



How System SSL Uses Crypto on System z

Greg Boyd

gregboyd@mainframecrypto.com

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
- Copyright © 2014 Greg Boyd, Mainframe Crypto, LLC. All rights reserved.
- All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. IBM, System z, zEnterprise and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.
- **THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY.** Greg Boyd and Mainframe Crypto, LLC assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Greg Boyd or Mainframe Crypto, LLC be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if expressly advised in advance of the possibility of such damages.

QR Code



- Share #15660

Agenda

- System SSL Basics
 - What is it?
 - How it works
- Crypto Hardware
- How do I tell what I'm using (hardware/software)?
- Performance (Reports and Expectations)
- Heartbleed

Secure Sockets Layer/Transport Layer Security

V#, Serial Number, CA's Signature
Signature Algorithm,
Issuer Name: Caxyz
Validity Date & Time
Subject Name: Greg
Subject's Public Key Signature
Algorithm: RSA with SHA-1
Extensions

- Communication protocol developed by Netscape to provide security on the internet
 - Establishes a communication session between a client and a server
 - Authenticates one or both parties
 - May provide security (encryption)
 - May provide data integrity



Two methods on z/OS

- System SSL
 - Component of z/OS, provides C/C++ callable APIs
 - Leverages crypto hardware and ICSF as appropriate
 - Primary implementation
- Java
 - Part of IBM SDK for z/OS, Java Technology Edition provides Java callable APIs
 - Leverages crypto hardware and ICSF ... maybe
 - Used by Java-based workloads running on z/OS

System SSL Security Level 3

z/OS Version	FMID
OS/390 R10; z/OS 1.1	JCPT2A1
z/OS 1.2; z/OS 1.3	JCPT321
z/OS 1.4; z/OS 1.5	JCPT341
z/OS 1.6; z/OS 1.7	JCPT361
z/OS 1.8	JCPT381
z/OS 1.9	JCPT391
z/OS 1.10	JCPT3A1
z/OS 1.11	JCPT3B1
z/OS 1.12	JCPT3C1
z/OS 1.13	JCPT3D1
z/OS 2.1	JCPT411

SSL/TLS : High Level Flow

Client

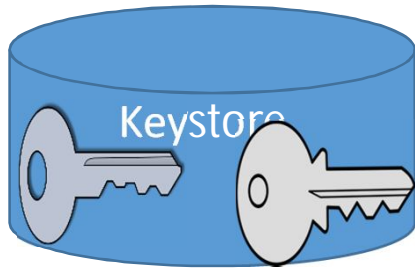
1. Initiates the communication session
2. Requests specific data to be provided by the Server
3. Usually via a browser but not always
4. May need to prove its identity by having a certificate

Server

1. Provides data at the client's request
2. Provides access based on its security environment
3. Usually an application responding to the request
4. Protects its identity via a certificate

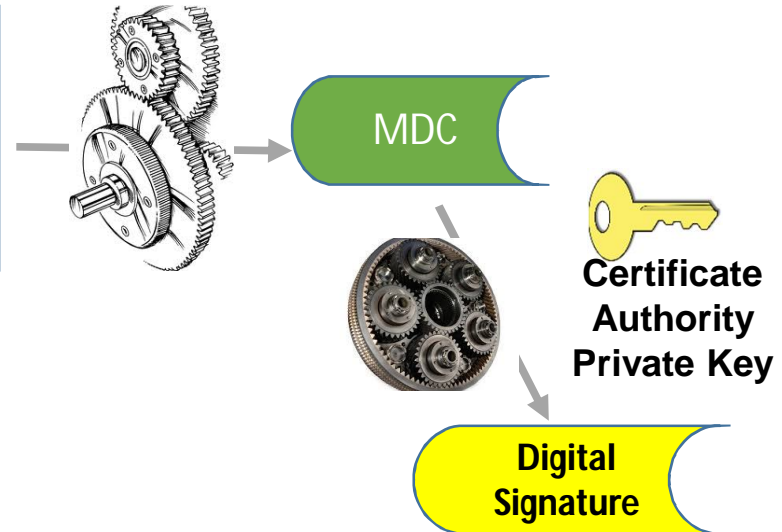
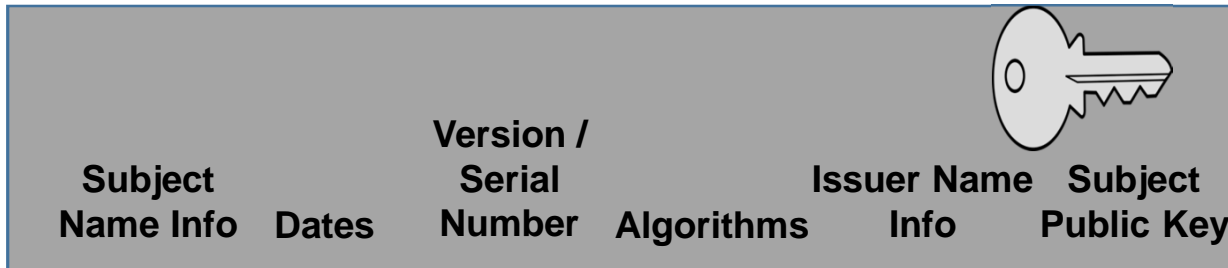
SSL/TLS Protocol

- Two phases
 - Handshake phase relies on certificates and public/private key algorithms to provide authentication
 - Signature Verification
 - Public key authentication
 - Record phase relies on symmetric algorithms and hashes to provide security and integrity
 - DES/TDES, AES, RC4, Blowfish ...
 - SHA1, SHA-2, MD5 ...

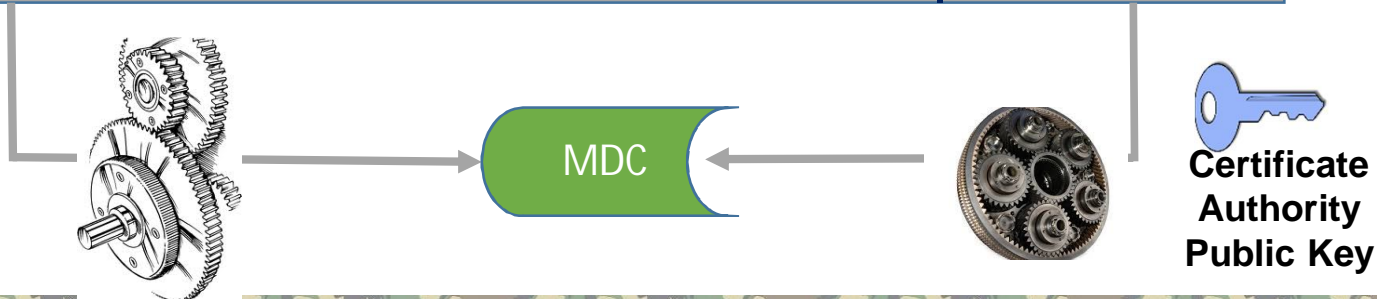
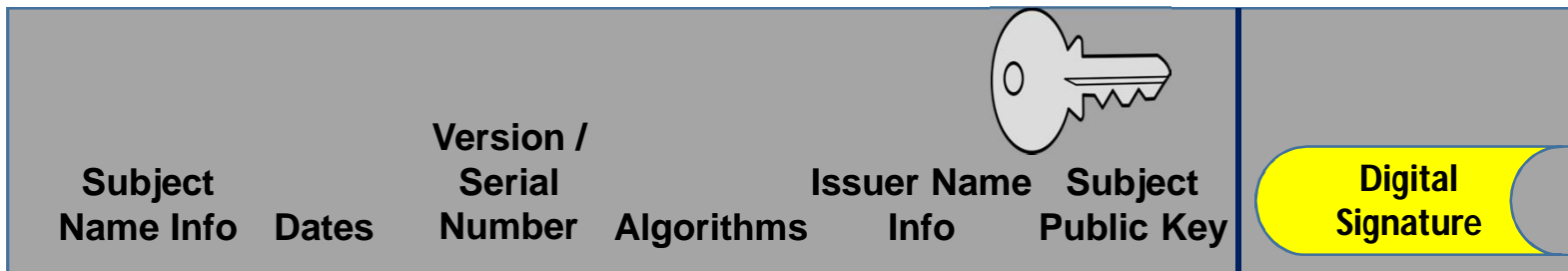


Digital Certificate

Certificate Request



Certificate



Why Both Asymmetric and Symmetric?

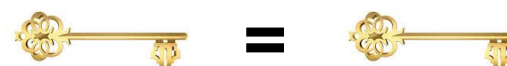
- Asymmetric

- + Can be used to establish a secret between two parties
- Performance impact



- Symmetric

- + Better performance
- Key distribution (key must be shared securely between the parties)



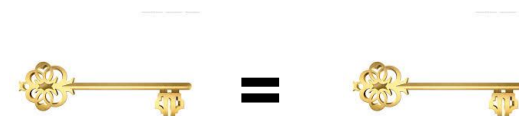
SSL & Crypto Devices

- Crypto Express4S (CEX4S); Crypto Express3 (CEX3)
 - Combines PCICA & PCIXCC in single feature
 - RSA asymmetric algorithms up to 4096-bit keys
 - ECC asymmetric algorithms
- Crypto Express2 (CEX2)
 - Combines PCICA & PCIXCC in single feature
 - RSA asymmetric algorithms up to 2048-bit keys
- PCIXCC, PCIX Cryptographic Coprocessor
 - RSA (2048-bit keys) asymmetric algorithms
- PCICA, PCI Cryptographic Accelerator
 - RSA (2048-bit keys) asymmetric algorithms



SSL & Crypto Devices ...

- CPACF, CP Assist for Cryptographic Functions
 - z890/z990
 - clear key encryption: DES/TDES
 - hash engine: SHA-1
 - z9
 - clear key encryption: DES/TDES and AES-128
 - hash engine: SHA-1, SHA-256
 - z10/z196/z114/zEC12
 - clear key encryption: DES/TDES and AES
 - hash engine: SHA-1, SHA-2 (full SHA-2 suite)



The specific algorithms available to System SSL/TLS depend on the installed hardware and the version of z/OS

System SSL hardware crypto usage

Crypto Type	Algorithm	Only CPACF available	CPACF + Coprocessor/Accelerator
Asymmetric Encrypt/Decrypt	RSA/ECC signature generation	In software	In coprocessor mode only. Otherwise in software (accelerator does not support this operation)
	RSA/ECC signature verification	In software	In coprocessor/accelerator
	PKA/ECC encrypt/decrypt for handshake	In software	In coprocessor/accelerator
Symmetric Encrypt / Decrypt	DES	CPACF (non-FIPS mode only: DES not allowed in FIPS mode)	
	3DES	CPACF	
	AES-CBC-128	CPACF	
	AES-CBC-256	In software on z9, CPACF in z10, z196, EC12	
Hashing	SHA-1, SHA-256, SHA-512	CPACF	
	MD5	In software (non-FIPS mode only: MD5 not allowed in FIPS mode)	

FIPS Mode Support

- **NIST Cert #1692 (z/OS 1.13); NIST Cert #1600 (z/OS 1.12); NIST Cert #1492 (z/OS 1.11)**
 - TDES
 - AES (128- or 256-bit)
 - SHA-1, SHA-2
 - RSA (1024- to 4096-bit)
 - DSA (1024-bit)
 - DH (2048-bit)
 - ECC (160- to 521-bit)
- FIPS On Demand



<http://csrc.nist.gov/groups/STM/cmvp/validation.html>

SSL Exploiters

CICS

LDAP

WebSphere

MQ Series

Tivoli Access Manager for
Business Integration Host
Edition

Policy Director
Authorization Services

Secure TN3270

IMS

PKI Services

EIM

Sendmail

Secure FTP

IPSEC

IBM HTTP Server

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

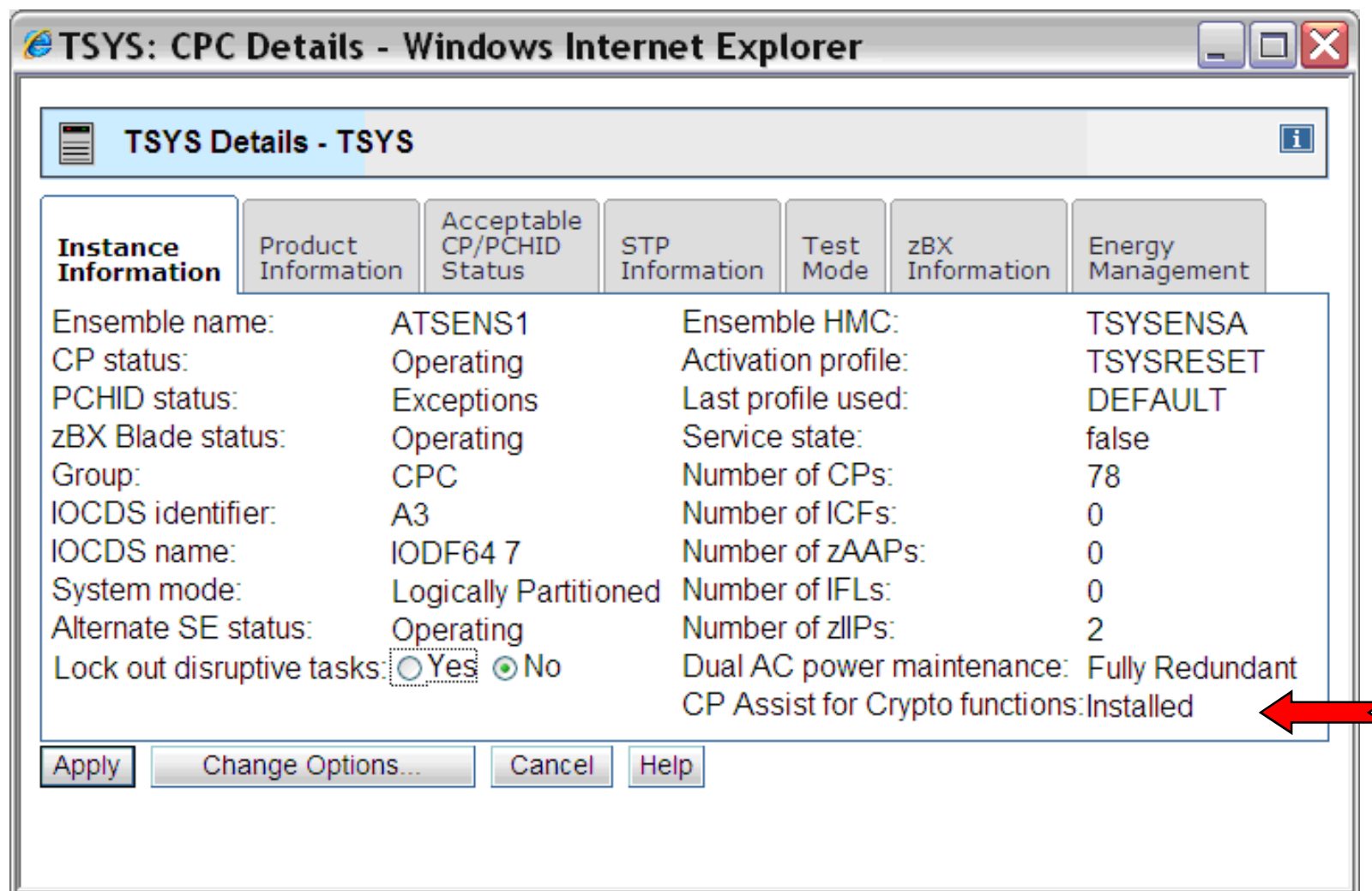
How do I tell, what ciphersuites – F GSKSRVR, DISPLAY CRYPTO

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

Crypto Microcode Installed?



Instance Information	Product Information	Acceptable CP/PCHID Status	STP Information	Test Mode	zBX Information	Energy Management
Ensemble name:	ATSENS1		Ensemble HMC:			TSYSENSA
CP status:	Operating		Activation profile:			TSYSRESET
PCHID status:	Exceptions		Last profile used:			DEFAULT
zBX Blade status:	Operating		Service state:			false
Group:	CPC		Number of CPs:			78
IOCDS identifier:	A3		Number of ICFs:			0
IOCDS name:	IODF64 7		Number of zAAPs:			0
System mode:	Logically Partitioned		Number of IFLs:			0
Alternate SE status:	Operating		Number of zIIPs:			2
Lock out disruptive tasks:	<input type="radio"/> Yes <input checked="" type="radio"/> No		Dual AC power maintenance:			Fully Redundant
			CP Assist for Crypto functions:			Installed

Buttons: Apply, Change Options..., Cancel, Help

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

Crypto Devices Available

TSYS: Cryptographic Configuration - Windows Internet Explorer

Cryptographic Configuration - TSYS

Cryptographic Information

Select	Number	Status	Crypto Serial Number	Type	UDX Status	TKE Commands
<input checked="" type="radio"/>	0	Configured	90003883	X3 Coprocessor	IBM Default	Denied
<input type="radio"/>	1	Deconfigured	Not available	X3 Coprocessor	Not available	Not available
<input type="radio"/>	2	Deconfigured	Not available	X3 Coprocessor	Not available	Not available
<input type="radio"/>	3	Deconfigured	Not available	X3 Coprocessor	Not available	Not available
<input type="radio"/>	4	Configured	90004902	X3 Coprocessor	IBM Default	Denied
<input type="radio"/>	5	Deconfigured	Not available	X3 Coprocessor	Not available	Not available
<input type="radio"/>	6	Configured	90004543	X3 Coprocessor	IBM Default	Permitted
<input type="radio"/>	7	Configured	90004529	X3 Coprocessor	IBM Default	Permitted

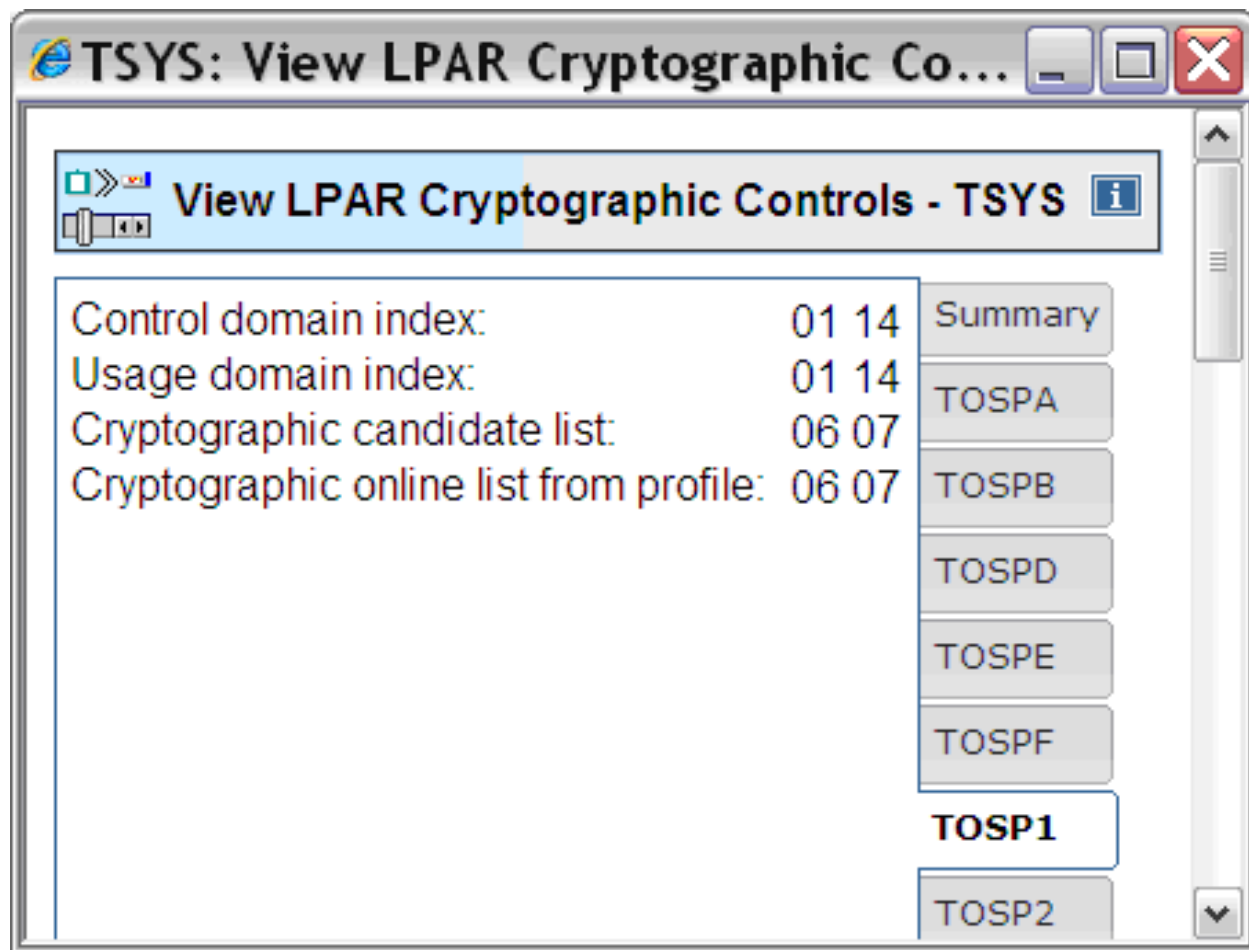
Select a Cryptographic number and then click the task push button.

View Details... Test RN Generator Zeroize Usage Domain Zeroize TKE Commands... Crypto Type Configuration...

Zeroize All Test RN Generator on All UDX Configuration... Refresh Cancel Help

- From the CPC Menu, select Crypto Configuration

How do I tell, what hardware I'm using (LPAR)



- From CPC Operational Customization, click on View LPAR Cryptographic Controls

How do I tell, what hardware I'm using (LPAR)

TSYS: View LPAR Cryptographic Controls - Windows Internet Explorer

View LPAR Cryptographic Controls - TSYS

Installed Crypto Express3: 00 01 02 03 04 05 06 07

Cryptographic Candidate List

Partition	Active	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
TOSPA	Yes																
TOSPB	Yes																
TOSPD	Yes																
TOSPE	Yes																
TOSPF	Yes																
TOSP1	Yes							X	X								
TOSP2	Yes							X	X								
TOSP4	Yes																

Usage Domain Index

Partition	Active	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
TOSPA	Yes																
TOSPB	Yes																
TOSPD	Yes																
TOSPE	Yes																
TOSPF	Yes																
TOSP1	Yes		X													X	
TOSP2	Yes			X										X			
TOSP4	Yes																

Summary

- TOSPA
- TOSPB
- TOSPD
- TOSPE
- TOSPF
- TOSP1
- TOSP2
- TOSP4
- TOSP5
- TOSP6
- TOSP7
- TOSP8
- TOSP9
- TOSP1A

Coprocessor Management Panel

Select the coprocessors to be processed and press ENTER.
Action characters are: A, D, E, K, R and S. See the help panel for details.

CoProcessor	Serial Number	Status	AES	DES	ECC	RSA
XXXXP11						
_____	_____	_____	---	---	-----	---

___ G01	00000001	ONLINE	U	U	C	U
___ G02	00000002	ACTIVE	A	U	A	E
___ G03	00000003	ACTIVE	A	U	A	C
___ E05	00000004	ACTIVE	A	U	-	C
___ H07		ACTIVE				

RMF Crypto Hardware Activity Report

CRYPTO HARDWARE ACTIVITY

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 -----

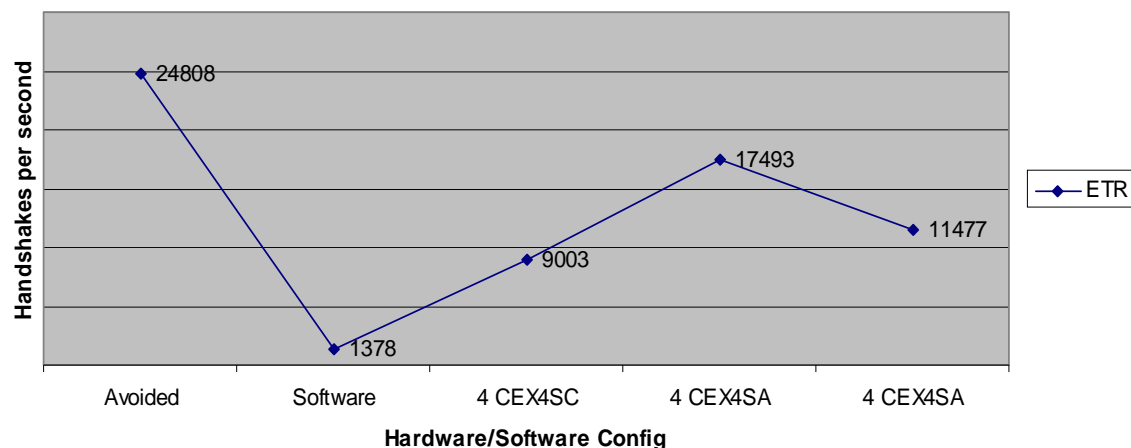
----- TOTAL -----					-- ME-FORMAT RSA OPERATIONS --				-- CRT-FORMAT RSA OPERATIONS --		
TYPE	ID	RATE	EXEC TIME	UTIL%	KEY	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%
CEX2A	3	766.9	0.434	33.3	1024	362.4	0.521	18.9	369.5	0.183	6.8
					2048	0.00	0.000	0.0	34.99	2.175	7.6
CEX3A	5	998.9	0.365	36.5	1024	246.4	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		

Performance – System SSL on zEC12

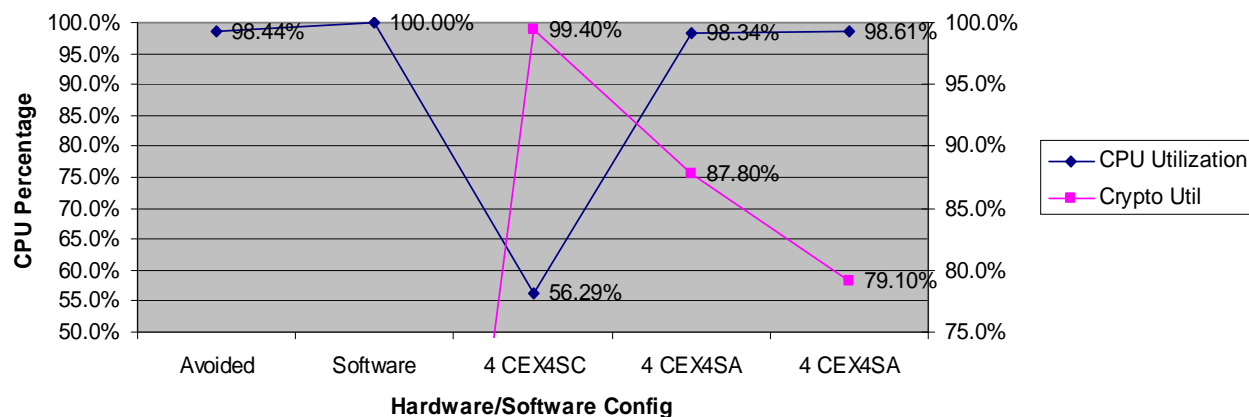
**zEC12 System SSL Handshakes
Transaction Throughput**



zEC12 HA1 – 4

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 System SSL
CPU Util**



Crypto Performance
Whitepaper

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

System SSL Summary

- SSL combines the strengths of symmetric and asymmetric algorithms to provide secure communications
- The product or application invoking SSL makes the decision about when and how to use the crypto environment
- Where the SSL workload is executed depends on the environment (hardware and software) and the security protocols that you require and configure; The crypto environment, SSL and the calling application must be in sync
- SSL and ICSF are designed to find a way to service the request efficiently; but does not provide a lot of data on how/where its being serviced

Heartbleed – An explanation

- <http://xkcd.com/1354/>
- Or google 'Heartbleed xkcd'

- System SSL is not affected
- OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable

- Fix
 - Recompile using patched libraries (fix the problem)
 - Vendor change private key (that might have been exposed)
 - You change your passwords (that might have been viewed)

Some useful sites

- [Heartbleed Vulnerabilities](#)
 - <https://zmap.io/heartbleed/>
 - <http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/>
- [IBM Security Portal](#)
 - http://www.ibm.com/systems/z/advantages/security/integrity_sub.html

System SSL References

- Protocols
 - SSL V3 <http://tools.ietf.org/html/rfc6101>
- IBM Manuals
 - z/OS V2.1 Cryptographic Services System Secure Sockets Layer Programming – SC14-7495
 - z/OS V1.13 Cryptographic Services System Secure Sockets Layer Programming – SC24-5901
- Performance Doc
 - zEC12 -
<http://www.ibm.com/systems/z/advantages/security/zec12cryptography.html>
 - z196 and z10 -
<http://www.ibm.com/systems/z/advantages/security/z10cryptography.html>
 - Comm Server Performance Index -
<http://www.ibm.com/support/docview.wss?uid=swg27005524>

Crypto References

- For information on hardware cryptographic features reference whitepapers on Techdocs (www.ibm.com/support/techdocs)
 - WP100810 – A Synopsis of System z Crypto Hardware
 - WP100647 – A Clear Key/Secure Key/Protected Key Primer

Questions



QR Code



- Share #15660