IBM *e*server zSeries and Total Storage Update (zSTSU)

What is Crypto Hardware?

IBM Advanced Technical Support

Trademarks

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

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

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Linux is a registered trademark of Linus Torvalds
Penguin (Tux) compliments of Larry Ewing
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.
Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

MasterCard is a registered trademark of MasterCard International
RSA BSAFE is a registered trademark of RSA Data Security
RSA is a registered trademark of RSA Inc.
Visa is a register trademark of Visa international

* 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.

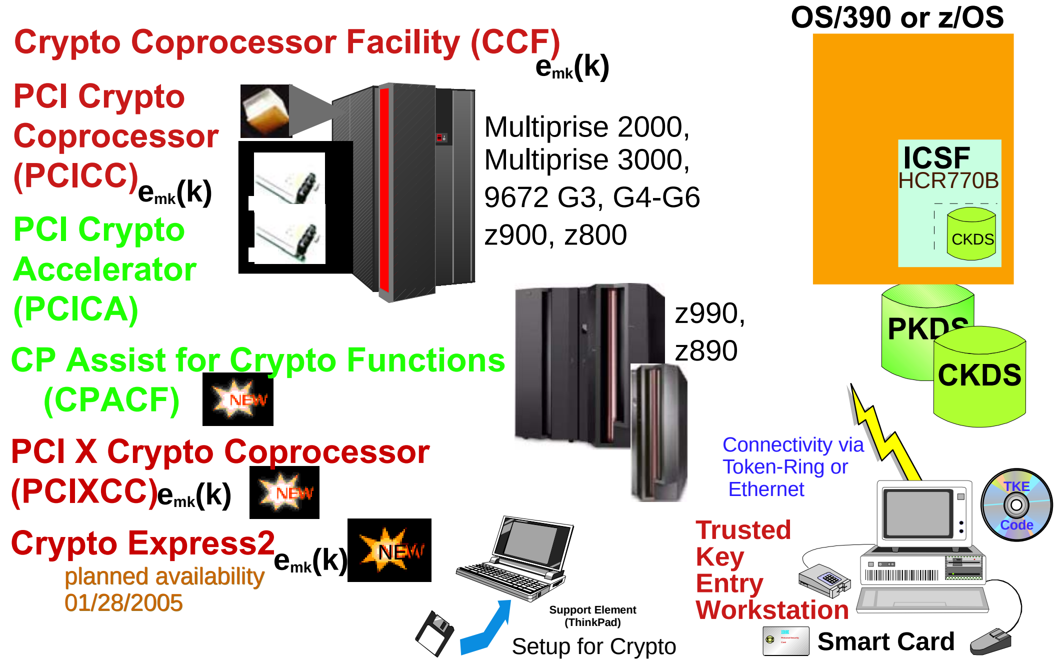
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available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

IBM zSeries Crypto Environment



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

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

PCI Crypto Accelerator (PCICA)

CP Assist for Crypto Functions (CPACF) NEW

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

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

planned availability 01/28/2005

Multiprise 2000, Multiprise 3000, 9672 G3, G4-G6 z900, z800

z990, z890

OS/390 or z/OS

ICSF HCR770B

CKDS

PKDS

CKDS

Connectivity via Token-Ring or Ethernet

Trusted Key Entry Workstation

Smart Card

Support Element (ThinkPad)

Setup for Crypto

IBM zSeries Crypto Basic Facts to Understand

- Built on the IBM Common Cryptographic Architecture (CCA)
  - Describes the connection between crypto hardware and the software interfaces using it
  - Describes the crypto key structure and its connection to the remaining components, software and hardware
- CCA described in IBM Systems Journal
  - IBM SYSTEMS JOURNAL, VOL 30, NO 2, 1991
- Provides
  - Foundation for key structure and key management
  - Consist structure for application requests that can be used across IBM platforms supporting CCA designed hardware
- Initial CCA defined a base of 18 application programming interfaces (APIs)

http://www-3.ibm.com/security/cryptocards/pdfs/CCA_Basic_Services_241_Revised_20030918.pdf

IBM zSeries Crypto Basic Facts to Understand . . .

- Application programming interface used dictates the crypto hardware feature used to execute it, for instance,
  - CSNBENC, will only work on CCF or PCIXCC
  - CSNBSYE naming AES as the algorithm will work on CCF and CPACF, however, when DES is the named algorithm it will only work on CPACF and fail on CCF.
- To understand the use and function of IBM Cryptography, one must understand
  - Crypto technology, i.e., do reading and understand concepts
  - Any unique industry crypto requirements
  - IBM Common Crypto Architecture
  - Applications - high level understanding
  - IBM Crypto features

IBM zSeries Crypto Basic Facts to Understand . . .

- Status of zSeries Crypto hardware can be found by
  - z/OS 1.5 CSFICQ API results
  - CCVT, however, this data area is limited as a customer defined programming interface (i.e., only those fields defined as part of the programming interface can be depended on for consistency and should be used)
    - CCVTDACC
    - CCVTCCVE
    - CCVTPRPC
    - CCVTINST
    - CCVTINS2
    - CCVTLNTH
    - CCVT_FMID
    - CCVT_USERPARM

    - CCVTDACC
    - CCVTCCVE
    - CCVTHFLG
    - CCVTPRPC
    - CCVTINST
    - CCVTINS2
    - CCVTLNTH
    - CCVT_FMID
    - CCVT_USERPARM

CCVTHFLG Flag bytes.

Bit	Meaning When Set On
0	Crypto assist available.
1	Add'l secure Crypto device available.
2	Support for 64-bit callers.
3-7	Reserved.

  - For those ISVs and others who used CCVTSFG1, this is not a defined programming interface and not reliable

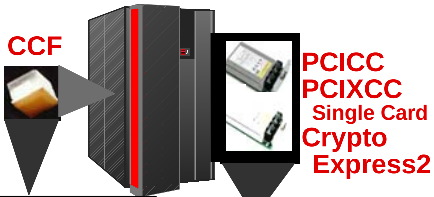
IBM zSeries Crypto Basic Facts to Understand . . .

- CCA described in IBM Systems Journal
  - IBM SYSTEMS JOURNAL, VOL 30, NO 2, 1991
- ICSF => only method to send requests to hardware
  - Handles directing requests to **appropriate** hardware
  - Provides the CCA Application Programming Interface (API) to the hardware
  - Supplied base interface for cryptographic key entry
  - ICSF documentation to read before each install or upgrade
    - Latest level of ICSF System Programmer's Guide
      - ✓ Appendix: z990 and z890 with a PCI X Cryptographic Coprocessor
      - ✓ Appendix: z990 and z890 without a PCI X Cryptographic Coprocessor
      - ✓ Chapter on Migration from Previous Releases of ICSF
      - ✓ Summary of changes
    - Latest level of ICSF Application Programmer's Guide
      - ✓ Same Appendices
      - ✓ Summary of changes

IBM zSeries Crypto Basic Facts to Understand . . .

- CCA deals with primarily with secure keys
  - Exceptions are
    - ENCODE and DECODE APIs for support of older crypto implementations
    - AES, which is an algorithm implementation not included in CCA
    - RSA functions using keys not stored in the CCA Key Data Set will use clear key values but those values must be in acceptable CCA structure
    - RSA private keys stored within secure PCI devices will use the clear key values only within those secure devices
  - Key values entered in the clear are imported into the CCA structure and converted to protection under master key

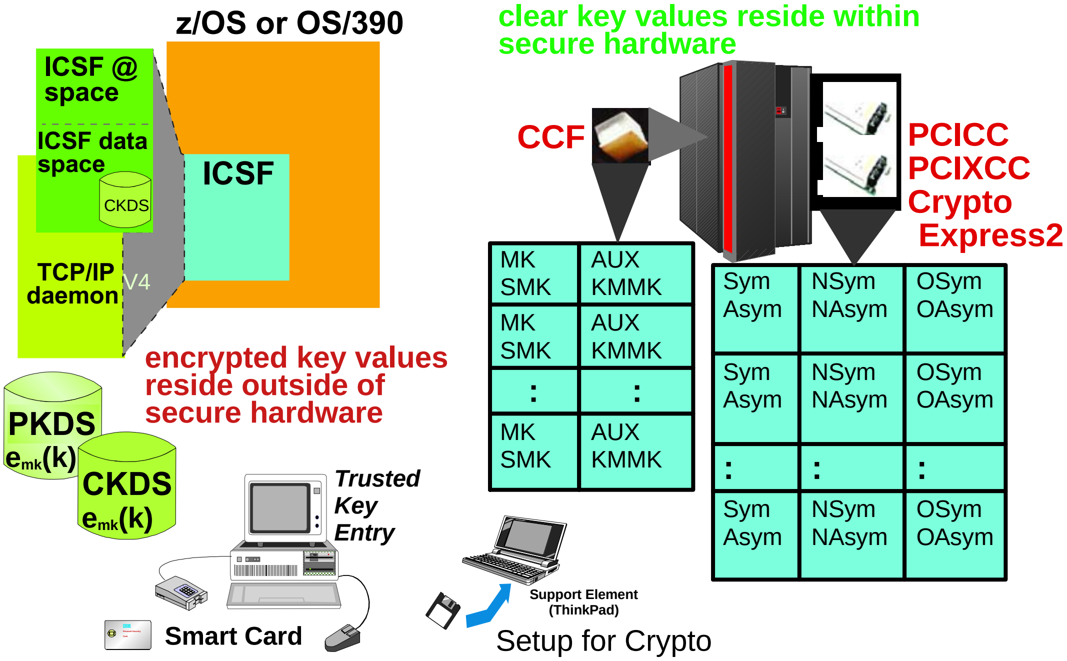
all clear key values reside within secure hardware



MK SMK	AUX KMMK
MK SMK	AUX KMMK
:	:
MK SMK	AUX KMMK

Sym Asym	NSym NAsym	OSym OAsym
Sym Asym	NSym NAsym	OSym OAsym
:	:	:
Sym Asym	NSym NAsym	OSym OAsym

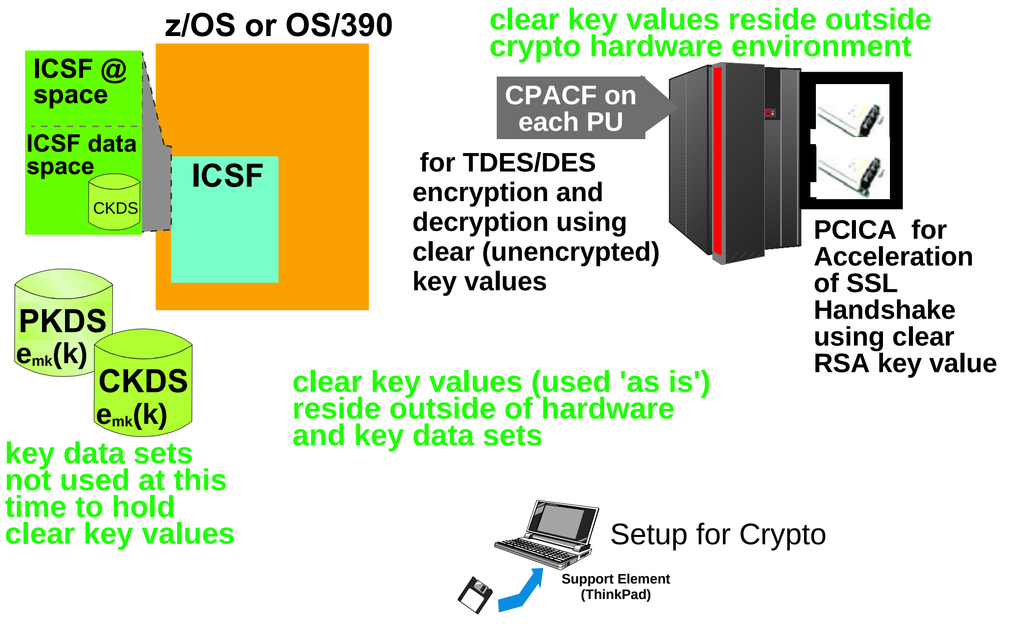
IBM zSeries and S/390 Secure Key Crypto Solution



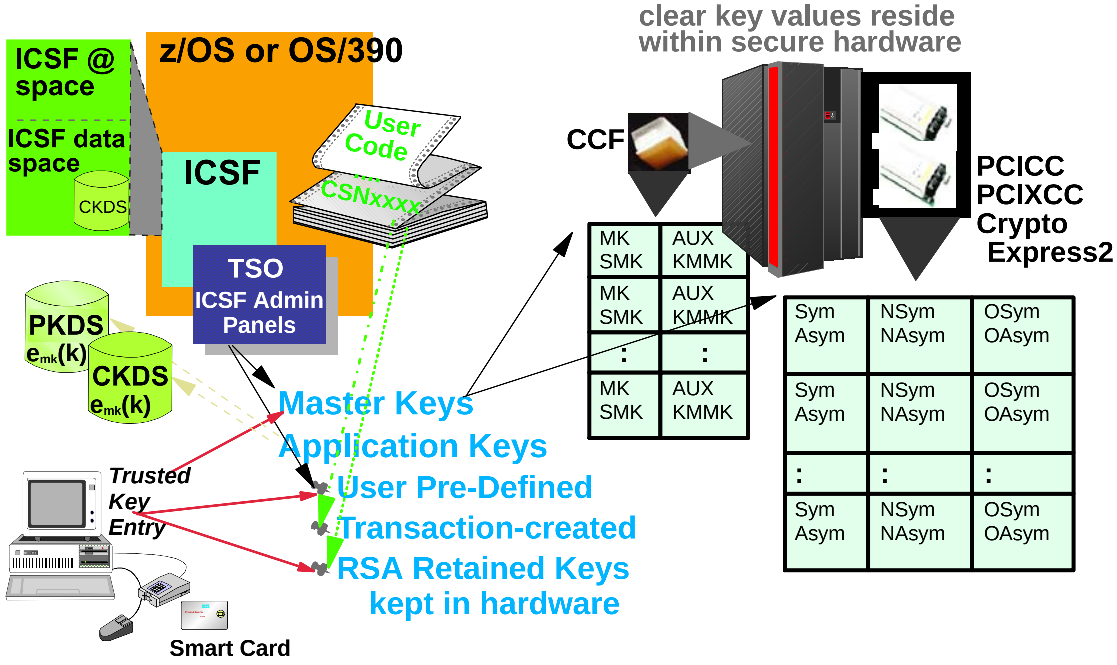
MK SMK	AUX KMMK
MK SMK	AUX KMMK
:	:
MK SMK	AUX KMMK

Sym Asym	NSym NAsym	OSym OAsym
Sym Asym	NSym NAsym	OSym OAsym
:	:	:
Sym Asym	NSym NAsym	OSym OAsym

zSeries and S/390 Clear Key Crypto Solution


z/OS or OS/390
ICSF @ space
ICSF data space
CKDS
ICSF
PKDS
$e_{mk}(k)$
CKDS
$e_{mk}(k)$
clear key values reside outside crypto hardware environment
CPACF on each PU
for TDES/DES encryption and decryption using clear (unencrypted) key values
PCICA for Acceleration of SSL Handshake using clear RSA key value
clear key values (used 'as is') reside outside of hardware and key data sets
key data sets not used at this time to hold clear key values
Setup for Crypto
Support Element (ThinkPad)

zSeries and S/390 Crypto Software: Key Entry

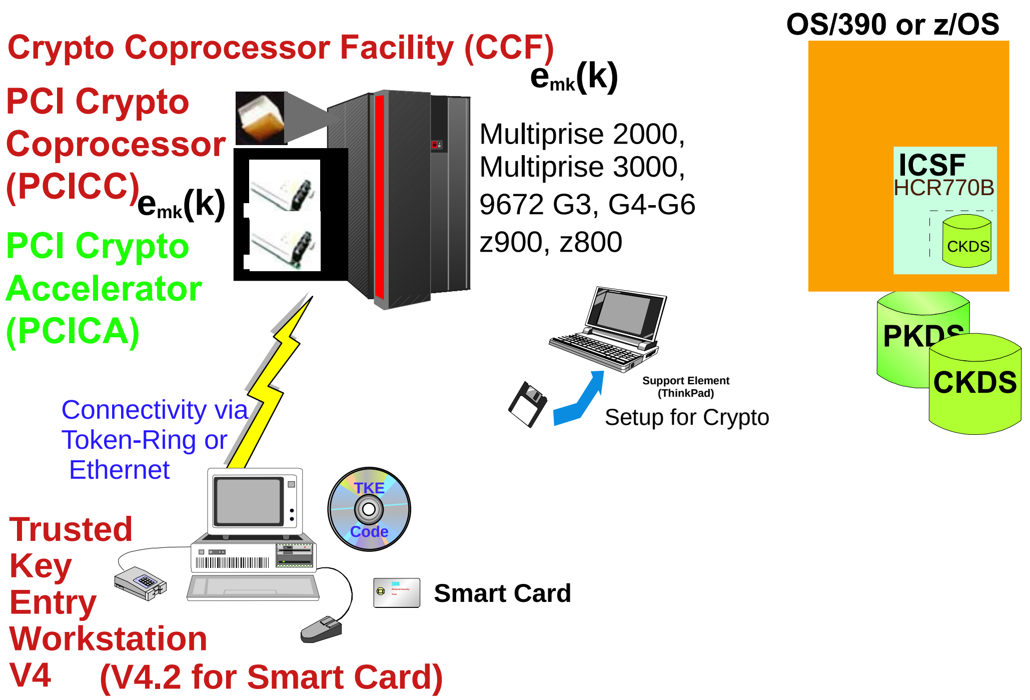


Master Keys
Application Keys
User Pre-Defined
Transaction-created
RSA Retained Keys
kept in hardware

MK SMK	AUX KMMK
MK SMK	AUX KMMK
:	:
MK SMK	AUX KMMK

Sym Asym	NSym NAsym	OSym OAsym
Sym Asym	NSym NAsym	OSym OAsym
:	:	:
Sym Asym	NSym NAsym	OSym OAsym

IBM zSeries Crypto Environment: 1st Generation



Crypto Coprocessor Facility (CCF)

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

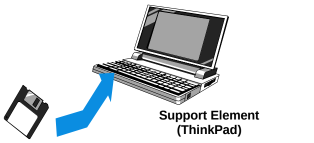
PCI Crypto Accelerator (PCICA)

Multiprise 2000,
Multiprise 3000,
9672 G3, G4-G6
z900, z800

Connectivity via
Token-Ring or
Ethernet

Trusted
Key
Entry
Workstation
V4 (V4.2 for Smart Card)

Crypto Coprocessor Facility (CCF)

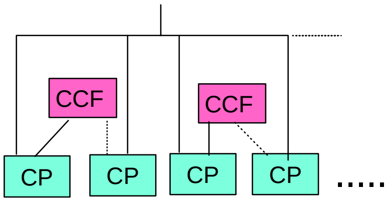


Setup for Crypto

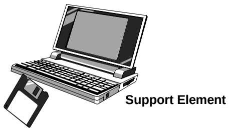
- **CCF => base crypto hardware** $e_{mk}(k)$
  - Built into most IBM processors G3 - G6, z900 & z800
    - Multiprise 2000/3000 are exceptions where processor could be ordered without CCFs
    - Some G3s also were ordered without CCFs
  - Requires configuration data load to become usable
  - Requires hardware setup in PR/SM environments
- Presence of at least 1 CCF indicated by feature code 0800
- Enablement diskette contains the configuration data, feature code 0875
- ICSF => only method to send requests to hardware
  - Handles directing requests to **appropriate** hardware
  - Encipher and Decipher requests only get routed to CCFs
- CCFs are only usable in OS/390 or z/OS operating system environments

Crypto Coprocessor Facility (CCF) . . .

- Within processor the CCF is physically attached to a CP
  - Hence, references to CP on Configuration screen & in D M=CPU
- Each CCF can be shared across multiple LPARs
  - Usage Domain definition identifies the area(s) reserved for use for the partition
  - ICSF Options data set domain parameter identifies the reserved area to be used during the active session on the partition
  - Usage Domain number(s) must be unique among all defined usage domains on the CCFs within the processor



Crypto Coprocessor Facility (CCF) . . .



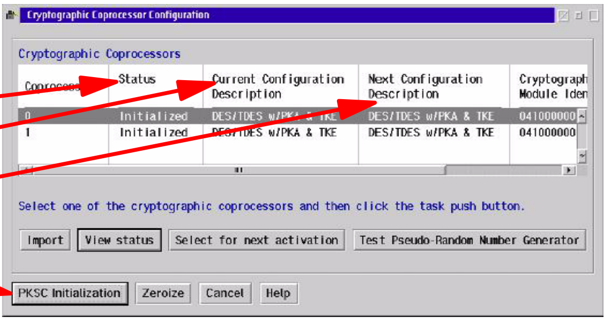
- **Hardware setup via Support Element access**
  - Enablement via load of configuration data which requires an outage of the processor
  - Association of the configuration data with each CCF module called selection for next activation
  - LPAR association with the CCF modules
  - Definition of the crypto characteristics
- **ICSF activation**
- **TKE Installation, if needed**
  - Can only be used for key entry
  - Does not process DATA key types (See TechDocs for workaround)
  - Part of the 9672, Multiprise, or zSeries processor
  - Master Key loading
- **Define Master Keys**

CCF Hardware Installation Confirmation

- **Configuration**
  - Check Status
    - ✓ Status
    - ✓ Config in hw
    - ✓ Avail at next POR
    - ✓ PKSC
  - Use D M=CPU

```
PROCESSOR STATUS
ID  CPU  CR          SERIAL
0    +   -       091F1E2066
1    +   -       191F1E2066
```

- **LPAR**
  - Display Change LPAR Cryptographic Controls

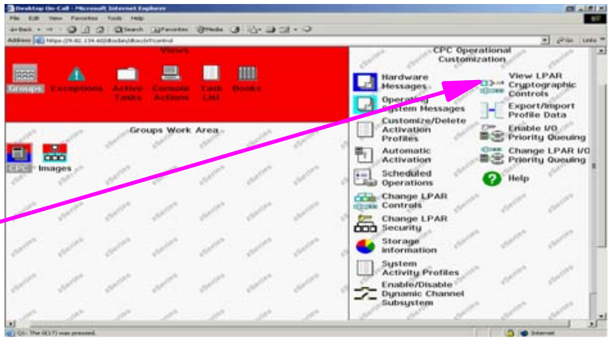

Cryptographic Coprocessor Configuration

Cryptographic Coprocessors

Coprocess	Status	Current Configuration Description	Next Configuration Description	Cryptograph Module Iden
0	Initialized	DES/TDES w/PKA & TKE	DES/TDES w/PKA & TKE	041000000
1	Initialized	DES/TDES w/PKA & TKE	DES/TDES w/PKA & TKE	041000000

Select one of the cryptographic coprocessors and then click the task push button.

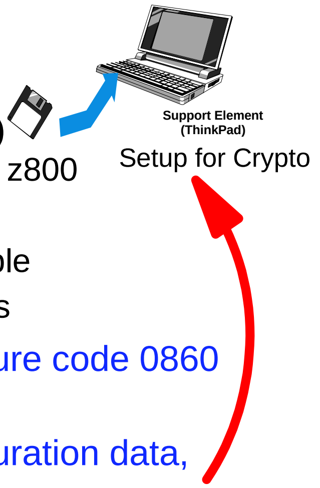
Import
View status
Select for next activation
Test Pseudo-Random Number Generator
PKSC Initialization
Zeroize
Cancel
Help


Views
Groups
Exceptions
Active Tasks
Console Actions
Task List
Books
Groups Work Area
CPC
Images
CPC Operational Customization
Hardware Messages
Operating System Messages
Customize/Delete Activation Profiles
Automatic Activation
Scheduled Operations
Change LPAR Controls
Change LPAR Security
Storage Information
System Activity Profiles
Enable/Disable Dynamic Channel Subsystem
View LPAR Cryptographic Controls
Export/Import Profile Data
Enable I/O Priority Queuing
Change LPAR I/O Priority Queuing
Help

Crypto Coprocessor Facility (CCF): What it Can Do

- Protecting Data
  - Use Secure Hardware
  - Use Clear key with ICSF performing AES
- Performing Financial Processes
- Hashing and Message Authentication
- Key management
- Digital Signatures
- Encryption and Decryption of symmetric key values using Asymmetric key
  - SSL Handshake Acceleration via Decrypt of pre-master secret

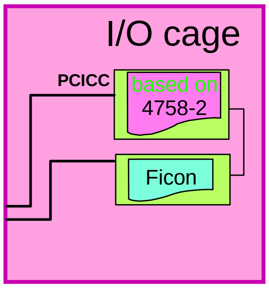
PCI Crypto Coprocessor (PCICC)



- PCICC => adjunct secure crypto hardware **e_{mk}(k)**
  - Available for IBM processors G5 - G6 and z900 - z800
  - Requires CCF to operate in OS/390 or z/OS
  - Requires configuration data load to become usable
  - Requires hardware setup in PR/SM environments
- Presence of at least 1 PCICC indicated by feature code 0860 on G5/G6 or 0861 on z900/800
- Enablement diskette (FCV) contains the configuration data, feature code 0865
- ICSF => only method to send requests to hardware
  - Handles directing requests to **appropriate** hardware
  - Encipher and Decipher requests only get routed to CCFs
- PCICCs are usable in OS/390 or z/OS operating system environments and Linux with Linux crypto driver

PCI Crypto Coprocessor (PCICC) . . .

- Within processor each PCICC card is physically package in a book that is installed within the I/O cage
  - No consoles commands are available for status of PCI Crypto
- PCICC book packages consist of
  - Single card on G5 and G6
  - Dual (2) cards on z900 and z800
- Each PCICC card can be shared across multiple LPARs
  - PCICC cards associated with a LPAR take the domain settings associated with the CCFs
  - Each PCICC card is associated with an AP index
  - PCICCs to be immediately available at operating system load are defined in the PCI Online list
  - PCICCs possibly available for use and that can be brought online are defined in the PCI Candidate list

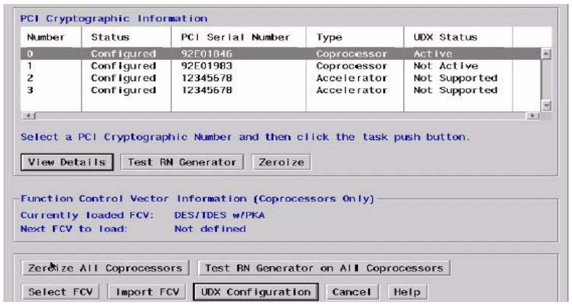


PCI Crypto Coprocessor (PCICC) . . .

- Hardware setup via Support Element access
  - Enablement via load of configuration data which requires an outage of the LPAR, if Candidate List not pre-defined since last deactivate
  - LPAR association with the PCICC card(s)
  - Bringing cards online
- ICSF activation and CCF enablement required
- Define Master Keys to PCICCs
  - Master Key values must match those entered into CCFs
  - Weak and semi-weak values are not allowed

PCI Crypto Hardware Installation Confirmation

- Configuration
  - Check PCI Configuration Status
  - View Console
    - PCICA Available
      CSFM411I PCI CRYPTOGRAPHIC ACCELERATOR A02 IS ACTIVE
    - PCICC
      CSFM119E INCORRECT MASTER KEY (BOTH) ON PCI CRYPTOGRAPHIC COPROCESSOR P00, SERIAL NUMBER 92E01846.
- LPAR
  - Display Change LPAR Crypto Cntls



PCI Cryptographic Information

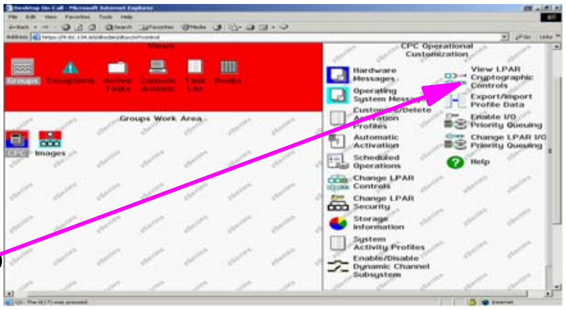
Number	Status	PCI Serial Number	Type	UDX Status
0	Configured	92E01846	Coprocessor	Active
1	Configured	92E01983	Coprocessor	Not Active
2	Configured	12345678	Accelerator	Not Supported
3	Configured	12345678	Accelerator	Not Supported

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

Function Control Vector Information (Coprocessors Only)

Currently loaded FCV: DES/TDES w/PKA

Next FCV to load: Not defined



Views
Groups
Exceptions
Active Tasks
Console Actions
Task List
Books
Groups Work Area
Images
CPC Operational Customization
Hardware Messages
Operating System Messages
Customize/Delete Activation Profiles
Automatic Activation
Scheduled Operations
Change LPAR Controls
Change LPAR Security
Storage Information
System Activity Profiles
Enable/Disable Dynamic Channel Subsystem
View LPAR Cryptographic Controls
Export/Import Profile Data
Enable I/O Priority Queuing
Change LPAR I/O Priority Queuing
Help

PCI Crypto Coprocessor Facility (PCICC): What it Can Do

- Performs new functions
- Performs functions that gain added security over operation on CCF
- Preferred routing of RSA functions

PCI Crypto Accelerator (PCICA)

- PCICA => adjunct clear key crypto hardware
  - Available for IBM processors z900 - z800 and z990 - z890
  - Requires CCF to operate in OS/390 or z/OS
  - Requires hardware setup in PR/SM environments
    - Candidate and Online list definition required
- Presence of at least 1 PCICA indicated by feature code 0862
- ICSF => only method to send requests to hardware
  - Handles directing requests to **appropriate** hardware
  - PCICA in z900 and z800 environments are only routed 1 API, decrypt of symmetric key
- PCICAs are usable in OS/390 or z/OS operating system environments and Linux with Linux crypto driver

Trusted Key Entry Workstation (TKE)

- Separate crypto system
  - Part of processor system not to be treated as a PC
  - OS/2 Warp operating system with all necessary applications
  - Contains 4758 PCI Crypto Coprocessor making TKE a crypto system separate from host
- Performs key entry for host use
- Not to be used for anything else otherwise support negated
- TKE V4 code is available as MCL updates to TKE V3.x workstations
- TKE is final component for a FIPS 140-1 Level 4 system
- TKE is required for certain Visa and MasterCard financial centers

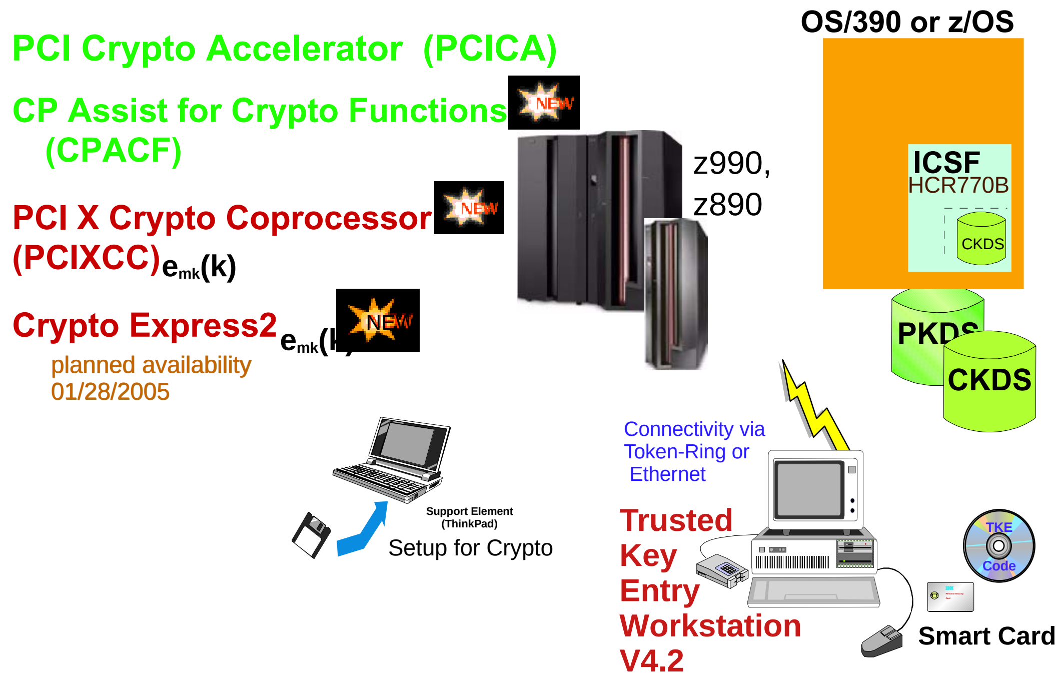
New Changes to 1st Generation Crypto Hardware

- PCICC can be updated to support the use of 2048-bit RSA keys for key distribution - encrypt and decrypt of symmetric keys.
  - The change is for allowance of private key lengths 2048-bit
  - Feature code 0867 must be ordered and installed for function
  - Update will require
    - Force of new data into PCICC cards
    - Loss of master keys caused by installation of new support
- TKE V4.x is supported on CCFs and PCICCs
  - However, new function provided by TKE is not
    - Key types handled are not expanded beyond TKE V3
    - Smart Cards can be used with CCFs or PCICCs on G6 and z900/800
  - Smart Card supported for z990/890 with TKE V4.2
    - Feature code 0887 represents 2 Smart Card Readers and 10 smart cards

IBM zSeries 1st Generation Crypto Console Messages

- CCF - CRYPTO (n) Online
  - IEE504I
- PCICC - (INCORRECT or CORRECT) MASTER KEY (BOTH) ON PCI CRYPTOGRAPHIC COPROCESSOR P0x, SERIAL NUMBER nnnnnnnn
  - CSFM119I Incorrect
  - CSFM116I Correct
- PCI CRYPTOGRAPHIC ACCELERATOR A00 IS ACTIVE

IBM zSeries Crypto Environment: 2nd Generation



PCI Crypto Accelerator (PCICA)

CP Assist for Crypto Functions (CPACF)

PCI X Crypto Coprocessor (PCIXCC)e_{mk}(k)

Crypto Express2 e_{mk}(k)

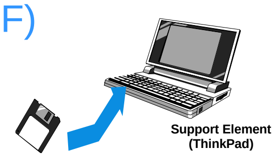
planned availability 01/28/2005

NEW
NEW
NEW
OS/390 or z/OS
z990,
z890
ICSF
HCR770B
CKDS
PKDS
CKDS
Connectivity via Token-Ring or Ethernet
Support Element (ThinkPad)
Setup for Crypto
Trusted Key Entry Workstation V4.2
TKE
Code
Smart Card

IBM zSeries 2nd Generation Facts

- NEW Hardware
  - CPACF, totally new function with some older function offloaded
    - 5 Problem State Instructions using clear key values
    - Documented in z990 Principles of Operation
    - 4 of those instructions can be executed using ICSF APIs
    - TDES and DES algorithms using clear key values did not exist in ICSF previously
  - One way hash, SHA-1, enabled without configuration is available on CPACF
  - PCIXCC is new architected card not the same as PCICC
  - ICSF support of PCIXCC not the same as support of CCF
  - CKDS can be brought into z990 environment without changes
  - PKDS is required to be initialized
- PCIXCC is described in IBM Journal of Research & Developmt
  - IBM J. RES. & DEV. VOL. 48 NO. 3/4 MAY/JULY 2004

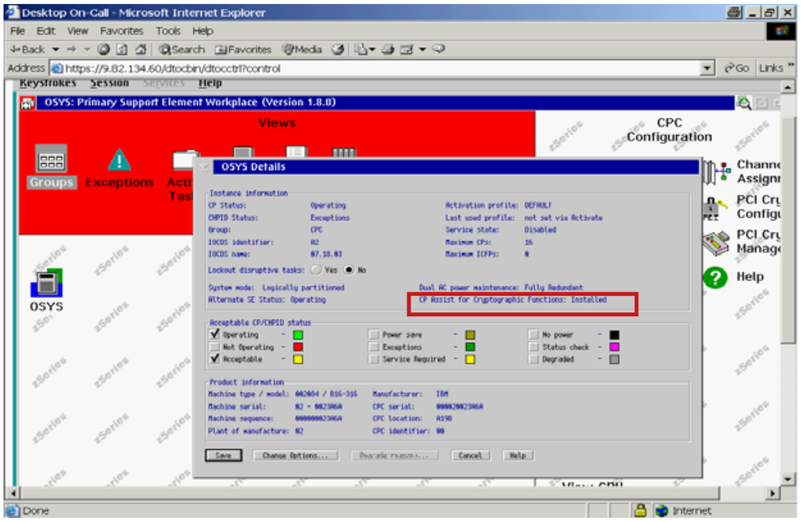
CP Assist for Cryptographic Functions (CPACF)



- CPACF => base crypto hardware
  - Built into z990 & z890 IBM processors
  - Requires configuration data load to become usable
    - Unlike CCF and PCICC configuration data in part of server code load
  - Requires no setup for PR/SM environments
  - Each Physical Unit on the processor has CPACF hardware
- Enablement diskette contains the configuration data, feature code 3863
- ICSF => only method to send requests to hardware
  - Handles directing requests to **appropriate** hardware
  - TDES/DES clear key requests only get routed to CPACFs
- CPACFs are only usable in OS/390 or z/OS operating system environments

CPACF Hardware Installation Confirmation

- From Support Element, select the CPC in question
  - Double-click on the CPC to get the Details window
  - CP Assist for Cryptographic Functions is/is not installed


Desktop On-Call - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://9.82.134.60/dtocbin/dtocctrl?control
Go Links
Keystrokes Session Services Help
OSYS: Primary Support Element Workplace (Version 1.8.0)
Views
Groups
Exceptions
Acti Tas
OSYS
CPC Configuration
Channe Assignr
PCI Cry Configu
PCI Cry Manage
Help
View CPU
Done
Internet

OSYS Details

Instance information

CP Status: Operating
CHPID Status: Exceptions
Group: CPC
IOCDS identifier: A2
IOCDS name: 07.18.03
Activation profile: DEFAULT
Last used profile: not set via Activate
Service state: Disabled
Maximum CPs: 16
Maximum ICFPs: 0
Lockout disruptive tasks: ○ Yes ● No
System mode: Logically partitioned
Alternate SE Status: Operating
Dual AC power maintenance: Fully Redundant
CP Assist for Cryptographic Functions: Installed

Acceptable CP/CHPID status

☑ Operating - 🟩
☐ Not Operating - 🟥
☑ Acceptable - 🟨
☐ Power save - ■
☐ Exceptions - 🟩
☐ Service Required - 🟨
☐ No power - ■
☐ Status check - ■
☐ Degraded - ■

Product information

Machine type / model: 002084 / B16-316
Machine serial: 02 - 0023A6A
Machine sequence: 0000000023A6A
Plant of manufacture: 02
Manufacturer: IBM
CPC serial: 000020023A6A
CPC location: A19B
CPC identifier: 00

Save | Change Options... | Degrade reasons... | Cancel | Help

PCI Crypto Accelerator (PCICA)

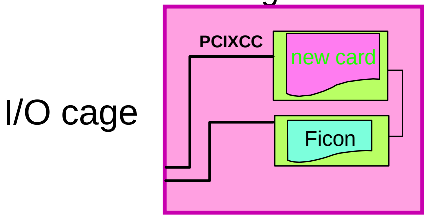
- PCICA => adjunct clear key crypto hardware
  - Only 1st generation feature that can be brought forward
- Feature code 0862 is unchanged
- ICSF => only method to send requests to hardware
  - Handles directing requests to **appropriate** hardware
  - PCICA in z990 and z890 environments are routed 3 APIs,
    - Decrypt of symmetric key
    - Encrypt of symmetric key
    - Digital Signature Verify
- PCICAs are usable in OS/390 or z/OS operating system environments and Linux with Linux crypto driver

PCI XCrypto Coprocessor (PCIXCC)

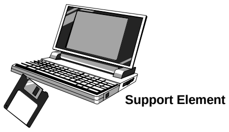
- PCIXCC => adjunct secure crypto hardware **e_{mk}(k)**
  - Available for IBM processors z990 - z890
  - Requires CPACF to operate in OS/390 or z/OS
  - Uses CPACF configuration data
  - Requires hardware setup in PR/SM environments
- Presence of PCIXCC indicated by feature code 0868
- Single card package
- ICSF => only method to send requests to hardware
  - Handles directing requests to **appropriate** hardware
  - Encipher and Decipher requests only get routed to CCFs
- PCICCs are usable in OS/390 or z/OS operating system environments and Linux with Linux crypto driver

PCI XCrypto Coprocessor (PCIXCC) . . .

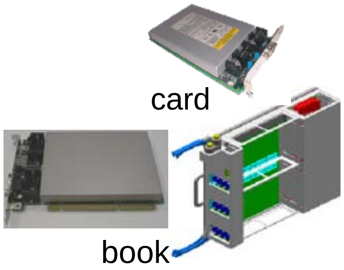
- Within processor each PCIXCC card is physically package in a book that is installed within the I/O cage
  - No consoles commands are available for status of PCI XCrypto
- Each PCIXCC card can be shared across multiple LPARs
  - PCIXCC cards associated with a LPAR must be defined with domain settings
  - Each PCIXCC card is associated with an AP index
  - PCIXCCs to be immediately available at operating system load are defined in the PCI Online list
  - PCIXCCs possibly available for use and that can be brought online are defined in the PCI Candidate list

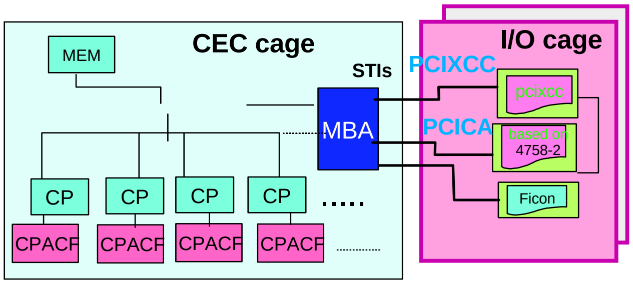


PCI XCrypto Coprocessor (PCIXCC) . . .



- Hardware setup via Support Element access
  - Enablement via load of configuration data which requires an outage of the LPAR, if Candidate List not pre-defined since last deactivate
  - LPAR association with the PCIXCC card(s)
  - Bringing cards online
- ICSF activation and CPACF enablement required
- Define Master Keys to PCICCs
  - Weak and semi-weak values are not allowed



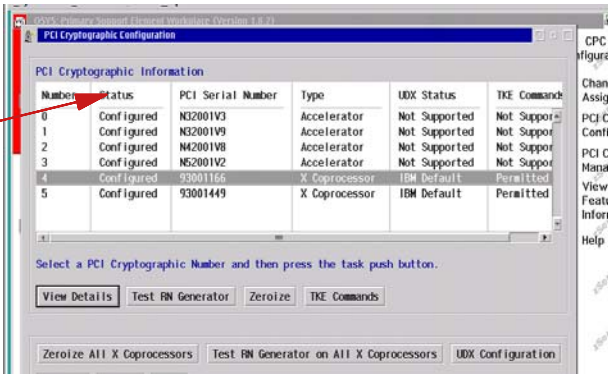


PCIXCC Hardware Installation Confirmation

- Configuration
  - Check PCI Configuration Status
  - View Console
    - PCICA Available

      CSFM411I PCI CRYPTOGRAPHIC ACCELERATOR A02 IS ACTIVE
    - PCIXCC

      CSFM419E INCORRECT MASTER KEY (BOTH) ON PCI X CRYPTOGRAPHIC COPROCESSOR X04, SERIAL NUMBER 93001166.
- LPAR
  - Display Change LPAR Crypto Cntls



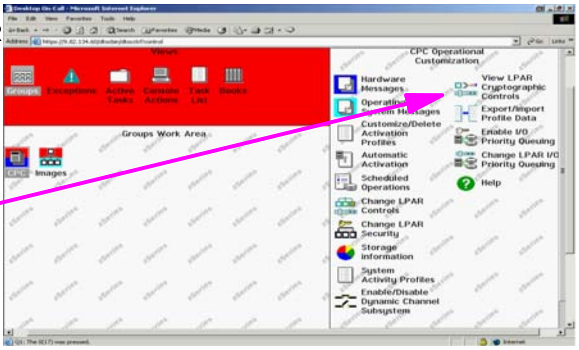
OSYS: Primary Support Element Workplace (Version 1.8.2)
PCI Cryptographic Configuration
CPC
figura
Chan
Assig
PCI C
Confi
PCI C
Mana
View
Featu
Infor
Help

PCI Cryptographic Information

Number	Status	PCI Serial Number	Type	UDX Status	TKE Commands
0	Configured	N32001V3	Accelerator	Not Supported	Not Suppor
1	Configured	N32001V9	Accelerator	Not Supported	Not Suppor
2	Configured	N42001V8	Accelerator	Not Supported	Not Suppor
3	Configured	N52001V2	Accelerator	Not Supported	Not Suppor
4	Configured	93001166	X Coprocessor	IBM Default	Permitted
5	Configured	93001449	X Coprocessor	IBM Default	Permitted

Select a PCI Cryptographic Number and then press the task push button.

View Details
Test RN Generator
Zeroize
TKE Commands
Zeroize All X Coprocessors
Test RN Generator on All X Coprocessors
UDX Configuration



Desktop On-Call - Microsoft Internet Explorer
Views
Groups
Exceptions
Active Tasks
Console Actions
Task List
Books
Groups Work Area
CPC
Images
CPC Operational Customization
Hardware Messages
Operating System Messages
Customize/Delete Activation Profiles
Automatic Activation
Scheduled Operations
Change LPAR Controls
Change LPAR Security
Storage Information
System Activity Profiles
Enable/Disable Dynamic Channel Subsystem
View LPAR Cryptographic Controls
Export/Import Profile Data
Enable I/O Priority Queuing
Change LPAR I/O Priority Queuing
Help

IBM zSeries Crypto Express2

- Targeted for GA end of January 2005
- Crypto Express2 is PCIXCC packaged as a dual card package with faster speeds to meet PCICA speeds for RSA processing

IBM zSeries 2nd Generation Crypto Console Messages

- PCIXCC - (INCORRECT or CORRECT) MASTER KEY (BOTH) ON PCI X CRYPTOGRAPHIC COPROCESSOR X0x, SERIAL NUMBER nnnnnnnn
  - CSFM419I Incorrect
  - CSFM416I Correct
- CPACF has no hardware related message. Only see
  - CSFM400I CRYPTOGRAPHY - SERVICES ARE NOW AVAILABLE.

New Changes to 2nd Generation Crypto Hardware

- Cryptographic support for 19-digit Personal Account Numbers (PANs) on PCIXCC targeted for December 17, 2004, via the ICSF Virtual Support for z/OSâ and z/OS.e V1.6 Web deliverable.
- Less than 512-bit keys for clear key RSA operations on PCIXCC
- TKE V4.x is supported on CCFs and PCICCs
  - However, new function provided by TKE is not
    - Key types handled are not expanded beyond TKE V3
    - Smart Cards can be used with CCFs or PCICCs on G6 and z900/800
  - Smart Card supported for z990/890 with TKE V4.2
    - Feature code 0887 represents 2 Smart Card Readers and 10 smart cards
- TKE on z990/890 must be enabled for TKE Commands via Support Element and PCI Configuration