

IBM Americas, ATS, Washington Systems Center

Crypto Performance Update Share 14668 Anaheim, CA March, 2014

Greg Boyd (boydg@us.ibm.com)

© 2014 IBM Corporation





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

Crypto Performance Update





Clear Key / Secure Key / Protected Key

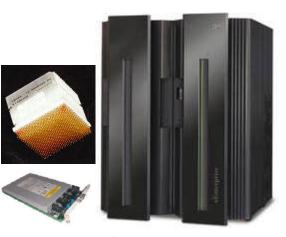
- Clear Key key <u>may</u> be in the clear, at least briefly, somewhere in the environment
- Secure Key key value does not exist in the clear outside of the HSM (secure, tamperresistant boundary of the card)
- Protected Key key value does not exist outside of physical hardware, although the hardware 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

Crypto Performance Update

March, 2014

© 2014 IBM Corporation

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

Page 7

March, 2014

© 2014 IBM Corporation



PCI Cards

Secure Coprocessor (default)

- -Requires master key be loaded
- -Data confidentiality
- -Data integrity
- -Financial functions
- -Key generation/manipulation
- -RSA public key operations

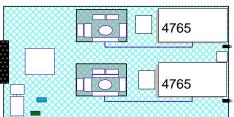
Accelerator

-RSA public key operations

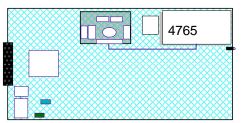
Enterprise PKCS #11

-PKCS #11 secure key

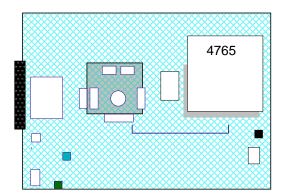




CEX3-1P



CEX4S

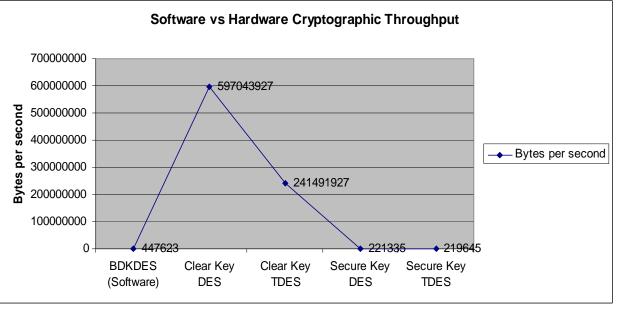


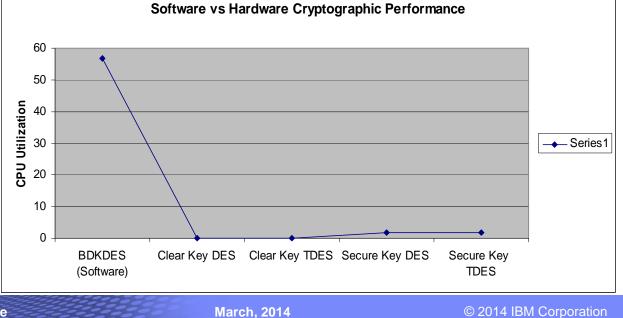


Software vs Hardware Encryption

	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/supp ort/techdocs/atsmastr.nsf /WebIndex/WP101240



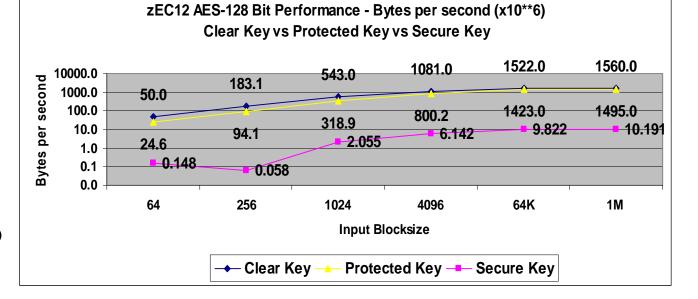


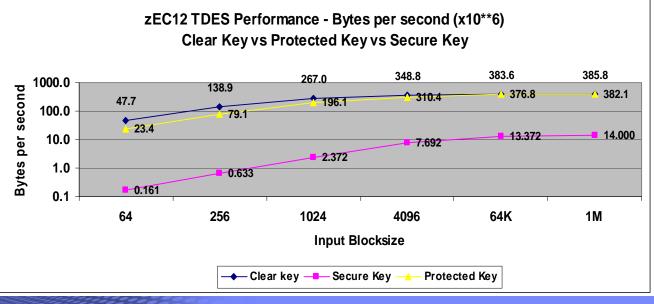


zEC12 Symmetric Key Performance

 From the Crypto Performance whitepaper at

http://www.ibm.co m/systems/z/adv antages/security/ zec12cryptograp hy.html

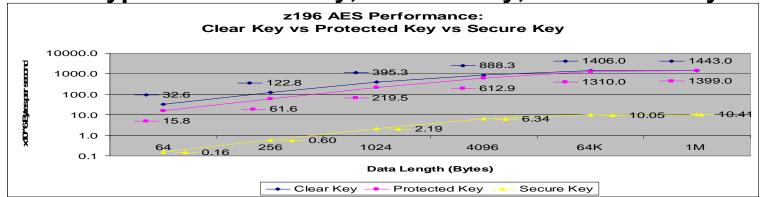




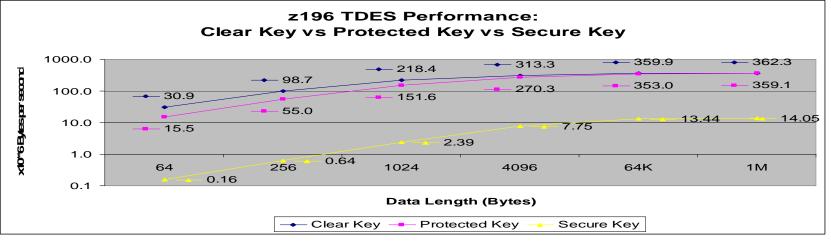


z196 Crypto Performance

• AES Encryption – Clear Key, Secure Key, Protected Key

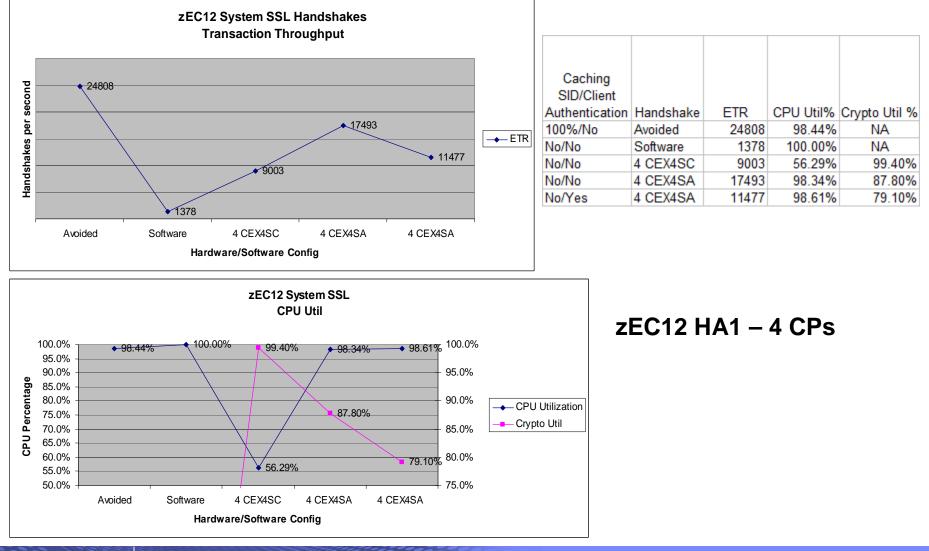


TDES Encryption – Clear Key, Secure Key, Protected Key



_	-	_	_	-	ł
			_		
	-			-	
_					

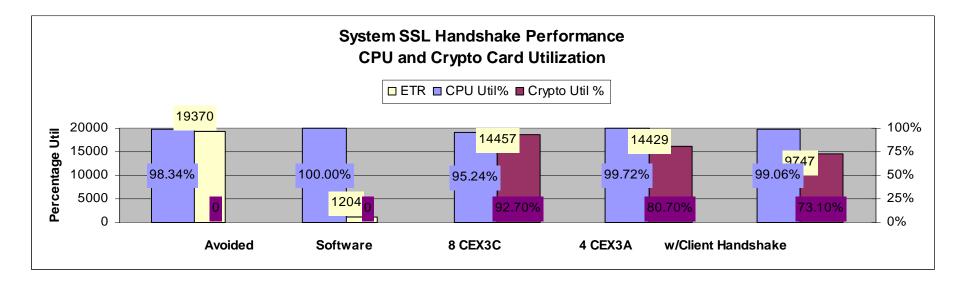
System SSL Performance – zEC12



March, 2014



System SSL Performance – z196

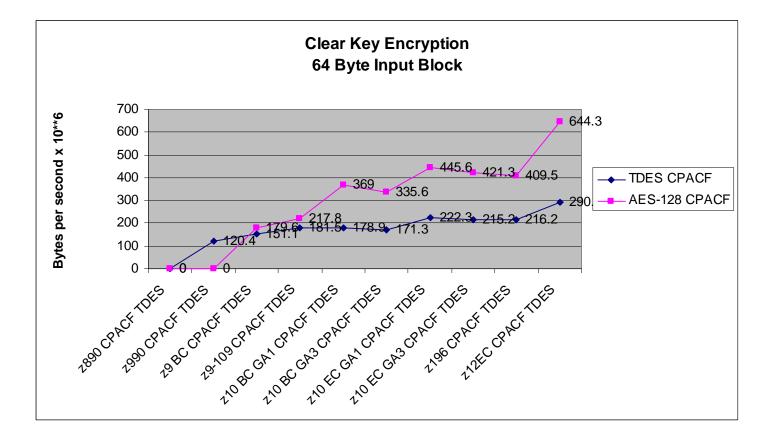


Caching				Crypto Util
SID	Handshake	ETR	CPU Util%	%
100%	Avoided	19370	98.34%	NA
No	Software	1204	100.00%	NA
No	8 CEX3C	14457	95.24%	92.70%
No	4CEX3A	14429	99.72%	80.70%
No	4 CEX3A	9747	99.06%	73.10%

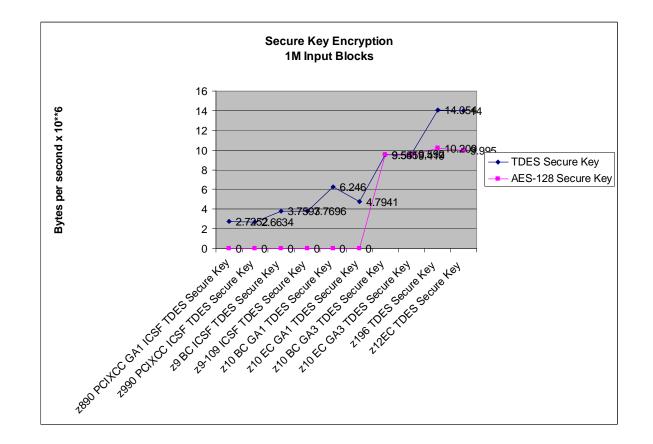
March, 2014



Crypto performance across CECs – Native Clear Key

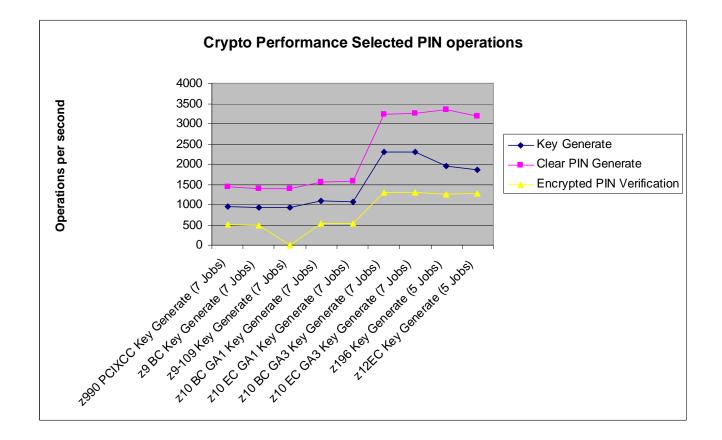


Crypto performance across CECs – Secure Key





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?

TSYS Det	tails - TSYS	1				<u>i</u>
	Product Information	Acceptable CP/PCHID Status	STP Information	Test Mode	zBX Information	Energy Management
Ensemble nam	e: AT	SENS1	Ensemble	HMC:		TSYSENSA
CP status:	Op	perating	Activation	profile:		TSYSRESET
PCHID status:	Ex	ceptions	Last profi	le used:		TSYSRESET
BX Blade stat	us: Op	perating	Service s	tate:		false
Group:		PC O	Number of	of CPs:		76
OCDS identifie	er: A1		Number o	of ICFs:		0
OCDS name:	10	DF41	Number of	f zAAPs	5:	0
System mode:		gically artitioned	Number of	of IFLs:		0
Alternate SE st	Section Stars	perating	Number of	of zIIPs:		4
ock out disrup		Yes No	Dual AC	ower m	aintenance:	Fully
asks:	amaa 76 000		04/00/00/00/00/00/00/00/00/00/00/00/00/0			Redundant

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

Crypto Performance Update

March, 2014



PCI Configuration

🛛 🏹	yptogra	ohic Configura	ation - SSYS			H
Cryptog	raphic Info	ormation ——				
Select	Number	Status	Crypto Serial Number	Туре	Operating mode	TKE Commands
۲	0	Configured	16C3L316	X4 CCA Coprocessor		Denied
0	1	Configured	16C2D340	X4 Accelerator	IBM Default	Not supported
0	2	Configured	16C3L329	X4 Accelerator	IBM Default	Not supported
0	3	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available
0	4	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available
0	5	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available
0	6	Configured	16C2H307	X4 CCA Coprocessor	IBM Default	Permitted
0	7	Configured	16C2D337	X4 EP11 Coprocessor	IBM Default	Permitted
0	8		Not available	X4 CCA Coprocessor		Not available
0	9		Not available	X4 CCA Coprocessor		Not available

From CPC Operational Customization, click on View LPAR Cryptographic Controls



Reconfig

🥹 SSYS: Cryptographic Configuration - Mozilla Firefox: IBM Edition 📃 💷 🔀					
9.82.29.37 https://9.82.29.37:9950/hmc/content?taskId=35&refresh=113					
Crypto Type Configuration - SSYS					
The selected Crypto is currently configured as a CCA Coprocessor. Cryptographic number:0					
Status: Configured Configuration for the Crypto					
 CCA Coprocessor EP11 Coprocessor Accelerator 					
Zeroize the Coprocessor Note: Zeroize may also be performed using the Cryptographic Configuration panel.					
Note: The Crypto must be deconfigured to change the Crypto type configuration. OK Refresh Cancel Help					



PCI Assignments

<u>S</u> OSP01	Index	Control Domain	Usage Domain	Crypto Number	Cryptographic Candidate List	
General	0	Ē	177	0		
rocessor	1	V	V	1	E	
Security	2			2		
torage	3		E	3		
Options	4	Ē	(FT)	4		
oad Crypto	5	177	100	5	P	
stypto	6			6	V	
	7			7		
	8	Ē	(177)	8		
	9	177	10	9	E	
	10			10		
	11			11		
	12	E		12		
	13			13		
	14	V	V	14		
	15			15		

		- · ·	
_	_	-	
-	-	-	
	_	_	
		- 10 C	

Are your Master Keys loaded and correct?

	Serial						
CoProcessor	Number	Status	AES	DES	ECC	RSA	P11
G01	0000001	ONLINE	U	U	C	U	
G02	00000002	ACTIVE	A	U	A	Е	
G03	0000003	ACTIVE	A	U	A	C	
Н07		ACTIVE					
SC06	00000006	ACTIVE	A	U	A	C	
SP07	0000008	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
PRNG function count	72	DEA function count
PRNG cycle count	73	DEA cycle count
PRNG blocked function count	74	DEA blocked function count
PRNG blocked cycle count	75	DEA blocked cycle count
SHA function count	76	AES function count
SHA cycle count	77	AES cycle count
SHA blocked function count	78	AES blocked function count
SHA blocked cycle count	79	AES blocked cycle count
	PRNG function count PRNG cycle count PRNG blocked function count PRNG blocked cycle count SHA function count SHA cycle count SHA blocked function count	PRNG function count72PRNG cycle count73PRNG blocked function count74PRNG blocked cycle count75SHA function count76SHA cycle count77SHA blocked function count78



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

*** Z ***	10 Summa	ary - CR TOTAL	YPTO for	Cour all (nters IPUs	Info	rmation	***
PRNG C PRNG E SHA FU SHA C SHA C SHA B DEA FU DEA C DEA B DEA B AES FU AES B	Blocked unction ycle Cou locked (unction ycle Cou locked (unction ycle Cou locked (Sunt Function Cycle Co Count function Cycle Cou Count Function Cycle Cou Count Count	Cour unt Cour unt Cour unt	nt nt		332	592.	0/Sec 0/Sec 73/Sec 47/Sec 0/Sec 0/Sec 24/Sec 0/Sec 0/Sec 0/Sec 0/Sec 0/Sec 0/Sec 0/Sec
***		CRYPTO	D BUS	SY SU	MARY	,		***
PRNG SHA DEA AES	Crypto	Busy: Busy: Busy: Busy:	0.00)% – 5% –	for for	the 3 the 3 the 3 the 3	CPUS CPUS	
Total	Crypto	Busy:	2.55	5% -	for	the 3	CPUS	

This information may be useful in determining:

• A count of <u>How Many CPACF encryption</u> <u>functions were executed</u>

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 <u>other Crypto functions may be executing in software</u> <u>and/or on Crypto Express Cards</u> (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

March, 2014

		_		
	-	_	-	_
		_	_	_
_	_			

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

_		_	
			States and Address Taxable
	_	<u> </u>	
			-
		_	
_	_		

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

IKM	_	_	-	
	-	_	_	
		-		

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

Page 30

March, 2014



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

_	_	_		-
	_	_		
			1	
			-	
		_		

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

IBM ATS, Washington Systems Center

RMF Crypto Hardware Activity Report

CRYPTOHARDWAREACTIVITY

PAGE 1

z/OS V1R13 SYSTEM ID TRX2

RPT VERSION V1R13 RMF

START 09/28/2011-08.15.00 INTERVAL 007.14.59 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						
CRYP1	OGRAPHIC ACCELERATOR							
	TOTAL	ME-FORMAT RSA OPERATIONS CRT-FORMAT RSA OPERATIONS						
TYPE ID	RATE EXEC TIME UTIL% KE	EY RATE EXEC TIME UTIL% RATE EXEC TIME UTIL%						
CEX2A 3	766.9 0.434 33.3 102	24 362.4 0.521 18.9 369.5 0.183 6.8						
	20	048 0.00 0.000 0.0 34.99 2.175 7.6						
CEX3A 5	998.9 0.365 36.5 102	24 246.4 0.534 13.2 554.3 0.205 11.3						
	20	048 0.00 0.000 0.0 83.16 0.689 5.7						
	40	96 0.00 0.000 0.0 115.1 0.547 6.3						
ICSF S	ICSF SERVICES							
	ENCRYPTION	DECRYPTION MAC HASH PIN PIN						
	SDES TDES AES SD	ES 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 80	00.0 4400 189.5 4573 4400 105.0 48.00 48.00						
1000								





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

Sel	ect Action	ᅌ 🤄 👻 Filter			
Select ^	Channel ID ^	Туре 🛆	Adapter Usage (%)	^]	
	0500	Crypto (ID = 0)		81	
	0501	Crypto (ID = 1)		97	
	0280	Crypto (ID = 3)		100	
	0281	Crypto (ID = 4)		30	
	032C	Crypto (ID = 5)		0	



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

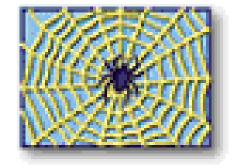
Omegamon

le Edit View Favorites Iools Help Back · O Favorites Iools Help Back · O Favorites Iools Help Back · O Favorites Favorites O F O Favorites O F O Favorites O F O Favorites O F O Favorites O Favori	Service Call Per	formance - Mi	crosoft Internet	Explorer			
Back Image: Source Strate of the source Strate							
Iddress @ http://j9.82.38.36:1920///cnp/kdh/lib/cnp.html?-12000=SYSADMIN&-5001=MOPHYSICAL&-1021A=REPORT © 0 0 ink * Increase VXADMIN Increase VXADMIN <td></td> <td></td> <td>vorites 🙆 🔍 🔭 📐 🕅</td> <td>. 🗆 🚯 🚯 😣</td> <td></td> <td></td> <td></td>			vorites 🙆 🔍 🔭 📐 🕅	. 🗆 🚯 🚯 😣			
All Enterprise PXADUIN Log Pall Enterprise PXADUIN Log E Edit View Help Image: Provide Image: Provide Image: Provide Image: Provid							
In Ederprise Portal Image: Service Translet	-	6:1920///cnp/kdh/lib	/cnp.html?-12000=SYSAD	MIN&-5001=MOPH	'SICAL&-1021A=	REPORT 👻 🖻	
le Edit View Help							
Image: State of a set of a							
Were Physical Universal Message Console Average Service Time per Call Image of the service Time per Call GRS Ring Systems Data for Sysplex B Report Classes Data for Sysplex Service Classes Data for Sysplex Service Classes Data for Sysplex Service Definition Data for Sysplex Service Definition Data for Sysplex Service Classes Data for Sysplex Service Translate Classer NR forentate Alter Control Vector Translate Control Vector Translate				🔺 - a 🕞 🔽 🖣			
Image: Construct of Sysplex Image: Construct of Sysplex Prystal Image: Construct of Sysplex Prystal Image: Construct of Sysplex Service Classes Data for Sysplex Image: Classes Data for Sysplex Service Classes Data for Sysplex Image: Classes Data for Sysplex Service Classes Data for Sysplex Image: Classes Data for Sysplex Service Classes Data for Sysplex Image: Classes Data for Sysplex Service Classes Data for Sysplex Image: Classes Data for Sysplex Service Classes Data for Sysplex Image: Classes Data for Sysplex Service Classes Data for Sysplex Image: Classes Data for Sysplex Service Classes Data for Sysplex Image: Classes Data for Sysplex Service Classes Data for Sysplex Image: Classes Data for Sysplex Service Data for Sysplex Image: Classes Data for Sysplex Service Data for Sysplex Image: Classes Data for Sysplex Service Data for Sysplex Image: Classes Data for Sysplex Service Data for Sysplex Image: Classes Data for Sysplex Service Data for Sysplex Image: Classes Data for Sysplex Ansity Si TK Rey Fond 0 Ansity Si TK Rey Import 0 0.000 0 <t< td=""><td></td><td></td><td></td><td>🕎 🖅 🛄 ២ 🏠 Iniversal Messade Consol</td><td>-</td><td></td><td></td></t<>				🕎 🖅 🛄 ២ 🏠 Iniversal Messade Consol	-		
GRS Ring Systems Data for Sysplex Converting Report Classes Data for Sysplex Converting Service Classes Data for Sysplex Converting Service Classes Data for Sysplex Converting Service Classes Data for Sysplex Converting Physical Converting Physical Converting Service Classes Data for Sysplex Converting Service Classes Data for Sysplex </td <td></td> <td></td> <td>werage Arrivals per Minute</td> <td></td> <td>Average Service Tin</td> <td>ne per Call</td> <td></td>			werage Arrivals per Minute		Average Service Tin	ne per Call	
Project Cases Data for Sysplex Service Clauses Data for Sysplex Service Clauses Data for Sysplex Service Clauses Data for Sysplex Physical Physical Physical Physical Association Data for Sysplex	• «		Calls per minut	e		msec per call	
Presource Groups Data for Sysplex Image: Classe Data for Sysplex Senice Classe Data for Sysplex Image: Classe Data for Sysplex Physical Image: Classe Data for Sysplex Image: Classe Data for Sysplex Physical Image: Classe Data for Sysplex Image: Classe Data for Sysplex Physical Image: Classe Data for Sysplex Image: Classe Data for Sysplex Senice Call Performance Image: Classe Data for Sysplex Image: Classe Data for Sysplex Image: Classe Data for Sysplex Average Pending per Call Image: Classe Data for Sysplex Average Pending per Call Image: Classe Data for Sysplex Average Pending per Call Image: Classe Data for Sysplex Average Pending per Call Image: Classe Data for Sysplex Image:							
Service Definition Data for Sysplex Image: Control of the system Control of the system <th< td=""><td>Resource Groups Data for</td><td>Sysplex 🥮</td><td></td><td></td><td></td><td></td><td></td></th<>	Resource Groups Data for	Sysplex 🥮					
Physical Image: Control of the state of the							
Service Call Performance III Average Pending per Call III Average Eytes III ANSIX 0.17 EDC Generate 0 0.000 0 0.5%D CSINAECK III IIII IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII							
A Sv2Desc ArrivalRate SvCTime Pending Bytes SWFID SvcCall A MSIX 917 EDC Generate 0 0.000 0 0 SYSD CSNA4EX A MSIX 917 Key Expont 0 0.000 0 SYSD CSNA4EX A MSIX 917 Key Expont 0 0.000 0 SYSD CSNA4EX A MSIX 917 Key Translate 0 0.000 0 SYSD CSNA4EX A MSIX 917 Key Translate 0 0.000 0 SYSD CSNA4EX Ciphert Draipher 0 0.000 0 SYSD CSNAEX Ciphert Translate 0 0.000 0 SYSD CSNBCPE Ciear PIN Generate 0 0.000 0 SYSD CSNBCPE Cortol Vector Translate 0 0.000 0 SYSD CSNBCPE Detaiker Import 0 0.000 0 SYSD CSNBCPE							
ANSI X3 17 EDC Generate 0 0.000 0 0 SYSD CSNAKEX ANSI X3 17 Key Export 0 0.000 0 0 SYSD CSNAKEX ANSI X3 17 Key Import 0 0.000 0 0 SYSD CSNAKEX ANSI X3 17 Key Import 0 0.000 0 SYSD CSNAKEX ANSI X3 17 Key Import 0 0.000 0 SYSD CSNAKEX ANSI X3 17 Key Import 0 0.000 0 SYSD CSNAKEX ANSI X3 17 Key Import 0 0.000 0 SYSD CSNAKEX Cipher Decipher 0 0.000 0 SYSD CSNBCTT Ciphertext Translate 0 0.000 0 SYSD CSNBCVT Ciear PIN Generate 0 0.000 0 SYSD CSNBCVT Control Vector Translate 0 0.000 0 SYSD CSNBCVE Data Key Import 0 0.000 0 SYSD CSNBDCC Decipher 0				Average Pending per Call			erage Bytes 🔟 🖯 🗖
ANSI X9 17 Key Export 0 0.000 0 0 SYSD CSNAKEX ANSI X9 17 Key Import 0 0.000 0 0 SYSD CSNAKEX ANSI X9 17 Key Import 0 0.000 0 0 SYSD CSNAKEX Cipher Decipher 0 0.000 0 0 SYSD CSNAKEX Cipher Ext Translate 0 0.000 0 0 SYSD CSNBCTT Cipher Ext Translate 0 0.000 0 0 SYSD CSNBCTT Cipher Ext Translate 0 0.000 0 0 SYSD CSNBCTT Ciear PIN Encypt 0 0.000 0 0 SYSD CSNBCPE Ciear PIN Generate 0 0.000 0 0 SYSD CSNBCPE Control Vector Translate 0 0.000 0 0 SYSD CSNBCPE Data Key Import 0 0.000 0 0 SYSD CSNBCPC Data Key Import 0 0.000 0 0 SYSD CSNBCPC Decipher 0							
ANSI X9 17 Key Import 0 0.000 0 0 SYSD CSNAKIN ANSI X9 17 Key Translate 0 0.000 0 0 SYSD CSNAKTR ANSI X9 17 Transport Key Partial 0 0.000 0 0 SYSD CSNAKTR Ciphertext Translate 0 0.000 0 0 SYSD CSNAKTR Ciphertext Translate 0 0.000 0 0 SYSD CSNACT Ciphertext Translate 0 0.000 0 0 SYSD CSNBCT Ciear PIN Generate 0 0.000 0 0 SYSD CSNBCVE Ciear PIN Generate 0 0.000 0 0 SYSD CSNBCVE Carlor Vector Translate 0 0.000 0 0 SYSD CSNBCVE Data Key Export 0 0.000 0 0 SYSD CSNBCVE Data Key Export 0 0.000 0 SYSD CSNBCVE Decipher 0 0.000 0 SYSD CSNBCVE Decipher 0 <td> ANSIX9.17 EDC Generate ANSIX9.17 Key Export </td> <td></td> <td></td> <td></td> <td>equests per call</td> <td></td> <td>Bytes per call</td>	 ANSIX9.17 EDC Generate ANSIX9.17 Key Export 				equests per call		Bytes per call
ANSIX9.17 Transport Key Partial 0 0.000 0 9 YSD CSNTKN Cipher Decipher 0 0.000 0 9 YSD CSNBCT Ciphertex Translate 0 0.000 0 9 YSD CSNBCT Ciphertex Translate with ALET 0 0.000 0 9 YSD CSNBCT Ciear PiN Encrypt 0 0.000 0 9 YSD CSNBCFE Ciear PiN Encrypt 0 0.000 0 9 YSD CSNBCFE Ciear PiN Generate Alternate 0 0.000 0 9 YSD CSNBCFE Ciear PiN Generate Alternate 0 0.000 0 9 YSD CSNBCFE Data Key Import 0 0.000 0 9 YSD CSNBCVE Data Key Import 0 0.000 0 9 YSD CSNBCKE Data Key Import 0 0.000 0 9 YSD CSNBCKE Decipher 0 0.000 0 9 YSD CSNBDCE Decipher 0	ANSI X9.17 Key Import			1		1	
Cipher Decipher 0 0.000 0 0 SYSD CSFEDC Ciphertex Translate 0 0.000 0 SYSD CSNBCTT Ciphertex Translate with ALET 0 0.000 0 SYSD CSNBCTT Clear Key Import 0 0.000 0 SYSD CSNBCTT Clear PIN Encrypt 0 0.000 0 SYSD CSNBCFA Clear PIN Generate 0 0.000 0 SYSD CSNBCFA Corntol Vector Translate 0 0.000 0 SYSD CSNBCVT Decipher 0 0.000 0 SYSD CSNBCVT Decipher 0 0.000 0 SYSD CSNBCVT Data Key Export 0 0.000 0 SYSD CSNBCVC Decipher 0 0.000 0 SYSD CSNBCC Decipher 0 0.000 0 SYSD CSNBCC Decipher 0 0.000 0 SYSD	ANSI X9.17 Key Translate						
Ciphertext Translate 0 0.000 0 9 SYSD CSNBCTT Ciphertext Translate with ALET 0 0.000 0 8 SYSD CSNBCTT Clear Key Import 0 0.000 0 8 SYSD CSNBCFT Clear FIN Generate 0 0.000 0 8 SYSD CSNBCFF Clear FIN Generate Alternate 0 0.000 0 8 SYSD CSNBCFA Clear FIN Generate Alternate 0 0.000 0 8 SYSD CSNBCFA Control Vector Translate 0 0.000 0 8 SYSD CSNBCFA Data Key Export 0 0.000 0 8 SYSD CSNBDKX Data Key Import 0 0.000 0 8 SYSD CSNBDKX Decipher 0 0.000 0 8 SYSD CSNBDCX Decipher 0 0.000 0 8 SYSD CSNBDKC Digital Signature Verify 0 0.000 0 8 SYSD CSNBDKC Encipher <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>							
Ciphertext Translate with ALET 0 0.000 0 SYSD CSNBCTT Clear Key Import 0 0.000 0 SYSD CSNBCFE Clear PIN Generate 0 0.000 0 SYSD CSNBCFE Clear PIN Generate 0 0.000 0 SYSD CSNBCFE Clear PIN Generate Alternate 0 0.000 0 SYSD CSNBCFE Control Vector Translate 0 0.000 0 SYSD CSNBCVE Data Key Export 0 0.000 0 SYSD CSNBDCC Decipher 0 0.000 0 SYSD CSNBDCC Decipher with ALET 0 0.000 0 SYSD CSNBDCC Decipher with ALET 0 0.000 0 SYSD CSNBDSC Digital Signature Generate 0 0.000 0 SYSD CSNBDSC Direcipher 0 0.000 0 SYSD CSNBDSC Encipher 0 0.0000 <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
Clear Key Import 0 0.000 0 SYSD CSNBCKI Clear PIN Encrypt 0 0.000 0 SYSD CSNBCFE Clear PIN Generate 0 0.000 0 SYSD CSNBCFA Clear PIN Generate Alternate 0 0.000 0 SYSD CSNBCFA Control Vector Translate 0 0.000 0 SYSD CSNBCVT Ontrol Vector Translate 0 0.000 0 SYSD CSNBCVT Data Key Import 0 0.000 0 SYSD CSNBDKV Data Key Import 0 0.000 0 SYSD CSNBDKV Decipher 0 0.000 0 SYSD CSNBDCC Decipher 0 0.000 0 SYSD CSNBDKV Decipher 0 0.000 0 SYSD CSNBDCC Digital Signature Generate 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0							
Clear PIN Encrypt 0 0.000 0 SYSD CSNBCPE Clear PIN Generate 0 0.000 0 SYSD CSNBCPA Clear PIN Generate Alternate 0 0.000 0 SYSD CSNBCVF Control Vector Translate 0 0.000 0 SYSD CSNBCVF Data Key Export 0 0.000 0 SYSD CSNBCVF Data Key Export 0 0.000 0 SYSD CSNBCVF Data Key Export 0 0.000 0 SYSD CSNBCVF Decipher 0 0.000 0 SYSD CSNBDCC Digital Signature Generate 0 0.000 0 SYSD CSNBDKC Distribut Key Generate 0 0.000 0							
Clear PIN Generate 0 0.000 0 SYSD CSNBPGN Clear PIN Generate Alternate 0 0.000 0 SYSD CSNBPGN Clear PIN Generate Alternate 0 0.000 0 SYSD CSNBPCH Control Vector Translate 0 0.000 0 SYSD CSNBCVF Data Key Export 0 0.000 0 SYSD CSNBDK/v Data Key Import 0 0.000 0 SYSD CSNBDK/v Decipher 0 0.000 0 SYSD CSNBDCC Decipher with ALET 0 0.000 0 SYSD CSNBDSV Digital Signature Generate 0 0.000 0 SYSD CSNBDSV Diversified Key Generate 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher 0 0.000							
Clear PIN Generate Alternate 0 0.000 0 SYSD CSNBCPA Control Vector Translate 0 0.000 0 SYSD CSNBCVT Cryptographic Variable Encipher 0 0.000 0 SYSD CSNBCVE Data Key Export 0 0.000 0 SYSD CSNBCVE Data Key Export 0 0.000 0 SYSD CSNBDKV Decipher 0 0.000 0 SYSD CSNBDKV Decipher with ALET 0 0.000 0 SYSD CSNBDCC Digital Signature Generate 0 0.000 0 SYSD CSNBDCC Digital Signature Verify 0 0.000 0 SYSD CSNBDKC Encipher 0 0.000 0 SYSD CSNBDKC Encipher 0 0.000 0 SYSD CSNBDKC Distribute Key Export 0 0.000 0 SYSD CSNBDKC Distrisfied Key Generate 0							
Control Vector Translate 0 0.000 0 SYSD CSNBCVT Cryptographic Variable Encipher 0 0.000 0 SYSD CSNBCVE Data Key Export 0 0.000 0 SYSD CSNBDKX Data Key Import 0 0.000 0 SYSD CSNBDKX Decipher 0 0.000 0 SYSD CSNBDCC Digital Signature Generate 0 0.000 0 SYSD CSNBDKC Dispital Signature Verify 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher under Master Key 0 0.000 0							
Cryptographic Variable Encipher 0 0.000 0 SYSD CSNBCVE Data Key Export 0 0.000 0 SYSD CSNBCVE Decipher 0 0.000 0 SYSD CSNBDCC Decipher with ALET 0 0.000 0 SYSD CSNDDSC Digital Signature Generate 0 0.000 0 SYSD CSNBDKC Dispital Signature Verify 0 0.000 0 SYSD CSNBDKC Dispital Signature Verify 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0							
Data Key Export 0 0.000 0 0 SYSD CSNBDKX Data Key Import 0 0.000 0 SYSD CSNBDKX Decipher 0 0.000 0 SYSD CSNBDKX Decipher 0 0.000 0 SYSD CSNBDC Decipher with ALET 0 0.000 0 SYSD CSNBDCC Decipher with ALET 0 0.000 0 SYSD CSNBDCC Digital Signature Generate 0 0.000 0 SYSD CSNBDKC Digital Signature Verify 0 0.000 0 SYSD CSNBDKC Digital Signature Verify 0 0.000 0 SYSD CSNBDKC Dispital Signature Verify 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 <	Cryptographic Variable Encipher						
Decipher 0 0.000 0 0 SYSD CSNBDEC Decipher with ALET 0 0.000 0 SYSD CSNBDCC Decipher with ALET 0 0.000 0 SYSD CSNBDCC Decode 0 0.000 0 SYSD CSNDDSC Digital Signature Generate 0 0.000 0 SYSD CSNDDSC Digital Signature Verify 0 0.000 0 SYSD CSNDDSC Dirersified Key Generate 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD	🛎 Data Key Export						
Decipher with ALET 0 0.000 0 SYSD CSNBDEC Decode 0 0.000 0 SYSD CSNBDCC Digital Signature Generate 0 0.000 0 SYSD CSNDDSC Digital Signature Verify 0 0.000 0 SYSD CSNDDSV Diversified Key Generate 0 0.000 0 SYSD CSNBDKC Encipher 0 0.000 0 SYSD CSNBENC Encipher under Master Key 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0	🔊 Data Key Import		0 0 SYSD CSNBDKM				
Decode 0 0.000 0 0 SYSD CSNBDCC Digital Signature Generate 0 0.000 0 0 SYSD CSNDDSC Digital Signature Verify 0 0.000 0 0 SYSD CSNDDSC Digital Signature Verify 0 0.000 0 0 SYSD CSNDDSC Disprisified Key Generate 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher under Master Key 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC	Decipher						
Digital Signature Generate 0 0.000 0 0 SYSD CSNDDSC Digital Signature Verify 0 0.000 0 0 SYSD CSNDDSV Dispital Signature Verify 0 0.000 0 SYSD CSNDDSV Dispital Signature Verify 0 0.000 0 SYSD CSNDDSV Dispital Signature Verify 0 0.000 0 SYSD CSNBDKC Encipher 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encode 0 0.000 0 SYSD CSNBENC							
Digital Signature Verify 0 0.000 0 0 SYSD CSNDDSv Diversified Key Generate 0 0.000 0 SYSD CSNBDKC Dincipher 0 0.000 0 SYSD CSNBENC Encipher under Master Key 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC							
Diversified Kay Generate 0 0.000 0 0 SYSD CSNBDKG Encipher 0 0.000 0 SYSD CSNBDNC Encipher under Master Key 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher 0 0.000 0 SYSD CSNBENC							
Encipher 0 0.000 0 0 SYSD CSNBENC Encipher under Master Key 0 0.000 0 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 0 SYSD CSNBENC D Encode 0 0.000 0 SYSD CSNBENC							
Encipher under Master Key 0 0.000 0 SYSD CSFEMK Encipher with ALET 0 0.000 0 SYSD CSNBENC Encipher with ALET 0 0.000 0 SYSD CSNBENC Encode 0 0.000 0 SYSD CSNBENC							
Encipher with ALET 0 0.000 0 0 SYSD CSNBENC Encode 0 0.000 0 0 SYSD CSNBENC							
	Encode						
	4	0.000		10 20 30 40 5	0 60 70 80	90 100 0	20 40 60 80 1
🕒 Hub Time: Wed, 02/06/2008 07:43 AM Server Available Service Call Performance - 9.82.38.36 - SYSADMIN		ne: Wed. 02/06/2008 07:43 AM	Server Available	Se	rvice Call Performance - 9	82.38.36 - SYSADMIN	
	10			, oc			have a h
Applet CMWApplet started	Applet CMWApplet started					🔰 🔤 In	lernet



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

March, 2014



CPU Measurement Facility Doc

IBM Research article

 "IBM System z10 performance improvements with software & hardware synergy"

-<u>http://www.research.ibm.com/journal/rd/531/jackson.pdf</u>

- 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

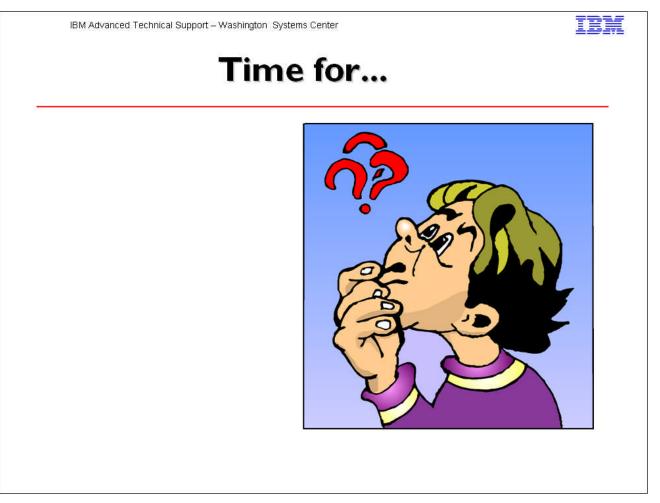
 COUNTERS and an update on SAMPLING - HIS report tool and STG Lab Services

 Redpaper Setting Up and Using System z CPU Measurement Facility with z/OS

-http://www.redbooks.ibm.com/redpieces/pdfs/redp4727.pdf



Questions ...





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.

March, 2014