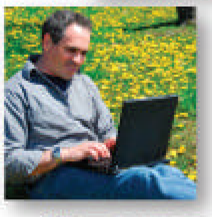
SHARE
Technology · Connections · Results

The ABCs of Trusted Key Entry

Jessica Bonner
IBM

February 25, 2007
Session Number 5544



Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

- IBM*
- Linux
- System z*
- S/390*
- zSeries*
- OS/2*
- Z9*

* Registered trademarks of IBM Corporation

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

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

Objective

- To give an overview of Trusted Key Entry (TKE)
- Discuss TKE’s functions and features
- Explain the master key loading process

Topics

- **Overview of hardware and key parts**
- TKE Introduction
- TKE History
- Features/Functions
- TKE Concepts
- Master & Operational Key Loading
- Linux on System z

Why use TKE?

TKE is the only way to **'SECURELY'** load the master key parts into the Secure Coprocessors on a host.

Cryptographic Coprocessors

Model	Installed Coprocessors	Optional Coprocessors
z900 z800	CCF	PCICC PCICA
z990 z890	None	PCIXCC CEX2C PCICA
z9 EC z9 BC	None	CEX2C CEX2A

Refresher on Master Keys

- Master keys are installed in *domains* in the cryptographic coprocessors.
- 16 physical domains per coprocessor
- Two master keys per domain
  - the symmetric master key used to encrypt the DES and Triple DES keys
  - the asymmetric master key used to encrypt the RSA private keys
- A CKDS and PKDS are bound to the value of the master keys in the coprocessor
- A master key is entered in a coprocessor via either the ICSF ISPF panels or TKE in several parts, splitting the master key secret among several security officers who know only their own part of the master key. There must be at least two parts to a master key.

Key Parts

- Symmetric Key Part – is double length key part
  - 16 hexadecimal digits
  - 012345679ABCDEF 0123456789ABCDEF

- Asymmetric Key Part – is triple length key part
  - 24 hexadecimal digits
  - FEDCBA9876543210 FEDCBA9876543210 FEDCBA9876543210

- 2 or more key parts are Xor'ed together to create a complete key

Topics

- Overview of hardware and key parts
- **TKE Introduction**
- TKE History
- Features/Functions
- TKE Concepts
- Master & Operational Key Loading
- Linux on System z

TKE Introduction

- The feature consists of a workstation, an application on embedded operating system, and 4764 cryptographic card
- Optional - Smart card readers and smart cards.

- Trusted Key Entry (TKE) is an optional feature on zSeries and System z9 processors. One TKE can manage multiple host systems.

- TKE provides a basic key management system that allows authorized personnel a method for key identification, exchange, separation, update, backup and management.

TKE History

Version	Operating System	New Function
TKE 1.0	OS/2	Initial Release
TKE 2.0	OS/2	RSA Key Generation
TKE 2.3	OS/2	Blind Key Entry Support
TKE 3.0	OS/2	PCICC Support
TKE 3.1	OS/2	Access Control Point Support
TKE 4.0	OS/2	PCIXCC support
TKE 4.1	OS/2	Operational Key Entry
TKE 4.2	OS/2	Smart Cards
TKE 5.0	Embedded Operating System	HMC layout
TKE 5.1	Embedded Operating System	Service User

Features

- Secure remote crypto coprocessor key management for both:
  - Master Keys
  - Operational Keys
- Dual control key management
- Secure key part storage (with optional smart card feature)
- Role based access control
- Public key authentication of security officers
- Granular access control points (ACPs)
- Management of multiple coprocessors across multiple z/OS images
- Coprocessor grouping
- Coprocessor domain isolation
- Coprocessor zeroization per domain

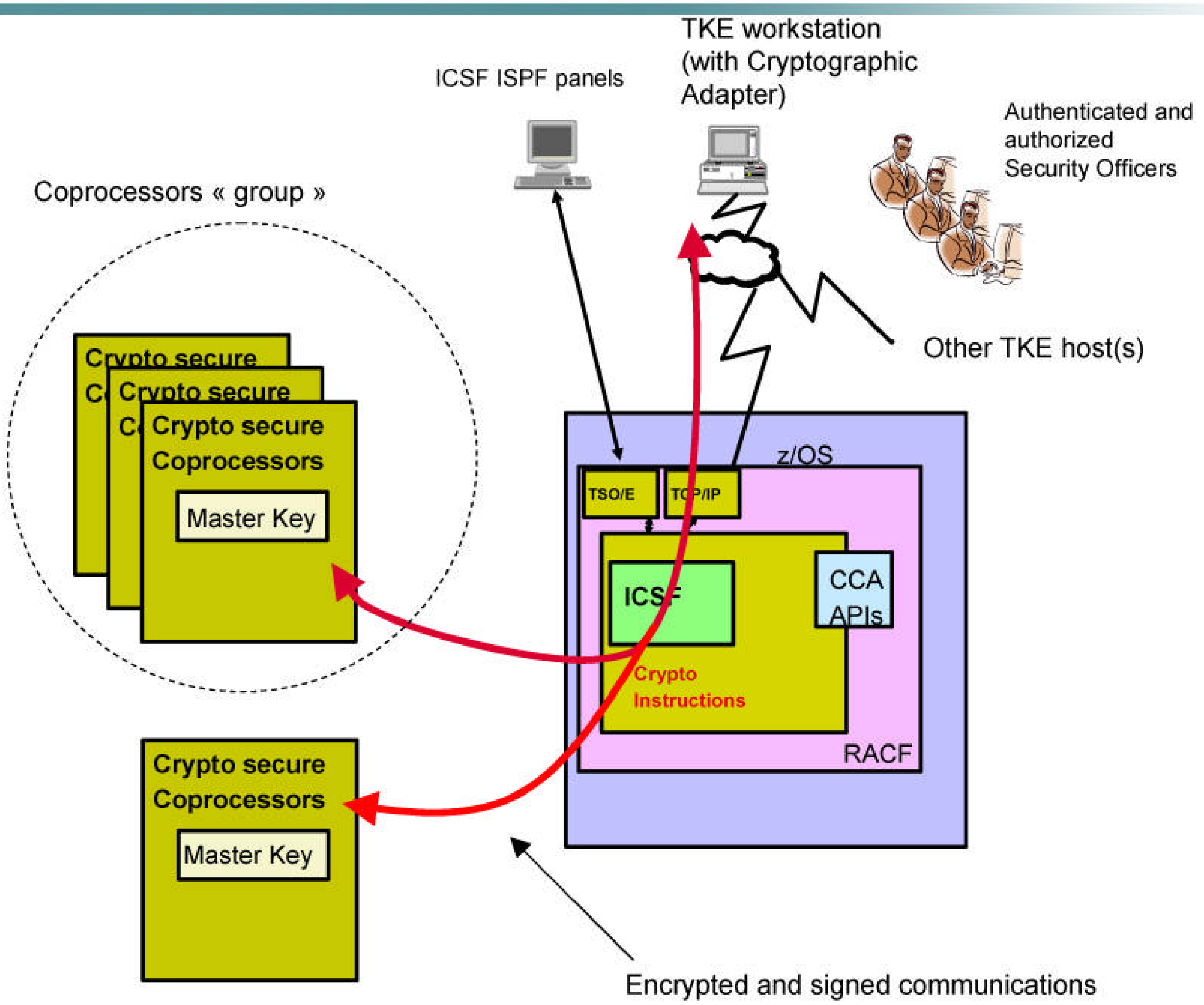
Topics

- Overview of hardware and key parts
- TKE Introduction
- TKE History
- Features/Functions
- TKE Concepts
- Master & Operational Key Loading
- Linux on System z

TKE Concepts

- Overview of components and host interactions
- Smart Cards
- Roles & Authorities
- Access Control Points

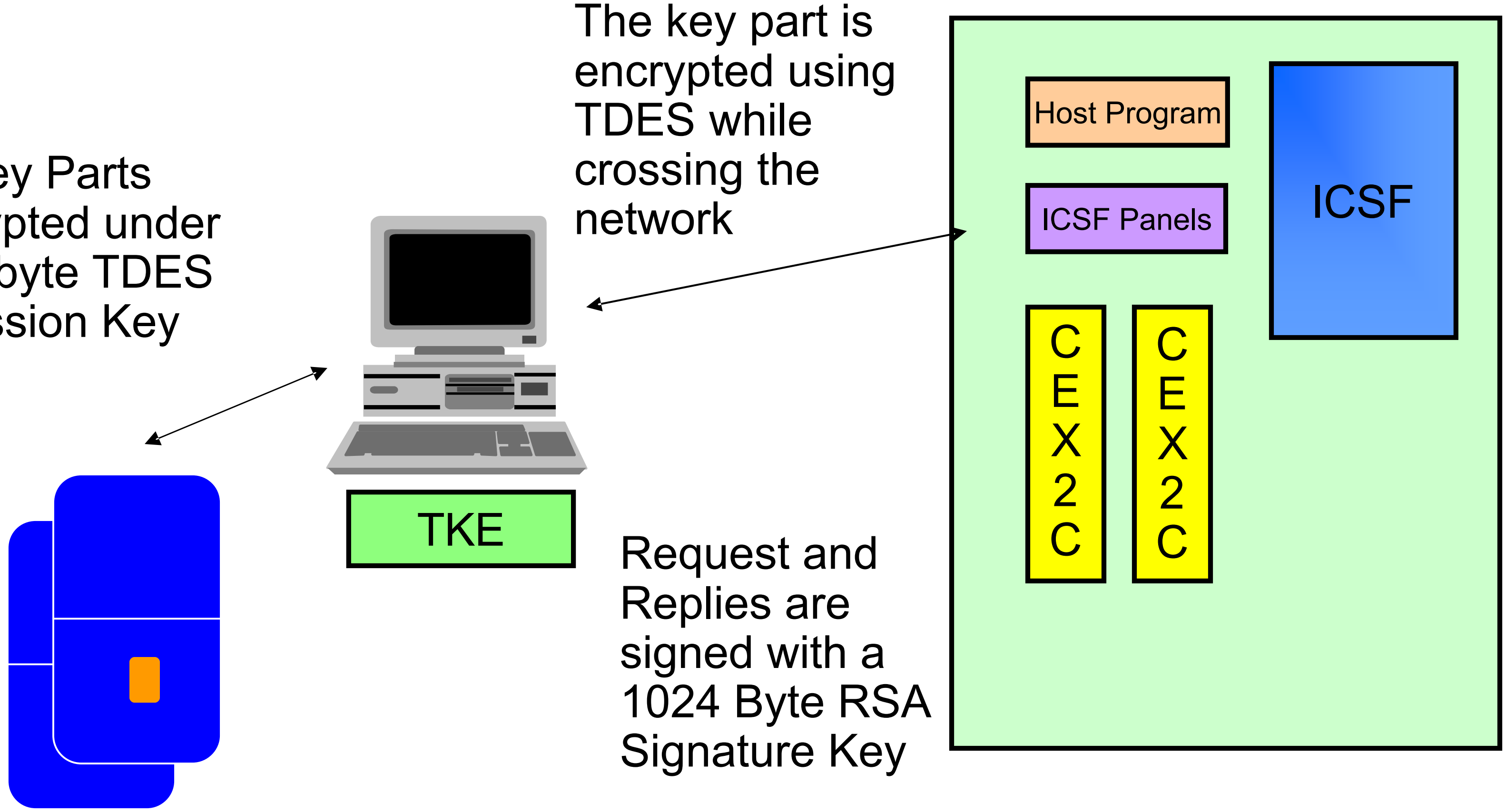
TKE Host Interactions



Integrity

- TKE security consists of separate mechanisms to provide integrity and secrecy
  - Integrity of the crypto module
  - Integrity of the authorities
  - The above integrity mechanisms are used as part of the process to establish secrecy
- Authenticity of the requests and replies from TKE and crypto module are digitally signed
- A sequence number is also added to all signed messages to eliminate the possibilities of replay attacks

Communication Encryption Methods



Key Parts Encrypted under a 24 byte TDES Session Key

The key part is encrypted using TDES while crossing the network

Request and Replies are signed with a 1024 Byte RSA Signature Key

TKE Concepts

- Overview of components and host interactions
- **Smart Cards**
- Roles & Authorities
- Access Control Points

What is a Smart Card?

- A smart card is a pocket-sized card with embedded integrated circuits which can process information

- Data that is stored on the smart card is transferred to the TKE workstation while encrypted under a session key. The key part is loaded to the host encrypted under a Diffie-Hellman transfer key.

- The smart cards are equipped with specialized cryptographic engines that allow to use algorithms, such as RSA

Smart Cards

- Smart card support increases operations security, secret information never leaves the card in the clear
- TKE smart cards can store key parts, signature keys and TKE crypto adapter logon keys
- Secret information on the smart card is protected by a PIN

Smart Cards Terminology

- Zone – A security concept ensuring that only members of the same zone can exchange key parts
- Entity – A member of a zone
  - CA smart card
  - TKE smart card
  - Crypto adapter
- CA smart card - Certificate Authority, establishes a zone, protected by 2 six-digit pins
- TKE smart card – Used for storing RSA logon keys and key parts, protected by a four-digit pin

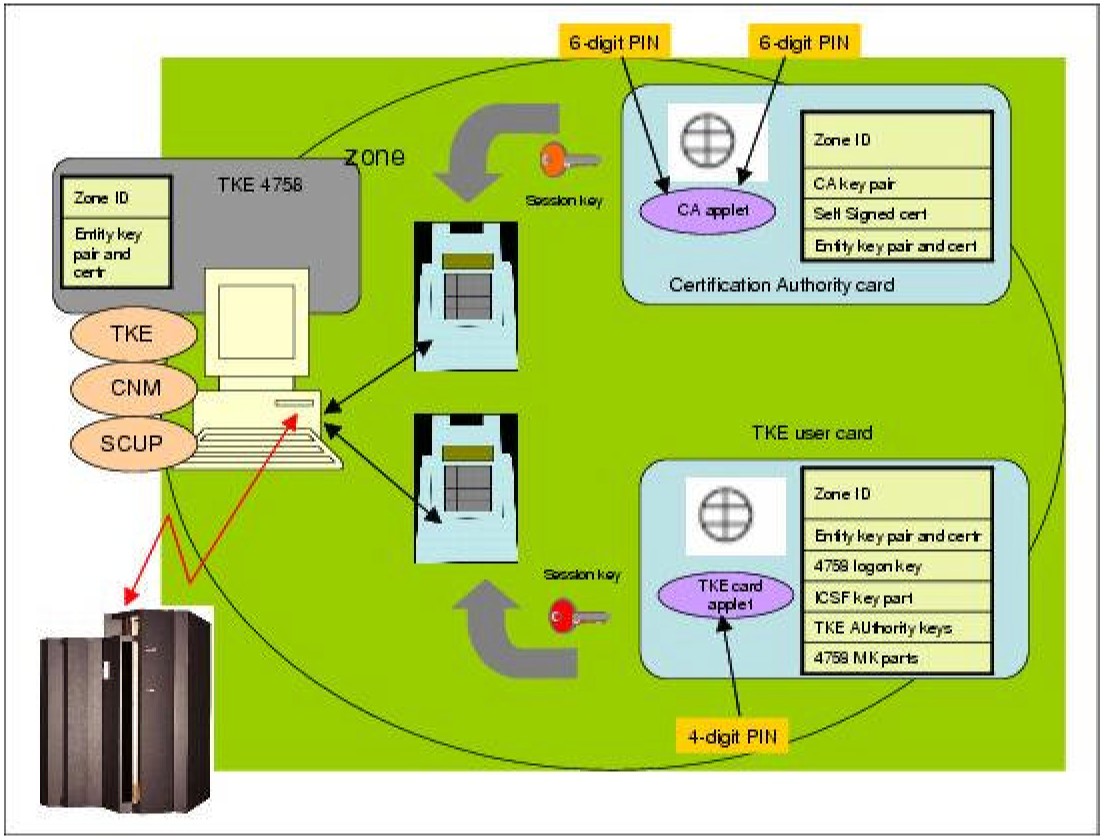
Zone

Why does the zone matter?

- Only entities of the same zone (whose public keys have been certified by the zone CA), can exchange encrypted secrets. In our case:

- This means that being in a different zone then the TKE crypto cannot accept the key parts stored on this smart card that is foreign to the Crypto adapter zone.

Smart Card Communication



TKE Concepts

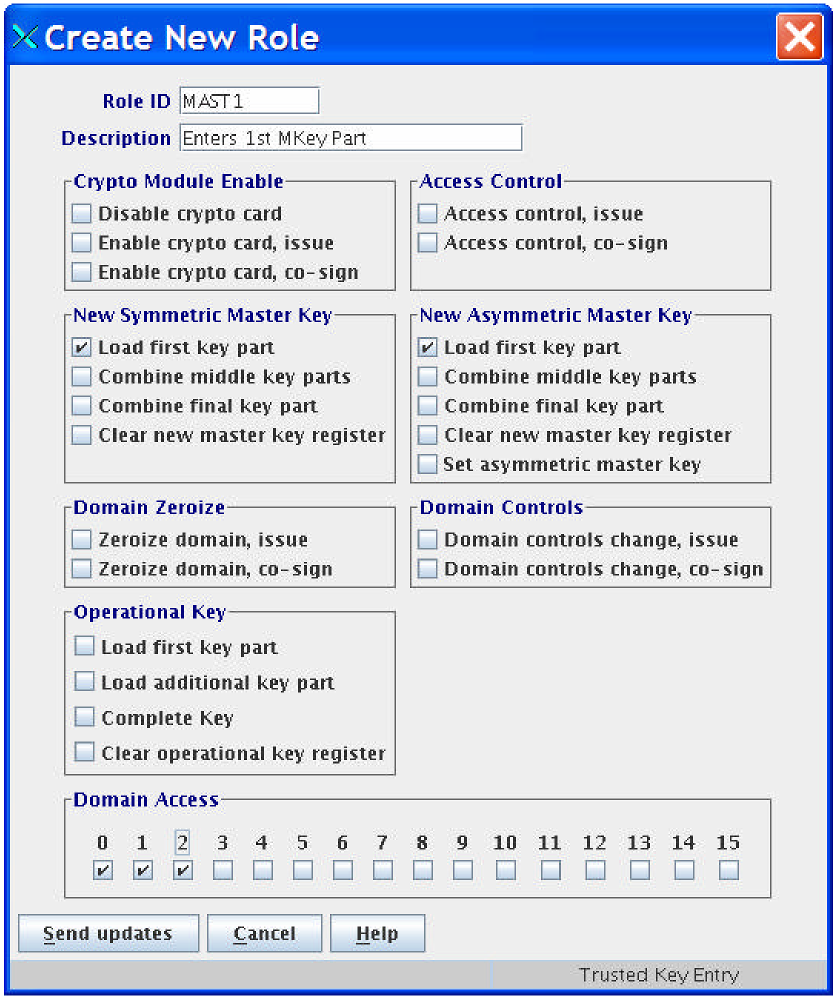
- Overview of components and host interactions
- Smart Cards
- **Roles & Authorities**
- Access Control Points

Role Based Access Control

- TKE controls access to the host crypto coprocessors using roles
  - A role is a set of permissions
  - Permissions are very granular to allow for strict control over the host crypto coprocessor
  - Roles can be reused for different authorities (or people)

- Before creating roles it is a good idea to sit down and think about how you want them defined.
  - How many people will be executing TKE functions?
  - Which functions do would you like to be dual control?

Creating a Role



Create New Role

Role ID: MAST1

Description: Enters 1st MKey Part

Crypto Module Enable
- □ Disable crypto card
- □ Enable crypto card, issue
- □ Enable crypto card, co-sign

Access Control
- □ Access control, issue
- □ Access control, co-sign

New Symmetric Master Key
- ☑ Load first key part
- □ Combine middle key parts
- □ Combine final key part
- □ Clear new master key register

New Asymmetric Master Key
- ☑ Load first key part
- □ Combine middle key parts
- □ Combine final key part
- □ Clear new master key register
- □ Set asymmetric master key

Domain Zeroize
- □ Zeroize domain, issue
- □ Zeroize domain, co-sign

Domain Controls
- □ Domain controls change, issue
- □ Domain controls change, co-sign

Operational Key
- □ Load first key part
- □ Load additional key part
- □ Complete Key
- □ Clear operational key register

Domain Access

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
☑	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□

- Enter the Role ID and Description
- Select the set of permissions this role can perform
- Select the Domains this role can access

Examples of Roles

- ISSUER
  - Disable crypto card
  - Enable crypto card, issue
  - Access control issue
  - Zeroize domain issue
  - Domain control change issue
- Cosign
  - Access control co-sign
  - Enable crypto card co-sign
  - Zeroize domain co-sign
  - Domain control change co-sign
- AddComp
  - Load additional key part
  - Complete Key
- MFirst
  - Symmetric/Asymmetric load first key part
  - Clear new master key register
- MMiddle
  - Symmetric/Asymmetric combine middle key parts
- MLast
  - Symmetric/Asymmetric combine final key part
  - Clear new master key register
- 1stClear
  - Load first key part
  - Clear operational key register

TKE Authority

- An authority is a person who is able to issue signed commands to the host crypto coprocessor
- An authority is identified to the crypto module by the authority index.
- On a PCIXCC/CEX2C there can be up to 100 authorities
- An authority has 3 elements
  - Role
  - Authority Signature Key
  - Personal information
- An authority signs commands by using the secret key of its signature key pair
- The host crypto coprocessor verifies the signature by using the public key of the same RSA key pair.

TKE Concepts

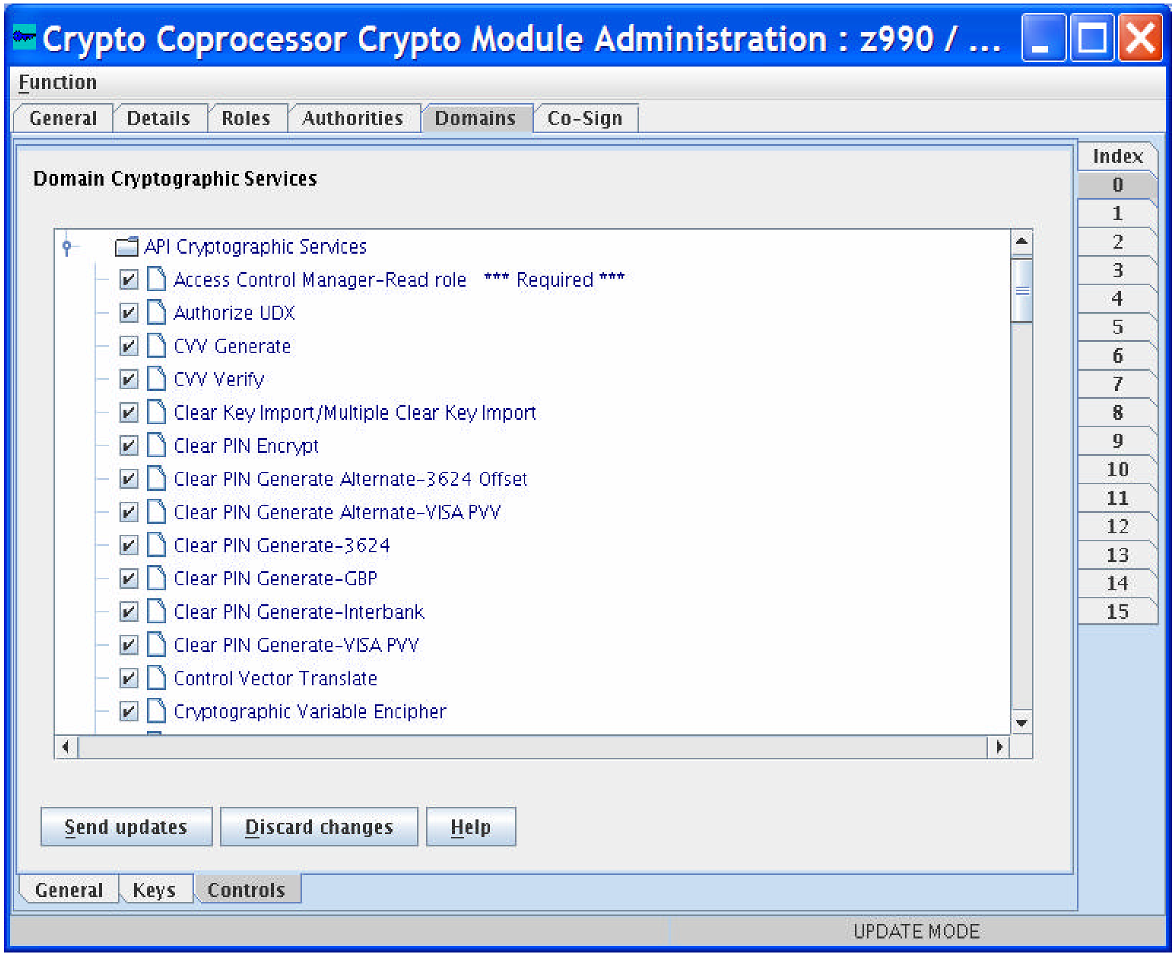
- Overview of components and host interactions
- Smart Cards
- Roles & Authorities
- **Access Control Points**

Access Control Points

- With TKE you are able to administer access control points to ISPF Services, API Cryptographic Services and User Defined Extensions for the PCICC and PCIXCC/CEX2C from this page.

- There are expandable folders for the Domain Cryptographic services. Within the folders are the services you can enable or disable:
  - ISPF Services
  - API Cryptographic Services
  - UDXs (appears only if you have created UDXs on your system)

Access Control Point settings



Domain Cryptographic Services

API Cryptographic Services

- ☑ Access Control Manager-Read role *** Required ***
- ☑ Authorize UDX
- ☑ CVV Generate
- ☑ CVV Verify
- ☑ Clear Key Import/Multiple Clear Key Import
- ☑ Clear PIN Encrypt
- ☑ Clear PIN Generate Alternate-3624 Offset
- ☑ Clear PIN Generate Alternate-VISA PVV
- ☑ Clear PIN Generate-3624
- ☑ Clear PIN Generate-GBP
- ☑ Clear PIN Generate-Interbank
- ☑ Clear PIN Generate-VISA PVV
- ☑ Control Vector Translate
- ☑ Cryptographic Variable Encipher

Using TKE the user is able to deactivate an API Cryptographic Services that they may not want to be allowed on a domain level per host coprocessor card.

Topics

- Overview of hardware and key parts
- TKE Introduction
- TKE History
- Features/Functions
- TKE Concepts
- **Master & Operational Key Loading**
- Linux on System z

Storing Key Materials

- Binary files
  - Stored either on the hard drive or removable media
- TKE Smart Cards
  - Key materials are stored on the smart card is secured by the PIN
- A TKE smart card can store
  - 1 Crypto Adapter Logon Key
  - 1 Authority Signature Key
  - 10 – Mix of master key parts, operational key parts, 4764 crypto adapter key parts

Storage method

There are advantages and disadvantages of each storage method. Each installation needs to make this decision based on their needs.

- Which method of storage should I choose?
  - Smart cards
  - Binary files
  - Print files (for key parts) and keyboard entry

Smart cards

- Advantages
  - Makes environment more secure
  - Key Parts are never in the clear
  - Authority keys are generated on smart card, private key never leaves the smart card

- Disadvantages
  - Forgotten PINs = Useless cards
  - Need TKE + SC Readers to reload master keys, disaster recovery issue

Binary Files

- Advantages
  - Ability to load key parts at any TKE workstation
  - Users can make multiple copies on diskettes or DVD-RAMs
- Disadvantages
  - Key parts are not protected on the workstation during communication between the 4764 card and binary file

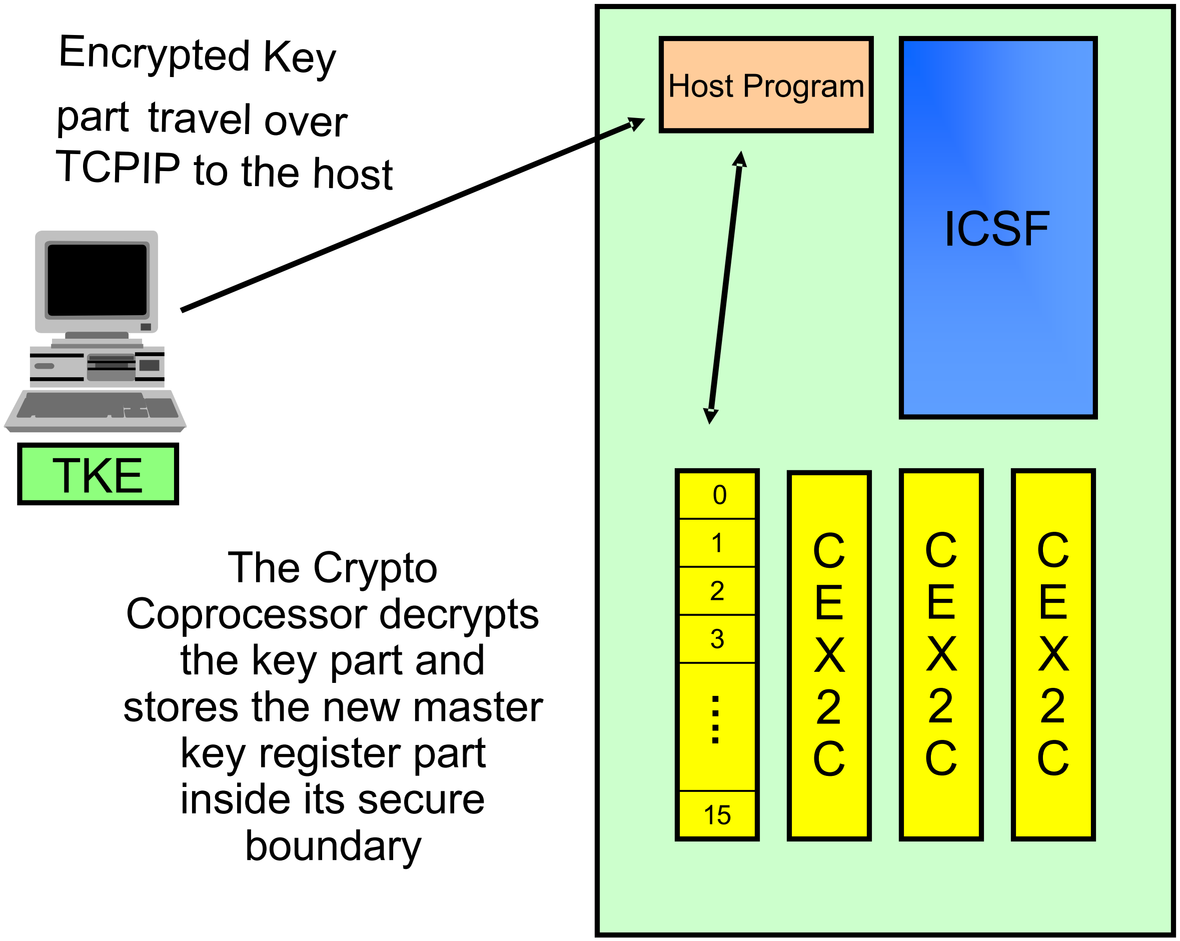
Keyboard Entry

- Advantages
  - Ability to load master key parts from TSO panels, if need be

- Disadvantages
  - No protection of key parts when storing them

Loading Master Key Parts

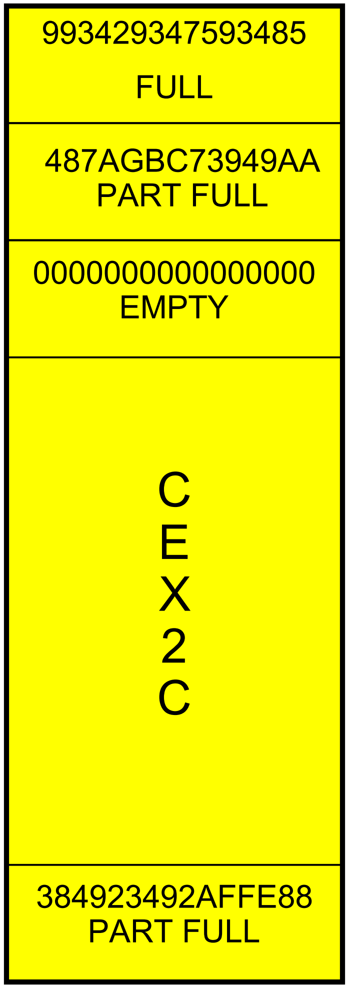
Encrypted Key part travel over TCPIP to the host



The Crypto Coprocessor decrypts the key part and stores the new master key register part inside its secure boundary

Host program takes the request and passes it down to the crypto coprocessor

Loading Key Parts



993429347593485
FULL

487AGBC73949AA
PART FULL

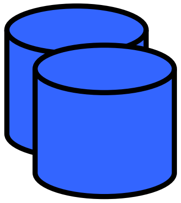
0000000000000000
EMPTY

CEX2C

384923492AFFE88
PART FULL

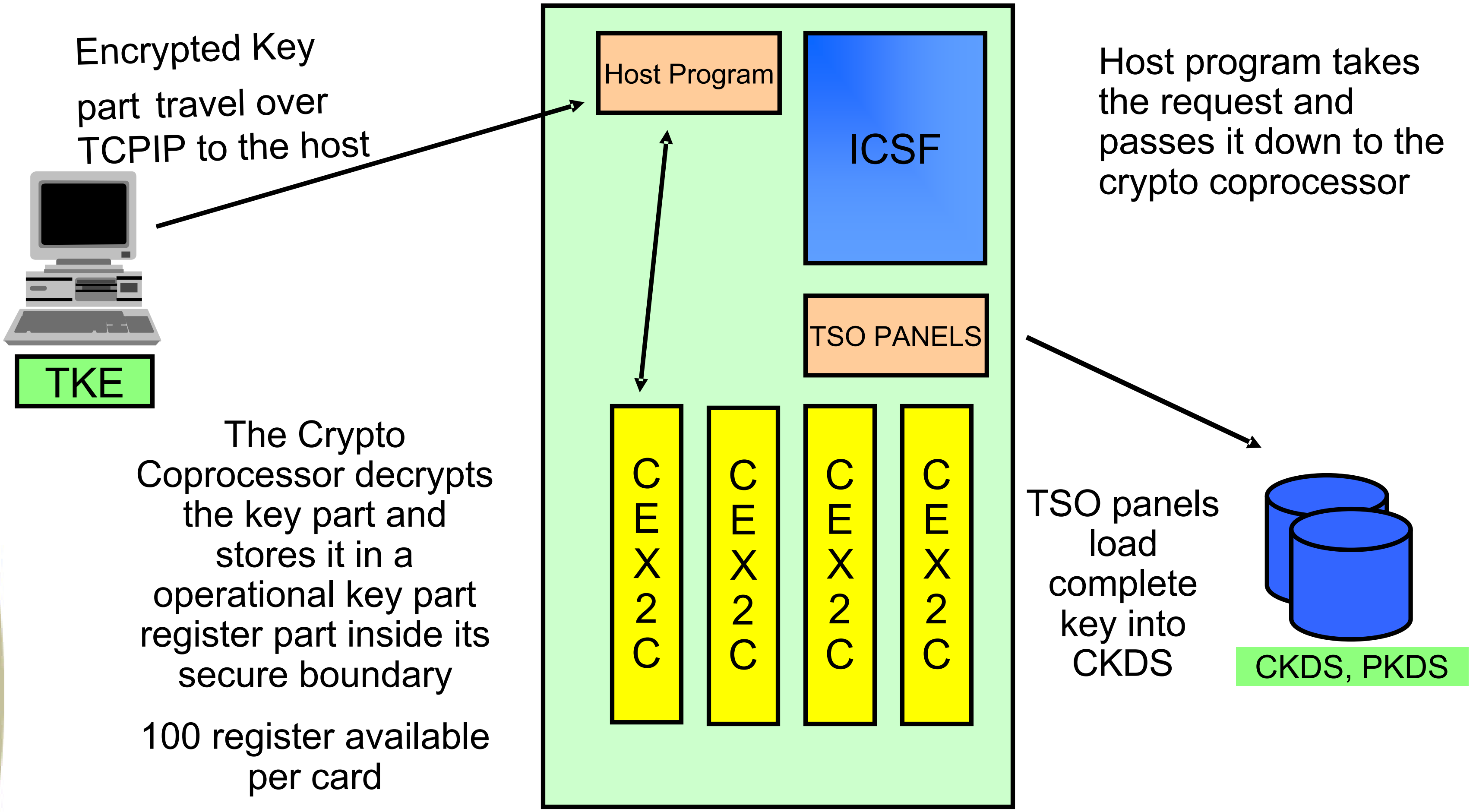
When key is complete ICSF TSO panels are used to complete process.

The CKDS/PKDS are initialized using the hash of the complete master key.



CKDS, PKDS

Loading Operational Key Parts



Encrypted Key part travel over TCPIP to the host

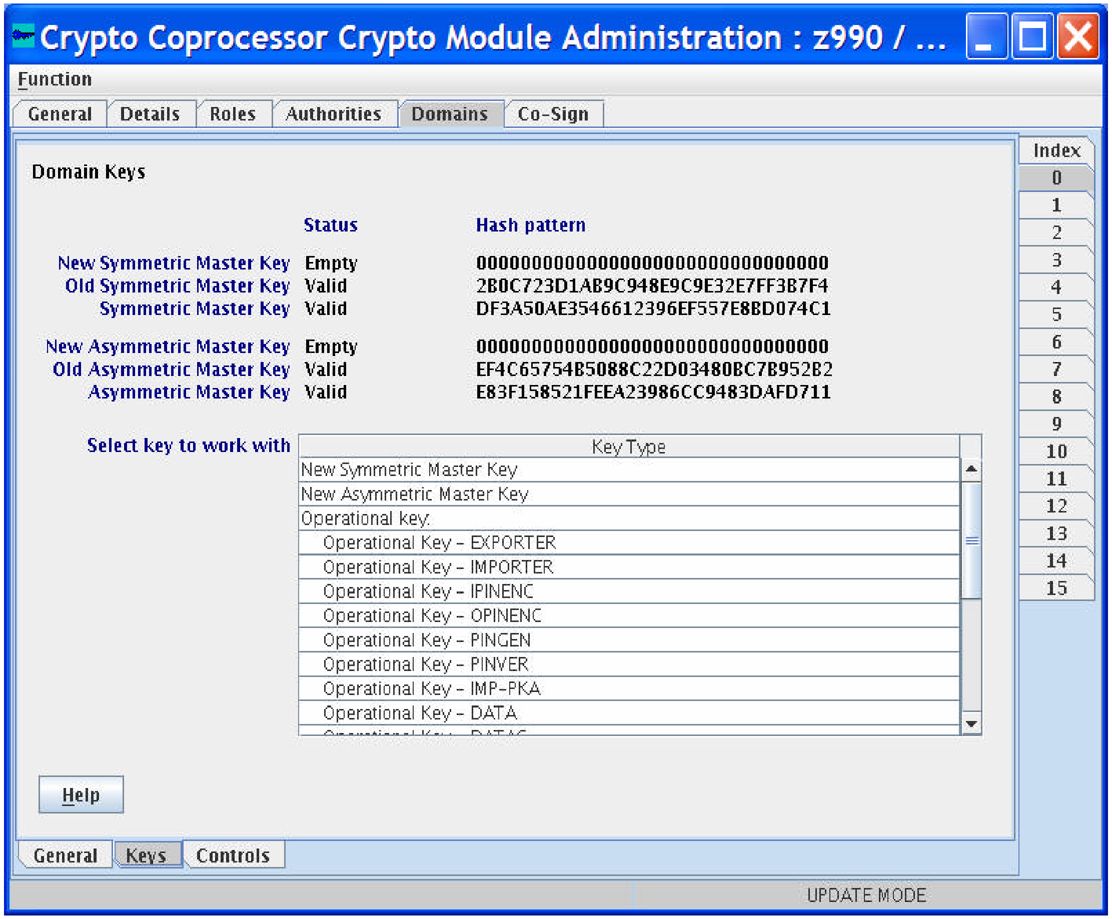
Host program takes the request and passes it down to the crypto coprocessor

The Crypto Coprocessor decrypts the key part and stores it in a operational key part register part inside its secure boundary

100 register available per card

TSO panels load complete key into CKDS

Crypto Coprocessor Notebook Keys Page



Domain Keys

	Status	Hash pattern
New Symmetric Master Key	Empty	00000000000000000000000000000000
Old Symmetric Master Key	Valid	2B0C723D1AB9C948E9C9E32E7FF3B7F4
Symmetric Master Key	Valid	DF3A50AE3546612396EF557E8BD074C1
New Asymmetric Master Key	Empty	00000000000000000000000000000000
Old Asymmetric Master Key	Valid	EF4C65754B5088C22D03480BC7B952B2
Asymmetric Master Key	Valid	E83F158521FEEA23986CC9483DAFD711

Select key to work with

Key Type
New Symmetric Master Key
New Asymmetric Master Key
Operational key
Operational Key – EXPORTER
Operational Key – IMPORTER
Operational Key – IPINENC
Operational Key – OPINENC
Operational Key – PINGEN
Operational Key – PINVER
Operational Key – IMP-PKA
Operational Key – DATA
Operational Key – DATAC

- Generating and loading master keys are done from this page

- Types of keys
  - Symmetric Master Keys
  - Asymmetric Master Keys
  - Operational Keys
  - RSA keys

Operational Keys TKE supports

From TKE the user can load 16 predefined operational key types on a CEX2C/PCIXCC. There is also a USER DEFINED key type where a customer can enter a valid control vector and TKE will generate a key part.

- EXPORTER
- IMPORTER
- IPINENC
- PINGEN
- PINVER
- IMP-PKA
- DATA
- DATAC
- DATAM
- DATAMV
- IKEYXLAT
- OKEYXLAT
- MAC
- MACVER
- USER DEFINED
- UDATAM
- UDATAMV

Topics

- TKE Introduction
- TKE History
- Features/Functions
- TKE Concepts
- Master & Operational Key Loading
- Linux on System z

Topics

- Overview of hardware and key parts
- TKE Introduction
- TKE History
- Features/Functions
- TKE Concepts
- Master & Operational Key Loading
- **Linux on System z**

Linux on System z

- TKE can be used to load master keys on a Linux LPAR
- TKE communicated with the LPAR using a Linux catcher, this performs the same function as the TKE host program on a zOS image
- CEX2C cards can be shared between a zOS image or CEX2C can be exclusive to the Linux on System z image
- Functions –
  - Create Role
  - Create Profiles
  - Load symmetric master key
  - Load asymmetric master key

Topics

- Overview of hardware and key parts
- TKE Introduction
- TKE History
- Features/Functions
- TKE Concepts
- Master & Operational Key Loading
- Linux on System z

TKE Terminology

Binary Files

Dual Control

Dual Control

Host Crypto

Host Crypto Card

Card

[illegible]

ACP

Workstation

Adapter

[illegible]

[illegible]

Symmetric Master Key

TKE Logon

Smart Cards

Signature Keys

Host Program

Asymmetric Master Key

Host

Logon

Authority Index

[illegible]

[illegible]

[illegible]

Publications

- TKE Manuals –

  www-03.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/

  - Trusted Key Entry PCIX Workstation User's Guide, SA23-2211-02

- Redbooks – www.redbooks.ibm.com

  - zSeries Trusted Key Entry (TKE) V4.2 Update, SG24-6499-00
  - z9-109 Crypto and TKE V5 Update, SG24-7123-00