2, "Establishing the security environment," on page 5.

Chapter 2. Establishing the security environment

For a key management on the host cryptographic coprocessors using smart cards, you first need to enable the TKE smart card support and establish the connection between the applicable host and the TKE workstation. Also, use the **Setup Module Policy** wizard to create required authorities and assign signature keys and roles to them.

Complete these one-time tasks before you can use the secure Trusted Key Entry features for key management:

- "Enabling the TKE smart card support" on page 5
- "Creating and connecting a host " on page 11
- "Creating the required roles and authorities" on page 15

Enabling the TKE smart card support

For the scenario described in this document, an enabled smart card environment is required. You can use a wizard to create and initialize the smart cards required for setting up this environment.

Zone concepts

Smart-card support for a TKE environment is designed around the concept of a zone to ensure the secure transfer of key parts between the members of the zone. A zone is created with a zone ID when you use the **Smart Card Utility Program** (SCUP) to create a CA smart card. In other words, a zone is defined by a CA smart card.

In the described scenario, these zone members can communicate with each other:

- a certificate authority (CA) smart card
- a Trusted Key Entry workstation (TKE) that was enrolled in a zone using the CA smart card
- four TKE smart cards, two for the module administrators and two for the key administrators. All TKE
 smart cards are created using the CA smart card.

Within a zone, you use the CA smart card when you create the required TKE smart cards. The TKE workstation must be enrolled in the same zone as the TKE smart cards.

Smart card support provides the ability to manage master key parts. The enrolled TKE smart cards are used to create and store key parts, or to load the key parts onto the cryptographic coprocessor. In addition, the smart cards can contain a key that is used to sign the load commands.

A CA smart card is protected by two 6-digit PINs. TKE smart cards are secured by one 6-digit PIN. In your environment, you can distinguish between a CA administrator (owning the CA smart card), the module administrators managing access to the domains of a cryptographic adapter, and the key administrators owning the TKE smart cards for key generation.

Initialize a CA smart card and TKE smart cards

A certificate authority (CA) smart card is an entity that establishes a zone using the **Smart Card Utility Program** (SCUP). A CA smart card is protected by two 6-digit PINs. This CA smart card is required to create and initialize TKE smart cards. Use the **TKE Smart Card Wizard** to accomplish the initialization of both card types.

Before you begin

In a real live production environment, this task must be performed in common by all involved administrators.

About this task

You employ a CA smart card to create TKE smart cards. You then use TKE smart cards on which you generate the roles for administrating the cryptographic adapters and the keys.

Procedure

1. On the TKE console in Figure 4 on page 6, open the **Smart Card Utility Program**.

IBM Trusted Key Entry Co	nsole	
🗖 Welcome	Trusted Key Entry (TKE Version)	
Pi Trusted Key Entry 료 Service Management	Applications Begin Zone Remote Enroll Process for a Crypto Adapter Crypto Adapter Cryptographic Node Management Utility 6.1 Cryptographic Node Management Utility 6.1 Cryptographic Node Module Public Configuration Data Configuration Migration Tasks Smart Card Utility Program 9.1 Crusted Key Entry 9.1 Crusted	Used to begin the zone remote enroll process for a Crypto Adapter Used to complete the zone remote enroll process for a Crypto Adapter Used to manage a Crypto Adapter Used to manage a Crypto Adapter Used to save and migrate public configuration data on a Crypto Adapter Used to save and migrate full configuration data on a Crypto Adapter Used to initialize Smart Cards Used to securely manage leys on a z/OS Host ram 9.1 - Click to launch Used to manage available files in all data directories Used to query TKE Workstation code information
	TKE Security Policy Guidance	Used to provide recommendations for TKE Workstation and Host Crypto Module management security policies

Figure 4. TKE Console - starting the Smart Card Utility Program

2. Log on to the local cryptographic adapter of the TKE workstation.

You must sign on with a profile that is on the associated cryptographic coprocessor. Therefore, depending on how you have initialized your environment, the **Crypto Adapter Logon** window is displayed with profile IDs that represent a single or group passphrase logon. The individual or group profile you choose must have enough authority to do the functions that need to be performed. In this scenario, use the TKEADM profile to be allowed to initialize a CA smart card and to enroll the TKE workstation. The TKEADM profile is a system-supplied role and profile which is created when the cryptographic adapter on the TKE is initialized. It is intended for a person with the responsibility of initially setting up a TKE, completing migration tasks, or managing the TKE.

	Crypto Adapter Lo	gon		×
	Profiles suitable for	logon		
Profile ID	Profile type	Role		
TKEADM	Passphrase	TKEADM		-
TKEUSER	Passphrase	TKEUSER		
				•
4			•	
	Ok Cance	el		

Figure 5. Select the TKEADM profile

After entering the correct passphrase, the **Smart Card Utility Program** opens. Start the **TKE Smart Card Wizard** from the **File** drop-down menu as shown in <u>Figure 6 on page 7</u>.

		TKE Sma	rt Card Utility Pr	ogram \	/ersion 9.1 ·	- Smart Card Reader	s _[$\exists \times$
File CA Sma	rt Card TKE Sn	nart Card	EP11 Smart Card	Crypto	Adapter			Help
Display smar Display smar TKE Zone Wi TKE Smart Ca Exit	t card informat t card key ider zard ard Wizard	tion htifiers			Zone er Zone ID Zone de Zone ke	nroll status: :: escription: ev type:		
Exit and Logo Authority Crypto Ad Key parts:	off or Administrati apter Logon ke	or key: ey:			Alterna Alterna Alterna Alterna	te zone enroll status: te zone ID: te zone description: te zone key type:		
Key type	Description	Origin	MDC-4 or CMAC	SHA-1	ENC-ZERO	AES-VP or HMAC-VP	Length	•

Figure 6. Invoke the TKE Smart Card Wizard

On the welcome panel, read the information, then press **Next**.

3. On the upcoming window, you select the required CA and TKE smart card types as shown in the **TKE Smart Card Wizard** in Figure 7 on page 7. Then press the **Next** button and let the wizard guide you through the creation and initialization of one CA smart card and four TKE smart cards as required for the scenario.

TKE Smart Card Wizard
Select which smart cards you would like created:
Certificate Authority (CA) smart cards
TKE smart cards for managing the TKE workstation
TKE smart cards for managing CCA host crypto modules running in normal mode
 The Authority Keys that will be placed on these smart cards can only be used for signing CCA normal mode commands
TKE smart cards for managing CCA host crypto domains running in imprint and PCI-compliant mode
 The Authority Keys that will be placed on these smart cards can only be used for signing CCA imprint or PCI-compliant mode commands
EP11 smart cards for managing EP11 crypto modules
NOTE: It is assumed you are creating these smart cards in the same zone. Make sure you keep the initial CA smart card in until you are done creating all the selected choices in the zone.

Figure 7. Select smart card types to be created

In an environment where a zone is already defined by a CA smart card, you only need to select the TKE smart cards and you can continue with step "9" on page 8.

4. Press **OK** on the information message that appears.

When prompted, insert a new smart card to be initialized and personalized as a CA smart card into smart card reader 1. Then press **OK**. An information is displayed that the smart card is being initialized. Press **OK** again.

If your smart card is not new, you get a warning that all data will be overwritten (not shown here). Press **Cancel**, if you want to keep the card unchanged and insert a new smart card.

5. You are prompted to enter two six-digit PINs. Each PIN must be entered twice.

6. Enter a zone description and a description for the CA smart card.

For our scenario, enter *testlinux* as the zone description.



Figure 8. Enter a zone description

The CA smart card is initialized and personalized.

Press **OK** to confirm the successful creation. Optionally, you can make a backup of the CA smart card.

7. Press **Yes** on the **Enroll TKE crypto adapter** dialog in Figure 9 on page 8. With this action, you enroll the crypto adapter installed on the TKE workstation, in the *testlinux* zone.

Enroll TKE crypto	adapter 🛛 🔀
Would you like to use the CA smart card to TKE zone?	enroll the TKE crypto adapter in a

Figure 9. Enrolling the TKE crypto adapter in the testlinux zone

8. Enroll a locally installed cryptographic adapter.

	Enroll Crypto Adapter 🛛 📈
Do you want to enroll a workstation) or remote	n IBM Crypto Adapter that is local (installed in this (installed in another workstation)?
Local	
○ Remote	
	OK Cancel

Figure 10. Enroll a locally installed cryptographic adapter

Pressing **OK** to confirm your selection displays information about the successful enrollment of the cryptographic adapter. The wizard now starts the creation of the TKE smart cards.

9. Create four TKE smart cards, two for module adminivstration, and two for key administration.

TKE Smart Card Wizard
You are about to create TKE smart cards that will be used when managing CCA host crypto modules running in normal mode.
Cancel

Figure 11. Creating TKE smart cards

After pressing **OK**, the wizard offers you four available TKE smart card types. The first one is for role **MAIss (Module Admin Issue)**:

	Initialize TKE smart cards
?	Do you want to initialize and personalize a MAIss (Module Admin Issue) smart card?
	Yes Skip Cancel

Figure 12. Creating the MAIss (Module Admin Issue) smart card

Pressing **YES** prompts you to insert the first of the four required smart cards into reader 2 (not shown here). After inserting the smart card into the reader, you are informed about building the TKE smart card for this role.

In a scenario where a CA smart card is already available, and you start with the creation of the TKE smart cards, you are at first prompted to insert this CA smart card into reader 1 and enter the two PINs. Then you are prompted to insert the first TKE smart card into reader 2. Finally, you are informed about the building process.



Figure 13. Process information

The first module administrator now must enter a PIN twice to protect the new smart card.



Figure 14. Personalize a TKE smart card

The TKE Smart Card Wizard now creates the smart card for the MAIss role.



Figure 15. Personalizing the MAIss smart card

Press **OK**. The wizard now asks whether you want to create a smart card for the **MACos** (Module Admin Cosign) role. Answer by pressing **Yes** to let the second module administrator create the second smart card with role **MACos** in the same way.

The onwner of the **MAIss** authority may issue module administration commands, which must be cosigned by the owner of the **MACos** authority.

After creating these two smart card types for module administrating, the wizard asks you for the number of key administrators. For the scenario described here, select **2** to distribute the key parts on two smart cards owned by two key administrators.



Figure 16. Distribute the key parts on two smart cards

10. Initialize two TKE smart cards to be owned by the two key administrators.

The two roles for the key administrators are called **CCAFst** (CCA First Key Admin) and **CCAMl1** (CCA Middle/Last Key Admin 1).



Figure 17. Initialize CCAFst smart card

The process of creating the **CCAFst** and **CCAMl1** smart cards is the same as described for **MAIss** in step <u>"9" on page 8</u>.

After a successful personalization of all four smart cards, the wizard offers you to create another set of TKE smart cards, for example for backup. Select **No** in our scenario.

Results

After completion, you get information that the TKE smart cards have been successfully created. These cards are now ready to accept role and authority information and a signature key.

	TKE Smart Card Wizard 🛛 🛛 🔀
?	The following smart cards were created and enrolled in the TKE zone testlinux (5BC59D9A):
	- MAIss (Module Admin Issue) (904486FCS) - MACos (Module Admin Cosign) (C88E71E8S) - CCAFst (CCA First Key Admin) (F033E267S) - CCAMI1 (CCA Middle/Last Key Admin 1) (3B1F266AS)
	NOTE: Smart card descriptions will appear more than once if you created multiple sets of smart cards.
	Ok

Figure 18. Overview of enrolled smart cards

You can exit the **Smart Card Utility Program** (SCUP) now.

Creating and connecting a host

You need to define and connect the Linux on Z host system to the Trusted Key Entry program (TKE). Then you can create master keys on any attached cryptographic adapters and use them for cryptographic operations.

Before you begin

Defining the host is a one time task. Check the **Host ID** list of the dialog shown in Figure 20 on page 12, whether the host is already available. In our scenario, this list is empty, which may not be the case in a real environment. If your host is already defined to the TKE, you can continue with step <u>"5" on page 12</u>. Else, start at the beginning of the procedure.

Ensure the following:

- The host to which you want to connect the TKE must be an up and running Linux on Z instance with an attached CCA cryptographic coprocessor.
- The catcher.exe TKE daemon, listening to port 50003, is started on this host.

Procedure

- 1. Invoke the **Trusted Key Entry** program from the **Trusted Key Entry Console** in Figure 3 on page 4. This initial window provides access to applications and utilities available on the TKE workstation.
- 2. In the list of applications, click on Trusted Key Entry.

Similar as described in step <u>"2" on page 6</u> of <u>"Initialize a CA smart card and TKE smart cards" on page 5</u>, whenever you launch a TKE application or utility, you must sign on with a profile that has enough authority to do the functions that are performed by the selected application or utility. The steps described here use the system-provided default TKEUSER user profile.

Crypto Adapter Logon						
Profiles suitable for logon						
Profile ID	Profile type	Role				
TKEUSER	Passphrase	TKEUSER	•			
•			•			
	Ok Cancel	Help				

Figure 19. Crypto Adapter Logon

3. Select the TKEUSER profile (or an existing profile of your choice) and click **OK**.

In the subsequent **Passphrase Logon** dialog, log-on with the passphrase associated with the TKEUSER profile. A window is displayed (Figure 20 on page 12) that normally shows a list of the host systems defined to the Trusted Key Entry workstation.

-	Trusted Key Entry	- Smart Card Re	aders Available			
<u>Function</u> <u>Utilities</u> <u>Prefe</u>	rences <u>H</u> elp					
Hosts		Crypto Mod	ules	<i></i>		
Host ID	Description	Host ID	CM index	Status	Description	
Create Host Change Host Delete Host Open Host Close Host						
Domain Groups	_					=
Group ID	Description					
					<u>H</u> elp)
			Signature k	ey NOT loade	d	

Figure 20. Host systems defined to the Trusted Key Entry

4. To define a new host to the TKE, open the context menu for hosts (Figure 20 on page 12), and select the **Create Host** action. The **Create New Host** dialog opens.

	Create New Host 🛛 🛛 🔀
Host <u>I</u> D Host <u>d</u> escription Host <u>N</u> ame / IP <u>P</u> ort number	S70TEST01 CCA crypto cards on S70TEST01 10.10.0.22 50003
<u>O</u> K <u>C</u> ancel	Help Trusted Key Entry

Figure 21. Create a new host

Enter the values of the host to which your cryptographic coprocessor is connected. Input for all entry fields is required, except for an optional host description. It is assumed that this host is a Linux instance on an IBM Z system running the catcher.exe TKE daemon, listening to port 50003. After pressing **OK**, the new host is visible within the list of **Host ID**s (Figure 22 on page 13) and the TKE is connected with all detected cryptographic coprocessors attached to this host.

5. Open the new or applicable host and select the attached cryptographic coprocessor on which you want to set the master key on one of its domains.

From the host's context menu select action **Open Host**.

	Trusted Key Entry - Sn	nart Card Reade	rs Available		
Eunction Utilities Preference	es <u>H</u> elp				
Hosts		Crypto Modules	1		
Host ID	Description	Host ID	CM index	Status	Description
S70TEST01 Create Host Delete Host Open Host Close Host Close Host Group ID	Description				▲ ■ ■
			Signature ke	y NOT loaded	

Figure 22. Open the host

a) Log on to the selected host with the appropriate credentials.

L	.og on to Host 🛛 📈
Host ID Host description Host <u>u</u> ser ID	S70TEST01 CCA crypto cards on S70TEST01 bbsh
<u>P</u> assword	Enable Mixed Case Passwords
<u>O</u> K <u>C</u> ance	<u>H</u> elp

Figure 23. Log on to the host

b) If applicable, the TKE now requests a verification of any new detected cryptographic coprocessor. Check the displayed information.

	Authenticate crypto module 🛛 📈					
?	A new crypto module has been installed in index 6C05					
	Before accepting this Crypto Coprocessor crypto module you should verify that the Crypto module ID is identical to the value supplied to you.					
	Crypto module type : Crypto Coprocessor					
	Crypto module ID : YH10DV731308					
	Crypto module Part Number : 01KV353					
	Description : CCA_SEG3_EPOCH_ECC_SIGNATURE_KEY_FOR_DV731308					
	Root Subject Key Identifier (SKI): 5F471748					
	Do you accept the crypto module?					

Figure 24. Authenticate crypto module

Press the Yes button to continue if you see information about the expected coprocessor.

The **Crypto Modules** view of Figure 25 on page 14 now displays the available adapters. In our scenario, three adapters in CCA coprocessor mode are available on the current host, one CEX6C module and two CEX5C modules.

c) Open the cryptographic coprocessor.

Select a cryptographic coprocessor of your choice and trigger action **Open Crypto Module** from its context menu.

	Trusted Key Entry - S	Sma	art,Card Readers	Available				
Eunction Utilities Preference	es <u>H</u> elp							
Hosts			Crypto Modules					
Host ID	Description		Host ID	CM in	dex	Status	Description	
S70TEST01	CCA crypto cards on S70TEST01		S70TEST01	5C01		Authenticated	intentionally left	🔺
			S70TEST01	5C02		Authenticated	intentionally left	
		=	S70TEST01	6005		Authenticated	intentionally left	
					Open	Crypto Module		
		•					`	
Domain Groups								=
Group ID	Description							
· · ·		-						
		•						•
							Ц	elp
				Sign	ature k	key NOT loaded		

Figure 25. List of crypto modules

The **Crypto Module Administration** dialog for the selected cryptographic adapter opens (see Figure 26 on page 16).

Results

The attached cryptographic adapter is now ready for communication with the Trusted Key Entry workstation.

What to do next

Depending on your current environment, you now need to define the required roles and authorities for module administration and for loading and setting master keys.

Creating the required roles and authorities

Use the Setup Module Policy wizard to create the proposed suitable roles and authorities.

Before you begin

You need the four initialized TKE smart cards produced as described in <u>"Initialize a CA smart card and TKE smart cards" on page 5</u>. These cards do not yet contain any signature keys. The generation of these signature keys is part of the described procedure.

About this task

An authority is identified to the host cryptographic coprocessor or domain by the *authority index*. Each authority has an associated role that defines which actions the authority can perform, that is, which signed commands the authority can issue or co-sign.

Each authority is furthermore created together which an authority signature key. This signature key is actually a key pair. An authority sends a command (a request to perform an action) to a host cryptographic coprocessor or domain. It signs its commands using the private key of its signature key pair. The host cryptographic coprocessor or domain verifies the signature by using the public key of the same key pair. If the verification is successful, and the requested action is allowed by the associated role, the command can be performed.

This procedure is described for role **CCAFst**. You need to perform the same steps for roles **CCAMl1**, **MAIss**, and **MACos** accordingly.

Procedure

1. In the **Crypto Module Administration** window, press the **Setup Module Policy** button (see Figure 26 on page 16).

Crypto Module Administration. Crypto Module : S70TEST01 / 6C05 - Smart Card Readers Available	
Eunction	
General Details Roles Authorities Domains Co-Sign	
General Crypto Module Information	
Description intentionally left blank	
Host description CCA counts on S70TEST01	
Cryste module index 6C05	
Crypto module type Crypto Coprocessor	
Status Crunto module enabled	
Status crypto inounie enableu	
Send updates Disable Crypto Module Set Clock Setup Module Policy	
	IPDATE MODE

Figure 26. Crypto Module Administration

There are two other paths to invoke the **Setup Module Policy** wizard. From the **Crypto Module Adminstration** window shown in <u>Figure 26 on page 16</u>, you can either select the **Roles** or the **Authorities** tab. In both cases, you then open the context menu from the window's white space and select option **Setup Module Policy**.

The Setup Module Policy welcome window opens.

Setup Module Policy 🔀				
Welcome to the Setup Module Policy Wizard!				
The purpose of this wizard is to create a set of module-wide roles and module-wide authorities for managing the settings on your Host Crypto Module or the Host Crypto Modules in your domain group. The administrators created by this wizard will be able to manage module-wide settings or domain-specific settings of normal-mode domains.				
NOTE: The policies implemented by this wizard require smart cards that you initialize and personalize using the TKE Smart Card Wizard .				
Examine the policy definition and guidance information, or press Next to continue.				
Next Policy Definition and Guidance Cancel				

Figure 27. Setup Module Policy welcome window

Pressing Next invokes an information message that a set of module-specific roles will be created.

Press **OK** to display Figure 28 on page 17.

2. Select the source of the signature key for the roles.

For all crypto module types, a default authority with index 0 is created on the crypto module when it is manufactured or reinitialized. Starting with the CEX6C, a default authority with index 99 is additionally created. The default authority for index 99 uses a 512-bit Brainpool ECC key. Select **Default key for index 99** for a CEX6C. For prior versions of the coprocessor choose **Default key for index 0**.

	Select Source of Signature Key For Command 🛛 🔀
	Smart card in reader <u>1</u>
	Smart card in reader <u>2</u>
ę.	<u>Binary file</u>
e.	○ Key storage
	Default key for index 0
	Default key for index 99
	Default key for index 100
	Continue Cancel Help
	Trusted Key Entry

Figure 28. Source of the signature key

Then, in Figure 29 on page 17, select the authority index which is associated with INITADM's signature key and the INITADM role. In the scenario, the authority index 99 is associated with the default signature key for index 99.

Specify authority index	\times
Enter the authority index to be used with the default signature key.	:
Authority index to be used 99	
Continue Cancel Help	
Trusted Key	Entry

Figure 29. Specify authority index for the signature key

Press the **Continue** button in Figure 29 on page 17. On the succeeding confirmation message, press **OK** to display Figure 30 on page 18.



Figure 30. Roles created

3. Let the wizard continue to create the required authorities.

Press the **Next** button as shown in Figure 31 on page 18.

S	etup Module Policy	\sim
Module specific a	uthorities will now be	created.
Next	Policy Definition and Guidance	Cancel

Figure 31. Starting to create authorities

Insert the TKE smart card that you created with role **CCAFst** into smart card reader 2.





Press OK. The wizard confirms that the smart card is new without a signature key on it.

	Message
i	A new authority signature key will now be generated for you.
	ОК

Figure 33. Generating an authority signature key

Confirm with **OK**. On the **Select Key Type** dialog (Figure 34 on page 19) specify your desired key type for the signature key to be generated. For the scenario, a **320-bit EC key** is used.

Select Key Type	\times					
<u>1024-bit RSA key (Deprecated)</u> 2048-bit RSA key						
 <u>2</u>048-bit RSA key <u>3</u>20-bit EC key 						
Continue <u>C</u> ancel <u>H</u> elp						
Trusted Key En	try					

Figure 34. Select signature key type

When prompted, enter the PIN on the smart card. Then the wizard notifies you about the successful creation of the signature key.



Figure 35. Signature key successfully stored

4. Press **OK** on the notification about the generated signature key.

You get a message about the successful creation of the authority. The wizard creates the following authorities:

Authority 10 with role **MAIss** Authority 11 with role **MACos** Authority 20 with role **CCAFst** Authority 21 with role **CCAMI**



Figure 36. Authority successfully created

5. Press **OK** on the message and continue to create the next required authority, until you finished to handle all four role/authority combinations (profiles).

Create another authority						
Do you want to create another profile? Choosing No will advance you to the next task in the wizard.						
Yes						

Figure 37. Create another authority

Press **Yes** and then insert the next TKE smart card in reader 2 to create the authority for the next role. Again, select type **320-bit EC key**. After a successful creation of all authorities by all involved administrators, a completion notice is shown (Figure 38 on page 20).

	Setup Module Specific Authorities 🛛 📈
i	Creation of module specific authorities has completed.
	Authorities that were created:
	10 - MAIss (Module Admin Issue)
	11 - MACos (Module Admin Cosign)
	20 - CCAFst (CCA First Key Admin)
	21 - CCAMI1 (CCA Middle/Last Key Admin 1)
	OK

Figure 38. Authority and role completion notice

Press **OK**.

6. Limit the INITADM authority.

Now that you created all required profiles for your security environment, you must remove all authority from the default INITADM role.

	Setup Module Specific Authorities 🛛 📈
i	Would you like to limit authority that INITADM has?
	Yes No

Figure 39. Limit the INITADM authority

Pressing **Yes** displays a message about the successful command execution. Press **OK** on subsequent information dialogs until the wizard returns to the **Crypto Module Administration** dialog.

7. If required, change the roles **CCAFst** and **CCAMI** to include the privilege for activating the new master key. This is shown for **CCAFst**. This step is not applicable for roles **MAIss** and **MACos**.

In Figure 40 on page 21, select **Change Role** from the context menu of **CCAFst** and check **Set AES master key** as shown in Figure 41 on page 21.

		Eunction								
General Details Roles Authorities Domains Co-Sign										
	0									
	Description									
	CCA First MK Admin									
reate Role	CCA Middle/Last Key									
Change Role	ADM default role									
elete Role	Module Admin Cosign									
iew Role	Module Admin Issue									
uided Create Roles										
atun Madula Baliau										
etup Mouule Policy										
	UPDATE MODE									
	rities Domains C reate Role hange Role elete Role ew Role uided Create Roles etup Module Policy	rities Domains Co-Sign								

Figure 40. Changing the roles

Change Role	\times
Role ID CCAFst	
]
Ŷ ✓ Role Access Control Points	
🗠 🔲 Crypto Module Enable	
- Set clock	
🗠 🔲 Access Control	=
🗠 🔽 AES Master Key	
🗢 📝 ECC (APKA) Master Key	
🗢 📝 DES Master Key	-
🗠 🔽 RSA Master Key	
🕈 🗹 Set Master Key	
🚽 🗹 Set AES master key	
🚽 🔲 Set ECC (APKA) master key	
- 🔲 Set DES master key	
📃 📃 Set RSA master key	•
1	•
Send updates Cancel Help	
	Trusted Key Entry

Figure 41. Including Set AES master key for role CCAFst

This action requires a signature key and sufficient authority. Use the authority of the **MAIss** role for issuing the role change and use the **MACos** role for co-signing the command. The wizard guides you through this procedure with adequate prompts.

8. Verify your created roles by selecting the appropriate tab as shown in Figure 42 on page 22.

To verify the privileges allowed for role **CCAFst**, select this role from Figure 42 on page 22, and invoke **View Role** from its context menu to see the result shown in Figure 43 on page 22.

Crypto	Module Administration. C	rypto Module : S70TEST01 / 6C05 - Smart Card Readers Available 📃 📕	$\exists \times$
Eunction			
General Details	Roles Authorities Domain	s Co-Sign	
Roles		a	
	Role ID	Description	7
CCAFst		CCA First MK Admin	•
CCAMI	Create Role	CCA Middle/Last Key	
INITADM	Change Role	ADM default role	1
MACos	Delete Bole	Module Admin Cosign	
MAIss	View Role	Module Admin Issue	*
	Guided Create Roles		
<u>H</u> elp	Setup Module Policy		
		UPDATE MODE	

Figure 42. View roles

	View Role	X
Role ID	CCAFst	
Description	CCA First MK Admin	
•		
Ŷ ₽ Ro	le Access Control Points	A
- D	Crypto Module Enable	
	Set clock	
~ []	Access Control	
♀ 🔽	AES Master Key	=
	🗹 Load new first key part 🛛 🔫 🛶 🛶	
	Combine new middle key parts	
_	Combine new final key part	
	🖉 Clear new master key register 🔫 🗕 🗕	
	Clear old master key register	
- 1	ECC (APKA) Master Key	
~ ₽	DES Master Key	
~ ₽	RSA Master Key	
۲ 🖌	Set Master Key	
	🗹 Set AES master key	
	Set ECC (APKA) master key	
•		•
<u>0</u> K <u>H</u>	elp	
		Trusted Key Entry

Figure 43. View privileges for role CCAFst

For the **CCAMI** role, you can view the privileges in Figure 44 on page 23.



Figure 44. View privileges for role CCAMI

Results

After you completed this procedure for all required roles (**CCAFst**, **CCAMl**, **MAIss**, and **MACos**), your security environment is readily set up. The key administrators owning the pertaining smart cards can now commonly start to generate and load the key parts and activate the new master key to be used as the current master key as described in "Activating the master key" on page 33.

24 Linux on Z and LinuxONE: How to set an AES master key

Chapter 3. Setting an AES master key on a CCA coprocessor

After completing the setup of the smart card environment, you can create an AES master key on an attached cryptographic coprocessor running in CCA coprocessor mode.

In contrast to the one-time tasks described in <u>Chapter 2</u>, "Establishing the security environment," on page 5, a master key change may occur multiple times, depending on your security policies. Therefore, all sub-tasks of this topic must be performed each time a master key change is necessary.

Let two key administrators generate two parts of the master key on two separate smart cards (**CCAFst** and **CCAMl1** smart cards). Both users are authorized to create master key parts on a smart card and to load them onto the host coprocessor. The administrator with role **CCAMl1** is additionally authorized to combine the loaded key parts to create the final master key on the cryptographic adapter. Both users are allowed to activate a loaded master key.

Generating key parts

In the scenario, this task must be performed sequentially by both key administrators using their different smart cards.

About this task

This task must be performed by the involved key administrators holding the pertaining smart cards where to independently store the key parts.

Procedure

1. In the Trusted Key Entry application, open the host and the desired cryptographic coprocessor (actions **Open Host** and **Open Crypto Module**) to reach the **Crypto Module Administration** dialog. Then select the domain where to set the AES master key.

Click on the **Domains** tab and then click on your domain on the right side (Figure 45 on page 25). In this document, the domain with index 26 is used on the attached coprocessor. Domains are assigned during LPAR definition on the support element (SE).

When clicking on index 26, the window for domain 26 opens as shown in Figure 46 on page 26.

	Crypto Module Administration. Crypto Module : S70TEST01 / 6C05 - Smart Card Readers Available	
<u>F</u> ur	nction	
Ge	eneral Details Roles Authorities Domains Co-Sign	-
D	omains	Index 26
	Domain Index Description	
26	<u>}</u>	

Figure 45. Domain selection for setting the master key

2. Press the **Keys** button at the lower edge of the dialog from Figure 46 on page 26.

Crypto Module Administration. Crypto Module : S70TEST01 / 6C05 - Smart Card Readers Available	
Eunction	
General Details Roles Authorities Domains Co-Sign	
Domain General	Index 26
Domain Index 26	
Description	
Default Key Wrapping Methods	
External Formatted Tokens Enhanced Method	
Internal Formatted Tokens Enhanced Method	
Domain Mode The domain is in NORMAL mode.	
Zeroize domain Send updates Discard changes Enter imprint mode Help	
General Keys Controls-Desc Controls-ACP Dec Tables PINs Certificates	
UPDATE MODE	

Figure 46. Setting master key on selected domain

The window shown in Figure 47 on page 27 opens. In this scenario, you generate two key parts for an AES master key:

- Key part 1 is generated by the key administrator who owns the TKE smart card for role **CCAFst** with authority 20.
- Key part 2 is generated by the key administrator who owns the TKE smart card for role **CCAMI1** with authority 21.
- 3. Select the key type **AES Master Key** from Figure 47 on page 27, and from the context menu, select **Generate multiple key parts to... -> Smart card**.

	Crypto	o Module	Administrat	ion. Cryp	to Modul	e : S70TEST01	./6C05 -	- Smar	rt Card Rea	ders Available	9	
<u>Function</u>												
General	Details	Roles	Authorities	Domains	Co-Sign							
												Index
Domain k	(eys											26
			Status	Hash	pattern							
- I	New AES M	laster Key	Empty	00000	00000000	000						
	OID AES M	laster Key laster Key	Empty Not valid	00000	00000000	000						
	Iow DES M	actor Ko	Empty	00000	00000000		00000					
	Old DES M	aster Key	Empty	00000	00000000	000000000000000000000000000000000000000	000000					
	DES M	laster Key	Not valid	00000	00000000	000000000000000000000000000000000000000	00000					
New EC	C (APKA) M	laster Key	Empty	00000	00000000	000						
EC	с (арка) м с (арка) м	aster Key	Not valid	00000	000000000	000						
	lew RSA M	aster Key	Empty	00000	00000000	000000000000000000000000000000000000000	00000					
	Old RSA M	aster Ke	Empty	00000	00000000	000000000000000000000000000000000000000	00000				•	
	R5A M	laster Key	NOLVAIIU	00000	00000000		00000					
Sel	ect key to	work with	n 📃			Ke	еу Туре					
			Symmetric Ma	aster Keys:							^	
			AES Maste	r Key	Conorat	a cinala kay na	rt	-			=	
			Asymmetric M	laster Kevs:	Generat	e multiple key pa	harts to		nart card			
			ECC (APKA)	Master Key	Generat	e a set of mast	er key part	ts Bi	nary file		-	
					Load sin	ngle key part	71	→ Pr	int file			
<u>H</u> elp					Load all	key parts from.		•				
	-				Load all	new master ke	ys					
General	Keys	Controls-	Desc Contro	ols-ACP D	Clear			•				
					Set, imm	nediate					UPDATE MODE	
					Secure k	key part entry						

Figure 47. Generate multiple key parts on a smart card

- 4. You are now guided through the process by a series of prompts.
 - a) Enter the number of key parts to be generated for the final master key.



Figure 48. Enter the total number of key parts to be generated

b) Press OK on the Generate Key Part message dialog.

Key Part	\times
rt 1 of 2	
Cancel	
	Key Part rt 1 of 2 Cancel

Figure 49. Generate first key part

c) Create the first master key part and place it on the smart card that has the authority signature key for authority 20 (for role **CCAFst**).

Insert this smart card into reader 1.

d) You are now asked if you want to use the same smart card reader for the whole process. Select **No** in Figure 50 on page 28, because in the scenario, you use two different smart card readers.



Figure 50. Use different same smart card readers for the entire process

- e) Then the wizard prompts you to insert the smart card for key part 1 into reader 1 and to enter the smart card PIN.
- f) Enter a key part description.

E	Enter key pa	art descrip	ition 🔀
Description	AES key part	1	
Co <u>n</u> tinue	<u>C</u> ancel	<u>H</u> elp	
			Trusted Key Entry

Figure 51. Enter key part description

Pressing Continue displays a confirmation about the successful creation of the key part.

g) Now the second key administrator is guided through the same dialogs to create key part 2 on his smart card.

Note: Ensure to use smart card reader 2 for the second and third key part.

After pressing **OK** when saving the second key part, the program returns to the **Crypto Module Administration** dialog.

Results

The smart cards now contain the signature key and key parts needed to perform a key load operation. You can verify the generated key parts on the smart cards using the **Smart Card Utility Program** (**File -> Display smart card information**).

Loading key parts

After the generation of the key parts on the smart cards you load them onto the cryptographic coprocessor.

About this task

Both key administrators must load their key part. The process for both differs slightly, so both loading actions are described in this procedure.

Procedure

1. On the **Crypto Module Administration** dialog, in the **Key Type** list select the **AES Master Key** entry. Right click to open its context menu and select **Load all key parts from ... Smart card** as shown in Figure 52 on page 29.

Crypto Module Administration. Crypto Module : S	70TEST01 / 6C05 - Smart Card Readers Available 📃 📃 🔀
<u>F</u> unction	
General Details Roles Authorities Domains Co-Sign	
	Index
Domain Keys	26
Status Hash pattern	
New AES Master Key Empty 000000000000000000000000000000000000	
Old AES Master Key Empty 000000000000000000000000000000000000	
Old DES Master Key Empty 000000000000000000000000000000000000	000000000000000000000000000000000000000
DES Master Key Not valid 0000000000000000	0000000000000
New ECC (APKA) Master Key Empty 0000000000000000	
Old ECC (APKA) Master Key Empty 0000000000000000	
ECC (APKA) Master Key Not valid 000000000000000	
New RSA Master Key Empty 000000000000000000000000000000000000	0000000000000
Old RSA Master Key Empty 000000000000000000000000000000000000	0000000000000
KSA Master Key Nut Valiti 00000000000000000000000000000000000	
Select key to work with	Key Type
Symmetric Master Keys:	
AES Master Key	Caparata single key part
DES Master Key	Generate single key parts to
ECC (APKA) Master Key	Generate a set of master key parts
	Load single key part
	Load all key parts from
Пер	Load all new master keys Binary file
Ganaral Kava Cantrola Daga Controla ACD Dag Tables D	Clear > Keyboard
General Areys Controls-Desc A Controls-ACP A Decitables AP	Set, immediate
	Secure key part entry UPDATE MODE

Figure 52. Load all key parts from smart card

- a) When prompted, enter the number of key parts (2) to be loaded.
- b) When the **New AES Master Key** register is not empty, answer **Yes** to the **Clear Key Register** question (Figure 53 on page 29), because the currently loaded new master key will now be stored in this register.

	Clear Key Register 🛛 🛛 🔀
?	Do you want to clear the key register?
	Yes <u>N</u> o Cancel

Figure 53. Clear the key register

To clear the **New AES Master Key** register, you need a signature key and a certain level of authority. Authority 20 with the role **CCAFst** is allowed to perform this action. So, when prompted, select smart card reader 1 as the source of the signature key and insert the **CCAFst** smart card.

In the message about the successful clearing of the key register, press the **OK** button.

c) Select the first key part by pressing **OK** in the **Load Master Key** dialog as shown in Figure 54 on page 29.

Load Mas	ter Key	\times
Select first key pa	art	
ОК	Cancel	

Figure 54. Select first key part to be loaded

- d) In the upcoming prompt, selecting smart card reader 1 as the source for key part 1 and press the **Continue** button.
- e) In Figure 55 on page 30, select the shown AES key part 1 and press **OK**.

Select key part from smart card						
Card ID F409EB0AS Zone description testlinux Card description CCAFst (CCA First Key Admin)						
Card contents						
Key type	Description	Origin	MDC4 or CMAC	SHA1	ENC-Zero	
ICSF AES master key part AES key part 1 Crypto adapter 64				64A5310C		
OK Cancel Help						
				Tru	isted Key Ent	:ry

Figure 55. Load first key part

Press **OK** to proceed to the **Key part information** dialog (Figure 56 on page 30).

f) Now press the **Load key** button.

	Key part information	\sim
Description	AES key part 1	
AES-VP	C286ECE80954FE86B8FF708CE	F014FC6
	C7C1D7A45395D0D08F37EBE019	965FA28
Key type	New AES Master Key, Firs	st part
	7	
Load <u>k</u> ey	<u>Cancel</u> <u>H</u> elp	
		Trusted Key Estay
		Trusted Key Entry

Figure 56. Key part information

Press \mathbf{OK} in the upcoming confirmation message (Command was executed successfully) to proceed.

2. Select the last (second) key part.

Load Mas	ter Key	\times
Select last key pa	art	
OK	Cancel	

Figure 57. Select last (second) key part

Press **OK** to load the second key part.

If the **CCAFst** administrator now tries to continue, an error message is displayed, because the key administrator with authority 20 may only load the first key part. Now the second key administrator needs to continue to process this step.



Figure 58. Error ...

Press **Retry** to use the smart card with key part 2 owned by the key administrator with authority 21. When prompted, select smart card reader 2 as the source of the required signature key and press **Continue**. Then insert the TKE smart card 2 into reader 2 and enter the password for this smart card. As expected, the wizard offers to use authority index 21 in Figure 59 on page 31.

Specify authority index 🛛 📈				
An authority index is going to be used with Leave the field below unchanged to use the on the smart card, or enter a new index. Authority index to be used 21	the key. e index specified			
Continue Cancel Help				
	Trusted Key Entry			

Figure 59. Specify authority index

Press the **Continue** button and then select smart card reader 2 as the source of the missing master key part to be loaded.

3. Now you can load key part 2, the last key part in our scenario.

You see a view showing information about the AES key part 2 (see Figure 60 on page 32) that you have been previously generated on the inserted smart card.

Select key part from smart card						
Card ID 3B1F266AS Zone description testlinux Card description CCAMI1 (CCA Middle/Last Key Admin 1)						
Card contents						
Key type	Description	Origin	MDC4 or CMAC	SHA1	ENC-Zero	
ICSF AES master key part	AES key part 2	Crypto adapter				9244DC6F
			ı			
OK Cancel He	lp					
				Tru	isted Key Ent	ry

Figure 60. Load key part 2

Now proceed with key part 2 as previously described for key part 1 in Figure 55 on page 30. Press **OK** until you return to Figure 61 on page 32 where you can see that the **New AES Master Key** register is now **Full**.

Crypto Module	Administration.	Crypto Module : S70TEST01 / 6C05 - Smart Card Readers Available	
Eunction			
General Details Roles	Authorities D	omains Co-Sign	
Domain Keys			Index 26
	Status	Hash pattern	
New AES Master Ke	y Full	CECDEDB8B672E59B	
Old AES Master Ke	y Empty	00000000000000	
AES Master Ke	y Not valid	000000000000000000000000000000000000000	
New DES Master Ke	y Empty	000000000000000000000000000000000000000	
DES Master Ke	v Not valid	000000000000000000000000000000000000000	
New ECC (ADKA) Master Ka	. Empty	0000000000000	
Old ECC (APKA) Master Ke	y Empty	000000000000000	
ECC (APKA) Master Ke	y Not valid	00000000000000	
New RSA Master Ke	y Empty	000000000000000000000000000000000000000	
Old RSA Master Ke	y Empty	000000000000000000000000000000000000000	
RSA Master Ke	y Not valid	000000000000000000000000000000000000000	
Select key to work wit	h	Кеу Туре	
	Symmetric Maste	er Keys:	
	AES Master Ke	ay 🔤	
	DES Master Ke	By	-
Help			
Пеф			
General Keys Controls	Desc Controls	ACP Dec Tables PINs Certificates	
		UPDATE MOI	DE

Figure 61. Key parts loaded into New AES Master Key register

Results

Now both key administrators finished loading the complete master key into the **New AES Master Key** register on the cryptographic adapter.

Activating the master key

Finish the AES master key creation by setting the new master key as the current master key. In our scenario, both key administrators are authorized to perform this task.

Before you begin

Most probably, there will be data encrypted by a secure key wrapped by the currently valid master key. Therefore, you should activate a new master key only after ensuring that no data loss will occur. If you maintain a secure key repository, perform this procedure only if the keys in this repository are already reenciphered under the key you want to make current. For Linux, you find information about re-enciphering utilities for a key repository in *Pervasive Encryption for Data Volumes* available at:

https://www.ibm.com/support/knowledgecenter/linuxonibm/com.ibm.linux.z.lxdc/lxdc_linuxonz.html

About this task

For each domain on a cryptographic coprocessor, the TKE maintains three master key registers (see Figure 62 on page 34):

New AES Master Key

This register contains the new master key to be set. While the new master key remains in this register, it cannot be used to generate new secure keys until it is activated as described in this topic. Activation transfers the new master key into the **AES Master Key** register and clears the New AES Master Key register.

Old AES Master Key

This register contains the previously used master key. Secure keys enciphered with the master key contained in the OLD register can still be used until the master key is changed again.

AES Master Key

This register contains the currently valid master key.

Procedure

1. Select **Set, immediate** from the AES Master key pull-down choice as shown in Figure 62 on page 34.

Crypto Module Adm	ninistration. Crypto M	lodule : S70TEST01 / 6C05 - Smart	t Card Readers Available	
Eunction				
General Details Roles Aut	thorities Domains C	o-Sign		
				Index
Domain Keys				26
				· · · · · · · · · · · · · · · · · · ·
Si	itatus Hashipa	ittern		
New AES Master Key Fi	ull CECDED	B8B672E59B		
Old AES Master Key El AES Master Key N	mpty 0000000 Int valid 0000000	000000000		
New DEC Master Key F				
Old DES Master Key El	mpty 0000000	000000000000000000000000000000000000000		
DES Master Key N	lot valid 0000000	000000000000000000000000000000000000000		
New ECC (APKA) Master Key E	mpty 0000000	00000000		
Old ECC (APKA) Master Key E	mpty 0000000	00000000		
ECC (APKA) Master Key N	lot valid 0000000	00000000		
New RSA Master Key El	mpty 0000000	000000000000000000000000000000000000000		
BSA Master Key El	mpty 000000 Int valid 0000000	000000000000000000000000000000000000000		
,,				
Select key to work with		Кеу Туре		
Sy	ymmetric Master Keys:			
	AES Master Key	Caparata cipala kau part		
As	symmetric Master Keys:	Generate multiple key part		
·		Generate a set of master key parts		
Halp		Load single key part		
Пеір		Load all key parts from		
General Keys Controls-Des	Controls-ACP Dec	Load all new master keys		
deneral rega controls-bes	A Controlomer / Dec	Clear 🕨		
		Set, immediate	UPDATE MODE	
		Secure key part entry		

Figure 62. AES master key status: Full

The **Set, immediate** action transfers the master key from the **New AES Master Key** register (CECDE...) to the **AES Master Key** register. This master key will from now on be used to generate a secure key by wrapping the clear key. The **Set, immediate** action also transfers the previous master key from the **AES Master Key** register to the **Old AES Master Key** register.

Important: You can proactively re-encipher existing secure keys with the new master key which is still stored in the **New AES Master Key** register. Such re-enciphered secure keys are not valid until the new master key is activated to become the current master key.

So changing the master key must be coordinated between the persons who change the master key and the persons who own the secure keys, or who own applications that use the secure keys, or who own the data that is encrypted with these secure keys.

If you maintain secure keys in a key repository, or some type of a cryptographic key data set (CKDS), these keys need to be re-enciphered before the new master key is activated. If you implemented the infrastructure for protected volume encryption, using a key repository as described in <u>Pervasive</u> <u>Encryption for Data Volumes</u>, the available utilities support you in a staged re-enciphering of the secure keys in this repository: In a first stage, a secure key is re-enciphered with the key in the **New AES Master Key** register. The re-enciphered key is kept in the repository in a separate file. This ensures that while the new master key has not been set active, the secure keys continue to be valid. Once the new master key has been set active, the secure keys continue to be valid. Once the new master key has been set active, the secure keys in the re-enciphering process replaces the secure key with its re-enciphered version which was previously created during the first stage.

Before you can execute the **Set, immediate** action, you get a warning that informs you about the result of this action.

Warning!				
\wedge	Warning!			
	Under normal circumstances, master keys should be set using ICSF procedures services that coordinate setting the master key with initializing or re-enciphering key storage, or set using the TKE "Coordinated change master keys" function. If you continue with this option, the master key will be set but no action will be taken on the associated key store. This may cause the keys in key storage to become unusable when accessed by ICSF in that domain This operation transfers the current master key to the old-master-key register, transfer the new master key to the current-master-key register, and clears the new-master-key register.			
	If key storage needs to be re-enciphered before the master key is set, you should NOT use this option. Do you want to continue?			
	OK Cancel			

Figure 63. Warning

Important: In our scenario, there is no previous master key in the **Old AES Master Key** register. If this register is not empty in your environment, ensure that you really do no longer need the master key that may be stored in this register, because you will no longer be able to read any data that is encrypted with a secure key created with this old master key. You might consider re-enciphering existing secure keys wrapped by the old master key with the new master key before activating the new master key.

2. If you are sure about your key hierarchy and usage, press the **OK** button at the end of the warning (Figure 63 on page 35).

You can see the result in Figure 64 on page 35. The master key with a hash beginning with CECDED... is now in the **AES Master Key** register with status **Valid**.

Crypto Module Ac	dministration.	Crypto Module : S70TEST01 / 6C05 - Smart Card Readers Available		
Eunction				
General Details Roles Authorities Domains Co-Sign				
Domain Keys			Index 26	
	Status	Hash pattern		
New AES Master Key Ol <mark>d AES Master Key</mark> AES Master Key	Empty Empty Valid	00000000000000 000000000000000 CECDEDB88672E598		
New DES Master Key Old DES Master Key DES Master Key	Empty Empty Not valid	00000000000000000000000000000000000000		
New ECC (APKA) Master Key Old ECC (APKA) Master Key ECC (APKA) Master Key	Empty Empty Not valid	00000000000000 00000000000000 00000000		
New RSA Master Key Old RSA Master Key RSA Master Key	Empty Empty Not valid	00000000000000000000000000000000000000		
Select key to work with		Кеу Туре		
	Symmetric Maste	er Keys:		
	AES Master Ke	ey 📃		
DES Master Key				
Asymmetric Master Keys:				
Help				
General Keys Controls-Desc Controls-ACP Dec Tables PINs Certificates				
		UPDATE MODE		

Figure 64. Checking the new valid AES master key

If applicable, a previously current master key is saved on the cryptographic coprocessor in the **Old AES Master Key** register for recovery actions, as long as you do not overwrite this register by generating a new current AES master key.

Results

Now you have loaded and activated one AES master key on one domain on one cryptographic coprocessor. The Linux on Z instance, where the cryptographic coprocessor is attached can use this master key to generate a secure key for data and volume encryption.

More information

• To learn about security products for Linux on Z and LinuxONE, search for the following terms in your web browser:

IBM Knowledge Center -> Products -> Linux on IBM Systems -> Linux on Z and LinuxONE -> Security

Or you can directly click or enter the following URL directly:

https://www.ibm.com/support/knowledgecenter/de/linuxonibm/liaaf/security.html

• For information on the features and advantages of the infrastructure for protected volume encryption, search for this video in your web browser:

Pervasive encryption for data volumes video

Or you can directly click or enter the following URL directly:

https://youtu.be/jDK3ZwEdX4I

• Documentation on how to establish and exploit the infrastructure for protected volume encryption is provided in the IBM Knowledge Center. Search for the following title in your web browser:

(Linux on Z) Pervasive encryption for data volumes ->

Or you can directly click or enter the following URL directly:

https://www.ibm.com/support/knowledgecenter/linuxonibm/com.ibm.linux.z.lxdc/lxdc_linuxonz.html

Linux on Z and LinuxONE: How to set an AES master key

Accessibility

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Documentation accessibility

The Linux on Z and LinuxONE publications are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when you use the PDF file and want to request a Web-based format for this publication, use the Readers' Comments form in the back of this publication, send an email to eservdoc@de.ibm.com, or write to:

IBM Deutschland Research & Development GmbH Information Development Department 3282 Schoenaicher Strasse 220 71032 Boeblingen Germany

In the request, be sure to include the publication number and title.

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

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility at

www.ibm.com/able

40 Linux on Z and LinuxONE: How to set an AES master key

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.

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

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 is for planning purposes only. The information herein is subject to change before the products described become available.

Trademarks

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

Adobe is either a registered trademark or trademark of Adobe Systems Incorporated in the United States, and/or other countries.

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



SC34-7712-00

