System SSL and Crypto on z Systems

Greg Boyd

gregboyd@mainframecrypto.com

November 2015

Copyrights . . .

- 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

. . . And Trademarks

- Copyright © 2015 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.

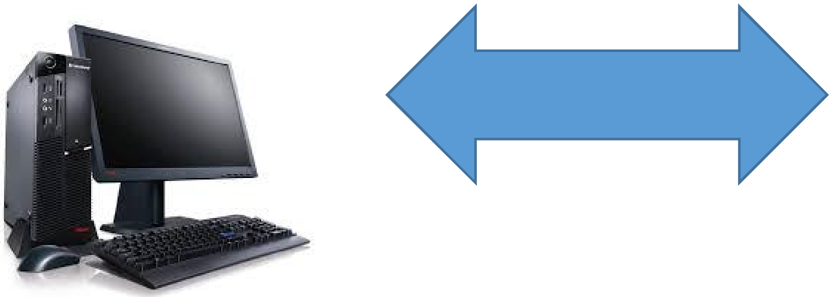
Agenda

- 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



Generations

- SSL
- SSL V2.0 (Feb 1995)
- SSL V3.0 (Nov 1996)
- TLS V1.0 (Jan 1999)
- TLS V1.1 (Apr 2006)
- TLS V1.2 (Aug 2008)
- TLS V1.3 (Draft)

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 APIs

- SSL APIs
  - 28 APIs for performing Secure Sockets Layer Communications
- Certificate Management Services (CMS) APIs
  - 176 APIs to create/manage key database files, use certificates in the key database file or key ring for purposes other than SSL and PKCS #7 message support

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
z/OS 2.2	JCPT421

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

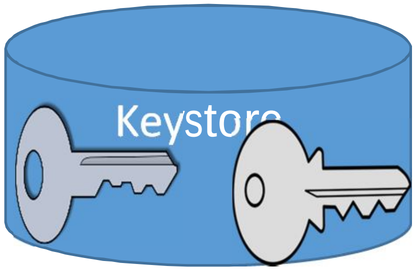
Server

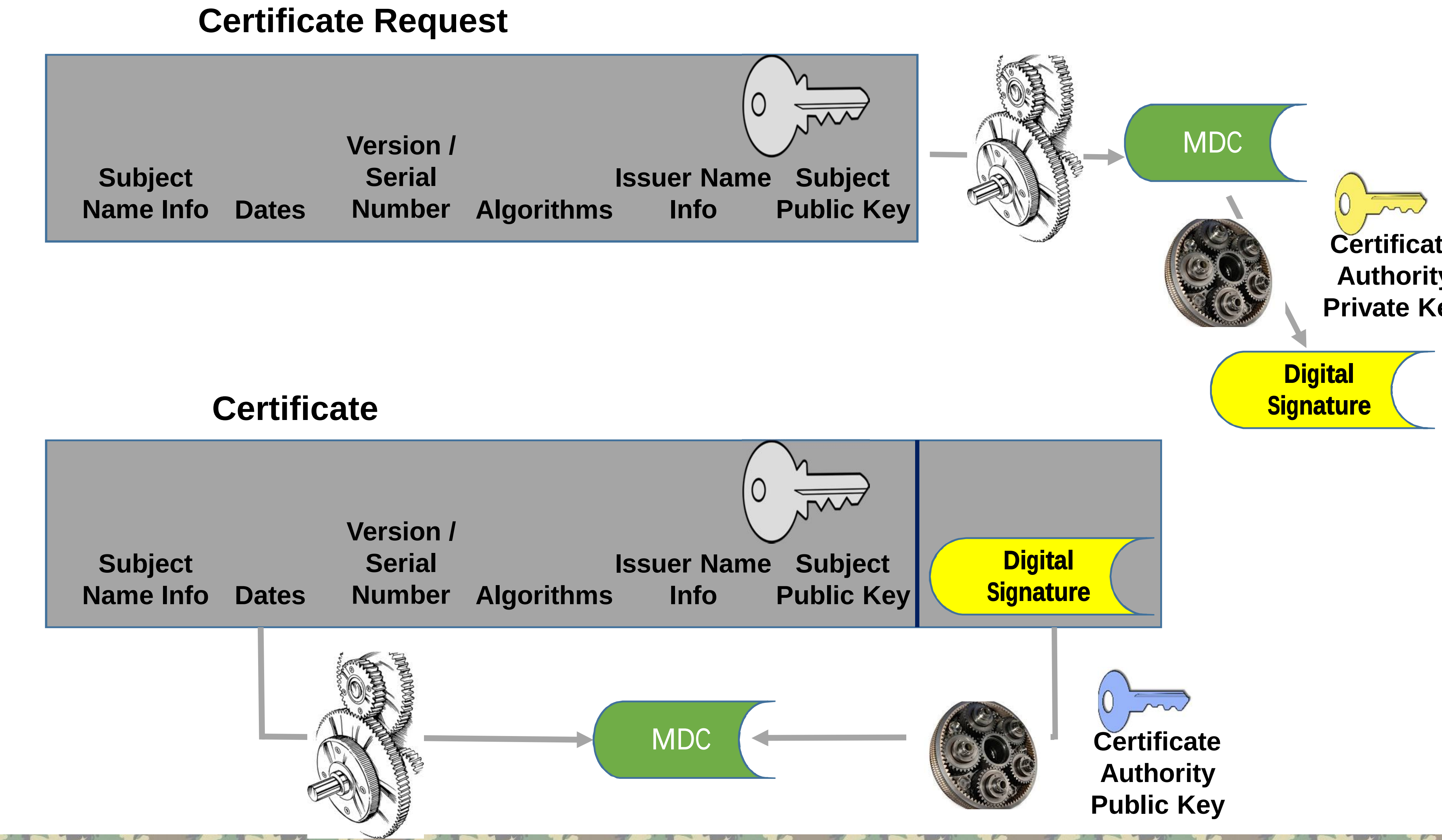
1. Provides data at the client's request
2. Provides access based on it’s security environment
3. Usually an application responding to the request
4. Protects it’s identity via a certificate

SSL/TLS Protocol

- Two phases
  - Handshake phase - relies on certificates anc public/private key algorithms to provide authentication and encryption of session key
    - Authentication - Signature Verification using PKA
    - Data Security - Public key encryption/decryption of the session key
  - Record phase - relies on symmetric algorithms and hashes to provide security and integrity
    - Data security - symmetric encryption of the message
    - Data Integrity – hash of the message

Digital Certificate




Certificate Request

Subject Name Info | Dates | Version / Serial Number | Algorithms | Issuer Name Info | Subject Public Key

MDC

Certificate Authority Private Key

Digital Signature

Certificate

Subject Name Info | Dates | Version / Serial Number | Algorithms | Issuer Name Info | Subject Public Key | Digital Signature

MDC

Certificate Authority Public Key

Crypto Operations & Hardware

Handshake - Asymmetric algorithms

- RSA
  - Crypto Express Accelerator & ICSF
  - Crypto Express Coprocessor & ICSF
  - System SSL software routines
- ECC
  - Requires ICSF and Crypto Express cards

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

Crypto Operations & Hardware

Record Phase – Symmetric Algorithms

- DES/TDES
  - CPACF (and ICSF for older versions of z/OS)
- AES
  - CPACF (and ICSF for older versions of z/OS)
  - System SSL software routines
- RC2/RC4
  - System SSL software routines

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

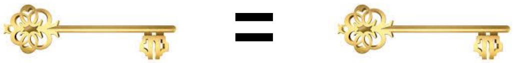
Crypto Operations & Hardware
Hashing

- SHA-1, SHA-2
  - CPACF (and ICSF for older versions of z/OS)
  - System SSL software routines
- MD5
  - System SSL software routines

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

Why Both Asymmetric and Symmetric?

- Asymmetric
  - + Strength, 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)

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)

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                          --                --
```

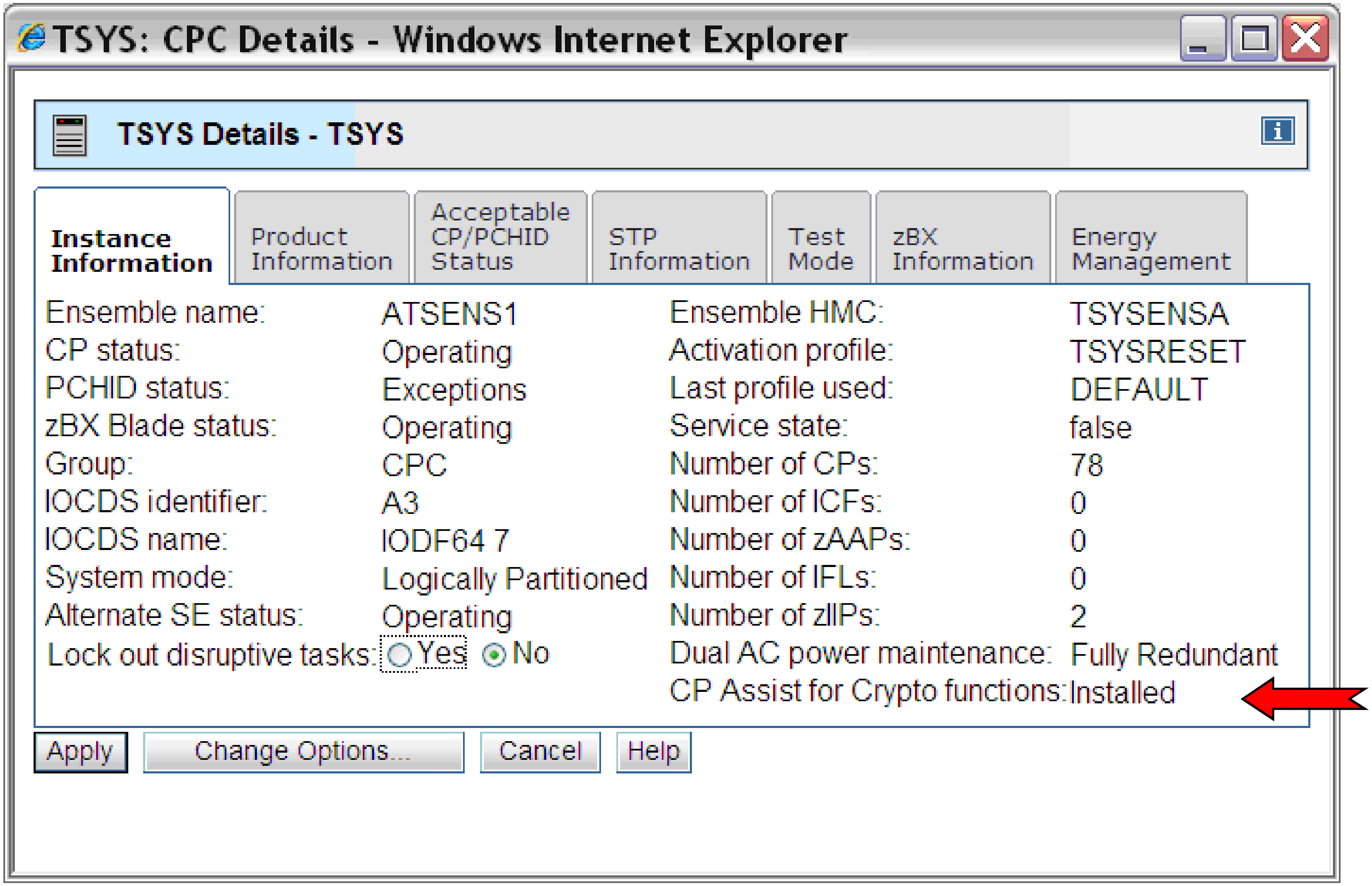
Environment: z196 running z/OS 1.13, but ICSF not active

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

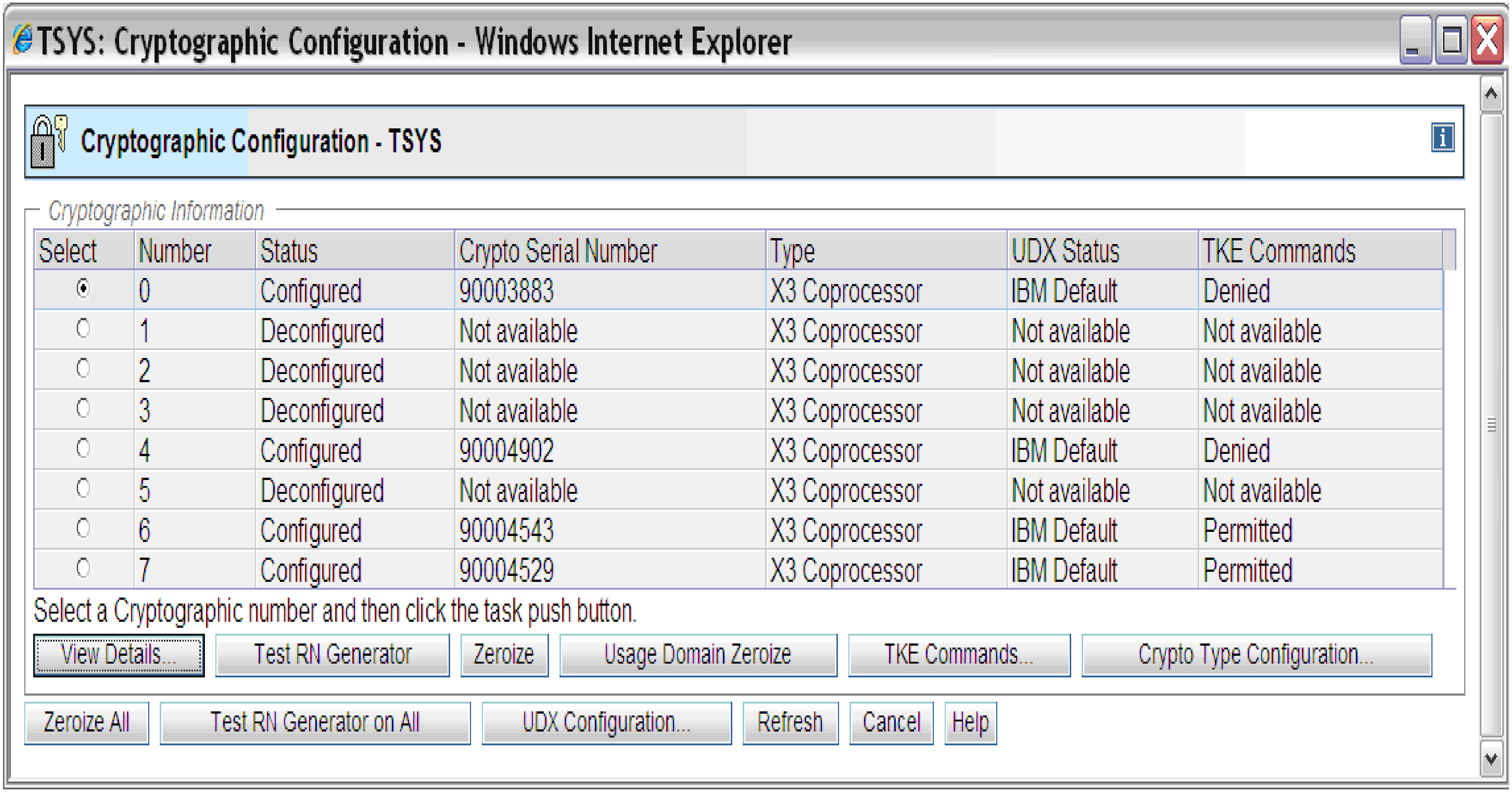
Crypto Microcode Installed?



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:	○ Yes ● No	Dual AC power maintenance:	Fully Redundant
		CP Assist for Crypto functions:	Installed

- 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

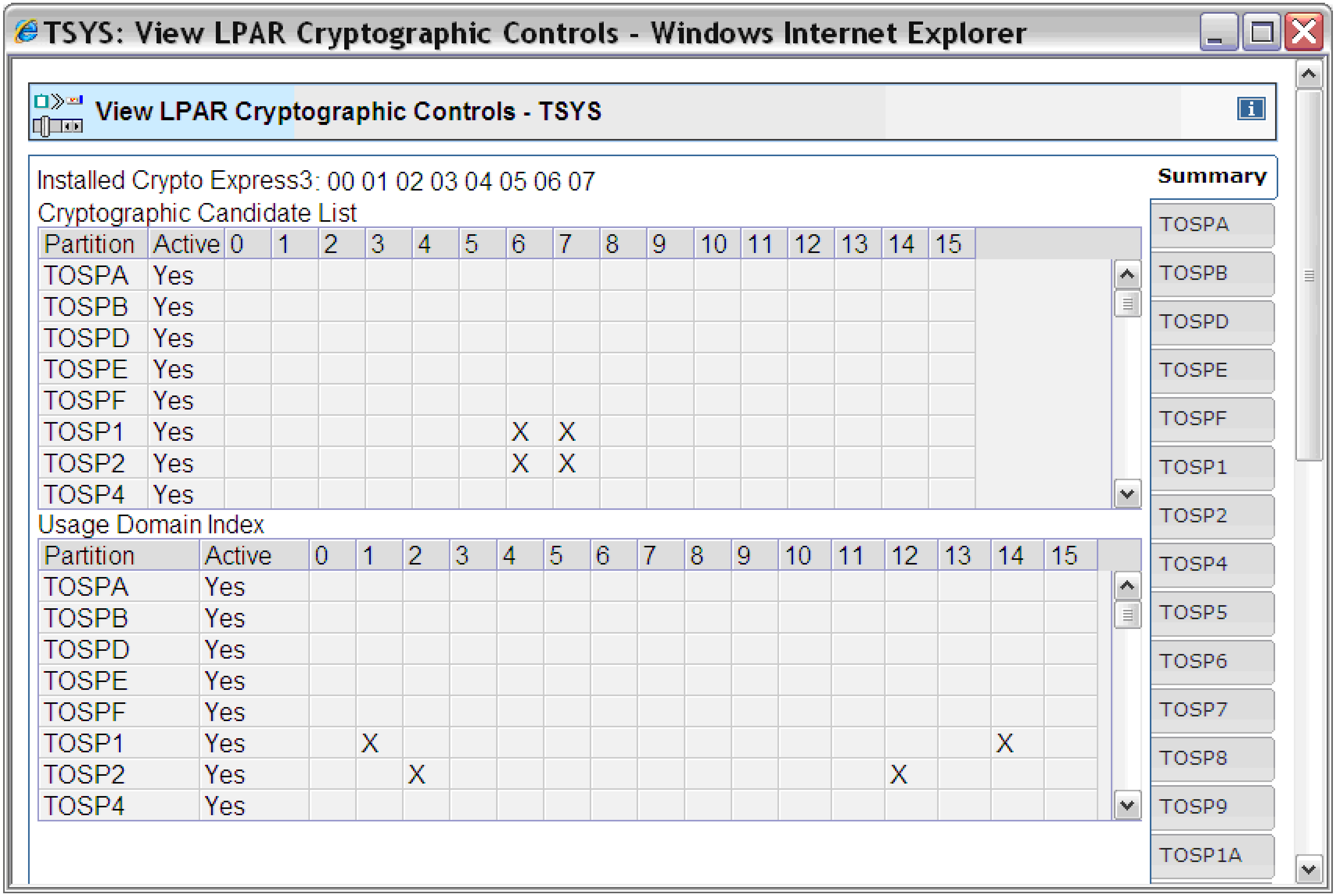
Cryptographic Information

Select	Number	Status	Crypto Serial Number	Type	UDX Status	TKE Commands
●	0	Configured	90003883	X3 Coprocessor	IBM Default	Denied
○	1	Deconfigured	Not available	X3 Coprocessor	Not available	Not available
○	2	Deconfigured	Not available	X3 Coprocessor	Not available	Not available
○	3	Deconfigured	Not available	X3 Coprocessor	Not available	Not available
○	4	Configured	90004902	X3 Coprocessor	IBM Default	Denied
○	5	Deconfigured	Not available	X3 Coprocessor	Not available	Not available
○	6	Configured	90004543	X3 Coprocessor	IBM Default	Permitted
○	7	Configured	90004529	X3 Coprocessor	IBM Default	Permitted

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

- From the CPC Menu, select Crypto Configuration

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

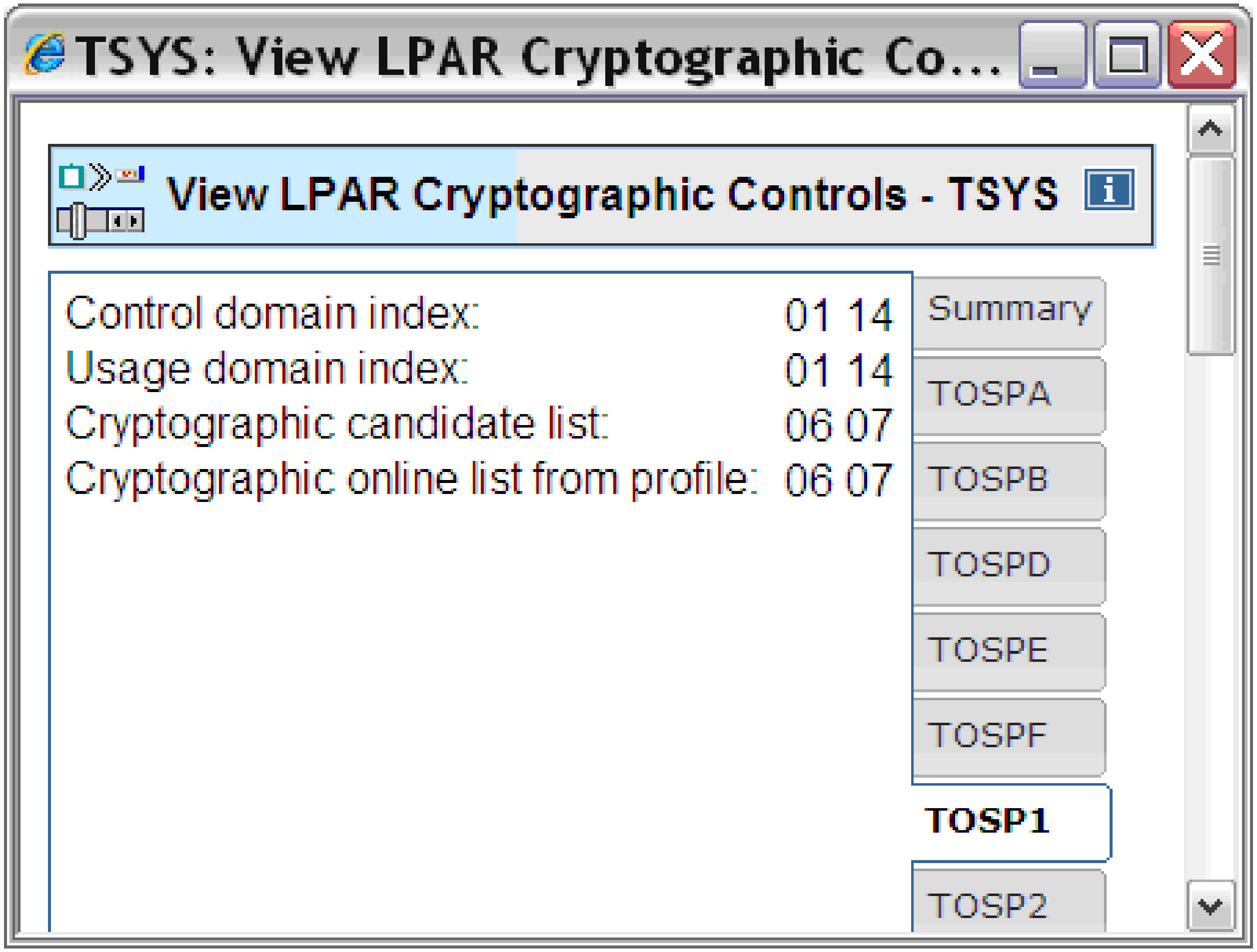
Cryptographic Candidate List

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																

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


TSYS: View LPAR Cryptographic Co...
View LPAR Cryptographic Controls - TSYS
Summary
TOSPA
TOSPB
TOSPD
TOSPE
TOSPF
TOSP1
TOSP2

Control domain index: 01 14
Usage domain index: 01 14
Cryptographic candidate list: 06 07
Cryptographic online list from profile: 06 07

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

ICSF Coprocessor Management Panel

```
CSFGCMP0 -------------- ICSF Coprocessor Management  -------------  Row 1 to 2 of 2
COMMAND  ===>

  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   P11
   -----------  -------------    -----------     ----- ----- ----- ----- ------
   _S_ G06         90004543        ACTIVE          A     A     A     A     U
   _S_ G07         90004529        ACTIVE          A     A     A     A     U
   _S_ G08         90004562        ACTIVE          A     A     A     A     U
   _S_ H09                         ACTIVE
```

RMF Crypto Hardware Activity Report – Part 1

```
                              CRYPTO HARDWARE ACTIVITY
                                                                              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
CEX5C    9     0.4      1.123       0.1               0.00
```

RMF Crypto Hardware Activity Report – Part 2

```
------------------ 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
CEX5P    10    446.5     0.243      8.3       ASYM FAST             274.3     0.175        2.4
                                              ASYM GEN               0.00     0.000        0.0
                                              ASYM SLOW             120.3     0.405        5.3
                                              SYMM COMPLETE          0.00     0.000        0.0
                                              SYMM PARTIAL          51.89     0.398        0.6
```

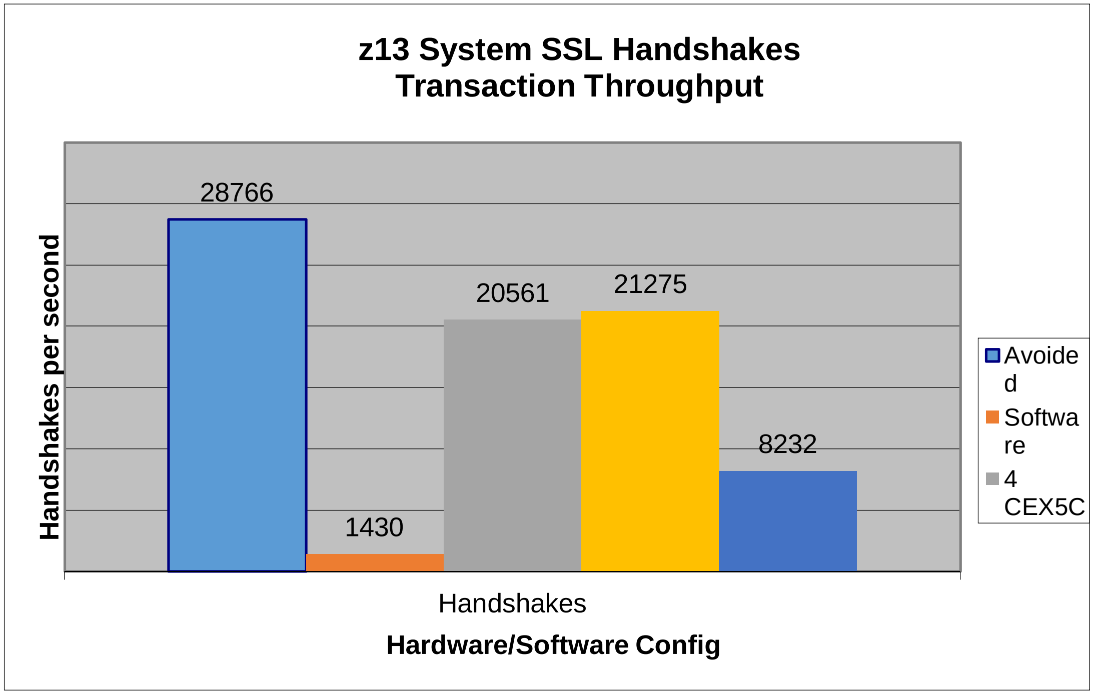
RMF Crypto Hardware Activity Report – Part 3

```
-------- 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
CEX5A 11 1335.5    0.151     0.3 1024     678.2     0.225       14.2       544.4     0.145        5.8
                                 2048      0.00     0.000        0.0        22.6     0.465        4.8
                                 4096      0.00     0.000        0.0        90.3     0.378        5.5
```

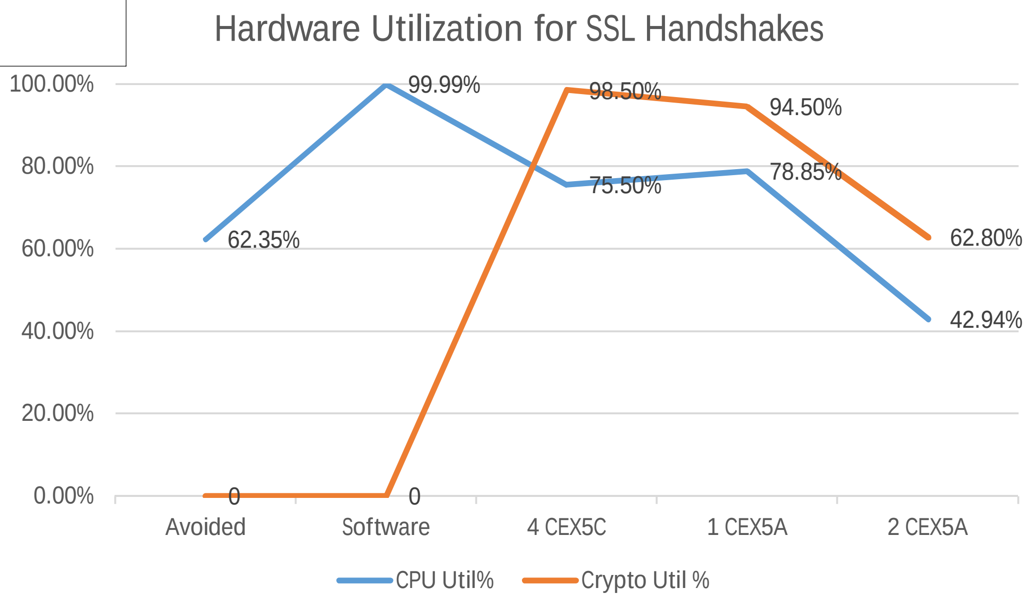
RMF Crypto Hardware Activity Report – Part 4

```
-------- ICSF SERVICES -------------------------------------------------------------------------------------------
          ---- ENCRYPTION -----    ---- DECRYPTION -----    ------------ HASH -------------        -------- PIN ---------
          SDES      TDES     AES      SDES      TDES     AES     SHA-1  SHA-256 SHA-512        TRANSLATE  VERIFY
RATE      0.00      0.00     0.00     0.00      0.00     0.00     0.00     0.00     0.00              0.00      0.00
SIZE      0.00      0.00     0.00     0.00      0.00     0.00     0.00     0.00     0.00
       ------- MAC --------    ------ AES MAC -----    ------ RSA DSIG ----   ----- ECC DSIG ------   – FORMAT PRESERVING ENCRYPTION –
       GENERATE  VERIFY   GENERATE  VERIFY   GENERATE  VERIFY  GENERATE  VERIFY   ENCIPHER       DECIPHER       TRANSLATE
RATE          0.00      0.00           0.00      0.00           0.00      0.00           0.00      0.00       0.00           0.00           0.00
SIZE          0.00      0.00           0.00      0.00                                                         0.00           0.00           0.00
```

System SSL Performance – z13



Caching SID/Client Authentication	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%

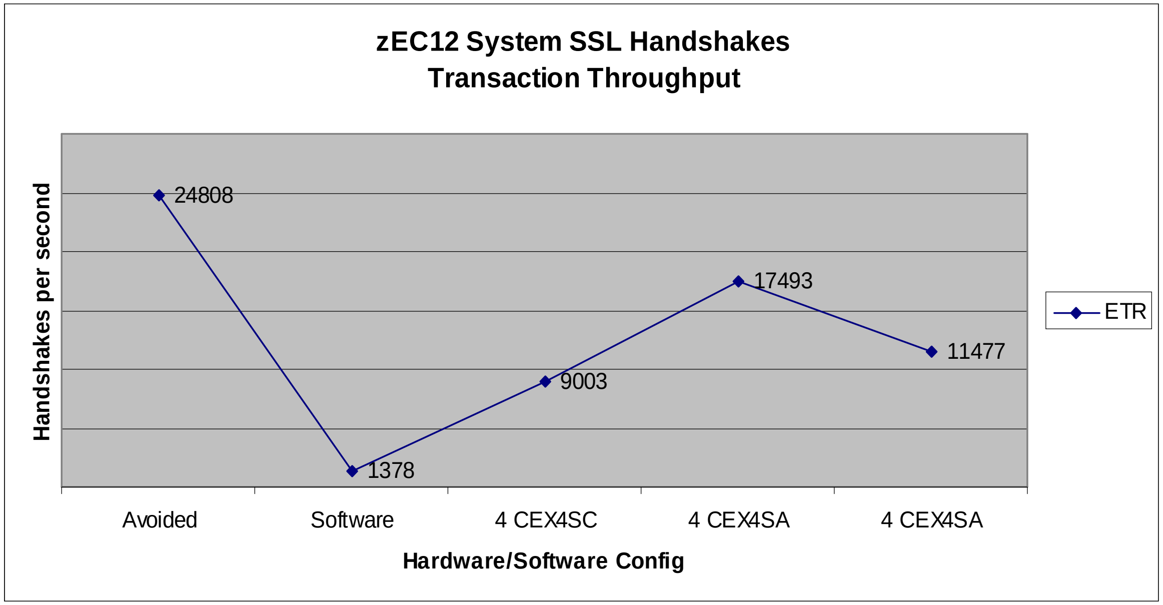


IBM z13 Model 2964-N96 (4 CPs)

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

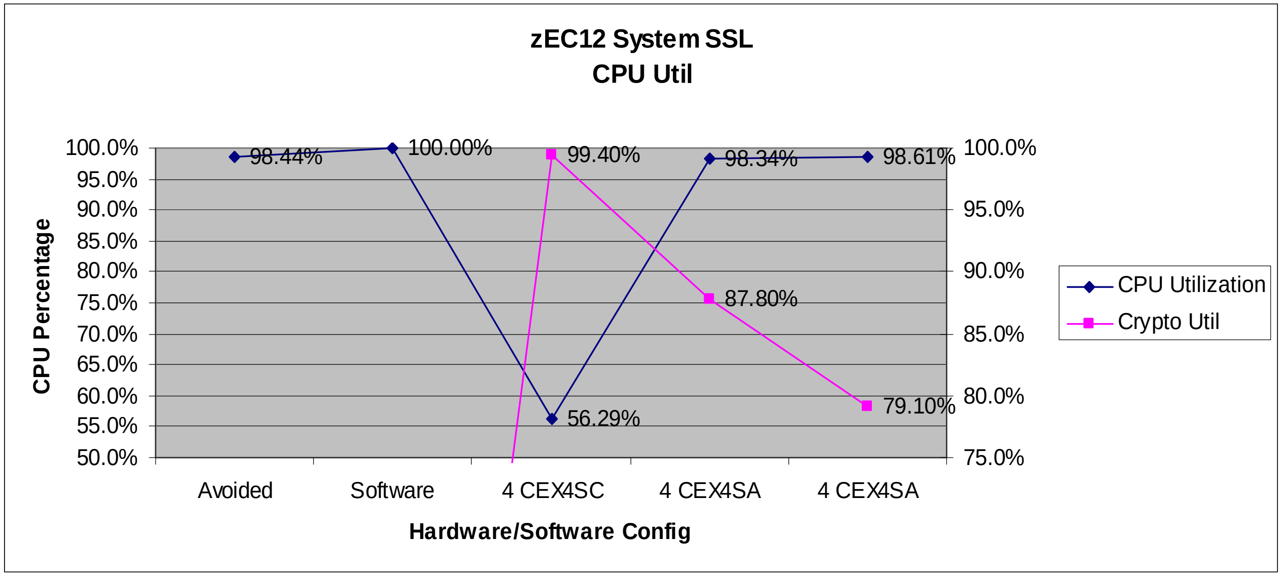
http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=ZSW03283USEN&attachment=ZSW03283USEN.PDF

Performance – System SSL on zEC12



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%



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

System SSL References

- Protocols
  - SSL V2 https://tools.ietf.org/html/rfc6101
  - SSL V3 http://tools.ietf.org/html/rfc6101
  - TLS V1.0 https://www.ietf.org/rfc/rfc2246.txt
  - TLS V1.1 https://www.ietf.org/rfc/rfc4346.txt
  - TLS V1.2 https://tools.ietf.org/html/rfc5246
  - TLS V1.3 https://tools.ietf.org/html/draft-ietf-tls-tls13-07
- IBM Manuals
  - z/OS V2.x Cryptographic Services System Secure Sockets Layer Programming – SC14-7495
  - z/OS V1.13 Cryptographic Services System Secure Sockets Layer Programming – SC24-5901

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
  - WP101213 – TLS (formerly SSL) Options in Websphere for z/OS
- Performance Docs
  - IBM z13 Performance of Cryptographic Operations
  - IBM zEC12 Performance of Cryptographic Operations
  - Comm Server Performance Index - http://www.ibm.com/support/docview.wss?uid=swg27005524

Other useful sites

- Heartbleed Vulnerability
  - http://xkcd.com/1354/
  - 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

Questions