IBM Americas, ATS, Washington Systems Center

10194 System SSL and Crypto on System z

Greg Boyd (boydg@us.ibm.com)
March 12, 2012
Atlanta, GA

Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

Trademarks

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

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

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.

Agenda

- **SSL Background**
- **SSL Flow**
- **Crypto Basics**
- **Crypto Hardware**
- **SSL & Crypto**
- **SSL on System z**
- **IPSEC**

V#, SN , CA's signature,sgn-alg
Issuer name: CAxyz
Validity Dates and Time type
Subject name: Greg
Subject's Public Key, AlgoID
SignAlgo: RSA with SHA-1
Extensions

SSL, TLS, AT/TLS

- **Communication protocols**
  - allows a session to be established between two parties, a client and a server
    - Authentication of the communicating partner, provide privacy (encryption), and data integrity of the information exchanged on the connection
    - Security is based on negotiated agreement between these two parties
  - May be used on an application-by-application basis

privacy, authentication, data integrity

Two Implementations of SSL

- **System SSL**
  - C/C++ callable APIs to support SSL/TLS.
  - Provides software support for SSL, or interfaces seamlessly with ICSF and the crypto hardware.
  - The SSL provider used by everything on z/OS, except Java-based workloads.
- **Java**
  - Part of the IBM SDK for z/OS, Java Technology Edition.
  - Java callable APIs to support SSL/TLS.
  - Provides software support for SSL, or interfaces not-so-seamlessly with ICSF and the crypto hardware.
  - The SSL provider used by Java-based workloads on z/OS

System SSL Security Level 3

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

SSL/TLS : High Level Flow

Client

1. initiates the communications
2. generally selects the data to be provided by the Server
3. most are browsers but not necessarily
4. can prove its identity by also having a certificate

Server

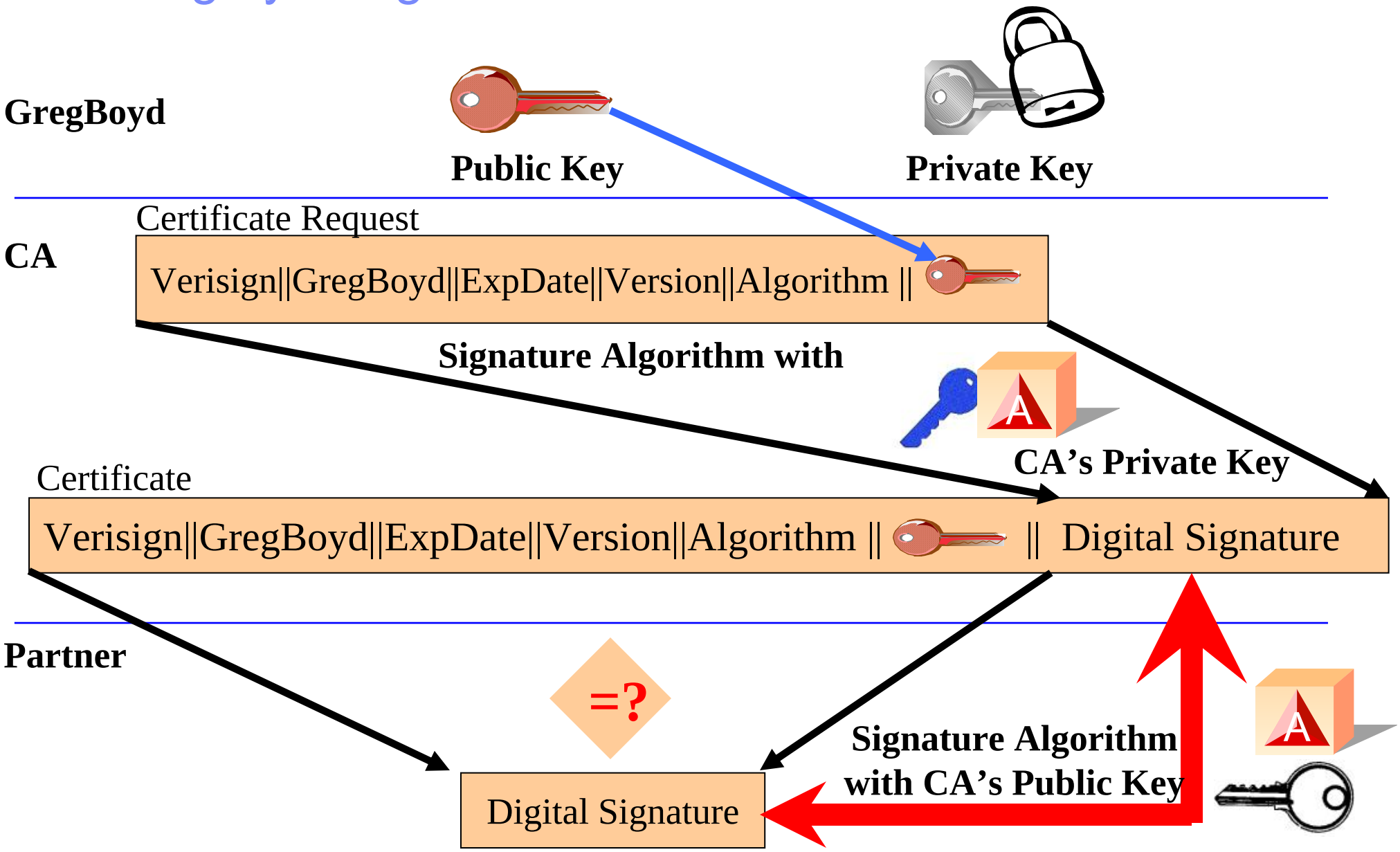
1. provides information and data to the client at the client's request
2. decides what data should be protected
3. is usually an application written to provide data services outbound
4. has the responsibility to protect its identity (will prove its identity via a certificate)

SSL/TLS Protocol

- **Handshake – Asymmetric**
  - Signature Verification
  - Public Key

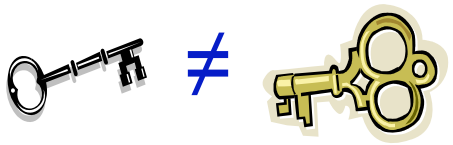
- **Record Level – Symmetric**
  - DES/TDES
  - AES
  - Hashing – SHA-1

Data Integrity – Digital Certificates



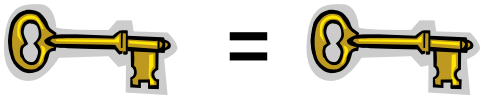
Why Asymmetric and Symmetric Keys?

- **Asymmetric**



  - plus - its strength, can be used to establish a secret between two parties
  - minus – expensive in terms of performance

- **Symmetric**



  - plus - less resource intensive
  - minus - requires key to be shared securely

SSL & Crypto Devices (z800/z900 & earlier)

- **CCF, Crypto Coprocessor Facility**
  - secure key DES/TDES
  - RSA asymmetric algorithms (1024-bit keys)

- **PCICC, PCI Cryptographic Coprocessor**
  - RSA asymmetric algorithms (2048-bit keys)

- **PCICA, PCI Cryptographic Accelerator**
  - high-performance RSA asymmetric algorithms (2048-bit keys)

SSL & Crypto Devices (z890, z990, z9, z10, z196/z114)

- **CPACF, CP Assist for Cryptographic Functions**

  - z890/z990: high performance, “clear key” DES, TripleDES (TDES), and hash engine (SHA-1) in every Coprocessor (CP)
  - z9/z10/z196/z114: high performance, “clear key” DES, TripleDES (TDES) and AES 128-, 256-bit, and hash engine (SHA-1, SHA-256 and SHA-512 (on z10/z196/z114))

The hardware platform and the z/OS Version determine which algorithms SSL/TLS will use to do record level clear key encryption

SSL & Crypto Devices ….

- **PCICA, PCI Cryptographic Accelerator**
  - RSA asymmetric algorithms (2048-bit keys)
  - No Longer Orderable, but still supported on the z890/z990; Not supported on the z9/z10

- **PCIXCC, PCIX Cryptographic Coprocessor**
  - RSA asymmetric algorithms (2048-bit keys)
  - No Longer Orderable, but still supported on the z890/z990; Not supported on the z9/z10

- **CEX2, Crypto Express2 or CEX3, Crypto Express3**
  - RSA asymmetric algorithms (2048-bit keys or 4096-bit keys on z10 and z9 w/MCL) - combines PCICA & PCIXCC into a single feature
  - Available on z890/z990 and z9/z10/z196/z114, with additional configuration capabilities on the z9/z10/z196/z114

Crypto Functions / Hardware

Crypto Functions	z800/z900	z890/z990	z9/z10	Z196/z114
Handshake Phase				
RSA Keys	PCICA, PCICC, CCF	PCICA, CEX2, PCIXCC	CEX2A, CEX2C CEX3A, CEX3C	CEX3A, CEX3C
ECC Keys	N/A	N/A	N/A	CEX3A/CEX3C***
Record Level - Symmetric Encryption				
Clear Key DES/TDES	CCF*	CPACF	CPACF	CPACF
Clear Key AES	Software	Software	CPACF**	CPACF**
RC2/RC4	Software	Software	Software	Software
Record Level – Hashing				
SHA-1	CCF	CPACF	CPACF	CPACF
MD5	Software	Software	Software	Software

*CCF is secure key device & doesn't support clear key APIs, but System SSL will use the secure key APIs.

**Requires HCR7730 or higher for AES-128 support

*** Requires z/OS 1.13 or later

FIPS Mode Support

- NIST Cert #1492 (z/OS 1.11), Cert #1600 (z/OS 1.12)
  - 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/documents/140-1/1401val2011.htm

SSL Exploiters

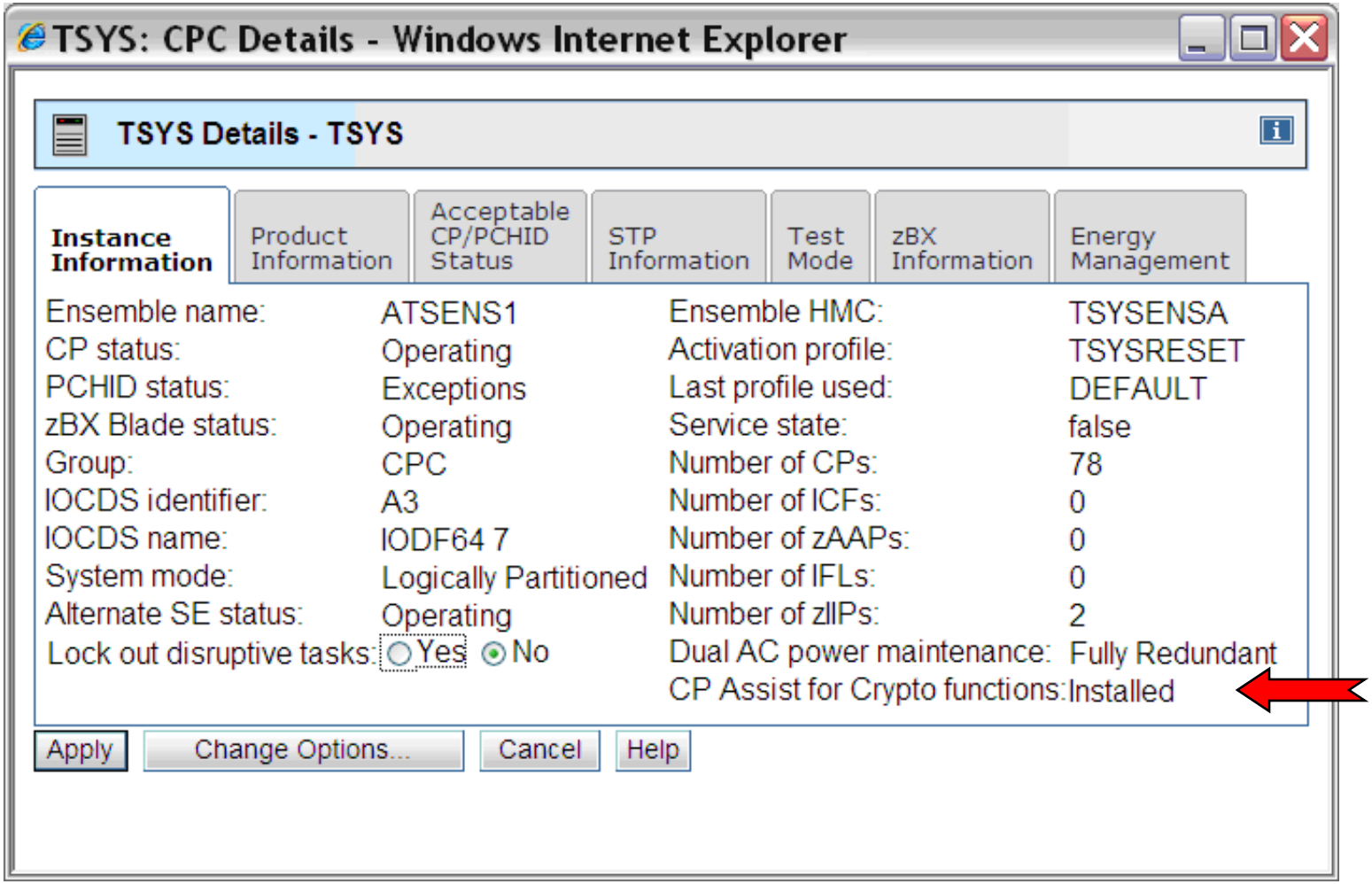
- CICS
- LDAP
- WebSphere
- MQ Series
- Tivoli Access Manager for Business Integration Host Edition
- Policy Director Authorization Services
- Secure TN3270
- IMS
- PKI Services
- EIM
- Sendmail
- Secure FTP
- IPSEC
- IBM HTTP Server

How do I tell, what ciphersuites - Use GSKSRVR STC

GSK01009I Cryptographic status

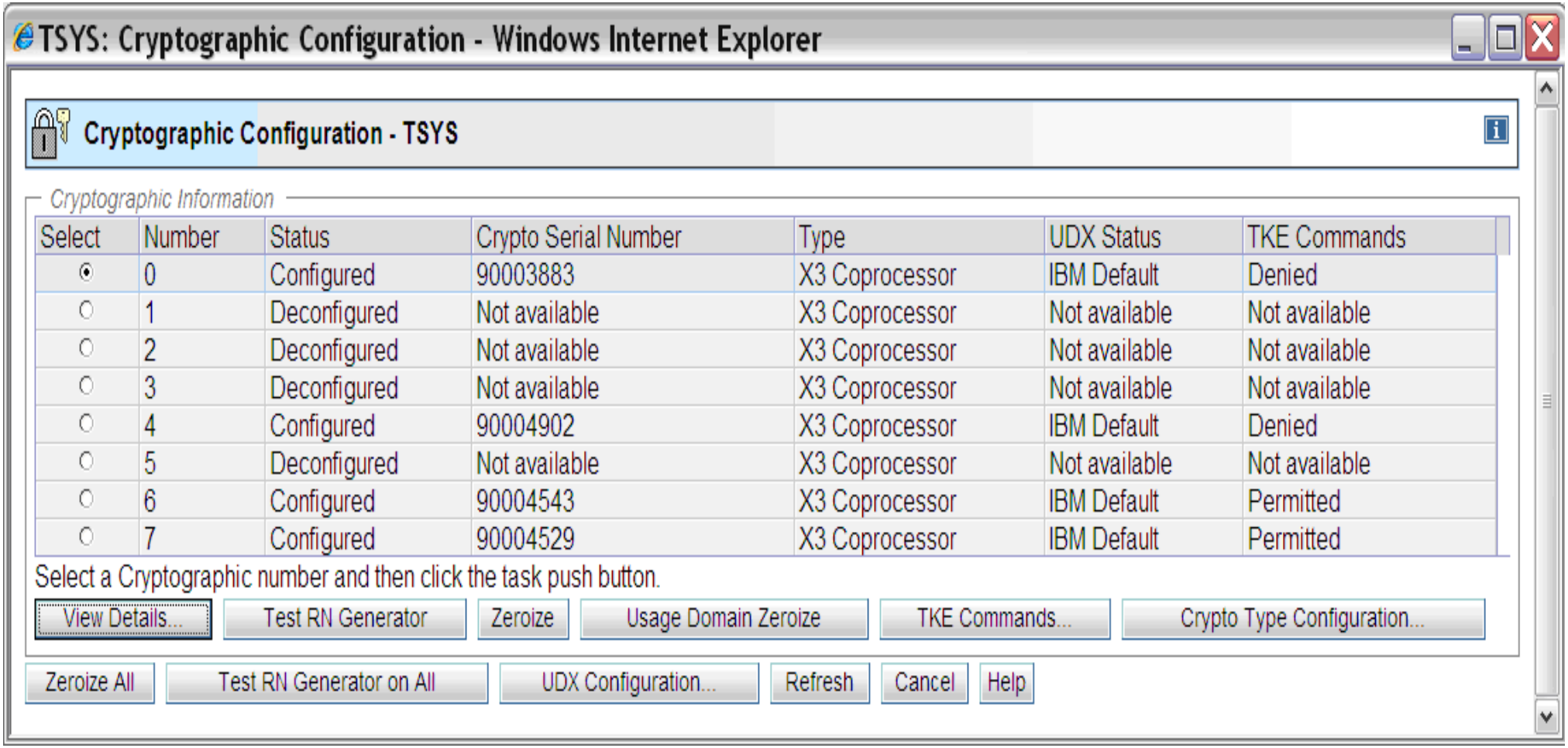
Algorithm	Hardware	Software
DES	56	56
3DES	168	168
AES	256	256
RC2	--	128
RC4	--	128
RSA Encrypt	4096	4096
RSA Sign	4096	4096
DSS	--	1024
SHA-1	160	160
SHA-2	512	512
ECC	--	521

Crypto Microcode Installed?



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

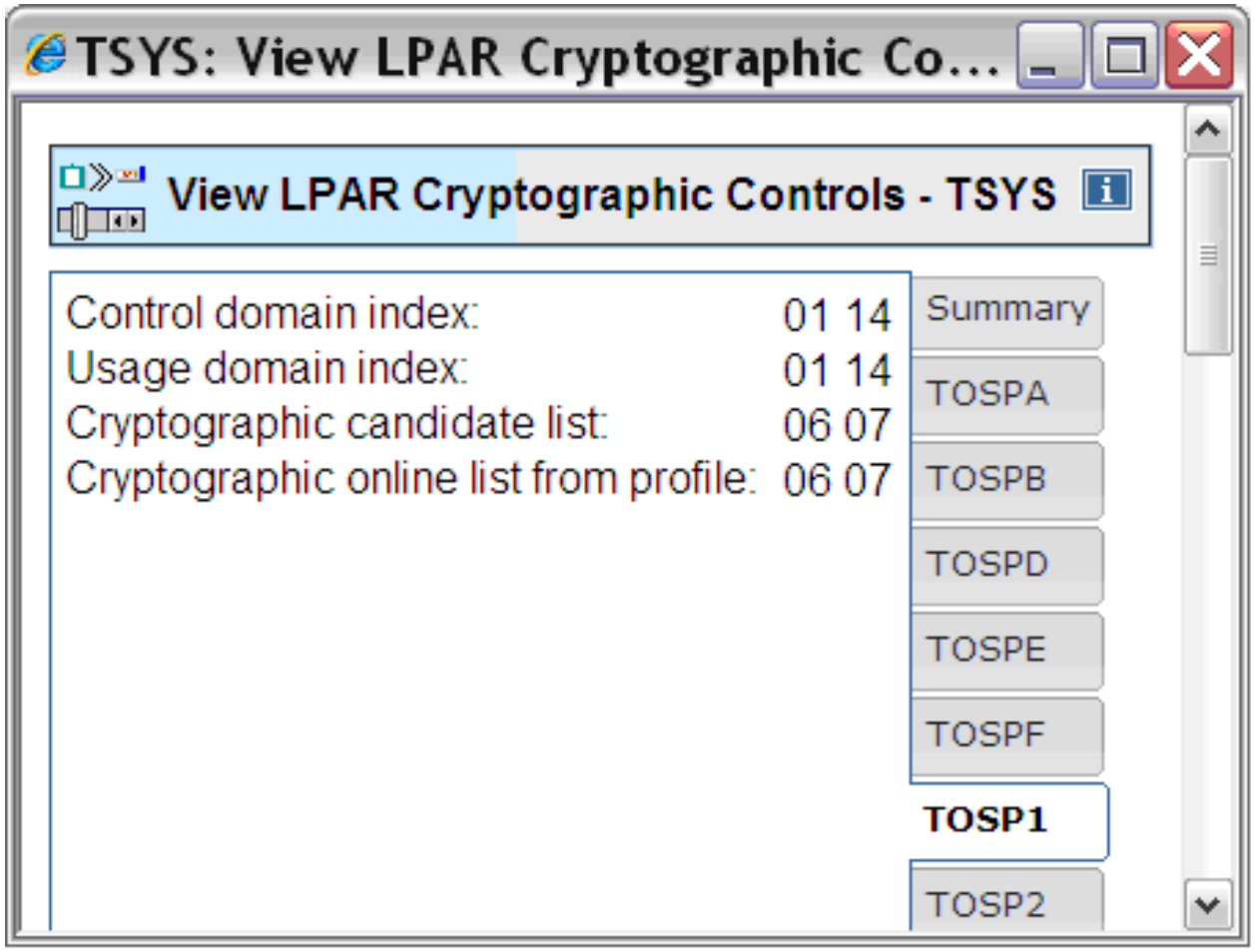
Crypto Devices Available



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

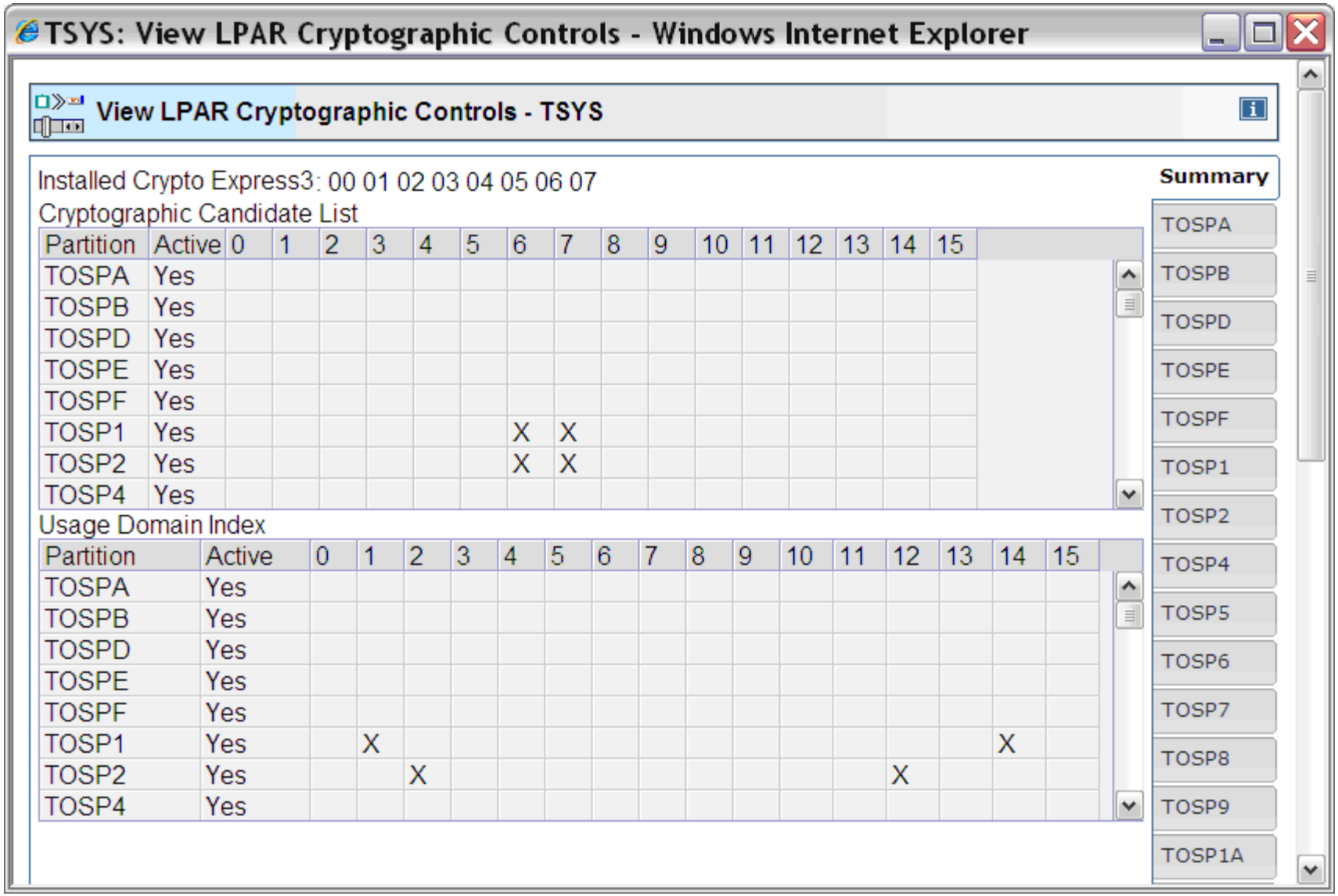
- **From the CPC Menu, select Crypto Configuration**

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)



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.

                    Serial
  CoProcessor       Number          Status    AES    DES    ECC    RSA
  -----------     ---------         ------    ---    ---    ----   ---
__ 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

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

PAGE 6

z/OS V1R10 SYSTEM ID SYS1 DATE 07/28/2009 INTERVAL 14.59.946

RPT VERSION V1R10 RMF TIME 16.30.00 CYCLE 1.000 SECONDS

---------- CRYPTOGRAPHIC COPROCESSOR ----------

		------ TOTAL --------			KEY-GEN
TYPE	ID	RATE	EXEC TIME	UTIL%	RATE
PCIXCC	0	0.00	0.0	0.0	0.00
	1	0.01	3205	32.1	0.01
	2	83.04	1.1	8.8	0
	3	0.00	0.0	0.0	0.00
CEX2C	4	210.8	4.4	93.3	1.91
	5	186.4	4.8	89.6	1.85

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

		---------- TOTAL ----------			----- ------- ME(1024) ----------			---------- ME(2048) ----------			---------- CRT(1024) ----------			---------- CRT(2048) ----------		
TYPE	ID	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%
PCICA	6	165.2	1.3	21.5	107.1	1.1	11.8	0.00	0.0	0.0	58.1	1.7	9.7	0.00	0.0	0.0
	7	892.3	3.6	64.3	350.1	4.1	28.6	0.00	0.0	0.0	512.6	2.4	24.7	29.65	18.5	11.0
	8	684.8	3.5	47.8	260.4	4.0	21.0	0.00	0.0	0.0	402.4	2.3	18.6	22.02	18.5	8.1

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

	DES ENCRYPTION		DES DECRYPTION		---------- MAC ----------		---------- HASH ----------			---------- PIN ----------	
	SINGLE	TRIPLE	SINGLE	TRIPLE	GENERATE	VERIFY	SHA-1	SHA-256	SHA-512	TRANSLATE	VERIFY
RATE	4975K	497.5	12438	1244K	12438	4975K	497.5	0.00	123K	1244K	1244K
SIZE	0.75	100K	10.00	0.01	10.00	0.01	10000	0.00	348.0		

Some thoughts on performance … on z196

Caching SID	Handshake	Client Auth.	ETR	CPU Util %	Crypto Util %
100%	Avoided	No	19370	98.34	N/A
No	Software	No	1204	100.0	N/A
No	8 CEX3C	No	14457	95.24	92.3
No	4 CEX3A	No	14429	99.72	80.7
No	4 CEX3A	Yes	9747	99.06	73.1

Reproduced from 'IBM Enterprise 196 Class Performance of Cryptographic Operations' available at www.ibm.com/systems/z/security/cryptography.html

Some thoughts on performance … z10

Caching SID	Handshake	Client Auth.	ETR	CPU Util %	Crypto Util %
100%	Avoided	No	13197	92.6	N/A
No	Software	No	912	99.5	N/A
No	8 CEX2C	No	9760	97.1	97.7
No	4 CEX2A	No	9618	95.1	75.4
No	4 CEX2A	Yes	6525	94.7	63.6

Reproduced from 'IBM System z10 Enterprise Class Performance of Cryptographic Operations' available at www.ibm.com/systems/z/security/cryptography.html

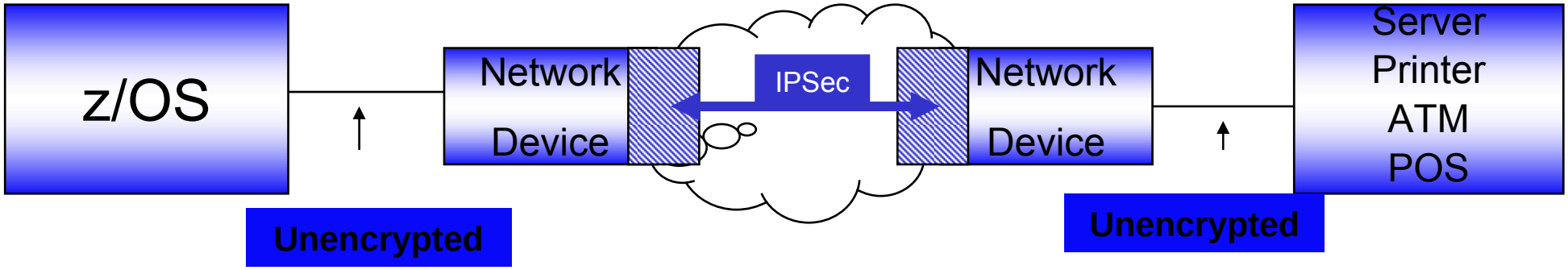
System SSL Summary

- 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

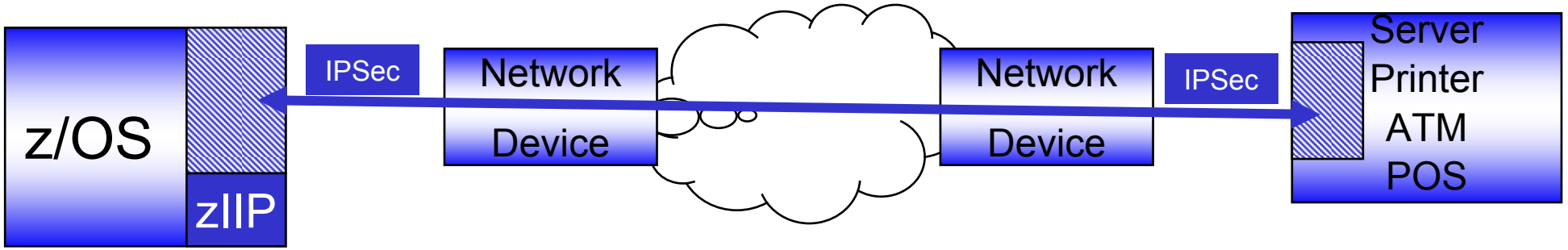
End-to-end network encryption

A compelling option to help protect sensitive data on the mainframe

- End-to-end network encryption is becoming more pervasive due to regulatory requirements and data security policies
- Growing requirement for companies that outsource some part of their network and want to control access to confidential data
- zIIP specialty engine support helps reduce the cost of adding IPSec protection



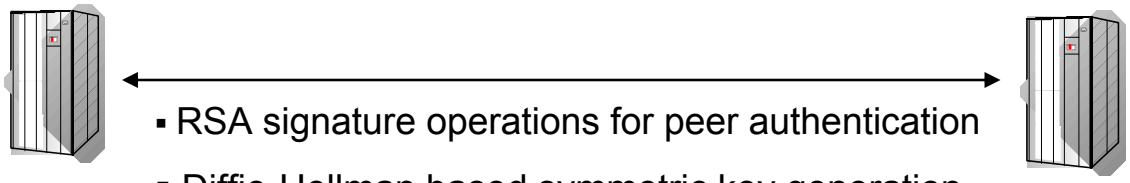
Encryption in network devices



End-to-end encryption

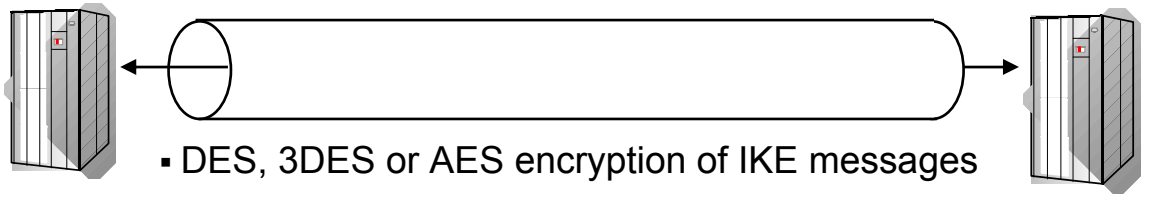
Creating IPSec Security Associations (SAs)

1 IKE peers negotiate an IKE (“phase 1”) tunnel (one bidirectional SA) over an unprotected UDP socket



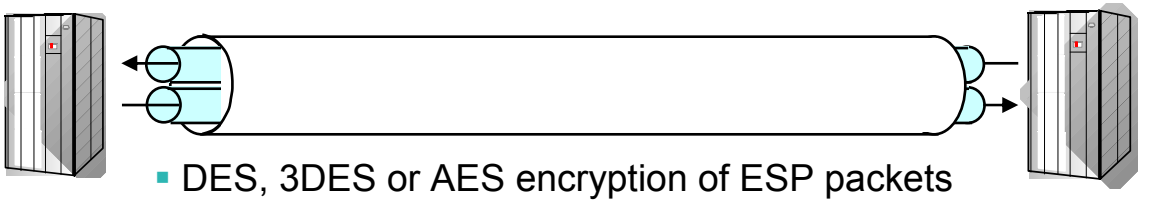
- RSA signature operations for peer authentication
- Diffie-Hellman based symmetric key generation
- IKE daemon invokes crypto operations

2 IKE peers negotiates an IPSec (“phase 2”) tunnel (two unidirectional SAs) under protection of the IKE tunnel



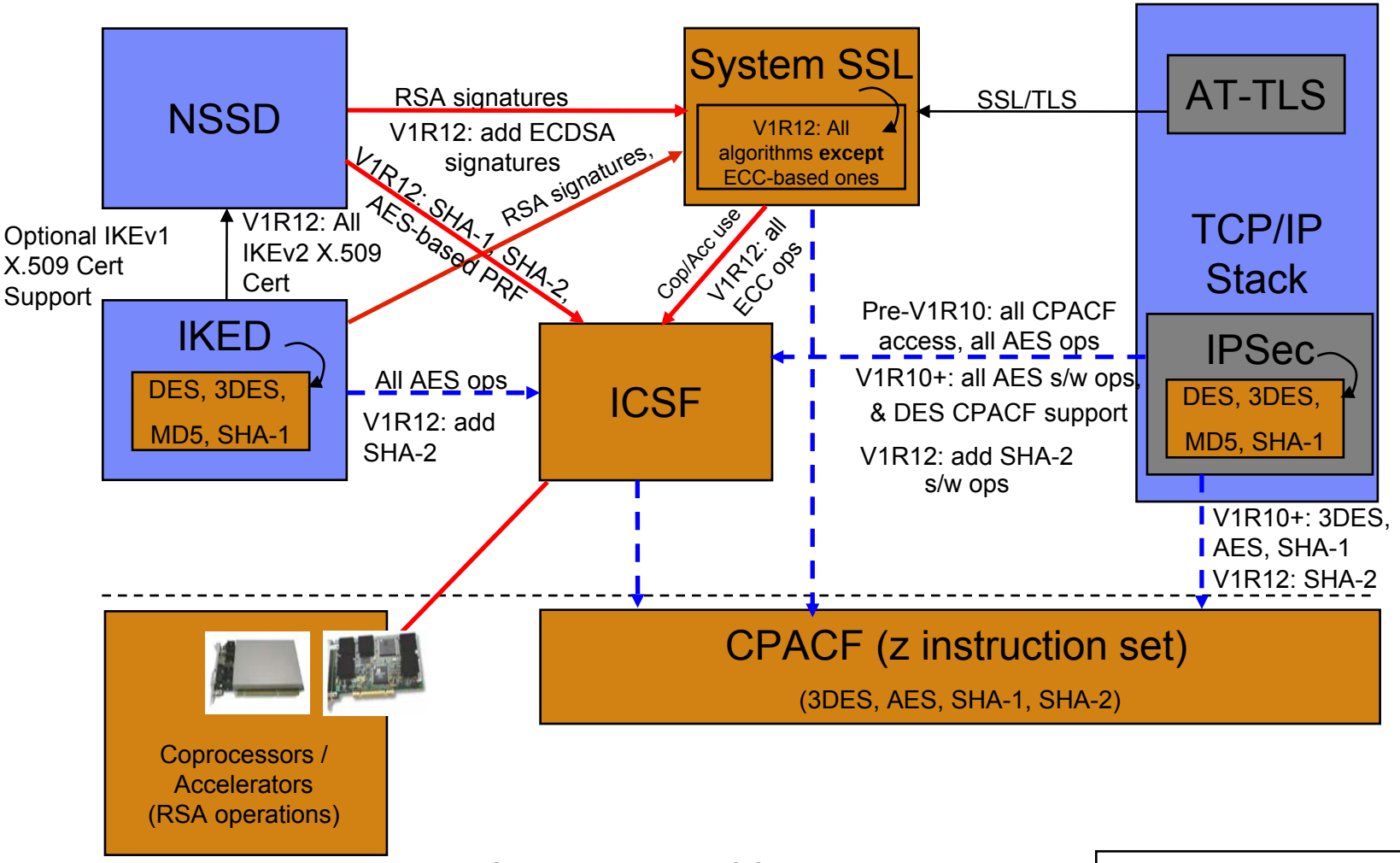
- DES, 3DES or AES encryption of IKE messages
- MD5 or SHA1 hashing for IKE message authentication
- IKE daemon invokes crypto operations

3 Data flows through IPSec tunnel using the Authentication Header (AH) and/or Encapsulating Security Payload (ESP) protocol



- DES, 3DES or AES encryption of ESP packets
- MD5 or SHA1 hashing for AH or ESP packets
- TCP/IP stack invokes crypto operations

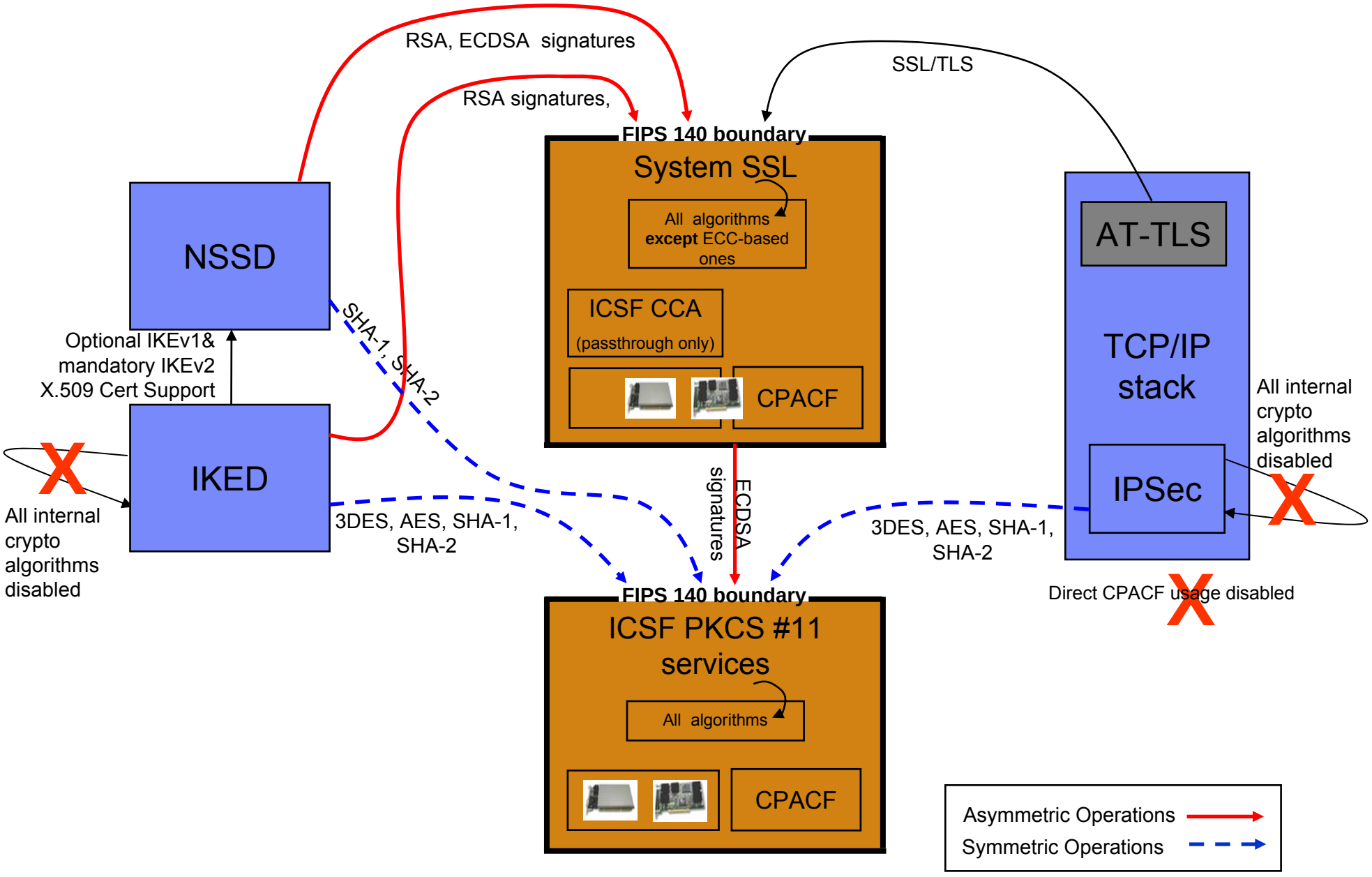
z/OS TCP/IP Cryptographic Landscape (non-FIPS)



Slides courtesy of Chris Meyer, z/OS Network Security Design

Asymmetric Operations
Symmetric Operations

z/OS TCP/IP Cryptographic Landscape (FIPS mode)



IKED hardware crypto usage (IKE)

- **RSA signature generate, signature verify for peer authentication**
  - Due to z/OS IKED single-threaded design, multiple Coprocessors or Accelerators will not provide any significant advantage for IKE operations
- **DES, 3DES, AES encryption of IKE payloads**
- **SHA-1 and MD5 HMACs for IKE message authentication**
- **SHA-2 HMACs and AES-XBC MAC for IKE message authentication (V1R12)**

Crypto Type	Algorithm	CPACF available only	CPACF + Coprocessor/Accelerator
Asymmetric Enc/Dec	Diffie-Hellman (MODP)	In software via System SSL	In software via System SSL
	EC Diffie-Hellman (requires ICSF) *	In software via ICSF	In software via ICSF
	RSA signature generation (clear key only)	In software via System SSL	In Coprocessor (not accelerator) if available (non-FIPS mode only **), otherwise in software via System SSL
	RSA signature verification	In software via System SSL	In Coprocessor/Accelerator
Symmetric Enc/Dec	DES	In software (non-FIPS mode only: DES not allowed in FIPS mode) **	
	3DES	In software (non-FIPS mode), via CPACF via ICSF (FIPS mode) **	
	AES-CBC-128 (requires ICSF)	In CPACF via ICSF	
	AES-CBC-256 (requires ICSF) *	In software on z9, CPACF in z10, all via ICSF	
Symmetric Authentication	SHA-1	In software (non-FIPS mode), via CPACF via ICSF (FIPS mode) **	
	SHA-256 (requires ICSF) *	In CPACF via ICSF	
	SHA-384, -512 (requires ICSF) *	In software on z9, CPACF in z10, all via ICSF	
	AES-XCBC (requires ICSF) *	In software via ICSF (non-FIPS mode only: FIPS 140 doesn't allow algorithm) **	
	MD5	In software (non-FIPS mode only: FIPS 140 doesn't allow algorithm) **	

* New algorithm for V1R12

** New with V1R12 FIPS 140 support

NSSD hardware crypto usage (IKE)

- **RSA and ECDSA (V1R12) signature generate, signature verify for peer authentication**
  - NSSD uses a heavily multi-threaded design so multiple Coprocessors or Accelerators can help increase throughput when IKED is acting as an NSS client.
- **SHA-1 and MD5 HMACs used in digital signature operations**
- **SHA-2 HMACs andAES-XBC MAC for IKE message authentication (V1R12)**

Crypto Type	Algorithm	CPACF available only	CPACF + Coprocessor/Accelerator
Asymmetric Encrypt/Decrypt	RSA signature generation (clear key only)	In software via System SSL	In Coprocessor (not accelerator) if available (non-FIPS mode only **), otherwise in software via System SSL
	RSA signature verification	In software via System SSL	In Coprocessor/Accelerator
	ECDSA signature operations *	In software via System SSL and ICSF	In software via System SSL and ICSF
Hashing for digital signatures	SHA-1	In CPACF via ICSF	
	SHA-256 (requires ICSF) *	In CPACF via ICSF	
	SHA-384, -512 (requires ICSF) *	In software on z9, CPACF in z10, all via ICSF	
	AES-XCBC (requires ICSF) *	In software via ICSF (non-FIPS mode only: FIPS 140 doesn't allow algorithm) **	
	MD5	In software via ICSF (non-FIPS mode only: FIPS 140 doesn't allow algorithm) **	

* New algorithm for V1R12

** New with V1R12 FIPS 140 support

Stack hardware crypto usage (IPSec: AH, ESP): Non-FIPS 140 mode

- **DES, 3DES, AES encryption of data traffic**
- **SHA-1 and MD5 HMACs for message authentication**
- **SHA-2 HMACs, AES-XCBC, and AES-GMAC MACs for message authentication (V1R12)**
- **Starting with V1R8 (APAR PK40178), all SRB-based processing in stack, *including these crypto operations*, can be offloaded to zIIP to reduce cost of IPSec protection.**

Crypto Type	Algorithm	CPACF (stack doesn't use coproc'r or accel'r)
Symmetric Enc/Dec	DES	In CPACF (via ICSF)
	3DES	In CPACF
	AES-CBC-128	In CPACF
	AES-CBC-256 *	In software via ICSF on z9, CPACF in z10
	AES-GCM-128, -256 *	In software via ICSF
Symmetric Authentication	SHA-1	In CPACF
	SHA-256 *	In CPACF
	SHA-384, -512 *	In software via ICSF on z9, CPACF in z10
	AES-XCBC MAC and AES-GMAC-128, -256 *	In software via ICSF
	MD5	In software

*** New algorithm for V1R12**

Stack hardware crypto usage (IPSec: AH, ESP): FIPS 140 mode (V1R12)

- **3DES, AES encryption of data traffic**
- **SHA-1 HMACs**
- **SHA-2 HMACs, AES-GMAC MACs for message authentication (V1R12)**
- **Note: FIPS 140 does not allow DES, MD5 or AES-XCBC**
- **All SRB-based processing in stack, *including these crypto operations*, can be offloaded to zIIP to reduce cost of IPSec protection.**

Crypto Type	Algorithm	CPACF (stack doesn't use coproc'r or accel'r)
Symmetric Enc/Dec	3DES	In CPACF via ICSF **
	AES-CBC-128	In CPACF via ICSF **
	AES-CBC-256 *	In software on z9, CPACF in z10, all via ICSF **
	AES-GCM-128, -256 *	In software via ICSF **
Symmetric Authentication	SHA-1	In CPACF via ICSF **
	SHA-256 *	In CPACF via ICSF **
	SHA-384, -512 *	In software on z9, CPACF in z10, all via ICSF **
	AES-GMAC-128, -256 *	In software via ICSF **

* New algorithm for V1R12

** New with V1R12 FIPS 140 support

References

- **For information on hardware cryptographic features reference whitepapers on Techdocs (http://www.ibm.com/support/techdocs)**
  - WP100810 – A Synopsis of System z Crypto Hardware
  - WP100647 – A Clear Key/Secure Key Primer
- **www.ieft.org/rfc.html**
  - RFC 2246, TLS Protocol Version 1.0
- **Hashing**
  - http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf (SHA-2)
  - http://www.ietf.org/rfc/rfc1321.txt?number=1321 (MD5)
- **Internet Key Exchange Daemon**
  - http://tools.ietf.org/html/rfc4306

References …..

- **Signatures**
  - http://www.itl.nist.gov/div897/pubs/fip186.htm (DSS)
  - http://www.rsa.com/rsalabs/node.asp?id=2125 (RSA)
- **Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRl Profile (RFC 3279)**
  http://www.ietf.org/mail-archive/web/ietf-announce/current/msg01889.html
- **SSL, Secure Sockets Layer**
  http://tldp.org/HOWTO/SSL-Certificates-HOWTO/x64.html
- **TLS, Transport Layer Security**
  http://www.ietf.org/rfc/rfc2246.txt
- **X.509 certificate, certificate revocation list, and certificate extensions**
  http://www.ietf.org/internet-drafts/draft-ietf-pkix-rfc3280bis-11.txt

Questions