IBM Americas, ATS, Washington Systems Center

Crypto Performance Update

Share 14668
Anaheim, CA
March, 2014

Greg Boyd (boydg@us.ibm.com)

ON DEMAND BUSINESS™

QR Code – Share 14668

- **Share 14668**
- **Anaheim, CA**
- **March, 2014**

Agenda

- **Crypto Refresher**
  - Crypto Functions
  - Clear Key vs Secure Key vs Protected Key
  - Crypto Hardware
- **Crypto Performance – Raw numbers**
- **Operational 'Things'**
- **Available metrics**

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**

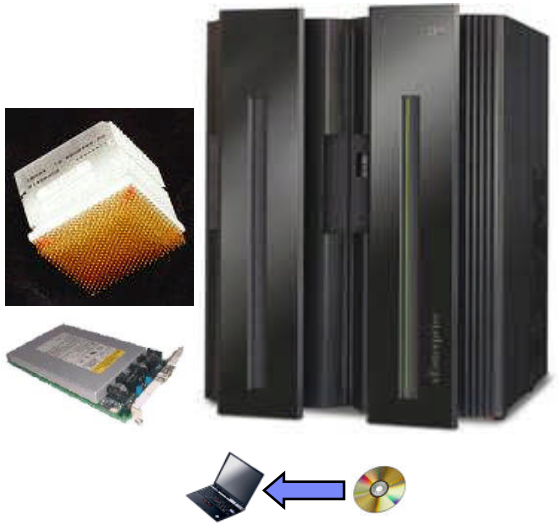
Clear Key / Secure Key / Protected Key

- **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 – zEC12, zBC12, z196/z114

- **CP Assist for Crypto Function (CPACF)**
  - **DES (56-, 112-, 168-bit), new chaining options**
  - **AES-128, AES-192, AES-256, new chaining options**
  - **SHA-1, SHA-256, SHA-512 (SHA-2)**
  - **PRNG**
  - **Protected Key**

Single CPACF per CP on zEC12 & z9



TechDoc WP100810 – A Synopsis of System z Crypto Hardware

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

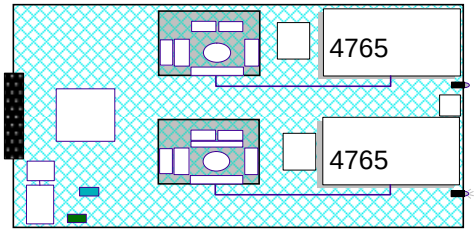
- **Secure Key DES/TDES**
- **Secure Key AES**
- **Financial (PIN) Functions**
- **Random Number Generate and Generate Long**
- **Key Generate/Key Management**
- **SSL Handshakes, ECDSA support**
- **Protected Key Support**
- **PKCS #11 (CEX4S only)**

TechDoc WP100810 – A Synopsis of System z Crypto Hardware

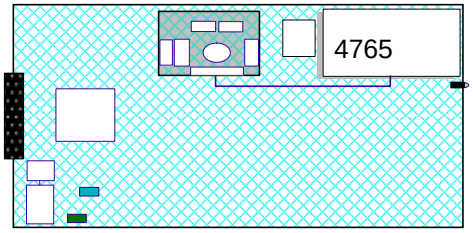
PCI Cards

- **Secure Coprocessor** (default)
  - Requires master key be loaded
  - Data confidentiality
  - Data integrity
  - Financial functions
  - Key generation/manipulation
  - RSA public key operations
- **Accelerator**
  - RSA public key operations
- **Enterprise PKCS #11**
  - PKCS #11 secure key

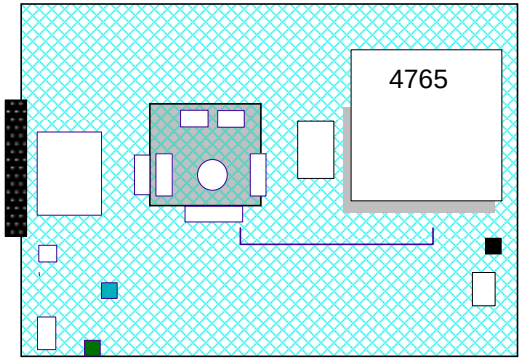
CEX3



CEX3-1P



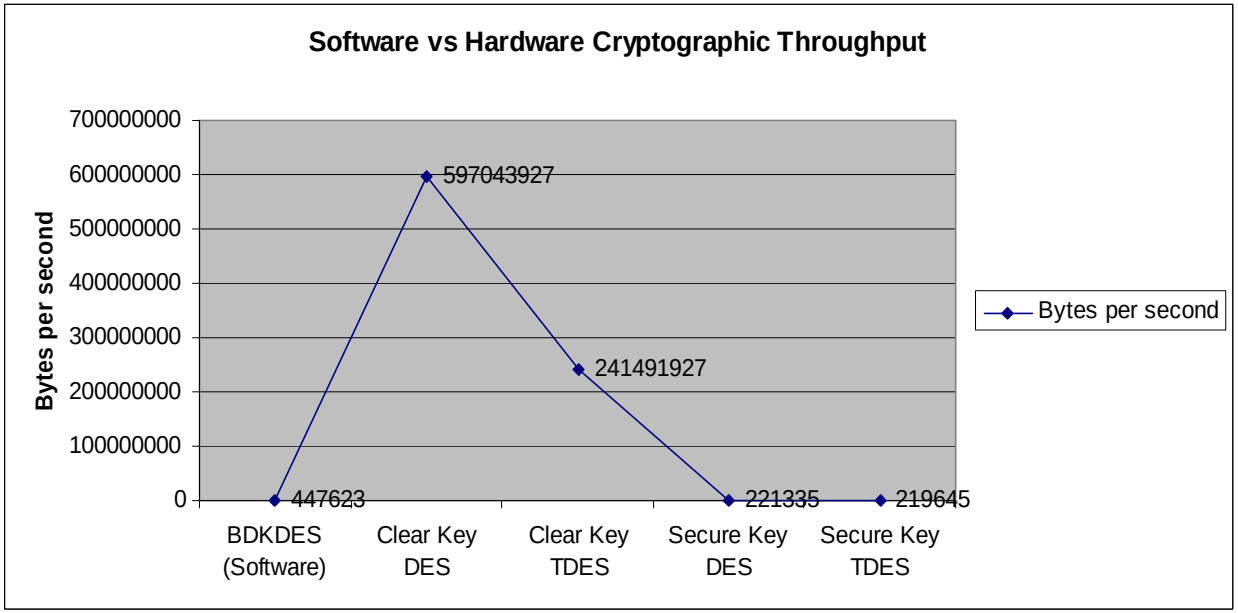
CEX4S

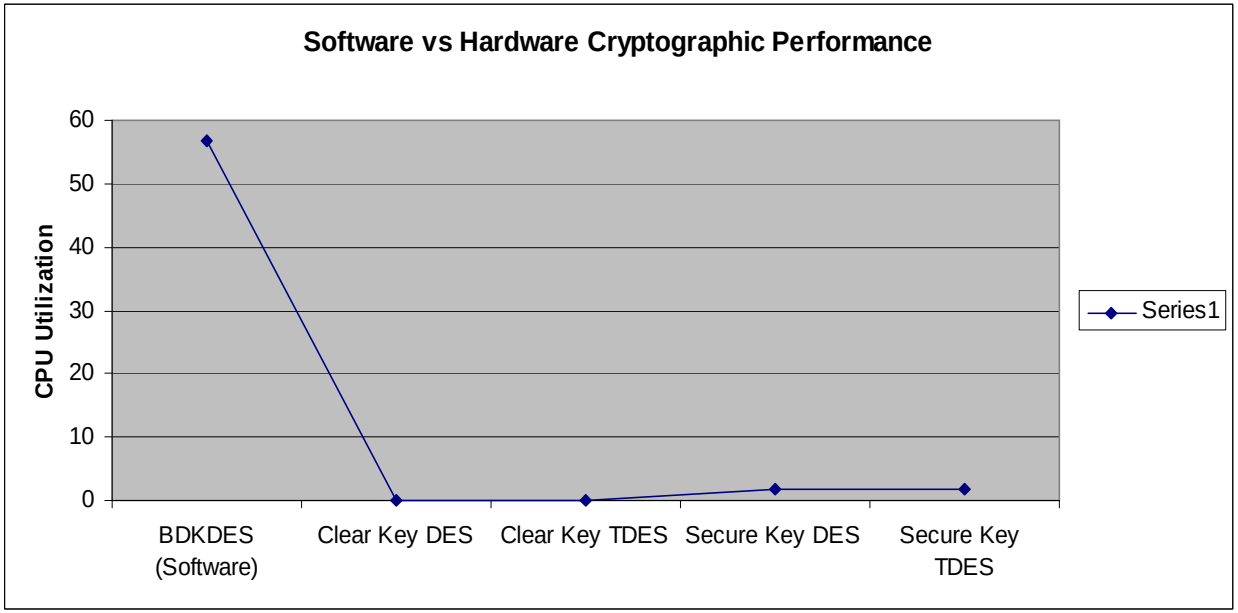


Software vs Hardware Encryption

	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

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

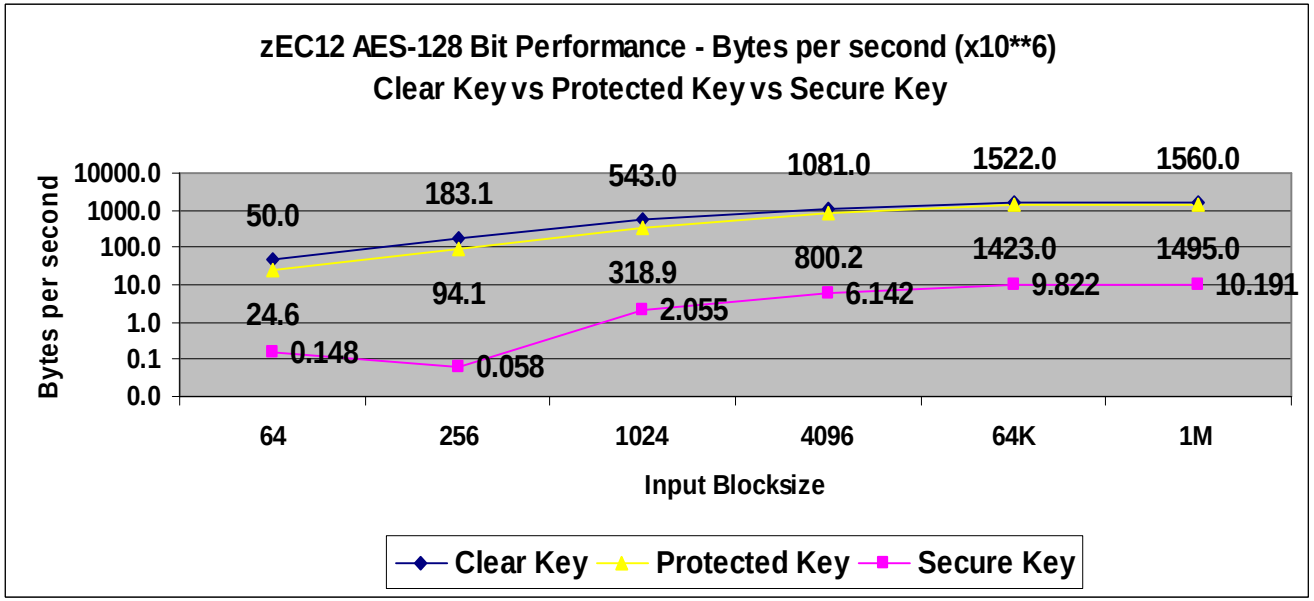


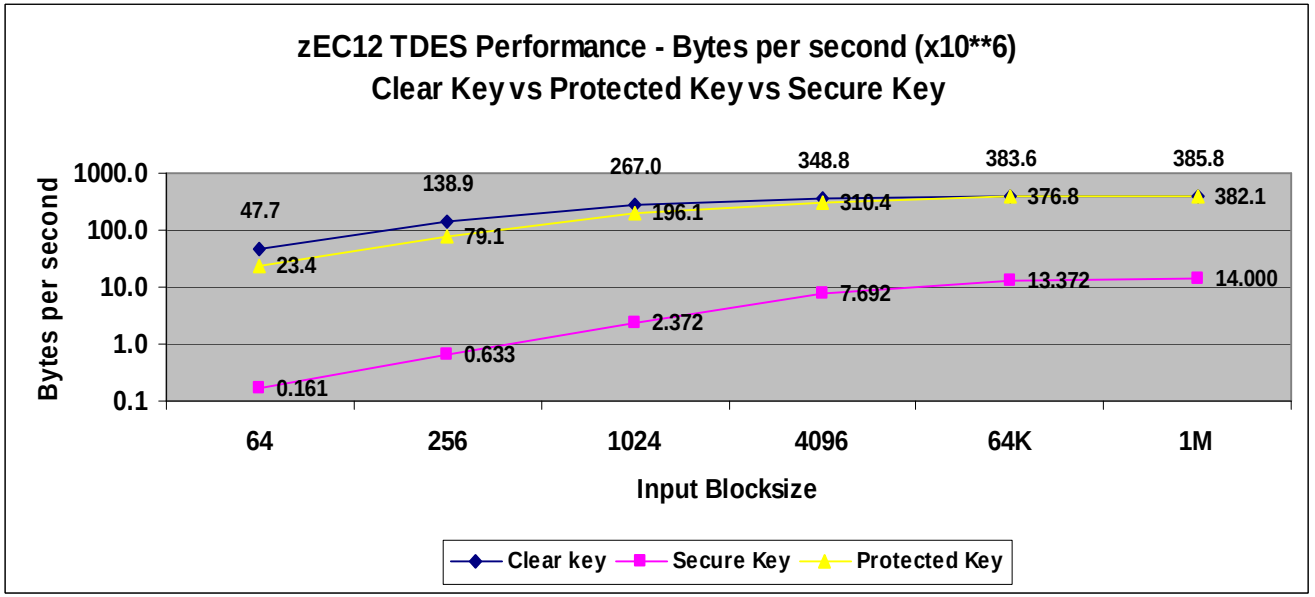


zEC12 Symmetric Key Performance

- From the Crypto Performance whitepaper at

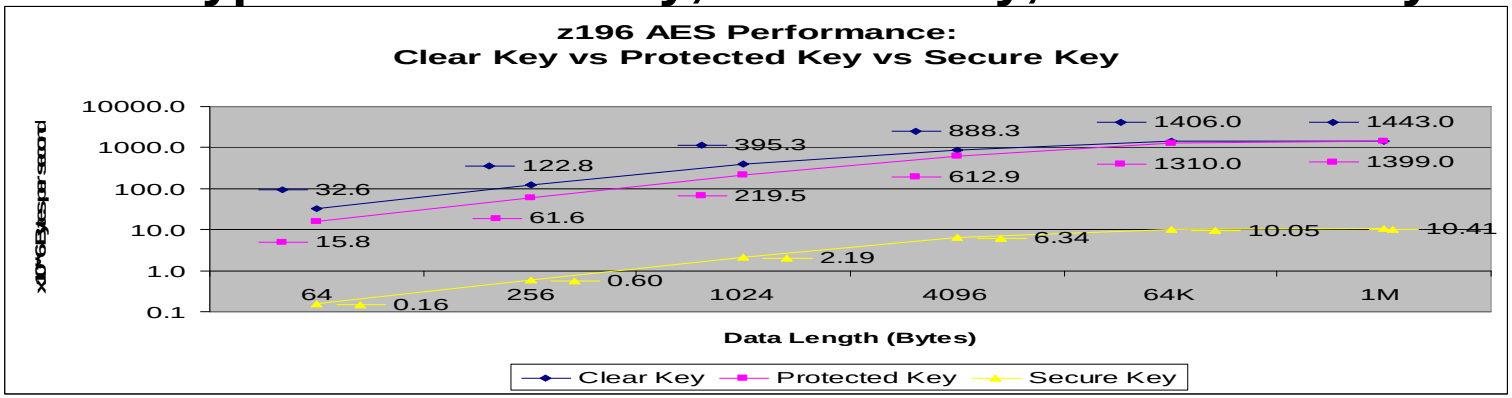
http://www.ibm.com/systems/z/advantages/security/zec12cryptography.html



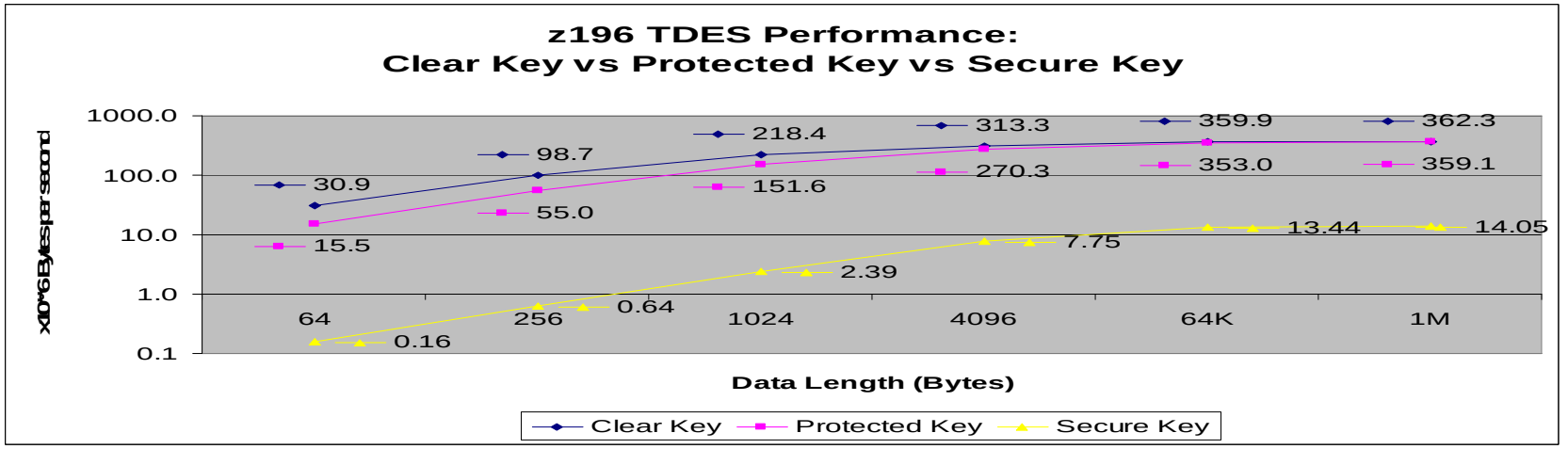


z196 Crypto Performance

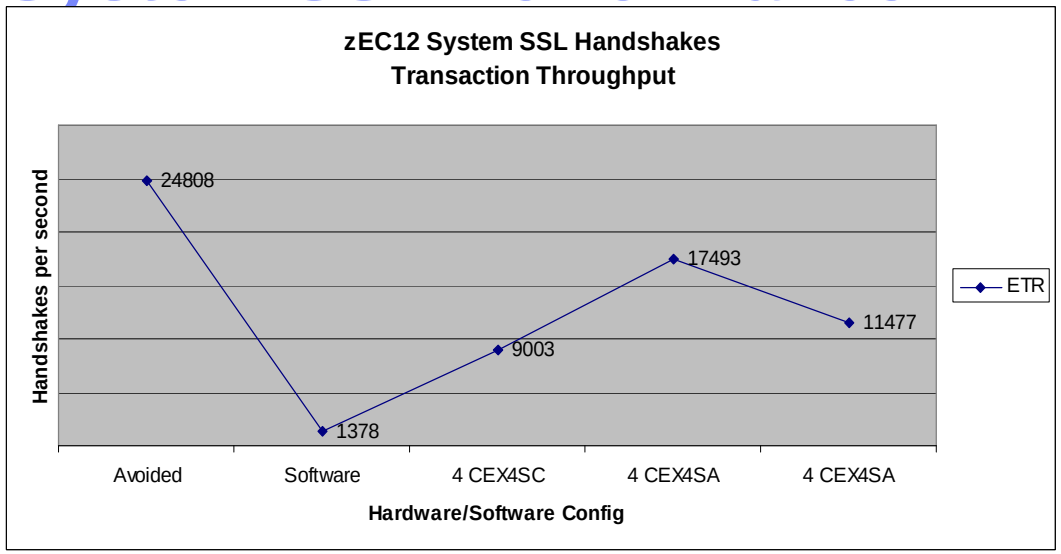
- **AES Encryption – Clear Key, Secure Key, Protected Key**



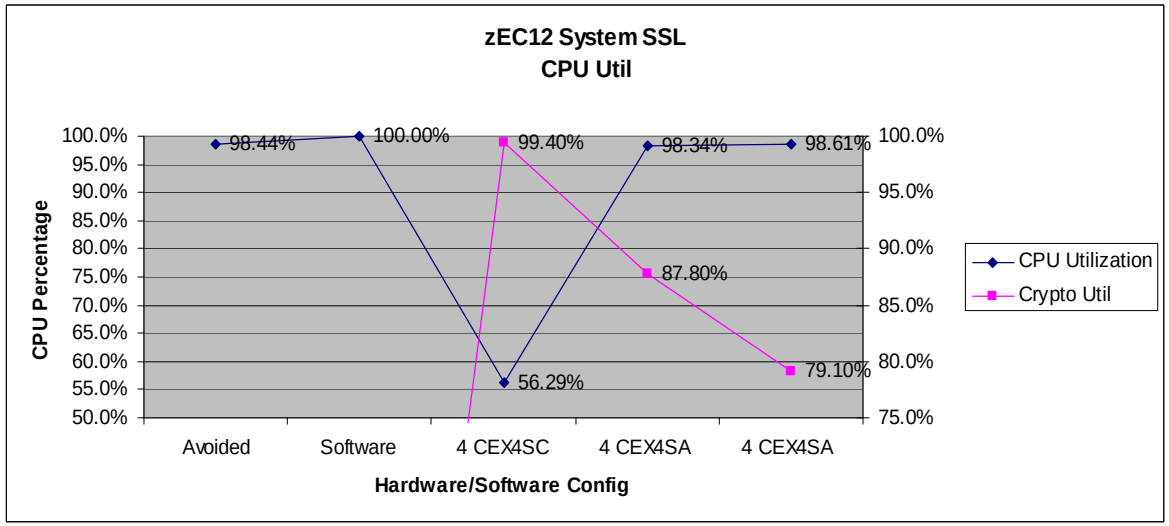
- **TDES Encryption – Clear Key, Secure Key, Protected Key**



System SSL Performance – zEC12

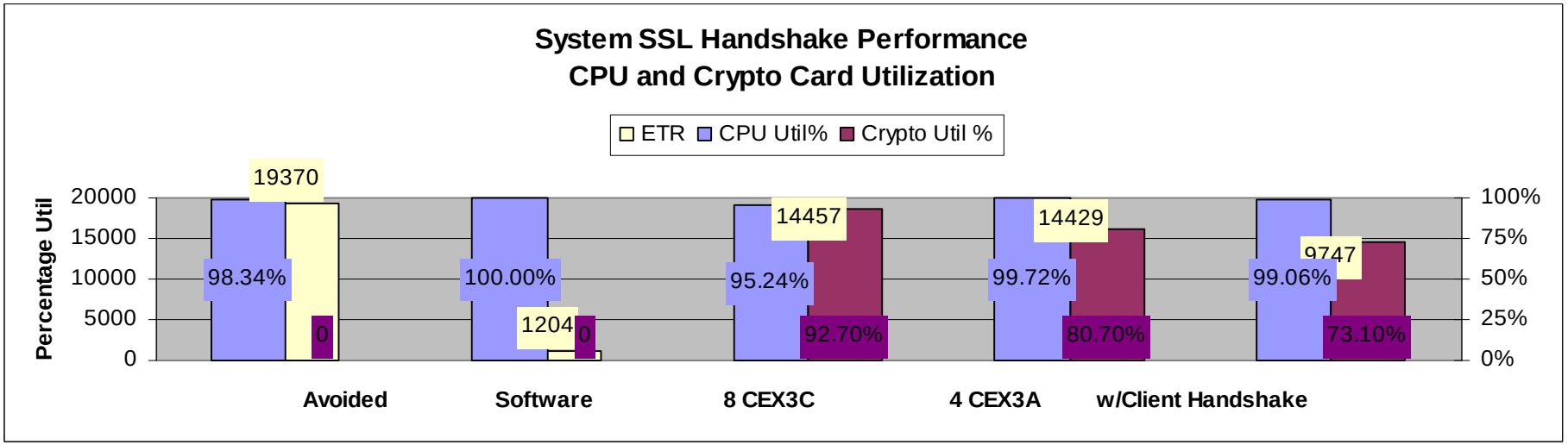


Caching SID/Client Authentication	Handshake	ETR	CPU Util%	Crypto Util %
100%/No	Avoided	24808	98.44%	NA
No/No	Software	1378	100.00%	NA
No/No	4 CEX4SC	9003	56.29%	99.40%
No/No	4 CEX4SA	17493	98.34%	87.80%
No/Yes	4 CEX4SA	11477	98.61%	79.10%



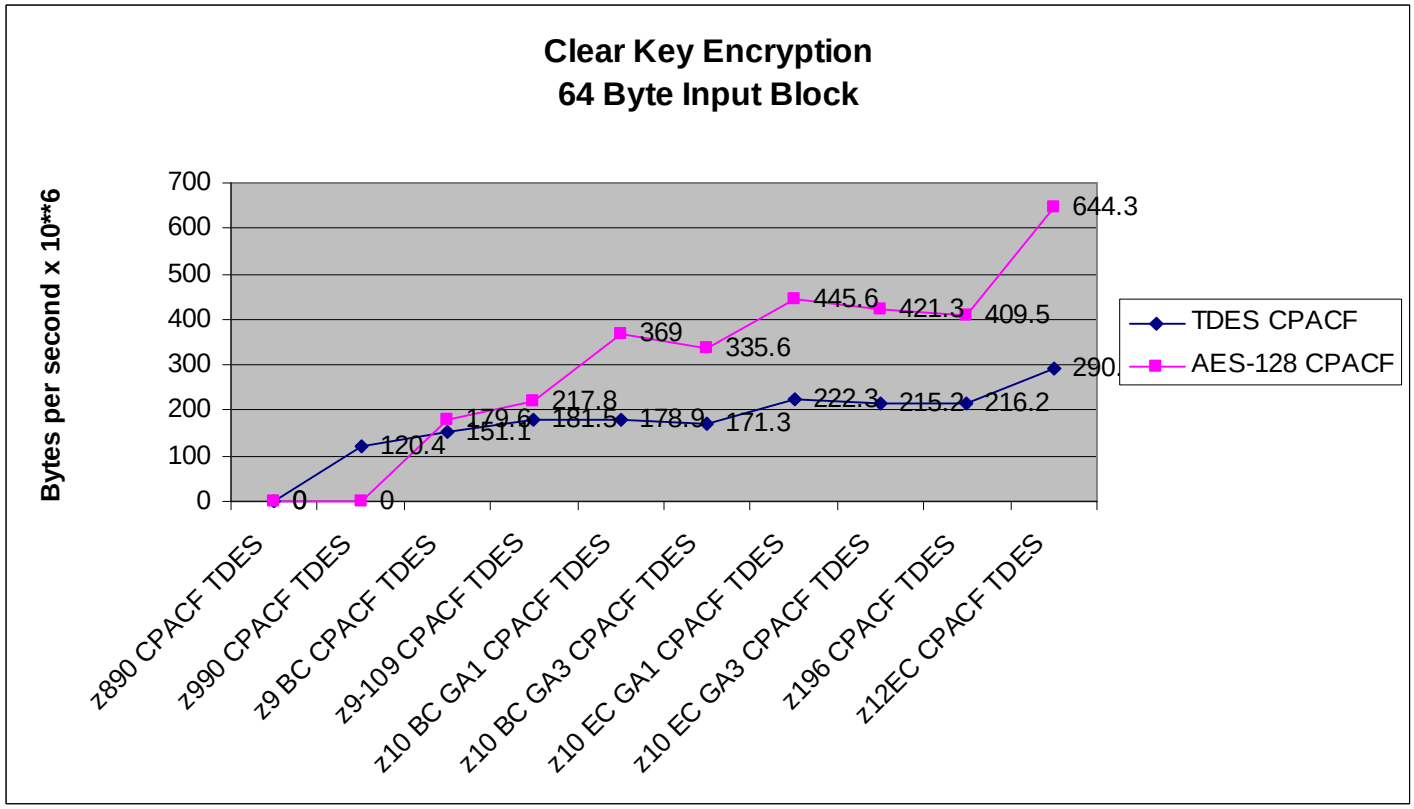
zEC12 HA1 – 4 CPs

System SSL Performance – z196

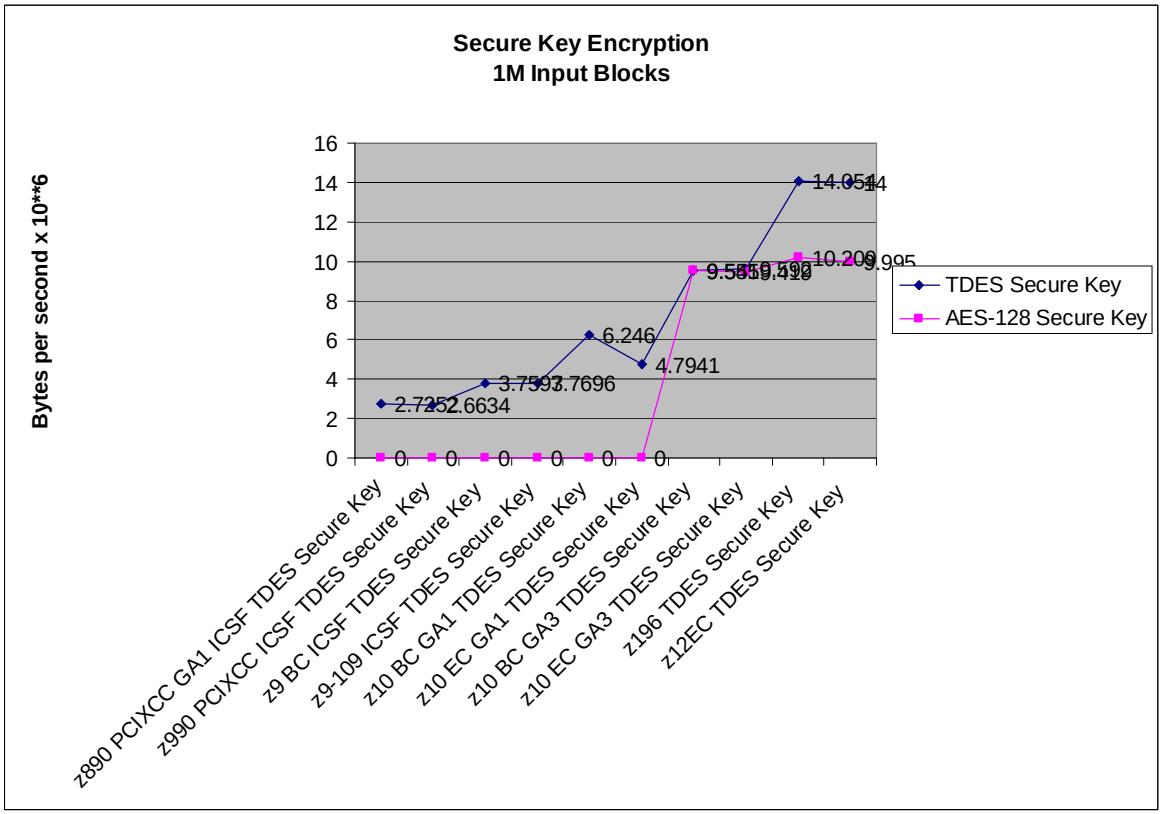


Caching SID	Handshake	ETR	CPU Util%	Crypto Util %
100%	Avoided	19370	98.34%	NA
No	Software	1204	100.00%	NA
No	8 CEX3C	14457	95.24%	92.70%
No	4CEX3A	14429	99.72%	80.70%
No	4 CEX3A	9747	99.06%	73.10%

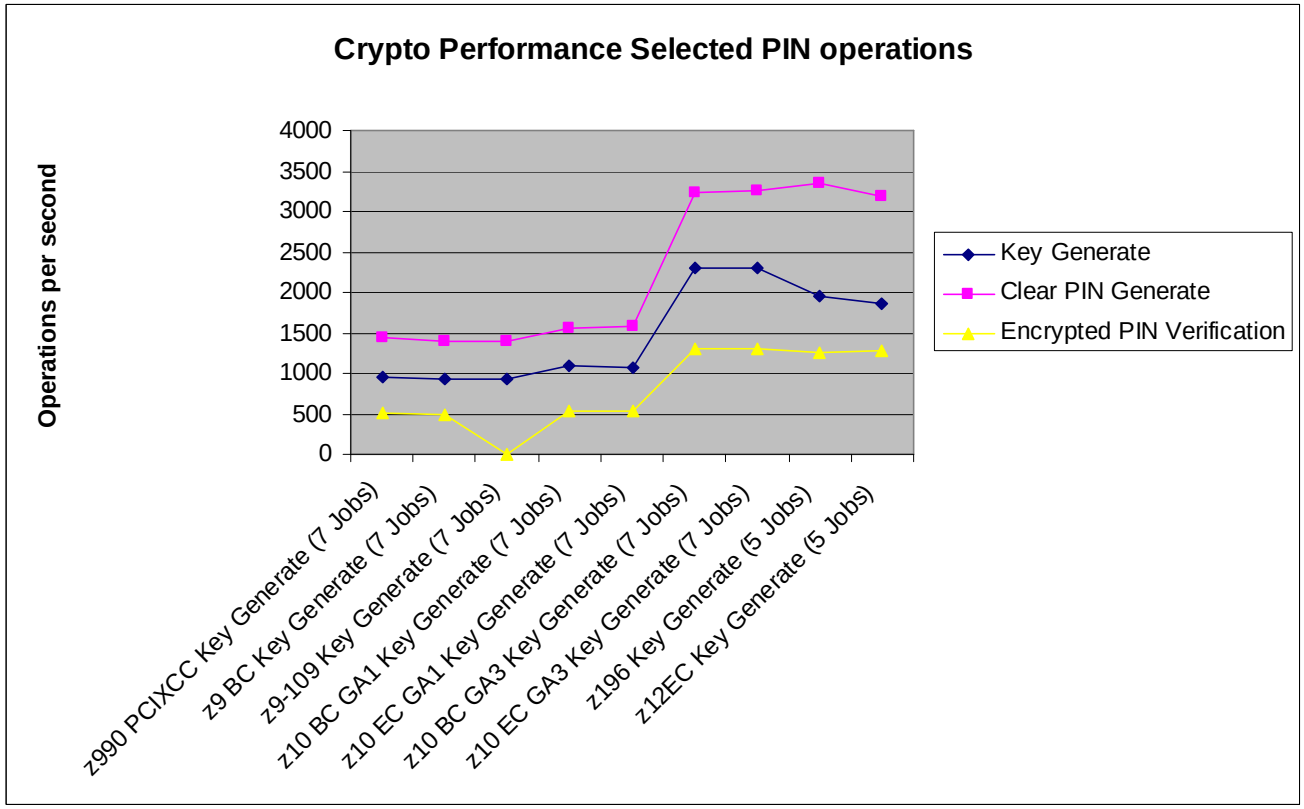
Crypto performance across CECs – Native Clear Key



Crypto performance across CECs – Secure Key



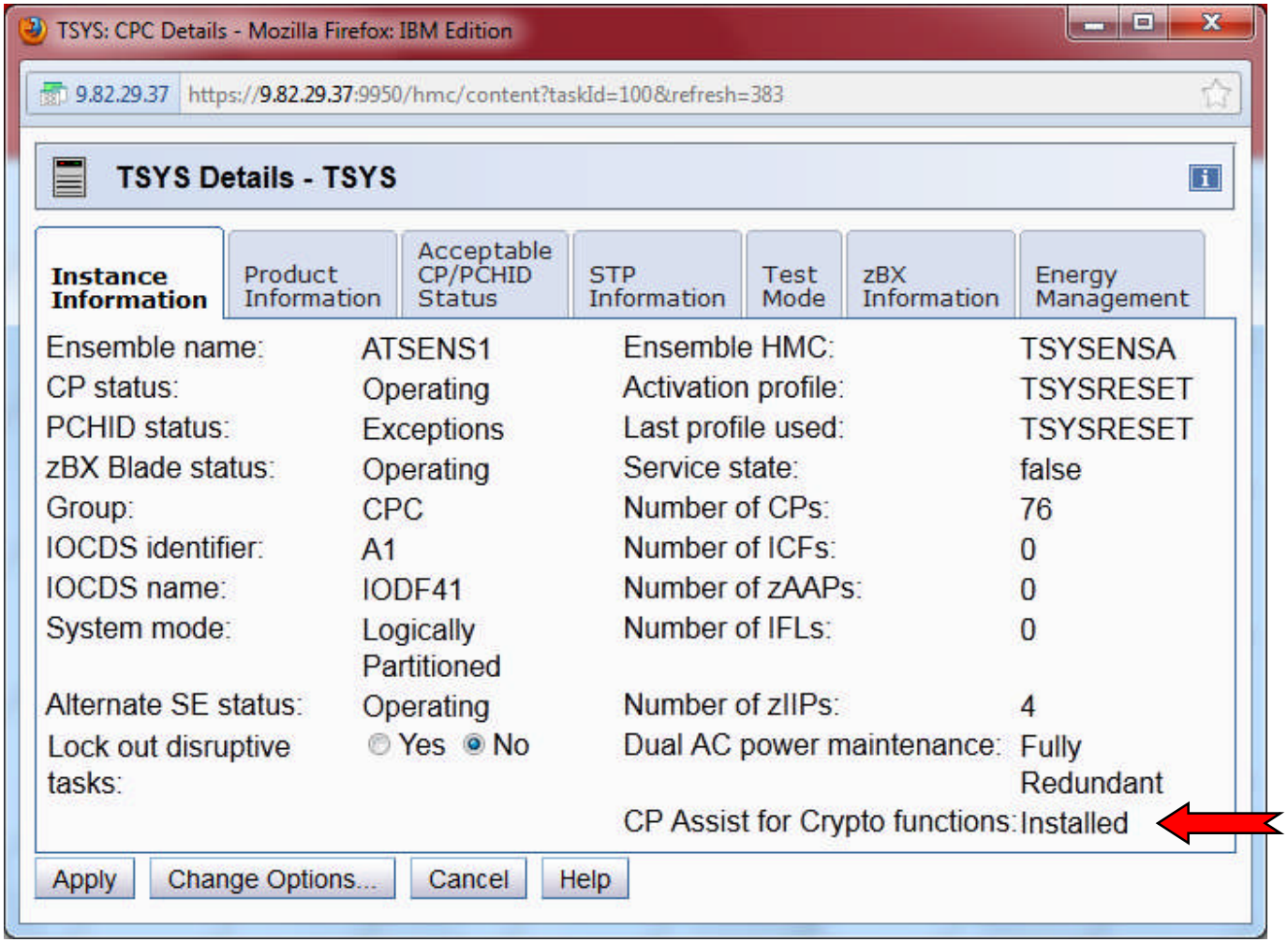
Crypto Performance across KEKs - PIN



ICSF Options - Performance Considerations

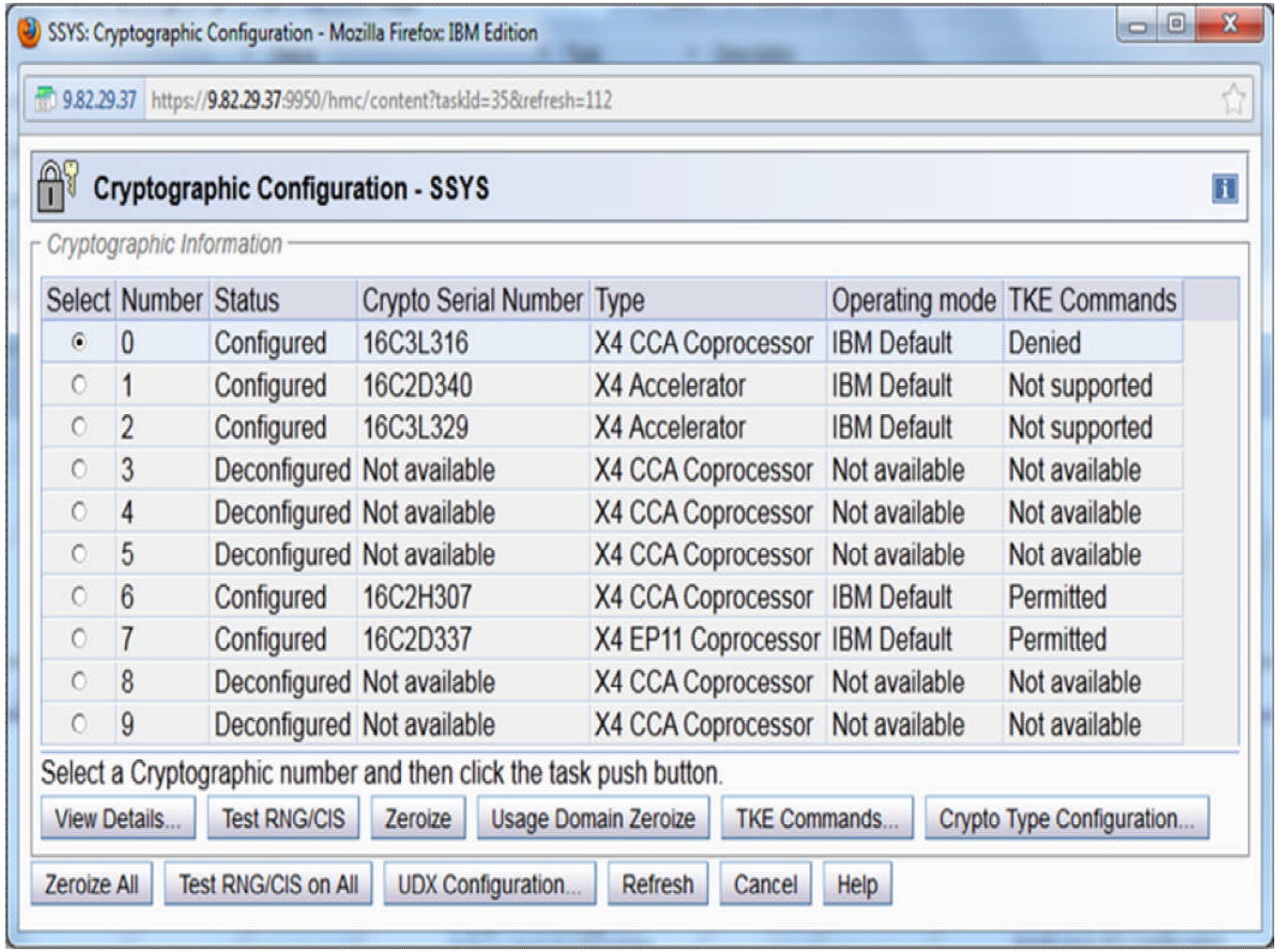
- **KEYAUTH(YES/NO) – check key integrity in memory**
- **CKTAUTH(YES/NO) – check key integrity on DASD**
- **CHECKAUTH(YES/NO) – skip SAF checks for Supervisor State or System Key callers**
- **SYSPLEXCKDS / SYSPLEXPKDS / SYSPLEXTKDS – enqueues and contention between systems**

Crypto Microcode Installed?



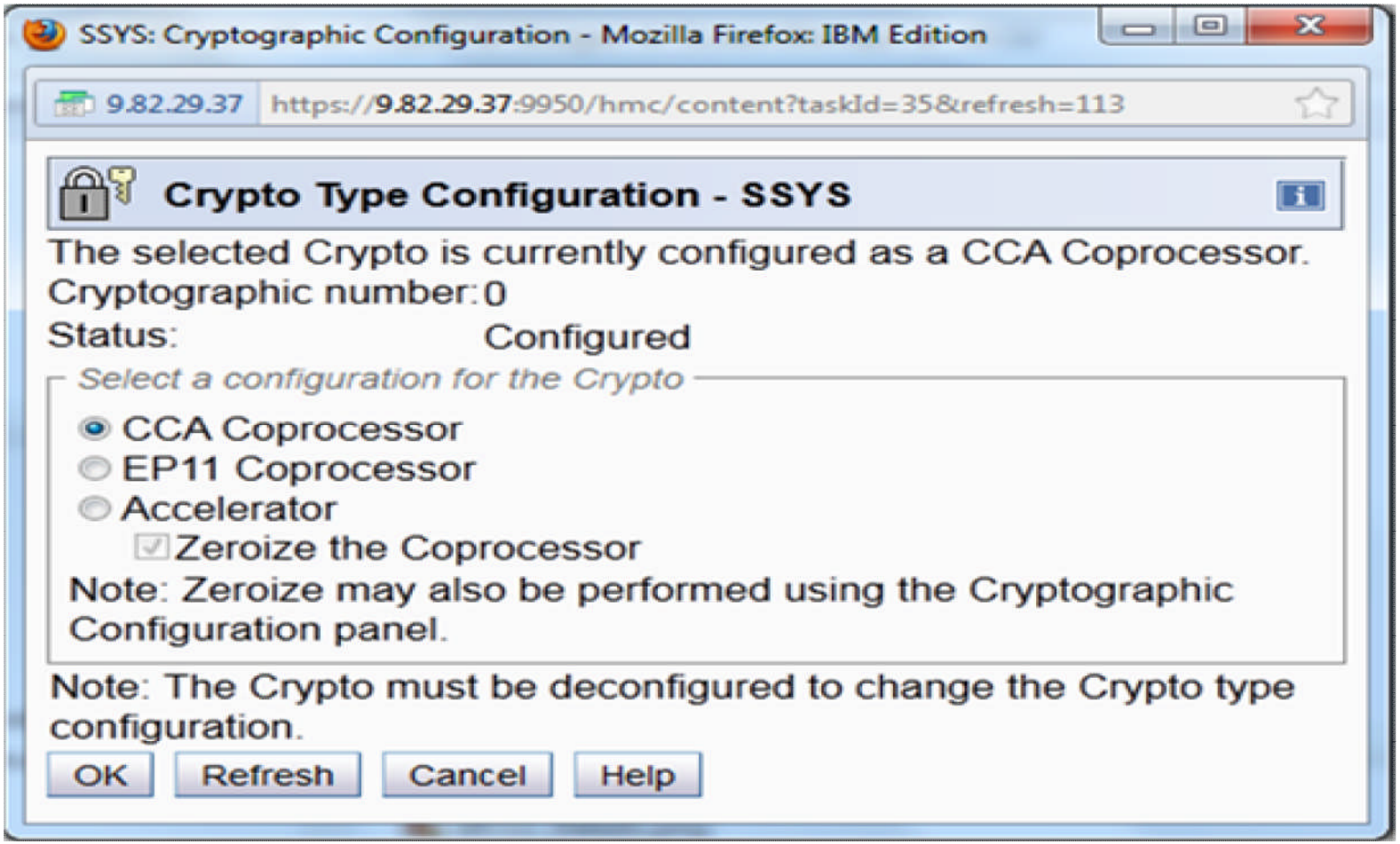
- **From the HMC, you must be in Single Object Mode, then look at the CPC Details**

PCI Configuration

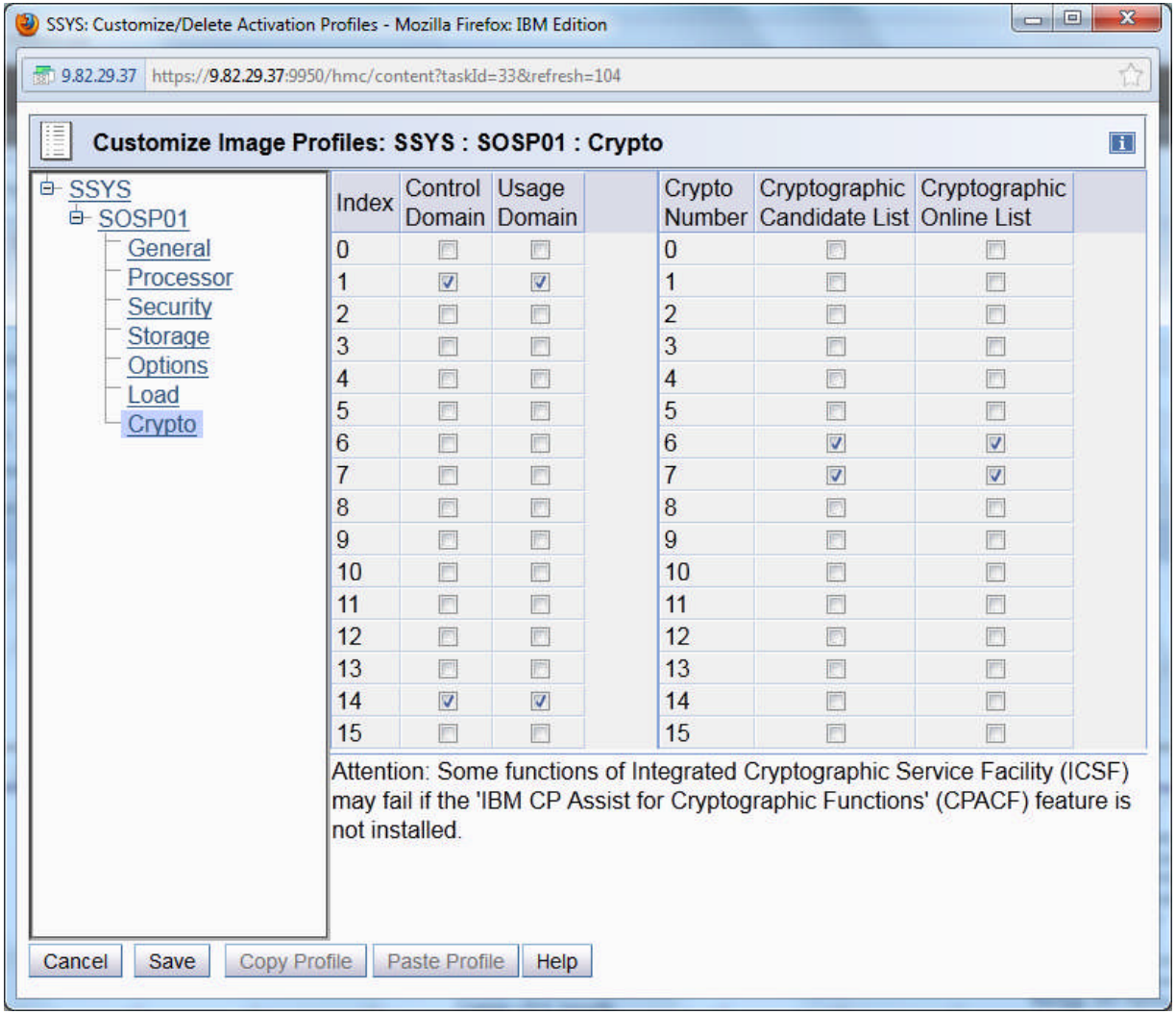


From CPC Operational Customization, click on View LPAR Cryptographic Controls

Reconfig



PCI Assignments



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, which ciphersuites – F GSKSRVR,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

CPU Measurement Facility

- **What is CPU MF?**
  - z10 and later facility that provides cache and memory hierarchy counters
  - 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)
- **How can the COUNTERS be used today?**
  - For performance analysis
  - Supplement current performance data from SMF, RMF, DB2, CICS, etc.
  - Measure (count) CPACF Usage

Counter #	Counter	Counter #	Counter
64	PRNG function count	72	DEA function count
65	PRNG cycle count	73	DEA cycle count
66	PRNG blocked function count	74	DEA blocked function count
67	PRNG 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**

See “A Synopsis of System z Crypto Hardware” by Greg Boyd **WP100810**
http://www.ibm.com/support/techdocs

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**

SMF Type 82 – ICSF Record (cont.)

- Subtype 10 – when clear key part entered for PKA-MK
- 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**

SMF Type 82 – ICSF Record (cont.)

- Subtype 17 – periodically to provide some indication of PCI Cryptographic Coprocessor usage
- **Subtype 18 – Cryptographic Processor Configuration**
- **Subtype 19 – PCI X Cryptographic Coprocessor Timing**
- **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**

SMF Type 82 – ICSF Record (cont.)

- **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

- **Formats the SMF Type 82 records into a readable report**
  - Sample Job, CSFSMFJ to
    - Capture the Type 82 records (with IFASMFDP)
    - Sort the records
    - Execute CSFMFR, via Batch TSO
  - Output may be large – multiple lines per Type 82 record
  - It's more readable than the raw SMF record, but …

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, more than performance**

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 2048-bit-ME
    - 1024-bit-CRT 2048-bit-CRT
    - 4096-bit-ME 4096-bit CRT

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

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 V1R13 SYSTEM ID TRX2 START 09/28/2011-08.15.00 INTERVAL 007.14.59

RPT VERSION V1R13 RMF END 09/28/2011-15.30.00 CYCLE 1.000 SECONDS

-------- CRYPTOGRAPHIC 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

-------- 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

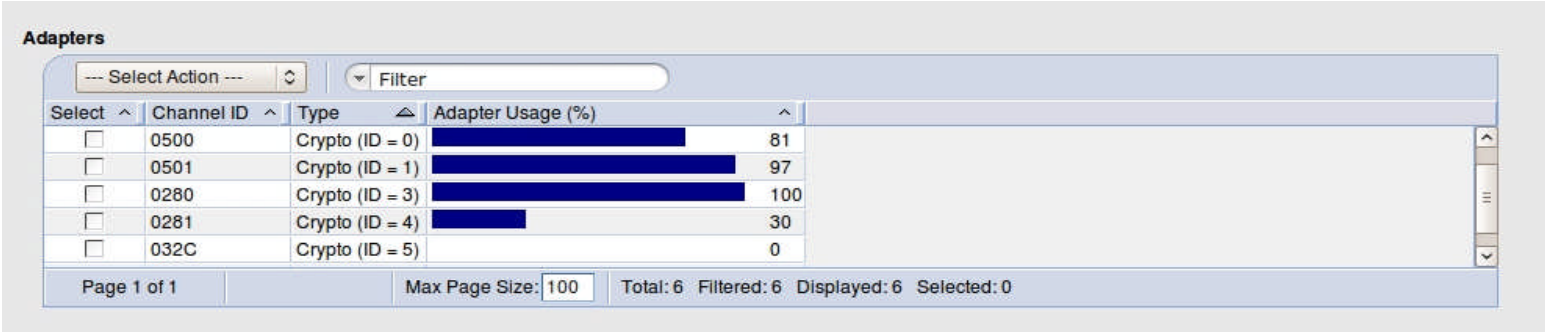
-------- ICSF SERVICES ----------

	---- 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		

Crypto Function Integration (Monitors Dashboard Support)

- The Monitors Dashboard on the HMC and SE was enhanced with a new Adapters table for zHelix.
- The Crypto Utilization percentage is displayed on the Monitors Dashboard according to the pchid number. The associated crypto number (AP Number) for this pchid is also shown in the table.
- 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

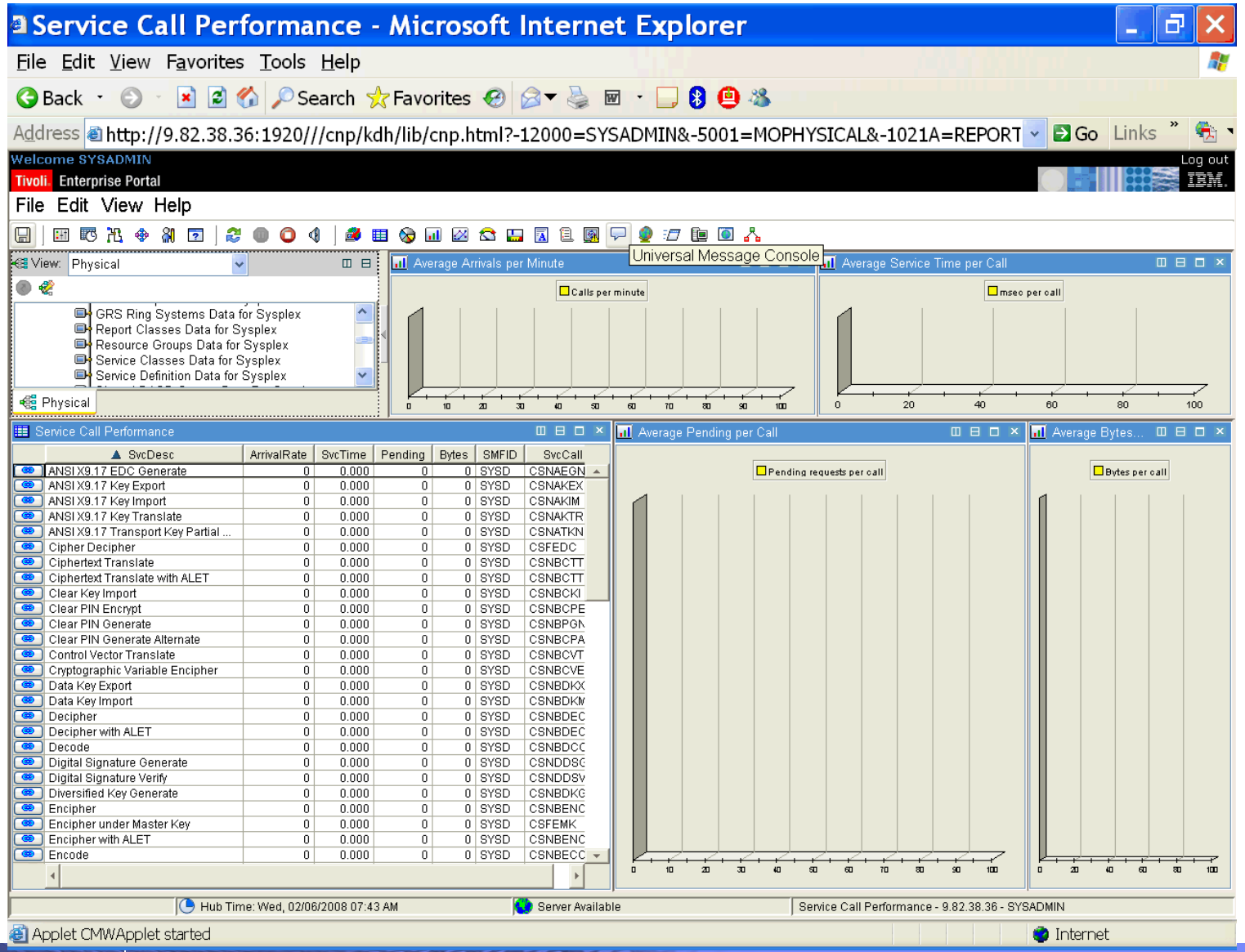
–Crypto Using and Delay Samples

- 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

SMF Type 30 - Common Address Space Work

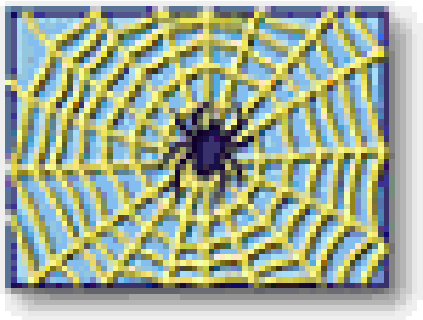
- **SMF30CSC – ICSF Service Count**
  - **CSNBENC (Single-DES) - # of service calls, # of bytes, # of CMD instructions**
  - **CSNBENC (Double & Triple-DES) - # of service calls, # of bytes, # of CMD instructions**
  - **CSNBDEC (Single-DES) - # of service calls, # of bytes, # of CMD instructions**
  - **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



IBM Redbooks & Manuals

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



Crypto Performance Whitepapers

- **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***
    - ***COUNTERS and an update on SAMPLING - HIS report tool and STG Lab Services***
- **Redpaper *Setting Up and Using System z CPU Measurement Facility with z/OS***
  - **http://www.redbooks.ibm.com/redpieces/pdfs/redp4727.pdf**

Questions …

IBM Advanced Technical Support – Washington Systems Center

Time for…

QR Code – Share 14668

- **Anaheim, CA**
- **March, 2014**

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

AlphaBlox*	GDPS*	RACF*	Tivoli*
APPN*	HiperSockets	Redbooks*	Tivoli Storage Manager
CICS*	HyperSwap	Resource Link	TotalStorage*
CICS/VSE*	IBM*	RETAIN*	VSE/ESA
Cool Blue	IBM eServer	REXX	VTAM*
DB2*	IBM logo*	RMF	WebSphere*
DFSMS	IMS	S/390*	zEnterprise
DFSMShsm	Language Environment*	Scalable Architecture for Financial Reporting	xSeries*
DFSMSrmm	Lotus*	Sysplex Timer*	z9*
DirMaint	Large System Performance Reference™ (LSPR™)	Systems Director Active Energy Manager	z10
DRDA*	Multiprise*	System/370	z10 BC
DS6000	MVS	System p*	z10 EC
DS8000	OMEGAMON*	System Storage	z/Architecture*
ECKD	Parallel Sysplex*	System x*	z/OS*
ESCON*	Performance Toolkit for VM	System z	z/VM*
FICON*	PowerPC*	System z9*	z/VSE
FlashCopy*	PR/SM	System z10	zSeries*
* Registered trademarks of IBM Corporation	Processor Resource/Systems Manager		

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

