IBM Americas, ATS, Washington Systems Center

Crypto Hardware on System z - Part 2

Greg Boyd (boydg@us.ibm.com)

ON DEMAND BUSINESS™

Agenda

- **Crypto Hardware - Part 1**
  - A refresher
  - A little bit of history
  - Some hardware terminology
  - CPACF
- **Crypto Hardware – Part 2**
  - A couple of refresher slides
  - Crypto Express Cards
  - HMC Slides

Crypto Functions

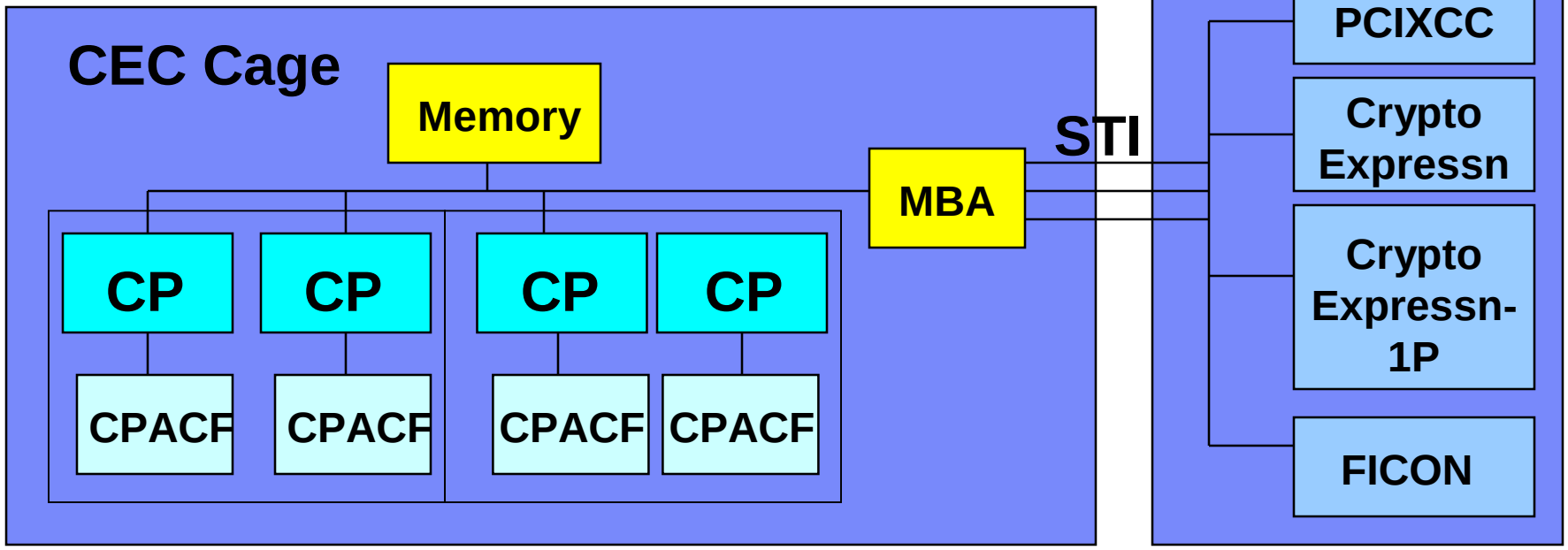
- **Data Confidentiality**
  - Symmetric – DES/TDES, AES
  - Asymmetric – RSA,Diffie-Hellman, EC
- **Data Integrity**
  - Modification Detection
  - Message Authentication
  - Non-repudiation
- **Financial Functions**
- **Key Security & Integrity**

Clear Key / Secure Key / Protected Key

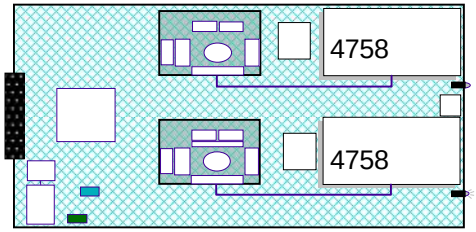
- **Clear Key – key may be in the clear, at least briefly, somewhere in the environment**
- **Secure Key – key value does not exist in the clear outside of the HSM (secure, tamper-resistant boundary of the card)**
- **Protected Key – key value does not exist outside of physical hardware, although the hardware may not be tamper-resistant**

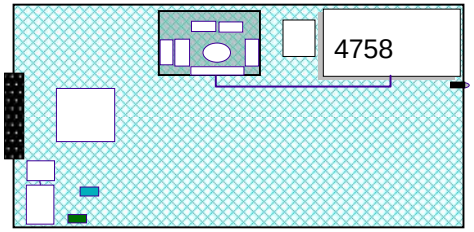
CPACF Machines (z890/z990 & later)

- CP Assist for Cryptographic Function (CPACF)
- Peripheral Component Interconnect (PCI Cards)

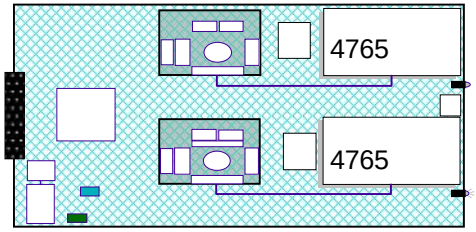


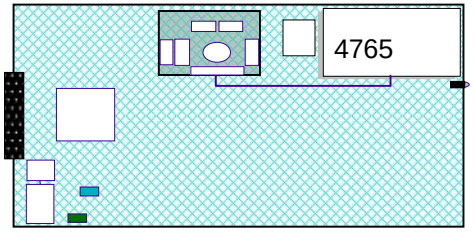
CEX2-1P/CEX2-1P (z890/z990, z9 EC/BC, z10 EC/BC)

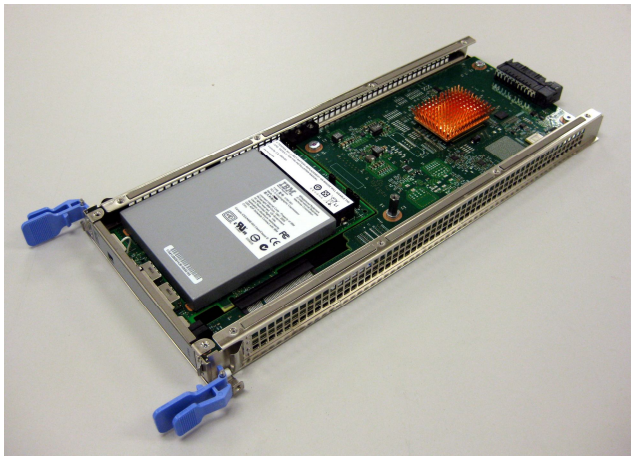




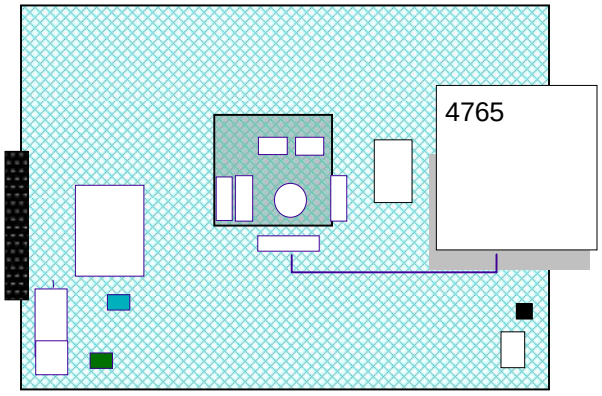
CEX3/CEX3-1P (z10 EC/BC, z196/z114, zEC12/zBC12)



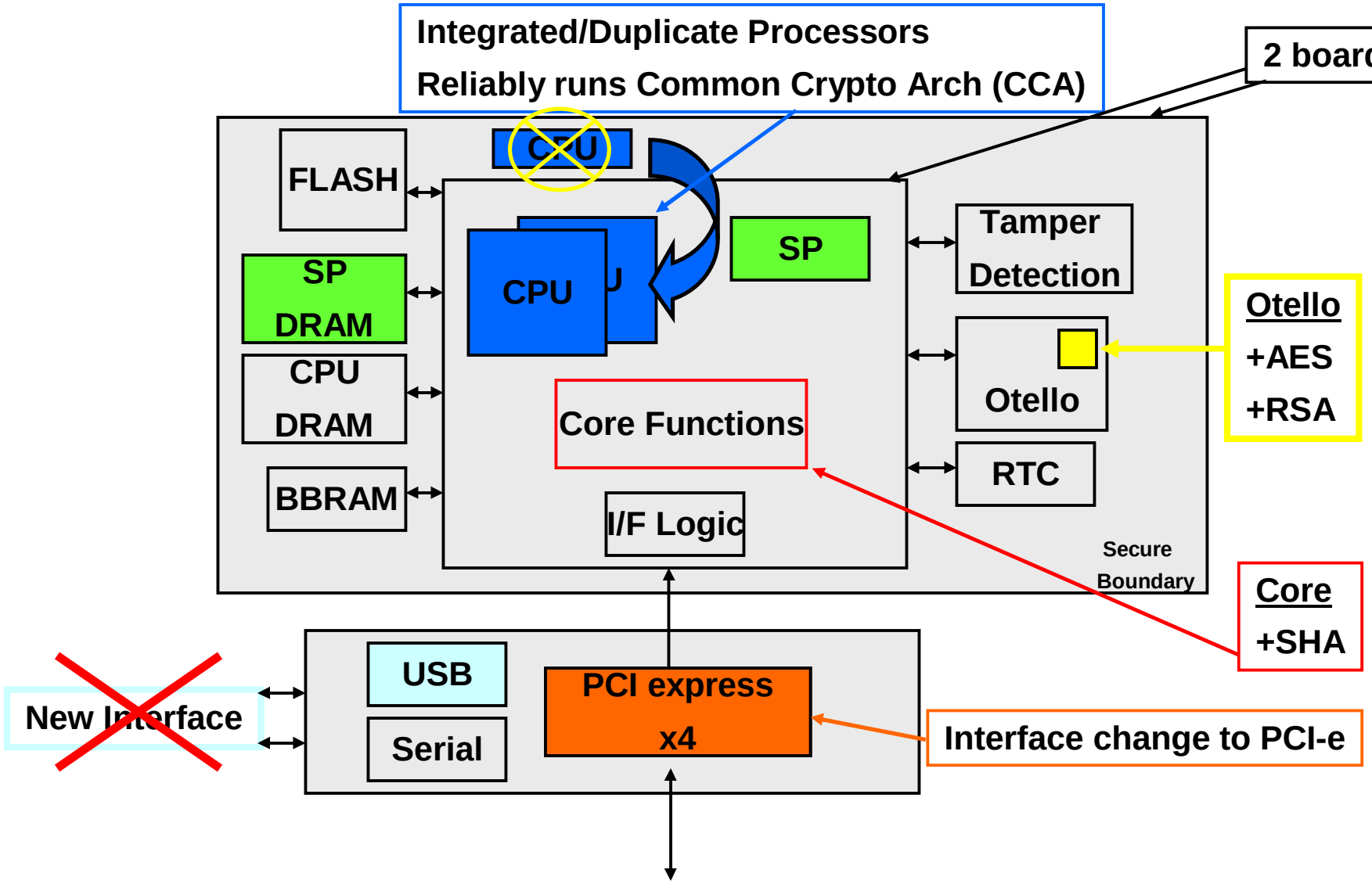




CEX4S (zEC12/zBC12)

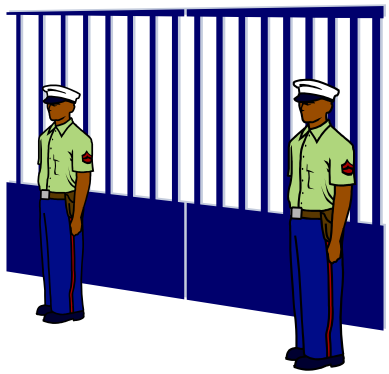


4765 Coprocessor



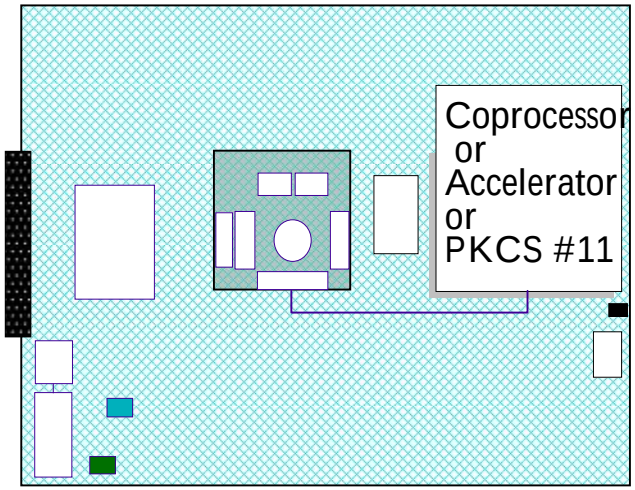
Hardware Security Module (HSM)

- **Tamper Detection**
  - Removal
  - Temperature
  - Probe Penetration
  - Power Sequencing
- **Tamper Response**
  - Zeroization of all keys
  - Permanently inoperable



Crypto Express

- Secure Key DES/TDES
- Secure Key AES
- Financial (PIN) Functions
- Key Generate/Key Management



- Random Number Generate and Generate Long
- Protected Key Support (CEX3)
- RSA & ECC Operations, including SSL Handshakes (CEX3)
- Secure Key PKCS #11 (CEX4S)

TechDoc WP100810 – A Synopsis of System z Crypto Hardware

Crypto Card Modes

- **Coprocessor**
  - Full CCA Function
  - Requires master key to be loaded
  - Supports User Defined Extension (UDX)
- **Accelerator**
  - Only supports SSL Handshakes (Public Key Encrypt, Public Key Decrypt, Digital Signature Verify)
- **EP11 (Enterprise PKCS #11)**
  - Only supports PKCS #11

User Defined eXtension

- **Extends the functionality of IBM's CCA (Common Cryptographic Architecture) application program**
  - Customized cryptographic verb controls per customer
- **UDX interfaces using HW control blocks and ICSF CB, therefore if hardware platform changes or ISCF level changes or both, then the UDX must be updated for the new control blocks**
- **On System z, IBM will develop the UDX to your specs**
  - Must be integrated in and work with ICSF

PCI Hardware – PKCS #11 Mode

- **PKCS #11 (from Wikipedia)**

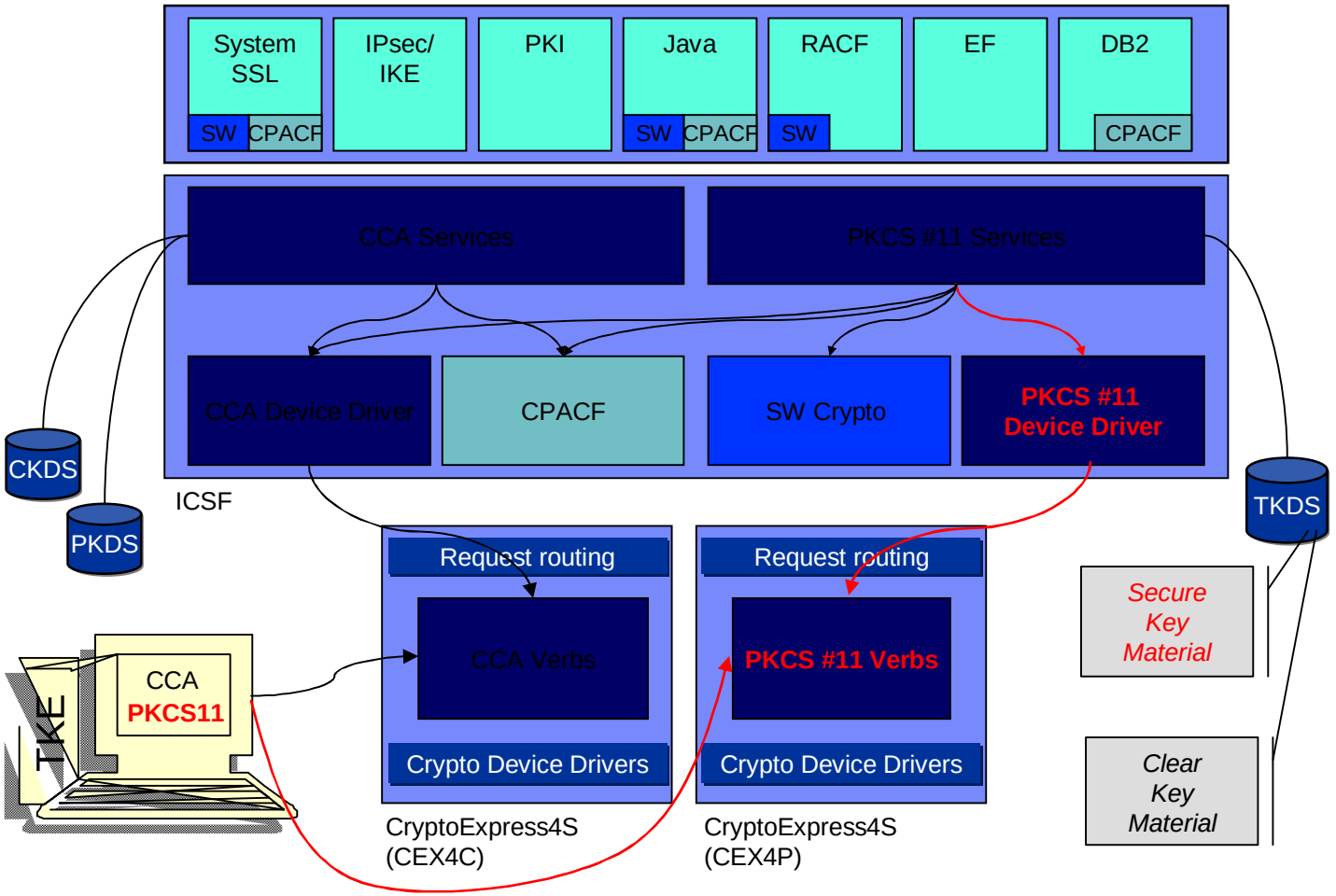
  Since there isn't a real standard for cryptographic tokens, this API has been developed to be an abstraction layer for the generic cryptographic token. **The PKCS #11 API defines most commonly used cryptographic object types (RSA keys, X.509 Certificates, DES/Triple DES keys, etc.) and all the functions needed to use, create/generate, modify and delete those objects.**

  PKCS #11 is largely adopted to access smart cards and HSMs. Most commercial Certification Authority software uses PKCS #11 to access the CA signing key or to enroll user certificates. Cross-platform software that needs to use smart cards uses PKCS #11, such as Mozilla Firefox and OpenSSL (using an extension).

- **PKCS #11 (from RSA, http://www.rsa.com/rsalabs/node.asp?id=2133)**

  This standard specifies an API, called Cryptoki, to devices which hold cryptographic information and perform cryptographic functions. **Cryptoki, pronounced crypto-key and short for cryptographic token interface, follows a simple object-based approach, addressing the goals of technology independence (any kind of device) and resource sharing (multiple applications accessing multiple devices), presenting to applications a common, logical view of the device called a cryptographic token.**

Enterprise PKCS #11 (EP11) Mode



EP11 enables Secure Key PKCS #11

Master Keys

- **Stored within the secure hardware boundary of the cryptographic coprocessor**
- **ICSF uses five master keys to protect operational keys**
  - DES Master Key (DES-MK aka SYM-MK) – 16 byte key (or now 24 byte)
    - Protects DES/TDES (symmetric) application keys

  - AES Master Key (AES-MK) - 256 bit key
    - Protects AES (symmetric) application keys

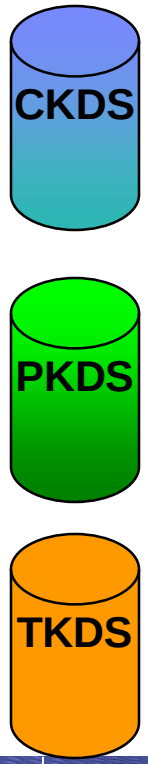
  - Asymmetric-keys master key (RSA-MK aka ASYM-MK) - 192 bit key
    - Protects RSA (asymmetric) private keys

  - Elliptic Curve Master Key (ECC-MK) - 256 bit key
    - Protects ECC (asymmetric) private keys

  - Enterprise PKCS #11 Master Key (P11-MK) - 256 bit key
    - Protects PKCS #11 keys

Nonvolatile Arrays for storing Master Keys

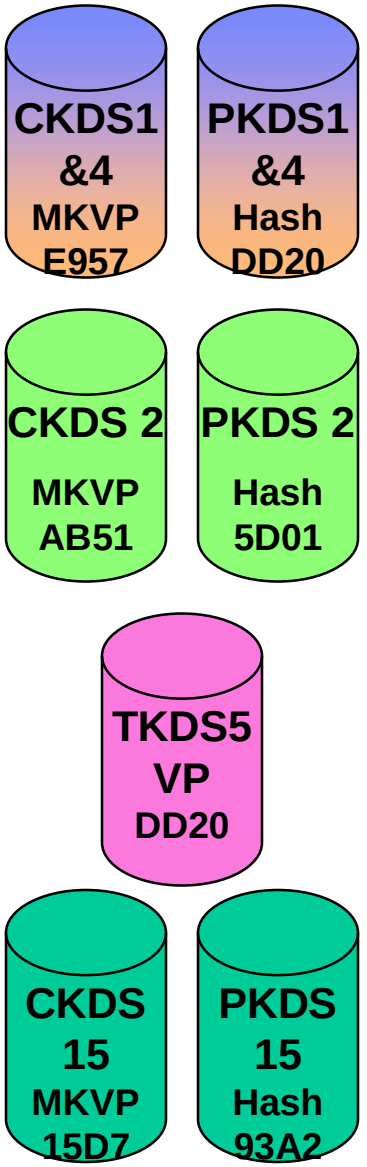
- **Current – where the master key resides**
- **New – staging area for building a new master key**
- **Old – provides one-back support**



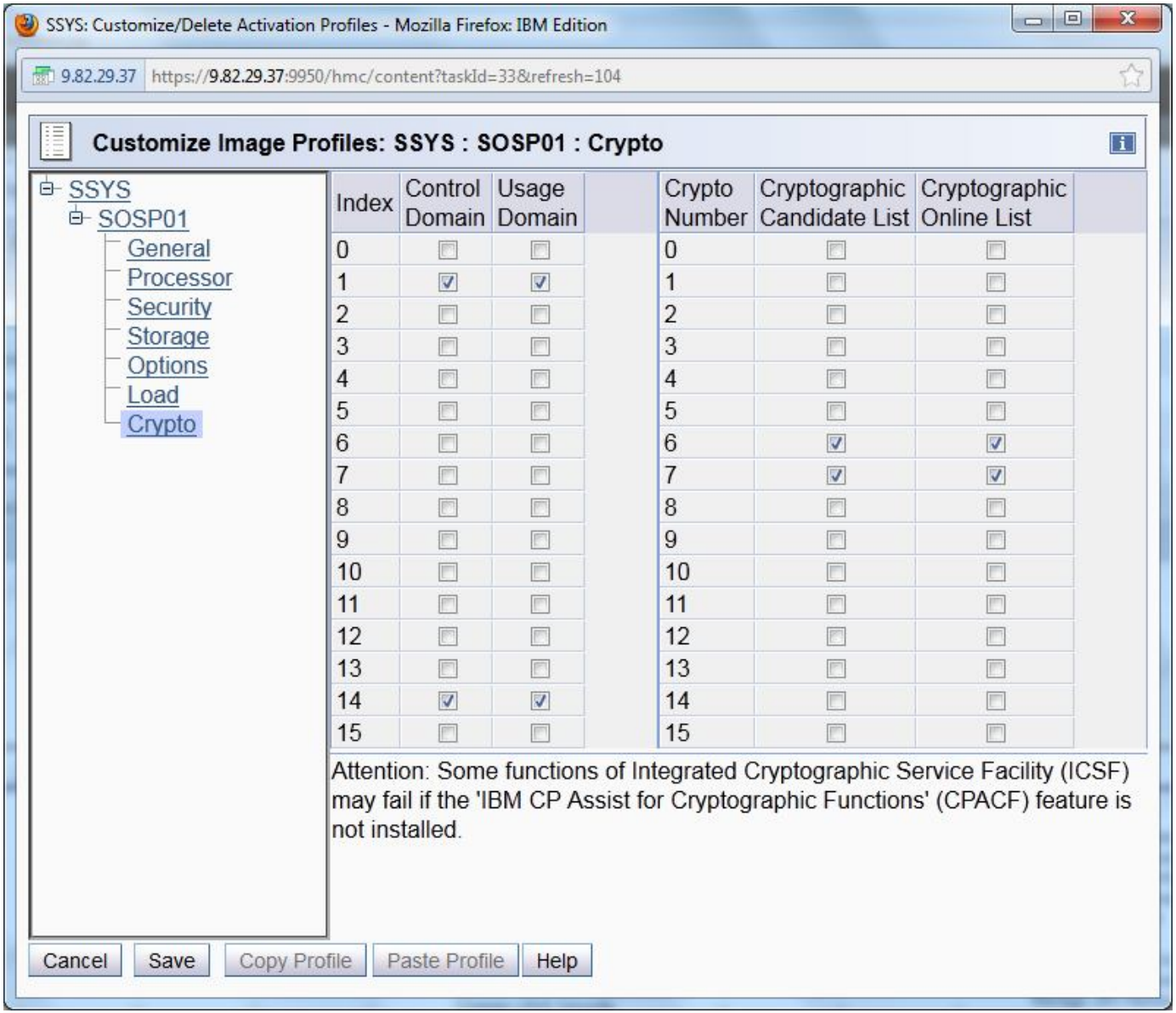
Current DES-MK	New DES-MK	Old DES-MK
Current AES-MK	New AES-MK	Old AES-MK
Current RSA-MK	New RSA-MK	Old RSA-MK
Current ECC-MK	New ECC-MK	Old ECC-MK
Current P11-MK	New P11-MK	

Usage Domains – storage of master keys

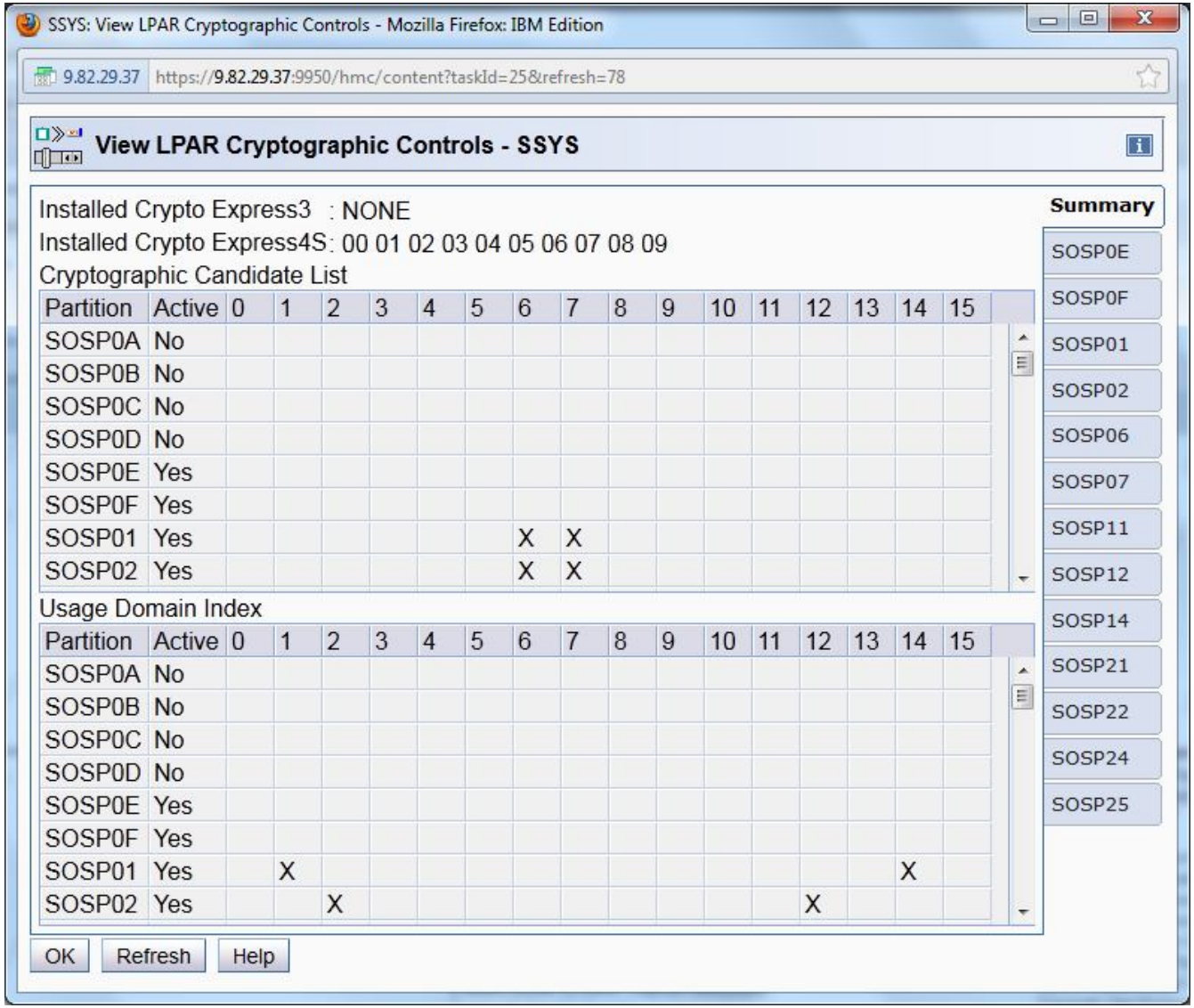
LPAR & Domain	DES Master Key	RSA Master Key	AES MK	ECC MK	P11 MK
LP1 UD1	ABC (MKVP=E957)	XYZ (Hash=DD20)	…	…	…
LP2 UD2	LP2KEY (MKVP=AB51)	PKAMST (Hash=5D01)	…	…	…
LP3					
LP4 UD4	ABC (MKVP=E957)	XYZ (Hash=DD20)	…	…	…
LP5					JKL (VP= 47CC)
…					
LP15 UD9	LP15KY (MKVP=15D7)	AKEY (MKVP=93A2)	…	…	…



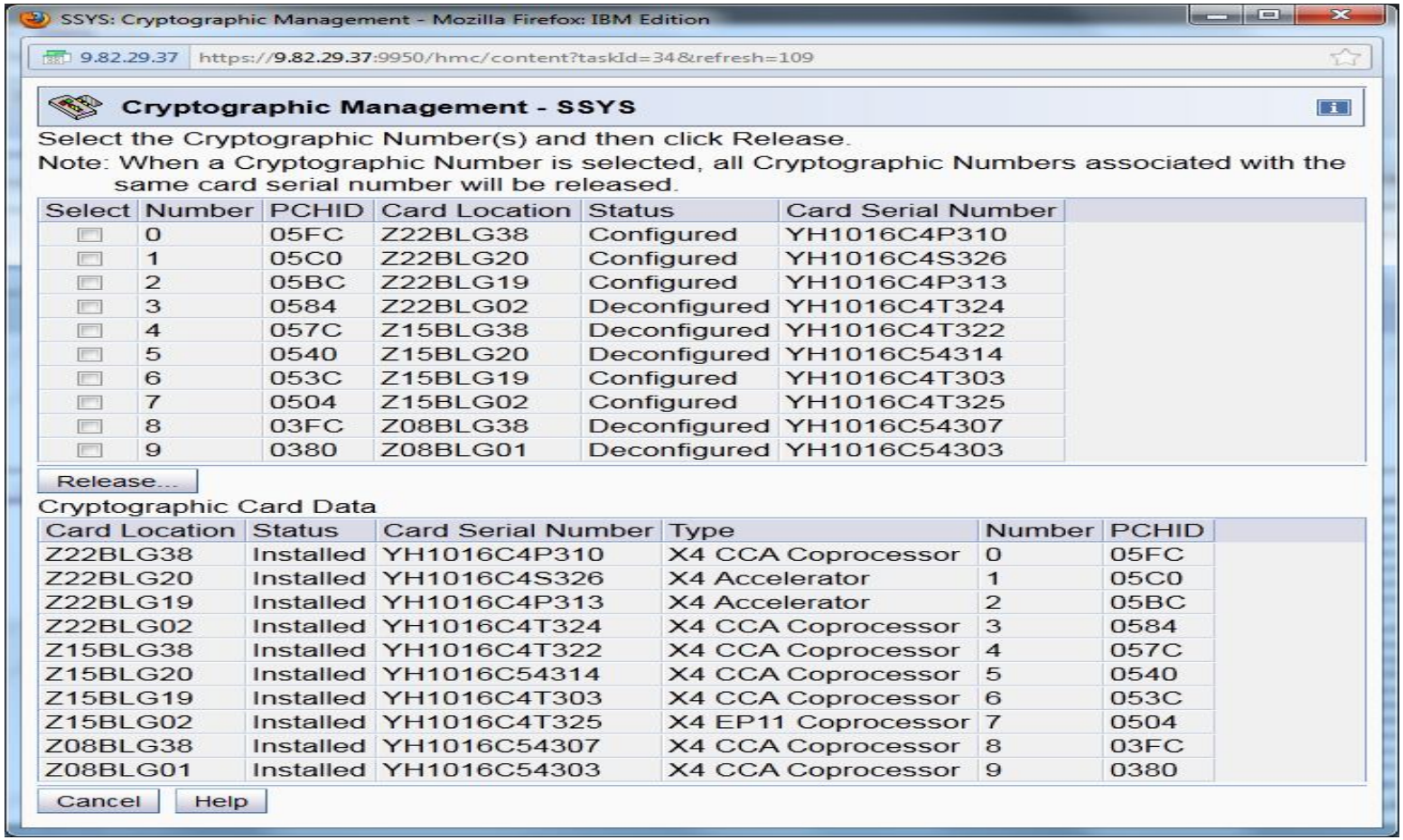
zEC12 Assigning Crypto to the Domain



zEC12 – View LPAR Crypto Controls



HMC/SE Screens – Cryptographic Management



SSYS: Cryptographic Management - Mozilla Firefox: IBM Edition

9.82.29.37 https://9.82.29.37:9950/hmc/content?taskId=34&refresh=109

Cryptographic Management - SSYS

Select the Cryptographic Number(s) and then click Release.

Note: When a Cryptographic Number is selected, all Cryptographic Numbers associated with the same card serial number will be released.

Select	Number	PCHID	Card Location	Status	Card Serial Number
☐	0	05FC	Z22BLG38	Configured	YH1016C4P310
☐	1	05C0	Z22BLG20	Configured	YH1016C4S326
☐	2	05BC	Z22BLG19	Configured	YH1016C4P313
☐	3	0584	Z22BLG02	Deconfigured	YH1016C4T324
☐	4	057C	Z15BLG38	Deconfigured	YH1016C4T322
☐	5	0540	Z15BLG20	Deconfigured	YH1016C54314
☐	6	053C	Z15BLG19	Configured	YH1016C4T303
☐	7	0504	Z15BLG02	Configured	YH1016C4T325
☐	8	03FC	Z08BLG38	Deconfigured	YH1016C54307
☐	9	0380	Z08BLG01	Deconfigured	YH1016C54303

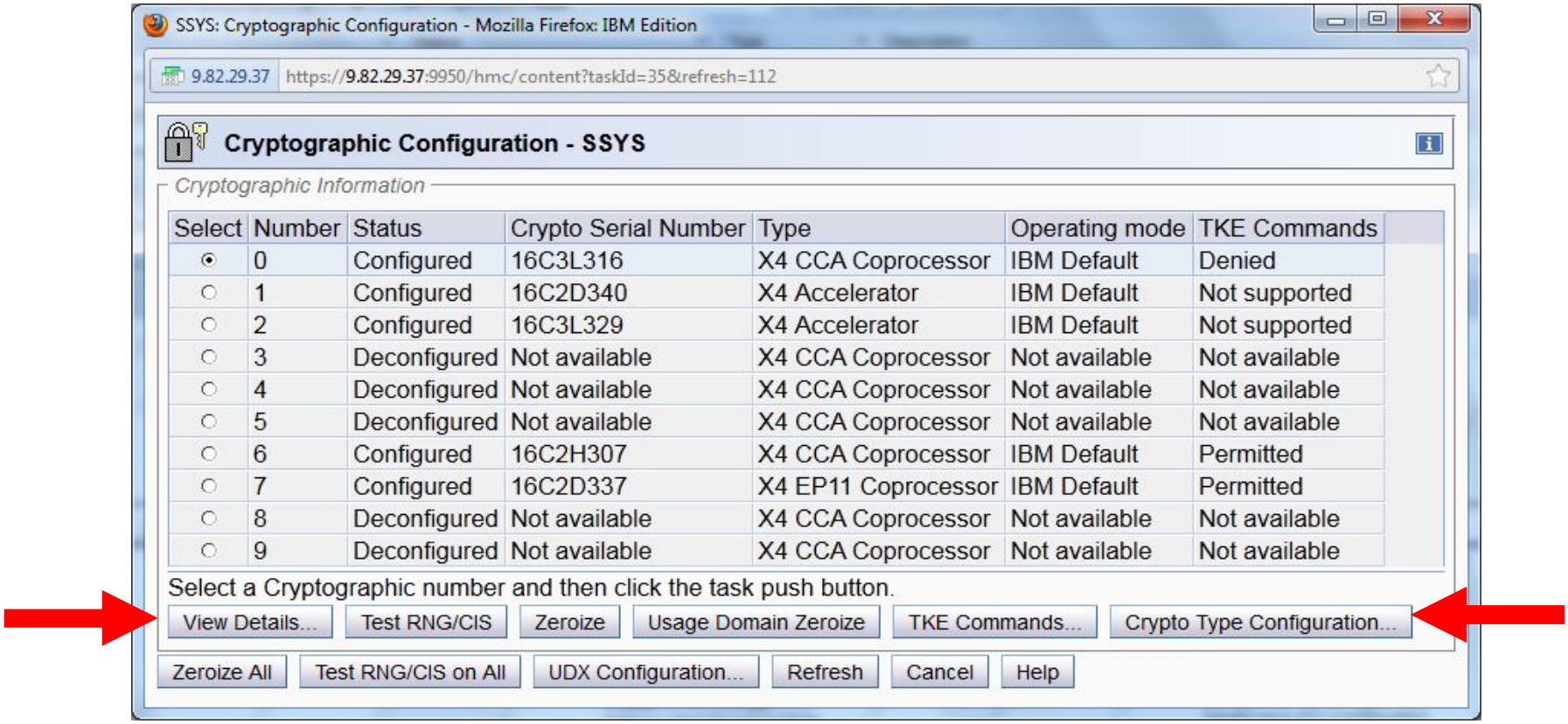
Release...

Cryptographic Card Data

Card Location	Status	Card Serial Number	Type	Number	PCHID
Z22BLG38	Installed	YH1016C4P310	X4 CCA Coprocessor	0	05FC
Z22BLG20	Installed	YH1016C4S326	X4 Accelerator	1	05C0
Z22BLG19	Installed	YH1016C4P313	X4 Accelerator	2	05BC
Z22BLG02	Installed	YH1016C4T324	X4 CCA Coprocessor	3	0584
Z15BLG38	Installed	YH1016C4T322	X4 CCA Coprocessor	4	057C
Z15BLG20	Installed	YH1016C54314	X4 CCA Coprocessor	5	0540
Z15BLG19	Installed	YH1016C4T303	X4 CCA Coprocessor	6	053C
Z15BLG02	Installed	YH1016C4T325	X4 EP11 Coprocessor	7	0504
Z08BLG38	Installed	YH1016C54307	X4 CCA Coprocessor	8	03FC
Z08BLG01	Installed	YH1016C54303	X4 CCA Coprocessor	9	0380

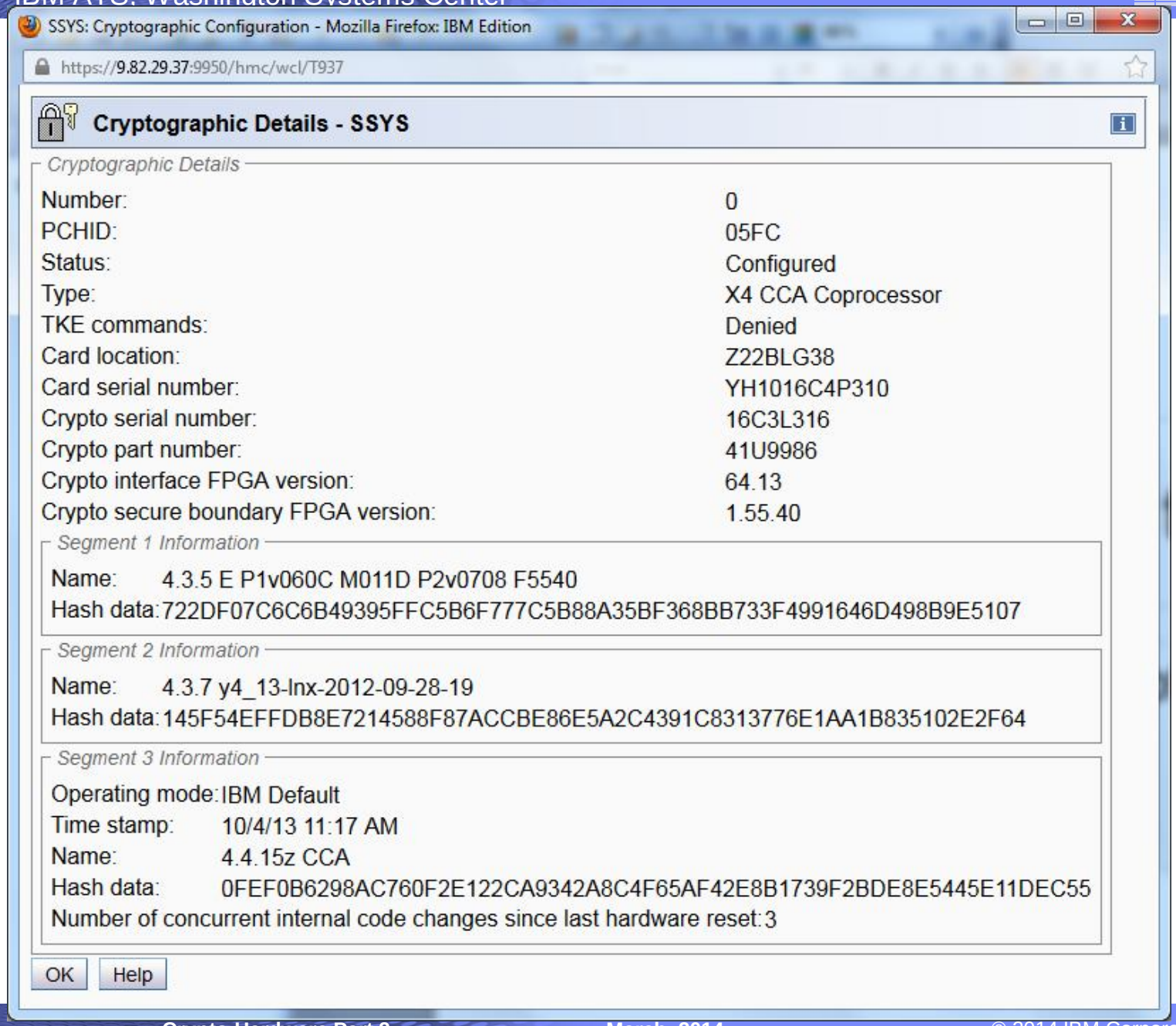
Cancel Help

HMC/SE Screens – Crypto Configuration

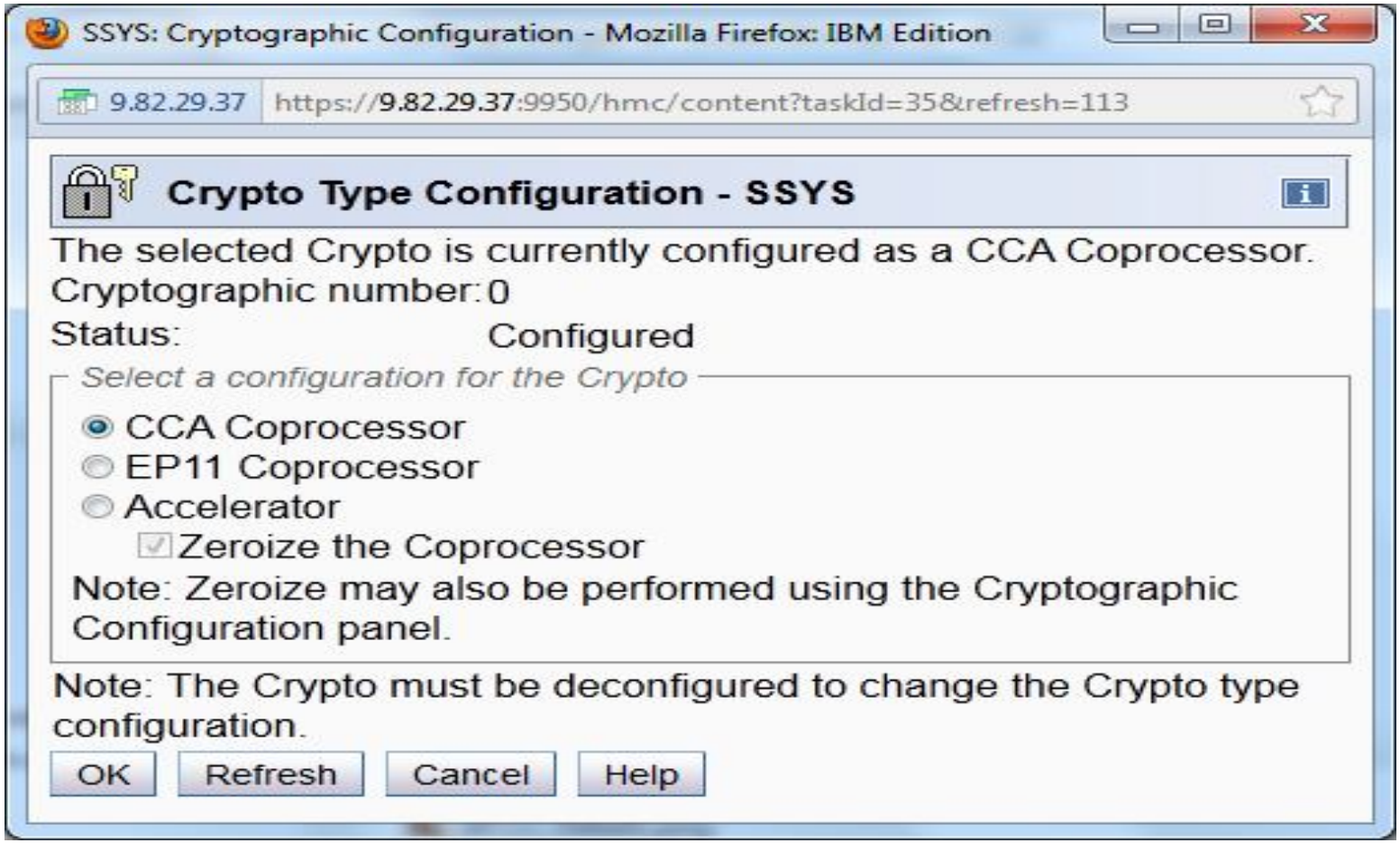


Select	Number	Status	Crypto Serial Number	Type	Operating mode	TKE Commands
◉	0	Configured	16C3L316	X4 CCA Coprocessor	IBM Default	Denied
○	1	Configured	16C2D340	X4 Accelerator	IBM Default	Not supported
○	2	Configured	16C3L329	X4 Accelerator	IBM Default	Not supported
○	3	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available
○	4	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available
○	5	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available
○	6	Configured	16C2H307	X4 CCA Coprocessor	IBM Default	Permitted
○	7	Configured	16C2D337	X4 EP11 Coprocessor	IBM Default	Permitted
○	8	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available
○	9	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available

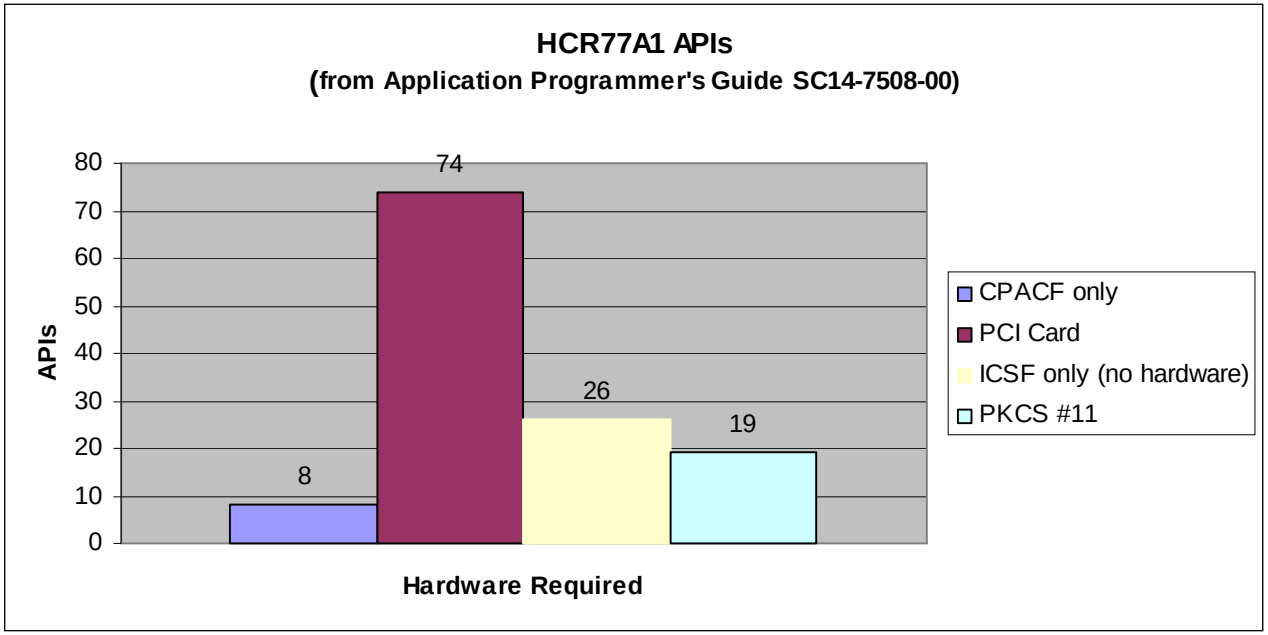
View Details

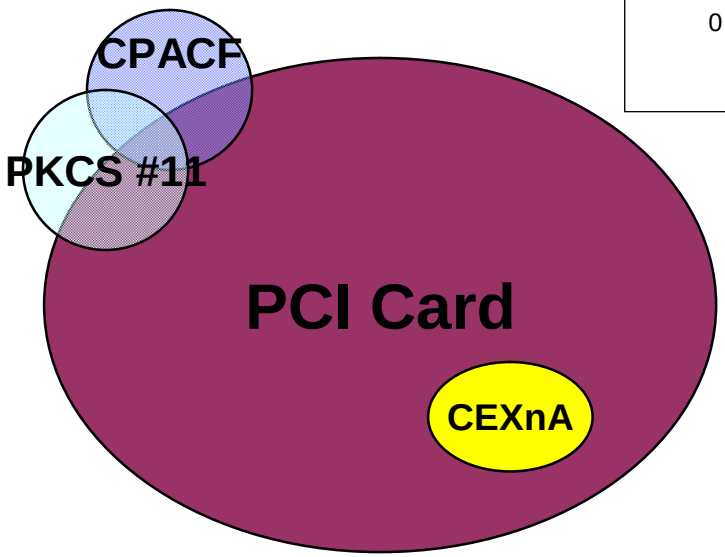


Reconfig – zEC12



APIs and Hardware





IBM Resources (on the web)

- **Redbooks – www.redbooks.ibm.com (search on ‘crypto’)**
  - IBM zEnterprise EC12 Configuration Setup, SG24-8034
  - IBM zEnterprise EC12 Technical Introduction, SG24-8050
  - IBM zEnterprise EC12 Technical Guide, SG24-8049
  - IBM zEnterprise BC12 Technical Guide, SG24-8138
- **ATS TechDocs Website – www.ibm.com/support/techdocs (search on ‘crypto’)**
  - WP100810 – A Synopsis of System z Crypto Hardware
  - WP100647 – A Clear Key / Secure Key /Protected Key Primer

Secure Key Crypto – Information & Download

- **Crypto Card – CryptoExpress3/ CryptoExpress4S**
  - ibm.com/security/cryptocards/pciecc/overview.shtml
  - Programmer's Guide

    ibm.com/security/cryptocards/pciecc/library.shtml
  - CCA Basic Services Reference and Guide for the IBM 4765 PCIe and IBM 4764 PCI-X Cryptographic Coprocessors

    http://www-03.ibm.com/security/cryptocards/pciecc/pdf/bs_latest_edition.pdf
- **Crypto Card – CryptoExpress2**
  - http://www.ibm.com/security/cryptocards/pciecc/overview.shtml
  - Programmer's Guide

    http://www.ibm.com/security/cryptocards/pciecc/pdf/SC33-8294-03.pdf
  - CCA Library Download

    http://www.ibm.com/security/cryptocards/pciecc/ordersoftware.shtml

A Couple of other things

- **FIPS 140-2**
  - Security Requirements for Cryptographic Modules (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)
  - Module Validation List (http://csrc.nist.gov/groups/STM/cmvp/validation.html)
- **AES**
  - FIPS 197 Announcing the AES (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf)
- **DES**
  - FIPS 46-3 Data Encryption Standard - Withdrawn (http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf)
  - SP800-67 Recommendation for the Triple DEA Block Cipher (http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf)

Questions?