Trusted Key Entry
Helping to Enter ICSF Keys Securely

CRP6

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

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:

*, 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 ratios 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

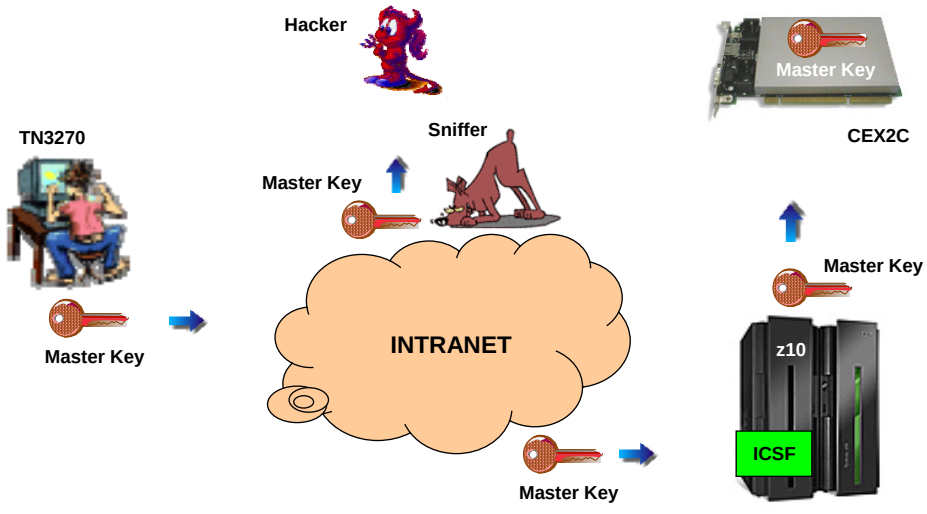
- **TKE Workstation screen capture used in this presentation was provided by Greg Boyd from Advanced Technical Support (ATS) team in Gaithersburg, MD.**

Agenda

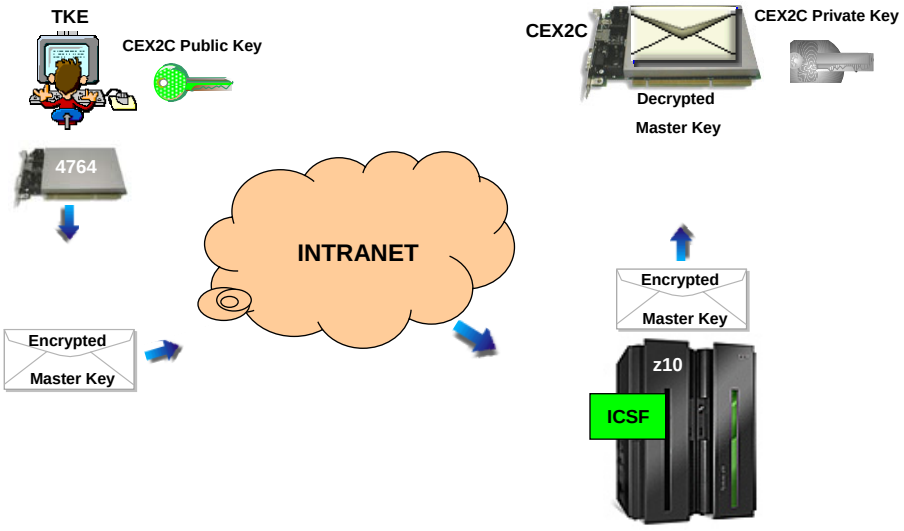
- Trusted Key Entry Workstation
- Cryptographic Node Management (CNM) Utility
- TKE Application
- Summary

Trusted Key Entry Workstation

Risk of Entering the Master Key without TKE



Entering the Master Key with TKE



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

TKE Support

IBM System z9 EC/BC

Secure coprocessor is

Crypto Express 2

IBM System z10 EC

Secure coprocessor is

Crypto Express 2

z990, z890

Secure coprocessor is PCIXCC or Crypto Express 2

TKE V5.2

9672 G5/G6, z900, z800

Secure coprocessor is CCF only

9672 G5/G6, z900, z800

Secure coprocessor are CCF and PCICC

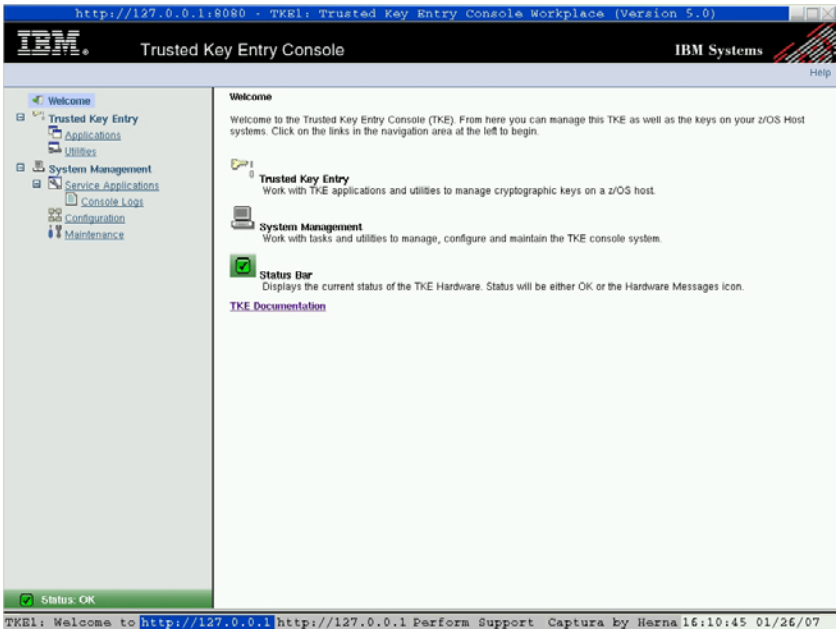
22nd Annual Vanguard Security Conference 2008

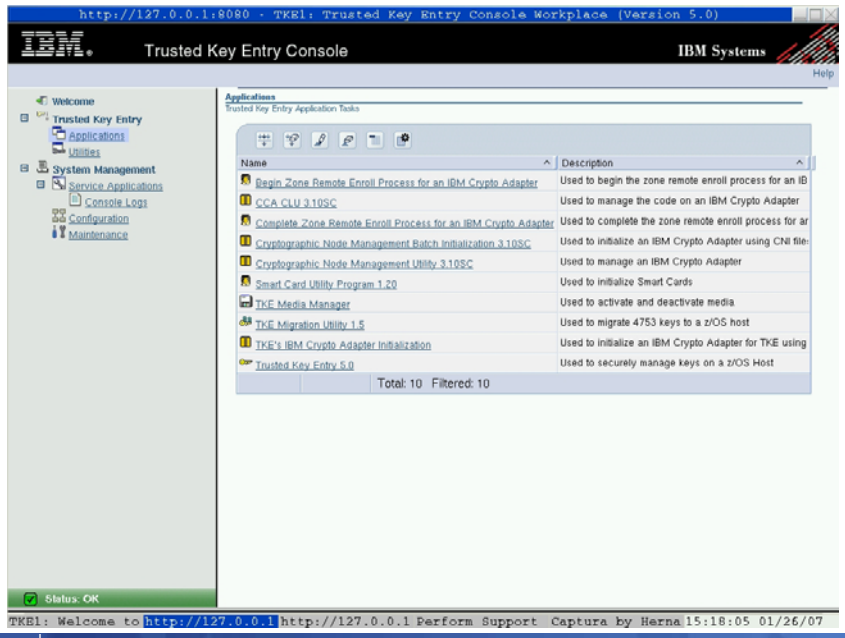
TKE (Trusted Key Entry) Version 5

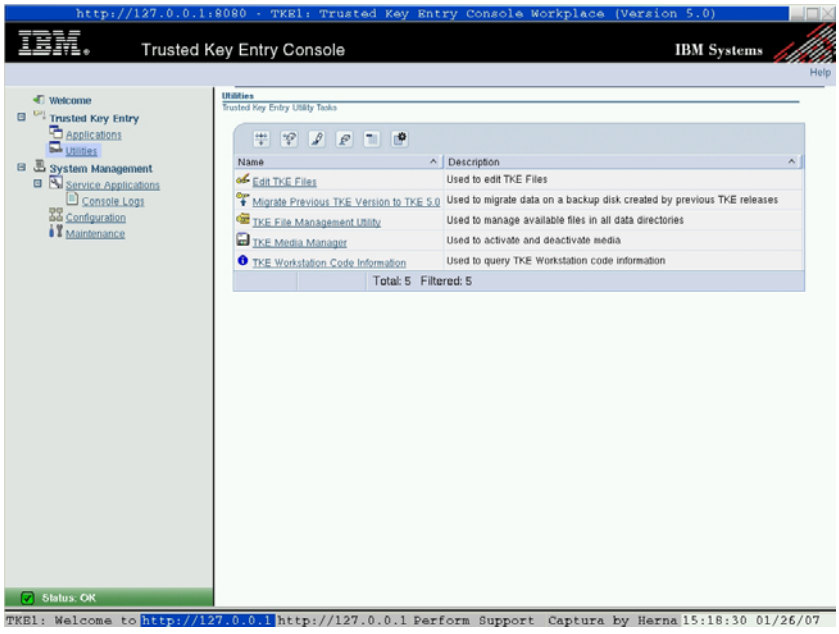
- **No desktop**
  - Now there is a framework with two main branches for TKE (includes Applications and Utilities related toTKE) and System Management (includes Service Applications, Configuration, and Maintenance for configuring and maintaining the TKE workstation)
- **No command prompt**
  - Any command line task has now been replaced by a GUI interface.

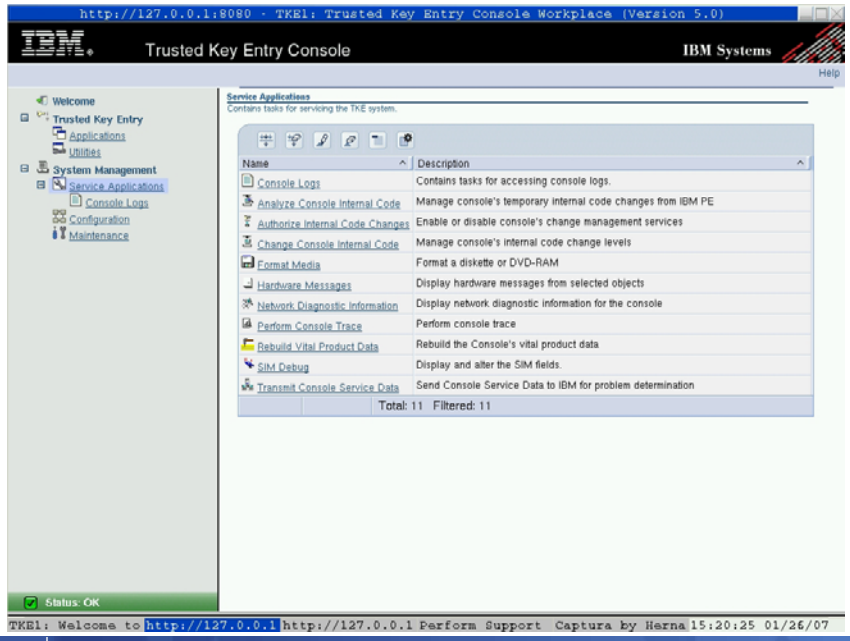
TKE (Trusted Key Entry) Version 5…

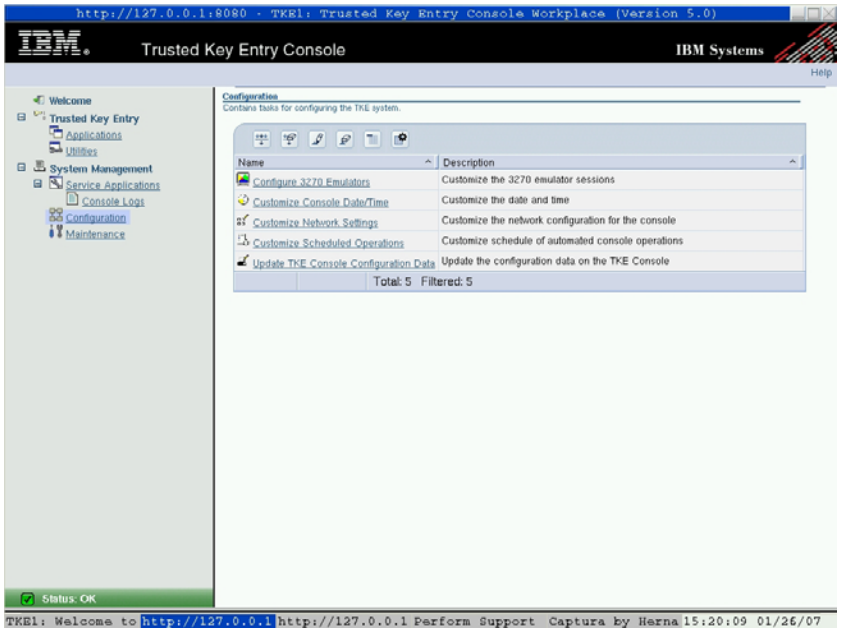
- **No access to directory paths**
  - Now provide TKE related data directories for accessing files (via a File Chooser) and access to floppy and CD/DVD-RAM.
  - To edit a file in these data directories or on media you'll use the new Edit TKE Files task.
  - To manipulate these files (copy, rename, or 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

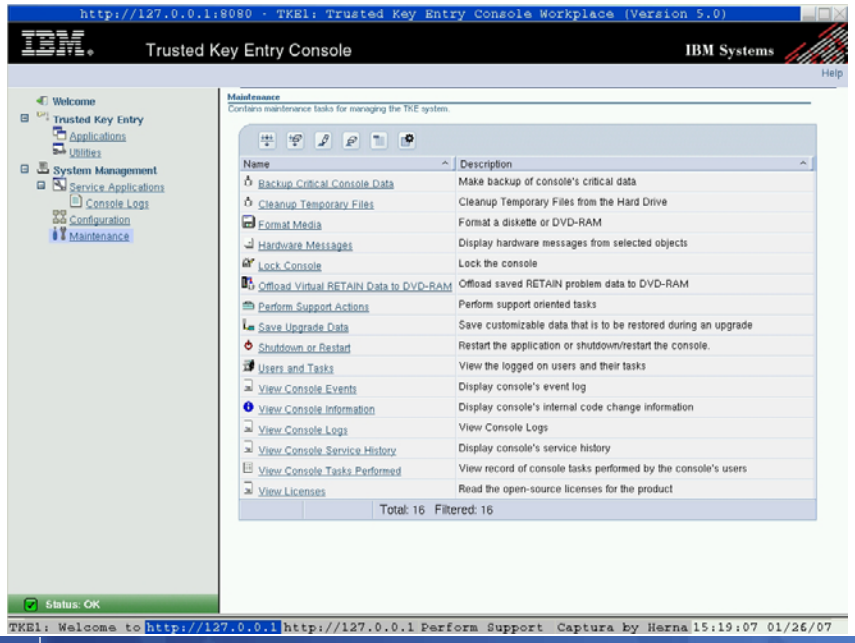








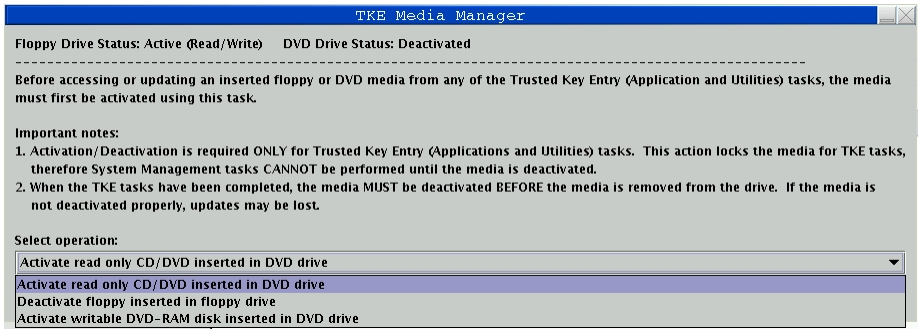


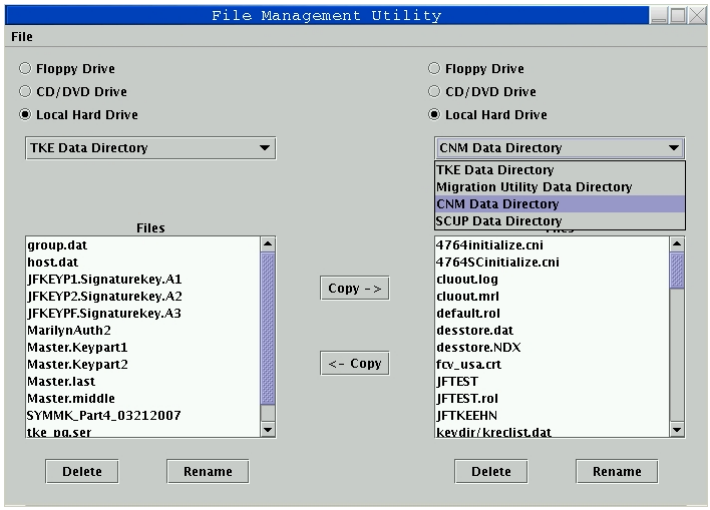


TKE (Trusted Key Entry) Media Manager

- **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.

TKE (Trusted Key Entry) Media Manager

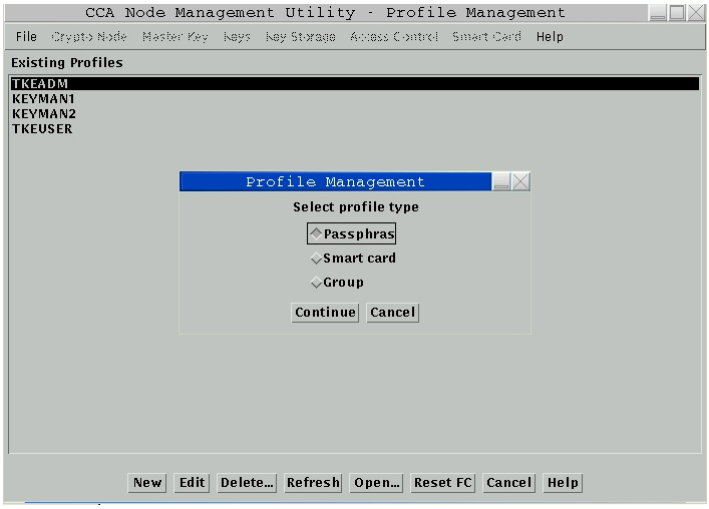


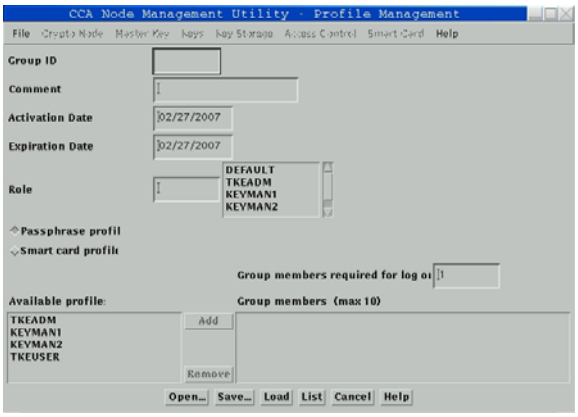


Cryptographic Node Management (CNM) Utility

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.

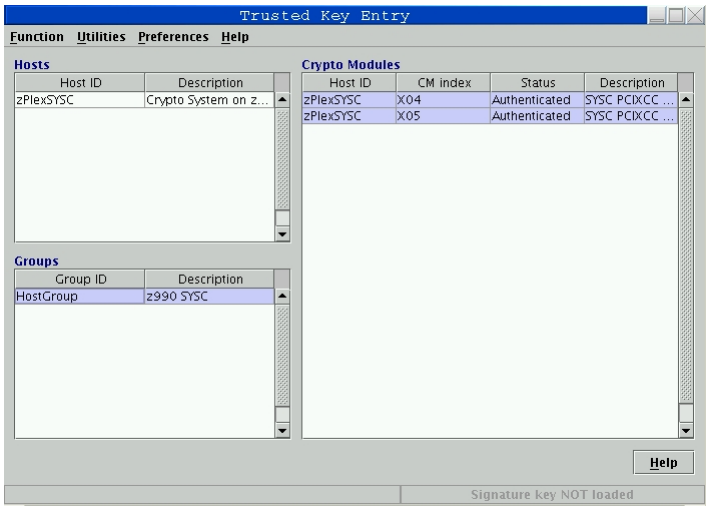




- **The TKE implements an access control mechanism that uses the *roles* and *profiles* concept**
  - When necessary, these roles and profiles are defined by the TKE administrator using the Crypto Node Management (CNM) software facility and according to customer security policy.

TKE Application

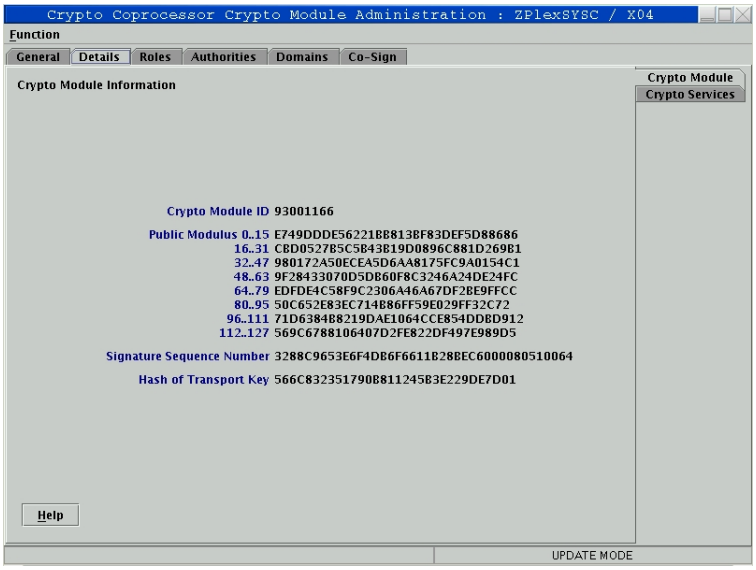
TKE Application Main Screen



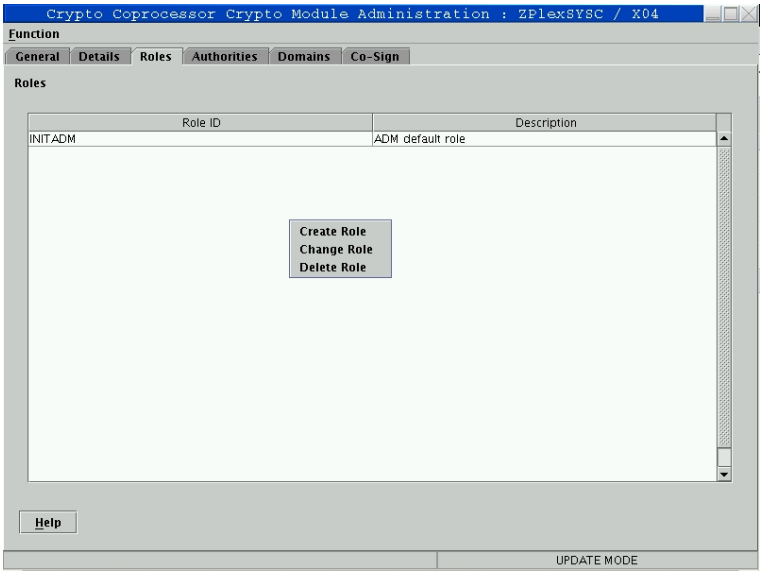
TKE (Trusted Key Entry) Application

- **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

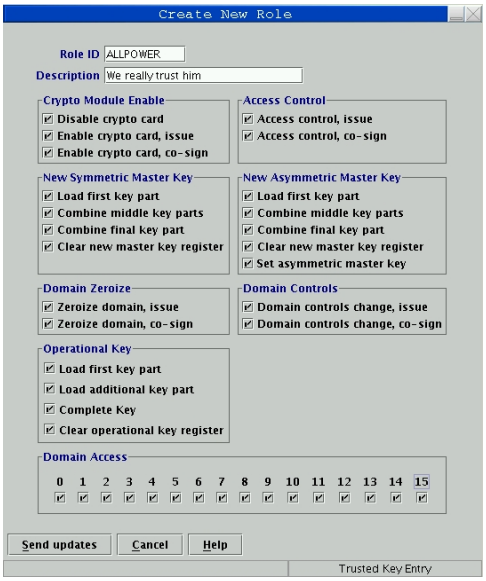
Crypto Module Notebook – Details Page



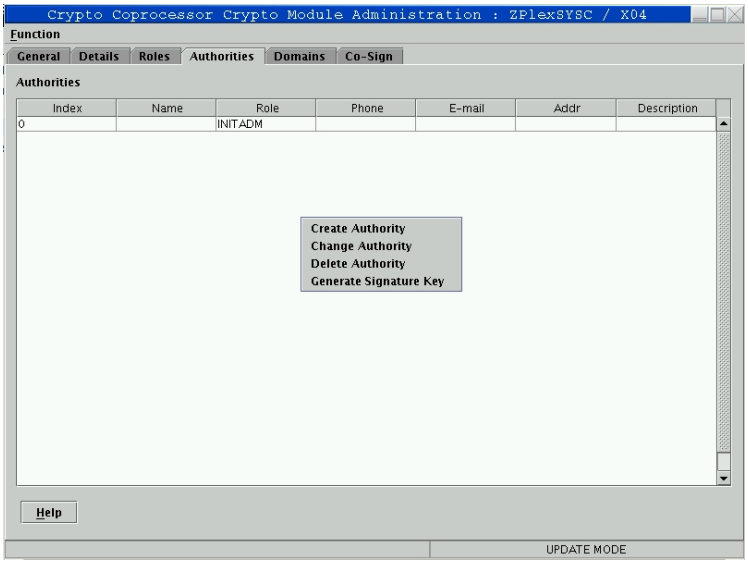
Crypto Module Notebook – Roles Page



Role Definition

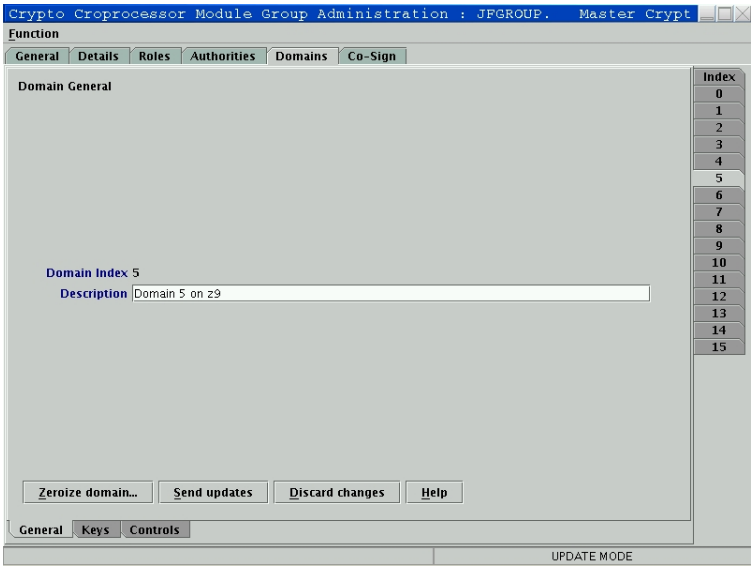


Crypto Module Notebook – Authorities Page

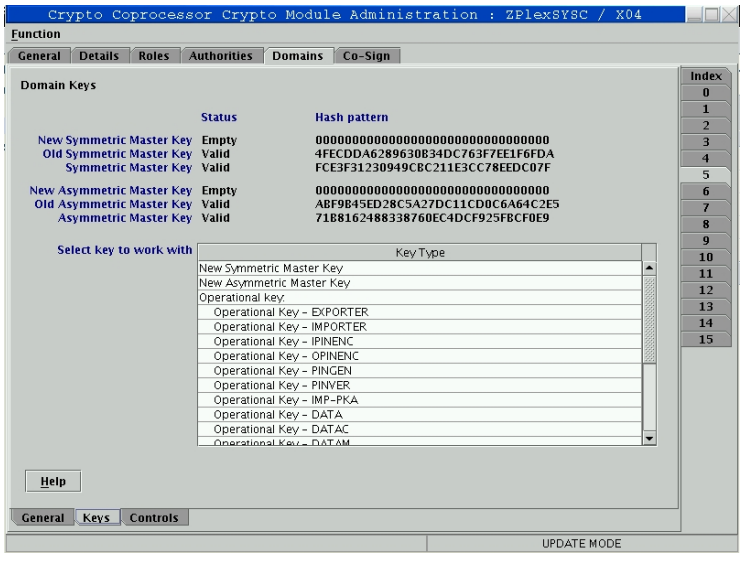


Creating a New Authority

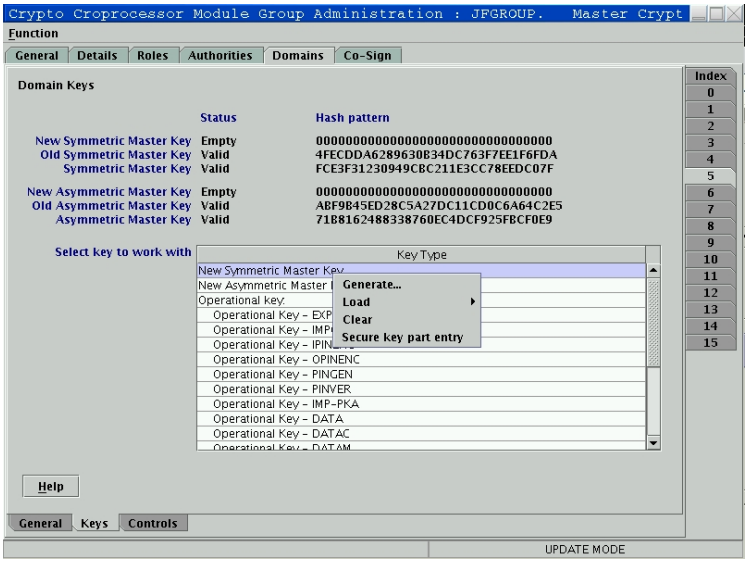
Crypto Module Notebook – Domains Page

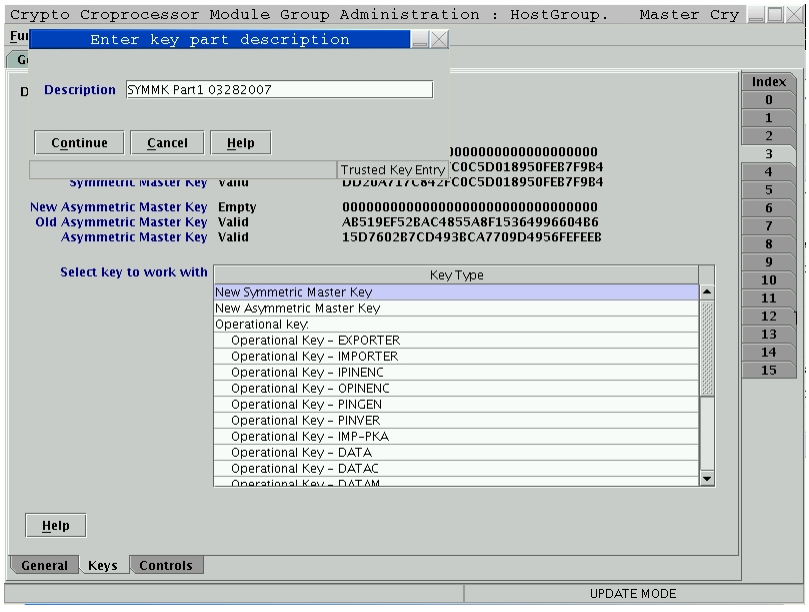


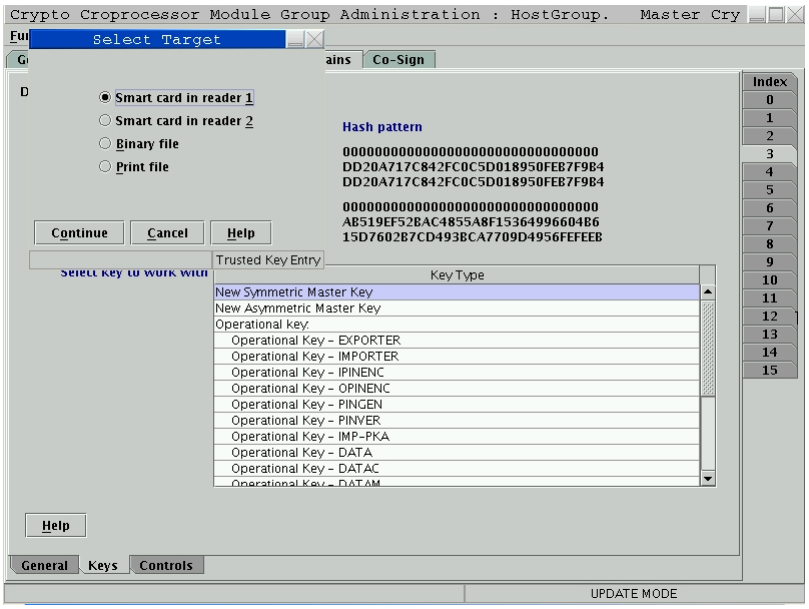
Domains Page – Key Tab

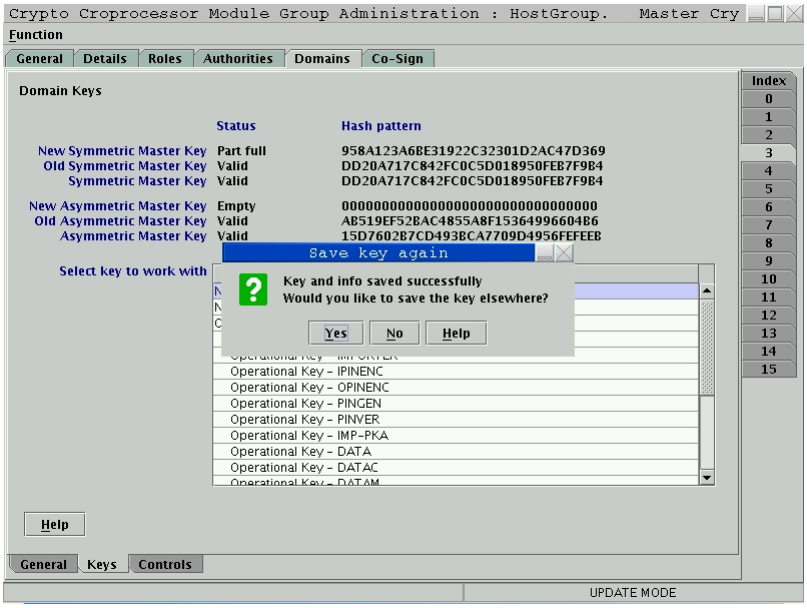


Generating a New Symmetric Master Key

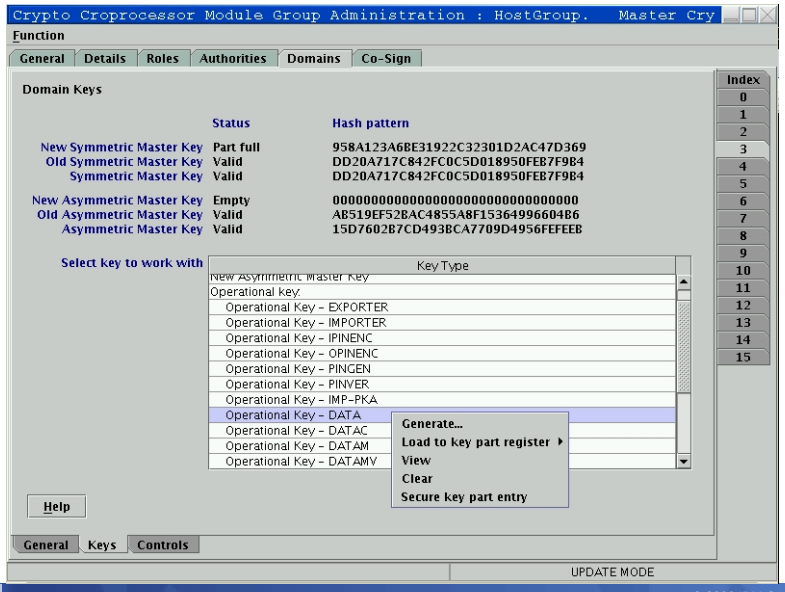


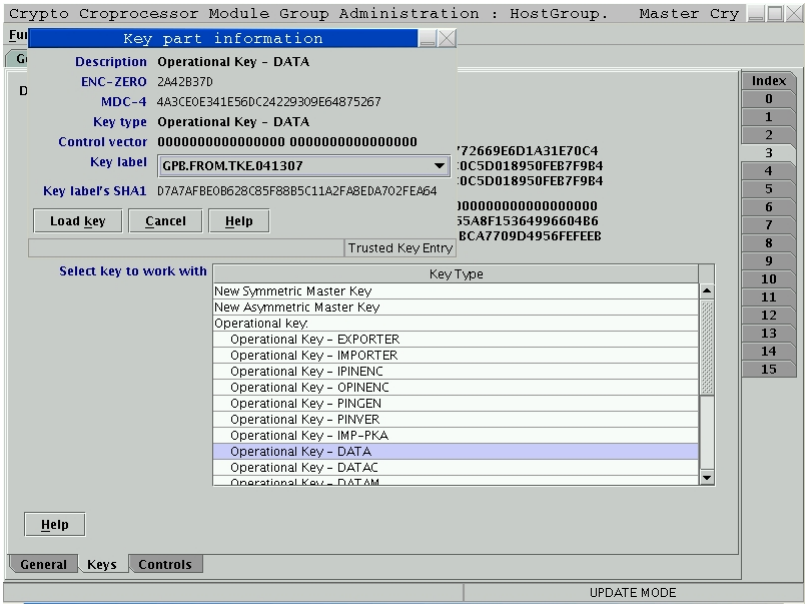


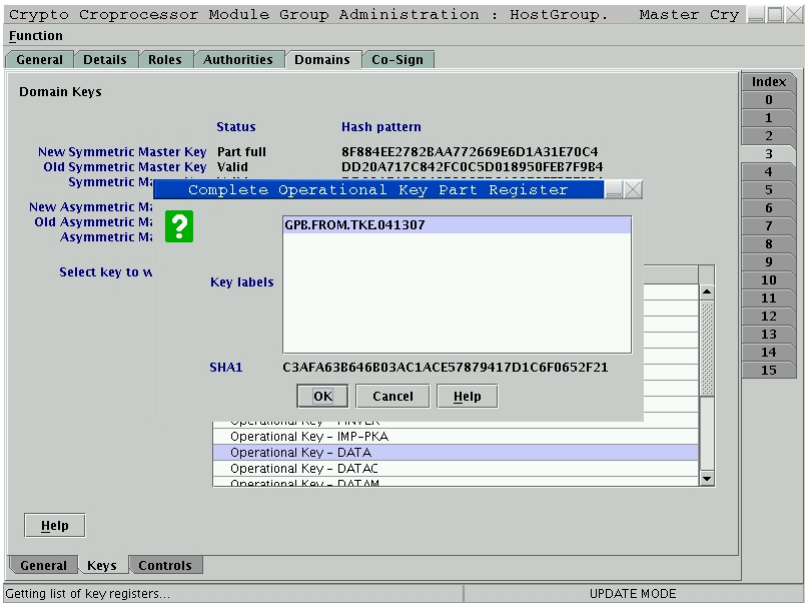




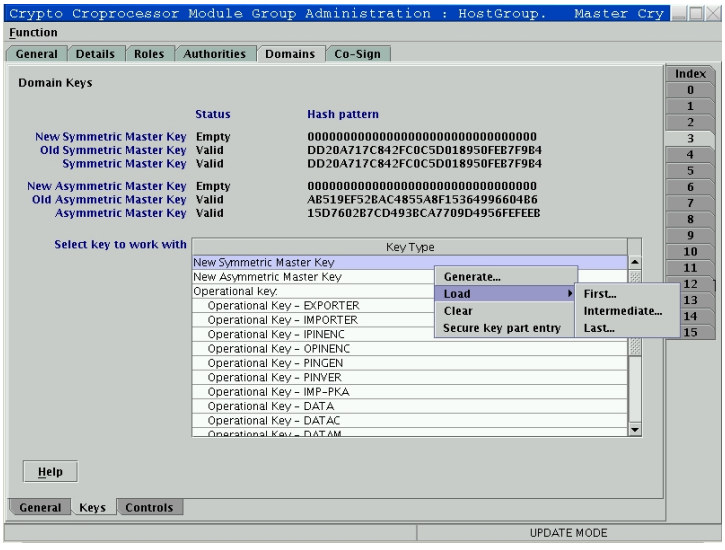
Generating an Operational Key

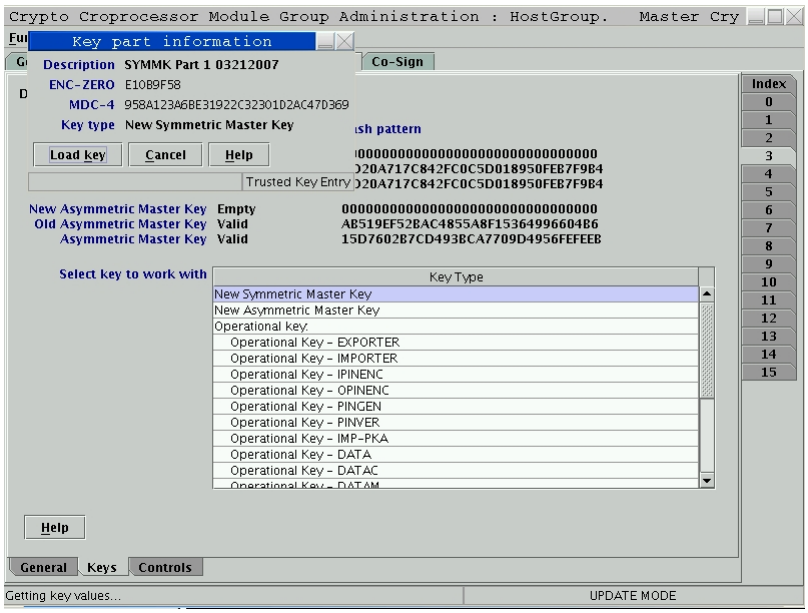






Loading a Master Key





Master Key or Operational Key Load

- **Master Key or Operational Key was transfered 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.**

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
IBM®
System z Crypto User Experience
CRP13
Vicente Ranieri Junior
Executive IT Specialist
System z Security RDS – South Region
© 2008 IBM Corporation