



World's Best RACF® &  
Enterprise Security Training

## Trusted Key Entry Helping to Enter ICSF Keys Securely CRP6

Vicente Ranieri Junior  
Executive IT Specialist  
System z Security RDS – South Region

© 2008 IBM Corporation



## Trademarks

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

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by © are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml):

\*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries. Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

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

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

\* All other products may be trademarks or registered trademarks of their respective companies.

### Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance rates stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

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

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the 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.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

## Acknowledgement

- **TKE Workstation screen capture used in this presentation was provided by Greg Boyd from Advanced Technical Support (ATS) team in Gaithersburg, MD.**

## Agenda

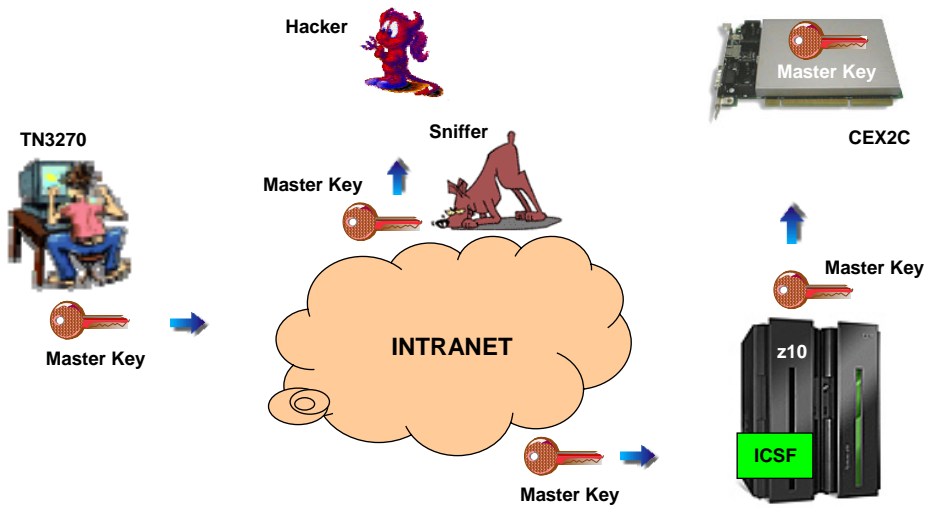
- Trusted Key Entry Workstation
- Cryptographic Node Management (CNM) Utility
- TKE Application
- Summary

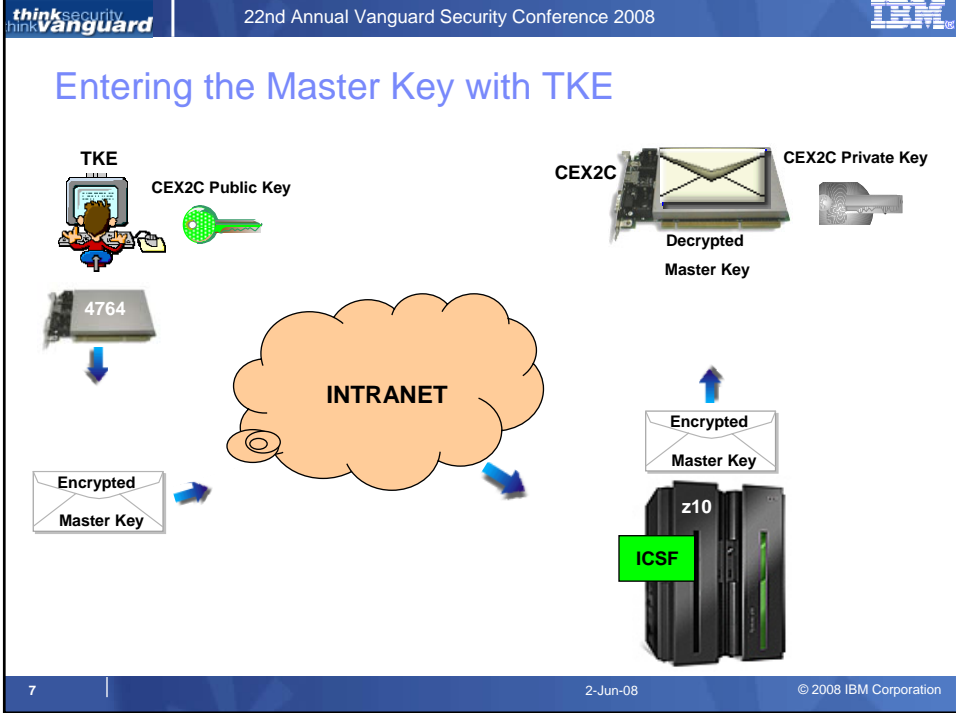


# Trusted Key Entry Workstation

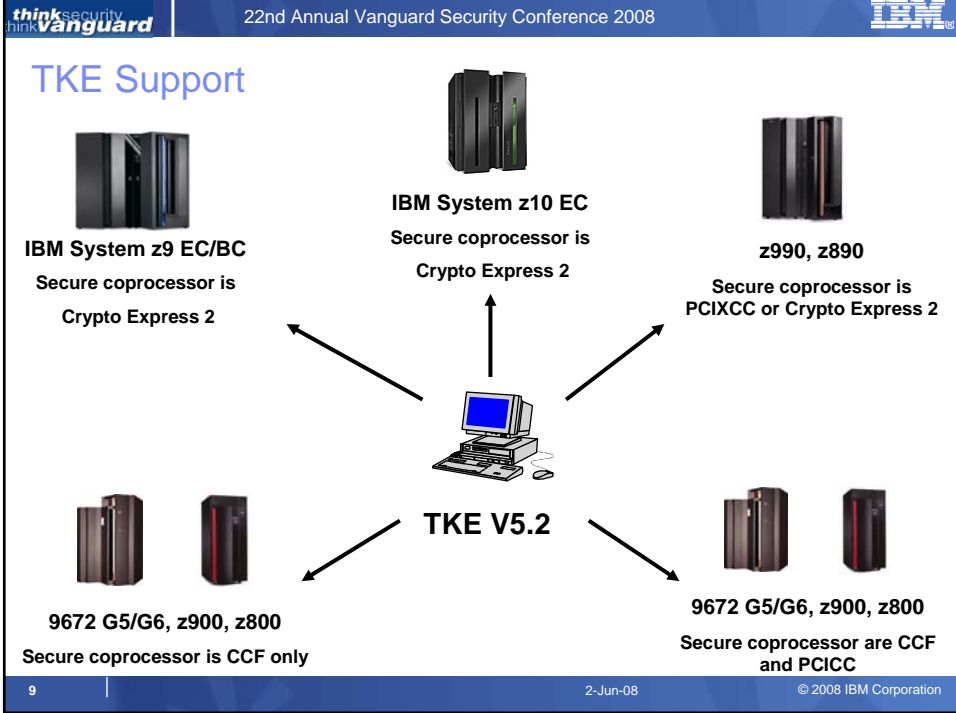


# Risk of Entering the Master Key without TKE





- think security think Vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM
- ## TKE (Trusted Key Entry) Workstation
- ❑ **System z priced feature, designed for highly secure management of secure coprocessors Master Keys and operational keys**
    - Optional Smart Card reader
    - Embedded closed Operational System
  - ❑ **Encrypted and signed communications over TCP/IP**
    - Additional ICSF Address Space Listener r
    - End point is the cryptographic coprocessor
    - Every command is signed (RSA) and encrypted (Diffie Hellmann)
    - Ethernet access only (V5)
  - ❑ **Operational Key Entry**
    - Key parts are loaded into crypto coprocessor card from TKE workstation
    - Any key type
    - User defined control vectors
    - Single, double and triple key lengths
- 8 | 2-Jun-08 | © 2008 IBM Corporation



- think security  
think Vanguard
- 22nd Annual Vanguard Security Conference 2008
- IBM
- ## TKE (Trusted Key Entry) Version 5
- ❑ **No desktop**
    - Now there is a framework with two main branches for TKE (includes Applications and Utilities related to TKE) and System Management (includes Service Applications, Configuration, and Maintenance for configuring and maintaining the TKE workstation)
  - ❑ **No command prompt**
    - Any command line task has now been replaced by a GUI interface.
- 10 | 2-Jun-08 | © 2008 IBM Corporation

## TKE (Trusted Key Entry) Version 5...

### ❑ No access to directory paths

- Now provide TKE related data directories for accessing files (via a File Chooser) and access to floppy and CD/DVD-RAM.
- To edit a file in these data directories or on media you'll use the new Edit TKE Files task.
- To manipulate these files (copy, rename, or delete) you'll use the new TKE File Management Utility task.

### ❑ No TKE.INI file

- Now there is a Preferences Menu on the TKE Task bar (Functions, Utilities, Help still exist).
- The Preferences menu allows you to enable/disable Blind Key Entry, Floppy Drive Only, Enable Tracing, Enable Smart Card Readers, and Show ECM bits as appropriate

http://127.0.0.1:8080 - TKE: Trusted Key Entry Console Workplace (Version 5.0)

IBM Trusted Key Entry Console IBM Systems Help

Welcome

- Trusted Key Entry
  - Applications
  - Utilities
- System Management
  - Service Applications
  - Console Logs
  - Configuration
  - Maintenance

Status: OK

TKEL: Welcome to <http://127.0.0.1> <http://127.0.0.1> Perform Support Captura by Herna16:10:45 01/26/07

think security think Vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

http://127.0.0.1:8080 - TKEL: Trusted Key Entry Console Workplace (Version 5.0)

Trusted Key Entry Console | IBM Systems | Help

Welcome

- Trusted Key Entry
  - Applications
  - Utilities
- System Management
  - Service Applications
  - Console Logs
  - Configuration
  - Maintenance

Applications

Trusted Key Entry Application Tasks

Name	Description
Begin Zone Remote Enroll Process for an IBM Crypto Adapter	Used to begin the zone remote enroll process for an IBM Crypto Adapter
CCA CLU 3.10SC	Used to manage the code on an IBM Crypto Adapter
Complete Zone Remote Enroll Process for an IBM Crypto Adapter	Used to complete the zone remote enroll process for an IBM Crypto Adapter
Cryptographic Node Management Batch Initialization 3.10SC	Used to initialize an IBM Crypto Adapter using CNI file
Cryptographic Node Management Utility 3.10SC	Used to manage an IBM Crypto Adapter
Smart Card Utility Program 1.20	Used to initialize Smart Cards
TKE Media Manager	Used to activate and deactivate media
TKE Migration Utility 1.5	Used to migrate 4753 keys to a z/OS host
TKE's IBM Crypto Adapter Initialization	Used to initialize an IBM Crypto Adapter for TKE using
Trusted Key Entry 5.0	Used to securely manage keys on a z/OS Host

Total: 10 Filtered: 10

Status: OK

TKEL: Welcome to http://127.0.0.1 http://127.0.0.1 Perform Support Captura by Herna 15:18:05 01/26/07

13 | 2-Jun-08 | © 2008 IBM Corporation

think security think Vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

http://127.0.0.1:8080 - TKEL: Trusted Key Entry Console Workplace (Version 5.0)

Trusted Key Entry Console | IBM Systems | Help

Welcome

- Trusted Key Entry
  - Applications
  - Utilities
- System Management
  - Service Applications
  - Console Logs
  - Configuration
  - Maintenance

Utilities

Trusted Key Entry Utility Tasks

Name	Description
Edit TKE Files	Used to edit TKE Files
Migrate Previous TKE Version to TKE 5.0	Used to migrate data on a backup disk created by previous TKE releases
TKE File Management Utility	Used to manage available files in all data directories
TKE Media Manager	Used to activate and deactivate media
TKE Workstation Code Information	Used to query TKE Workstation code information

Total: 5 Filtered: 5

Status: OK

TKEL: Welcome to http://127.0.0.1 http://127.0.0.1 Perform Support Captura by Herna 15:18:30 01/26/07

14 | 2-Jun-08 | © 2008 IBM Corporation

think security think Vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

http://127.0.0.1:8080 - TKEL: Trusted Key Entry Console Workplace (Version 5.0)

IBM Trusted Key Entry Console IBM Systems Help

Welcome

- Trusted Key Entry
  - Applications
  - Utilities
- System Management
  - Service Applications
  - Console Logs
  - Configuration
  - Maintenance

Status: OK

Service Applications  
Contains tasks for servicing the TKE system.

Name	Description
Console Logs	Contains tasks for accessing console logs.
Analyze Console Internal Code	Manage console's temporary internal code changes from IBM PE
Authorize Internal Code Changes	Enable or disable console's change management services
Change Console Internal Code	Manage console's internal code change levels
Format Media	Format a diskette or DVD-RAM
Hardware Messages	Display hardware messages from selected objects
Network Diagnostic Information	Display network diagnostic information for the console
Perform Console Trace	Perform console trace
Rebuild Vital Product Data	Rebuild the Console's vital product data
SIM Debug	Display and alter the SIM fields.
Transmit Console Service Data	Send Console Service Data to IBM for problem determination
Total: 11 Filtered: 11	

TKEL: Welcome to <http://127.0.0.1> <http://127.0.0.1> Perform Support Capture by Herna 15:20:25 01/26/07

15 | 2-Jun-08 | © 2008 IBM Corporation

think security think Vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

http://127.0.0.1:8080 - TKEL: Trusted Key Entry Console Workplace (Version 5.0)

IBM Trusted Key Entry Console IBM Systems Help

Welcome

- Trusted Key Entry
  - Applications
  - Utilities
- System Management
  - Service Applications
  - Console Logs
  - Configuration
  - Maintenance

Status: OK

Configurations  
Contains tasks for configuring the TKE system.

Name	Description
Configure 3270 Emulators	Customize the 3270 emulator sessions
Customize Console Date/Time	Customize the date and time
Customize Network Settings	Customize the network configuration for the console
Customize Scheduled Operations	Customize schedule of automated console operations
Update TKE Console Configuration Data	Update the configuration data on the TKE Console
Total: 5 Filtered: 5	

TKEL: Welcome to <http://127.0.0.1> <http://127.0.0.1> Perform Support Capture by Herna 15:20:09 01/26/07

16 | 2-Jun-08 | © 2008 IBM Corporation



think security  
think Vanguard

22nd Annual Vanguard Security Conference 2008

IBM

http://127.0.0.1:8080 - TRKE: Trusted Key Entry Console Workplace (Version 5.0)

Trusted Key Entry Console

IBM Systems

Help

Welcome

- Trusted Key Entry
  - Applications
  - Utilities
- System Management
  - Service Applications
  - Console Logs
  - Configuration
  - Maintenance

Maintenance  
Contains maintenance tasks for managing the TRKE system.

Name	Description
Backup Critical Console Data	Make backup of console's critical data
Cleanup Temporary Files	Cleanup Temporary Files from the Hard Drive
Format Media	Format a diskette or DVD-RAM
Hardware Messages	Display hardware messages from selected objects
Lock Console	Lock the console
Offload Virtual RETAIN Data to DVD-RAM	Offload saved RETAIN problem data to DVD-RAM
Perform Support Actions	Perform support oriented tasks
Save Upgrade Data	Save customizable data that is to be restored during an upgrade
Shutdown or Restart	Restart the application or shutdown/restart the console.
Users and Tasks	View the logged on users and their tasks
View Console Events	Display console's event log
View Console Information	Display console's internal code change information
View Console Logs	View Console Logs
View Console Service History	Display console's service history
View Console Tasks Performed	View record of console tasks performed by the console's users
View Licenses	Read the open-source licenses for the product

Total: 16 Filtered: 16

Status: OK

TRKE: Welcome to http://127.0.0.1 http://127.0.0.1 Perform Support Capture by Harna 15:19:07 01/26/07

17 | 2-Jun-08 | © 2008 IBM Corporation

think security  
think Vanguard

22nd Annual Vanguard Security Conference 2008

IBM

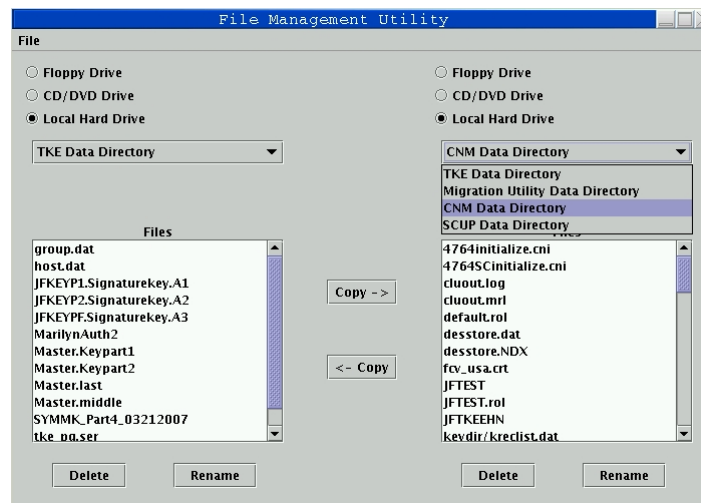
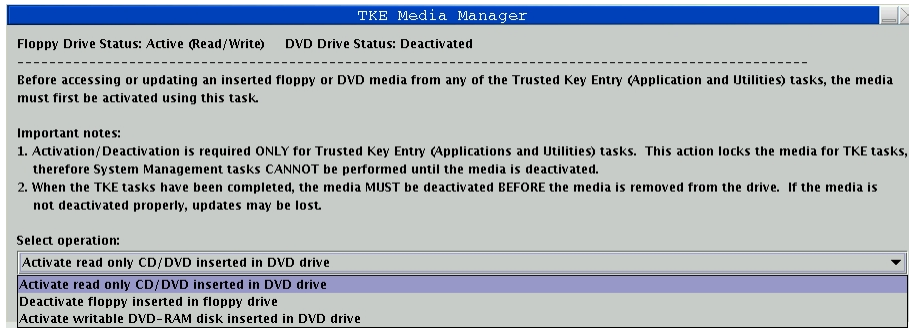
## TKE (Trusted Key Entry) Media Manager

**□ TKE Media Manager**

- For TKE related tasks to be able to use media (diskette, CD, DVD-RAM) the drive must be activated. Activation is thru the new TKE Media Manager task. If the media is not activated first, it will be automatically done for the user.
- When the user is done, the drive MUST be deactivated BEFORE the media is removed or any data saved to the media could be lost. Deactivation is NOT automatically done.
- If changing from one diskette to another, the floppy drive must be deactivated, media removed, new media inserted, and the drive activated again. If this is not performed data on the new diskette will not be recognized.

18 | 2-Jun-08 | © 2008 IBM Corporation

## TKE (Trusted Key Entry) Media Manager



# Cryptographic Node Management (CNM) Utility

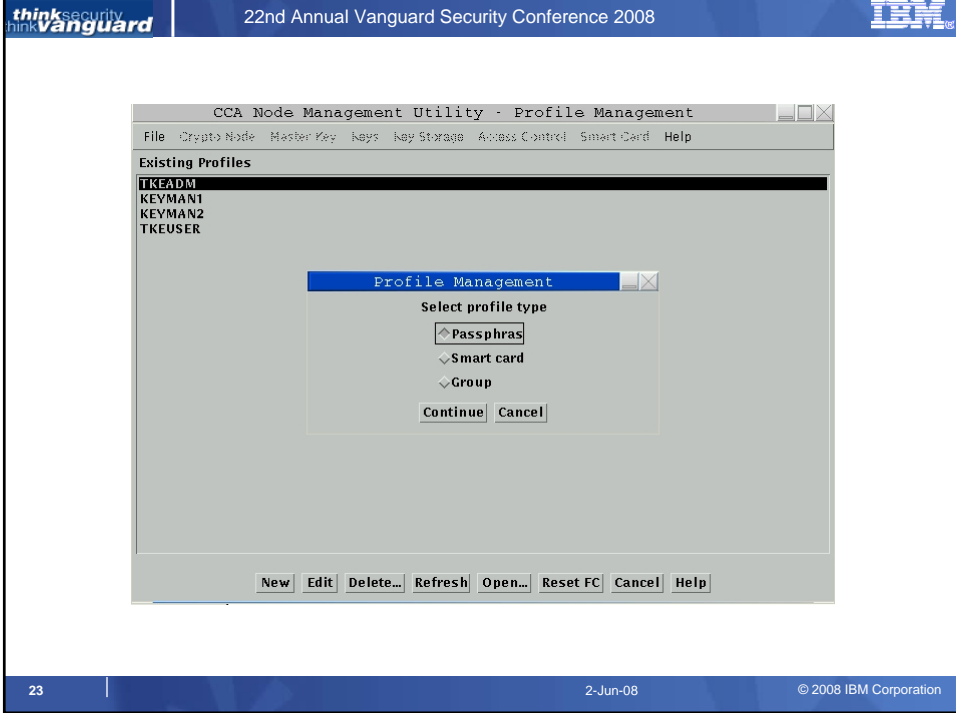


# Cryptographic Node Management Utility

## □ CNM Utility

- The CNM utility provides a graphical user interface to use in administering access control and managing CCA master keys on the cryptographic adapter in the TKE workstation.





23

2-Jun-08

© 2008 IBM Corporation

**The TKE implements an access control mechanism that uses the *roles* and *profiles* concept**

- When necessary, these roles and profiles are defined by the TKE administrator using the Crypto Node Management (CNM) software facility and according to customer security policy.

24

2-Jun-08

© 2008 IBM Corporation

# TKE Application



# TKE Application Main Screen

Hosts	
Host ID	Description
zPlexSYSC	Crypto System on z...

Crypto Modules			
Host ID	CM index	Status	Description
zPlexSYSC	X04	Authenticated	SYSC PCIXCC ...
zPlexSYSC	X05	Authenticated	SYSC PCIXCC ...

Groups	
Group ID	Description
HostGroup	z990 SYSC

think security  
think Vanguard

22nd Annual Vanguard Security Conference 2008

IBM

## TKE (Trusted Key Entry) Application

- ❑ **Crypto Module Notebook**
  - A crypto module or group of crypto modules are represented by the crypto module notebook
- ❑ **Access to secure cryptographic coprocessors is done through**
  - Authorities (security officers) identified by their password and digital signature
  - Roles identifying the functions to be performed by an authority
  - Option to require multiple signatures before performing a crypto function
  - Smart card support at TKE V4.2 and above

27 | 2-Jun-08 | © 2008 IBM Corporation

think security  
think Vanguard

22nd Annual Vanguard Security Conference 2008

IBM

## Crypto Module Notebook – Details Page

The screenshot shows a web-based interface titled "Crypto Coprocessor Crypto Module Administration : ZPlex8Y8C / X04". It features a navigation menu with tabs for "Function", "General", "Details", "Roles", "Authorities", "Domains", and "Co-Sign". The "Details" tab is active, displaying "Crypto Module Information".

**Crypto Module Information**

- Crypto Module ID 93001166
- Public Modulus 0.15 E749DDDE56221BE8813BF83DEF5D88686
- 16.31 CBD0527B5C5B43B19D0896C881D269B1
- 32.47 980172A50ECEA5D6AA8175FC9A0154C1
- 48.63 9F28433070D5DB60F8C3246A24DE24FC
- 64.79 EDFDE4C58F9C2306446A67D72BE9FFCC
- 80.95 50C652E83EC714886FF59E029FF32C72
- 96.111 71D638488219DAE1064CE854DD8D912
- 112.127 569C6788106407D2FE822DF497E989D5
- Signature Sequence Number 3288C9653E6F4DB6F6611B28BEC6000080510064
- Hash of Transport Key 566C832351790881124583E229DE7D01

Help

UPDATE MODE

28 | 2-Jun-08 | © 2008 IBM Corporation

think security think Vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

## Crypto Module Notebook – Roles Page

Function

General Details Roles Authorities Domains Co-Sign

Roles

Role ID	Description
INITADM	ADM default role

Create Role  
Change Role  
Delete Role

Help

UPDATE MODE

29 | 2-Jun-08 | © 2008 IBM Corporation

think security think Vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

## Role Definition

Create New Role

Role ID: ALLPOWER

Description: We really trust him

**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
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Send updates Cancel Help

Trusted Key Entry

30 | 2-Jun-08 | © 2008 IBM Corporation

think security think **vanguard** | 22nd Annual Vanguard Security Conference 2008 | IBM

## Crypto Module Notebook – Authorities Page

**Authorities**

Index	Name	Role	Phone	E-mail	Addr	Description
0	INITADM					

- Create Authority
- Change Authority
- Delete Authority
- Generate Signature Key

31 | 2-Jun-08 | © 2008 IBM Corporation

think security think **vanguard** | 22nd Annual Vanguard Security Conference 2008 | IBM

## Creating a New Authority

**Create New Authority**

Authority index: 9

Name: Greg Boyd Auth Indx 9

Phone: 3725041

E-mail: boydg@us.ibm.com

Address:

Description: Generate Signature Key for Auth Index #9

Role: INITADM

Signature key 0..31 D57CA536A597052AFB10E2C96F72461ADEE050036DC482CDB6F37843364FB9AE  
 32..63 9A3432CB803DFA38F6913C35CE499D7003B78C32F672848AE672EEE2DF454382  
 64..95 64DD3746EC2139CFAA83F0D2D2038BF1ECC8BF77BFA1A352AA7A05AF013156B  
 96..127 395C355D98342C8FFA888B707B2F47A5CC6F665DC052149445F428E074D7545F

Send updates | Cancel | Help

Trusted Key Entry

32 | 2-Jun-08 | © 2008 IBM Corporation



think security think **vanguard** | 22nd Annual Vanguard Security Conference 2008 | IBM

## Crypto Module Notebook – Domains Page

**Crypto Coprocessor Module Group Administration : JFGROUP. Master Crypt**

Function

General Details Roles Authorities **Domains** Co-Sign

Domain General

Domain Index 5  
Description Domain 5 on z9

Zeroize domain... Send updates Discard changes Help

General Keys Controls

UPDATE MODE

33 | 2-Jun-08 | © 2008 IBM Corporation

think security think **vanguard** | 22nd Annual Vanguard Security Conference 2008 | IBM

## Domains Page – Key Tab

**Crypto Coprocessor Crypto Module Administration : ZPlexSY8C / X04**

Function

General Details Roles Authorities **Domains** Co-Sign

Domain Keys

	Status	Hash pattern
New Symmetric Master Key	Empty	00000000000000000000000000000000
Old Symmetric Master Key	Valid	4FECDDA6289630834DC763F7EE1F6FDA
Symmetric Master Key	Valid	FC3F31230949C8C211E3CC78EEDC07F
New Asymmetric Master Key	Empty	00000000000000000000000000000000
Old Asymmetric Master Key	Valid	ABF9B45ED28C5A27DC11CD0C6A64C2E5
Asymmetric Master Key	Valid	71B8162488338760EC4DCF925FBCF0E9

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
- Operational Key - DATAM

Help

General Keys Controls

UPDATE MODE

34 | 2-Jun-08 | © 2008 IBM Corporation

think security think vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

## Generating a New Symmetric Master Key

**Function**  
General Details Roles Authorities Domains Co-Sign

**Domain Keys**

	Status	Hash pattern
New Symmetric Master Key	Empty	00000000000000000000000000000000
Old Symmetric Master Key	Valid	4FECDDA6289630834DC763F7EE1F6FDA
Symmetric Master Key	Valid	FCE3F31230949CBC211E3CC78EEDC07F
New Asymmetric Master Key	Empty	00000000000000000000000000000000
Old Asymmetric Master Key	Valid	ABF9B45ED28C5A27DC11CD0C6A64C2E5
Asymmetric Master Key	Valid	718816248838760EC4DCF925FBCF0E9

Select key to work with: Key Type

- New Symmetric Master Key
- New Asymmetric Master Key
- Operational key
- Operational Key - EXP
- Operational Key - IMPI
- Operational Key - IPIN
- Operational Key - IPINENC
- Operational Key - PINGEN
- Operational Key - PINVER
- Operational Key - IMP-PKA
- Operational Key - DATA
- Operational Key - DATAC
- Operational Key - DATAM

Buttons: Help, General, Keys, Controls, UPDATE MODE

35 | 2-Jun-08 | © 2008 IBM Corporation

think security think vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

## Generating a New Symmetric Master Key (Continued)

**Function**  
Enter key part description

Description: SYMMK Part1 03282007

Buttons: Continue, Cancel, Help

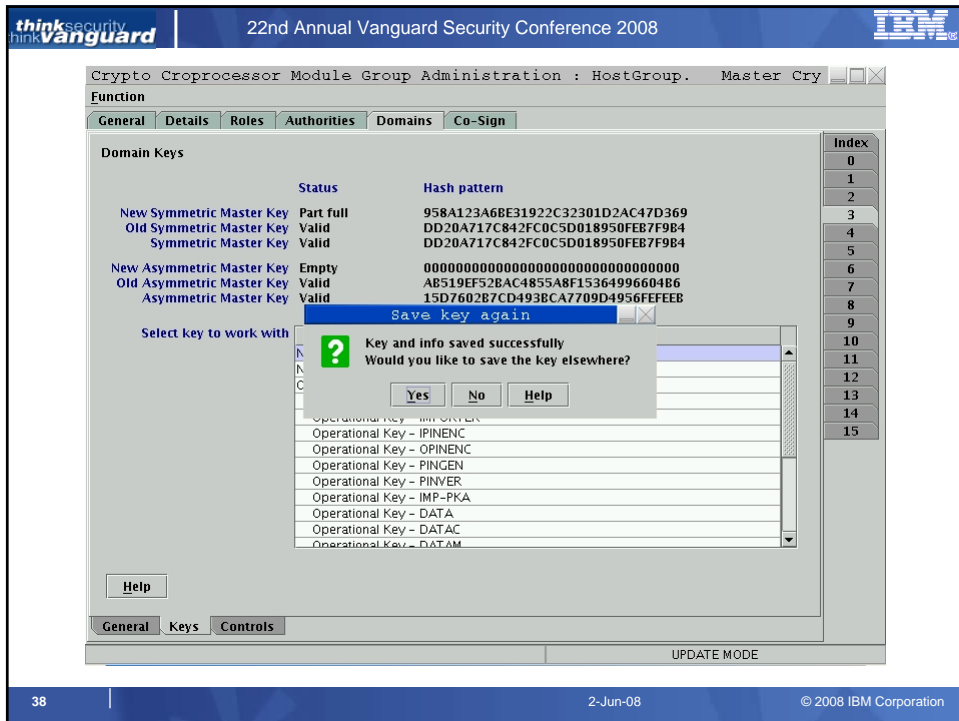
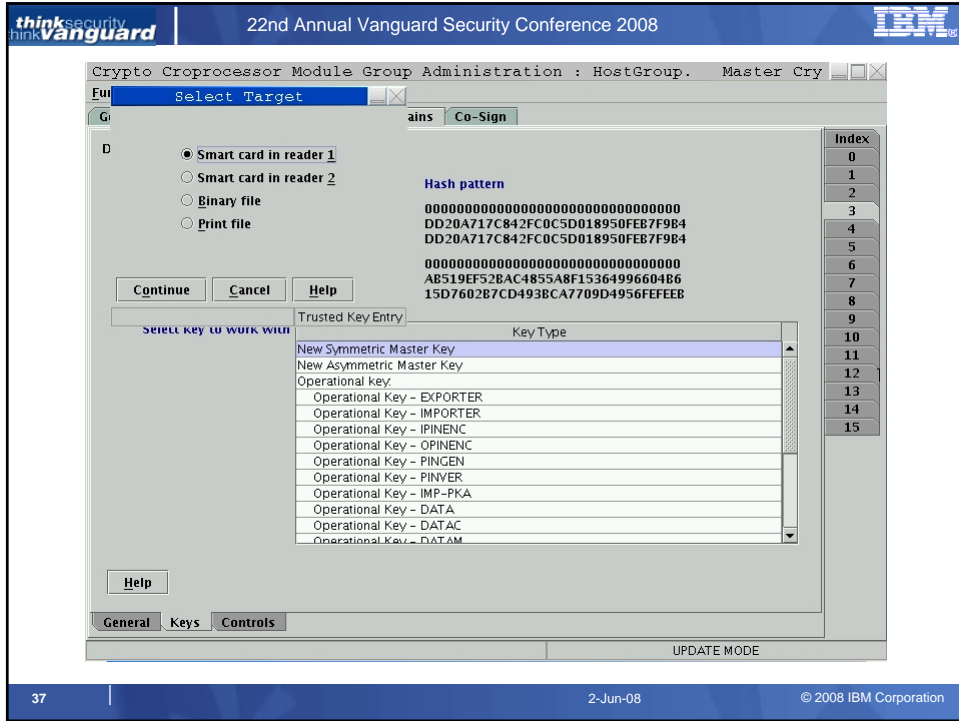
	Status	Hash pattern
Symmetric Master Key	Valid	10000000000000000000000000000000 COC5D018950FEB7F984 DU20A717C892FCOC5D018950FEB7F984
New Symmetric Master Key	Empty	00000000000000000000000000000000
Old Asymmetric Master Key	Valid	AB519EF52BAC4855A8F1536499660486
Asymmetric Master Key	Valid	15D7602B7CD4938CA7709D4956FEFEEB

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
- Operational Key - DATAM

Buttons: Help, General, Keys, Controls, UPDATE MODE

36 | 2-Jun-08 | © 2008 IBM Corporation



think security think vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

## Generating an Operational Key

Crypto Coprocessor Module Group Administration : HostGroup. Master Cry

Function: General | Details | Roles | Authorities | Domains | Co-Sign

Domain Keys			Index
	Status	Hash pattern	
New Symmetric Master Key	Part full	958A123A6BE31922C32301D2AC47D369	0
Old Symmetric Master Key	Valid	DD20A717C842FC0C5D018950FEB7F9B4	1
Symmetric Master Key	Valid	DD20A717C842FC0C5D018950FEB7F9B4	2
			3
			4
			5
New Asymmetric Master Key	Empty	00000000000000000000000000000000	6
Old Asymmetric Master Key	Valid	A8519EF528AC4855A8F1536499660486	7
Asymmetric Master Key	Valid	15D7602B7CD4938CA7709D4956FEFEEB	8
			9
			10
			11
			12
			13
			14
			15

Select key to work with: Key Type

- 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
- Operational Key - DATAM
- Operational Key - DATAMV

Generate...  
Load to key part register ▶  
View  
Clear  
Secure key part entry

39 | 2-Jun-08 | © 2008 IBM Corporation

think security think vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

## Key part information

Crypto Coprocessor Module Group Administration : HostGroup. Master Cry

Full Key part information

Description: Operational Key - DATA

ENC-ZERO: 2A42837D

MDC-4: 4A3CE0E341E56DC24229309E64875267

Key type: Operational Key - DATA

Control vector: 0000000000000000 0000000000000000

Key label: GPB.FROM.TKE.041307

Key label's SHA1: D7A7AFBE0B628C85F88B5C11A2FA8EDA702FEA64

72669E6D1A31E70C4  
0C5D018950FEB7F9B4  
0C5D018950FEB7F9B4

100000000000000000  
35A8F1536499660486  
BCA7709D4956FEFEEB

Trusted Key Entry

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
- Operational Key - DATAM

40 | 2-Jun-08 | © 2008 IBM Corporation

think security think Vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

Crypto Coprocessor Module Group Administration : HostGroup. Master Cry

Function

General Details Roles Authorities Domains Co-Sign

Domain Keys

	Status	Hash pattern
New Symmetric Master Key	Part full	8F884EE2782BAA772669E6D1A31E70C4
Old Symmetric Master Key	Valid	DD20A717C842FC0C5D018950FEB7F9B4
Symmetric M:		
New Asymmetric M:		
Old Asymmetric M:		
Asymmetric M:		

Complete Operational Key Part Register

Select key to w

Key labels

SHA1 C3AFA63B646B03AC1ACE57879417D1C6F0652F21

OK Cancel Help

Operational Key - FIRST...  
Operational Key - IMP-PKA  
Operational Key - DATA  
Operational Key - DATAC  
Operational Key - DATAM

Index

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

Getting list of key registers... UPDATE MODE

41 | 2-Jun-08 | © 2008 IBM Corporation

think security think Vanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

## Loading a Master Key

Crypto Coprocessor Module Group Administration : HostGroup. Master Cry

Function

General Details Roles Authorities Domains Co-Sign

Domain Keys

	Status	Hash pattern
New Symmetric Master Key	Empty	00000000000000000000000000000000
Old Symmetric Master Key	Valid	DD20A717C842FC0C5D018950FEB7F9B4
Symmetric Master Key	Valid	DD20A717C842FC0C5D018950FEB7F9B4
New Asymmetric Master Key	Empty	00000000000000000000000000000000
Old Asymmetric Master Key	Valid	AB519EF52BAC4855A8F1536499660486
Asymmetric Master Key	Valid	15D7602B7CD4938CA7709D4956FEFEEB

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  
Operational Key - DATAM

Generate...  
Load  
Clear  
Secure key part entry

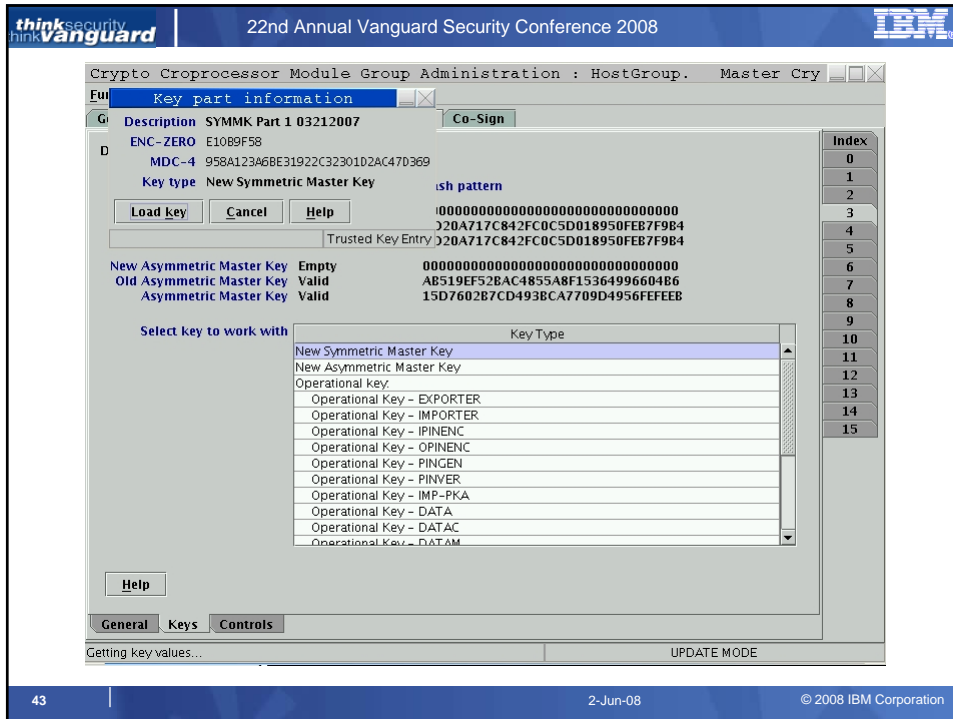
First...  
Intermediate...  
Last...

Index

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

UPDATE MODE

42 | 2-Jun-08 | © 2008 IBM Corporation



thinksecurity  
thinkVanguard | 22nd Annual Vanguard Security Conference 2008 | IBM

## Master Key or Operational Key Load

- Master Key or Operational Key was transferred from TKE to the cryptographic coprocessor in a secure way through an unsecure network
- Once the key is already inside the secure boundary of crypto module, ICSF panel must be used to transfer the key from New Master Key register to the Master Key register
- The same applies to the Operational Key. ICSF panel must be used to transfer the operational key from the part register to the CKDS / PKDS.

44 | 2-Jun-08 | © 2008 IBM Corporation

## Summary



## Summary

- Trusted Key Entry (TKE) is an optional feature of ICSF that provides a basic key management system.
- TKE allows authorized people a method for key identification, exchange, separation, update, backup, and management.
- It is a tool for security administrators to use in setting up and establishing the security policy and placing it into production.



# QUESTIONS





**VANGUARD SECURITY CONFERENCE 2008**  
22ND ANNUAL | JUNE 1 - 5 | LOS ANGELES, CA



**World's Best RACF® &  
Enterprise Security Training**



## **System z Crypto User Experience**

### **CRP13**

**Vicente Ranieri Junior**  
Executive IT Specialist  
System z Security RDS – South Region

© 2008 IBM Corporation