MAINFRAME CRYPTO

Crypto Performance: Expectations, Operations & Reporting

Greg Boyd

gregboyd@mainframecrypto.com

www.mainframecrypto.com

September 2015

Copyrights and Trademarks

- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 10 years

Agenda

- Crypto Levelset
  - Crypto Functionality
  - Clear Key vs Secure Key vs Protected Key
  - Crypto Hardware Technology
- Hardware performance metrics
- Operational factors
- Crypto performance data and reports

Crypto Functions

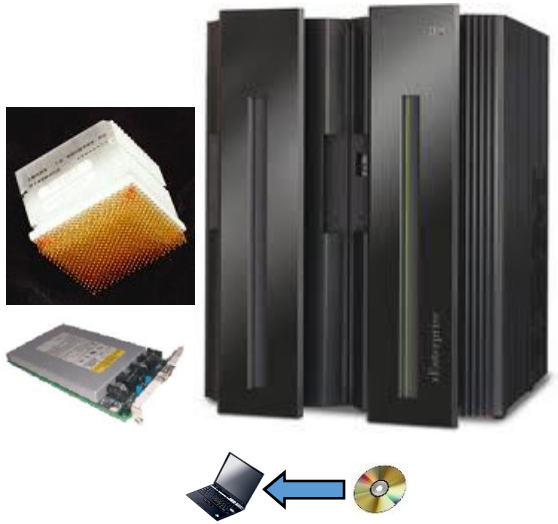
- Data Confidentiality
  - Symmetric – DES/TDES, AES
  - Asymmetric – RSA, Diffie-Hellman, ECC
- Data Integrity
  - Modification Detection
  - Message Authentication
  - Non-repudiation
- Financial Functions
- Key Security & Integrity

Clear Key / Secure Key / Protected Key

- Clear Key – key 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

System z **Clear Key** Crypto Hardware – z13, zEC12/zBC12, z196/z114, z10 EC & BC, z9 EC & BC, z990/z890

- CP Assist for Crypto Function (CPACF)
  - DES/TDES (56-, 112-, 168-bit)
  - AES-128, AES-192, AES-256
  - SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512)



TechDoc WP100810 – A Synopsis of System z Crypto Hardware

System z **Secure Key** Crypto Hardware – CEX5S, CEX4S, CEX3/CEX3-1P

- Secure Key DES/TDES
- Secure Key AES
- Financial (PIN) Functions
- Random Number Generate and Generate Long
- Key Generate/Key Management
- SSL Handshakes, ECDSA support
- Protected Key Support
- PKCS #11 (CEX4S only)

TechDoc WP100810 – A Synopsis of System z Crypto Hardware

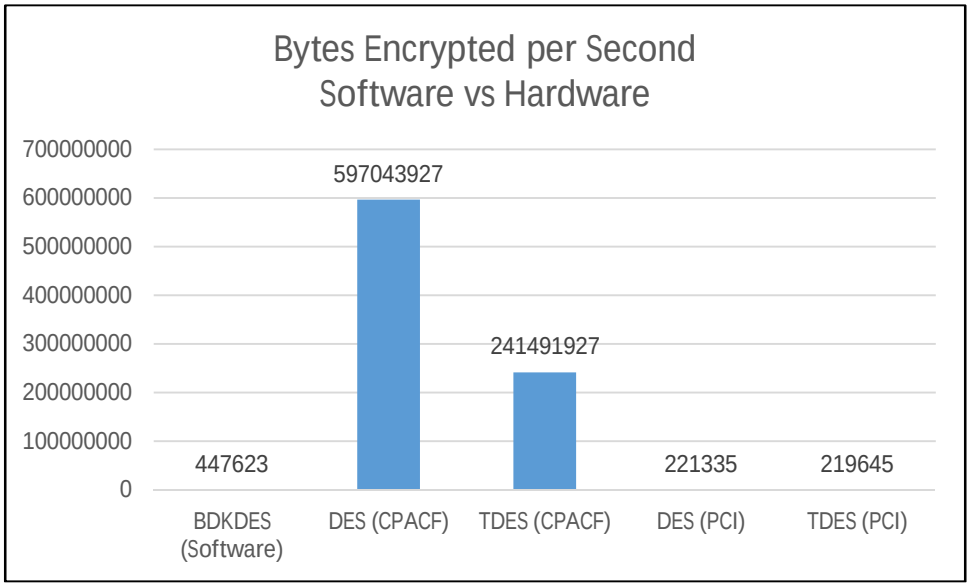
Crypto Card Modes

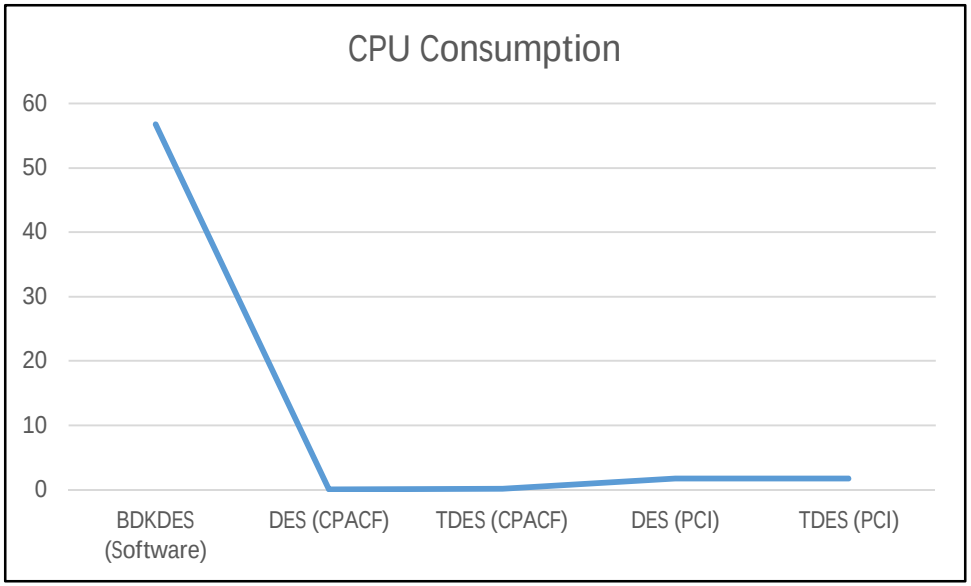
- Coprocessor
  - Secure key support
  - Financial PIN operations
  - Key generation
  - RSA public & private key operations
- Accelerator
  - RSA public key operations only
- EP11 (Enterprise PKCS #11)
  - PKCS #11 clear and secure key operations

Software vs Hardware Encryption

- Adapted from Ernie Nachtigall's TechDoc, WP101240 'IBM z10 DES Cryptographic Performance' available at http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101240

	Bytes/Sec	CPU Time
BDKDES (Software)	447623	56.82
Clear Key DES	597043927	0.04
Clear Key TDES	241491927	0.09
Secure Key DES	221335	1.66
Secure Key TDES	219645	1.67

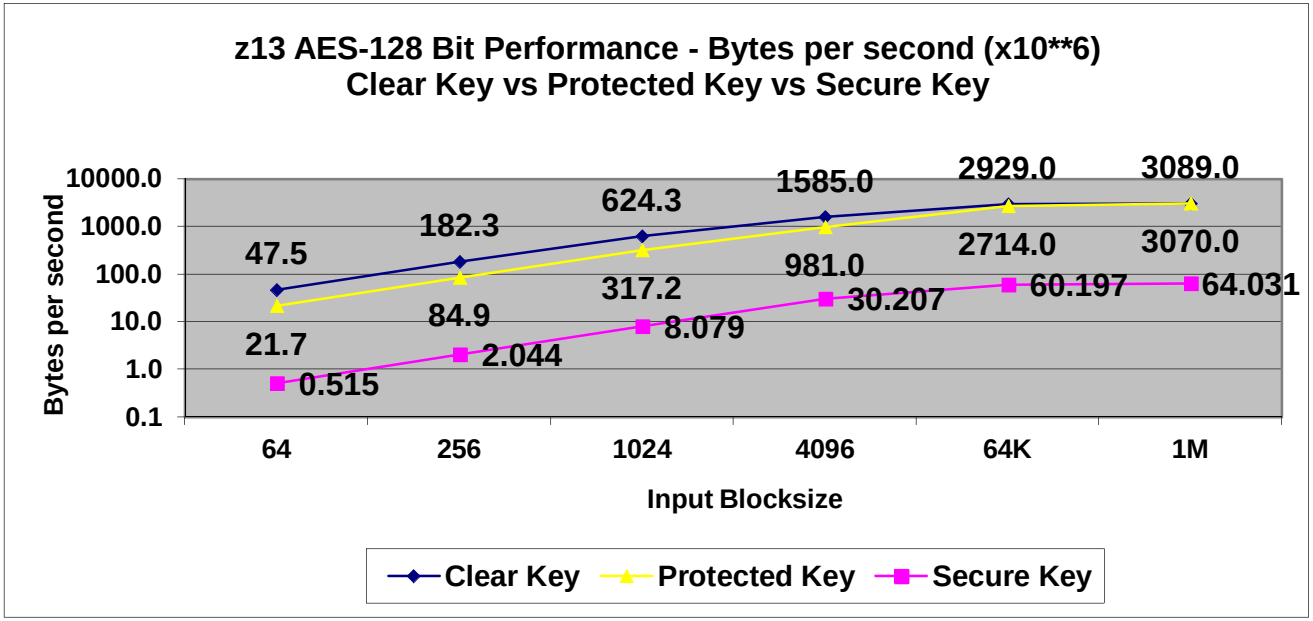


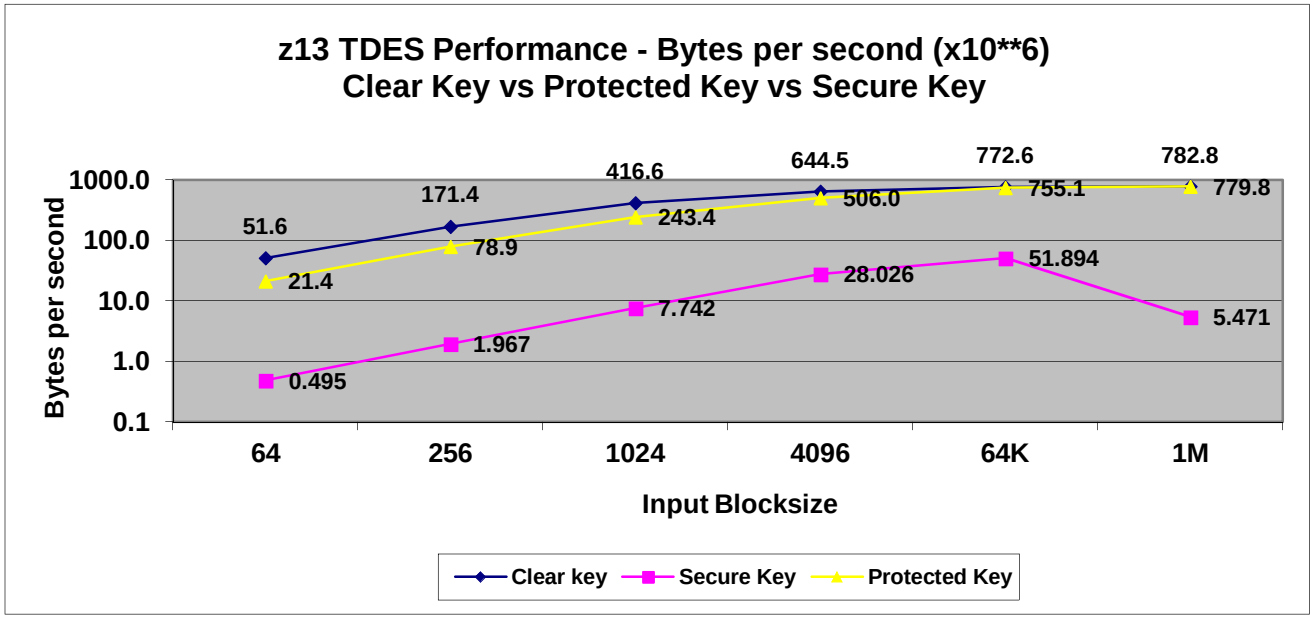


z13 Symmetric Key Performance

- Adapted from the IBM z13 Cryptographic Performance March 2015 document at

http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=ZSW03283USEN&attachment=ZSW03283USEN.PDF

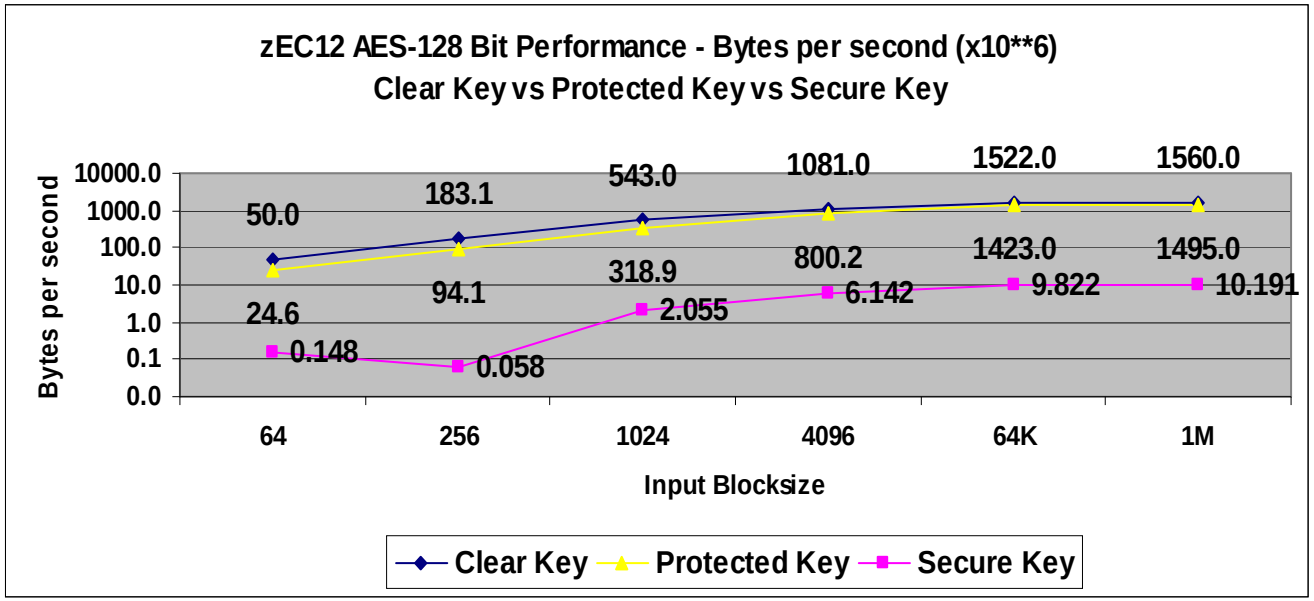


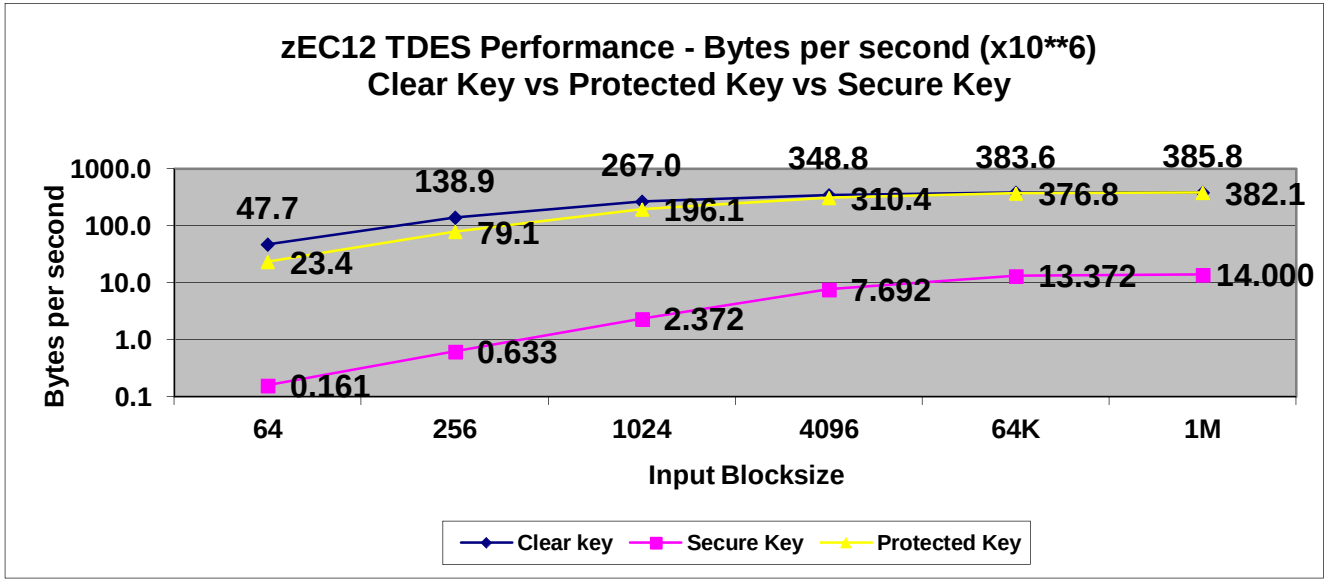


zEC12 Symmetric Key Performance

- Adapted from the IBM zEnterprise EC12 Performance of Cryptographic Operations document at

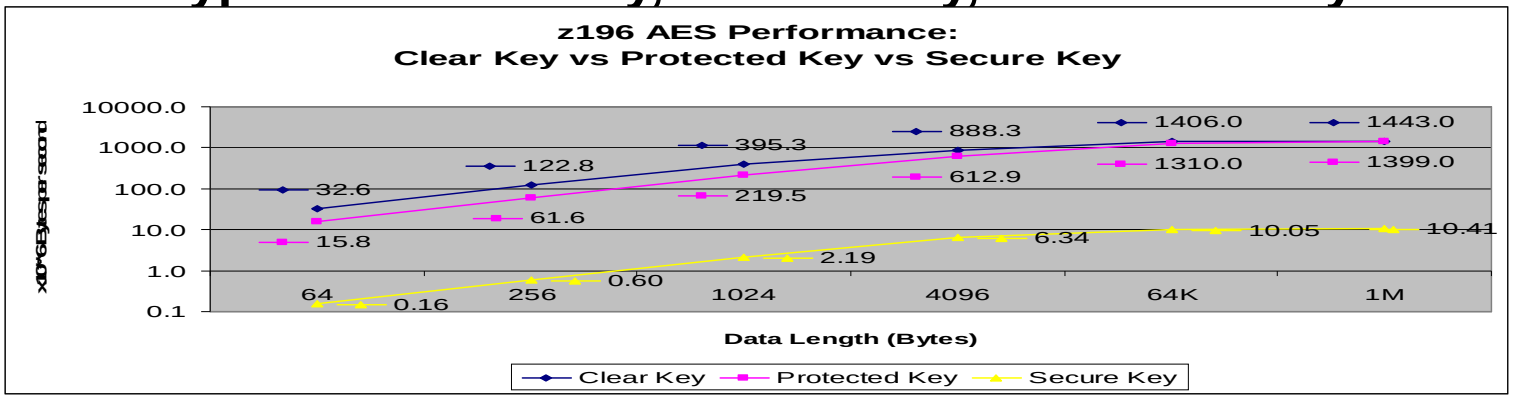
http://www.ibm.com/systems/z/advantages/security/zec12cryptography.html



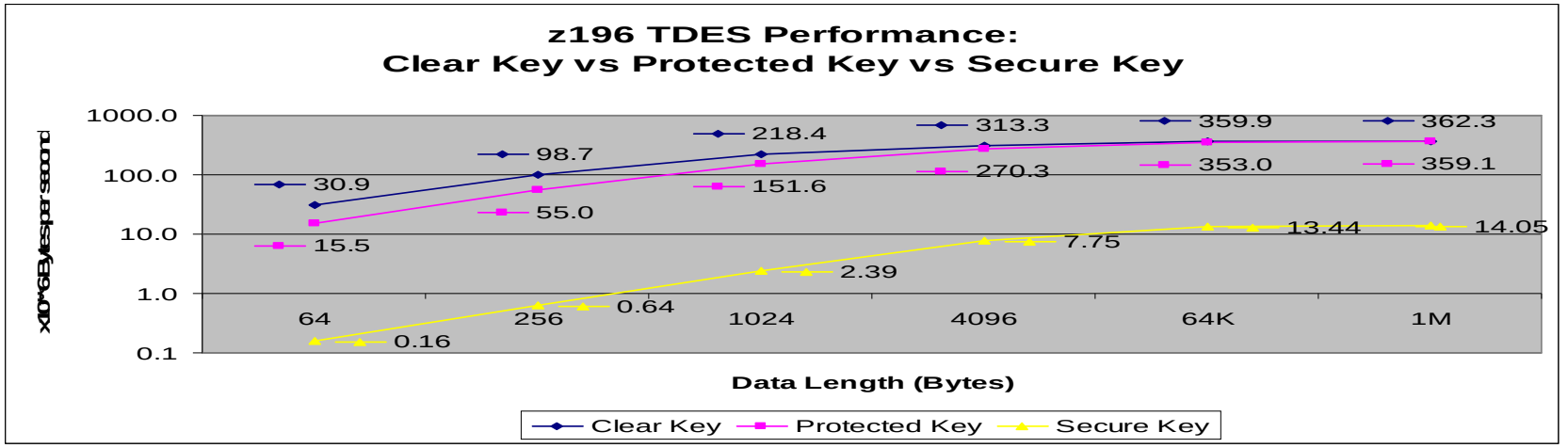


z196 Crypto Performance

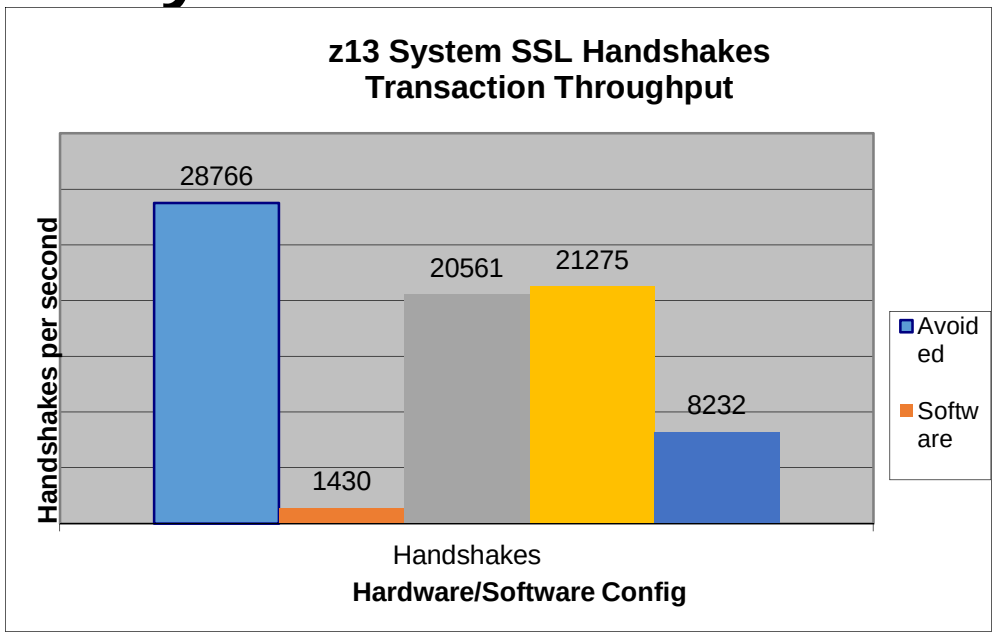
- **AES Encryption – Clear Key, Secure Key, Protected Key**



- **TDES Encryption – Clear Key, Secure Key, Protected Key**



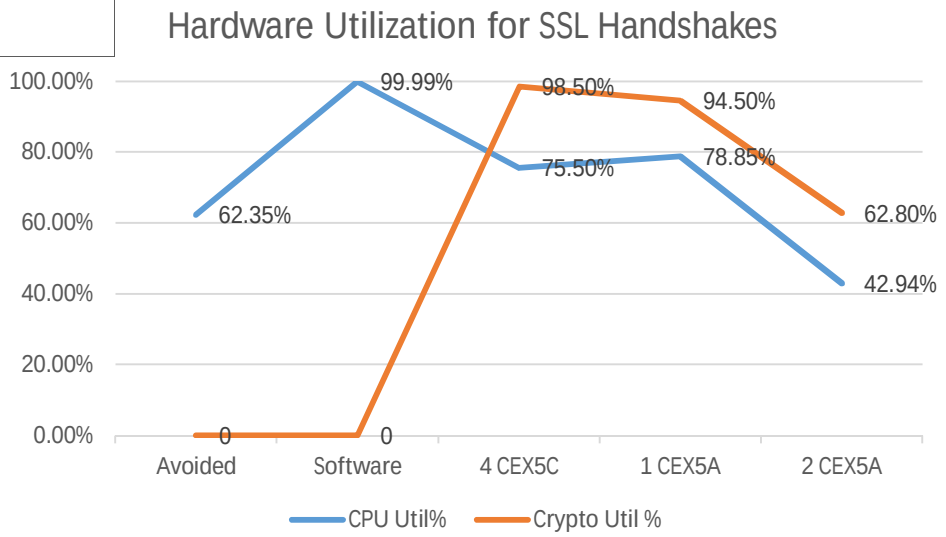
System SSL Performance – z13



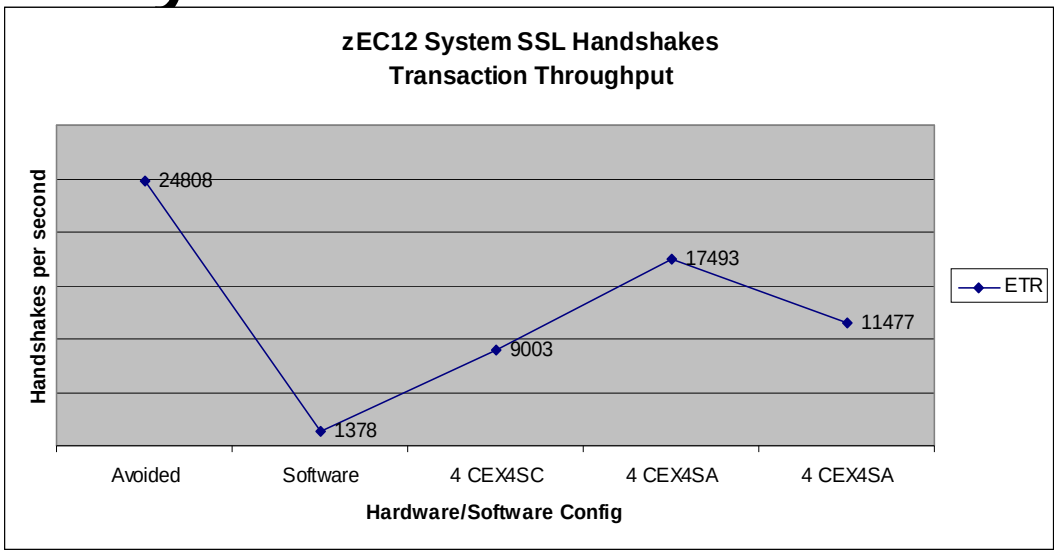
Caching SID/Client Authenti-cation	Hand-shakes	ETR	CPU Util%	Crypto Util %
100%/No	Avoided	28766	62.35%	NA
No/No	Software	1430	99.99%	NA
No/No	4 CEX5C	20561	75.50%	98.50%
No/No	1 CEX5A	21275	78.85%	94.50%
No/Yes	2 CEX5A	8232	42.94%	62.80%

IBM z13 Model 2964-N96 (4 CPs)

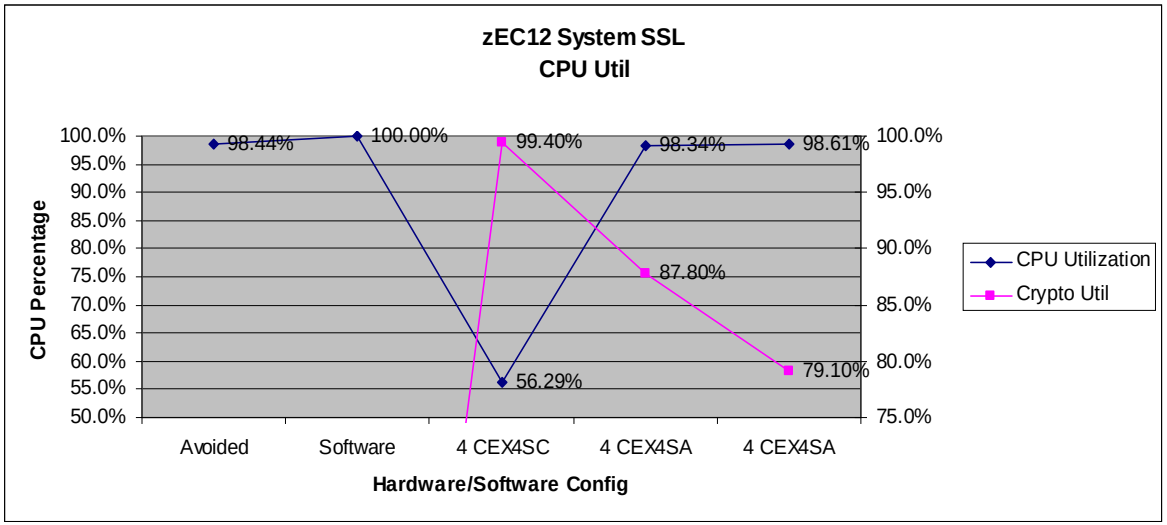
z/OS Version 2 Release 1 (z/OS V2.1)
and ICSF FMID HCR77B0



System SSL Performance – zEC12

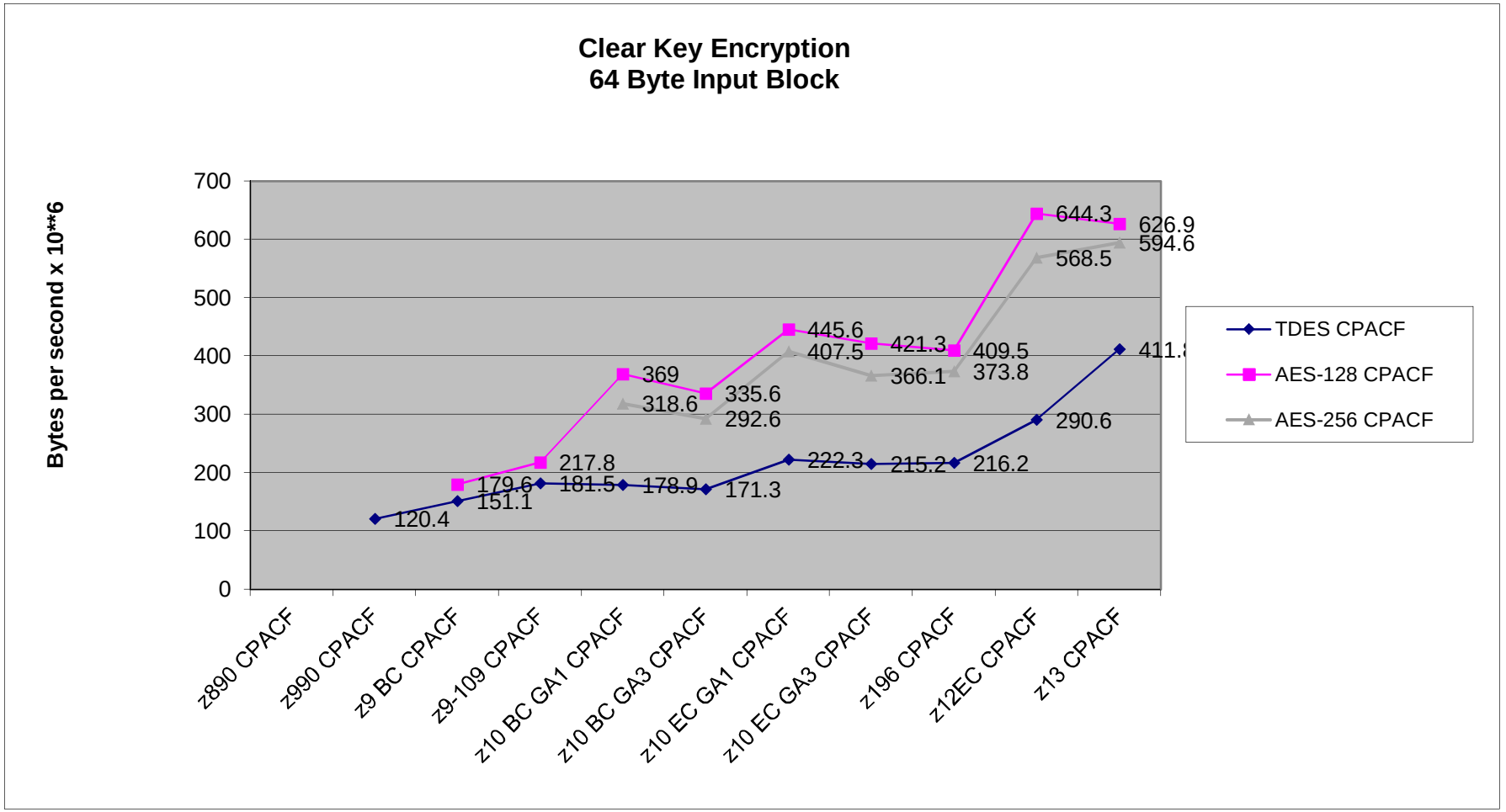


Caching SID/Client Authentication	Handshake	ETR	CPU Util%	Crypto Util %
100%/No	Avoided	24808	98.44%	NA
No/No	Software	1378	100.00%	NA
No/No	4 CEX4SC	9003	56.29%	99.40%
No/No	4 CEX4SA	17493	98.34%	87.80%
No/Yes	4 CEX4SA	11477	98.61%	79.10%

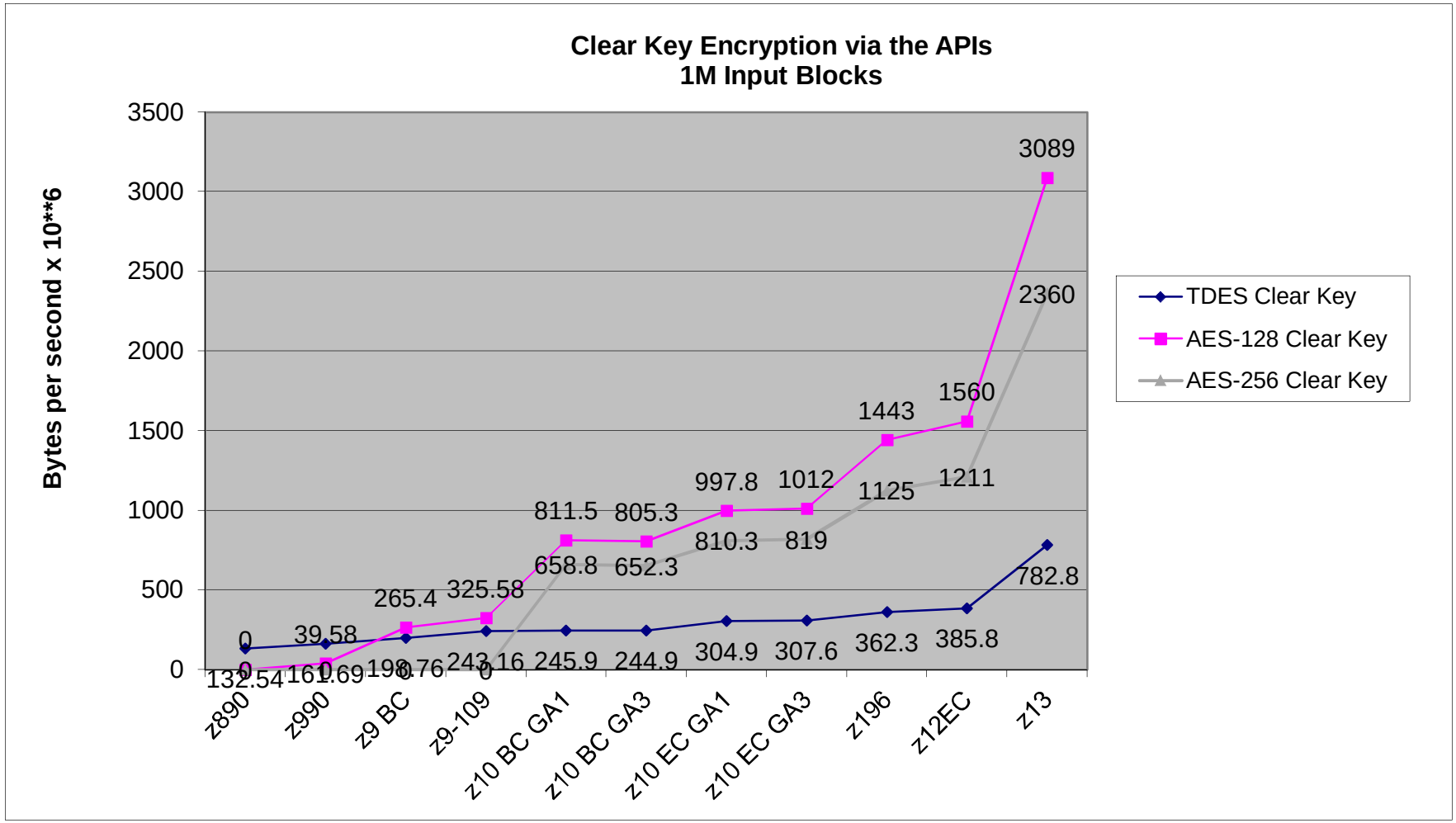


zEC12 HA1 – 4 CPs

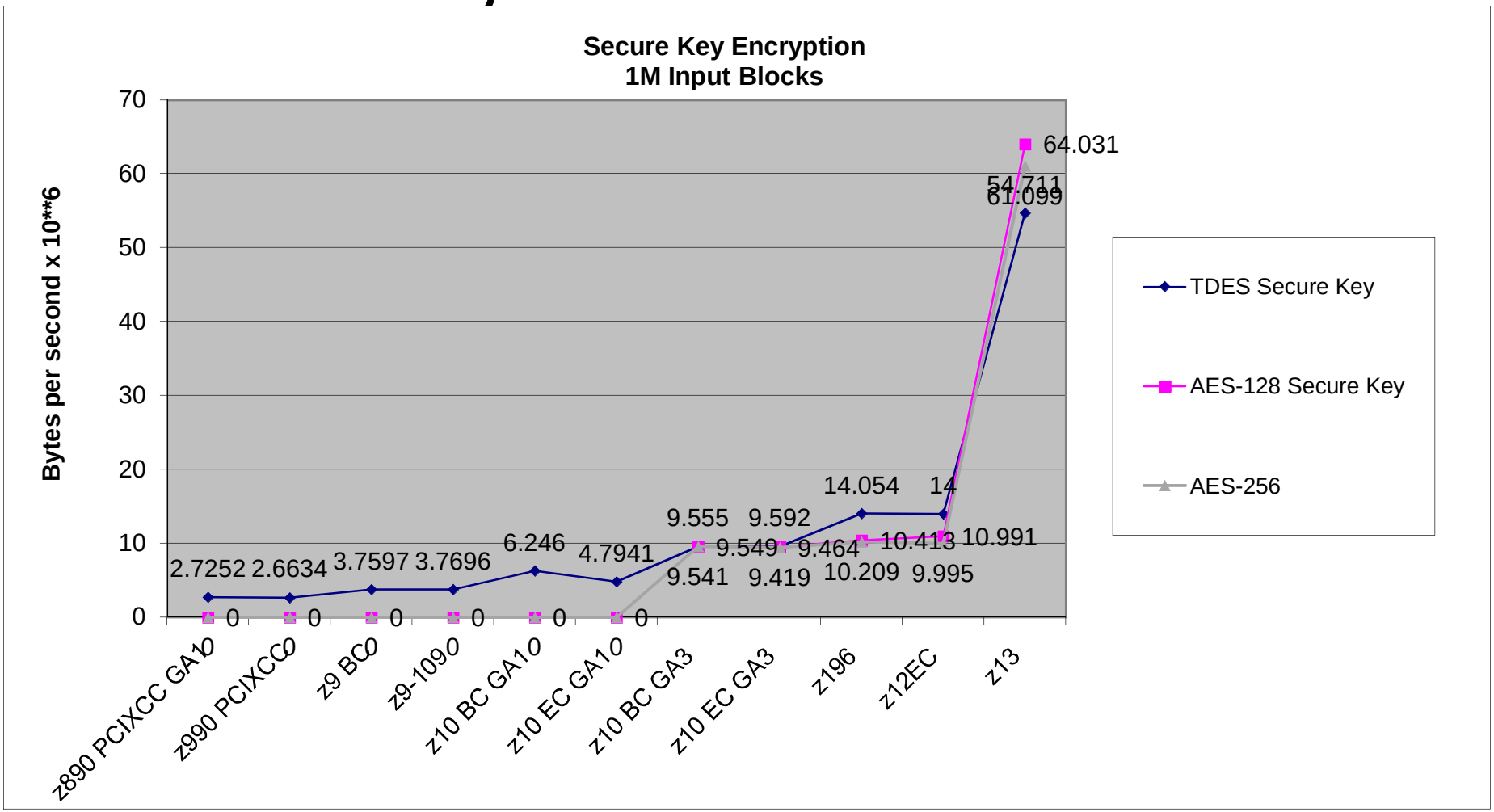
Crypto performance across CECs – Native Clear Key



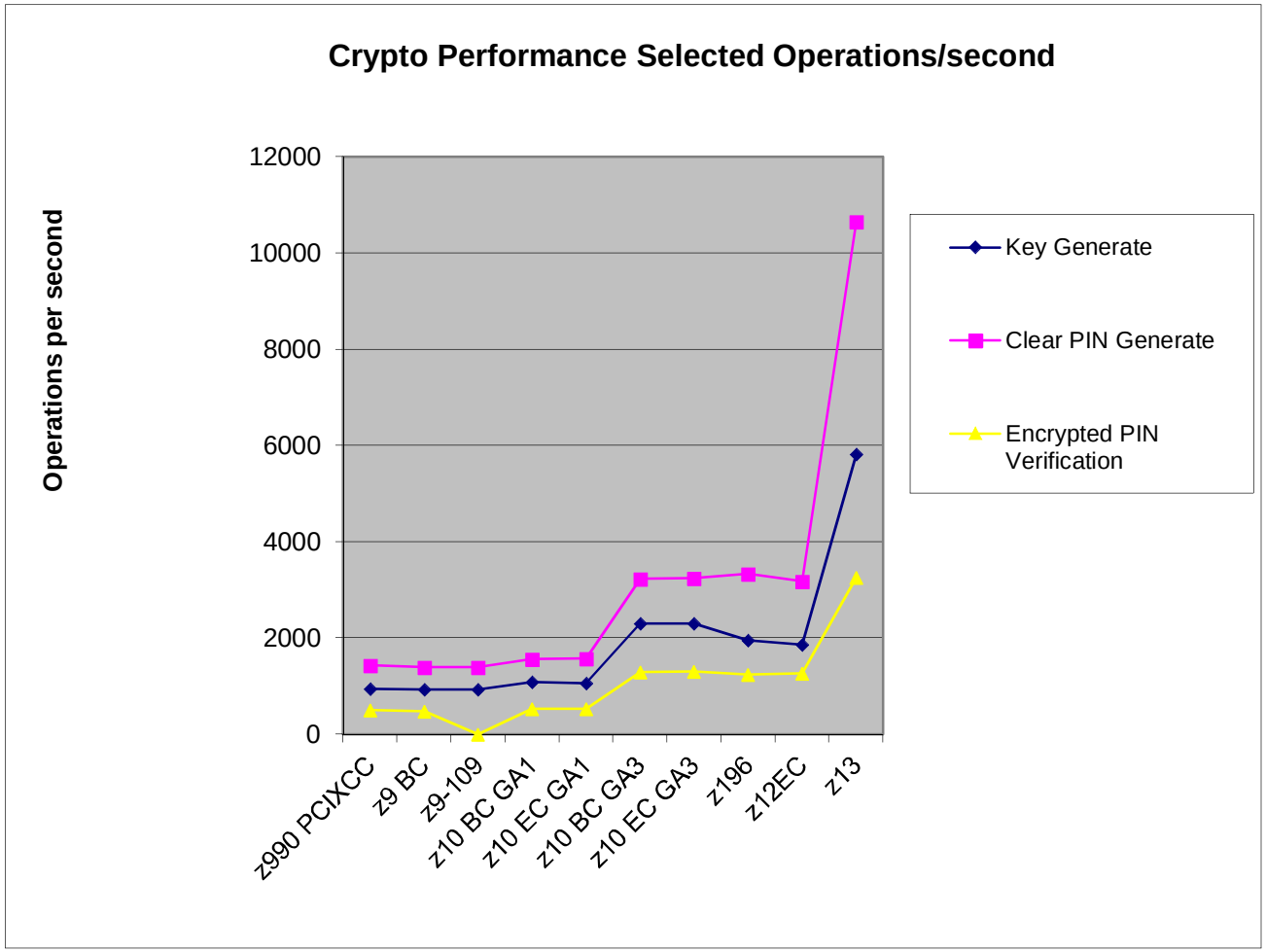
Crypto performance across CECs – using the APIs



Crypto performance across CECs – Secure Key



Crypto Performance across KEKs – selected APIs



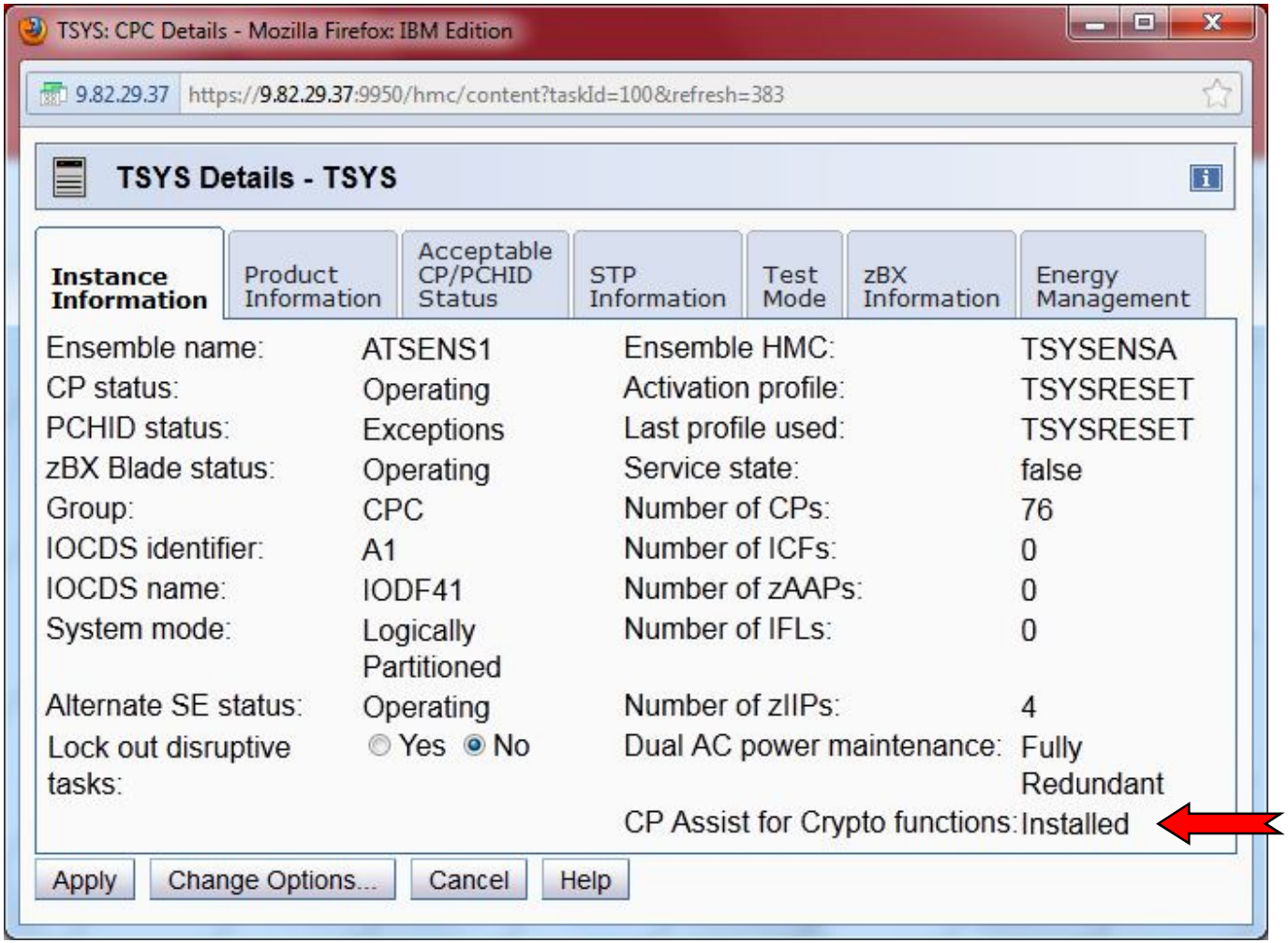
Config for Performance

- ICSF Options
  - KEYAUTH(YES/NO)* – check key integrity in memory
  - CKTAUTH(YES/NO)* – check key integrity on DASD
  - CHECKAUTH(YES/NO) – skip SAF checks for Supervisor State or System Key callers
  - SYSPLEXCKDS / SYSPLEXPKDS / SYSPLEXTKDS – enqueues and contention between systems
- Security Policies
  - Disable OWH and RNG SAF checks**
    - CSF.CSFSERV.AUTH.CSFOWH.DISABLE
    - CSF.CSFSERV.AUTH.CSFRNG.DISABLE

*KEYAUTH & CKTAUTH have been deprecated in HCR77A1

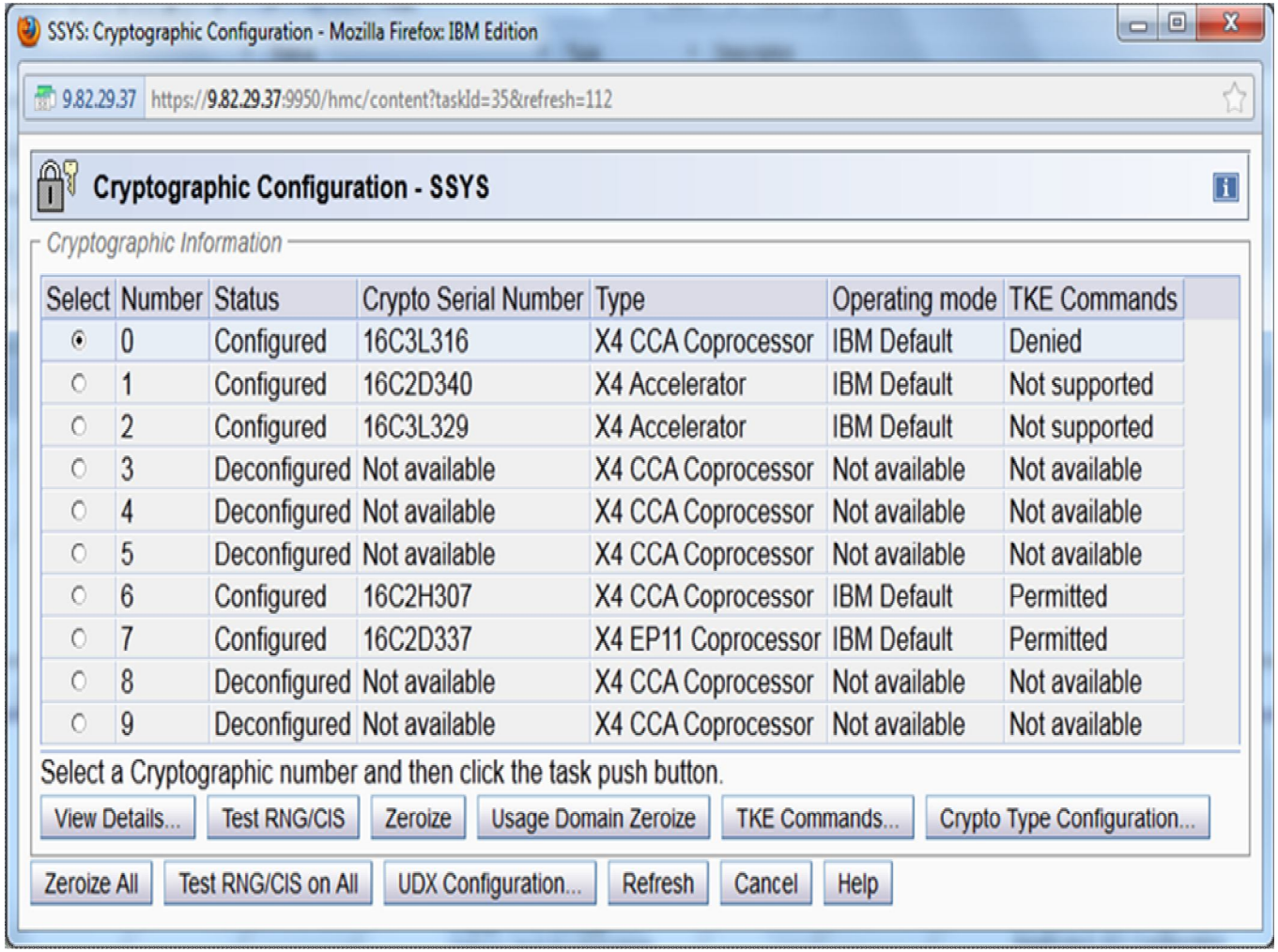
**OWH & RNG SAF Check Security Policies available in HCR77A1

Crypto Microcode Installed?



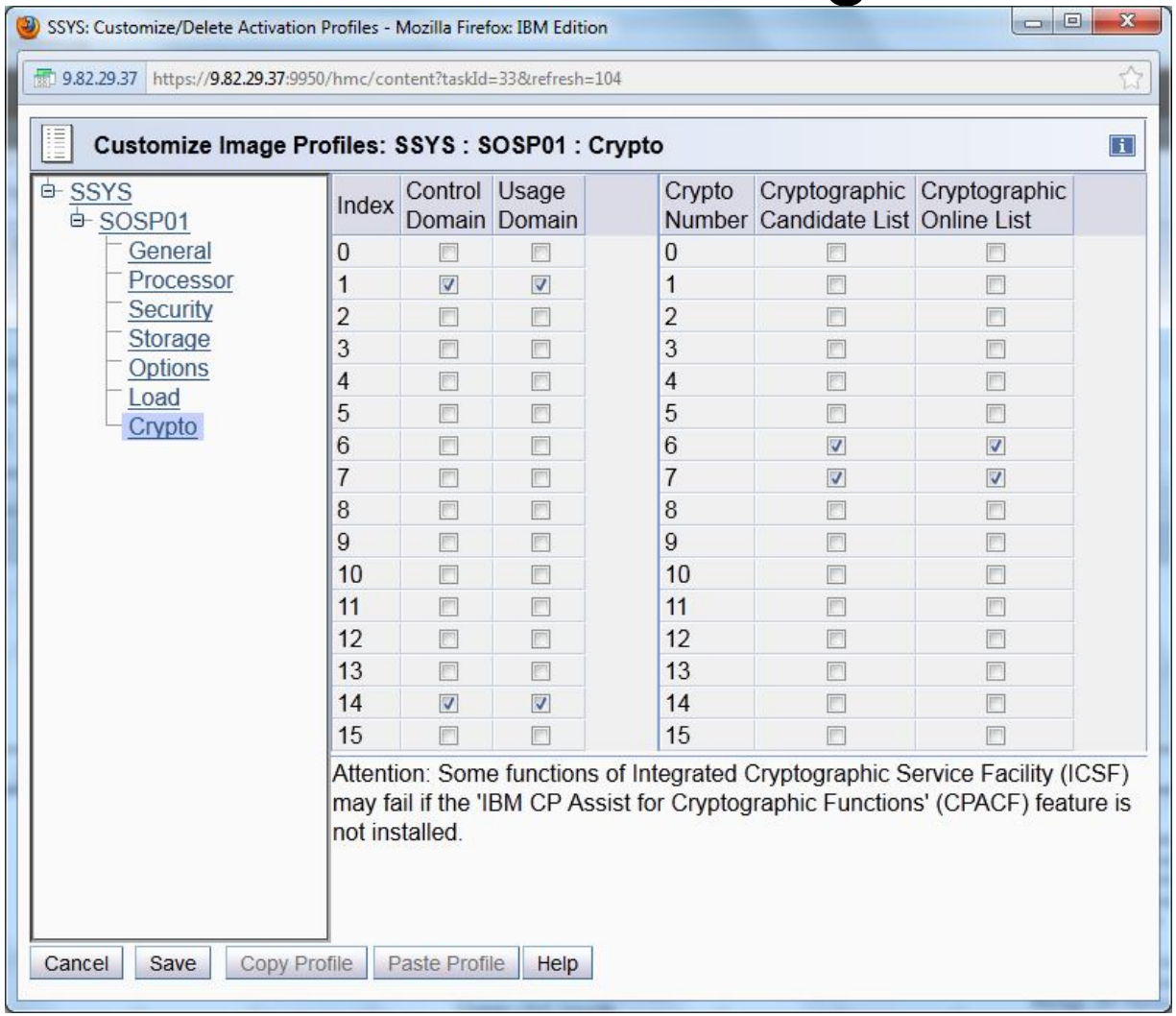
- From the HMC, in Single Object Mode, look at the CPC Details

PCI Cards Installed?



From HMC, CPC Operational Customization, View LPAR Cryptographic Controls

PCI Card LPAR Assignment



Are your Master Keys loaded and correct?

	CoProcessor	Serial Number	Status	AES	DES	ECC	RSA	P11
__	G01	00000001	ONLINE	U	U	C	U	
__	G02	00000002	ACTIVE	A	U	A	E	
__	G03	00000003	ACTIVE	A	U	A	C	
__	H07		ACTIVE					
__	SC06	00000006	ACTIVE	A	U	A	C	
__	SP07	00000008	ACTIVE					A

How do I tell, what ciphersuites – F GSKSRVR,DISPLAY CRYPTO

GSK01009I Cryptographic status

Algorithm	Hardware	Software
DES	56	56
3DES	168	168
AES	256	256
RC2	--	128
RC4	--	128
RSA Encrypt	--	4096
RSA Sign	--	4096
DSS	--	1024
SHA-1	160	160
SHA-2	512	512
ECC	--	--

Environment: z196 running z/OS 1.13, but ICSF not active

How do I tell, what ciphersuites – F GSKSRVR,DISPLAY CRYPTO

GSK01009I Cryptographic status

Algorithm	Hardware	Software
DES	56	56
3DES	168	168
AES	256	256
RC2	--	128
RC4	--	128
RSA Encrypt	4096	4096
RSA Sign	4096	4096
DSS	--	1024
SHA-1	160	160
SHA-2	512	512
ECC	521	521

Environment: z196 running z/OS 1.13, with ICSF active

CPU Measurement Facility

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

Counter #	Description	Counter #	Description
64	Pseudo RNG Function Count	72	DEA Function Count
65	Pseudo RNG Cycle Count	73	DEA Cycle Count
66	Pseudo RNG Blocked Function Count	74	DEA Blocked Function Count
67	Pseudo RNG Blocked Cycle Count	75	DEA 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

Sample Report – Crypto COUNTERS provide measurement of CPACF Crypto Co-Processor Usage

```
*** z10 Summary - CRYPTO  Counters Information ***
***             TOTAL for all CPUs              ***

PRNG Function Count                              0/Sec
PRNG Cycle Count                                 0/Sec
PRNG Blocked Function Count                      0/Sec
PRNG Blocked Cycle Count                         0/Sec
SHA Function Count                            0.73/Sec
SHA Cycle Count                             592.47/Sec
SHA Blocked Function Count                       0/Sec
SHA Blocked Cycle Count                          0/Sec
DEA Function Count                         6277.39/Sec
DEA Cycle Count                          332273396.24/Sec
DEA Blocked Function Count                       0/Sec
DEA Blocked Cycle Count                          0/Sec
AES Function Count                               0/Sec
AES Cycle Count                                  0/Sec
AES Blocked Function Count                       0/Sec
AES Blocked Cycle Count                          0/Sec

***             CRYPTO BUSY SUMMARY             ***

PRNG  Crypto Busy:    0.00%  - for the 3 CPUs
SHA   Crypto Busy:    0.00%  - for the 3 CPUs
DEA   Crypto Busy:    2.55%  - for the 3 CPUs
AES   Crypto Busy:    0.00%  - for the 3 CPUs
---------------------------
Total Crypto Busy:    2.55%  - for the 3 CPUs
```

This information may be useful in determining:

- A count of How Many CPACF encryption functions were executed
- How much CPU Time (cycles) were used

The encryption facility executed both SHA functions and TDES functions for this specific test.

Ran DASD dumps sequentially over 20 minute duration With option: ENCRYPT(CLRTDES) - These numbers come from a synthetic Benchmark and do not represent a production workload

- **It is important to remember that other Crypto functions may be executing in software and/or on Crypto Express Cards (if installed & implemented). This is not measured by the CPU MF Crypto COUNTERS**
- **CPU MF Crypto COUNTERS can help assess how many of the Crypto Functions are occurring on the CPACF Co-Processors**

Slide adapted from several Share presentations by John Burg

SMF Type 82 – ICSF Record

- Subtype 1 – ICSF Initialization
- Subtype 3 – change in number of available processors
- Subtype 4 – when ICSF handles error conditions for crypto feature failure or tampering
- Subtype 5 – change in SSM
- Subtype 6 & 7 – when a key part is entered via Key Entry Unit (KEU)
- Subtype 7 – Key Part Entry Section
- Subtype 8 – Cryptographic Key Data Set Refresh Section
- Subtype 9 – Dynamic CKDS Update
- Subtype 10 – when clear key part entered for PKA-MK

SMF Type 82 – ICSF Record (cont.)

- Subtype 11 – when clear key part entered for DES-MK
- Subtype 12 – for each request and reply from calls to CSFSPKSC service by TKE
- Subtype 13 – Dynamic PKDS Update
- Subtype 14 – Cryptographic Coprocessor Master Key Entry
- Subtype 15 – PCI Cryptographic Coprocessor Retained Key Create/Delete
- Subtype 16 – PCI Cryptographic Coprocessor TKE
- Subtype 17 – periodically to provide some indication of PCI Cryptographic Coprocessor usage
- Subtype 18 – Cryptographic Processor Configuration
- Subtype 19 – PCI X Cryptographic Coprocessor Timing

SMF Type 82 – ICSF Record (cont.)

- Subtype 20 – Cryptographic Processor Processing Times
- Subtype 21 – ICSF Sysplex Group Change Section
- Subtype 22 – Trusted Block Create Callable Services Section
- Subtype 23 – Token Data Set Update
- Subtype 24 – Duplicate Tokens Found
- Subtype 25 – Key Store Policy
- Subtype 26 – Public Key Data Set Refresh
- Subtype 27 – PKA Key Management Extensions
- Subtype 28 –High Performance Encrypted Key (Protected Key)
- Subtype 29 – TKE Workstation Audit Record

REXX EXEC CSFSMFR/Batch Job CSFSMFJ

- Formats the SMF Type 82 records into a readable report
  - Run CSFSMFJ to
    - Capture the Type 82 records (with IFASMFDP)
    - Sort the records by date/time
    - Execute CSFMFR, via Batch TSO
  - Each Type 82 generates multiple lines of output
  - Formats the Type 82 for easier reading, but still lots of hex data to interpret

Subtype=0014 Cryptographic Coprocessor Timing
Written periodically to provide some indication of coprocessor and accelerator
Nov 2011 0:00:19.26
TME... 00000786 DTE... 0111305F SID... SYSC SSI... 00000000 STY... 0014
TFL... 10000000
TFL 10 Coprocessor is a CEX3C
TNQ... C89B5841F5841AB1 TDQ... C89B5841F59D39B1 TWT... C89B5841F59D5AB1
TQU... 00000000 TSF... áä TIX... 00
TSN... 91008705 TDM... 02 TRN... 40

- Forensics report, not a performance report
- See the ICSF Systems Programmer's Guide

SMF Type 70, Subtype 2 - RMF Processor Activity

- Cryptographic Coprocessor Data Section
  - Processor Index, Processor Type
  - Scaling Factor
  - Execution Time of all operations
  - Number of all operations on the coprocessor
  - Number of all RSA-key-generation operations
- Cryptographic Accelerator Data Section
  - Processor Index, Processor Type
  - Validity bit mask, Number of engines on the accelerator
  - Scaling factor
  - Execution time & number of operations by
    - 1024-bit-ME
    - 1024-bit-CRT
    - 4096-bit-ME
    - 2048-bit-ME
    - 2048-bit-CRT
    - 4096-bit CRT

SMF Type 70, Subtype 2 - RMF Processor Activity

- Cryptographic PKCS11 Coprocessor Data Section
  - Processor Index, Processor Type
  - Scaling Factor
  - Aggregate Execution Time, Number of Operations
    - Slow asymmetric-key functions
    - Fast asymmetric-key functions
    - Asymmetric-key generation
    - Symmetric-key functions complete
    - Symmetric-key functions partial

SMF Type 70, Subtype 2 - RMF Processor Activity (cont.)

- ICSF Services Data Section
  - Single DES (Encipher & Decipher): Number of calls, bytes, and instructions
  - Triple DES (Encipher & Decipher): Number of calls, bytes, and instructions
  - MAC Generate/Verify: Number of calls to generate/verify, number of bytes for which MAC was generated/verified, number of PCMF instructions used to generate/verify the MAC
  - SHA-1: Number of calls to hash, number of bytes that were hashed, number of PCMF instructions used to hash the data
  - PIN: number of translate calls, number of verify calls
  - SHA-224, SHA-256, SHA-384, SHA-512 : Number of calls to hash, number of bytes that was hashed, number of PCMF instructions used to hash the data
  - ICSF Data Level
  - AES Encipher & Decipher: number of calls sent to cop, number of bytes processed, number of operations

RMF Crypto Hardware Activity Report

(From z/OS RMF Report Analysis 2.1, SC34-2665-00)

C R Y P T O H A R D W A R E A C T I V I T Y

PAGE 1

z/OS V2R1 SYSTEM ID TRX2 START 09/28/2013-08.15.00 INTERVAL 007.14.59
RPT VERSION V2R1 RMF END 09/28/2013-15.30.00 CYCLE 1.000 SECONDS

-------- CRYPTOGRAPHIC CCA COPROCESSOR ----

		---------- TOTAL ----------			KEY-GEN
TYPE	ID	RATE	EXEC TIME	UTIL%	RATE
CEX2C	0	0.00	0.000	0.0	0.00
	1	2.16	295.9	63.9	2.14
	2	0.00	0.000	0.0	0.00
CEX3C	4	2.15	227.8	48.9	2.15
CEX4C	7	0.29	1.926	0.1	0.00

---------- CRYPTOGRAPHIC PKCS11 COPROCESSOR ----------

		---------- TOTAL ----------			---------- OPERATIONS DETAILS ----------			
TYPE	ID	RATE	EXEC TIME	UTIL%	FUNCTION	RATE	EXEC TIME	UTIL%
CEX4P	8	373.4	0.295	11.0	ASYM FAST	177.2	0.175	3.1
					ASYM GEN	0.00	0.000	0.0
					ASYM SLOW	160.9	0.405	6.5
					SYMM COMPLETE	0.00	0.000	0.0
					SYMM PARTIAL	35.36	0.398	1.4

RMF Crypto Hardware Activity Report

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

		--------- TOTAL ----------			- ME-FORMAT RSA OPERATIONS -			- CRT-FORMAT RSA OPERATIONS -		
TYPE	ID	RATE	EXEC TIME	UTIL%	KEY	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%
CEX2A	3	766.9	0.434	33.3	1024	362.4	0.521	18.9	369.5	0.183	6.8
					2048	0.00	0.000	0.0	34.99	2.175	7.6
CEX3A	5	998.9	0.365	36.5	1024	246.4	0.534	13.2	554.3	0.205	11.3
					2048	0.00	0.000	0.0	83.16	0.689	5.7
					4096	0.00	0.000	0.0	115.1	0.547	6.3
CEX4A	6	918.4	0.301	27.6	1024	394.6	0.409	16.1	435.4	0.179	7.8
					2048	0.00	0.000	0.0	88.33	0.415	3.7
					4096	0.00	0.000	0.0	0.00	0.000	0.0

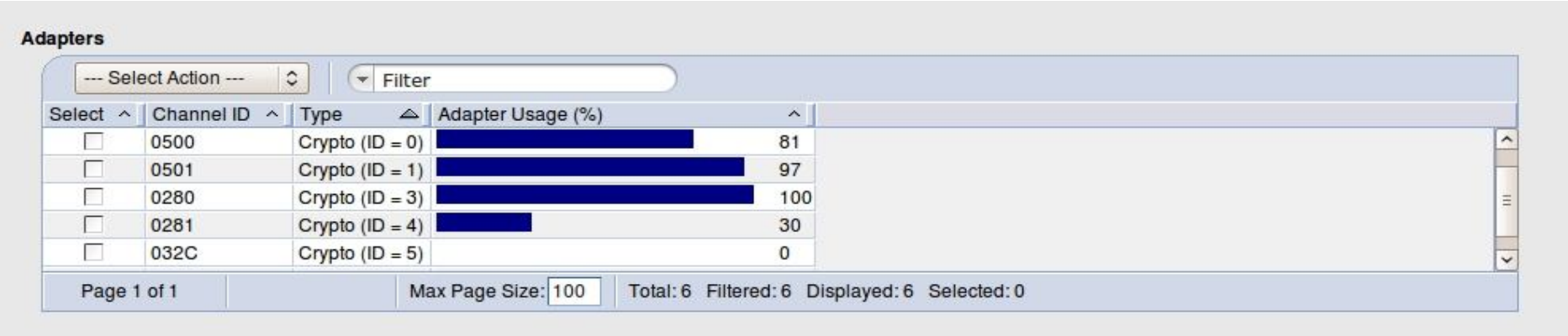
-------- ICSF SERVICES ----------

	--- ENCRYPTION ----			--- DECRYPTION ---			------- MAC --------		---------- HASH ----------			-------- PIN ----------	
	SDES	TDES	AES	SDES	TDES	AES	GENERATE	VERIFY	SHA-1	SHA-256	SHA-512	TRANSLATE	VERIFY
RATE	15.41	10.27	0.02	5.14	10.27	0.02	34.23	35.87	15352	<0.01	<0.01	8.97	5.14
SIZE	3200	4400	189.0	800.0	4400	189.5	4573	4400	105.0	48.00	48.00		

HMC Dashboard Monitor

- The HMC/SE Monitors on the zEC12 now include a display for the crypto adapters.
- The Adapter Usage percentage is the same utilization that shows up in the RMF Crypto Hardware Activity Report.
- The Utilization on the card is calculated using the formula: U = (Ta2 - Ta1) * S / (T2 -T1)

Ta: time used for execution S: scaling factor T: Time of measurement interval



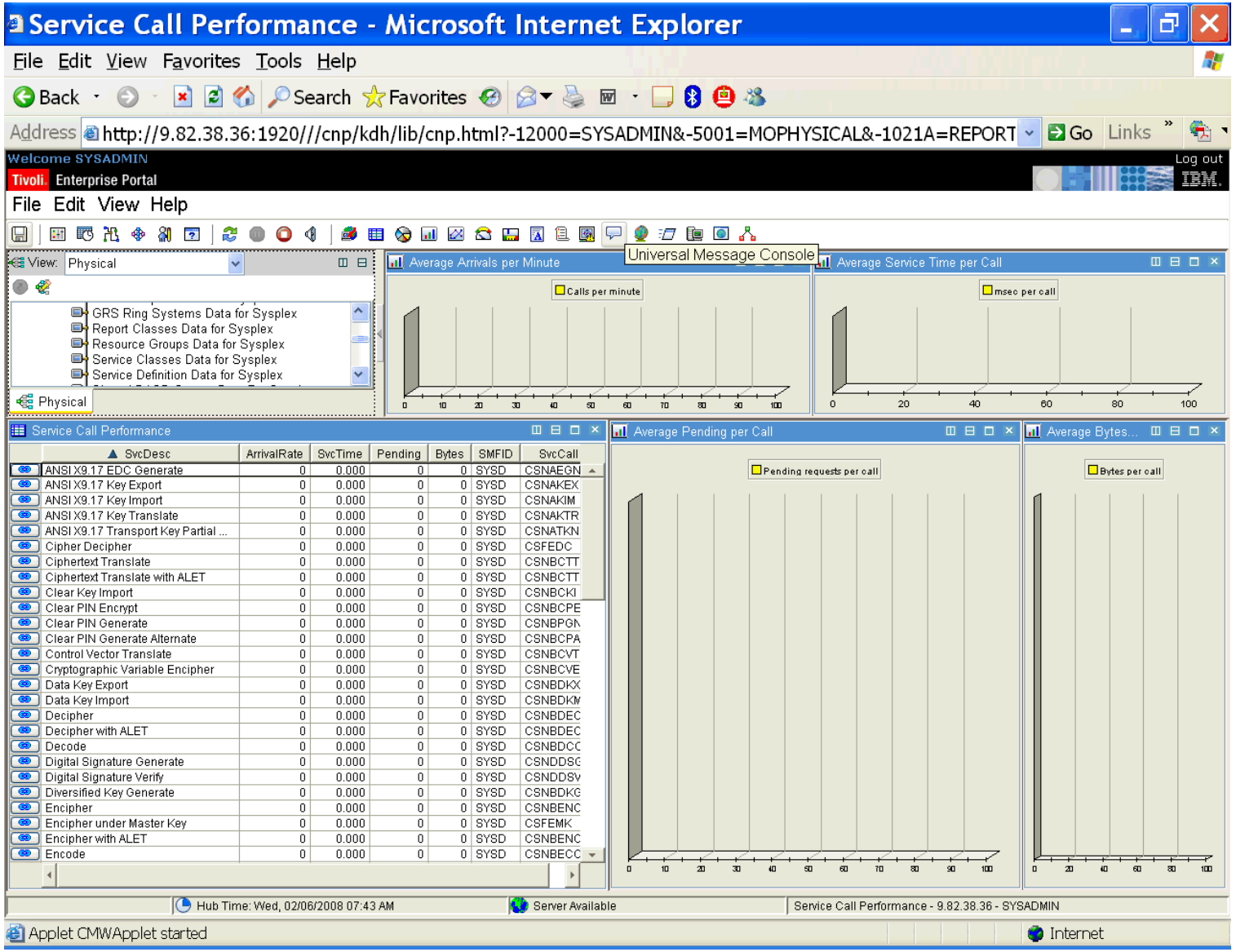
Workload Activity (SMF Type 72, Subtype 3)

- Crypto Using and Delay Samples
  - CAM crypto using samples: a TCB was found executing on a cryptographic asynchronous message processor
  - CAM crypto delay samples: a TCB was found waiting on a cryptographic asynchronous message processor
  - AP crypto using samples: a TCB was found executing on a cryptographic assist processor
  - AP crypto delay samples: a TCB was found waiting on a cryptographic assist processor

Common Address Space Work (SMF Type 30)

- SMF30CSC – ICSF Service Count
  - CSNBENC (Single-DES) - # of service calls, # of bytes, # of CMD instructions
  - CSNBENC (Double & Triple-DES) - # of service calls, # of bytes, # of CMD instructions
  - CSNBDEC (Single-DES) - # of service calls, # of bytes, # of CMD instructions
  - CSNBDEC (Double & Triple-DES) - # of service calls, # of bytes, # of CMD instructions
  - CSNBMGN (MAC Generate) - single and various double key MAC; # of service calls, # of bytes, # of CMD instructions
  - CSNBMVR (MAC Verify) - single and various double key MAC; # of service calls, # of bytes, # of CMD instructions
  - CSNBOWH (SHA-1) - # of Service calls, # of bytes, # of PCMF instructions
  - CSNBOWH (SHA-256 which includes SHA-224) - # of Service calls , # of bytes, # of PCMF instructions
  - CSNBOWH (SHA-512 which includes SHA-384) - # of Service calls , # of bytes, # of PCMF instructions
  - CSNBPTR - # of Service calls
  - CSNBPVR - # of Service calls

Omegamon


Service Call Performance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://9.82.38.36:1920///cnp/kdh/lib/cnp.html?-12000=SYSADMIN&-5001=MOPHYSICAL&-1021A=REPORT
Go Links
Welcome SYSADMIN
Log out
Tivoli Enterprise Portal
IBM
File Edit View Help
Universal Message Console
View: Physical
GRS Ring Systems Data for Sysplex
Report Classes Data for Sysplex
Resource Groups Data for Sysplex
Service Classes Data for Sysplex
Service Definition Data for Sysplex
Physical
Average Arrivals per Minute
Calls per minute
Average Service Time per Call
msec per call
Service Call Performance
SvcDesc ArrivalRate SvcTime Pending Bytes SMFID SvcCall
ANSI X9.17 EDC Generate 0 0.000 0 0 SYSD CSNAEGN
ANSI X9.17 Key Export 0 0.000 0 0 SYSD CSNAKEX
ANSI X9.17 Key Import 0 0.000 0 0 SYSD CSNAKIM
ANSI X9.17 Key Translate 0 0.000 0 0 SYSD CSNAKTR
ANSI X9.17 Transport Key Partial ... 0 0.000 0 0 SYSD CSNATKN
Cipher Decipher 0 0.000 0 0 SYSD CSFEDC
Ciphertext Translate 0 0.000 0 0 SYSD CSNBCTT
Ciphertext Translate with ALET 0 0.000 0 0 SYSD CSNBCTT
Clear Key Import 0 0.000 0 0 SYSD CSNBCKI
Clear PIN Encrypt 0 0.000 0 0 SYSD CSNBCPE
Clear PIN Generate 0 0.000 0 0 SYSD CSNBPGN
Clear PIN Generate Alternate 0 0.000 0 0 SYSD CSNBCPA
Control Vector Translate 0 0.000 0 0 SYSD CSNBCVT
Cryptographic Variable Encipher 0 0.000 0 0 SYSD CSNBCVE
Data Key Export 0 0.000 0 0 SYSD CSNBDKX
Data Key Import 0 0.000 0 0 SYSD CSNBDKM
Decipher 0 0.000 0 0 SYSD CSNBDEC
Decipher with ALET 0 0.000 0 0 SYSD CSNBDEC
Decode 0 0.000 0 0 SYSD CSNBDCC
Digital Signature Generate 0 0.000 0 0 SYSD CSNDDSG
Digital Signature Verify 0 0.000 0 0 SYSD CSNDDSV
Diversified Key Generate 0 0.000 0 0 SYSD CSNBDKG
Encipher 0 0.000 0 0 SYSD CSNBENC
Encipher under Master Key 0 0.000 0 0 SYSD CSFEMK
Encipher with ALET 0 0.000 0 0 SYSD CSNBENC
Encode 0 0.000 0 0 SYSD CSNBECC
Average Pending per Call
Pending requests per call
Average Bytes...
Bytes per call
Hub Time: Wed, 02/06/2008 07:43 AM
Server Available
Service Call Performance - 9.82.38.36 - SYSADMIN
Applet CMWApplet started
Internet

Summary

- There is performance data available, but …
- Your implementation will be the most significant factor in terms of performance
- Consider your ICSF options (and their impact on performance)
- Start collecting performance data now, and look for trends
- Hopefully the performance reporting will get better

IBM Manuals & Redbooks

- SC14-7507 ICSF System Programmer's Guide
- SC34-2665 z/OS RMF Report Analysis 2.1
- SA22-7630 z/OS System Measurement Facilities (SMF)
- SG24-6645 Effective zSeries Performance Monitoring Using Resource Measurement Facility
- REDP-4358 Monitoring System z Cryptographic Services

Crypto Performance Whitepapers

- z13
  - http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=ZSW03283USEN&attachment=ZSW03283USEN.PDF
- zEC12
  - http://www.ibm.com/systems/z/advantages/security/zec12cryptography.html
- z196 and z10
  - http://www.ibm.com/systems/z/advantages/security/z10cryptography.html

z/OS Communications Server performance index

- http://www.ibm.com/support/docview.wss?uid=swg27005524

CPU Measurement Facility Doc

- IBM Research article
  - ***"IBM System z10 performance improvements with software & hardware synergy"***
  - http://www.research.ibm.com/journal/rd/531/jackson.pdf
    - Contact IBM team for copy of the article
- Feb 2011 *Hot Topics - A z/OS Newsletter* - GA22-7501
  - ***"A whole lot of benefits from HIS data" article page 24***
- Redpaper *Setting Up and Using System z CPU Measurement Facility with z/OS*
  - http://www.redbooks.ibm.com/redpieces/pdfs/redp4727.pdf

Questions …