MAINFRAME CRYPTO

Unscrambling the Complexity of Crypto!

Crypto Hardware on IBM Z

Part 2

Greg Boyd

gregboyd@mainframecrypto.com

www.mainframecrypto.com

THE Z EXCHANGE

August 2020

Agenda

- Crypto Hardware - Part 1
  - Some basics
  - Some history
  - Some hardware terminology
  - CP Assist for Cryptographic Function (CPACF)
- Crypto Hardware – Part 2
  - Refresher
  - PCI Cards
  - Configuring from the HMC

Crypto Functions

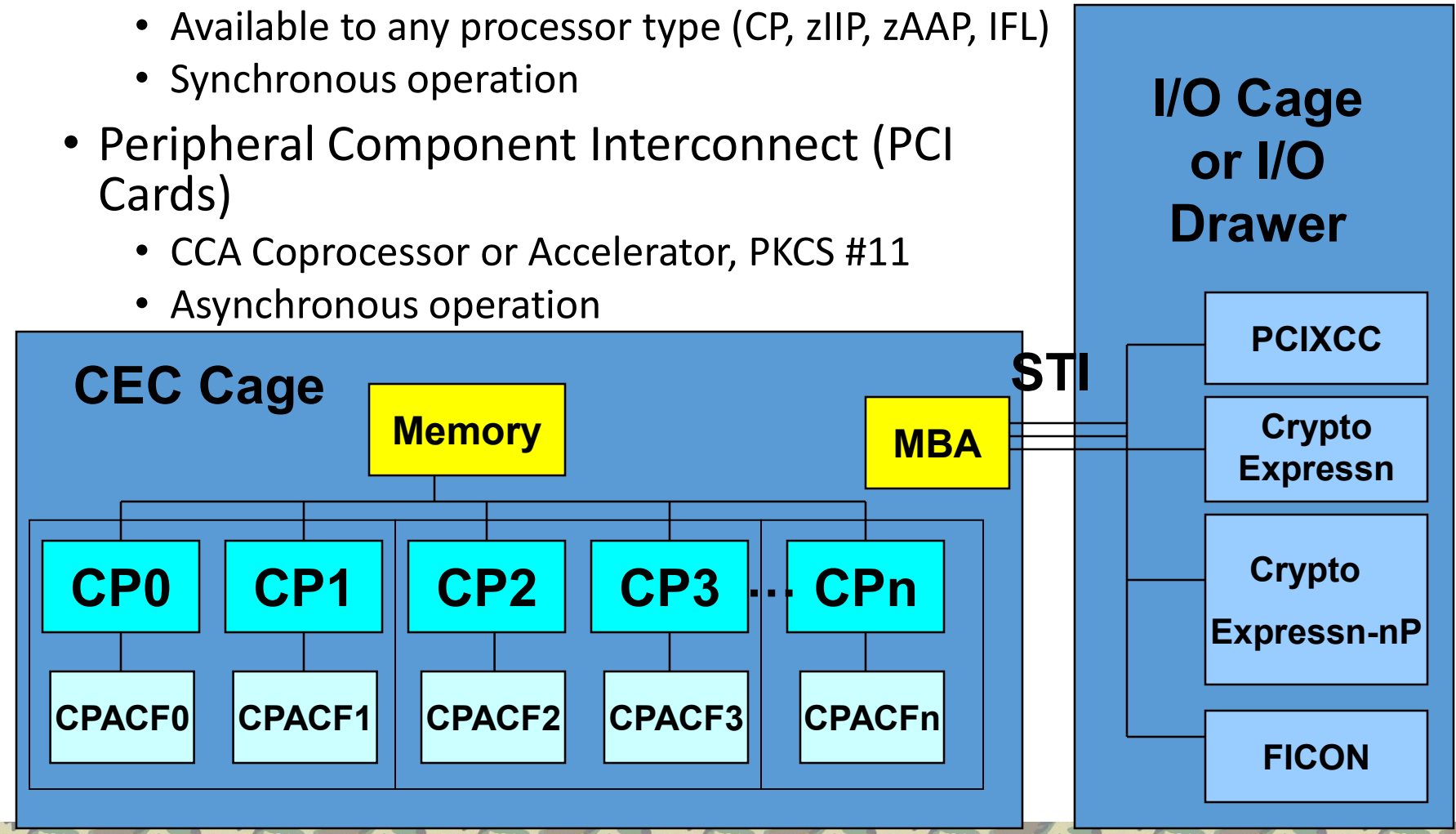
- Data Confidentiality
  - Symmetric – DES/TDES, AES
  - Asymmetric – RSA,Diffie-Hellman, ECC
- Data Integrity
  - Modification Detection
  - Message Authentication
  - Non-repudiation
- Financial Functions
- Key Security & Integrity

Clear Key / Secure Key / Protected Key

- Clear Key
  - Key value is 'in the clear' i.e. not encrypted by another key
    - As a variable in software
    - Stored in a dataset
- Secure Key
  - Clear value only exists inside secure , tamper-resistant boundary of the card
  - Before the key leaves the card, it is encrypted under another key
- Protected Key
  - Clear / secure key hybrid
  - Key is stored (outside of the card) encrypted as a secure key, i.e. encrypted under the master key
  - When key is used, it is first decrypted then re-encrypted using a wrapping key

z890/z990 and later

- CP Assist for Cryptographic Function (CPACF)
  - Available to any processor type (CP, zIIP, zAAP, IFL)
  - Synchronous operation
- Peripheral Component Interconnect (PCI Cards)
  - CCA Coprocessor or Accelerator, PKCS #11
  - Asynchronous operation



4769 Coprocessor

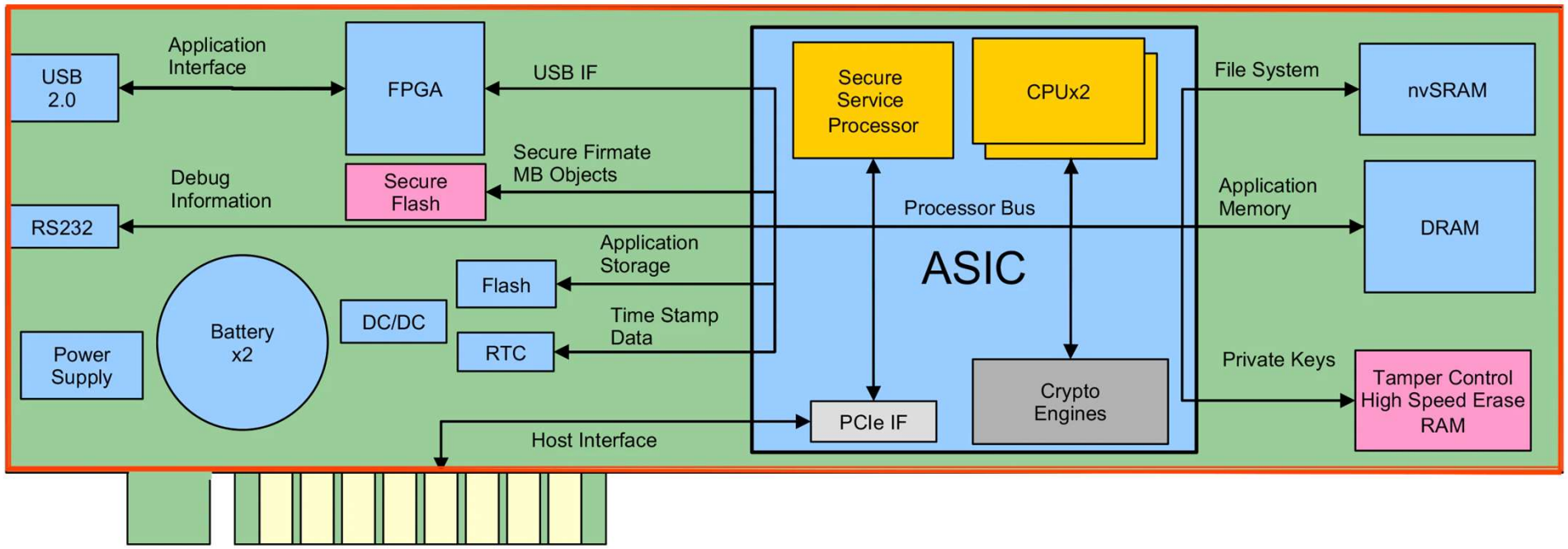
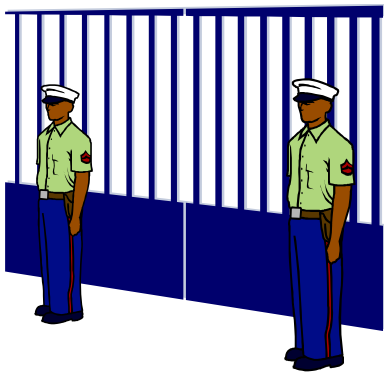


Image from
https://www.ibm.com/security/cryptocards/pciecc4/overview

Hardware Security Module (HSM)

- Tamper Detection
  - Temperature manipulation
  - Probe penetration
  - Power manipulation
  - Side-channel attacks
  - Removal
- Tamper Response
  - Zeroization of all keys
  - Permanently inoperable



PCIXCC (4764)

- Secure Key DES/TDES
- Financial (PIN) Functions
- Key Generate/Key Management
- Random Number Generate and Generate Long
- SSL Handshakes

TechDoc WP100810 – A Synopsis of System z Crypto Hardware

Crypto Express2 (4764)

- Secure Key DES/TDES
- **Secure Key AES**
- Financial (PIN) Functions
- Key Generate/Key Management
- Random Number Generate and Generate Long
- SSL Handshakes

Crypto Express3 (4765)

- Secure Key DES/TDES
- Secure Key AES
- Financial (PIN) Functions
- Key Generate/Key Management
- Random Number Generate and Generate Long
- RSA **& ECC** Operations (SSL Handshakes)
- **Protected Key Support**

Crypto Express4S (4765)

- Secure Key DES/TDES
  - **24-Byte DES MK**
- Secure Key AES
- Financial (PIN) Functions
- Key Generate/Key Management
- Random Number Generate and Generate Long*
- RSA **& ECC** Operations (SSL Handshakes)
- Protected Key Support
- **EP11 Mode (Secure Key PKCS #11)**

Crypto Express5S (4767)

- Secure Key DES/TDES
- Secure Key AES
- Financial (PIN) Functions
- Key Generate/Key Management
- Random Number Generate and Generate Long, **Prime Number Generate**
- RSA & ECC Operations (SSL Handshakes)
- Protected Key Support
- EP11 Mode (Secure Key PKCS #11)
- **Format Preserving Encryption**

Crypto Express6S (4768)

- Secure Key DES/TDES
- Secure Key AES
- Financial (PIN) Functions
- Key Generate/Key Management
- Random Number Generate and Generate Long, Prime Number Generate
- RSA & ECC Operations (SSL Handshakes)
- Protected Key Support
- EP11 Mode (Secure Key PKCS #11)
- Format Preserving Encryption
- **PCI-HSM**

Crypto Express7S (4769)

- Secure Key DES/TDES
- Secure Key AES
- Financial (PIN) Functions
- Key Generate/Key Management
- Random Number Generate and Generate Long, Prime Number Generate
- RSA & ECC Operations (SSL Handshakes)
- Protected Key Support
- EP11 Mode (Secure Key PKCS #11)
  - **PKCS #11 v2.4**
  - **Protected key support**
  - **Support for SHA3, EdDSA and EdDH**
  - **Dilitihium (Quantum Safe)**
- Format Preserving Encryption
- PCI-HSM

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

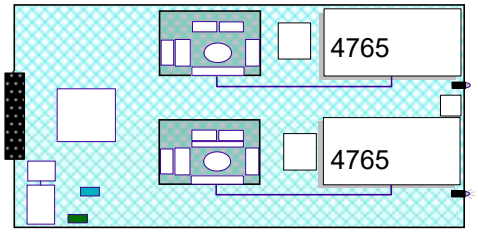
Certifications

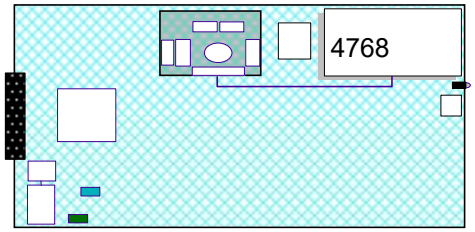
- FIPS 140-2 Level 4
  - https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules
    - Crypto Express5S (4767) – Certificate #3164
    - Crypto Express6S (4768) – Certificate #3410
  - https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/Modules-In-Process-List
    - Crypto Express7S (4769) – In process (Step #3 of 4)
- PCI HSM
  - https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true and search for 'IBM'
    - Hardware #L11 01KV353
    - Hardware #l12 01PP165
    - Firmware CCA 6.0xz
    - Firmware CCA 6.3xz
- Common Criteria EAL 4.0
  - Crypto Express6S (4768) - https://www.ibm.com/downloads/cas/JMD7BBN4

Single Port vs Dual Port

CEX7S-2P

CEX6S (which is only available as -1P)



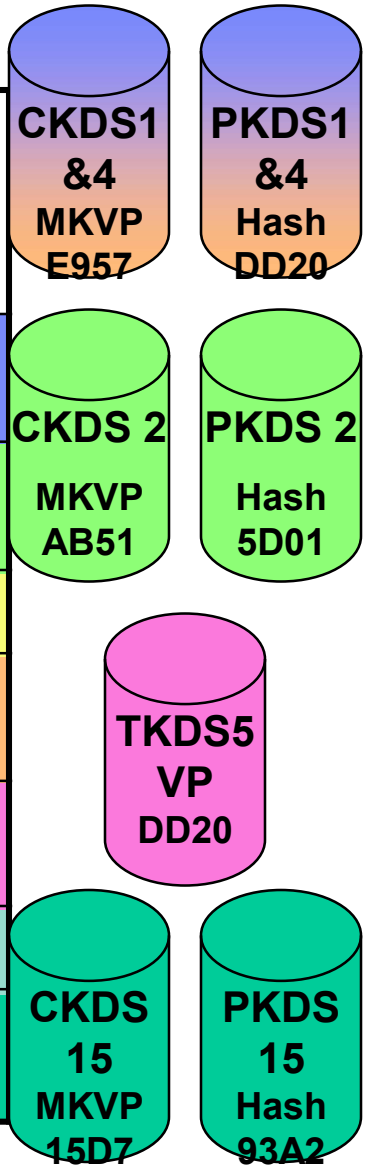


User Defined eXtension

- 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

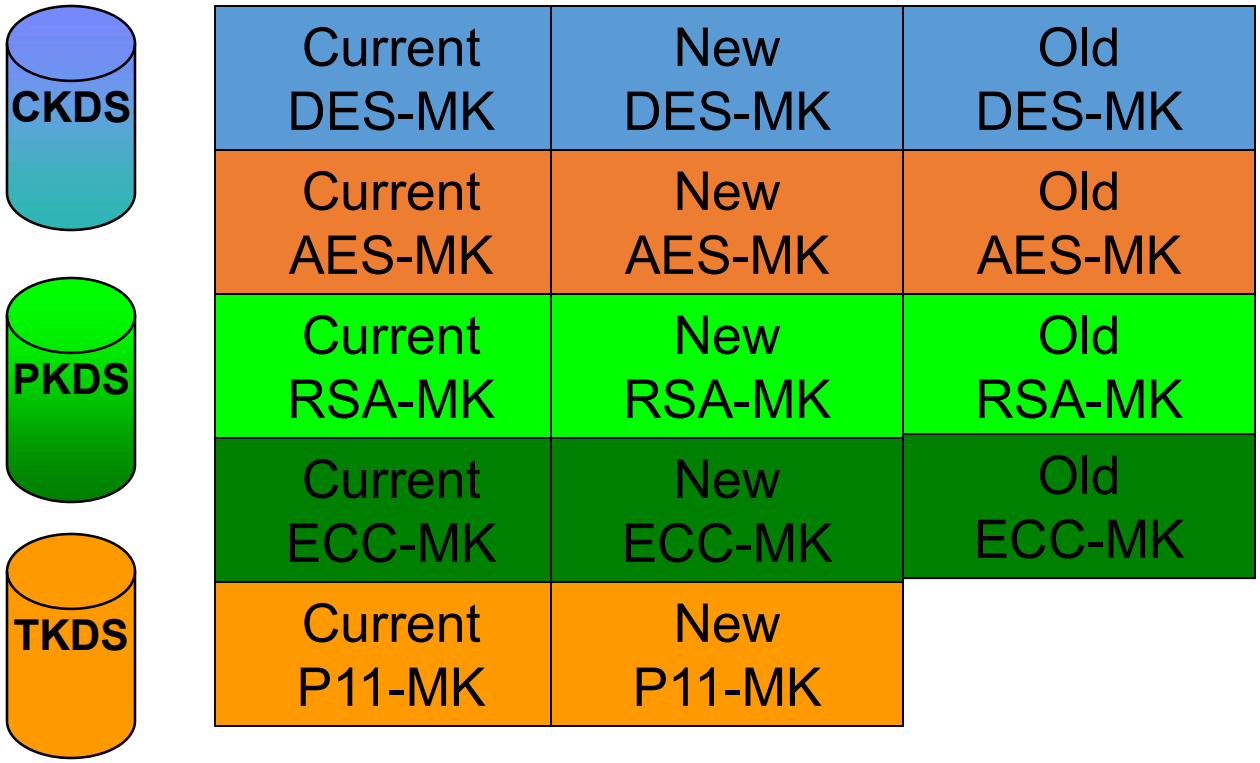
Usage Domains – storage of master keys

LPAR & Domain	DES Master Key	RSA Master Key	AES MK	ECC MK	P11 MK
LP1 UD1	ABC … MKVP=E957	DEF … Hash=DD20	…	…	…
LP2 UD2	F94C8… MKVP=AB51	C841F… Hash=5D01	…	…	…
LP3					
LP4 UD4	ABC … MKVP=E957	DEF … Hash=DD20	…	…	…
LP5					A48C MKVP=DD20
…					
LP15 UD9	AA7B9… MKVP=15D7	42683… MKVP=93A2	…	…	…

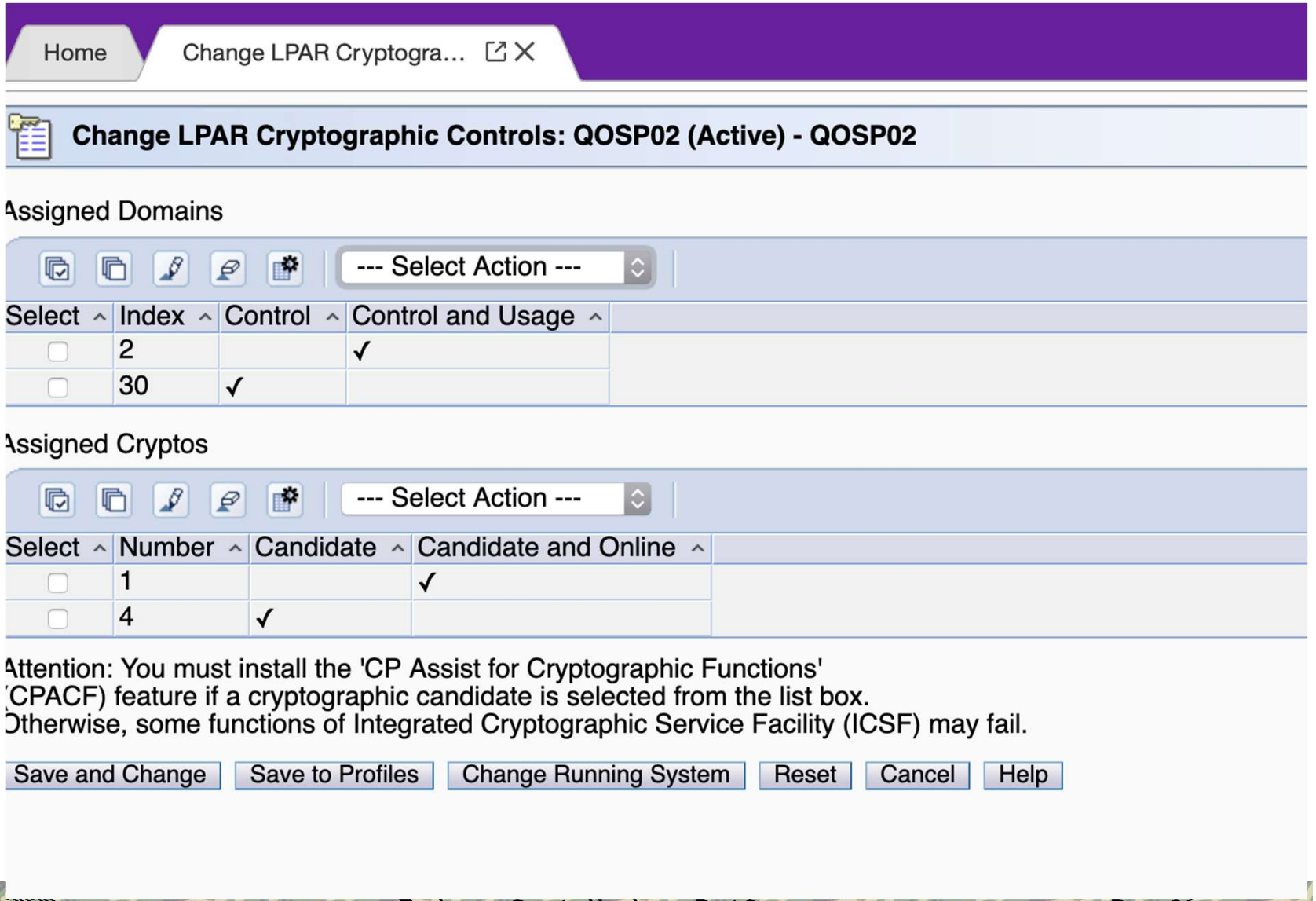


Nonvolatile Arrays for storing Master Keys

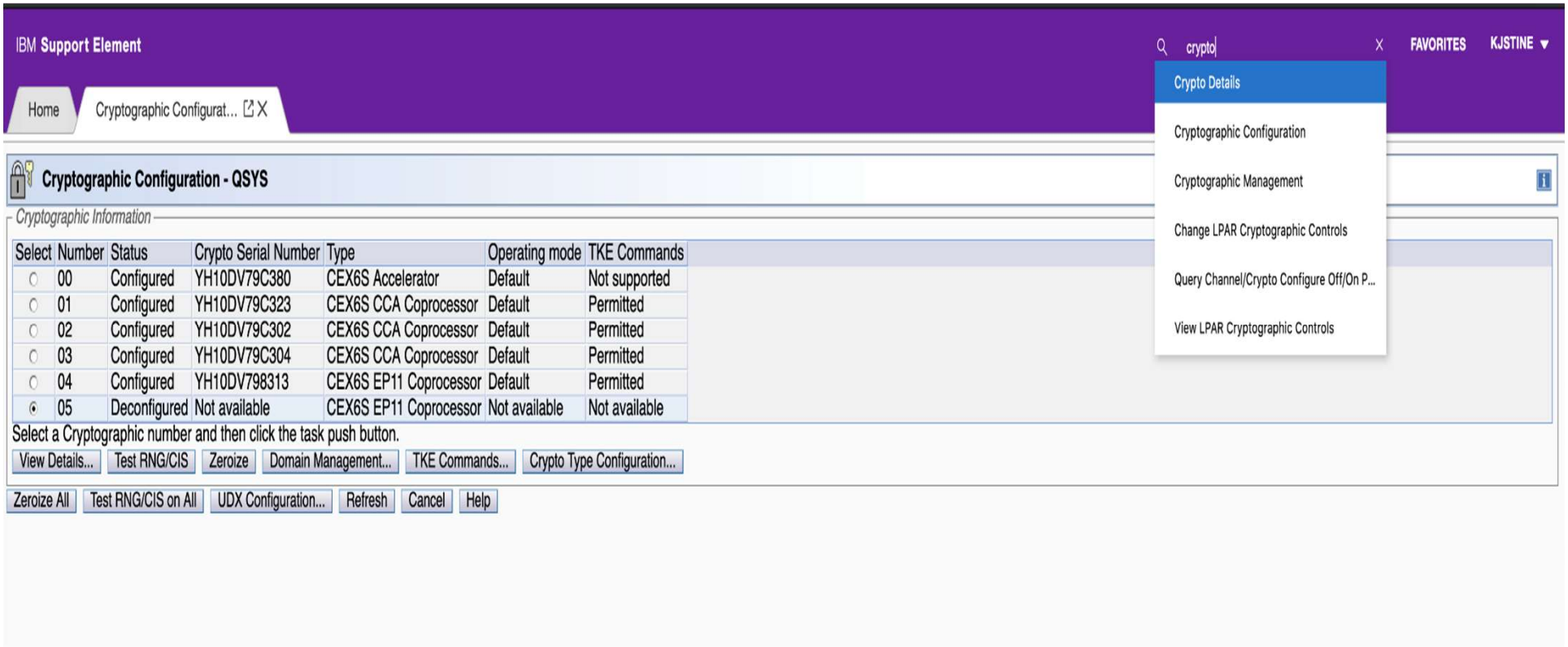
- Current – where the master key resides
- New – staging area for building a new master key
- Old – provides one-back support



Card and Domain Assignments



Crypto Configuration

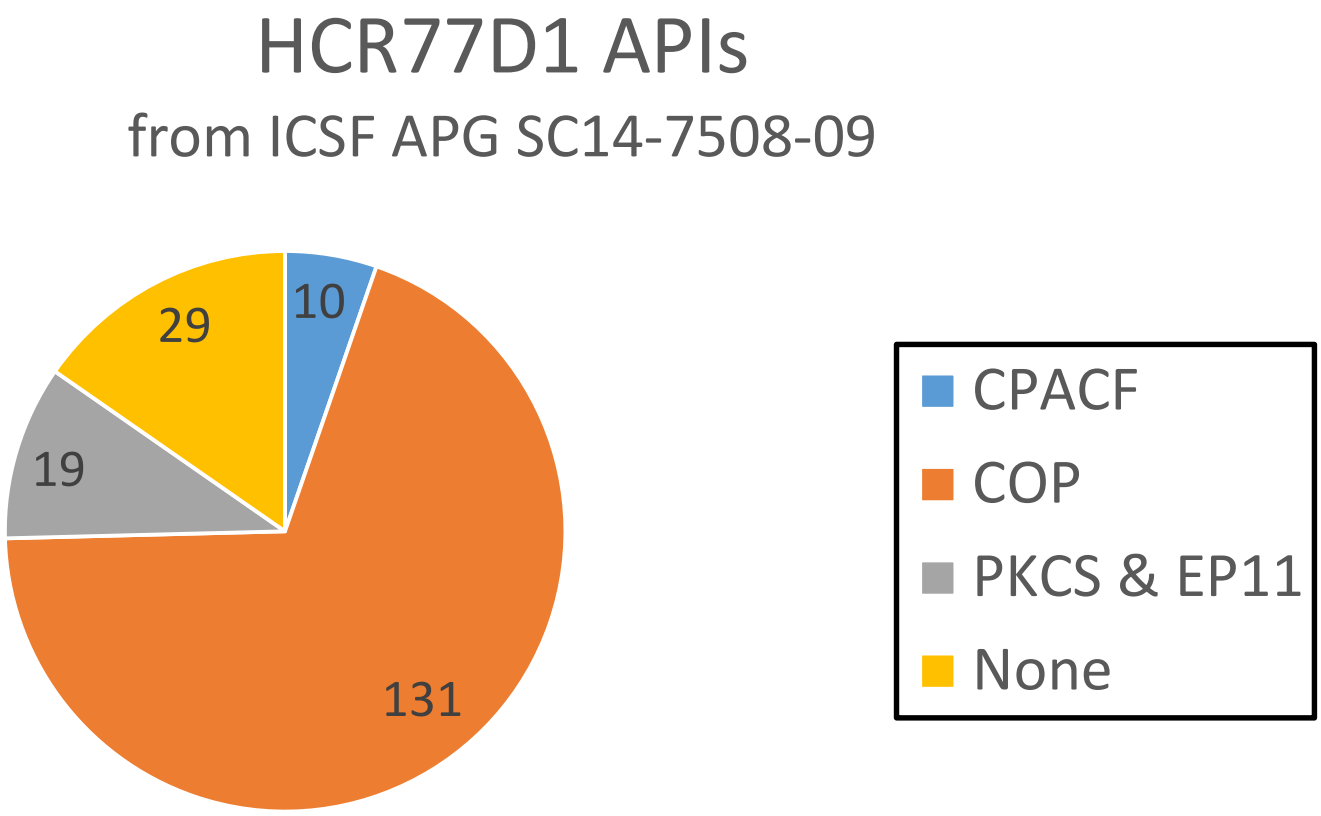


Crypto Engines

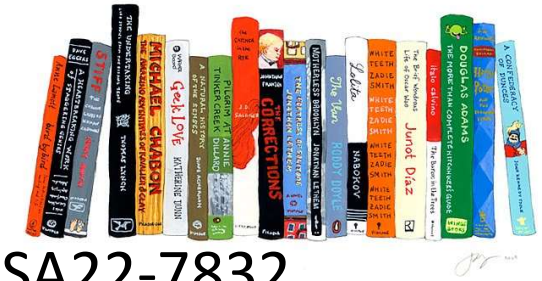
- Legend
  - P – Primary engine
  - O – Optional engine
    - Used if available when algorithm and parameters permit
  - 1 – Coprocessor required to export operational key as protected key

Table 609, Appendix J Cryptographic functions used by ICSF (ICSF APG, SC14-7508-09)				
Algorithm	**CPACF**	**CEXnC**	**CEXnA**	**Software**
DES/3DES/AES – Clear Key	P			
DES/3DES/AES – Secure Key		P		
DES/3DES/AES – Protected Key	P	1		
HMAC – Secure key		P		
SHA-1/SHA-2/SHA-3	P			
MD5/RIPEMD-160				P
ECC – Clear and secure private key		P		
RSA – Clear private key		P	O	
RSA – Secure private key		P		
RSA – Public key		P	O	
ECC – Public key		P		
DH		P		

APIs and Hardware



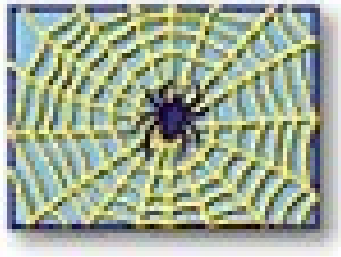
IBM Manuals



- z/Architecture Principles of Operations, SA22-7832
- ICSF Application Programmer's Guide, SC14-7508
- ICSF System Programmer's Guide SC14-7507
- ICSF Administrator's Guide SC14-7506

- https://www.ibm.com/security/cryptocards
- https://www.ibm.com/security/cryptocards/pciecc4/overview

IBM Resources (on the web)



- Redbooks – www.redbooks.ibm.com (search on 'crypto')
  - SG24-8860 IBM z15 (8561) Configuration Setup (September 22 Draft)
  - SG24-8851 IBM z15 (8561) Technical Guide
  - SG24-8850 IBM z15 Technical Introduction
- ATS TechDocs Website – www.ibm.com/support/techdocs (search on the document id)
  - WP100810 – A Synopsis of System z Crypto Hardware
  - WP100647 – A Clear Key / Secure Key /Protected Key Primer

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