



zSeries Explorers



IBM @server zSeries

Solução de Criptografia em z990 O que mudou ?

Vicente Ranieri Júnior

IBM Senior Certified Consulting IT Specialist
ranieri@br.ibm.com



The S/390 and z900, z800 Cryptographic Coprocessors

• 1994 : S/390 CMOS Cryptographic Coprocessor Facility (CCF)

- ▶ secure coprocessor
- ▶ standard feature on 9672 G4, G5, G6, z900
- ▶ optional feature on MP2000, MP3000, z800
- ▶ evaluated FIPS 140-1 level 4

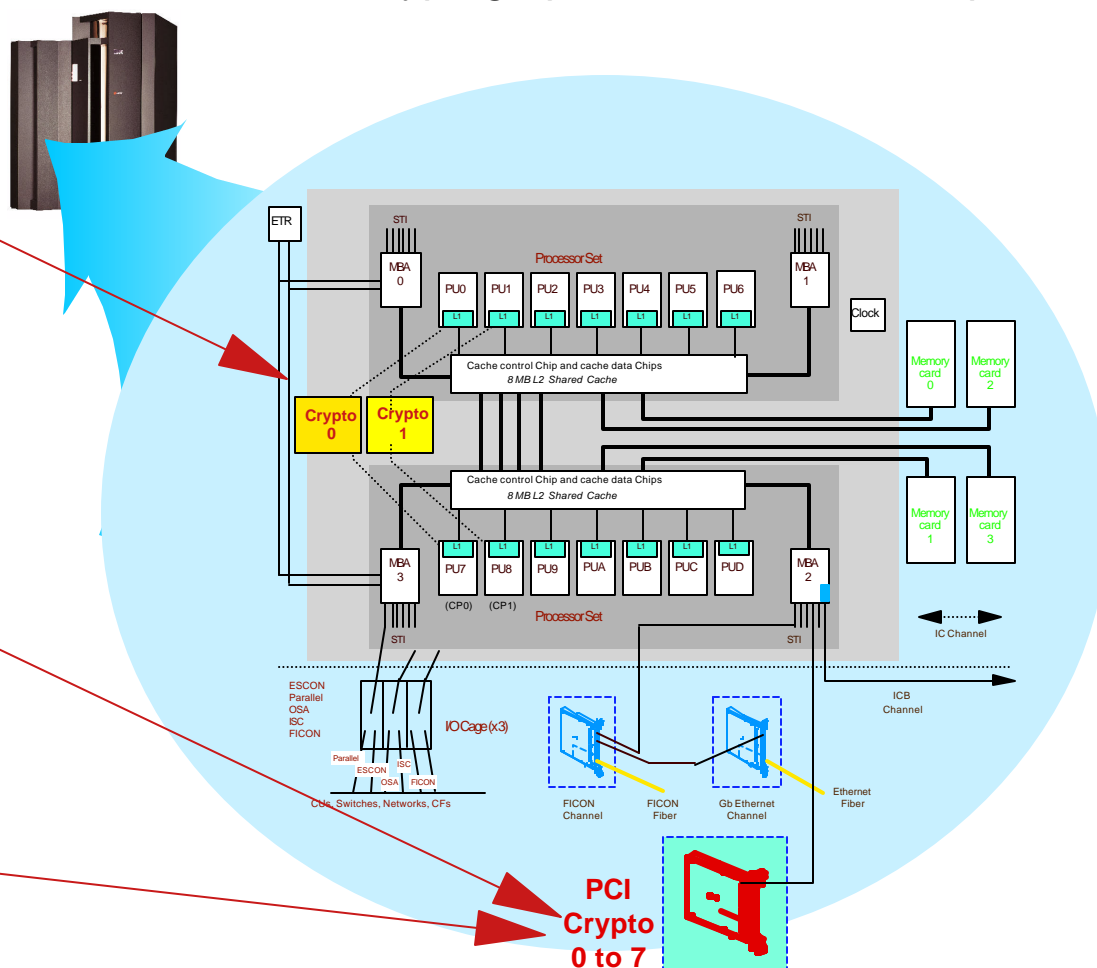
• 2000 : S/390 PCI Cryptographic Card (PCICC)

- ▶ secure coprocessor
- ▶ priced feature on 9672 G5, G6, z900, z800
- ▶ 0 to 8 'features' in a single system
- ▶ evaluated FIPS 140-1 level 4

• 2001 : PCI Cryptographic Accelerator (PCICA)

- ▶ SSL accelerator (non secure)
- ▶ priced feature on zSeries only
- ▶ 0 to 6 'features' in a system
- ▶ mix with PCICC for a total of 8
- ▶ no FIPS evaluation

IBM Common Cryptographic Architecture Compliant

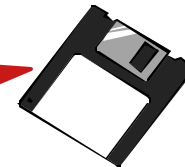




S/390-z900/z800 CCF and PCICC Enablement

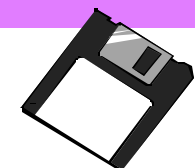
CCF

7060 <	G5/G6	z900 z800	PCICC	PCICA zSeries	Description
0800	0800	0800			CCF Hardware
0804	0814		0864		DES with PKA
0805	0815		0864		DES with PKA & TKE
0824	0834		0865		Triple DES with PKA
0825	0835	0875	0865		Triple DES with PKA & TKE
			0860 (G5/G6) / 0861 (z900/ z800)		PCI Crypto Coprocessor Card hardware
				0862	PCI Crypto Accelerator Card hardware
0866	0866	0866	0866		TKE (Token-Ring attachment)
0869	0869	0869	0869		TKE (Ethernet attachment)



One Crypto Enablement
Diskette for each CCF
**Requires a system Power On
Reset**

One PCICC FCV Diskette for the
system - Concurrent installation



No diskette for the PCICA



z990 Hardware Cryptographic Coprocessors

IBM Common Cryptographic Architecture Compliant

2003 CP Assist for Cryptographic Functions (CPACF)

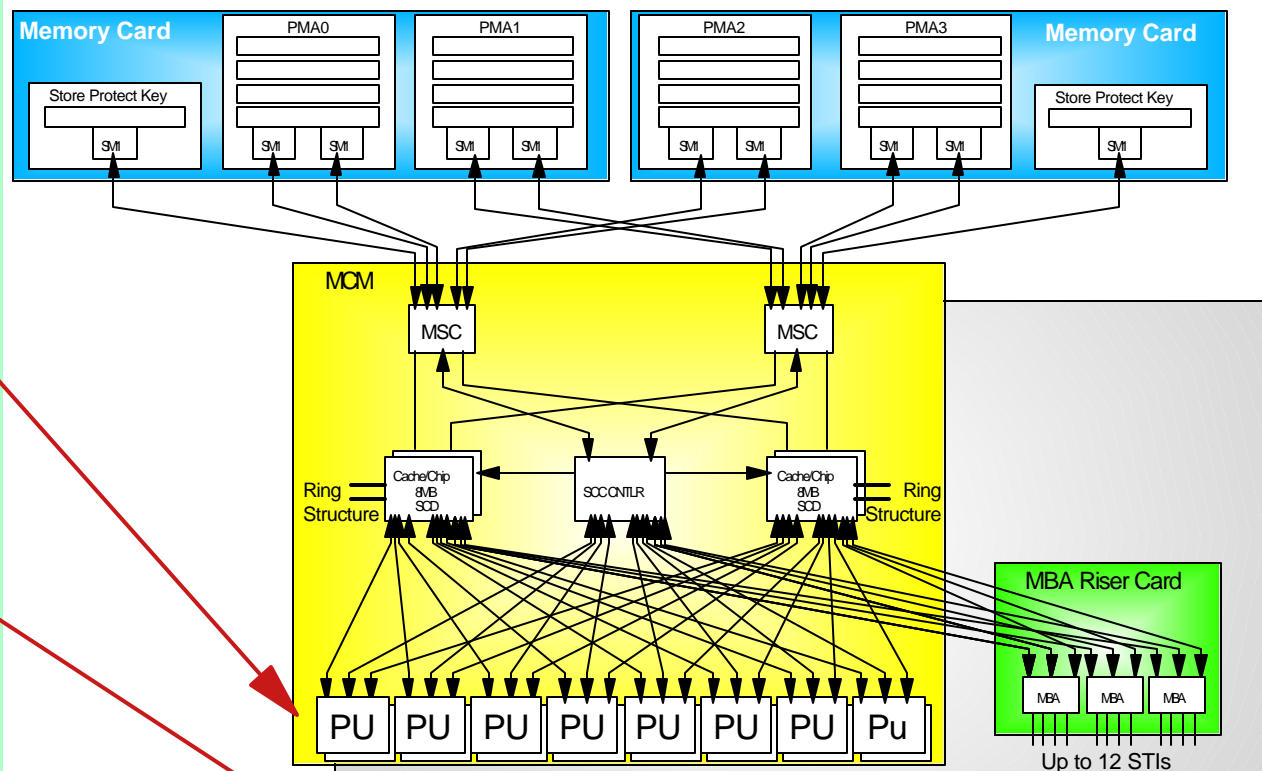
- ▶ One CPACF per processing unit
- ▶ standard orderable feature
- ▶ 5 new published crypto instructions or through ICSF
- ▶ non-secure (clear keys only)

2003 : PCI Cryptographic Accelerator (PCICA)

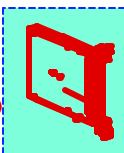
- ▶ priced feature (same feature as for z900, z800)
- ▶ SSL accelerator (non secure)
- ▶ 0 to 6 features in a system

2003 : PCIX Cryptographic Coprocessor (PCIXCC)

- ▶ priced feature
- ▶ secure coprocessor
- ▶ 0 to 4 features in a system
- ▶ mix with PCICA for a maximum of 8 features
- ▶ designed for FIPS 140-2 level 4



PCI
Crypto
0 to 7

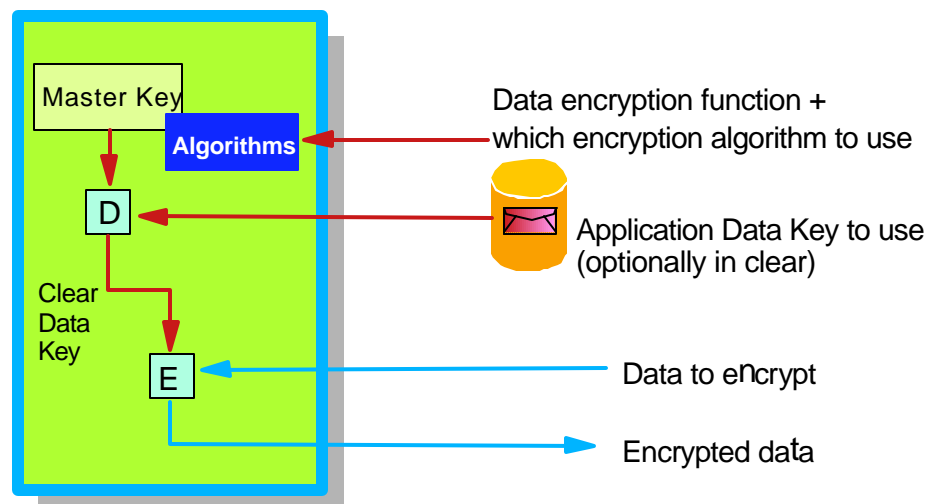




Secure and Non-Secure Coprocessors or Accelerators

Secure Coprocessor

tamper proof hardware
(CCF, PCICC or PCIXCC)

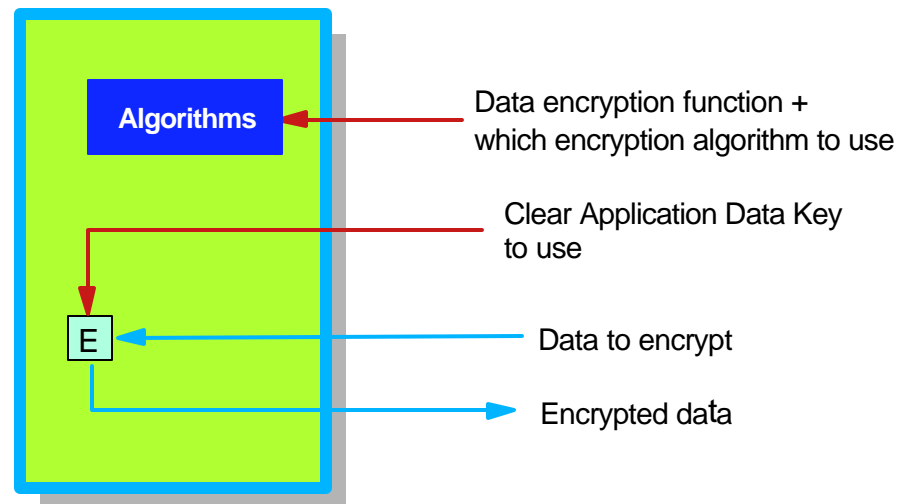


Evaluated FIPS 140-1 level 4

Can also operate with clear keys

Non-Secure Coprocessor or Accelerator

PCICA, CPACF





IBM @server zSeries

zSeries Explorers



Central Processor Assist for Cryptographic Functions (CPACF)

- ◆ Set of hardware cryptographic functions integrated in each PU
- ◆ Can be invoked directly using published zArchitecture problem state instructions or via ICSF
 - ✓ DES, T-DES encrypt/decrypt (clear key only), SHA-1 digest
 - ✓ Two engines per assist: one for DES/MAC and one for SHA
- ◆ Full error detection (double data flow and comparison) and recovery (checkpoints in millicode)
- ◆ Orderable standard feature: **FC 3863** - concurrent install/removal
- ◆ Certified FIPS for the algorithms
- ◆ Export controlled feature
- ◆ **Not a replacement for CCF**



z990 CPACF - ICSF support

- ★ **MDC Generate** (CSNBMDG,CSNBMDG1)
 - ★ **One-Way Hash** (CSNBOWH,CSNBOWH1)
 - ✓ SHA-1
 - ★ **Symmetric Key Decipher** (CSNBSYD, CSNBSYD1)
 - ★ **Symmetric Key Encipher** (CSNBSYE, CSNBSYE1)
 - ✓ Clear keys only
 - ✓ Single-, double- and triple-length keys
 - ✓ CBC, X9.23, CUSP, IPS, ECB processing
 - ★ **Encode** (CSNBECO) (DES, clear key)
 - ★ **Decode** (CSNBDCO) (DES, clear key)
-
- **AES** still available in software (CSNBSYD, CSNBSYE)



IBM @server zSeries

zSeries Explorers



z990 CPACF - zArchitecture Assembler Instructions

Problem state instructions

- ★ Cipher Message (KM)
- ★ Cipher Message with Chaining (KMC)
- ★ Compute Intermediate Message Digest (KIMD)
- ★ Compute Last Message Digest (KLMD)
- ★ Compute Message Authentication Code (KMAC) (*)

(*) available as asm instruction only - Not via ICSF



IBM @server zSeries

zSeries Explorers



PCI Cryptographic Accelerator (PCICA)

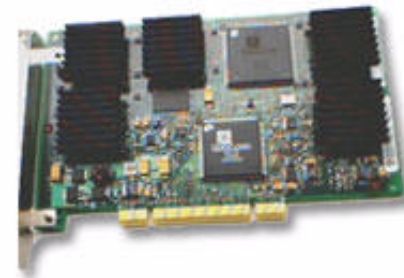
- ◆ Accelerator for SSL handshake - driven by ICSF
- ◆ Priced feature - FC 0862 (same as z900/z800) - FC 3863 must be installed
- ◆ No enablement diskette - Concurrent install/removal

- ★ **PKA Decrypt (CSNDPKD)**

- ✓ PKCS-1.2 formatting

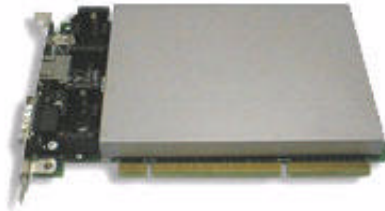
- ★ **PKA Encrypt (CSNDPKE)**

- ✓ ZERO-PAD formatting





PCI X Cryptographic Coprocessors (PCIXCC)

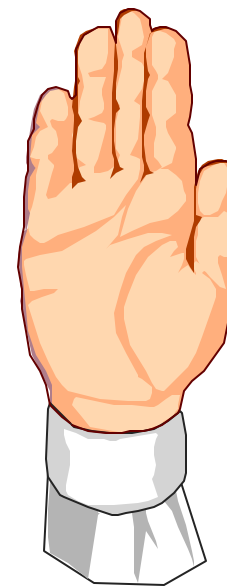


- ★ Secure coprocessor - driven by ICSF
- ★ Priced feature: FC 0868 - FC 3863 must be installed
- ★ Replacement for z/900 CCF and PCICC
- ★ No enablement diskette - Concurrent install/removal
- ★ No Function Control Vector (FCV)
- ★ Better performance and reliability
 - ✓ PPC 405 processor
 - ✓ Faster RSA, SHA and DES engines
 - ✓ More memory
 - ✓ Embedded LINUX operating system (replacing IBM CP/Q++ control program)



ICSF services dropped on z990

- ✗ Support for DSA signatures and key generation.
- ✗ Support for ANSI x9.17 services (offset and notarization), and associated key types.
- ✗ Support for Ciphertext_translate(CSNBCTT).
- ✗ Support for German Bank Pool - Pin Offset
- ✗ Support for CSFUDK - use CSNBDBG instead.
- ✗ Support for CDMF (40 bit encryption)





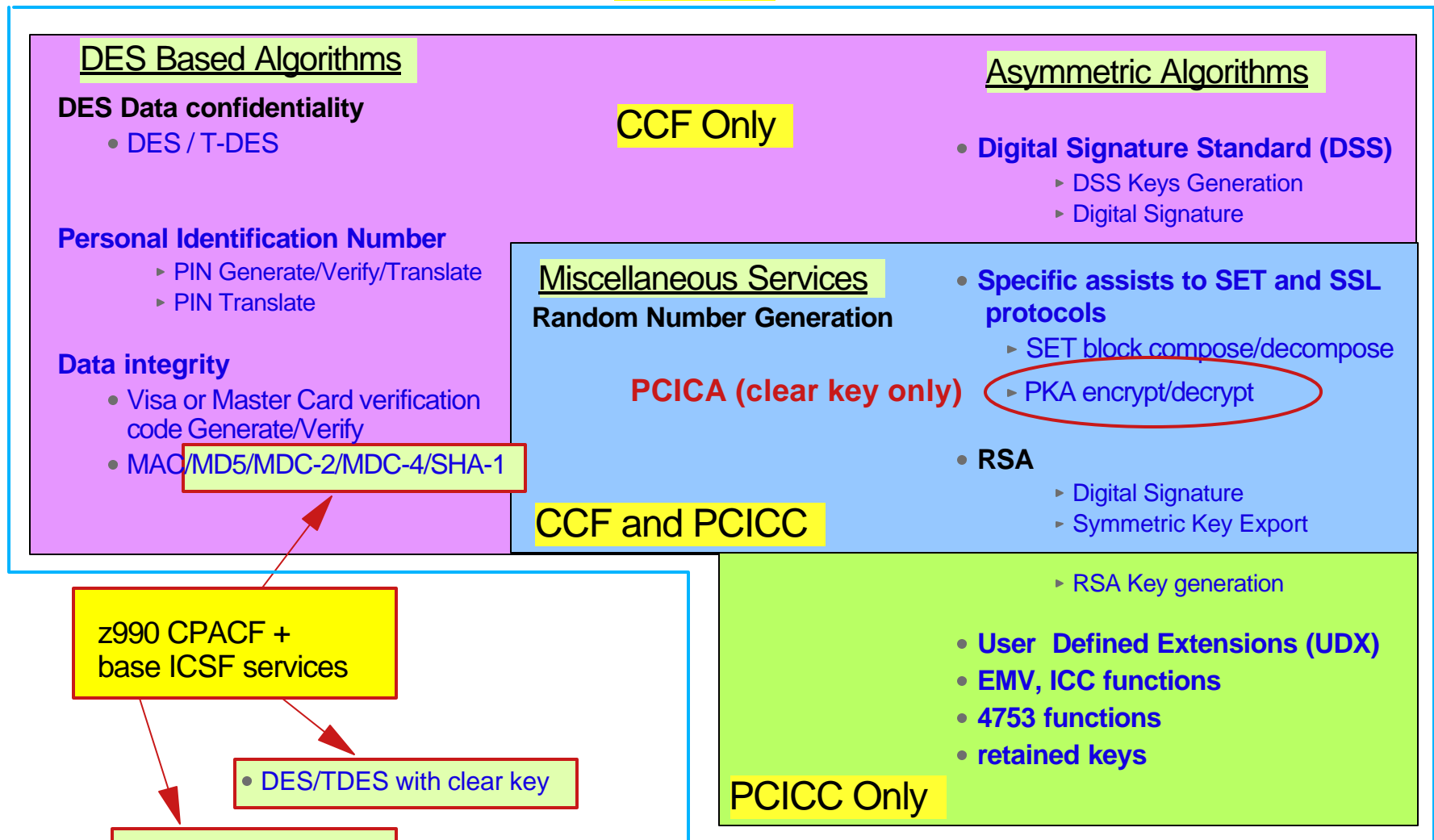
IBM @server zSeries

zSeries Explorers



Cryptographic Algorithms Supported in zSeries

PCIXCC





IBM @server zSeries

zSeries Explorers



Crypto Support General Availability

	Availability Date
PCIXCC Feature	9/19/2003
TKE 4.0 Workstation	9/30/2003
ICSF Support (z/OS V1R4) - z990	9/19/2003
ICSF Support (z/OS V1R2) - z990	9/19/2003
ICSF Support (z/OS V1R3) - z990	10/17/2003
ICSF Support (OS/390 V2R10) - z990	11/21/2003



IBM @server zSeries

zSeries Explorers



Reminder: Service End Dates

✗ Out of service

- All OS/ 390 Releases V2R9 and below

➤ OS/390 V2R10

- September 30, 2004

➤ z/OS V1R1

- March 31, 2004

➤ z/OS V1R2

- October 31, 2004

➤ z/OS V1R3

- March 31, 2005

➤ z/OS V1R4

- March 31, 2007



z990 PCI Crypto Configuration Rules

- ▲ Up to 2 PCICA features* per I/O cage and 6 features per CEC.
- ▲ Up to 4 PCIXCC features* per I/O cage and 4 features per CEC.
- ▲ Total number of PCICA / PCIXCC features* may not exceed 8 per CEC
- ▲ Any combination of PCIXCC, PCICA, OSA-Express and FICON-Express features* may not exceed 20 features per I/O cage and 60 features per CEC.
- ▲ PCIXCC and PCICA features do **not** use CHPIDs from the Logical Channel Subsystem pool.

(*) One PCICA feature = Two Coprocessors
One PCIXCC feature = One Coprocessor



PCI Crypto Feature Codes

PCICC (requires diskette FC 0864 or 0865)

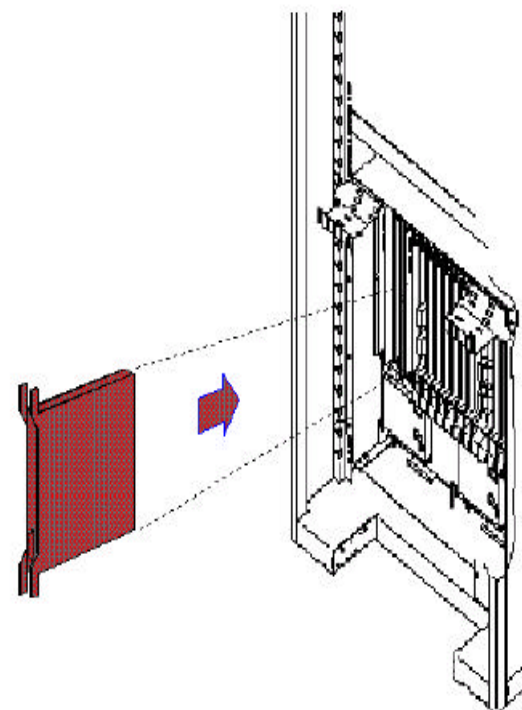
Feature Code	Maximum Number of Features	Maximum Number of Crypto Coprocessors
G5/G6 0860	8	8
zSeries 0861	8	16

PCICA (no diskette - FC 3863 must be enabled)

Feature Code	Maximum Number of Features	Maximum Number of Crypto Coprocessors
zSeries 0862	6	12

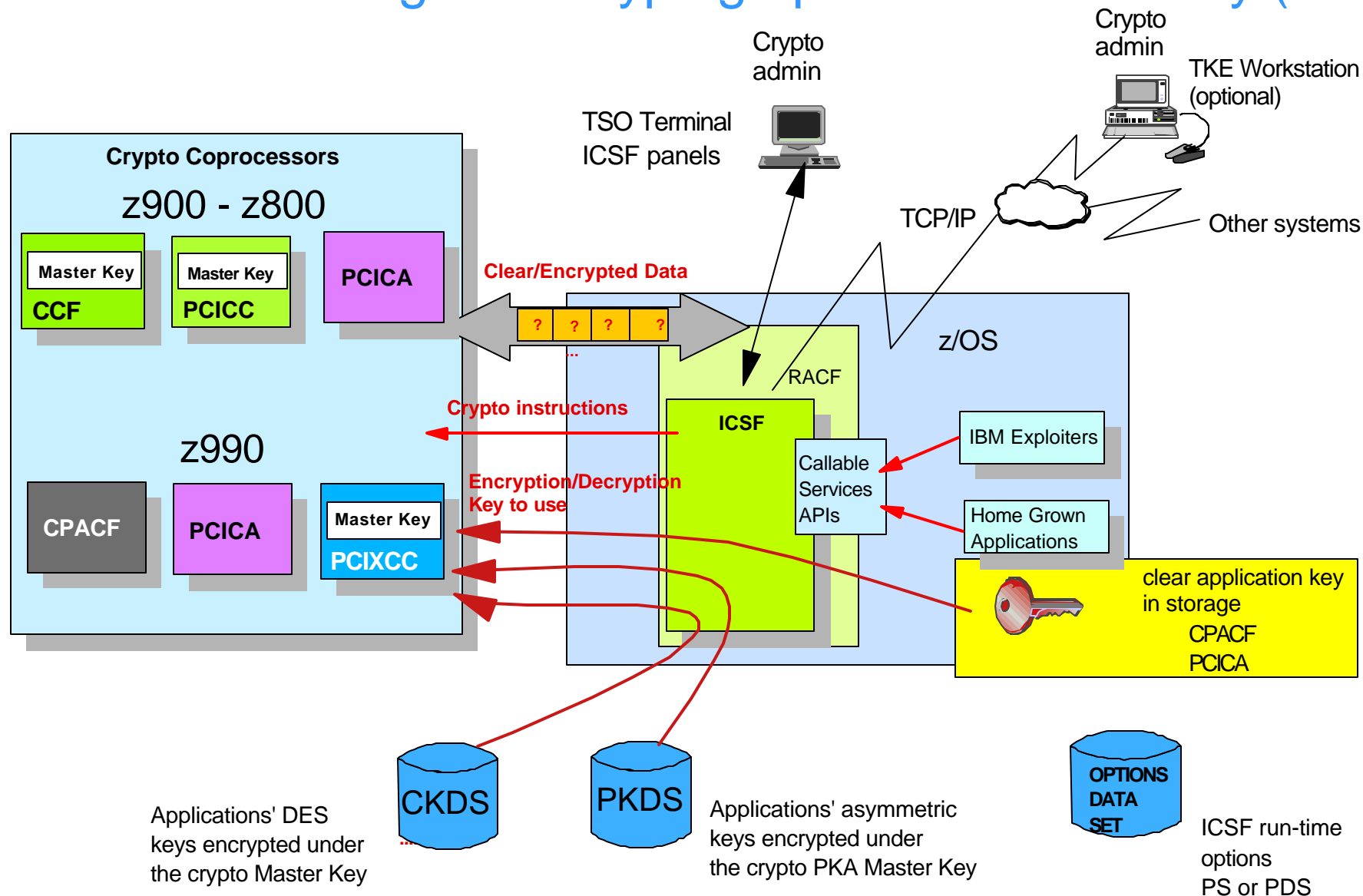
PCIXCC (no diskette - FC 3863 must be enabled)

Feature Code	Maximum Number of Features	Maximum Number of Crypto Coprocessors
zSeries 0868	4	4





z/OS Integrated Cryptographic Service Facility (ICSF)





IBM @server zSeries

zSeries Explorers



HCR7708 - Hardware Support

- ICSF HCR7708 will start on all crypto models
 - ▶ G5/G6 - all existing function enabled
 - ▶ z900 2064/2066 - all existing function enabled
 - ▶ z990 2084 -
 - Clear key DES functions (CP Assist instructions)
 - Clear key RSA functions with optional PCICA
 - PCIXCC **not** supported
 - No cryptography with encrypted keys
 - CKDS and PKDS **not** supported
 - TKE **not** supported



IBM @server zSeries

zSeries Explorers



HCR7708 - Services Available on a z990

- Encode (CSNBECO)
- Decode (CSNBDCO)
- MDC Generate (CSNBMDG,CSNBMDG1)
- One-Way Hash (CSNBOWH,CSNBOWH1)
- PKA Decrypt (CSNDPKD) - requires PCICA, PKCS-1.2 formatting
- PKA Encrypt (CSNDPKE) - requires PCICA, ZERO-PAD formatting
- Symmetric Key Decipher (CSNBSYD, CSNBSYD1)
- Symmetric Key Encipher (CSNBSYE, CSNBSYE1)



IBM @server zSeries

zSeries Explorers



HCR7708 - Services Available on a z990 (continued)

- ▶ Control Vector Generate (CSNBCVG)
 - ▶ PKA Key Token Build (CSNDPKB)
 - ▶ Code Conversion (CSNBXEA, CSNBXAE)
 - ▶ Character/Nibble Conversion (CSNBXBC, CSNBXCB)
 - ▶ X9.9 Data Editing (CSNB9ED)
- ✗ All other services will fail with **12/8** return/reason code



IBM @server zSeries

zSeries Explorers



HCR7708 on a z990 - Considerations

- Most hardware cryptographic applications will not run
- z/OS V1R4 System Secure Socket Layer will run
- All applications requiring CKDS or PKDS support will not run - this includes
 - ▶ z/OS Communication Server VTAM Session Level Encryption
 - ▶ z/OS Communication Server IP Services
 - ▶ z/OS OCSF hardware crypto CSP
 - ▶ z/OS Security Server RACF using PKDS
- HCR7708 is available as a web deliverable*
 - ▶ will be replaced by HCR770A

* <http://www-1.ibm.com/servers/eserver/zseries/zos/downloads/>



IBM @server zSeries

zSeries Explorers



HCR770A - Hardware Support

- HCR770A will start on all crypto models
 - ▶ G5/G6 - all existing function enabled
 - ▶ z900 2064/z800 2066 - all existing function enabled
 - ▶ z990 2084 -
 - most existing function enabled with optional PCIXCC and PCICA
 - clear key DES functions (CP Assist instructions)



IBM @server zSeries

zSeries Explorers



HCR770A - Changes

- PKDS initialization
 - ▶ Required before reading or writing keys
 - ▶ TSO panel utility available
- Options Data Set
 - ▶ CKTAUTH(YES|NO) - new
 - Controls authentication of CKDS records at dataspace creation and when CKDS is reenciphered
 - ▶ COMPENC - ignored
- CICS default waitlist has additional services
- NOCV KEKs
 - ▶ Caller not required to be in supervisor state to write a NOCV KEK to the CKDS



IBM eServer zSeries

zSeries Explorers



HCR770A on a z990 - Considerations

- Special Secure Mode (SSM)
 - ▶ Software enforced only via options data set
 - ▶ Hardware control is replaced by access control points in PCIXCC
- NOCV KEK usage will be controlled by access control points in PCIXCC
- Return/reason codes may change
 - ▶ Most parameter checking done in PCIXCC
- HCR770A is available as a web deliverable*
 - ▶ Replaces HCR7708

* **<http://www-1.ibm.com/servers/eserver/zseries/zos/downloads/>**



IBM @server zSeries

zSeries Explorers



Enhanced CCA Services

- Encrypted PIN Verify (CSNBPVR) will support VISAPVV4 (PIN must be 4 digits long)
 - ▶ G5, G6 or z900 2064 with PCICC required
 - ▶ z990 2084 with PCIXCC required
- MAC Generate (CSNBMGN) and MAC Verify (CSNBMVR) will support segmenting (FIRST, MIDDLE, LAST) of text for requests routed to PCICC
 - ▶ restriction on G5, G6 and 2064 with PCICC
 - ▶ 2084 with PCIXCC has no restrictions



IBM @server zSeries

zSeries Explorers



z990 CKDS, PKDS and UDX Considerations

z990 CKDS and PKDS

- Not used with clear keys, but required to be online
- G5, G6 , z900, z800 CKDS and PKDS directly reusable with z990 PCIXCC (assuming KMMK=SMK)
- CKDS initially created for z990 is not useable for legacy machines

z990 - User Defined Extensions (UDX) with PCIXCC

- Built under contract by IBM or approved third party vendor
- Customer is provided with a LIC CD to be loaded
- IBM will perform the existing PCICC UDXs migration under contract

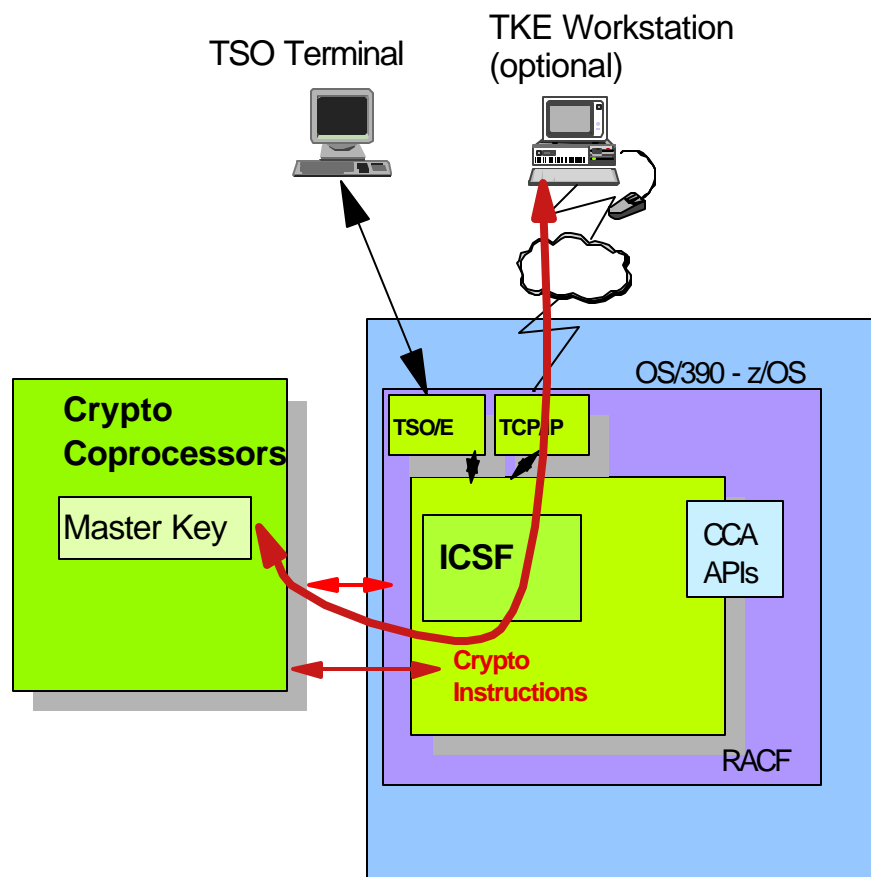


IBM @server zSeries

zSeries Explorers



Overview of Trusted Key Entry (TKE) workstation



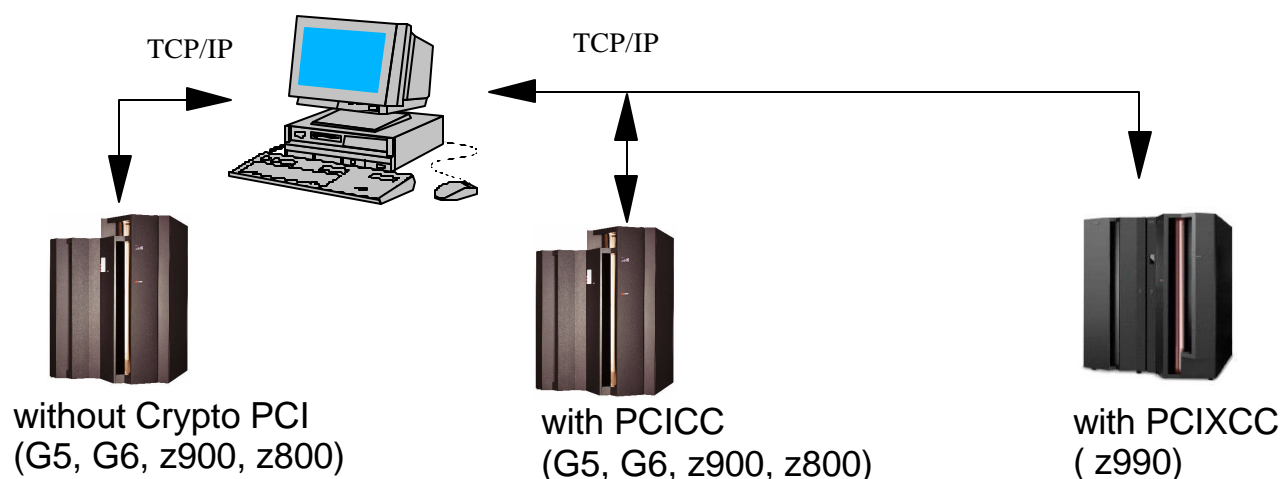
- Priced feature
- Highly secure connection over TCP/IP network to an ICSF host - The CSFTTCP listener program provided with ICSF
- Increased security for
 - Access to cryptographic coprocessors
 - Authorities (security officers) identified by their password and digital signature
 - Option to require multiple signatures before performing a crypto function
 - SOD for smart card support
 - Communications with coprocessors
 - Interactions are digitally signed both ways and, when appropriate, encrypted
- Can administer coprocessors as groups
- ICSF ISPF panels still needed



Support of z990 PCIXCC by TKE

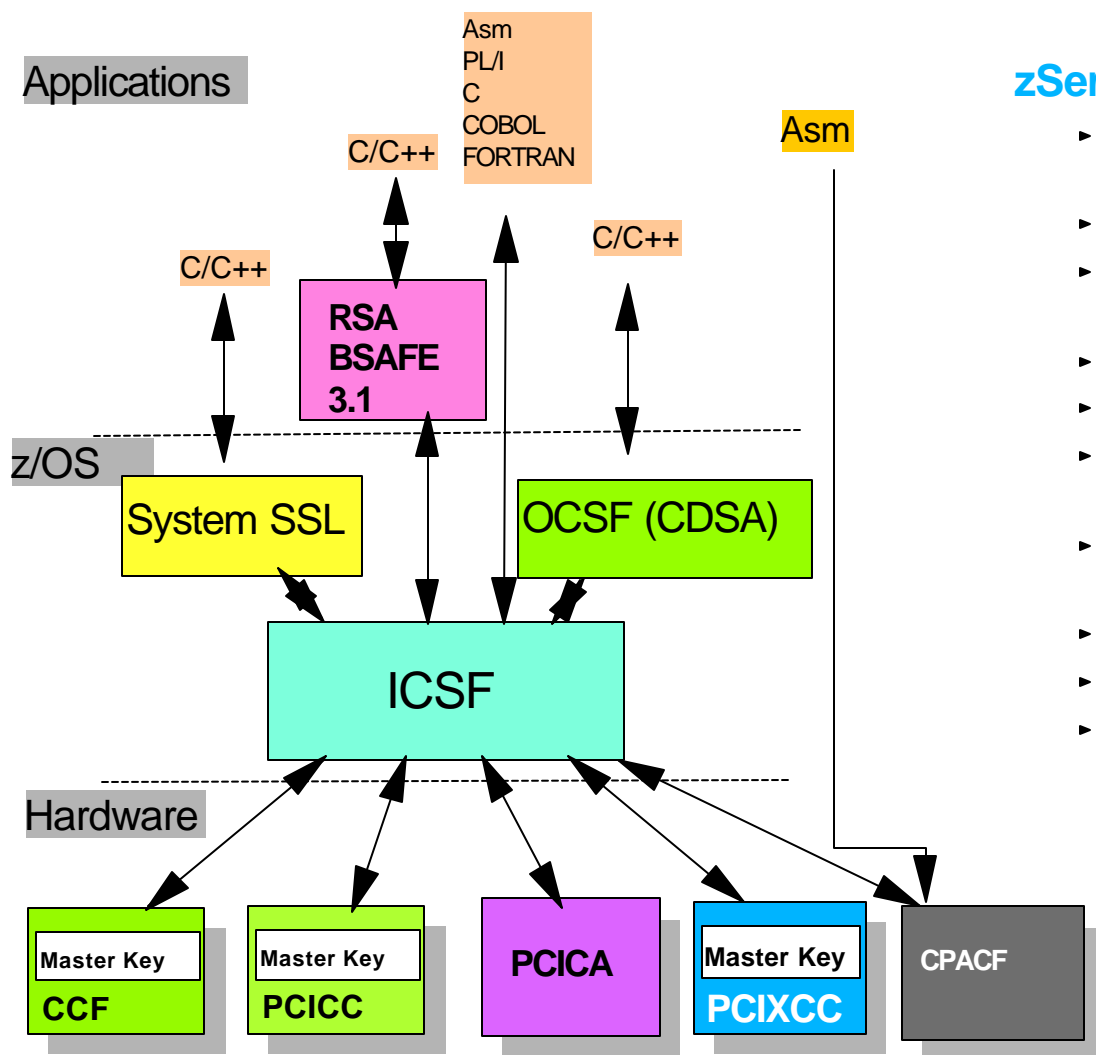
TKE V4.0 required

- Can be brand new or TKE V3.x (G5, G6 or zSeries) with TKE code Feature Code 0851
- Brand new TKE is FC 0886 (Ethernet) or 0889 (Token Ring)
- Secure PCIXCC key entry and key management





Cryptographic Coprocessors Exploiters



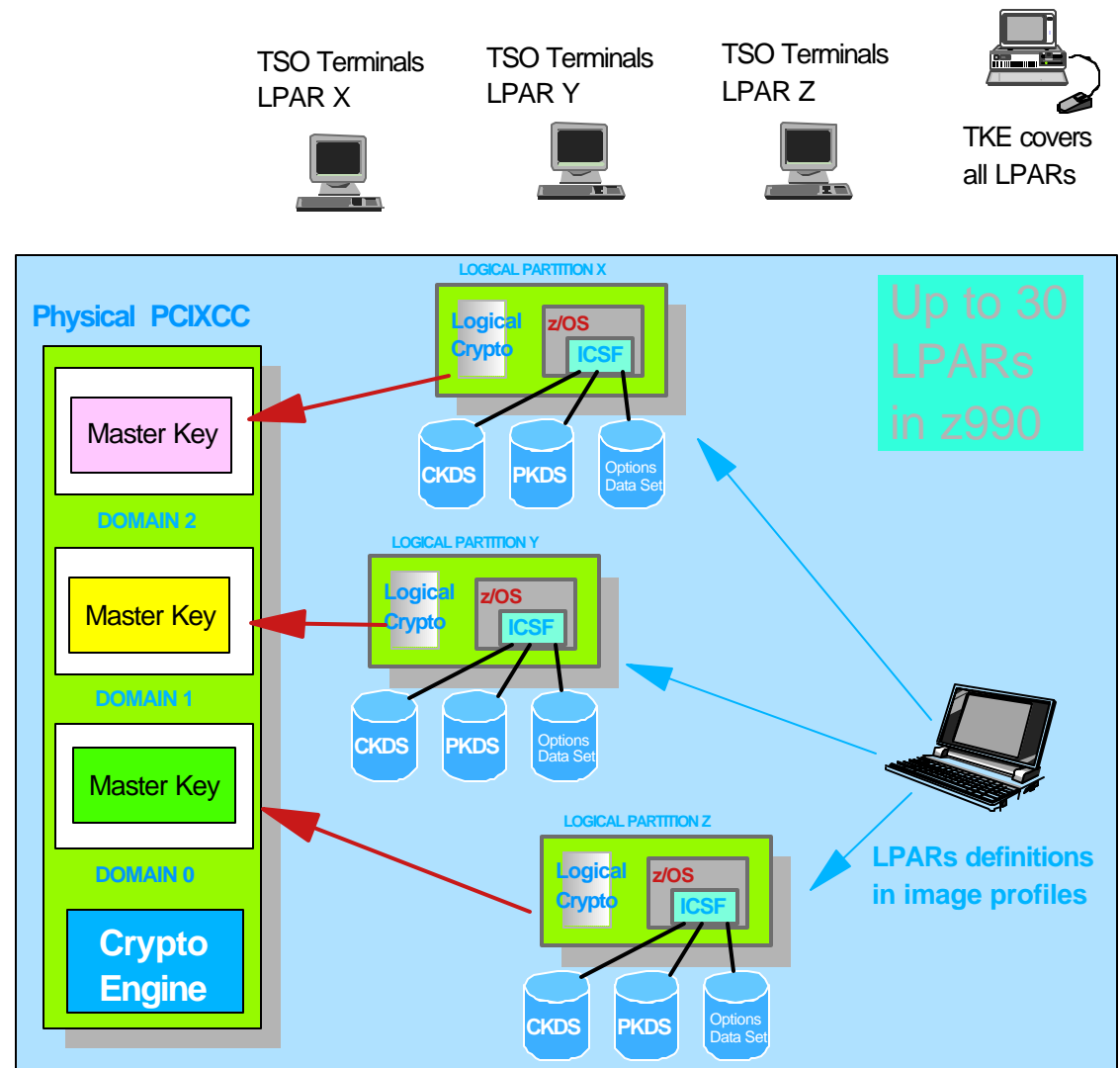
zSeries hardware crypto in use today by:

- System SSL (HTTP, LDAP, TN3270, FTP, CICS/TS, WAS)
- IBM Payment Suite e-commerce solutions
- Firewall Technology IPsec (VPN) and IKE (Internet Key Exchange)
- DCE Security Server
- VTAM
- CBT (Crypto Based Transactions) banking solution
- Open Cryptographic Services Facility (CDSA APIs)
- RACF
- z/OS Kerberos
- Java JCE and JSSE



The z/OS Cryptographic Coprocessors and PR/SM

- 16 'domains' in a physical secure coprocessor (CCF, PCICC, PCIXCC)
- Each domain has a physically separated set of master key registers
- Each logical partition uses a single dedicated domain in the secure coprocessors
- The domain to use is designated in the logical partition image profile and in the ICSF Options Data Set
- A coprocessor or accelerator can be made available to up to 16 logical partitions





Planning LPARs Domain and Cryptographic Coprocessors

Coprocessor ID	AP0	AP1	AP2	AP3	AP4	AP5	AP6	APn
Type	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC	PCICA or PCIXCC
LPAR 0	0	0				0	0	
LPAR 1			0	0	0			
LPAR 2	0	0	0	0				
LPAR 4	4 14	4 14	4 14	4 14	4 14	4 14	4 14	
LPAR 5				1	1	1	1	
LPAR n								

- ✓ LPAR 0 and 1 use domain 0, but are assigned to different cryptographic coprocessors. The combination domain number and cryptographic coprocessor number is unique across partitions.
- ✓ LPAR 4 uses domain 4 and 14. No other partition uses the same domain number.
- ✓ LPAR 5 uses domain 1 and no other partition uses the same domain number.
- ✗ LPAR 2 uses domain 0 on the set of cryptographic coprocessors already used by LPAR 0 and LPAR 1. LPAR 2 cannot be active concurrently with LPAR 0 or LPAR 1.
(Valid configuration for backup situations)



LPAR Activation Error

SCZHC2: Hardware Management Console Workplace (Version 1.8.0)

Views

Groups Exceptions Active Console Task Books

Activate Progress

Function duration time: 00:02:00
Elapsed time: 00:00:26

Object Name	Status
SCZP901:A02	Completed
SCZP901:A03	Failed-double click for more de
SCZP901:A04	Failed-double click for more de
SCZP901:A05	Failed-double click for more de

OK Help

SCZP802 A5
SCZP802 LINUX1

(WTSCZVM1) (TCPLEX:TC6)

SCZP901 A03 SCZP901 A04 SCZP901 A05 SCZP901 A06 SCZP901 A07 SCZP901 A08
SCZP901 A09 SCZP901 A0A SCZP901 A0B SCZP901 A11 SCZP901 A12 SCZP901 A13
SCZP901 A14 SCZP901 A15 SCZP901 A16 SCZP901 A17 SCZP901 A18

Display details by double-clicking an Image icon or start a task by dragging an Image icon to a task icon.

SCZP901:A03 Failure Details

Activation of logical partition A03 failed because one or more combination of cryptographic usage domain index and PCI cryptographic candidate list value(s) are currently in use by another active logical partition.

The combination of usage domain index and PCI candidate list values must be unique among all active logical partitions in the system.

Ask your system programmer to do the following.

Change the combination of usage domain index and PCI candidate list values selected so that there are no duplicate combinations among all active logical partitions.

ACTZ212

OK



IBM @server zSeries

zSeries Explorers

IBM

Logical Partition Image Profile - Processor Page (z900)

AFPS26SE - State Active - Keystrokes remote
Keystrokes Session Services Help

AFPS26SE Customize Image Profiles: AFPS26SE

Logical processor assignment

☐ Dedicated central processors

☒ Not dedicated central processors

Not dedicated central processor details

Initial processing weight 1 to 999 ☐ Initial capping

Number of processors - Initial Reserved

Cryptographic coprocessors

Cryptographic coprocessor 1
Cryptographic coprocessor 0

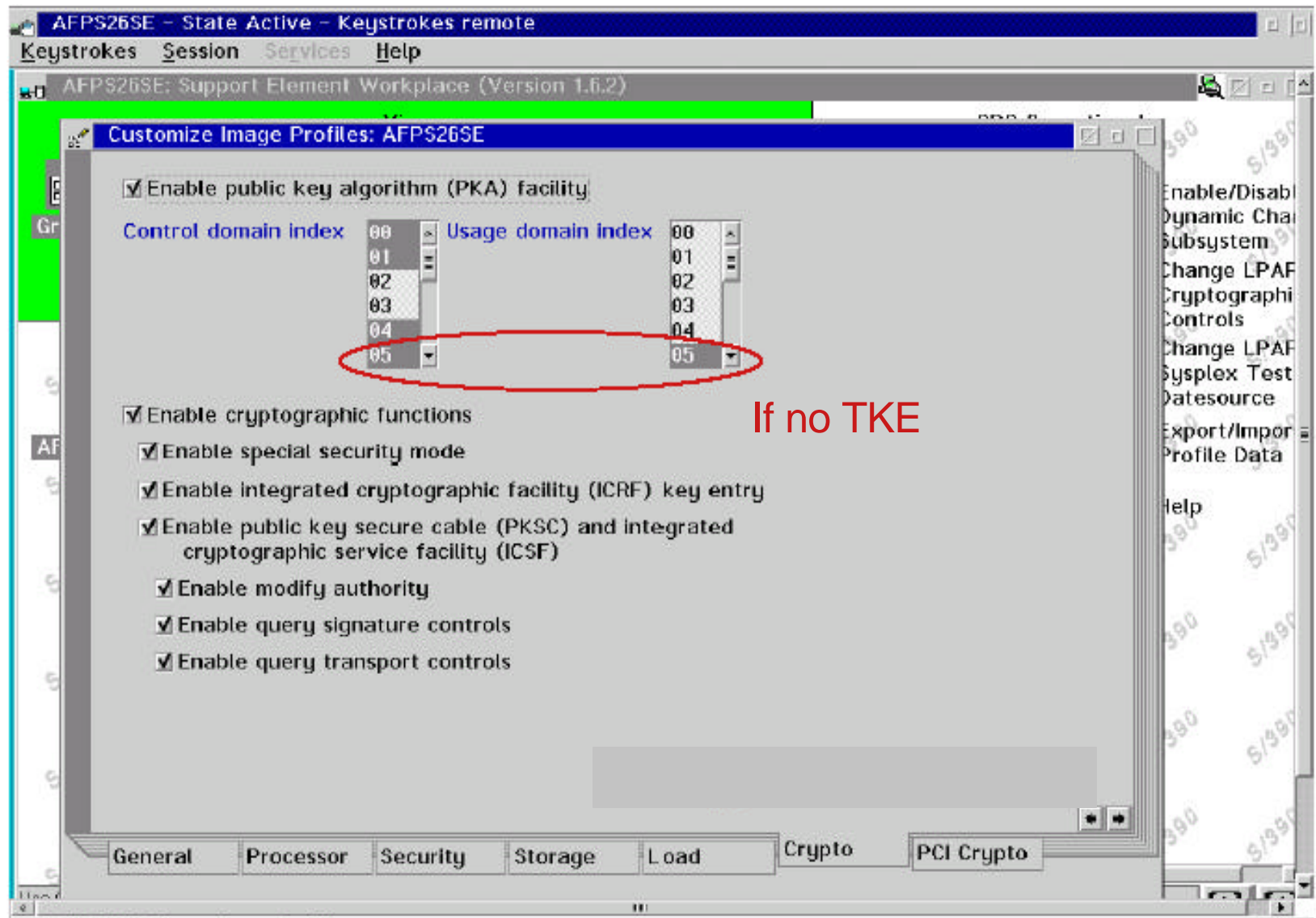
☐ Enable asynchronous data mover (ADM) facility

General Processor Security Storage Load Crypto **PCI Crypto**

Save Copy notebook Paste notebook Cancel Help

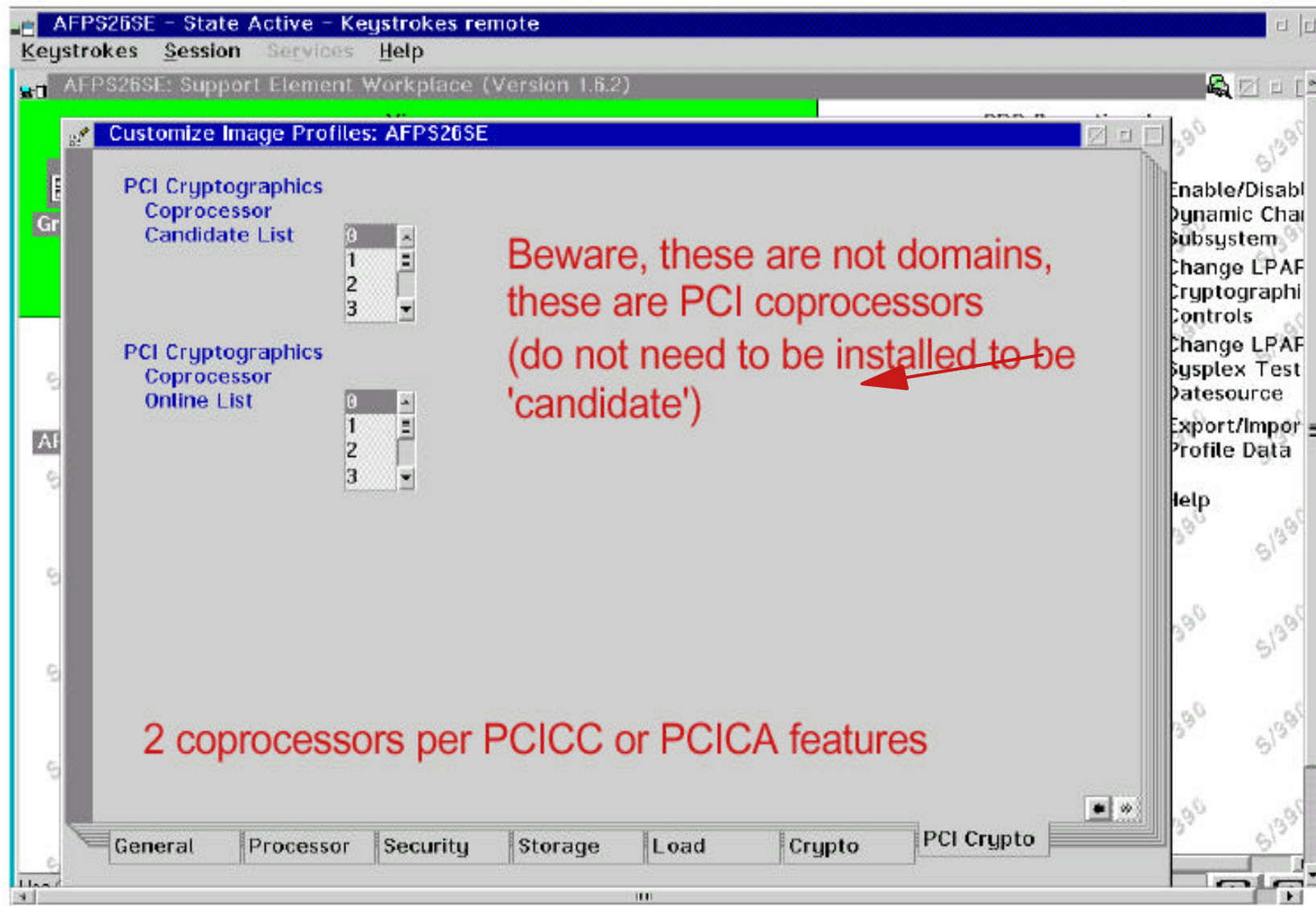


Logical Partition Image Profile - Crypto Page (z900)





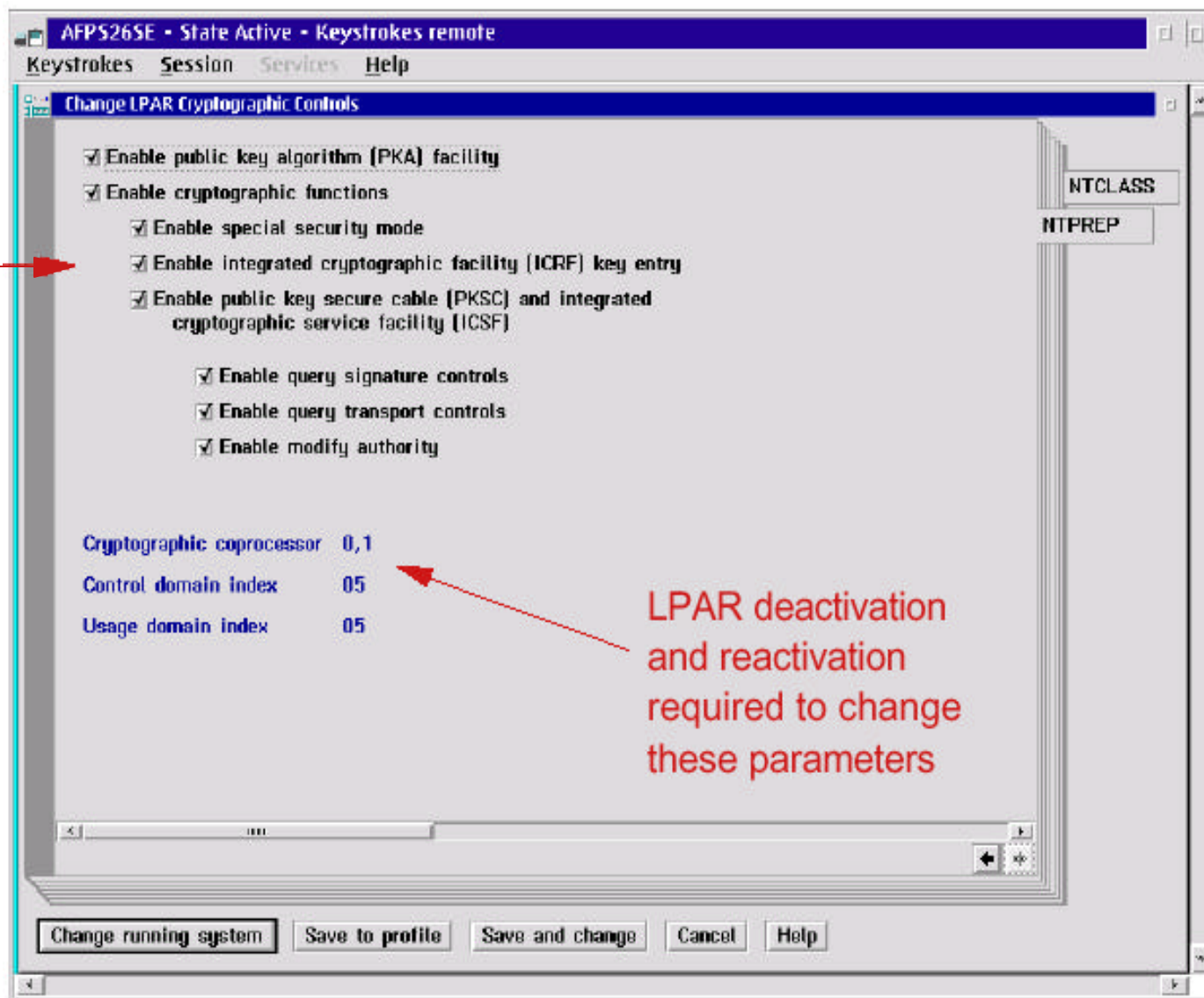
Logical Partition Image Profile - PCI Crypto Page (z900)





LPAR Dynamic Cryptographic Controls (z900)

can be changed
dynamically



LPAR deactivation
and reactivation
required to change
these parameters



IBM @server zSeries

zSeries Explorers

IBM

z990 CPACF DES/TDES Enablement (Support Element)

SCZP901 Details

Instance information

CP Status:	Operating	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 ICFPs:	3

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

<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 / A08-305	Manufacturer:	IBM
Machine serial:	02 - 0026A3A	CPC serial:	000020026A3A
Machine sequence:	000000026A3A	CPC location:	A19B
Plant of manufacture:	02	CPC identifier:	00

Save Change Options... Upgrade reasons... Cancel Help



IBM @server zSeries

zSeries Explorers



Logical Partition Image Profile - General Page (z990)

SCZHM2: Hardware Management Console Workplace (Version 1.8.0)

Views CPC Operational

Customize Image Profiles: SCZP901

Profile name: A02

Description: A02 image profile

Partition identifier: 2

Mode: ESA/390, ESA/390 TPF, Coupling facility, LINUX Only

Clock type assignment:
☒ Standard time of day
☐ Logical partition sysplex timer offset

General Processor Security Storage Options Load **PCI Crypto**

Save Copy notebook Paste notebook Cancel Help

Use CPC Operational Customization tasks to customize CPC operational characteristics.

Advanced I/O Queir
le I/O
ity Queir
ge LPAR
ity Queir

PCI Crypto Tab only



IBM @server zSeries

zSeries Explorers



Logical Partition Image Profile - PCI Crypto Page (z990)

Customize Image Profiles: SCZP901

Control domain index	06 07 08 09 10 11	Usage domain index	06 07 08 09 10 11
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

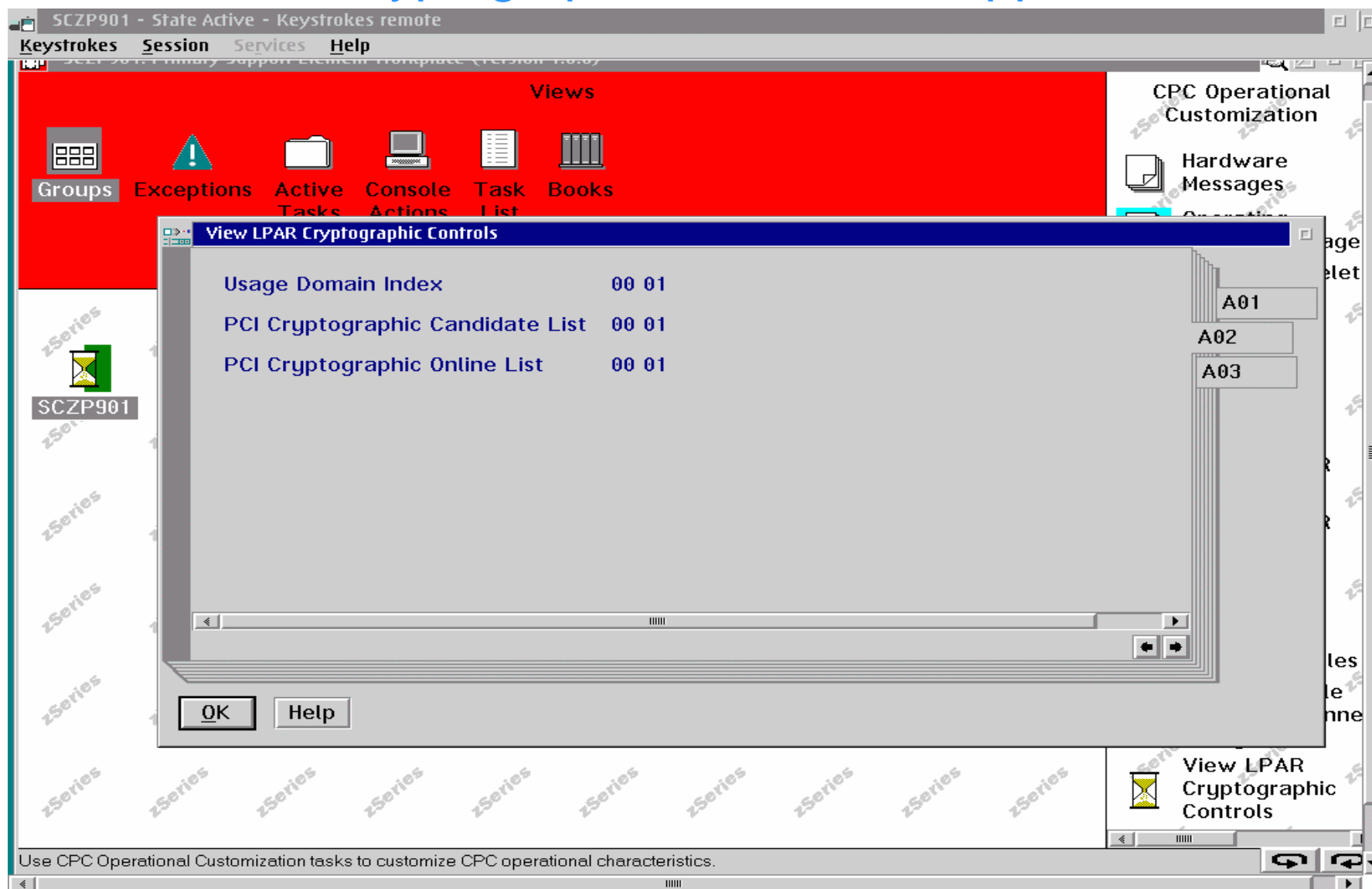


IBM @server zSeries

zSeries Explorers



LPAR Cryptographic Controls - Support Element





IBM @server zSeries

zSeries Explorers



z990 RMF Report Changes

- **Crypto Activity (CRYPTO) report in Postprocessor and Monitor I**
 - ▶ I/O Queuing (IOQ) reports in Postprocessor, Monitor I, Monitor II, Monitor III
 - ▶ Channel Path (CHAN) report in Postprocessor and Monitor I
 - ▶ New and changed OVERVIEW CONDITIONS for IOQUEUE and CRYPTO
- **New Spreadsheet Reporter**
 - ▶ Available for z/OS V1R2 and above
 - ▶ Shipped as SPE with APAR **OW56656** and with z/OS V1R5





IBM @server zSeries

zSeries Explorers



z/OS Crypto Activity SMF Recording

- SMF Record Type 30 contains SMF30CSC : number of crypto instructions executed on behalf of caller
- type 82 reports information about events and operations of ICSF
 - ▶ subtype 17 provides some information on the PCICC utilization
 - ▶ all other subtypes report on administrative kinds of operations
 - ▶ beginning with z/OS V1R3, CSFSMFJ and CSFSMFR sample jobs are available in SYS1.SAMPLIB to format type 82 records
- type 70 (RMF Processor Activity) - z/OS V1R2 with APAR OW49808
 - ▶ subtype 2 contains measurements of cryptographic coprocessors activity
- type 72 (RMF Workload Activity and Storage Data)
 - ▶ reports on class period and crypto support by WLM (z/OS V1R2 with APAR OW49808) using subtype 3 records



z/OS Crypto Hardware Activity

SMF Type 70-2

```
1                CRYPTO HARDWARE ACTIVITY                PAGE 1
                z/OS V1R3      SYSTEM ID VSN9      DATE 09/11/2002      INTERVAL 29.59.999
                RPT VERSION V1R2 RMF      TIME 14.00.00      CYCLE 1.000 SECONDS
0--- PCI CRYPTOGRAPHIC COPROCESSOR ---
----- TOTAL ----- KEY-GEN
ID  RATE EXEC TIME UTIL%  RATE
00 0.00  0.0  0.0  0.0
01 0.00  0.0  0.0  0.0
-
----- PCI CRYPTOGRAPHIC ACCELERATOR -----
----- TOTAL ----- ME(1024) ----- ME(2048) ----- CRT(1024) ----- CRT(2048) -----
ID  RATE EXEC TIME UTIL%  RATE EXEC TIME UTIL%  RATE EXEC TIME UTIL%  RATE EXEC TIME UTIL%  RATE EXEC TIME UTIL%
02 0.18  1.3  0.0  0.00  0.0  0.0  0.00  0.0  0.0  0.18  1.3  0.0  0.00  0.0  0.0
03 0.00  0.0  0.0  0.00  0.0  0.0  0.00  0.0  0.0  0.00  0.0  0.0  0.00  0.0  0.0
-
----- CRYPTOGRAPHIC COPROCESSOR FACILITY -----
DES ENCRYPTION  DES DECRYPTION  ---- MAC ----  - HASH -  ---- PIN ----
SINGLE TRIPLE  SINGLE TRIPLE  GENERATE  VERIFY  TRANSLATE  VERIFY
RATE  0.00  1.05  0.35  1.05  0.00  0.00  0.00  0.00  0.00  0.00
SIZE  0.00  209.3  176.0  297.3  0.00  0.00  0.00
```

SMF Type 72-3

```
---RESPONSE TIME---  EX  PERF  AVG  --USING%--  ----- EXECUTION DELAYS % -----  ---DLY%--  -CRYPTO%-  %
HH.MM.SS.TTT  VEL  INDX  ADRSP  CPU  I/O  TOTAL  CPU  I/O  AUX  AUX  SWIN  UNKN  IDLE  DLY  USG  QUIE
GOAL  00.00.05.000  90.0%
ACTUALS
*ALL  52.6% 31.8% 4.0  5.7  3.6  2.6  13.1  8.5  4.3  0.2  0.1  0.1  58.1 22.7 1.1 3.1 0.0
D0  57.5% 30.5% 4.0  2.1  3.5  2.3  13.3  9.0  4.2  0.1  0.0  0.1  60.3 20.5 0.2 1.1 0.0
D4  53.0% 49.4% 4.0  1.9  3.3  3.1  6.5  1.8  4.3  0.1  0.0  0.0  63.1 24.0 1.4 4.1 0.0
D6  45.5% 24.1% ***  1.8  3.9  2.3  19.8  14.8  4.3  0.1  0.4  0.1  50.3 23.7 0.3 0.3 0.0
```



Monitor I Crypto Hardware Activity Report

CRYPTO HARDWARE ACTIVITY

SYSTEM ID SYS1
RPT VERSION V1R5DATE 02/24/2003
TIME 09.00.00INTERVAL 60.00.378
CYCLE 1.000 SECONDSnew type
columnnew crypto
card
(type 5)header line
modified

----- CRYPTOGRAPHIC COPROCESSOR -----

----- TOTAL -----					KEY-GEN
TYPE	ID	RATE	EXEC TIME	UTIL%	RATE
PCIXCC	0	0.00	0.0	0.0	0.00
	1	0.01	3205	32.1	0.01
	6	83.44	1.1	8.8	0
	7	0.00	0.0	0.0	0.00

----- CRYPTOGRAPHIC ACCELERATOR -----

----- TOTAL -----					ME(1024)				CRT(1024)				CRT(2048)			
TYPE	ID	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%
PCICA	8	165.2	1.3	21.5	107.1	0	0	58.1	1.7	9.7	0	0	0	0	0	0
PCICA	9	2.4M	1.8	48.6	0	0	0	0	0	0	2.4M	1.8	48.6			

----- ICSF SERVICES EXECUTED ON PCIXCC -----

	DES ENCRYPTION		DES DECRYPTION		----- MAC -----		- HASH -	----- PIN -----	
	SINGLE	TRIPLE	SINGLE	TRIPLE	GENERATE	VERIFY		TRANSLATE	VERIFY
RATE	4975K	497.5	12438	1244K	12438	4975K	497.5	1244K	1346
SIZE	0.75	100K	10.00	0.01	10.00	0.01	10000		



IBM @server zSeries

zSeries Explorers



Bibliography

- z/OS Cryptographic Services ICSF Overview
- z/OS Cryptographic Services ICSF System Programmer's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Messages
- z/OS Cryptographic Services ICSF TKE Workstation User's Guide
- Processor Resource/Systems Manager Planning Guide
- Support Element Operations Guide
- SA22-7519
- SA22-7520
- SA22-7522
- SA22-7521
- SA22-7523
- SA22-7524
- SB10-7036
- SC28-6820-01

Redbook SG24-5455 Exploiting S/390 Hardware Cryptography with Trusted Key Entry
Redbook SG24-5942 S/390 PCI Crypto Coprocessor Implementation Guide
Redbook SG24-6870 zSeries Crypto Update



Acronyms

■ ANSI	American National Standards Institute	■ LIC	Licensed Internal Code
■ CA	Certification Authority	■ MAC	Message Authentication Code
■ CBC	Cipher Block Chaining	■ MD5	Message Digest 5
■ CCA	IBM Common Cryptographic Architecture	■ OAEP	Optimal Asymmetric Encryption Padding
■ CCF	Cryptographic Coprocessor Feature	■ OCSF	OS/390 Open Cryptographic Services Facility
■ CDMF	Commercial Data Masking Facility	■ OCSP	Online Certificate Status Protocol
■ CDSA	Common Data Security Architecture	■ PCICA	PCI Cryptographic Accelerator
■ CKDS	Cryptographic Key Data Set	■ PCICC	PCI Cryptographic Coprocessor
■ CRL	Certificate Revocation List	■ PCIXCC	PCI X Cryptographic Coprocessor
■ CRT	Chinese Remainder Theorem	■ PKA	Public Key Algorithm
■ CVC	Card Verification Code	■ PKCS	Public Key Cryptographic Standards
■ CVV	Card Verification Value	■ PKDS	Public Key Data Set
■ DES	Data Encryption Standard	■ PKI	Public Key Infrastructure
■ DSA	Digital Signature Algorithm	■ RA	Registration Authority
■ DSS	Digital Signature Standard	■ RACF	Resource Access Control Facility
■ ECB	Electronic Code Book	■ RSA	Rivest-Shamir-Adleman
■ FIPS	Federal Information Processing Standards	■ SET	Secure Electronic Transaction
■ ICSF	Integrated Cryptographic Service Facility	■ SHA-1	Secure Hash Algorithm 1
■ IETF	Internet Engineering Task Force	■ SLE	Session Level Encryption
■ IPKI	Internet Public Key Infrastructure	■ SSL	Secure Sockets Layer
■ KGUP	Key Generation Utility Program	■ TKE	Trusted Key Entry
■ LDAP	Lightweight Directory Access Protocol	■ TLS	Transport Layer Security
		■ VPN	Virtual Private Network



zSeries Explorers



IBM @server zSeries

Solução de Criptografia em z990 O que mudou ?

Vicente Ranieri Júnior

IBM Senior Certified Consulting IT Specialist
ranieri@br.ibm.com