IBM zServer Cryptographic Update

Ernest Nachtigall cissp;cisa

Vanguard Session B10

July 11, 2006

Trademarks

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

IBM*	GDPS*	RACF*	WebSphere*
IBM eServer*	Geographically Dispersed Parallel Sysplex	Rational*	z/OS*
IBM logo*	HiperSockets	Redbooks	z/VM*
CICS*	HyperSwap	Resource Link	zSeries*
DB2*	IMS	System z9	
Domino*	MQSeries*	Tivoli*	
FICON*	Parallel Sysplex*	Virtualization Engine	

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States, other countries or both.
Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
Linux is a trademark of Linus Torvalds in the United States and other countries..
UNIX is a registered trademark of The Open Group in the United States and other countries.
Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.

* 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.

Agenda

- Z9-109 Current (inherited) features
- z9-109 Enhancements
- SE/HMC changes
- TKE changes
- z9-109 Requests

Challenges

- Protecting the data from unauthorized access
  - RACF
  - Identification
    - PIN
    - Certificates
- Guarding the integrity of the data
  - Message authentication
  - HASHING
- Protecting disclosure of the information
  - Encryption

Inherited Features

- CPACF
  - DES/TDES
  - SHA-1
- Crypto Express 2 (CEX2C)
  - RSA
  - PIN
  - DES/TDES
  - EMV2000

IBM System z9 109 (z9-109)

Enhancements

- TKE V5
  - Redbook SG24-7123
- AES-128
- PRNG
- SHA-256
- CKDS Sysplex Coherency
  - SYSPLEXCKDS(YES|NO,FAIL (YES|NO))
    - **SMF Record Type 82 (Subtype 21)**

IBM System z9 109 (z9-109)

IBM z9 BC

Enhancements

- Configure CEX2C/ CEX2A
- PKI Services
  - Become your own Certificate Authority
  - Exchange certificates and encryption keys
  - Provide secured path from client to server
- RACF and Vanguard products

IBM System z9 109 (z9-109)

zSeries and S/390 Crypto Hardware

Crypto Coprocessor Facility (CCF) $e_{mk}(k)$

PCI Crypto Coprocessor (PCICC) $e_{mk}(k)$

PCI Crypto Accelerator (PCICA)

CP Assist for Crypto Functions (CPACF)

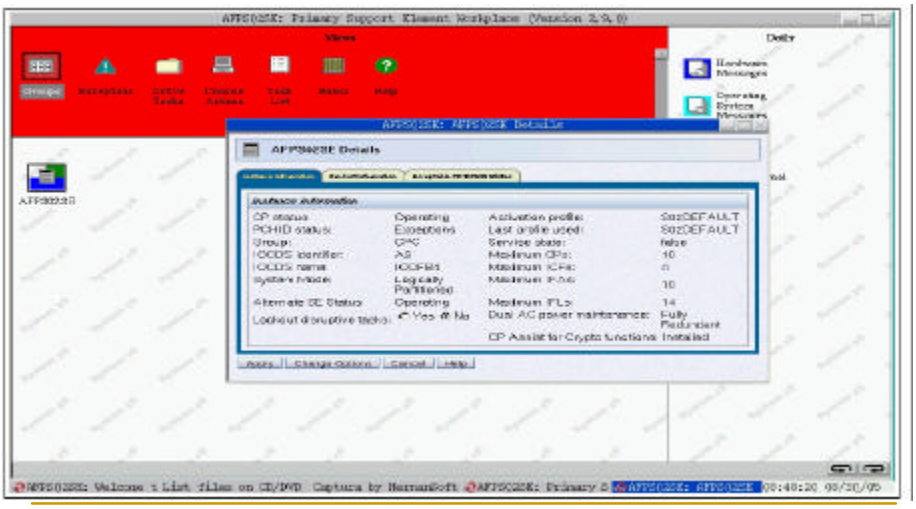
Crypto Express2 (CEX2) $e_{mk}(k)$

PCI X Cryptographic Coprocessor (PCIXCC) $e_{mk}(k)$

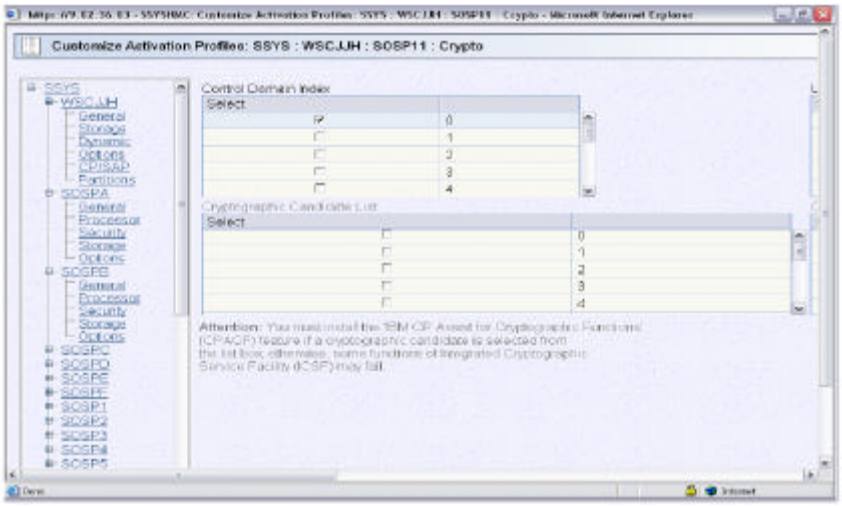
PCI Crypto Accelerator (PCICA)

Multiprise 2000, Multiprise 3000, 9672 G3-G6, z800/z900, z890/z990 z9-109

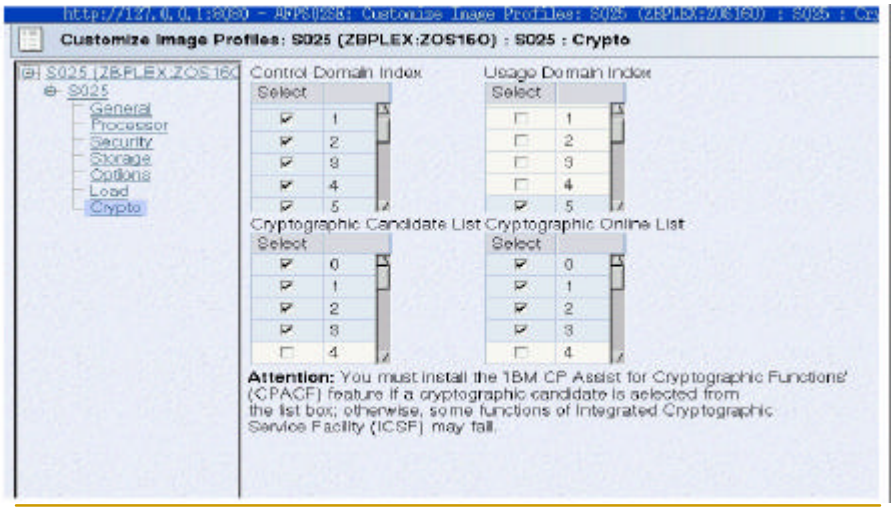
FC 3863 Installed



Crypto Definitions



Crypto Definitions



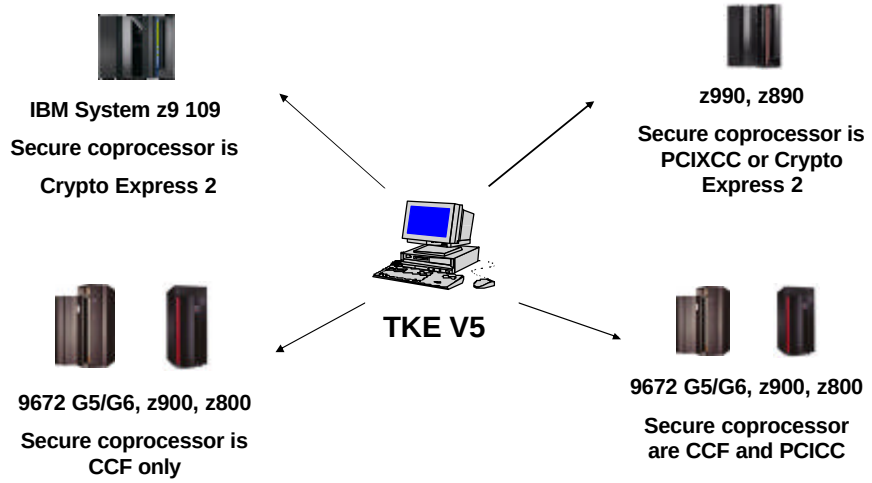
TKE (Trusted Key Entry) Workstation Overview

- Priced feature, designed for highly secure management of secure coprocessors Master Keys and operational keys
  - Optional Smart Card reader
  - Embedded closed OS
- Encrypted and signed communications over TCP/IP
  - Listener is ICSF
  - End point is the coprocessor
  - Every command is signed and encrypted
  - 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 (Trusted Key Entry) Access Control

- Access to secure cryptographic coprocessors is done through
  - Authorities (security officers) identified by their password and digital signature
  - Option to require multiple signatures before performing a crypto function
  - smart card support at TKE V4.2 and above
- 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 Support



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.
- 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.

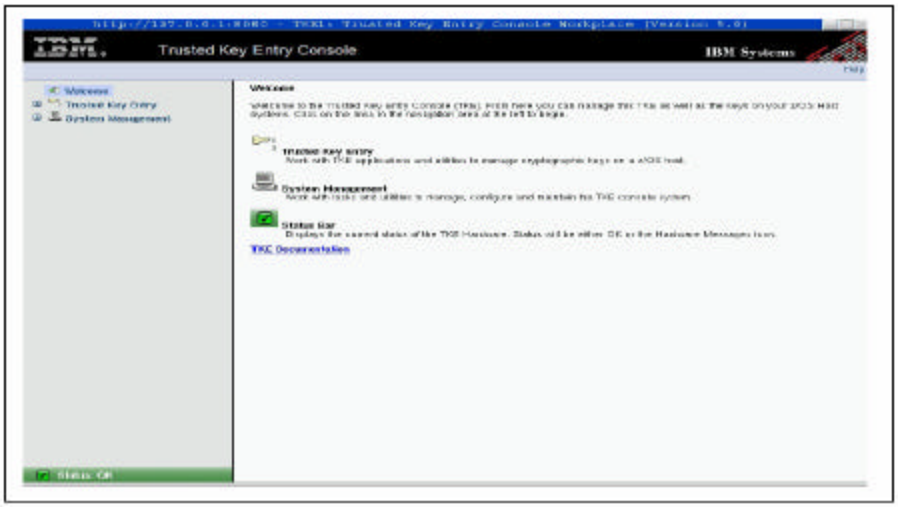
TKE (Trusted Key Entry) Version 5…

- 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 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.

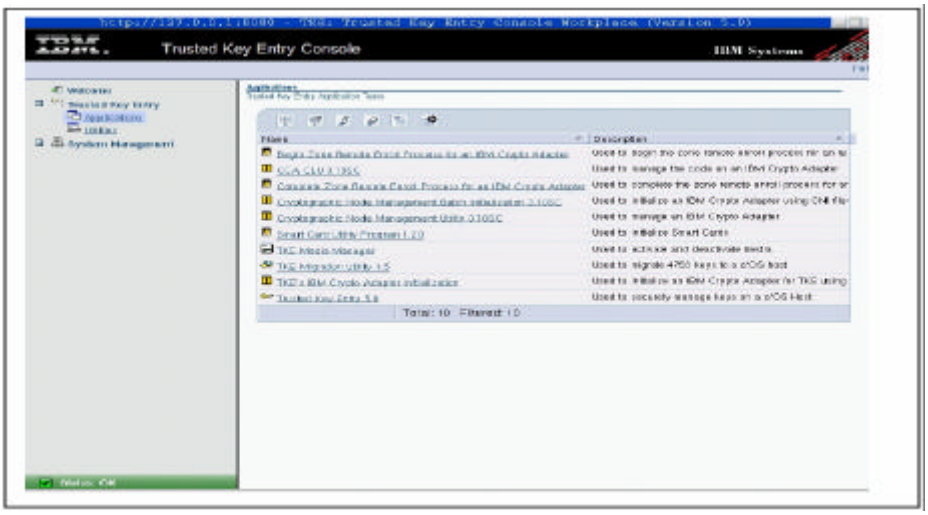
TKE (Trusted Key Entry) Version 5…

- Migrate TKE data from previous TKE versions
  - New task to be used to migrate TKE related data (Host.Dat, Group.Dat, 4758 roles and profiles, TCP/IP info, and emulator session information) from an existing TKE workstation to TKE 5.0.
  - Authority Signature Keys, master key parts, and operational key parts are not directly migrated but can manually be copied to diskette and then restored to the appropriate data directories using the TKE File Management Utility.

Trusted Key Entry



TKE



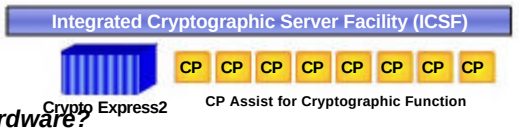
ICSF Customer Requests

- ISO16609 CBC TDES MAC
  - Strengthen data integrity
- Remote key loading for ATM's and POS
  - More flexible key management and privacy
- Secure key AES
- ANSI TR-31 Key block for DES key exchange

IBM System z9 109 (z9-109)

These are a sample of requests by customers. IBM makes no representation as to whether these requests will be addressed.

Mainframe Encryption



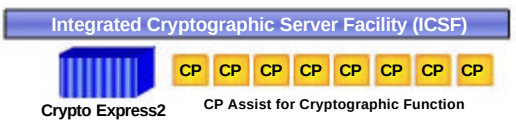
Why IBM Mainframe encryption hardware?

To accelerate encryption and provide Secure Key services

Secure Key

- For Secure Key exchanges
- Master keys in "tamper-resistant" package
- Dual control for Master Key management
- Important for banking functions
  - ✓ ATM support, Triple-DES, Trusted Key Entry
- Designed to comply with FIPS 140-2
- **CP Assist for Cryptographic Function (**z890, z990, z9-109)
- Support high levels of security for demanding applications
- Very high performance TDES, AES -128 (requires z9-109) and SHA-256 (requires z9-109)
  - ✓ SSL/TLS support

Mainframe Encryption



Why z/OS centralized key management?

- Over a decade of production use

Helps to protect and manage keys

- Support of encryption standards
- Generates keys
- Manage based on customer policies
- Provides key recovery capabilities
- Uses tamper resistant hardware for "secure keys"

Provides information for:

- Audit Compliance
- Management Controls
- Access Controls

Integrates with z/OS security features:

- z/OS Digital Certificate hosting services
  - Customer can be their own certificate authority
  - Identrus certified (z/OS 1.5)
- z/OS RACF for authorization, authentication

Additional Information

- http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100700
- http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS1666
- http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS1601
- Or http://www.ibm.com/support/techdocs
  - search on key words crypto

Questions