International Technical Support Organization

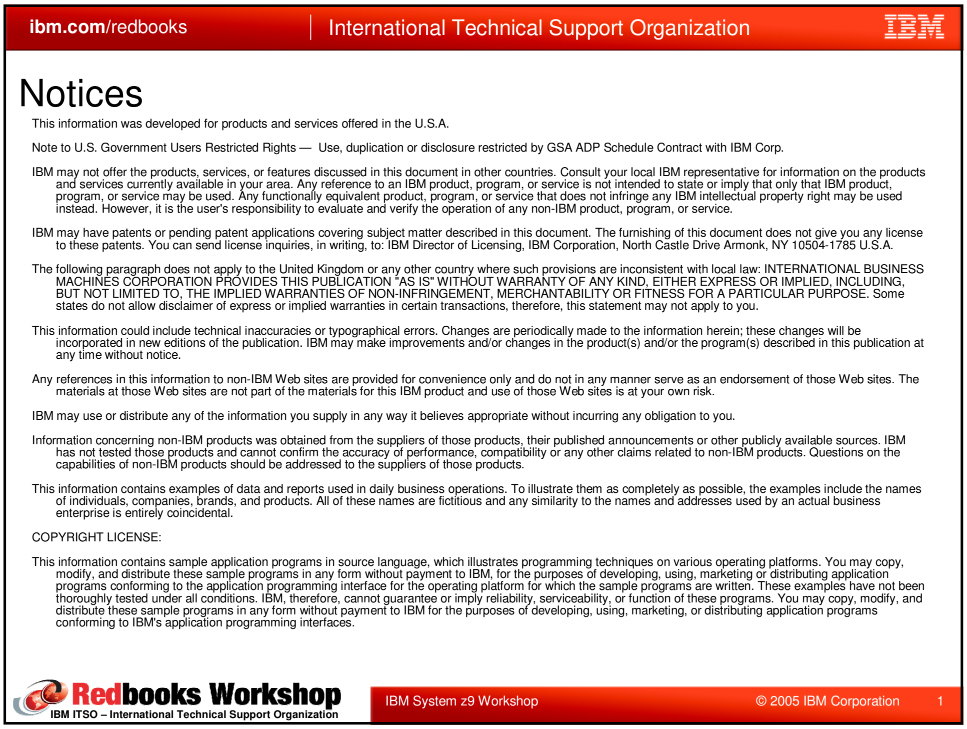
IBM System z9 - Cryptography

ibm.com/redbooks

Redbooks Workshop

IBM ITSO - International Technical Support Organization

IBM System z9 Workshop



ibm.com/redbooks | International Technical Support Organization

Notices

This information was developed for products and services offered in the U.S.A.

Note to U.S. Government Users Restricted Rights — Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

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.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of 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.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Redbooks Workshop IBM ITSO – International Technical Support Organization | IBM System z9 Workshop | © 2005 IBM Corporation | 1

ibm.com/redbooks | International Technical Support Organization

Positioning

Technical Details

Availability Enhancements

I/O growth solutions

I/O and Networking Enhancements

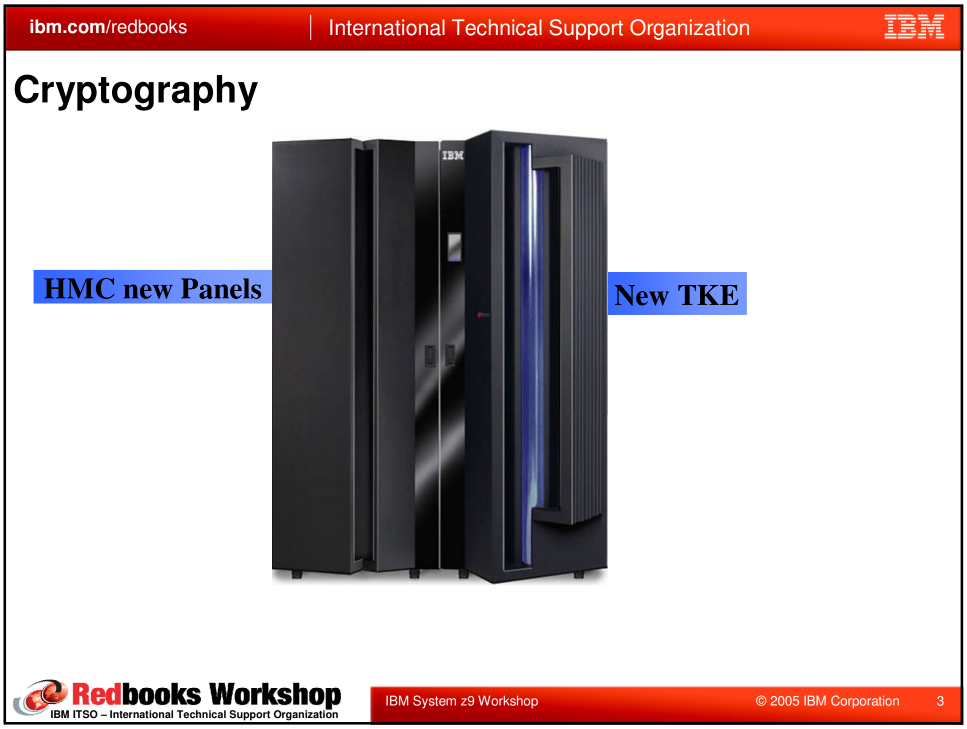
HMC/SE changes

LPAR Management

Cryptography

Redbooks Workshop
IBM ITSO – International Technical Support Organization

IBM System z9 Workshop © 2005 IBM Corporation 2



ibm.com/redbooks | International Technical Support Organization

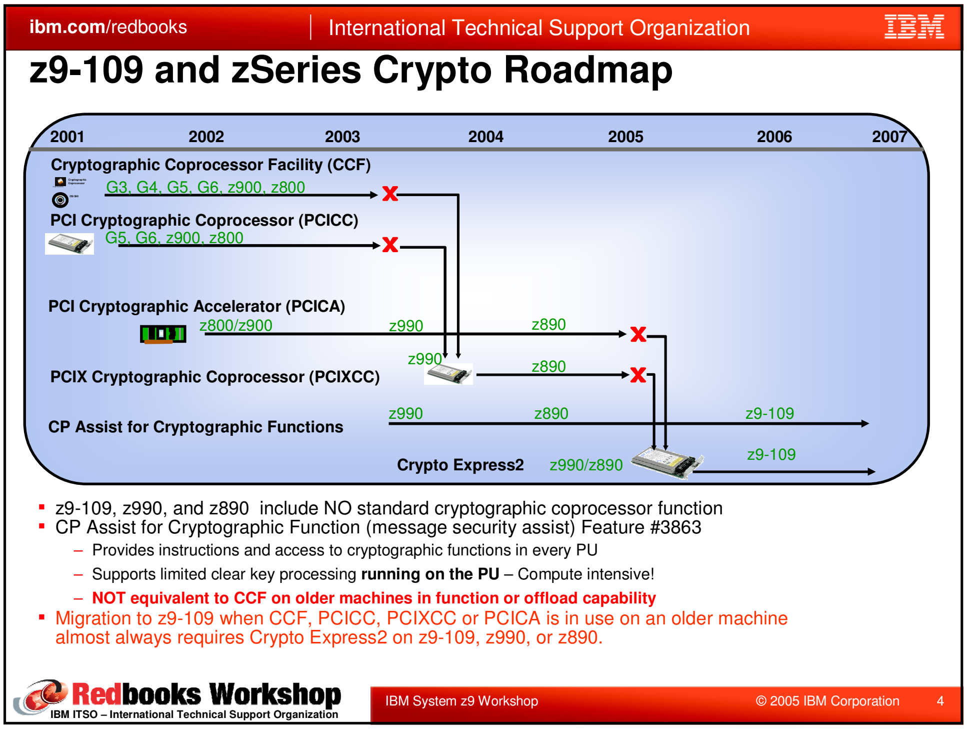
Cryptography

HMC new Panels

New TKE

Redbooks Workshop
IBM ITSO – International Technical Support Organization

IBM System z9 Workshop © 2005 IBM Corporation 3

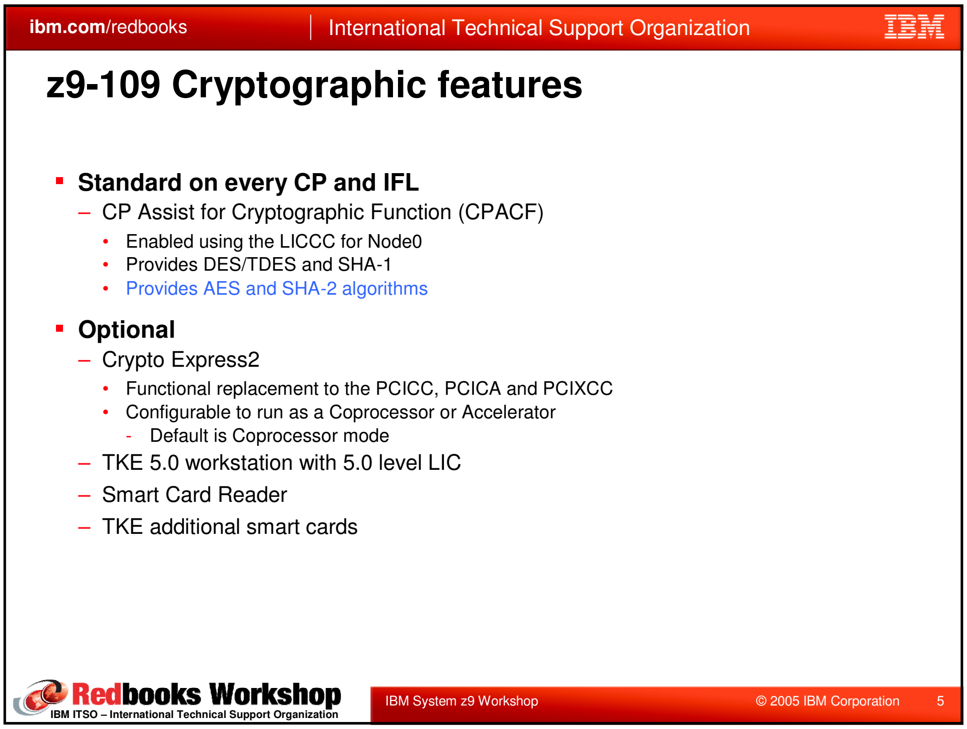


z9-109 and zSeries Crypto Roadmap

2001
2002
2003
2004
2005
2006
2007
Cryptographic Coprocessor Facility (CCF)
G3, G4, G5, G6, z900, z800
PCI Cryptographic Coprocessor (PCICC)
G5, G6, z900, z800
PCI Cryptographic Accelerator (PCICA)
z800/z900
z990
z890
PCIX Cryptographic Coprocessor (PCIXCC)
z990
z890
CP Assist for Cryptographic Functions
z990
z890
z9-109
Crypto Express2
z990/z890
z9-109

- z9-109, z990, and z890 include NO standard cryptographic coprocessor function
- CP Assist for Cryptographic Function (message security assist) Feature #3863
  - Provides instructions and access to cryptographic functions in every PU
  - Supports limited clear key processing **running on the PU** – Compute intensive!
  - **NOT equivalent to CCF on older machines in function or offload capability**
- Migration to z9-109 when CCF, PCICC, PCIXCC or PCICA is in use on an older machine almost always requires Crypto Express2 on z9-109, z990, or z890.

Redbooks Workshop
IBM ITSO – International Technical Support Organization

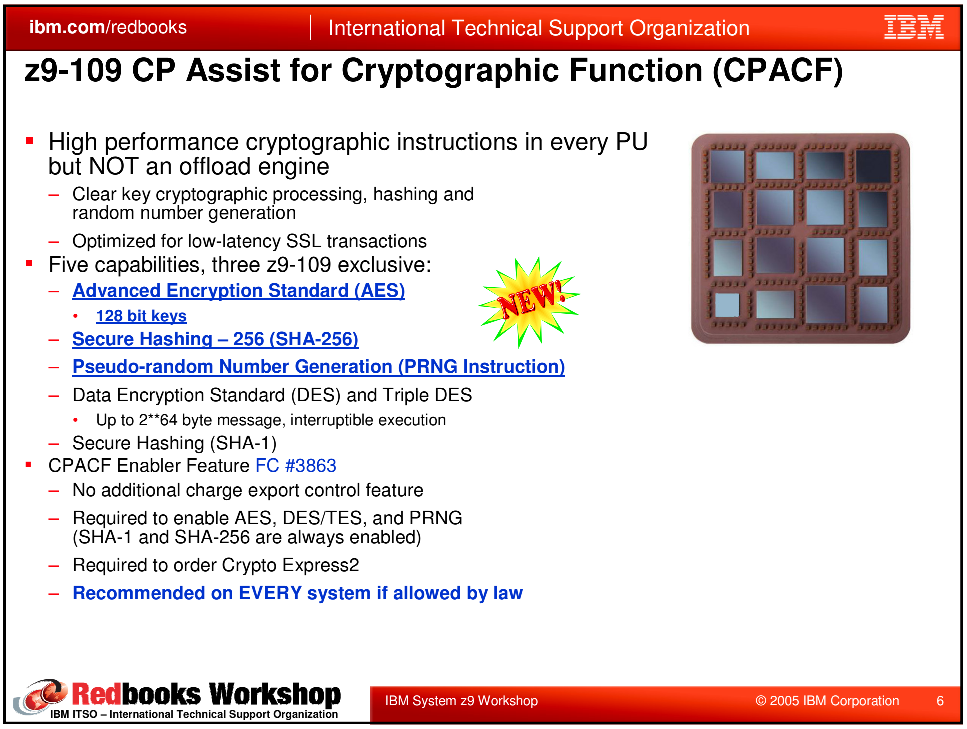


z9-109 Cryptographic features

- **Standard on every CP and IFL**
  - CP Assist for Cryptographic Function (CPACF)
    - Enabled using the LICCC for Node0
    - Provides DES/TDES and SHA-1
    - Provides AES and SHA-2 algorithms
- **Optional**
  - Crypto Express2
    - Functional replacement to the PCICC, PCICA and PCIXCC
    - Configurable to run as a Coprocessor or Accelerator
      - Default is Coprocessor mode
  - TKE 5.0 workstation with 5.0 level LIC
  - Smart Card Reader
  - TKE additional smart cards

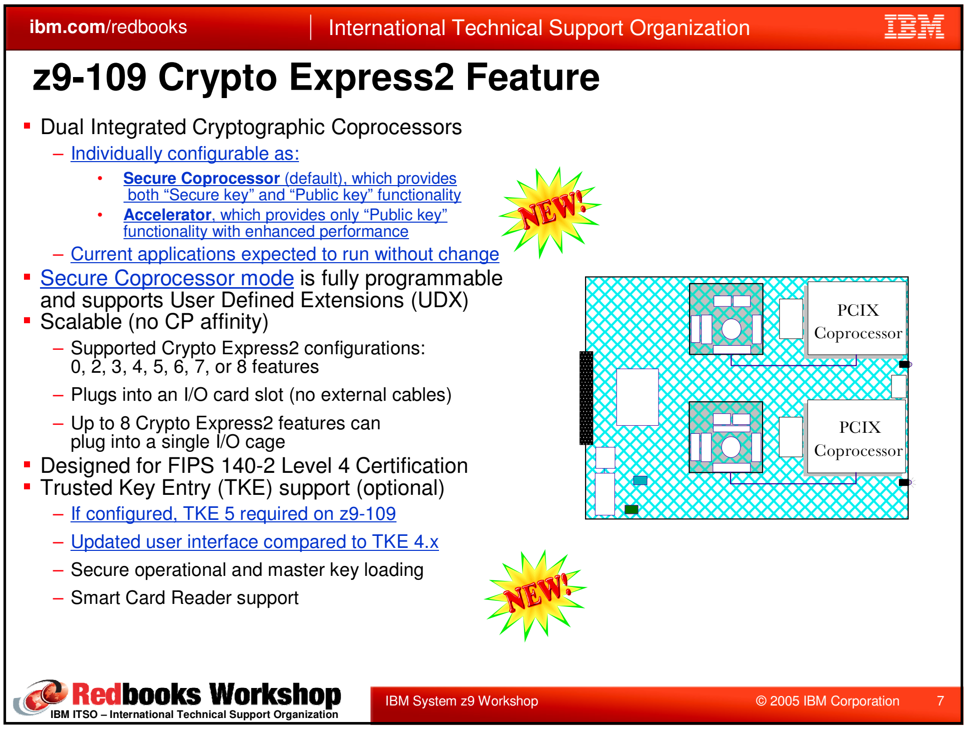
Redbooks Workshop
IBM ITSO – International Technical Support Organization

Redbooks Workshop
IBM ITSO - International Technical Support Organization



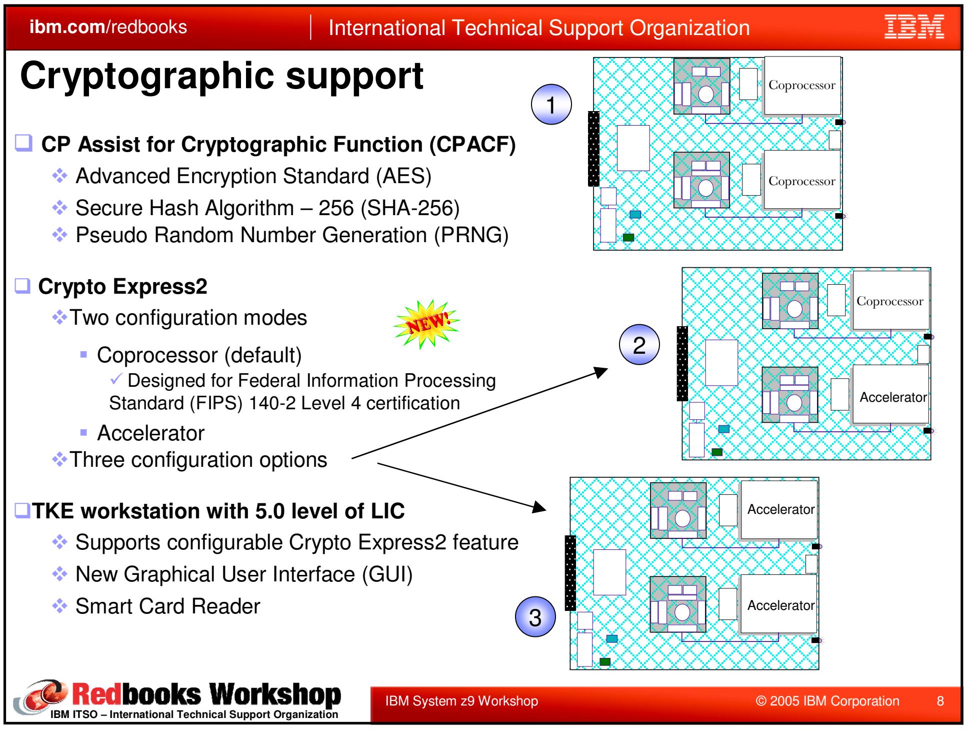
z9-109 CP Assist for Cryptographic Function (CPACF)

- High performance cryptographic instructions in every PU but NOT an offload engine
  - Clear key cryptographic processing, hashing and random number generation
  - Optimized for low-latency SSL transactions
- Five capabilities, three z9-109 exclusive:
  - Advanced Encryption Standard (AES)
    - 128 bit keys
  - Secure Hashing – 256 (SHA-256)
  - Pseudo-random Number Generation (PRNG Instruction)
  - Data Encryption Standard (DES) and Triple DES
    - Up to 2**64 byte message, interruptible execution
  - Secure Hashing (SHA-1)
- CPACF Enabler Feature FC #3863
  - No additional charge export control feature
  - Required to enable AES, DES/TES, and PRNG (SHA-1 and SHA-256 are always enabled)
  - Required to order Crypto Express2
  - **Recommended on EVERY system if allowed by law**



z9-109 Crypto Express2 Feature

- Dual Integrated Cryptographic Coprocessors
  - Individually configurable as:
    - **Secure Coprocessor** (default), which provides both "Secure key" and "Public key" functionality
    - **Accelerator**, which provides only "Public key" functionality with enhanced performance
  - Current applications expected to run without change
- Secure Coprocessor mode is fully programmable and supports User Defined Extensions (UDX)
- Scalable (no CP affinity)
  - Supported Crypto Express2 configurations: 0, 2, 3, 4, 5, 6, 7, or 8 features
  - Plugs into an I/O card slot (no external cables)
  - Up to 8 Crypto Express2 features can plug into a single I/O cage
- Designed for FIPS 140-2 Level 4 Certification
- Trusted Key Entry (TKE) support (optional)
  - If configured, TKE 5 required on z9-109
  - Updated user interface compared to TKE 4.x
  - Secure operational and master key loading
  - Smart Card Reader support

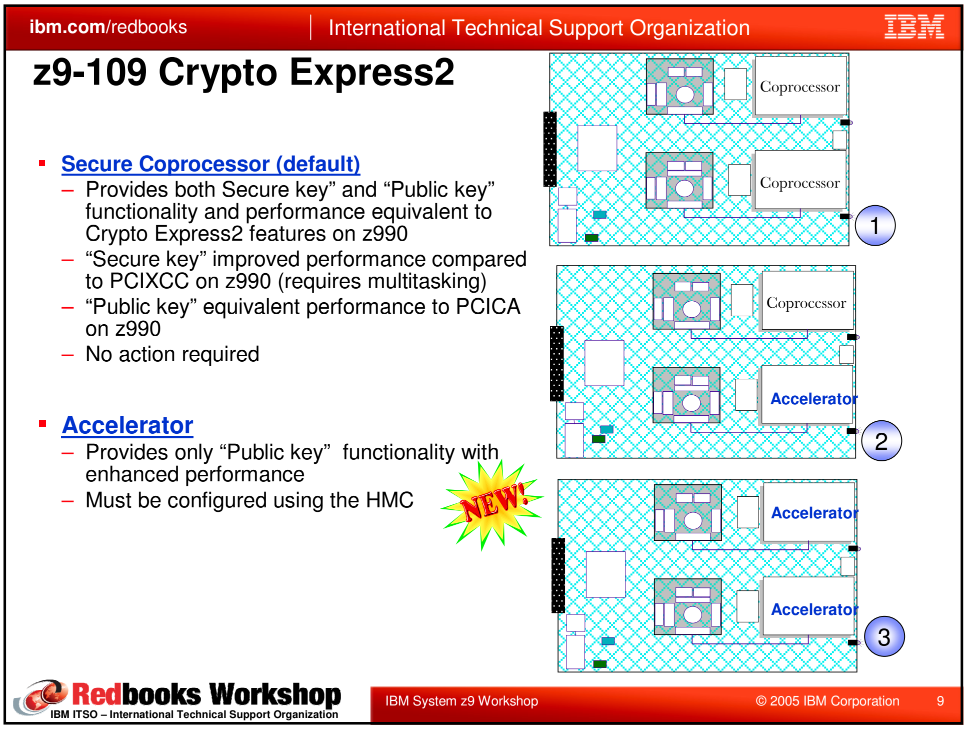


ibm.com/redbooks | International Technical Support Organization IBM

Cryptographic support

- ❑ **CP Assist for Cryptographic Function (CPACF)**
  - Advanced Encryption Standard (AES)
  - Secure Hash Algorithm – 256 (SHA-256)
  - Pseudo Random Number Generation (PRNG)
- ❑ **Crypto Express2**
  - Two configuration modes
    - Coprocessor (default)
      - ✓ Designed for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification
    - Accelerator
  - Three configuration options
- ❑ **TKE workstation with 5.0 level of LIC**
  - Supports configurable Crypto Express2 feature
  - New Graphical User Interface (GUI)
  - Smart Card Reader

Redbooks Workshop IBM ITSO – International Technical Support Organization | IBM System z9 Workshop | © 2005 IBM Corporation | 8

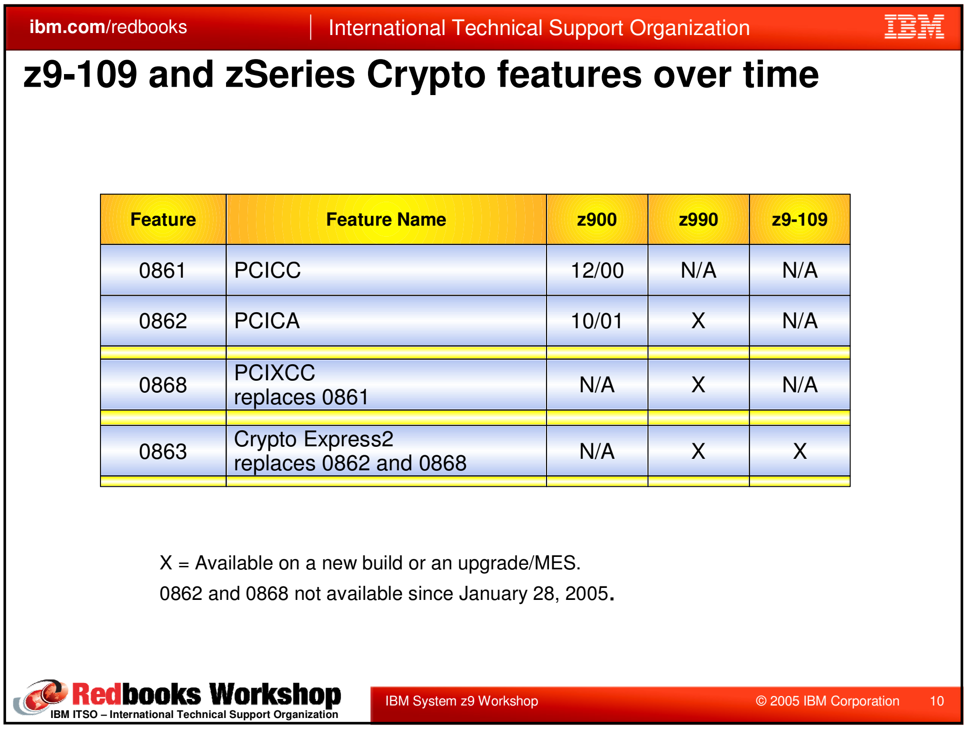


ibm.com/redbooks | International Technical Support Organization IBM

z9-109 Crypto Express2

- **Secure Coprocessor (default)**
  - Provides both Secure key" and "Public key" functionality and performance equivalent to Crypto Express2 features on z990
  - "Secure key" improved performance compared to PCIXCC on z990 (requires multitasking)
  - "Public key" equivalent performance to PCICA on z990
  - No action required
- **Accelerator**
  - Provides only "Public key" functionality with enhanced performance
  - Must be configured using the HMC

Redbooks Workshop IBM ITSO – International Technical Support Organization | IBM System z9 Workshop | © 2005 IBM Corporation | 9



ibm.com/redbooks | International Technical Support Organization IBM

z9-109 and zSeries Crypto features over time

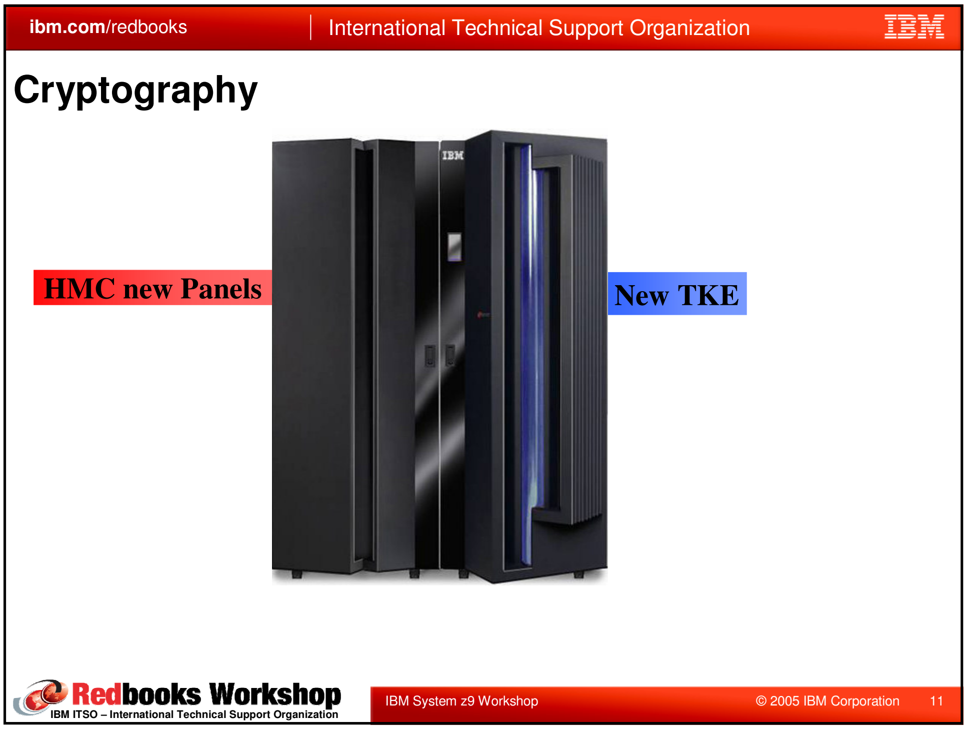
Feature	Feature Name	z900	z990	z9-109
0861	PCICC	12/00	N/A	N/A
0862	PCICA	10/01	X	N/A
0868	PCIXCC replaces 0861	N/A	X	N/A
0863	Crypto Express2 replaces 0862 and 0868	N/A	X	X

X = Available on a new build or an upgrade/MES.

0862 and 0868 not available since January 28, 2005.

Redbooks Workshop
IBM ITSO – International Technical Support Organization

IBM System z9 Workshop © 2005 IBM Corporation 10



ibm.com/redbooks | International Technical Support Organization IBM

Cryptography

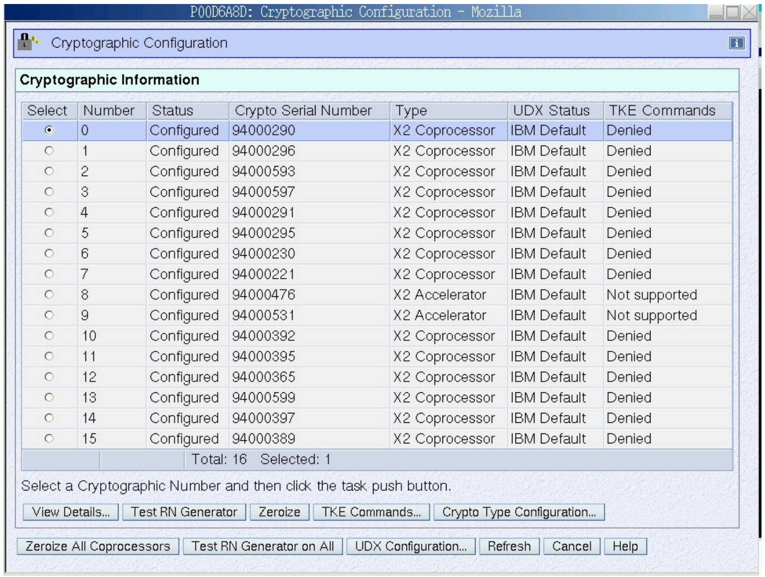
HMC new Panels

New TKE

Redbooks Workshop
IBM ITSO – International Technical Support Organization

IBM System z9 Workshop © 2005 IBM Corporation 11 ibm.com/redbooks | International Technical Support Organization IBM

Crypto Hw Configuration



P00D6A8D: Cryptographic Configuration - Mozilla

Cryptographic Configuration

Cryptographic Information

Select	Number	Status	Crypto Serial Number	Type	UDX Status	TKE Commands
●	0	Configured	94000290	X2 Coprocessor	IBM Default	Denied
○	1	Configured	94000296	X2 Coprocessor	IBM Default	Denied
○	2	Configured	94000593	X2 Coprocessor	IBM Default	Denied
○	3	Configured	94000597	X2 Coprocessor	IBM Default	Denied
○	4	Configured	94000291	X2 Coprocessor	IBM Default	Denied
○	5	Configured	94000295	X2 Coprocessor	IBM Default	Denied
○	6	Configured	94000230	X2 Coprocessor	IBM Default	Denied
○	7	Configured	94000221	X2 Coprocessor	IBM Default	Denied
○	8	Configured	94000476	X2 Accelerator	IBM Default	Not supported
○	9	Configured	94000531	X2 Accelerator	IBM Default	Not supported
○	10	Configured	94000392	X2 Coprocessor	IBM Default	Denied
○	11	Configured	94000395	X2 Coprocessor	IBM Default	Denied
○	12	Configured	94000365	X2 Coprocessor	IBM Default	Denied
○	13	Configured	94000599	X2 Coprocessor	IBM Default	Denied
○	14	Configured	94000397	X2 Coprocessor	IBM Default	Denied
○	15	Configured	94000389	X2 Coprocessor	IBM Default	Denied

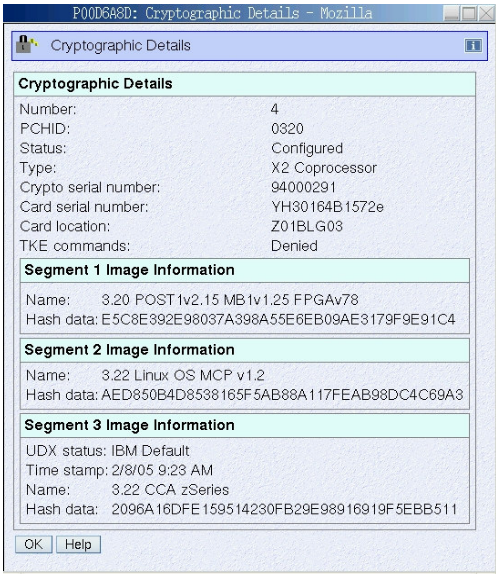
Total: 16 Selected: 1

Select a Cryptographic Number and then click the task push button.

Redbooks Workshop IBM ITSO – International Technical Support Organization | IBM System z9 Workshop © 2005 IBM Corporation 12

ibm.com/redbooks | International Technical Support Organization IBM

Cryptographic Details



P00D6A8D: Cryptographic Details - Mozilla

Cryptographic Details

Cryptographic Details

Number:	4
PCHID:	0320
Status:	Configured
Type:	X2 Coprocessor
Crypto serial number:	94000291
Card serial number:	YH30164B1572e
Card location:	Z01BLG03
TKE commands:	Denied

Segment 1 Image Information

Name: 3.20 POST1v2.15 MB1v1.25 FPGAv78
Hash data: E5C8E392E98037A398A55E6EB09AE3179F9E91C4

Segment 2 Image Information

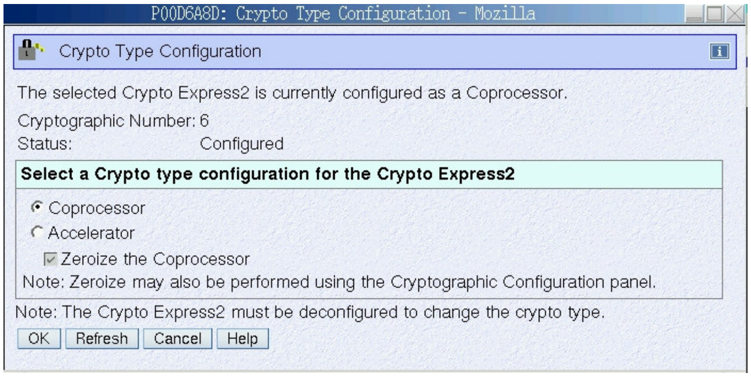
Name: 3.22 Linux OS MCP v1.2
Hash data: AED850B4D8538165F5AB88A117FEAB98DC4C69A3

Segment 3 Image Information

UDX status: IBM Default
Time stamp: 2/8/05 9:23 AM
Name: 3.22 CCA zSeries
Hash data: 2096A16DFE159514230FB29E98916919F5EBB511

Redbooks Workshop IBM ITSO – International Technical Support Organization | IBM System z9 Workshop © 2005 IBM Corporation 13

Crypto Type Configuration


P00D6A8D: Crypto Type Configuration - Mozilla
Crypto Type Configuration

The selected Crypto Express2 is currently configured as a Coprocessor.

Cryptographic Number: 6
Status: Configured

Select a Crypto type configuration for the Crypto Express2

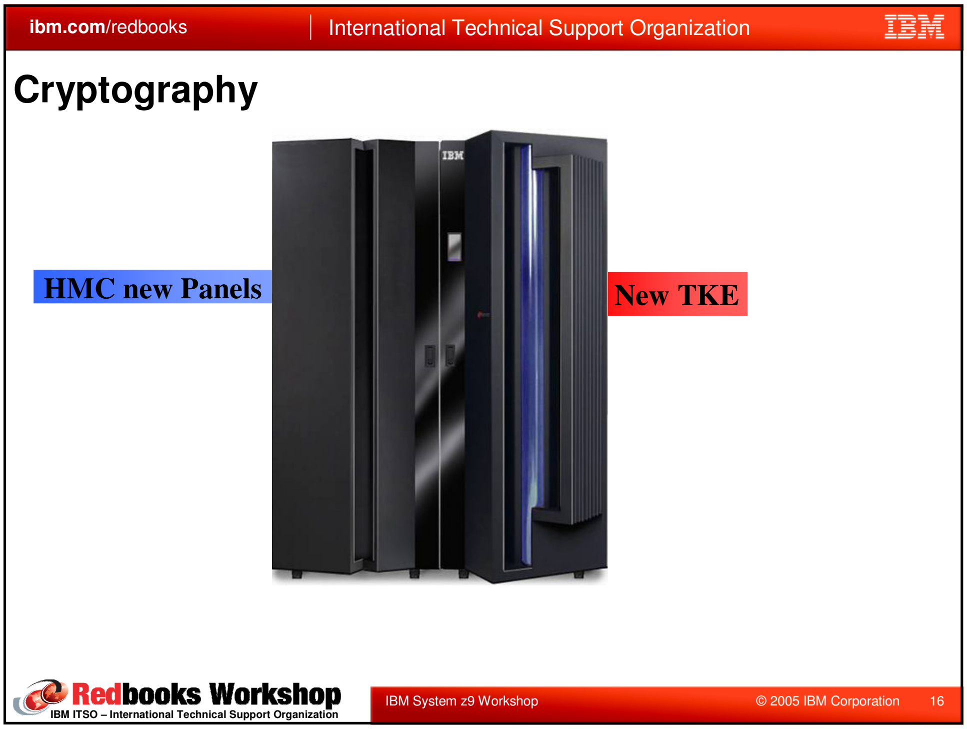
● Coprocessor
○ Accelerator
☑ Zeroize the Coprocessor
Note: Zeroize may also be performed using the Cryptographic Configuration panel.

Note: The Crypto Express2 must be deconfigured to change the crypto type.

z/OS Crypto Support

z/OS Release	Web Download	FMID	APAR	Comments
z/OS 1.4/1.5 (1.4 with z990 compatibility download or z990 exploitation feature)	09/2003, z990 Cryptographic Support	HCR770A	OA09157 OA11946	Co-Processor - okay No Accelerator
z/OS 1.4/1.5 (1.4 with z990 compatibility download or z990 exploitation feature)	05/2004, z990 and z890 Enhancements to Cryptographic Support	HCR770B	OA09157 OA11946	Co-Processor - okay No Accelerator
z/OS 1.6	05/2004, z990 and z890 Enhancements to Cryptographic Support Or 12/2004, ICSF 64-bit Virtual Support for z/OS 1.6 and z/OS.e 1.6	HCR770B	OA09157 OA11946	Co-Processor - okay No Accelerator
		HCR7720	OA11946	
z/OS 1.7	12/2004, ICSF 64-bit Virtual Support for z/OS 1.6 and z/OS.e 1.6	HCR7720	OA11946	Co-Processor - okay No Accelerator
z/OS V1.6 or V1.7	09/2005, Cryptographic Support for z/OS V1R6/R7 and z/OS.e V1R6/R7	HCR7730	All Included	Co-Processor - okay Accelerator - okay

- OA09157 = Co-Processor
  - Permits the use of the z9 Crypto Express2 Co-Processor as a z990/z890 Crypto Express2
- OA11946 = Accelerator toleration
  - When an Accelerator is defined, ICSF will abend without PTF for OA11946



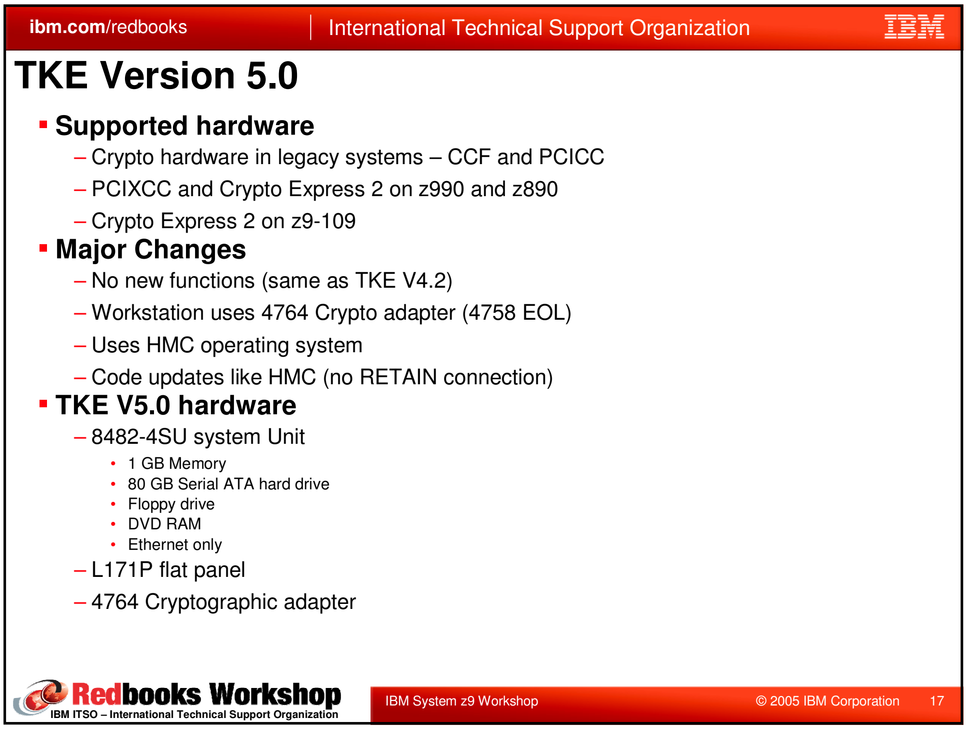
ibm.com/redbooks | International Technical Support Organization IBM

Cryptography

HMC new Panels

New TKE

Redbooks Workshop IBM ITSO – International Technical Support Organization | IBM System z9 Workshop | © 2005 IBM Corporation | 16

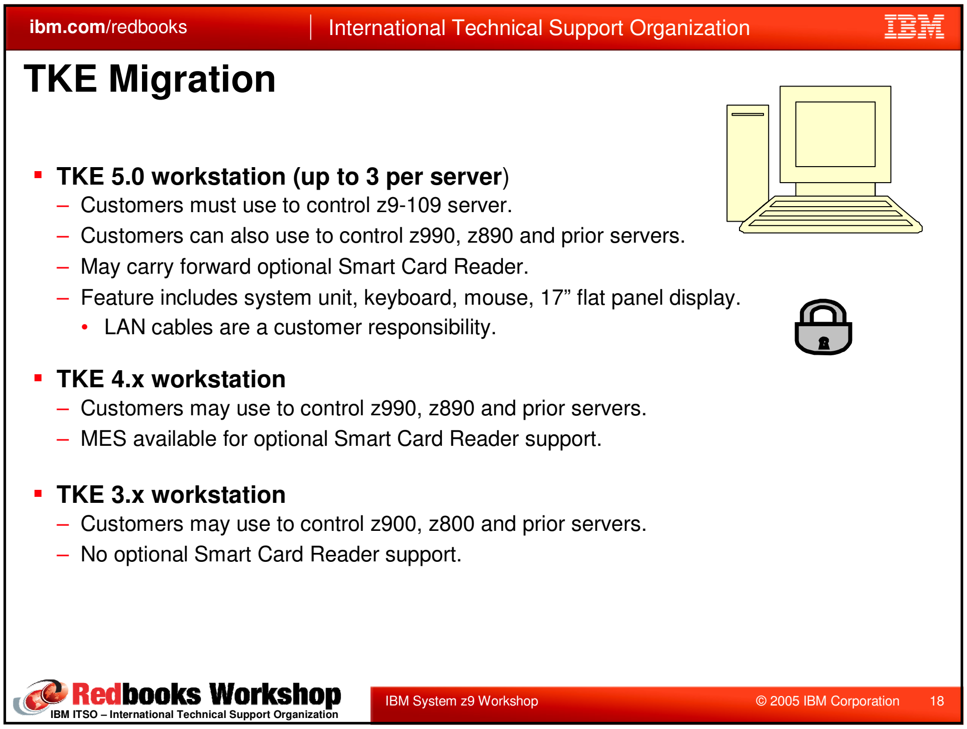


ibm.com/redbooks | International Technical Support Organization IBM

TKE Version 5.0

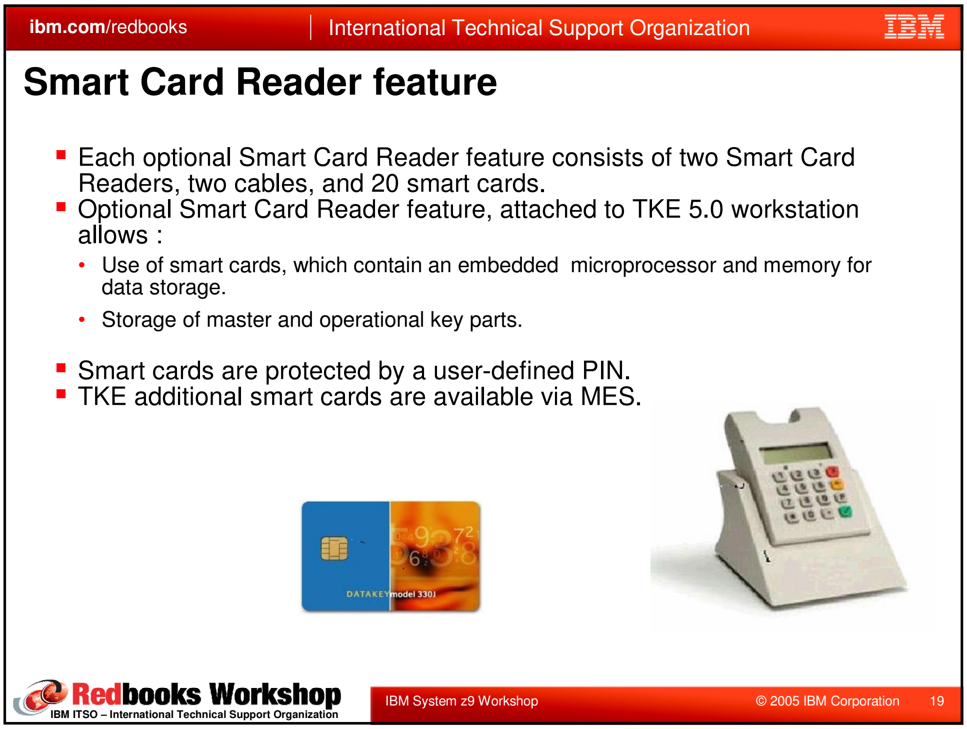
- **Supported hardware**
  - Crypto hardware in legacy systems – CCF and PCICC
  - PCIXCC and Crypto Express 2 on z990 and z890
  - Crypto Express 2 on z9-109
- **Major Changes**
  - No new functions (same as TKE V4.2)
  - Workstation uses 4764 Crypto adapter (4758 EOL)
  - Uses HMC operating system
  - Code updates like HMC (no RETAIN connection)
- **TKE V5.0 hardware**
  - 8482-4SU system Unit
    - 1 GB Memory
    - 80 GB Serial ATA hard drive
    - Floppy drive
    - DVD RAM
    - Ethernet only
  - L171P flat panel
  - 4764 Cryptographic adapter

Redbooks Workshop IBM ITSO – International Technical Support Organization | IBM System z9 Workshop | © 2005 IBM Corporation | 17



TKE Migration

- **TKE 5.0 workstation (up to 3 per server**)
  - Customers must use to control z9-109 server.
  - Customers can also use to control z990, z890 and prior servers.
  - May carry forward optional Smart Card Reader.
  - Feature includes system unit, keyboard, mouse, 17” flat panel display.
    - LAN cables are a customer responsibility.
- **TKE 4.x workstation**
  - Customers may use to control z990, z890 and prior servers.
  - MES available for optional Smart Card Reader support.
- **TKE 3.x workstation**
  - Customers may use to control z900, z800 and prior servers.
  - No optional Smart Card Reader support.



Smart Card Reader feature

- Each optional Smart Card Reader feature consists of two Smart Card Readers, two cables, and 20 smart cards.
- Optional Smart Card Reader feature, attached to TKE 5.0 workstation allows :
  - Use of smart cards, which contain an embedded microprocessor and memory for data storage.
  - Storage of master and operational key parts.
- Smart cards are protected by a user-defined PIN.
- TKE additional smart cards are available via MES.