



IBM

zSeries

## Vanguard Session J6

May 10, 2005

Ernie Nachtigall CISSP;CISA

IBM z890/z990 Cryptographic Update

**ON** DEMAND BUSINESS™

# Trademarks

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

AIX*	Database 2	e-business logo*	MVS	Resource Link
AIX/ESA*	DB2*	e(logo)server*	MVS/DFP	RMF
C/MVS	DB2 Connect	ESCON	MVS/ESA	S/390*
C/370	developerWorks*	FICON*	OS/2*	S/390 Parallel Enterprise Server
CICS*	DFSMS/MVS*	ibm.com*	OS/2 WARP*	WebSphere*
CICS/ESA*	DFSMSdfp	IBMLink	OS/390*Parallel Sysplex*	z/Architecture
CICS/MVS*	DFSMSdss	MQSeries*	Processor Resource/Systems Manager	z/OS*
COBOL/370	DFSMSHsm	Multiprise*	PR/SM	z/VM*
			RACF*	zSeries*

\* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Linux is a registered trademark of Linus Torvalds

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

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

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

\* 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.

## brief BIO

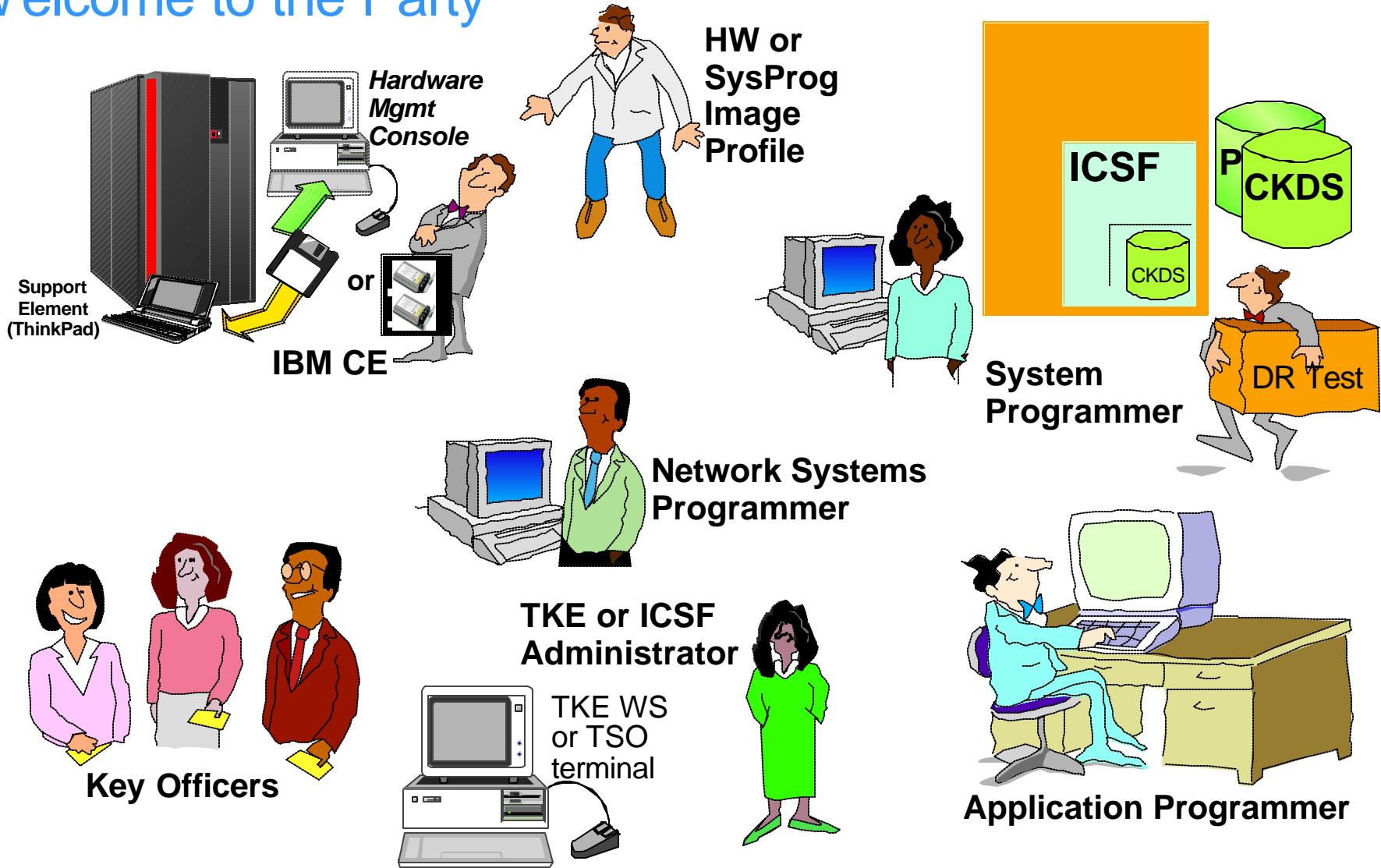
Ernest has been involved in the banking I/T area since 1970 and in cryptography since 1971.

He has been involved with or assisted in authoring teller, 3270, ABM, POS, CSPIN applications and is self-taught in COBOL;C;BASIC;PLI;PL/X and ASM.

Since 1988 he has been involved in the design, coding and support of various cryptographic implementations (IBM 3624, 4700, 4730, 4780, 4753, PCF, CUSP, ICSF, Racal/Zaxus/Thales, Atalla, Eracom).

Currently, he is the IBM Crypto Regional Designated Specialist for the Americas northern region and works closely with the Washington Systems Center security team.

# MainFrame Crypto Installation: Welcome to the Party



# S/390 and zSeries Crypto Solution

S/390 z800

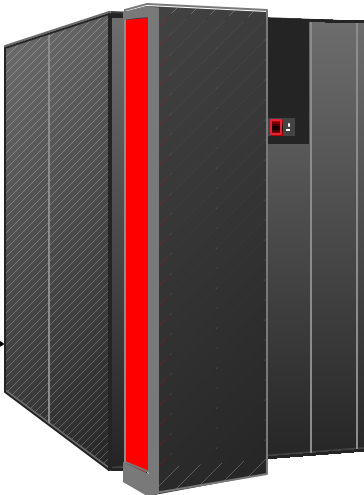
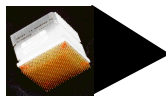
z890 z990

Peripheral z900

Component Interconnect  
Crypto Coprocessor  
PCICC/PCICA



Crypto Coprocessor Facility  
CCF



FC3863 CPACF  
clear key

PCICA

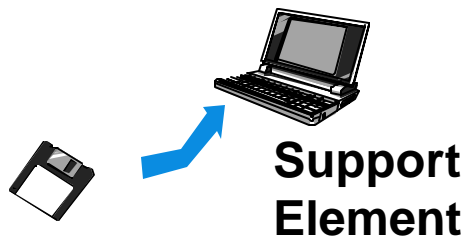


PCIXCC  
no PCICC



PCIXCC  
CEX2C  
z890 z990

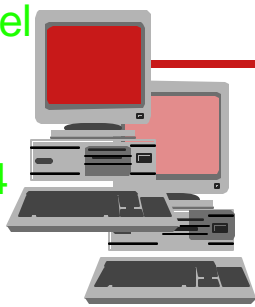
9672 Urged to z/OS Migrate



# TKE Support Based on ICSF Version Release

## TKE workstation V3

TKE code level 3.0  
 4758 card  
 OS/2 Warp 4  
 no Personal Security Card



TCP/IP



S/390 **G5-G6** with **PCICC**  
 ICSF 2.3 needed (OS/390 Rel.9)

S/390 - **G3 to G6** w/o **PCICC**  
 ICSF 2.1,2.2 (APAR needed) or  
 ICSF 2.3 (OS/390 2.9 or higher)

zSeries - **with or without PCICC**  
 z/OS ICSF  
 PCICA  
 All



## TKE workstation V4

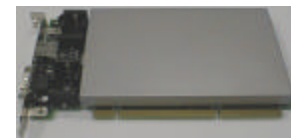
Trusted Key Entry  
 4758 Card



TCP/IP

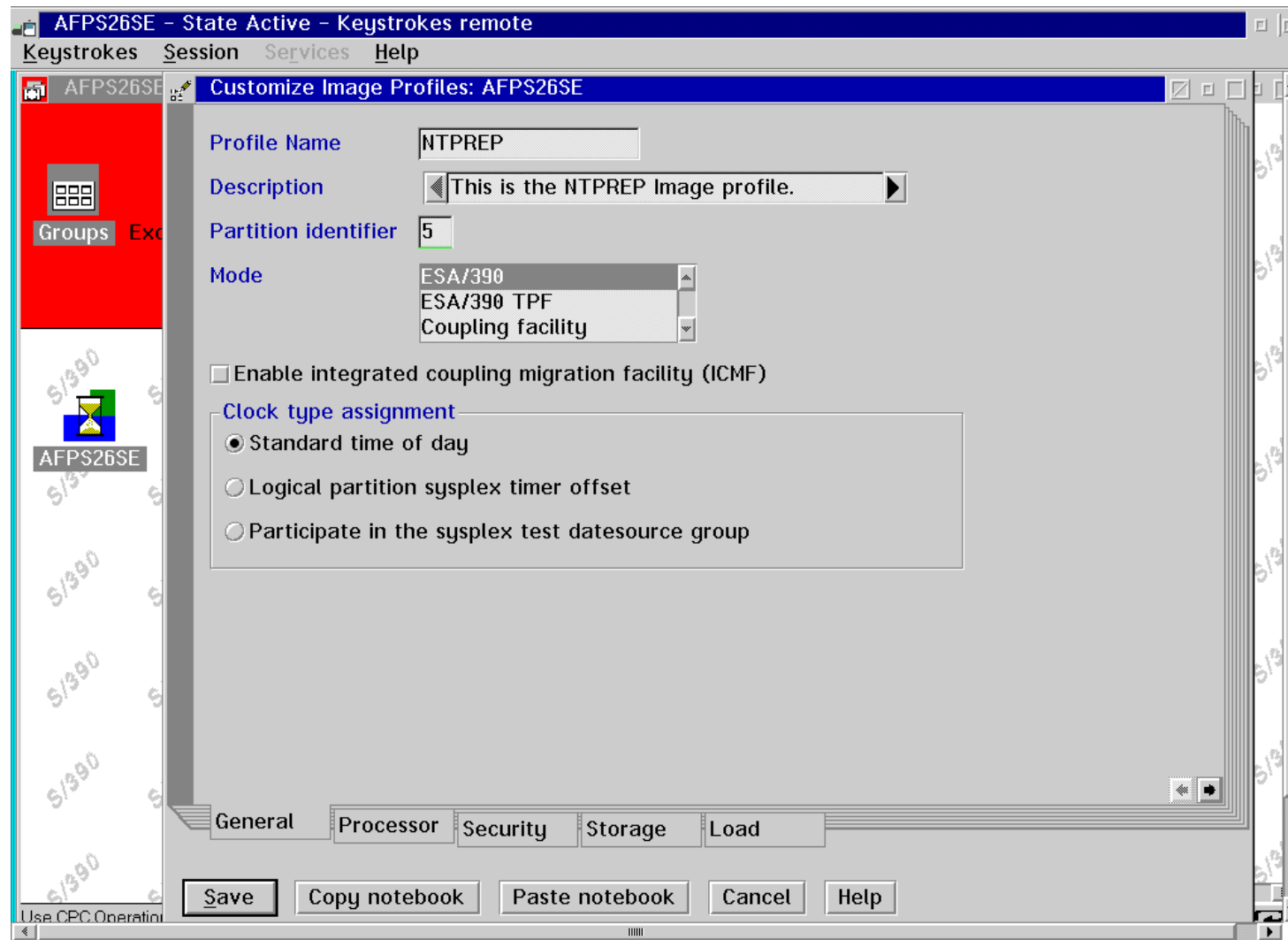


z890/z990 HCR770A HCR770B  
 HCR7720



PCIXCC  
 CEX2C  
 z890 z990  
**No weak keys**

# Profile Customization



Original chart provided courtesy of ITSO.

# CPACF Enabled

Instance information










CP Status:	<u>Operating</u>	Activation profile:	DEFAULT
CHPID Status:	Exceptions	Last used profile:	SCZP901
Group:	CPC	Service state:	Disabled
IOCDs identifier:	A3	Maximum CPs:	5
IOCDs name:	IODF12	Maximum IOCPs:	3

Lockout disruptive tasks:  Yes  No

System mode: Logically partitioned  
Alternate SE Status: Operating

**Dual AS power maintenance: Fully Redundant**  
**CP Assist for Cryptographic Functions: Installed**

Acceptable CP/CHPID status

<input checked="" type="checkbox"/> Operating - 	<input type="checkbox"/> Power save - 	<input type="checkbox"/> No power - 
<input type="checkbox"/> Not Operating - 	<input type="checkbox"/> Exceptions - 	<input type="checkbox"/> Status check - 
<input checked="" type="checkbox"/> Acceptable - 	<input type="checkbox"/> Service Required - 	<input type="checkbox"/> Degraded - 

Product information

Machine type / model:	002084 / A08-385	Manufacturer:	IBM
Machine serial:	02 - 0026A3A	CPC serial:	000020026A3A
Machine sequence:	00000026A3A	CPC location:	A19B
Plant of manufacture:	02	CPC identifier:	00

Save Change Options... Diagnose Reasons... Cancel Help



# LPAR DEFINITION PCI TAB

Customize Image Profiles: P00CSIM2

Control domain index: 00, 01, 02, 03, 04, 05

Usage domain index: 00, 01, 02, 03, 04, 05

PCI Cryptographic Candidate List: 00, 01, 02, 03, 04, 05

PCI Cryptographic Online List: 00, 01, 02, 03, 04, 05

Attention: You must install the "IBM CP Assist for Cryptographic Functions" (CPACF) feature if a PCI Cryptographic Candidate is selected from the list box; otherwise, some functions of Integrated Cryptographic Service Facility (ICSF) may fail.

General Processor Security Storage Options Load PCI Crypto

Save Copy notebook Paste notebook Cancel Help

## PCIXCC - Feature Code 0868

- Provides secure functions for
  - ▶ Symmetric DES, T-DES encryption/decryption
  - ▶ Message authentication, hashing
  - ▶ PIN processing
  - ▶ RSA asymmetric encryption/decryption and digital signature, + clear key RSA
  - ▶ Key generation and management, random number generation
  - ▶ EMV support
  - ▶ 4753 support
  - ▶ User Defined Extension (UDX) – Built under contract by IBM or approved third party vendor
- Exploited by
  - ▶ z/OS CCF and PCICC exploiters (support rolled back to OS/390 2.10)
- One “card” can be shared by up to 16 LPARs
- FC3863 must be installed
- Replaced by Crypto Express2 feature in January 2005

## PCICA - Feature Code 0862

- Same feature as in z900/z800
  - ▶ Clear key RSA operations only
  - ▶ Very high throughput for RSA asymmetric encryption/decryption of a symmetric key
    - As performed in the SSL handshake – 2000+ SSL handshakes/sec per feature (1024bit key)
  - ▶ RSA digital signature generation and verification
- Exploited by
  - ▶ z/OS System SSL
- One “card” can be shared by up to 16 LPARs
- FC3863 must be installed
- Replaced by Crypto Express2 feature in January 2005

## Crypto Express2 - Feature Code 0863 (+ APAR OA09157 on HCR770A and HCR770B)

- Dual Integrated Cryptographic Coprocessors
  - ▶ Provides PCIXCC and PCICA functionality
- Improved throughput over the PCIXCC
- 0 to 8 features in a system
  - ▶ The total number of Crypto Express2, PCICA and PCIXCC features cannot exceed 8 features per server
- All Crypto Express2 features can plug in a single I/O cage without restrictions
- Current applications expected to run without change
- Fully programmable, User Defined Extensions (UDX) support
- Designed for FIPS 140-2 Level 4 Certification
- FC 3863 must be installed
- Replaces PCIXCC and PCICA on January 2005
- A Crypto Express2 “card” can be shared by up to 16 LPARs

**HCR770A ----- Integrated Cryptographic Service Facility-----**

**OPTION ==>**

**Enter the number of the desired option.**

- 1 COPROCESSOR MGMT - Management of Cryptographic Coprocessors**
- 2 MASTER KEY - Master key set or change, CKDS/PKDS Processing**
- 3 OPSTAT - Installation options**
- 4 ADMINCNTL - Administrative Control Functions**
- 5 UTILITY - ICSF Utilities**
- 6 PPINIT - Pass Phrase Master Key/CKDS Initialization**
- 7 TKE - TKE Master and Operational Key processing**
- 8 KGUP - Key Generator Utility processes**
- 9 UDX MGMT - Management of User Defined Extensions**

**Licensed Materials - Property of IBM**

**5694-A01 (C) Copyright IBM Corp. 1989, 2003. All rights reserved.**

**US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.**

**Press ENTER to go to the selected option**

----- ICSF Coprocessor Management ----- Row 1 to 6 of 6  
COMMAND ==> SCROLL ==> PAGE

Select the coprocessors to be processed and press ENTER.  
Action characters are: A, D, E, **K**, R and S. See the help panel for details.

COPROCESSOR	SERIAL NUMBER	STATUS
-----	-----	-----
. A00		ACTIVE
. A01		ACTIVE
. A02		ACTIVE
. A03		ACTIVE
. <b>E04</b>	<b>93002173</b>	<b>ACTIVE</b>
. <b>F05</b>	<b>93002184</b>	<b>ACTIVE</b>
. X06	93001166	ACTIVE
. X07	93001449	ACTIVE
***** Bottom of data *****		

**COMMAND ==>**

The Coprocessor Management panel displays the status of all cryptographic coprocessors installed. Select the coprocessors to be processed.

<b>Prefix</b>	<b>Type of cryptographic coprocessor</b>	<b>Valid action characters</b>
-----	-----	-----
<b>A</b>	PCI Cryptographic Accelerator	a, d
<b>E</b>	<b>Crypto Express2 Coprocessor</b>	<b>a, d, e, k, r, s</b>
<b>F</b>	<b>Crypto Express2 Coprocessor</b>	<b>a, d</b>
<b>X</b>	PCI X Cryptographic Coprocessor	a, d, e, r, s

Action characters: (entered on the left of the coprocessor number)

- 'a' Makes available a coprocessor previously deactivated by a 'd'.
- 'd' Makes a coprocessor unavailable.
- 'e' Selects the PCIXCC/**CEX2C** for clear master key entry.
- 'k' **Selects the PCIXCC/CEX2C for DES operational key load.**
- 'r' Causes the PCIXCC/**CEX2C** default role to be displayed.
- 's' Causes complete hardware status to be displayed for an PCIXCC/**CEX2C**.

The action character 'e' can not be combined with any other action characters.

**The action character 'k' may be specified on only one coprocessor.**

**F3 = END HELP**

## Rerleases and Web Downloadables

Operating System	Level Shipped in Base Product	Level Required for Clear Key Support	Level Required for Secure Key Support	Level Required for Enhanced Secure Key Support	Level Required for 64-bit addressing caller support
OS/390 2.10	HCR7703	HCR770A <sup>1</sup>	HCR770A <sup>1</sup>	HCR770B <sup>4</sup>	N/A
z/OS 1.2	HCR7704	HCR770A <sup>1</sup>	HCR770A <sup>1</sup>	HCR770B <sup>4</sup>	N/A
z/OS 1.3 or z/OS.e 1.3	HCR7706	HCR7708 <sup>2</sup> or HCR770A <sup>1</sup>	HCR770A <sup>1</sup>	HCR770B <sup>4</sup>	N/A
z/OS 1.4 or z/OS.e 1.4	HCR7706 or HCR7708 <sup>6</sup>	HCR7708 <sup>3</sup>	HCR770A <sup>1</sup>	HCR770B <sup>4</sup>	N/A
z/OS 1.5 or z/OS.e 1.5	HCR7708	HCR7708	HCR770A <sup>1</sup>	HCR770B <sup>4</sup>	N/A
z/OS 1.6 or z/OS.e 1.6	HCR770A	HCR770A	HCR770A	HCR770B <sup>4</sup>	HCR7720 <sup>5</sup>

1. HCR770A is shipped in the z990 Cryptographic Support web deliverable.
2. HCR7708 is shipped in the z990 Cryptographic CP Assist Support for z/OS V1.3 web deliverable.
3. HCR7708 is shipped in both the z/OS V1R4 z990 Compatibility Feature and the z/OS V1R4 z990 Exploitation Feature.
4. HCR770B is shipped in the z990 and z890 Enhancements to Cryptographic Support web deliverable.
5. HCR7720 is shipped in the ICSF 64-bit Virtual Support for z/OS V1R6 and z/OS.e V1R6 Web deliverable (planned to be available December 2004).
6. HCR7708 is shipped in the z/OS V1R4 z990 Exploitation Support Feature. After February 24, 2004 this feature became mandatory for all new z/OS V1R4 orders



## WEB Downloads

- <http://www-1.ibm.com/servers/eserver/zseries/zos/downloads/>
- <http://www-1.ibm.com/support/docview.wss?uid=tss1flash10236&aid=1>

## ICSF FMID HCR770B Overview

- Integrated circuit card (ICC) applications
  - ▶ Financial institutions require smart card support to implement applications for smart cards
- Callable services enhancements
  - ▶ EMV2000 Integrated Circuit Card specification
  - ▶ VISA Integrated Circuit Card specification
- Financial services
  - ▶ Derived unique key per transaction for double-length PIN encrypting keys
    - ANSI X9.24-2002 Retail Financial Services specification
  - ▶ American Express card security code
    - Generation and validation
- DES operational key entry for z990
- Other enhancements

## ICC Applications

- EMV2000 Integrated Circuit Card specification
  - ▶ Support session key generation algorithms
  - ▶ Diversified Key Generate (CSNBDKG) will support new keywords for session key generation
    - TDES-XOR, TDESEMV2, TDESEMV4
- VISA Integrated Circuit Card specification
  - ▶ PIN Change/Unblock (CSNBPCU)
    - new service
    - supports the VISA PIN change algorithms
    - supports the EMV2000 session key generation

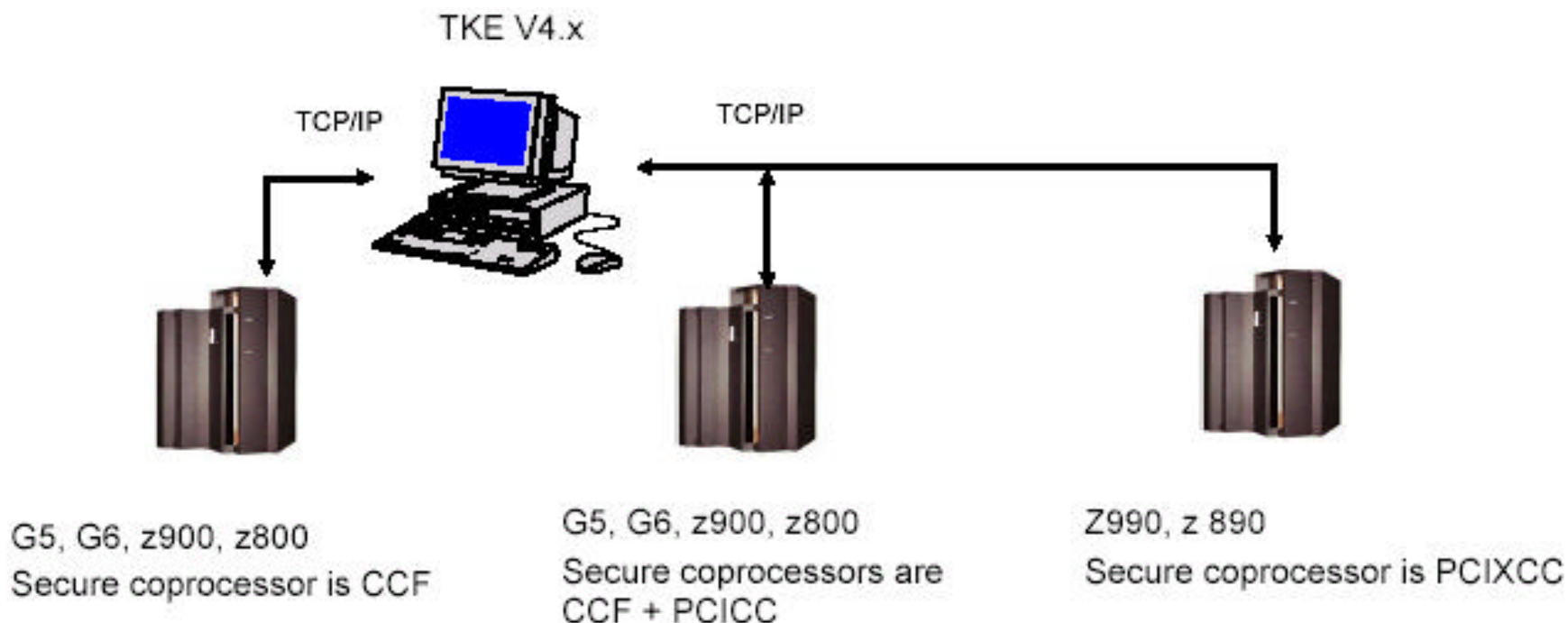
## Financial Services

- ANSI X9.24-2002 Retail Financial Services
  - ▶ support the double-length derived unique key per transaction algorithm
  - ▶ Encrypted PIN Translate (CSNBPTR) and Encrypted PIN verify (CSNBPVR)
- Transaction Validation (CSNBTRV)
  - ▶ new callable service
  - ▶ generates and validates American Express card security codes

## Trusted Key Entry (TKE) Workstation

TKE V4.0 required to support PCIXCC – at V4.2 as of Oct 29, 2004

- Brand new TKE is hdw FC 0886 (Ethernet) or 0889 (T/R)
- Can use TKE V3.x (G5, G6 or zSeries) – order TKE code CD
- TKE V4.2 LIC is FC **0853**



## Operational Key Entry

- Operational Key Entry - TKE
  - ▶ Any key type
  - ▶ User defined control vectors
  - ▶ Single, double and triple key lengths
- Operational Key Entry – TSO Panels
  - ▶ New TSO panel to load operational keys from PCIXCC
    - Simple, only key label required
  - ▶ NOCV KEK support

## HCR770B - Deliverable

- z990 and z890 Enhancements to Cryptographic Support
- Available as a web deliverable 2Q04
  - ▶ Available for OS/390 V2R10, z/OS V1R2, V1R3, V1R4.2 and V1R5
  - ▶ Available for z/OS V1R6
  - ▶ HCR7720 supersedes HCR770B supersedes HCR770A
- Hardware requirements: z990/z890 with May 2004 version of Licensed Internal Code

## Other Enhancements in HCR770B

- ZERO-PAD format processing for PKA Decrypt (CSNDPKD)
  - ▶ Only external (clear) RSA private keys supported
- MRP format processing for PKA Encrypt (CSNDPKE)
  - ▶ Same as ZERO-PAD formatting with even public exponent allowed
- TSO panels
  - ▶ Copy key value from Check Sum and Verification Pattern panel to Clear Master Key Entry panel
- KGUP
  - ▶ Double-length MAC and MACVER keys



## Other Enhancements in HCR770B

- ICSF Query Facility (CSFIQF) is a new service
  - ▶ Returns status information about ICSF
  - ▶ Export control information of a coprocessor
  - ▶ Diagnostic information of a coprocessor
  - ▶ Will execute on any system
  - ▶ ICSF Query Facility callable service will run on any processor
- PCICA utilization will be included in WLM Usage and Delay reports

## Cryptographic functions announced October 7, 2004 HCR7720

- 19-digit Personal Account Numbers (PANs) - PCIXCC, Crypto Express2
  - ▶ Designed to meeting the industry standard for Card Validation Value (CVV)
  - ▶ Designed to increase antifraud security
  - ▶ Previously supported 13-digit and 16-digit PANs
  - ▶ Exclusive to z890 and z990
- Less than 512-bit clear key RSA operations - PCIXCC, Crypto Express2
  - ▶ Designed to allow clear key RSA operations using keys less than 512-bits
  - ▶ Digital Signature Verify (CSNDDSV), Public Key Encrypt (CSNDPKE), and Public Key Decrypt (CSNDPKD).
  - ▶ Allows the migration of some additional cryptographic applications without rewriting the applications.
- **64-bit API support (System SSL)**

## Cryptographic functions announced October 7, 2004

- 2048-bit key (clear and secure) RSA operations - PCICC, PCIXCC, Crypto Express2
  - ▶ New for PCICC on z800, z900 (Previously supported up to 1024-bit keys)
  - ▶ The 2048-bit functional control vector will support four ICSF services: Public Key Decrypt, Symmetric Key Import, Export, and Generate
  - ▶ Standard for PCIXCC (as of 9/2003) and Crypto Express2 on z890, z990
- Supports new Automated Teller Machine (ATM) standards
  - ▶ Designed to increase antifraud security
- TKE 4.2 workstation with smart card reader support - G6 and zSeries servers
- Optional feature providing support for generating and storing key parts and key pairs
- Trusted Key Entry (TKE) 4.2 workstation is used by: CCF, PCICC, PCIXCC, and Crypto Express2
  - ▶ Available October 29, 2004

## May 2004 LIC

- PCIX Cryptographic Coprocessor (PCIXCC)
  - ▶ Derived Unique Key Per Transaction (DUKPT)
    - Added triple DES support (double length keys)
- Europay Mastercard and VISA (EMV) 2000 standard support
  - ▶ Diversified key generate enhancements
    - Session keys for secure messaging for PINs
    - Session keys for secure messaging for keys using SESS-XOR scheme
    - Session keys for all applicable EMV key types using the EMV 2000 Annex A1.3.1 derivation scheme
- Trusted Key Entry (TKE) enablement
  - ▶ Default setting is disabled
- PCIXCC and PCI Cryptographic Accelerator (PCICA)
  - ▶ Public Key Decrypt/Public Key Encrypt (PKD/PKE) enhancements
    - PKE Mod Raised to Power (MRP) support
    - PKD zero pad support
- All of the above functions are supported by the new Crypto Express2 feature

## APAR OA08172

- Clear key tokens in the ICSF CKDS
  - ▶ Key Token Build can build tokens
  - ▶ Key Record Write can write tokens
  - ▶ Key Record Read can not read tokens (unless SUP/KEY0)
  - ▶ CSNBSYD - Symmetric Decipher
  - ▶ CSNBSYE - Symmetric Encipher
- KGUP support
- Designed for fast DES CPACF access (via ICSF API CSNBSYD and CSNBSYE)
  - ▶ Updates to IBM Data Encryption for IMS and DB2 Databases
- Allows centralized storage of CPACF tokens within the ICSF CKDS
- **Recommend RACF protection of Key Label especially for shared CKDS with other systems**

## Availability of Crypto offerings

Announced October 7, 2004	Available PCICC z900, z800	Available PCIXCC z990, z890	Available Crypto Express2 z990, z890	Description
Crypto Express2	---	---	Jan. 28, 2005	Combines functions of PCICA and PCIXCC in one feature
19-digit PANs	Not applicable	Oct. 29, 2004	Jan. 28, 2005	Instead of 13 or 16-digit Personal Account Numbers (PANs) Card Validation Value (CVV) generation and verification services
Less than 512-bit clear key RSA operations	Currently available	Oct. 29, 2004	Jan. 28, 2005	Before only supported applications <u>above</u> 511 bits
2048-bit key (clear and secure) RSA operations	Oct. 29, 2004	Currently available	Jan. 28, 2005	New feature #0867 on PCICC. Integrated in PCIXCC and Crypto Express2 at introduction.

## CRYPTO FMIDs

Operating System	Level Shipped in Base Product	Level Required for Clear Key Support	Level Required for Secure Key Support	Level Required for Enhanced Secure Key Support	Level Required for 64-bit addressing caller support
OS/390 2.10	HCR7703	HCR770A <sup>1</sup>	HCR770A <sup>1</sup>	HCR770B <sup>4</sup>	n/a
z/OS 1.2	HCR7704	HCR770A <sup>1</sup>	HCR770A <sup>1</sup>	HCR770B <sup>4</sup>	n/a
z/OS 1.3 z/OS.e1.3	HCR7706	HCR7708 <sup>2</sup> or HCR770A <sup>1</sup>	HCR770A <sup>1</sup>	HCR770B <sup>4</sup>	n/a
z/OS 1.4 z/OS.e 1.4	HCR7706 or HCR7708 <sup>6</sup>	HCR7708 <sup>3</sup> or HCR770A	HCR770A <sup>1</sup>	HCR770B <sup>4</sup>	n/a
z/OS 1.5 z/OS.e 1.5	HCR7708	HCR7708	HCR770A <sup>1</sup>	HCR770B <sup>4</sup>	n/a
z/OS 1.6 z/OS.e 1.6	HCR770A	HCR770A	HCR770A	HCR770B <sup>4</sup>	HCR7720 <sup>5</sup>

- 1) HCR770A is shipped in the z990 Cryptographic Support web deliverable - no longer available
- 2) HCR7708 is shipped in the z990 Cryptographic CP Assist Support for z/OS 1.3 web deliverable - no longer available
- 3) HCR7708 is shipped in both the z/OS V1R4 z990 Compatibility Support feature (no longer orderable) or z/OS V1R4 z990 Exploitation Support feature
- 4) HCR770B is shipped in the z990 & z890 Enhancements to Cryptographic Support web deliverable
- 5) HCR7720 is shipped in ICSF 64-bit Virtual Support for z/OS 1.6 & z/OS.e 1.6
- 6) HCR7708 is shipped in the z/OS V1R4 z990 Exploitation Support feature



# Questions?

