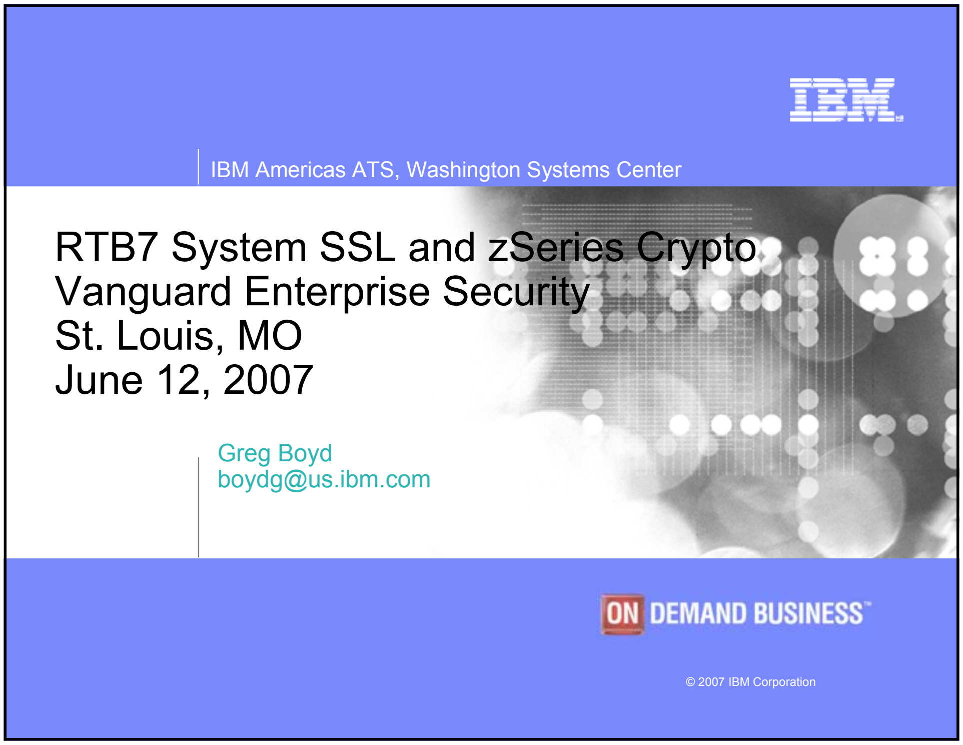
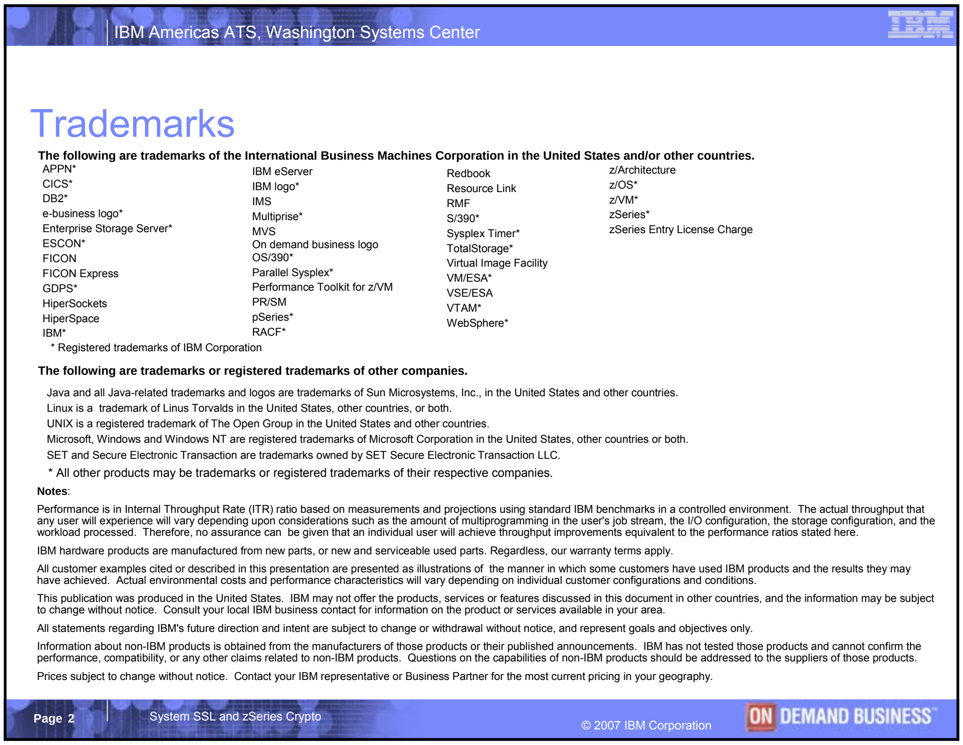


# RTB7 System SSL and zSeries Crypto
Vanguard Enterprise Security
St. Louis, MO
June 12, 2007

Greg Boyd
boydg@us.ibm.com



## Trademarks

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

APPN*
CICS*
DB2*
e-business logo*
Enterprise Storage Server*
ESCON*
FICON
FICON Express
GDPS*
HiperSockets
HiperSpace
IBM*
IBM eServer
IBM logo*
IMS
Multiprise*
MVS
On demand business logo
OS/390*
Parallel Sysplex*
Performance Toolkit for z/VM
PR/SM
pSeries*
RACF*
Redbook
Resource Link
RMF
S/390*
Sysplex Timer*
TotalStorage*
Virtual Image Facility
VM/ESA*
VSE/ESA
VTAM*
WebSphere*
z/Architecture
z/OS*
z/VM*
zSeries*
zSeries Entry License Charge

* Registered trademarks of IBM Corporation

**The following are trademarks or registered trademarks of other companies.**

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.
Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries or both.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* 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.

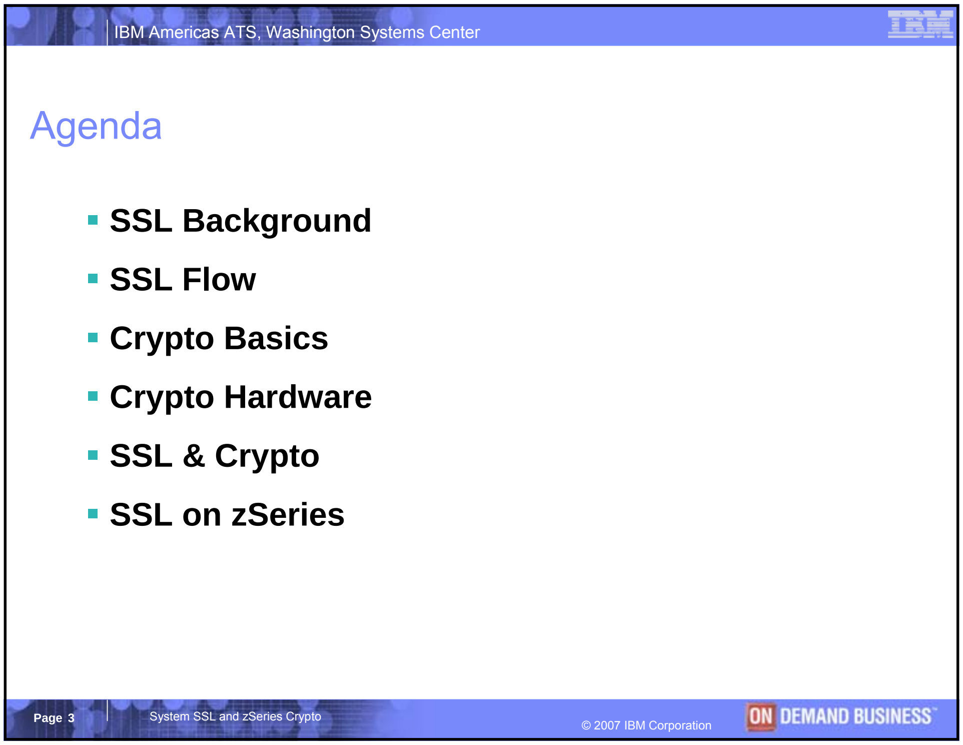
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations 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.

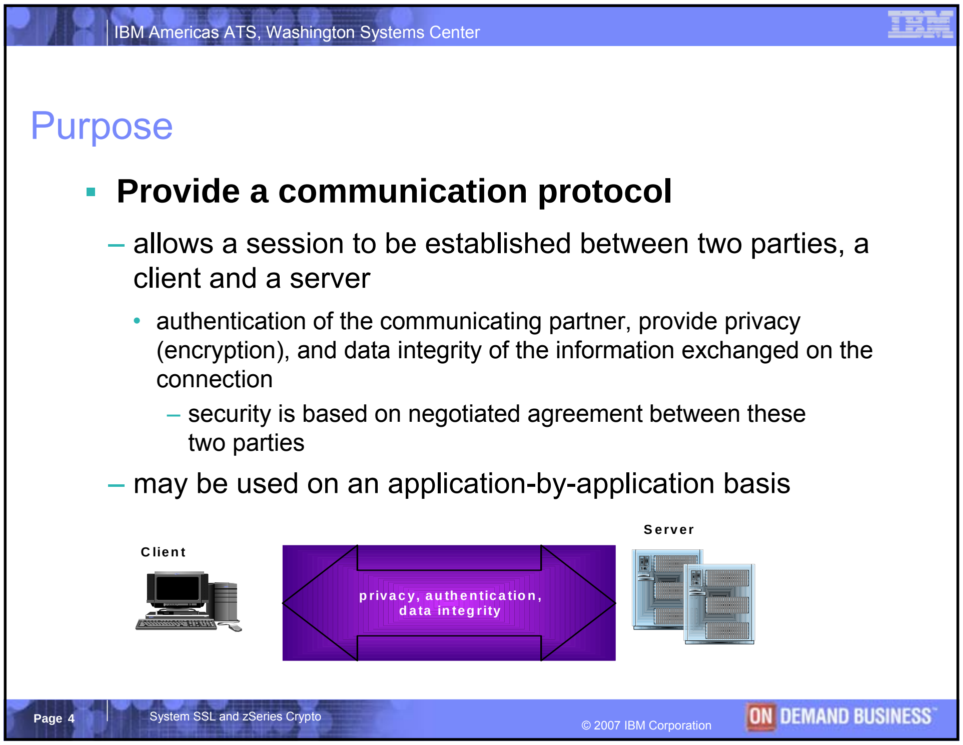
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products 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.



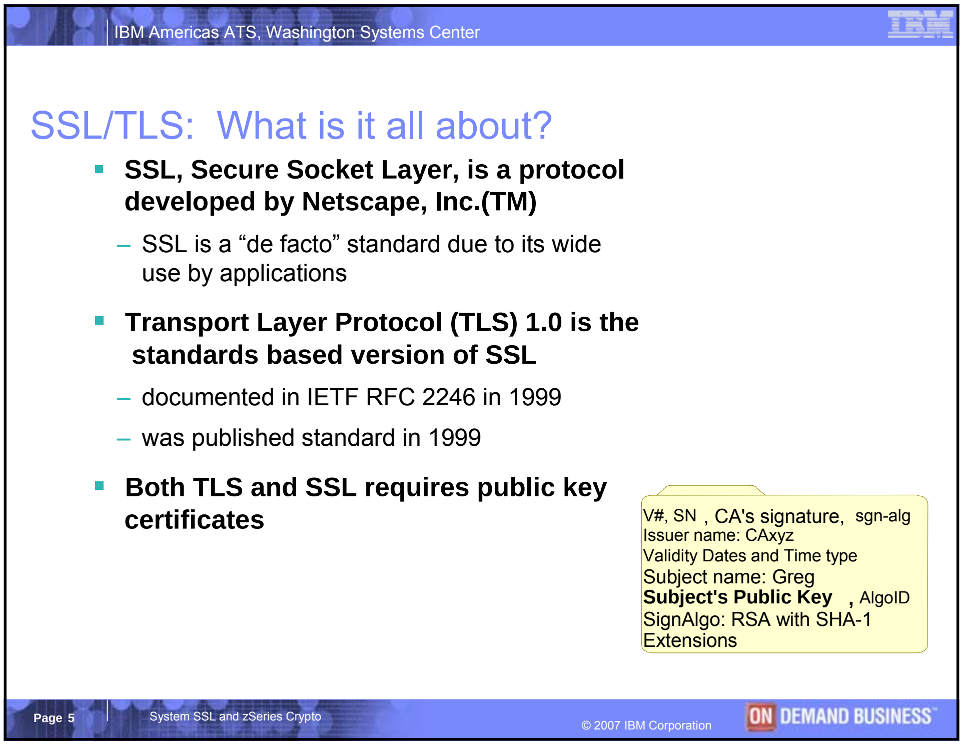
# Agenda

- SSL Background
- SSL Flow
- Crypto Basics
- Crypto Hardware
- SSL & Crypto
- SSL on zSeries



# Purpose

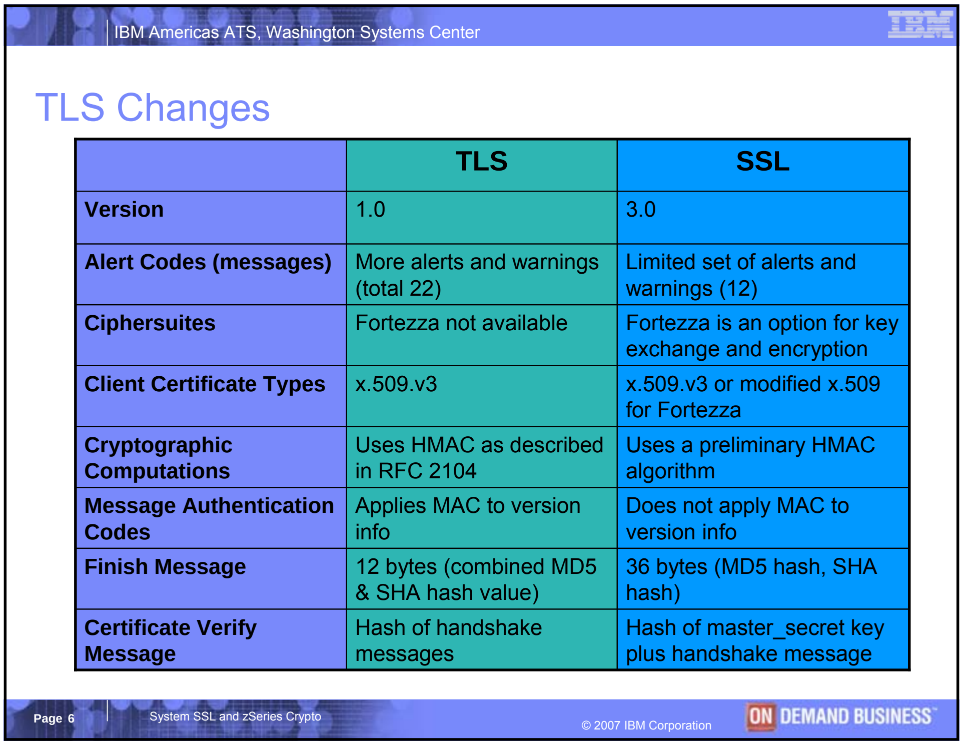
- **Provide a communication protocol**
  - allows a session to be established between two parties, a client and a server
    - authentication of the communicating partner, provide privacy (encryption), and data integrity of the information exchanged on the connection
      - security is based on negotiated agreement between these two parties
  - may be used on an application-by-application basis



## SSL/TLS: What is it all about?

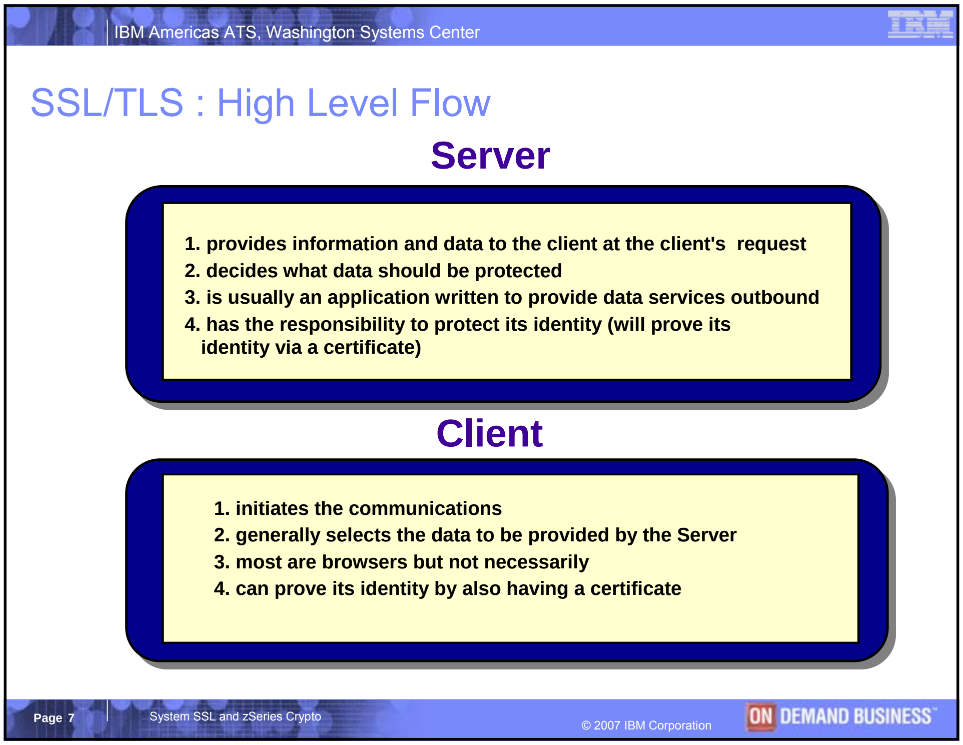
- **SSL, Secure Socket Layer, is a protocol developed by Netscape, Inc.(TM)**
  - SSL is a “de facto” standard due to its wide use by applications
- **Transport Layer Protocol (TLS) 1.0 is the standards based version of SSL**
  - documented in IETF RFC 2246 in 1999
  - was published standard in 1999
- **Both TLS and SSL requires public key certificates**

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



## TLS Changes

| | TLS | SSL |
|---|---|---|
| **Version** | 1.0 | 3.0 |
| **Alert Codes (messages)** | More alerts and warnings (total 22) | Limited set of alerts and warnings (12) |
| **Ciphersuites** | Fortezza not available | Fortezza is an option for key exchange and encryption |
| **Client Certificate Types** | x.509.v3 | x.509.v3 or modified x.509 for Fortezza |
| **Cryptographic Computations** | Uses HMAC as described in RFC 2104 | Uses a preliminary HMAC algorithm |
| **Message Authentication Codes** | Applies MAC to version info | Does not apply MAC to version info |
| **Finish Message** | 12 bytes (combined MD5 & SHA hash value) | 36 bytes (MD5 hash, SHA hash) |
| **Certificate Verify Message** | Hash of handshake messages | Hash of master_secret key plus handshake message |



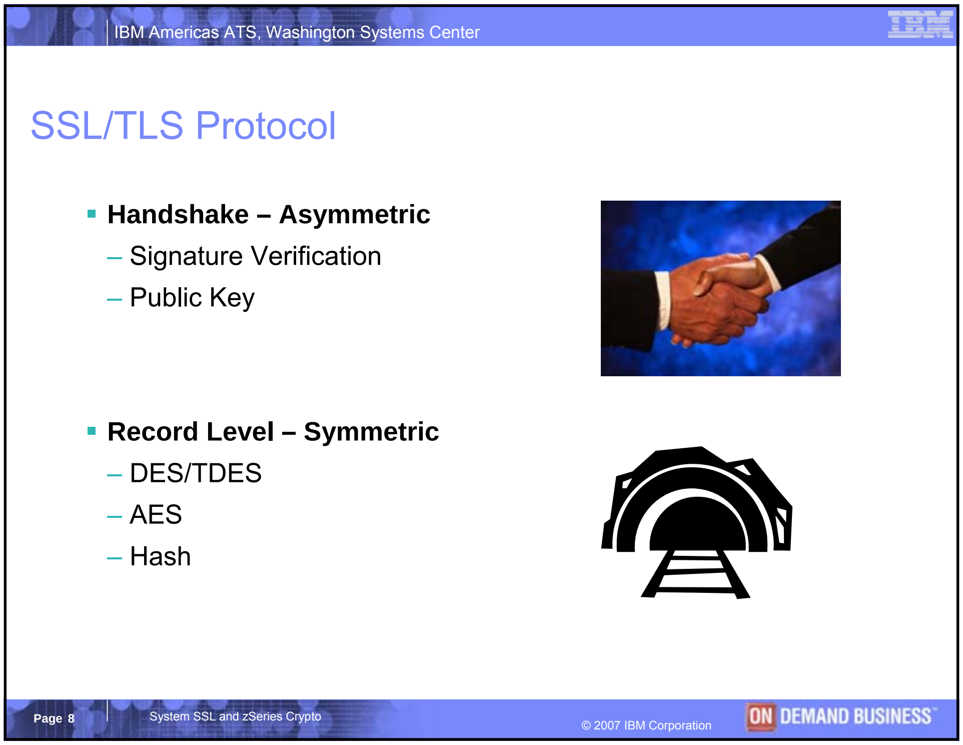
## SSL/TLS : High Level Flow

### 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)

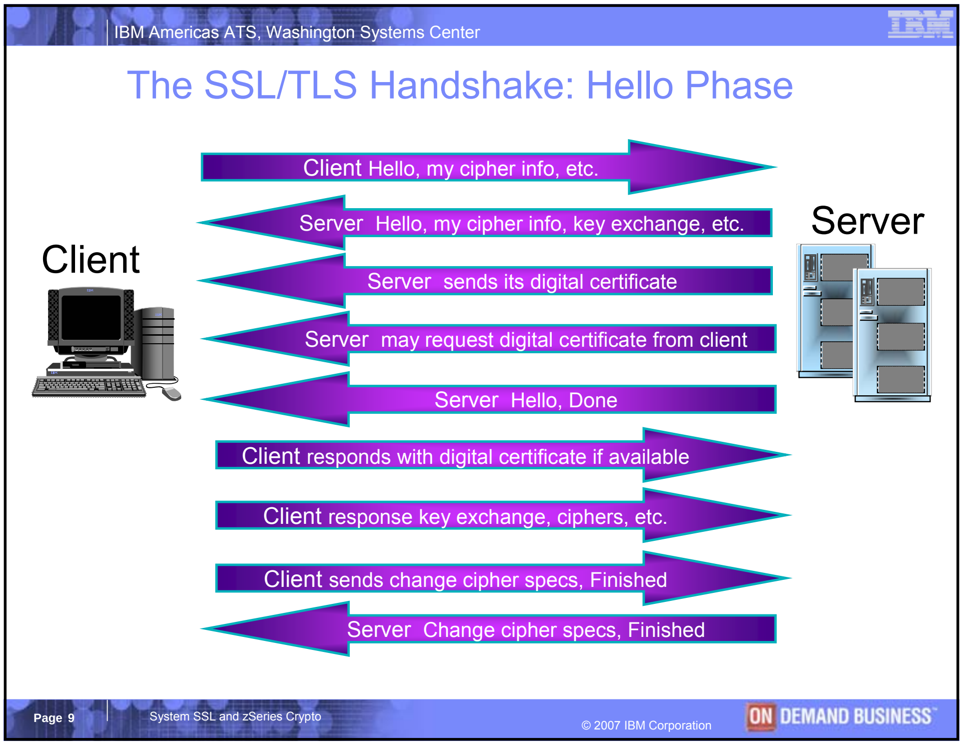
### Client

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



## SSL/TLS Protocol

- **Handshake – Asymmetric**
  - Signature Verification
  - Public Key
- **Record Level – Symmetric**
  - DES/TDES
  - AES
  - Hash



## The SSL/TLS Handshake: Hello Phase

Client Hello, my cipher info, etc.

Server Hello, my cipher info, key exchange, etc.

Server sends its digital certificate

Server may request digital certificate from client

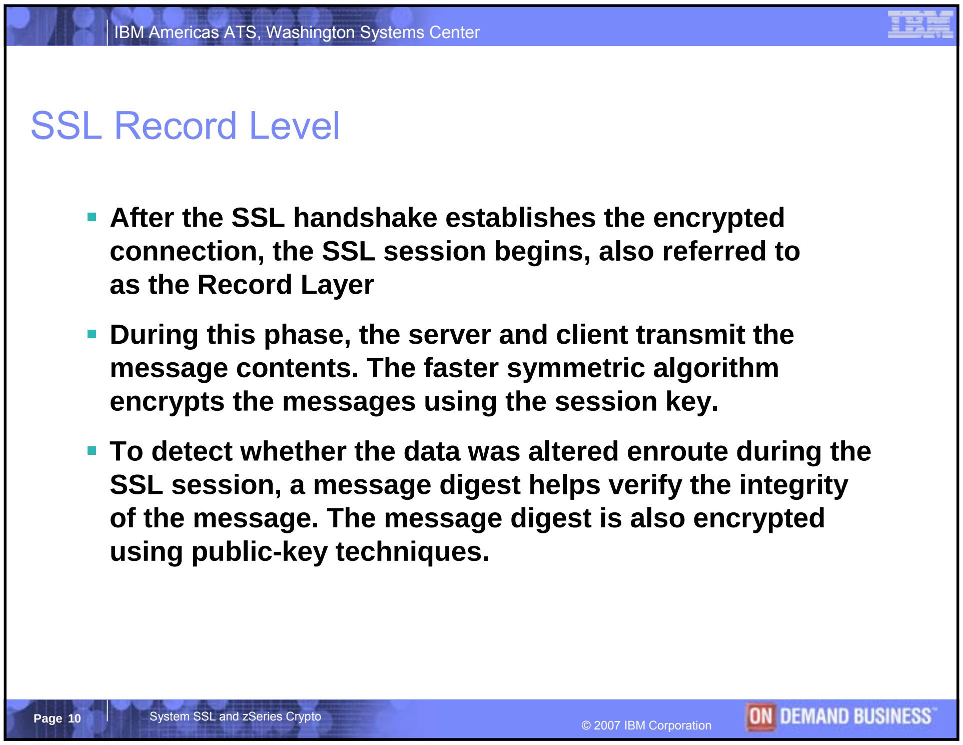
Server Hello, Done

Client responds with digital certificate if available

Client response key exchange, ciphers, etc.

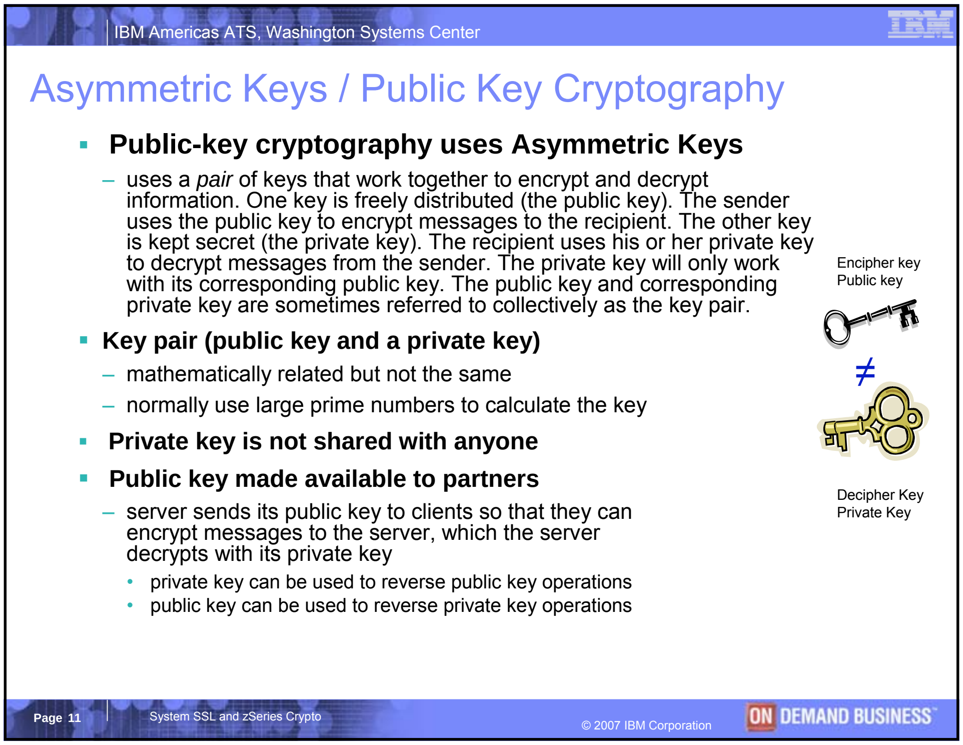
Client sends change cipher specs, Finished

Server Change cipher specs, Finished



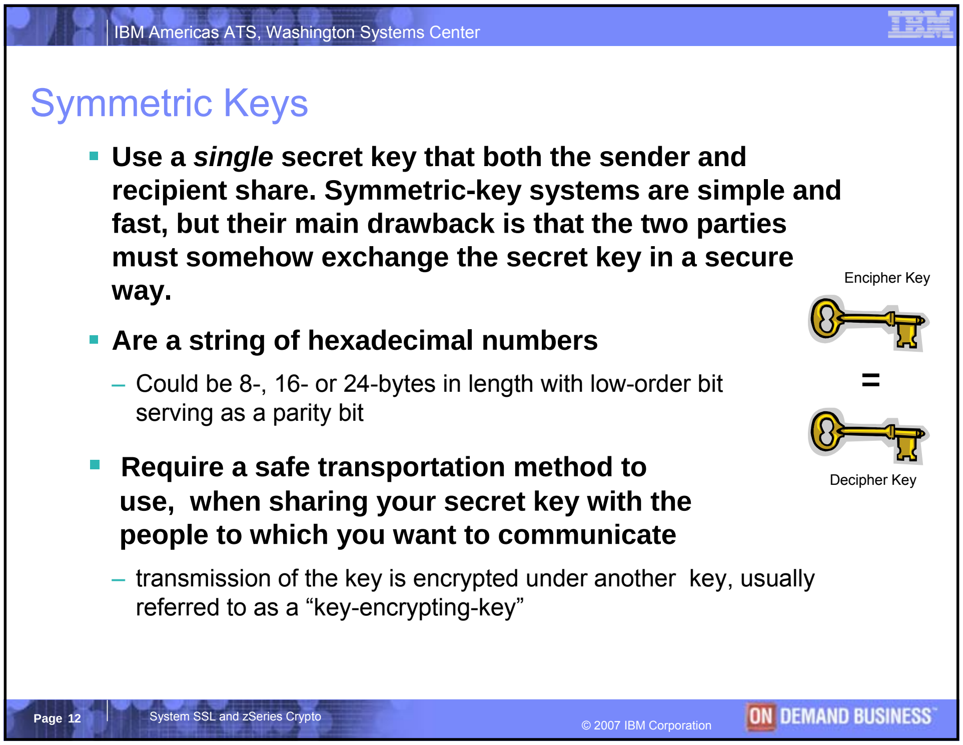
## SSL Record Level

- **After the SSL handshake establishes the encrypted connection, the SSL session begins, also referred to as the Record Layer**
- **During this phase, the server and client transmit the message contents. The faster symmetric algorithm encrypts the messages using the session key.**
- **To detect whether the data was altered enroute during the SSL session, a message digest helps verify the integrity of the message. The message digest is also encrypted using public-key techniques.**



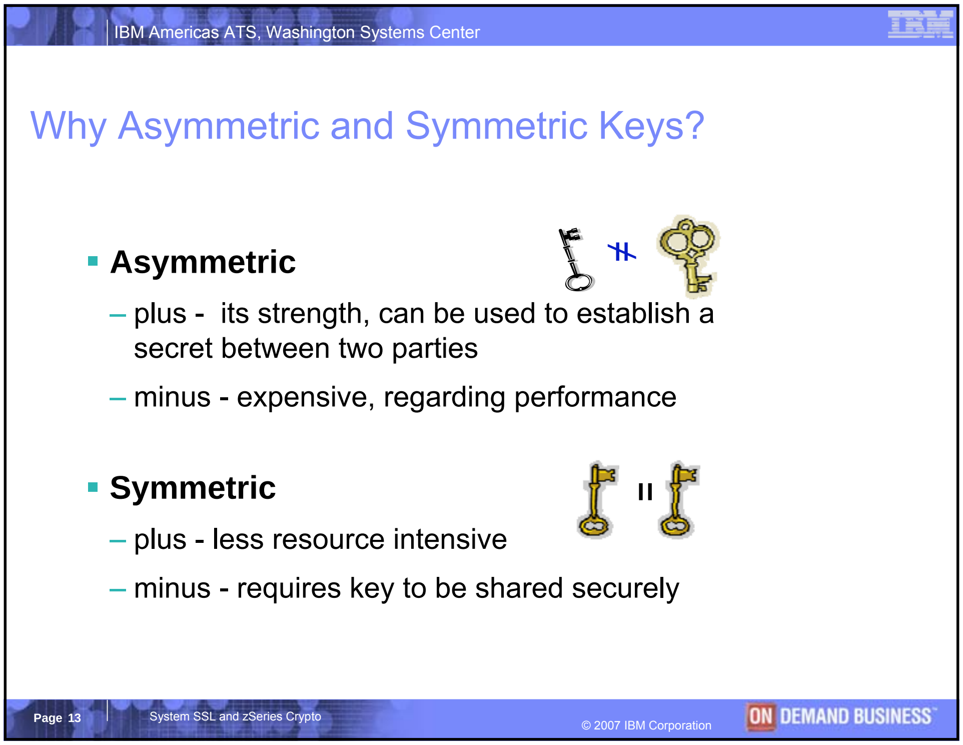
## Asymmetric Keys / Public Key Cryptography

- **Public-key cryptography uses Asymmetric Keys**
  - uses a *pair* of keys that work together to encrypt and decrypt information. One key is freely distributed (the public key). The sender uses the public key to encrypt messages to the recipient. The other key is kept secret (the private key). The recipient uses his or her private key to decrypt messages from the sender. The private key will only work with its corresponding public key. The public key and corresponding private key are sometimes referred to collectively as the key pair.
- **Key pair (public key and a private key)**
  - mathematically related but not the same
  - normally use large prime numbers to calculate the key
- **Private key is not shared with anyone**
- **Public key made available to partners**
  - server sends its public key to clients so that they can encrypt messages to the server, which the server decrypts with its private key
    - private key can be used to reverse public key operations
    - public key can be used to reverse private key operations



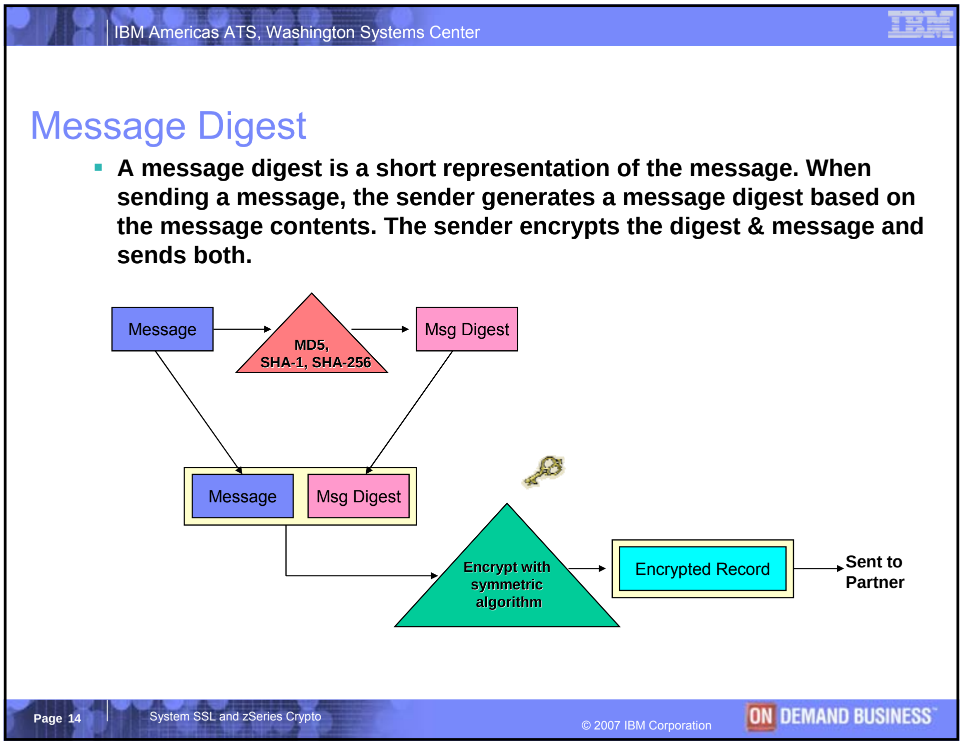
## Symmetric Keys

- **Use a *single* secret key that both the sender and recipient share. Symmetric-key systems are simple and fast, but their main drawback is that the two parties must somehow exchange the secret key in a secure way.**
- **Are a string of hexadecimal numbers**
  - Could be 8-, 16- or 24-bytes in length with low-order bit serving as a parity bit
- **Require a safe transportation method to use, when sharing your secret key with the people to which you want to communicate**
  - transmission of the key is encrypted under another key, usually referred to as a “key-encrypting-key”



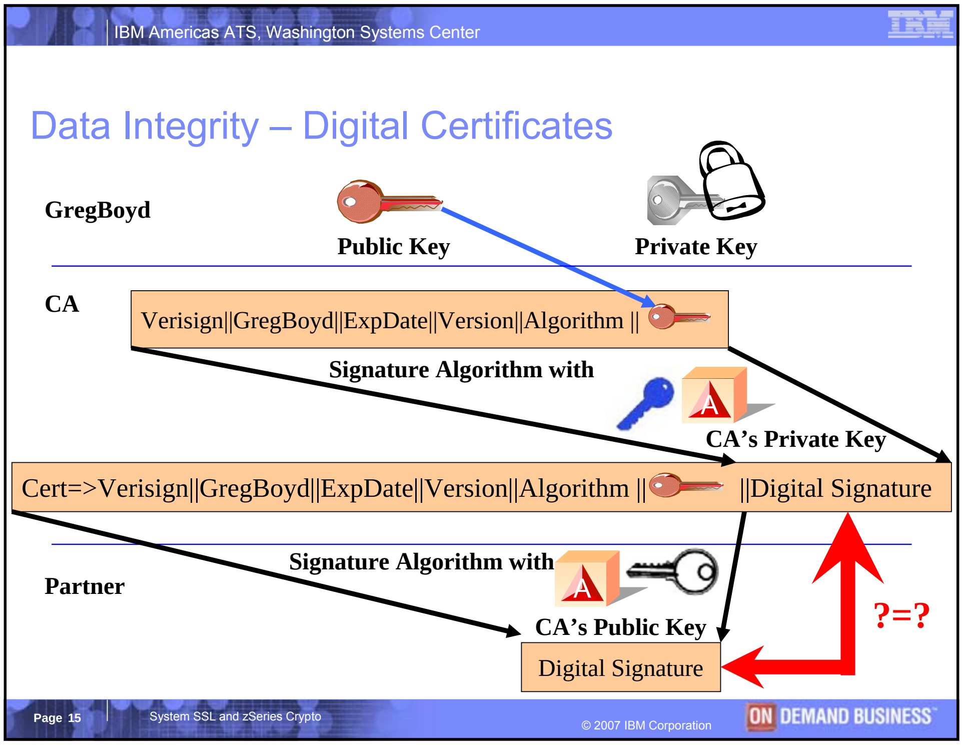
## Why Asymmetric and Symmetric Keys?

- **Asymmetric** ≠
  - plus - its strength, can be used to establish a secret between two parties
  - minus - expensive, regarding performance
- **Symmetric** =
  - plus - less resource intensive
  - minus - requires key to be shared securely



## Message Digest

- **A message digest is a short representation of the message. When sending a message, the sender generates a message digest based on the message contents. The sender encrypts the digest & message and sends both.**



## Data Integrity – Digital Certificates

GregBoyd

Public Key

Private Key

CA

Verisign||GregBoyd||ExpDate||Version||Algorithm ||

Signature Algorithm with

CA's Private Key

Cert=>Verisign||GregBoyd||ExpDate||Version||Algorithm || ||Digital Signature

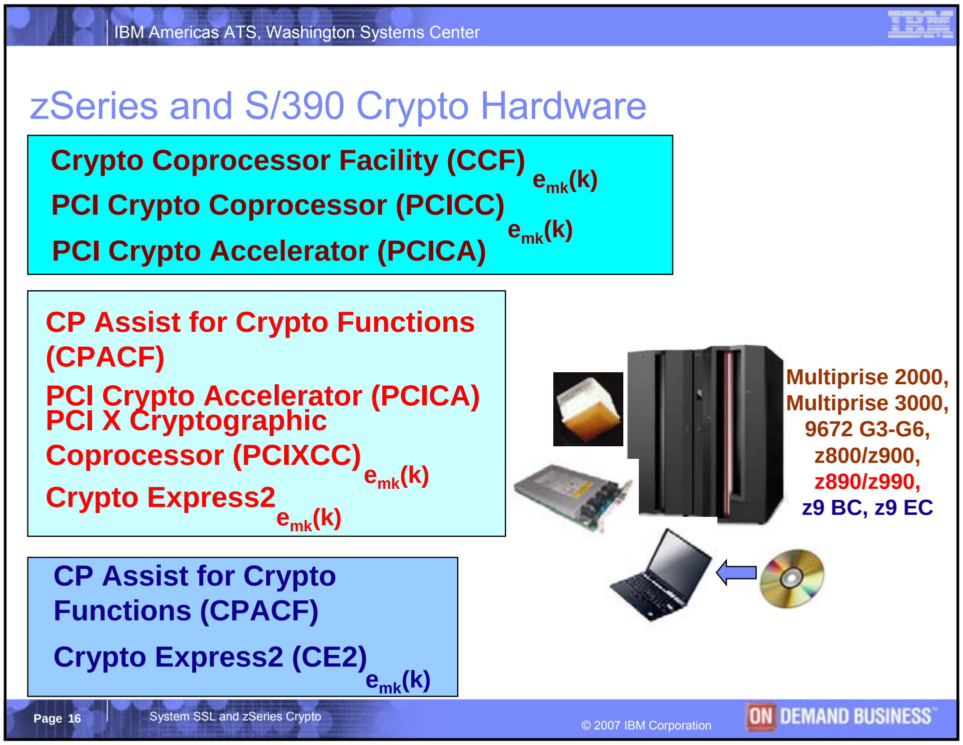
Partner

Signature Algorithm with

CA's Public Key

Digital Signature

?=?



## zSeries and S/390 Crypto Hardware

Crypto Coprocessor Facility (CCF) $e_{mk}(k)$

PCI Crypto Coprocessor (PCICC) $e_{mk}(k)$

PCI Crypto Accelerator (PCICA)

CP Assist for Crypto Functions (CPACF)

PCI Crypto Accelerator (PCICA)

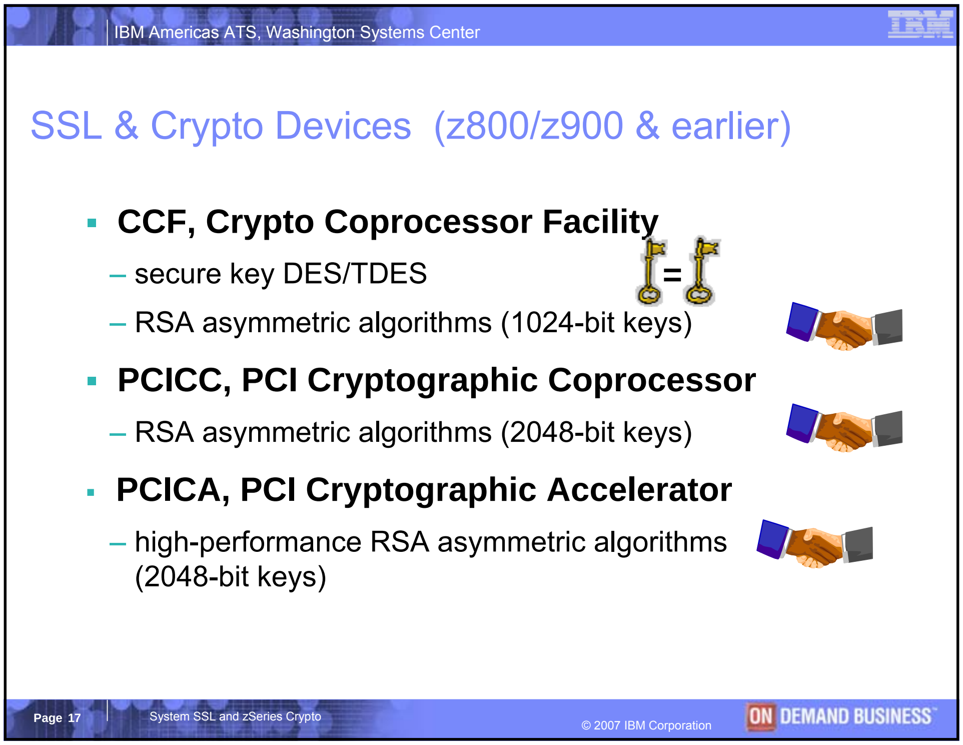
PCI X Cryptographic Coprocessor (PCIXCC) $e_{mk}(k)$

Crypto Express2 $e_{mk}(k)$

CP Assist for Crypto Functions (CPACF)

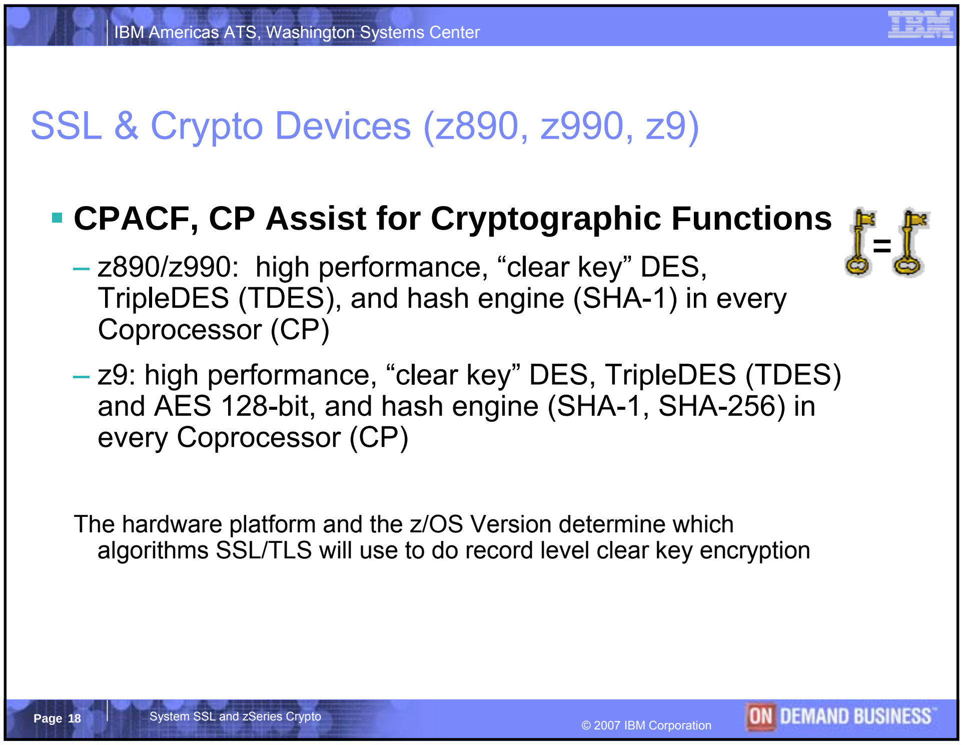
Crypto Express2 (CE2) $e_{mk}(k)$

Multiprise 2000,
Multiprise 3000,
9672 G3-G6,
z800/z900,
z890/z990,
z9 BC, z9 EC



## SSL & Crypto Devices (z800/z900 & earlier)

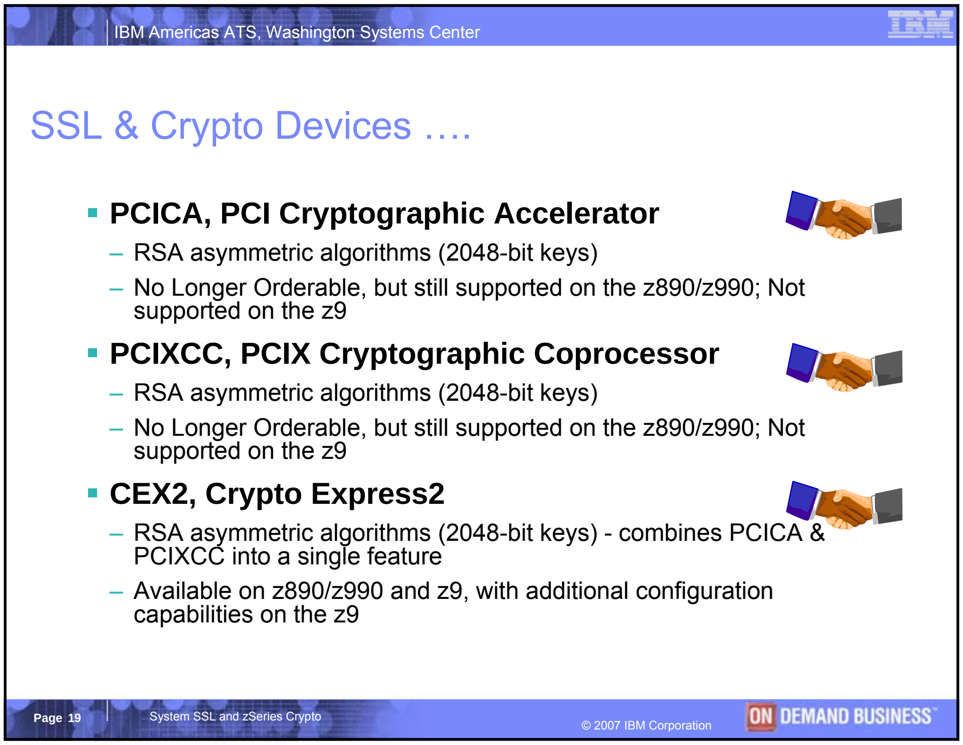
- **CCF, Crypto Coprocessor Facility**
  - secure key DES/TDES
  - RSA asymmetric algorithms (1024-bit keys)
- **PCICC, PCI Cryptographic Coprocessor**
  - RSA asymmetric algorithms (2048-bit keys)
- **PCICA, PCI Cryptographic Accelerator**
  - high-performance RSA asymmetric algorithms (2048-bit keys)



## SSL & Crypto Devices (z890, z990, z9)

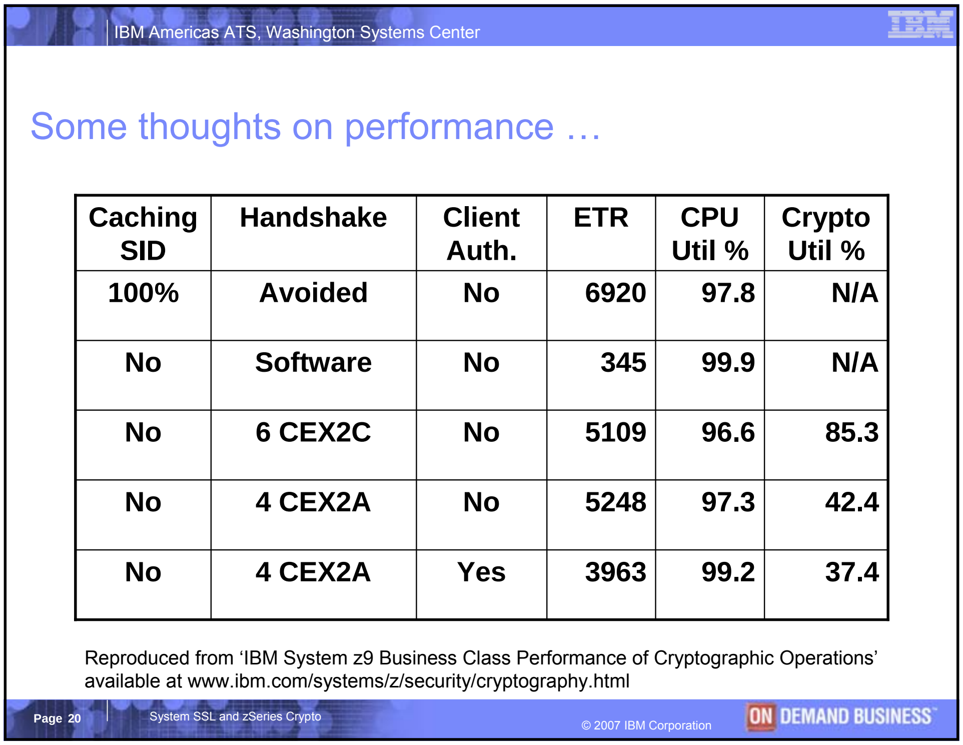
- **CPACF, CP Assist for Cryptographic Functions**
  - z890/z990: high performance, “clear key” DES, TripleDES (TDES), and hash engine (SHA-1) in every Coprocessor (CP)
  - z9: high performance, “clear key” DES, TripleDES (TDES) and AES 128-bit, and hash engine (SHA-1, SHA-256) in every Coprocessor (CP)

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 ….

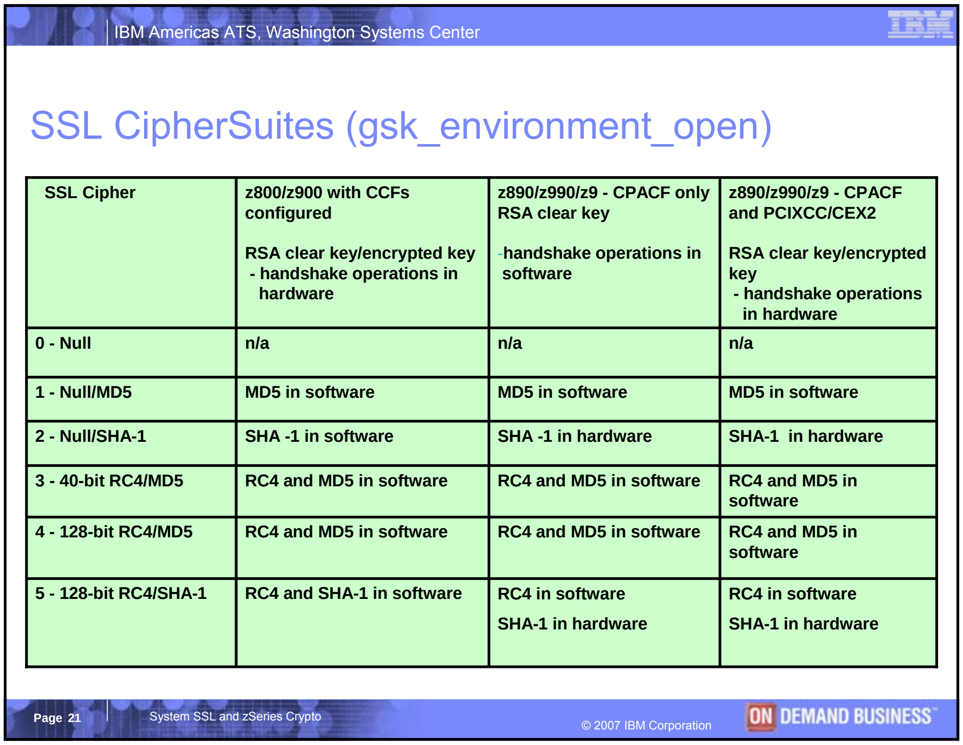
- **PCICA, PCI Cryptographic Accelerator**
  - RSA asymmetric algorithms (2048-bit keys)
  - No Longer Orderable, but still supported on the z890/z990; Not supported on the z9
- **PCIXCC, PCIX Cryptographic Coprocessor**
  - RSA asymmetric algorithms (2048-bit keys)
  - No Longer Orderable, but still supported on the z890/z990; Not supported on the z9
- **CEX2, Crypto Express2**
  - RSA asymmetric algorithms (2048-bit keys) - combines PCICA & PCIXCC into a single feature
  - Available on z890/z990 and z9, with additional configuration capabilities on the z9



## Some thoughts on performance …

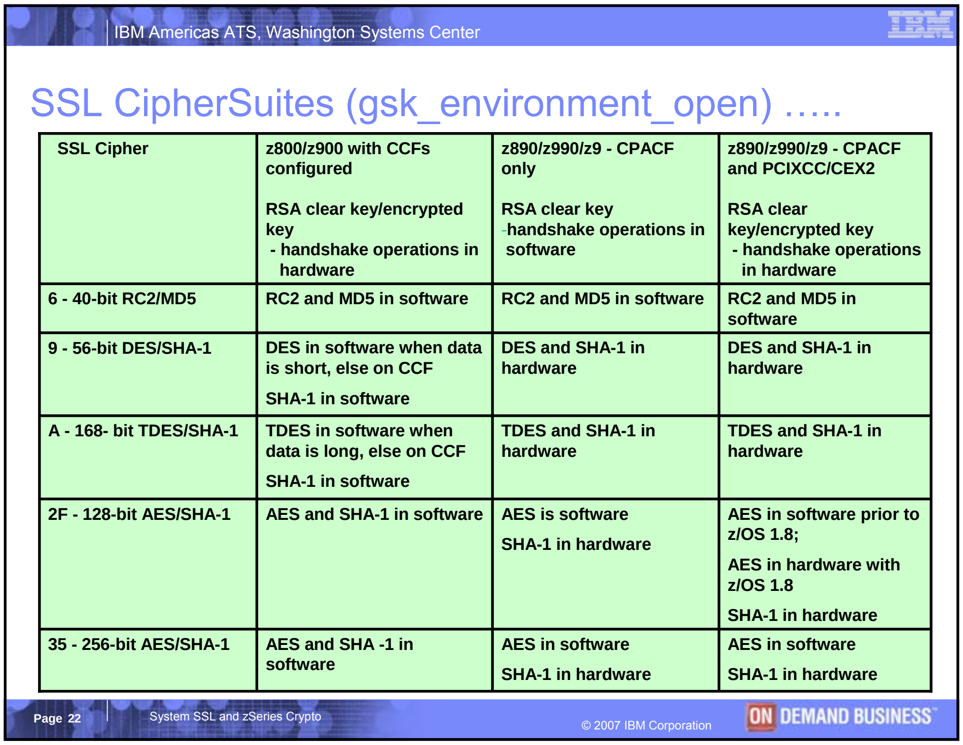
| Caching SID | Handshake | Client Auth. | ETR | CPU Util % | Crypto Util % |
|---|---|---|---|---|---|
| 100% | Avoided | No | 6920 | 97.8 | N/A |
| No | Software | No | 345 | 99.9 | N/A |
| No | 6 CEX2C | No | 5109 | 96.6 | 85.3 |
| No | 4 CEX2A | No | 5248 | 97.3 | 42.4 |
| No | 4 CEX2A | Yes | 3963 | 99.2 | 37.4 |

Reproduced from 'IBM System z9 Business Class Performance of Cryptographic Operations' available at www.ibm.com/systems/z/security/cryptography.html



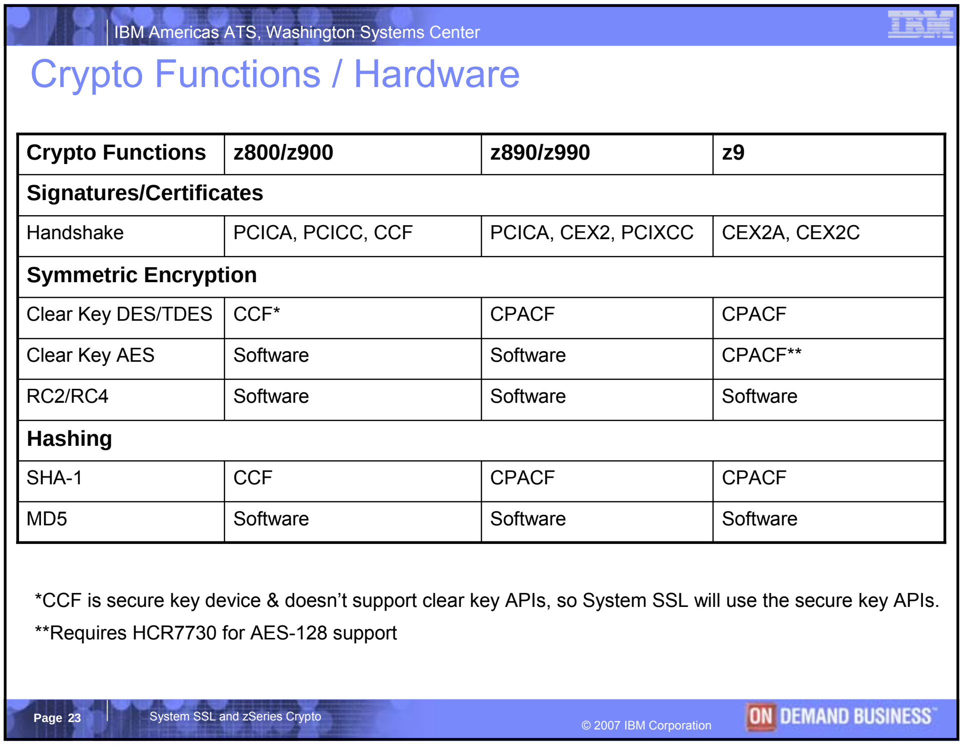
## SSL CipherSuites (gsk_environment_open)

| SSL Cipher | z800/z900 with CCFs configured<br>RSA clear key/encrypted key - handshake operations in hardware | z890/z990/z9 - CPACF only RSA clear key<br>-handshake operations in software | z890/z990/z9 - CPACF and PCIXCC/CEX2<br>RSA clear key/encrypted key - handshake operations in hardware |
|---|---|---|---|
| 0 - Null | n/a | n/a | n/a |
| 1 - Null/MD5 | MD5 in software | MD5 in software | MD5 in software |
| 2 - Null/SHA-1 | SHA -1 in software | SHA -1 in hardware | SHA-1 in hardware |
| 3 - 40-bit RC4/MD5 | RC4 and MD5 in software | RC4 and MD5 in software | RC4 and MD5 in software |
| 4 - 128-bit RC4/MD5 | RC4 and MD5 in software | RC4 and MD5 in software | RC4 and MD5 in software |
| 5 - 128-bit RC4/SHA-1 | RC4 and SHA-1 in software | RC4 in software<br>SHA-1 in hardware | RC4 in software<br>SHA-1 in hardware |



## SSL CipherSuites (gsk_environment_open) …..

| SSL Cipher | z800/z900 with CCFs configured<br>RSA clear key/encrypted key - handshake operations in hardware | z890/z990/z9 - CPACF only<br>RSA clear key -handshake operations in software | z890/z990/z9 - CPACF and PCIXCC/CEX2<br>RSA clear key/encrypted key - handshake operations in hardware |
|---|---|---|---|
| 6 - 40-bit RC2/MD5 | RC2 and MD5 in software | RC2 and MD5 in software | RC2 and MD5 in software |
| 9 - 56-bit DES/SHA-1 | DES in software when data is short, else on CCF<br>SHA-1 in software | DES and SHA-1 in hardware | DES and SHA-1 in hardware |
| A - 168- bit TDES/SHA-1 | TDES in software when data is long, else on CCF<br>SHA-1 in software | TDES and SHA-1 in hardware | TDES and SHA-1 in hardware |
| 2F - 128-bit AES/SHA-1 | AES and SHA-1 in software | AES is software<br>SHA-1 in hardware | AES in software prior to z/OS 1.8;<br>AES in hardware with z/OS 1.8<br>SHA-1 in hardware |
| 35 - 256-bit AES/SHA-1 | AES and SHA -1 in software | AES in software<br>SHA-1 in hardware | AES in software<br>SHA-1 in hardware |

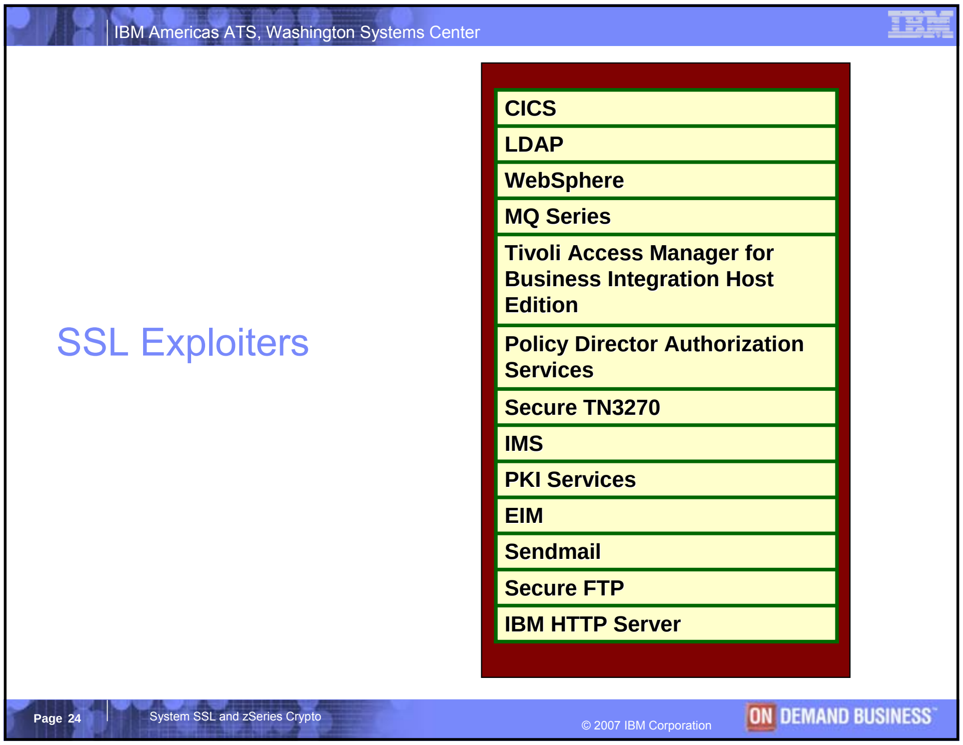


# Crypto Functions / Hardware

| Crypto Functions | z800/z900 | z890/z990 | z9 |
|---|---|---|---|
| **Signatures/Certificates** | | | |
| Handshake | PCICA, PCICC, CCF | PCICA, CEX2, PCIXCC | CEX2A, CEX2C |
| **Symmetric Encryption** | | | |
| Clear Key DES/TDES | CCF* | CPACF | CPACF |
| Clear Key AES | Software | Software | CPACF** |
| RC2/RC4 | Software | Software | Software |
| **Hashing** | | | |
| SHA-1 | CCF | CPACF | CPACF |
| MD5 | Software | Software | Software |

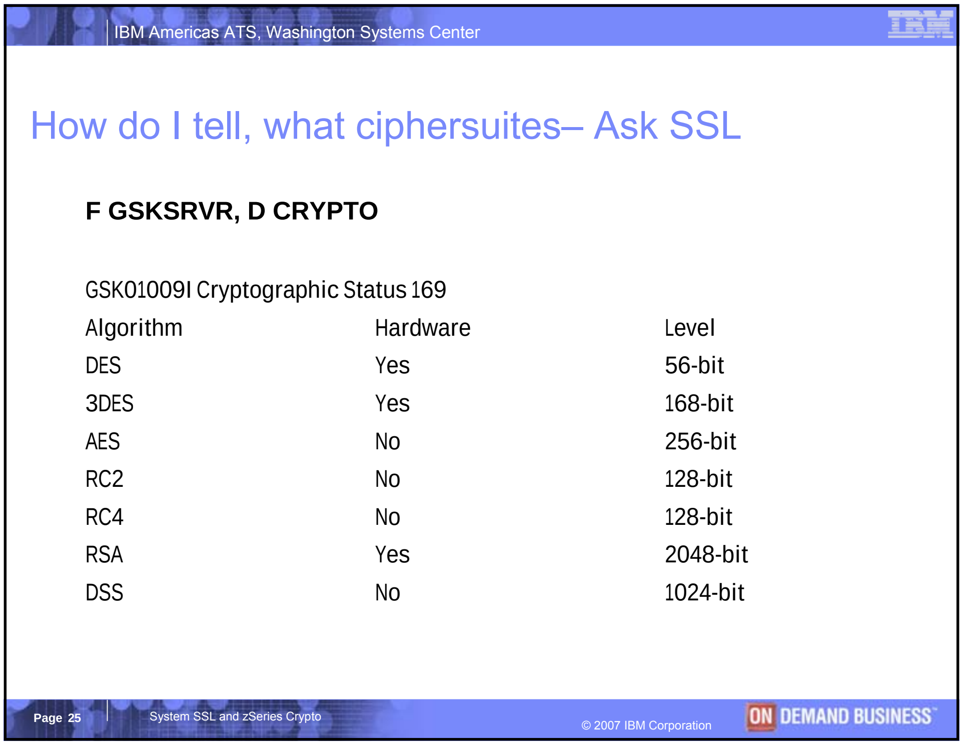
*CCF is secure key device & doesn't support clear key APIs, so System SSL will use the secure key APIs.

**Requires HCR7730 for AES-128 support



# 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**
- **IBM HTTP Server**

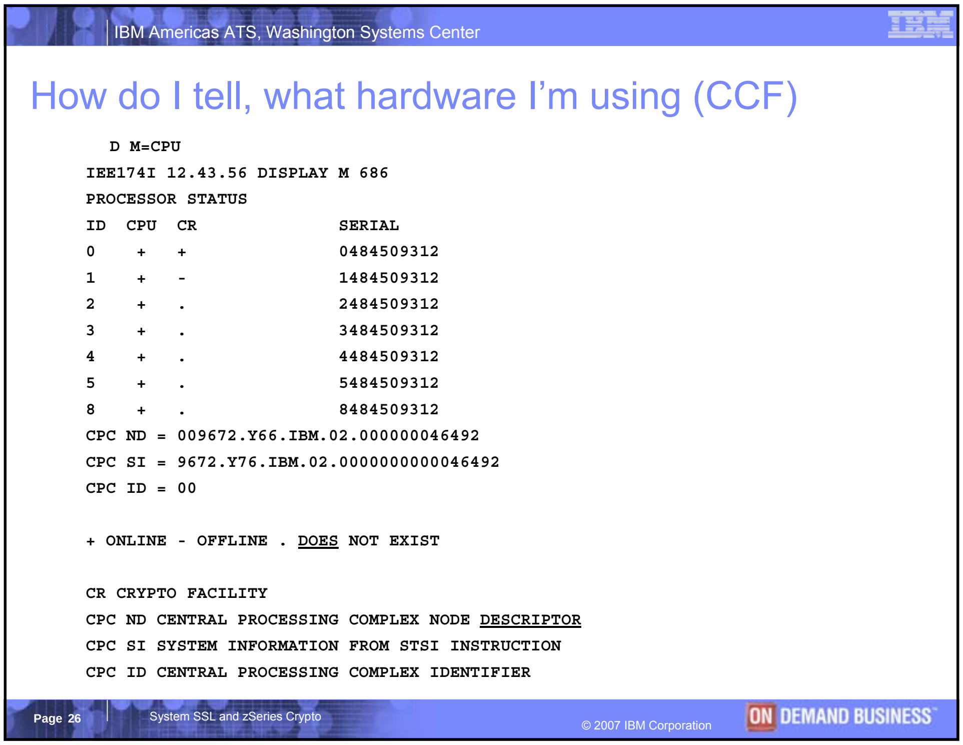


## How do I tell, what ciphersuites– Ask SSL

**F GSKSRVR, D CRYPTO**

GSK01009I Cryptographic Status 169

| Algorithm | Hardware | Level |
|---|---|---|
| DES | Yes | 56-bit |
| 3DES | Yes | 168-bit |
| AES | No | 256-bit |
| RC2 | No | 128-bit |
| RC4 | No | 128-bit |
| RSA | Yes | 2048-bit |
| DSS | No | 1024-bit |



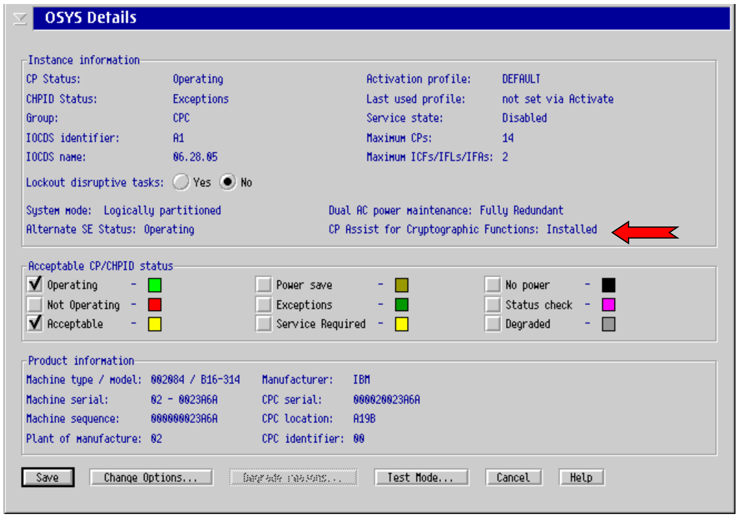
## How do I tell, what hardware I'm using (CCF)

```
  D M=CPU
IEE174I 12.43.56 DISPLAY M 686
PROCESSOR STATUS
ID  CPU  CR             SERIAL
0    +   +              0484509312
1    +   -              1484509312
2    +   .              2484509312
3    +   .              3484509312
4    +   .              4484509312
5    +   .              5484509312
8    +   .              8484509312
CPC ND = 009672.Y66.IBM.02.000000046492
CPC SI = 9672.Y76.IBM.02.0000000000046492
CPC ID = 00

+ ONLINE - OFFLINE . DOES NOT EXIST

CR CRYPTO FACILITY
CPC ND CENTRAL PROCESSING COMPLEX NODE DESCRIPTOR
CPC SI SYSTEM INFORMATION FROM STSI INSTRUCTION
CPC ID CENTRAL PROCESSING COMPLEX IDENTIFIER
```

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



**OSYS Details**

Instance information

CP Status: Operating — Activation profile: DEFAULT

CHPID Status: Exceptions — Last used profile: not set via Activate

Group: CPC — Service state: Disabled

IOCDS identifier: A1 — Maximum CPs: 14

IOCDS name: 06.28.05 — Maximum ICFs/IFLs/IFAs: 2

Lockout disruptive tasks: ○ Yes ● No

System mode: Logically partitioned — Dual AC power maintenance: Fully Redundant

Alternate SE Status: Operating — CP Assist for Cryptographic Functions: Installed

Acceptable CP/CHPID status

| | | |
|---|---|---|
| ☑ Operating - 🟩 | □ Power save - 🟫 | □ No power - ⬛ |
| □ Not Operating - 🟥 | □ Exceptions - 🟩 | □ Status check - 🟪 |
| ☑ Acceptable - 🟨 | □ Service Required - 🟨 | □ Degraded - ▨ |

Product information

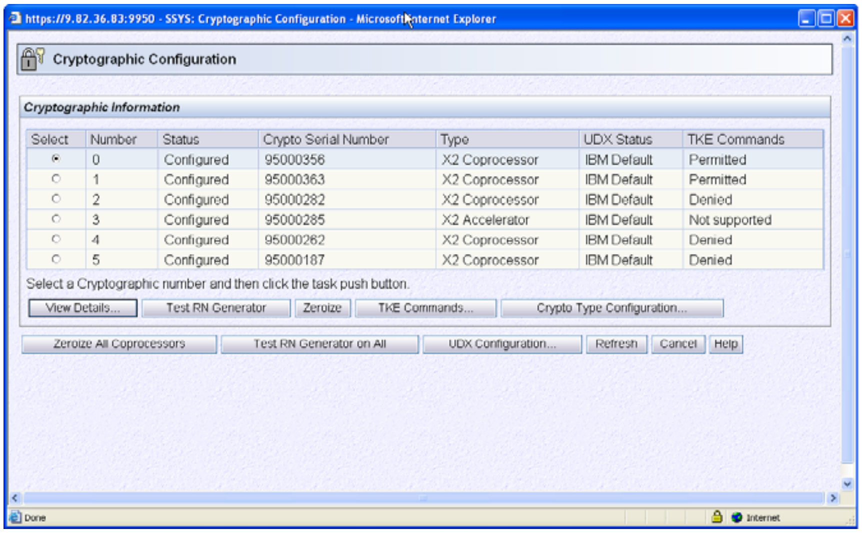
Machine type / model: 002084 / B16-314 — Manufacturer: IBM

Machine serial: 02 - 0023A6A — CPC serial: 000020023A6A

Machine sequence: 000000023A6A — CPC location: A19B

Plant of manufacture: 02 — CPC identifier: 00

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



https://9.82.36.83:9950 - SSYS: Cryptographic Configuration - Microsoft Internet Explorer

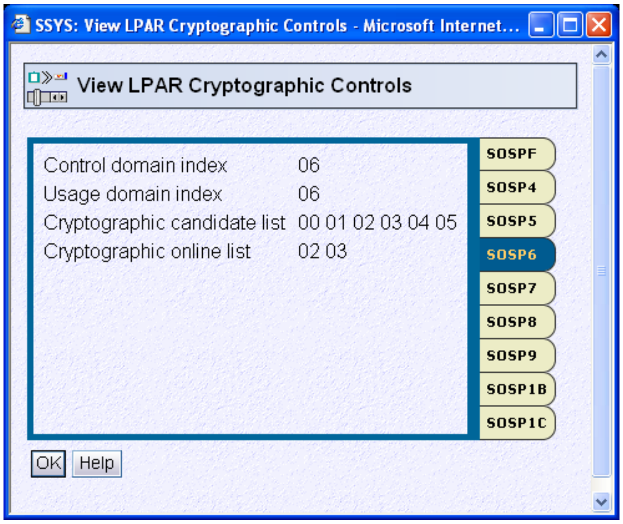
**Cryptographic Configuration**

*Cryptographic Information*

| Select | Number | Status | Crypto Serial Number | Type | UDX Status | TKE Commands |
|---|---|---|---|---|---|---|
| ● | 0 | Configured | 95000356 | X2 Coprocessor | IBM Default | Permitted |
| ○ | 1 | Configured | 95000363 | X2 Coprocessor | IBM Default | Permitted |
| ○ | 2 | Configured | 95000282 | X2 Coprocessor | IBM Default | Denied |
| ○ | 3 | Configured | 95000285 | X2 Accelerator | IBM Default | Not supported |
| ○ | 4 | Configured | 95000262 | X2 Coprocessor | IBM Default | Denied |
| ○ | 5 | Configured | 95000187 | X2 Coprocessor | IBM Default | Denied |

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

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



SSYS: View LPAR Cryptographic Controls - Microsoft Internet...

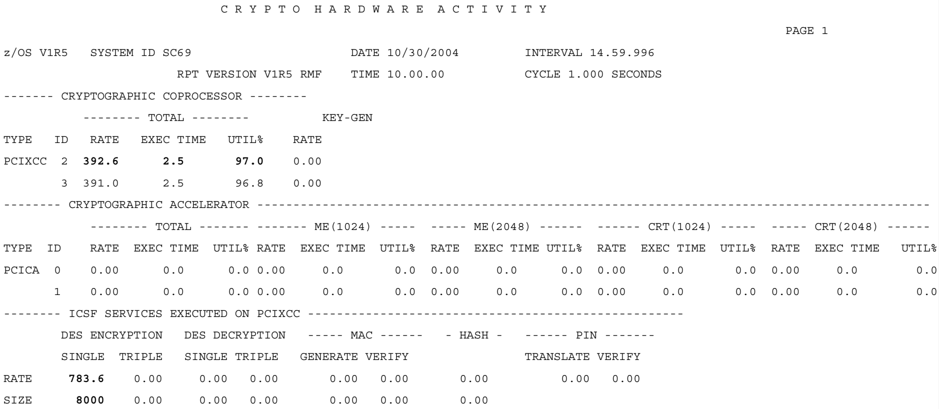
View LPAR Cryptographic Controls

| | |
|---|---|
| Control domain index | 06 |
| Usage domain index | 06 |
| Cryptographic candidate list | 00 01 02 03 04 05 |
| Cryptographic online list | 02 03 |

# ICSF Coprocessor Management Screen

```
------------------------- ICSF Coprocessor Management --------------------------
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
  --------------------  -----------------------  ------------
 .  A0                                      ACTIVE
 .  A1                                      ACTIVE
 .  A2                                      ACTIVE
 .  A3                                      ACTIVE
 .  X04              93001166               ACTIVE
 .  X05              93001449               ACTIVE
```

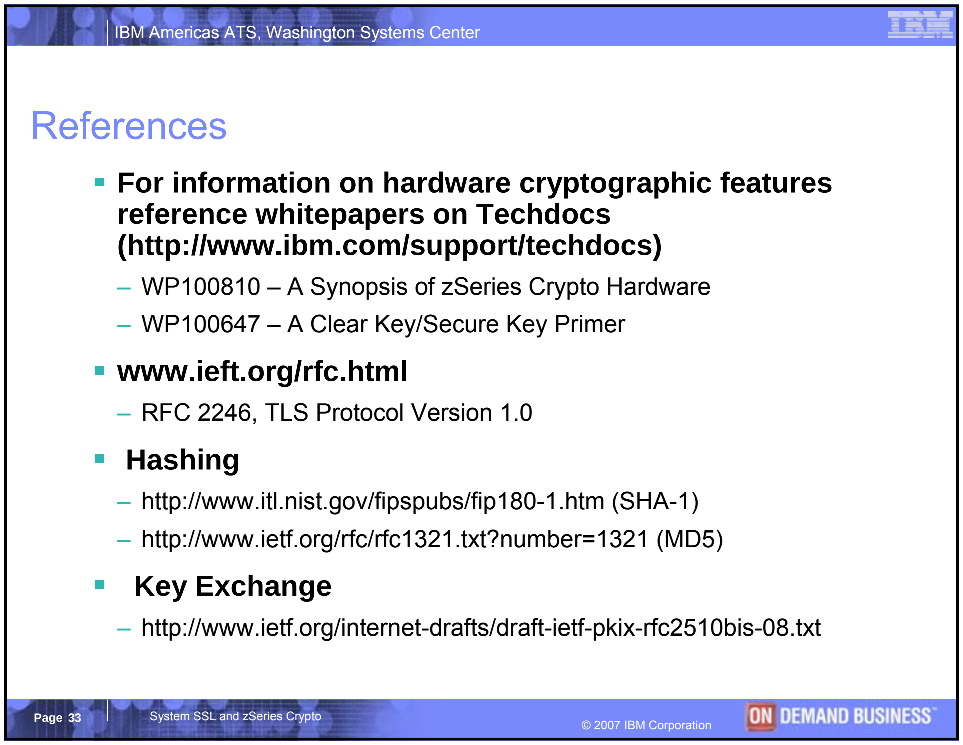
## RMF Crypto Hardware Activity



```
                              C R Y P T O   H A R D W A R E   A C T I V I T Y
                                                                                                            PAGE 1
z/OS V1R5   SYSTEM ID SC69                      DATE 10/30/2004         INTERVAL 14.59.996
                        RPT VERSION V1R5 RMF    TIME 10.00.00           CYCLE 1.000 SECONDS
------- CRYPTOGRAPHIC COPROCESSOR --------
           -------- TOTAL --------          KEY-GEN
TYPE   ID   RATE   EXEC TIME   UTIL%    RATE
PCIXCC  2  392.6      2.5         97.0    0.00
        3  391.0      2.5         96.8    0.00
-------- 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  0    0.00      0.0      0.0 0.00     0.0       0.0  0.00     0.0      0.0  0.00     0.0       0.0  0.00     0.0        0.0
       1    0.00      0.0      0.0 0.00     0.0       0.0  0.00     0.0      0.0  0.00     0.0       0.0  0.00     0.0        0.0
-------- ICSF SERVICES EXECUTED ON PCIXCC ----------------------------------------------------
        DES ENCRYPTION   DES DECRYPTION   ----- MAC ------   - HASH -   ------ PIN -------
        SINGLE  TRIPLE   SINGLE TRIPLE   GENERATE VERIFY                TRANSLATE VERIFY
RATE     783.6    0.00     0.00   0.00       0.00   0.00       0.00          0.00   0.00
SIZE      8000    0.00     0.00   0.00       0.00   0.00       0.00
```

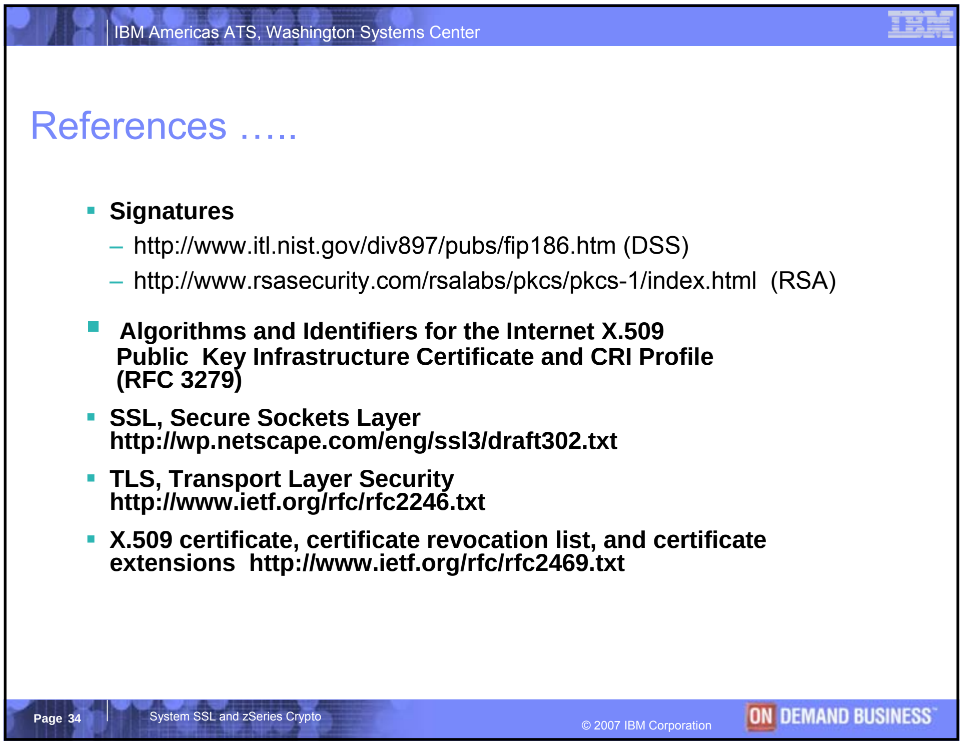
## Summary

- **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**



## References

- **For information on hardware cryptographic features reference whitepapers on Techdocs (http://www.ibm.com/support/techdocs)**
  - WP100810 – A Synopsis of zSeries Crypto Hardware
  - WP100647 – A Clear Key/Secure Key Primer
- **www.ieft.org/rfc.html**
  - RFC 2246, TLS Protocol Version 1.0
- **Hashing**
  - http://www.itl.nist.gov/fipspubs/fip180-1.htm (SHA-1)
  - http://www.ietf.org/rfc/rfc1321.txt?number=1321 (MD5)
- **Key Exchange**
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-rfc2510bis-08.txt



## References …..

- **Signatures**
  - http://www.itl.nist.gov/div897/pubs/fip186.htm (DSS)
  - http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html (RSA)
- **Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile (RFC 3279)**
- **SSL, Secure Sockets Layer http://wp.netscape.com/eng/ssl3/draft302.txt**
- **TLS, Transport Layer Security http://www.ietf.org/rfc/rfc2246.txt**
- **X.509 certificate, certificate revocation list, and certificate extensions http://www.ietf.org/rfc/rfc2469.txt**

# Questions