MAINFRAME CRYPTO

Unscrambling the Complexity of Crypto!

Crypto Hardware on IBM Z
Part 1

Greg Boyd

gregboyd@mainframecrypto.com

www.mainframecrypto.com

THE Z EXCHANGE

May 2020

NewEra Software eBook on Crypto

- http://survey.constantcontact.com/survey/a07eh2z6ogwk9yktggw/start

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

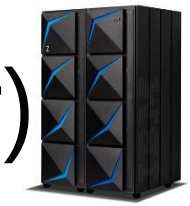
System z CCF Hardware – G5,G6, z800/z900

- DES (56-, 112-, 168-bit)
- SHA-1

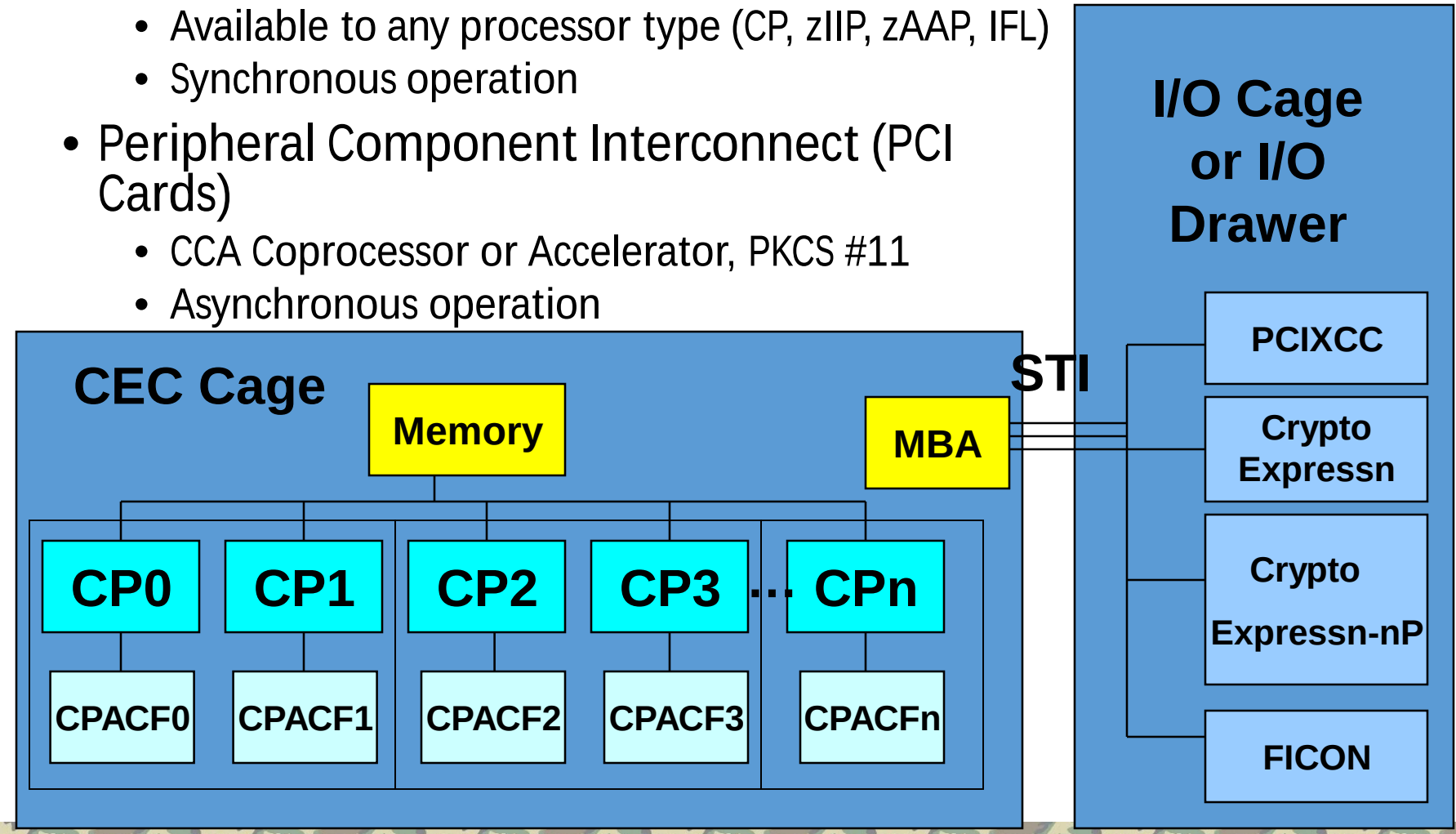
- Secure Key Only

TechDoc WP100810 – A Synopsis of System z Crypto Hardware

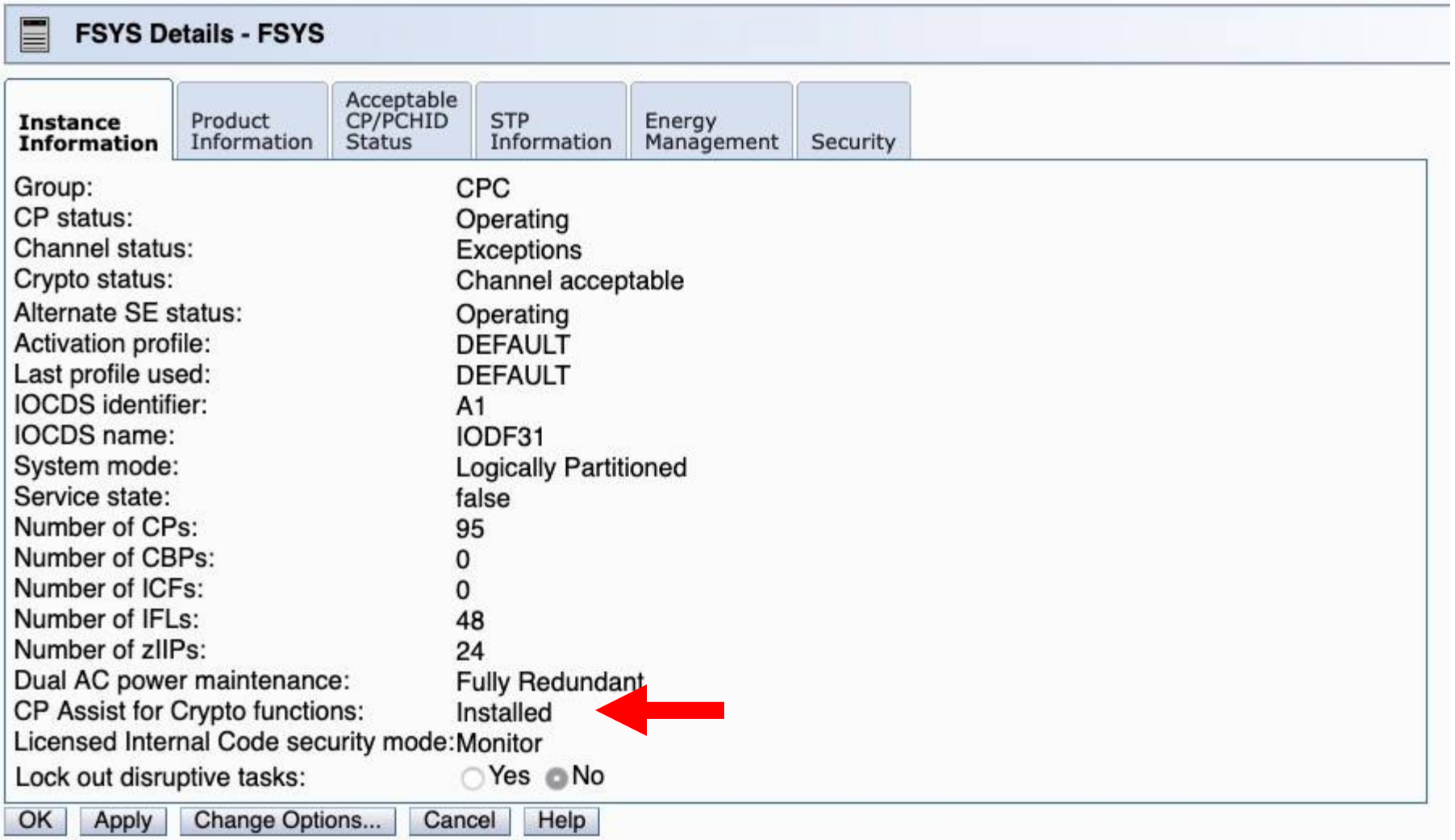
CPACF Machines (z890/z990 & later)



- 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



HMC/SE – CPACF Enablement (FC #3863)



MSA – Message Security Assist

z990

- MSA (z990/z890)
  - Cipher Message instruction (KM)
  - Cipher Message with Chaining instruction (KMC)
    - DES (56-, 112- and 168-bit keys)
  - Compute Intermediate Message Digest instruction (KIMD)
  - Compute Last Message Digest instruction (KLMD)
    - SHA-1
  - Compute Message Authentication Code instruction (KMAC)

z890

MSA – Message Security Assist

- MSA Extension 1 (z9)
  - KM/KMC - added AES-128 and PRNG
  - KIMD/KLMD - added SHA-256
- MSA Extension 2 (z10)
  - KM/KMC - added AES-192, AES-256
  - KIMD/KLMD - added SHA-512
- MSA Extension 3 (z10 EC GA3 & z10 BC GA2)
  - Added Protected Key support

z9

z10

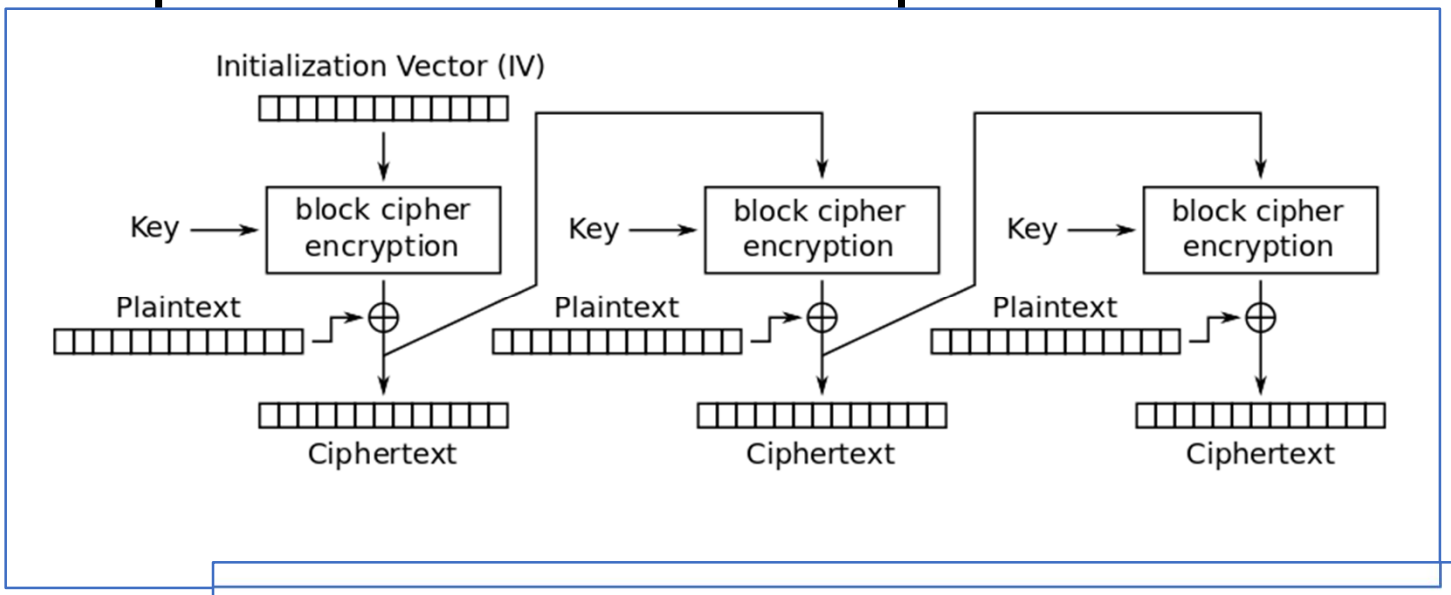
MSA – Message Security Assist

zEC12

- MSA Extension 4 (z196/z114, zEC12/zBC12)
  - Cipher Message With Cipher Feedback (CFB) instruction (KMF)
  - Cipher Message With Counter instruction (KMCTR)
  - Cipher Message With Output Feedback (OFB) instruction (KMO)
  - Perform Cryptographic Computation instruction (PCC)
  - Enhanced Instructions
    - KMAC Compute Message Authentication Code
      - Added AES support
      - Added Protected key Support
      - Added GHASH support
    - KM/KMC Cipher Message/Cipher Message with Chaining
      - Added AES Ciphertext Stealing (XTS) support
    - KIMD Compute Intermediate Digest
      - Added GHASH support

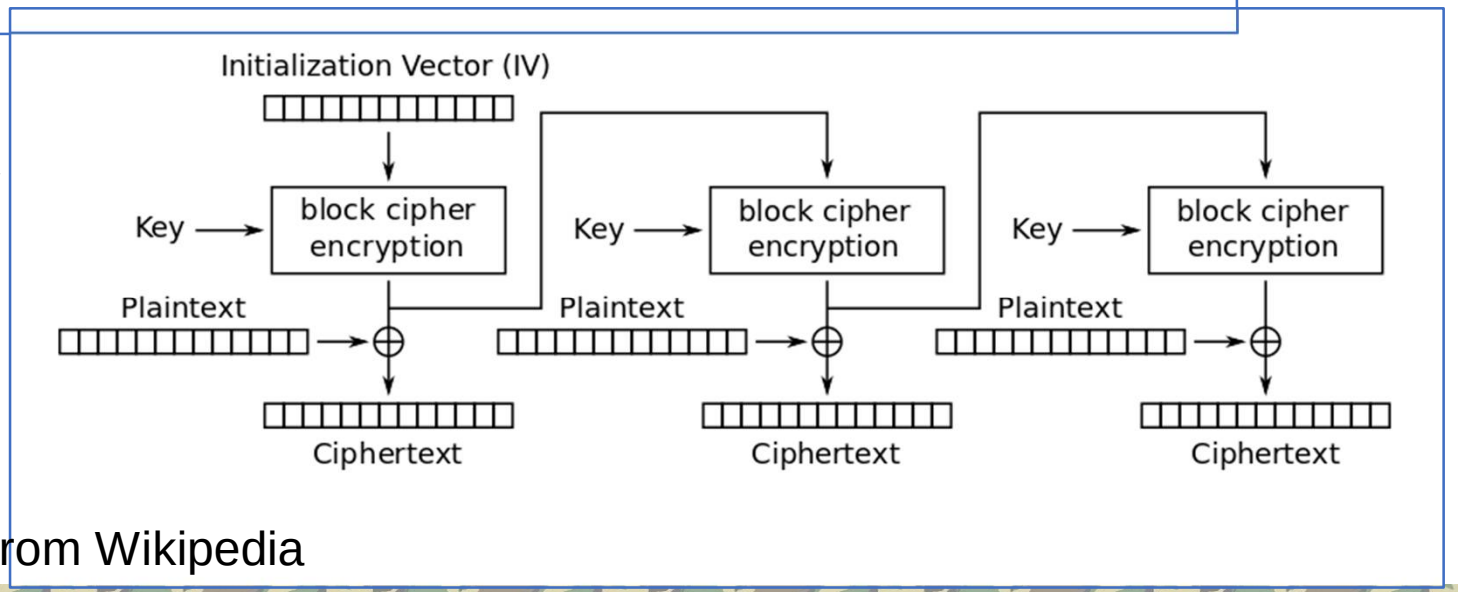
z196

Cipher Feedback vs Output Feedback Mode



Cipher Feedback Mode

Output Feedback Mode



Images from Wikipedia

MSA – Message Security Assist

- MSA Extension 5 (z13)
  - Perform Pseudo Random Number Operation instruction (PPNO)
- MSA Extension 5 (z14)
  - Perform Random Number Operation instruction (PRNO)
- MSA Extension 6 (z14)
  - Enhanced KIMD/KLMD
    - Added SHA-3 Hash Facility & SHA-3 Extendable-Output Facility
- MSA Extension 7 (z14)
  - Enhanced PRNO (Perform Random Number Operation instruction)
    - Added True Random Number Generator (TRNG)
- Message Extension 8 (z14)
  - Cipher Message with Authentication (KMA) for Galois-counter-mode (GCM)

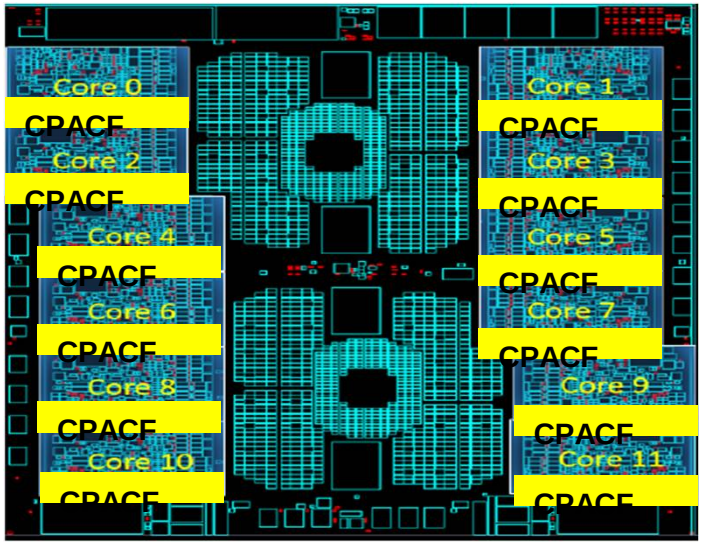
z14

z13

MSA – Message Security Assist

- Message Extension 9 (z15)
  - Compute Digital Signature Authentication (KDSA)
  - Enhanced instructions
    - PCC (Perform Cryptographic Computation) - added Elliptic Curve Scalar Multiply function
  - Enhance PCKMO to wrap Elliptic Curve keys

z15



CPU Measurement Facility

Cntr #	Counter	Cntr #	Counter	Cntr #	Counter
64	PRNG function count	72	DEA function count	80	ECC function count
65	PRNG cycle count	73	DEA cycle count	81	ECC cycle count
66	PRNG blocked function count	74	DEA blocked function count	82	ECC blocked function count
67	PRNG blocked cycle count	75	DEA blocked cycle count	83	ECC blocked cycle count
68	SHA function count	76	AES function count		
69	SHA cycle count	77	AES cycle count		
70	SHA blocked function count	78	AES blocked function count		
71	SHA blocked cycle count	79	AES blocked cycle count		

- Provides hardware instrumentation data for production systems
- CPU MF Counters also useful for performance analysis
- Data gathering controlled through z/OS HIS (HW Instrumentation Services)
- Supplements current performance data from SMF, RMF, DB2, CICS, etc.
- Measure (count) CPACF Usage
- Recorded in SMF Type 113

Cipher Message Instructions

- Cipher Message instructions
  - KM R1,R2
  - KMC R1,R2
- R1 pointer to output location
- R2 pointer to source location
- R2+1 length of source
- Reg 0 contains Function Code
- Reg 1 pointer to parameter block

Register 0 Function Codes

Bit 56 – Encrypt / Decrypt flag for cipher operations

Code	Function	Parm Block Size (Bytes)	Data Block Size (Bytes)
0	KM(C)-Query	16	-
1	KM(C)-DEA	8 (16)	8
2	KM(C)-TDEA-128	16 (24)	8
3	KM(C)-TDEA-192	24 (32)	8
9	KM(C)-Encrypted-DEA	32 (40)	8
10	KM(C)-Encrypted-TDEA-128	40 (48)	8
11	KM(C)-Encrypted-TDEA-192	48 (56)	8
18	KM(C)-AES-128	16 (32)	16
19	KM(C)-AES-192	24 (40)	16
20	KM(C)-AES-256	32 (48)	16

Code	Function	Parm Block Size (Bytes)	Data Block Size (Bytes)
26	KM(C)-Encrypted-AES-128	48 (64)	16
27	KM(C)-Encrypted-AES-192	56 (72)	16
28	KM(C)-Encrypted-AES-256	64 (80)	16
50	KM-XTS-AES-128	32	16
52	KM-XTS-AES-256	48	16
58	KM-XTS-Encrypted-AES-128	64	16
60	KM-XTS-Encrypted-AES-256	80	16
67	KMC-PRNG	32	8

Register 1 Parameter Block (KM/KMC)

KM/KMC (Query) Instruction
16-Byte Status Word

KMC (PRNG) Instruction
8-byte Chaining Value
8-Byte Key Part 1
8-Byte Key Part 2
8-Byte Key Part 3

KM Instruction
Cryptographic Key 8-, 16- or 24-bytes for DES/TDES 128-, 192- or 256-bits for AES
Wrapping Key Verification Pattern 24-bytes for DES/TDES 256-bits for AES
XTS Parameter 128-bits

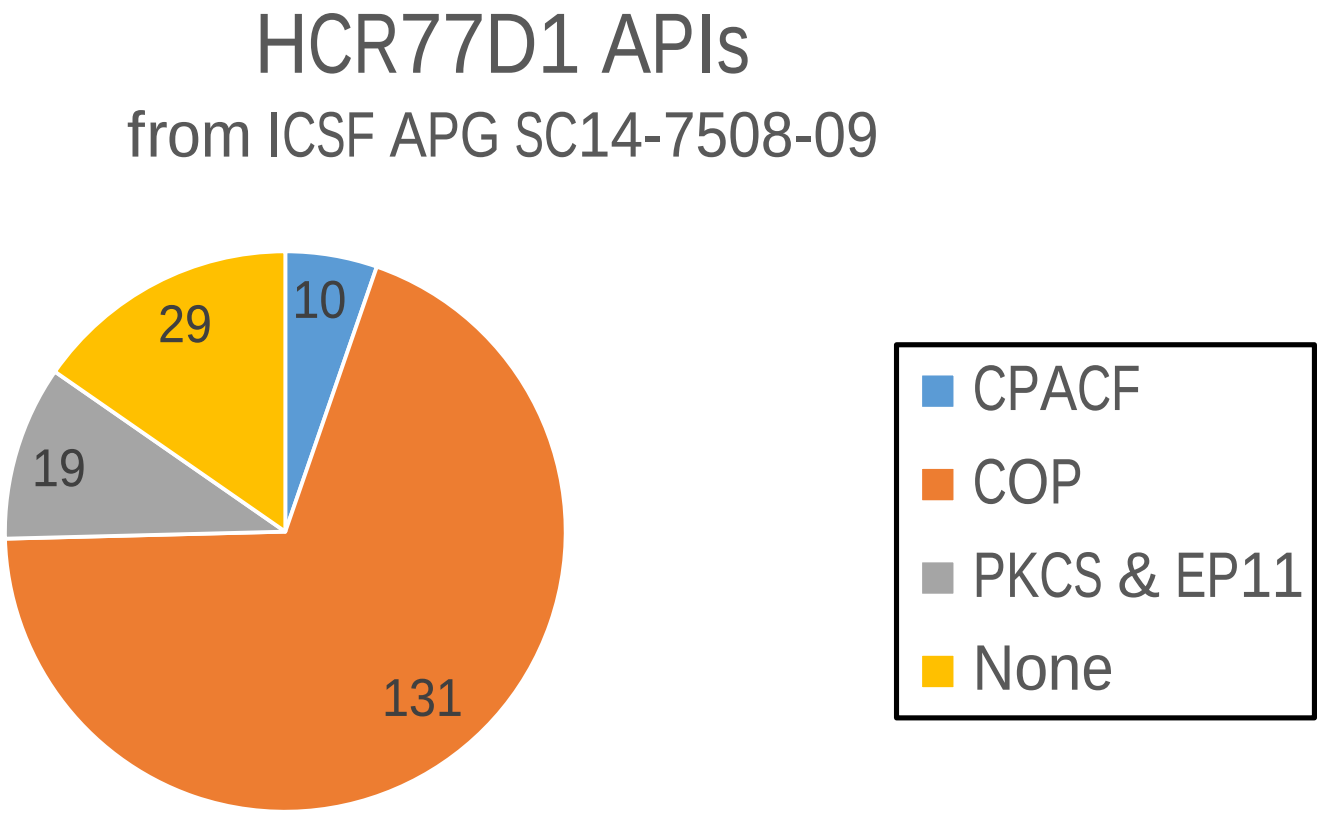
KMC Instruction
Chaining Value 8-bytes for DES/TDES 16-bytes for AES
Cryptographic Key 8-, 16- or 24-bytes for DES/TDES 128-, 192- or 256-bits for AES
Wrapping Key Verification Pattern 24-bytes for DES/TDES 256-bits for AES

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		

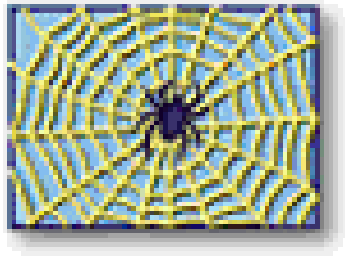
APIs and Hardware



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
- The Load-Program-Parameter and the CPU-Measurement Facilities SA23-2260

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
  - TC000066 – CPU MF - 2019 Update and WSC Experiences

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

Questions

- http://survey.constantcontact.com/survey/a07eh2z6ogwk9yktggw/start