# Hardware Crypto Benefits

SecureWorld Session I04

Marilyn Frazier Allmond
Advanced Technical Support
Washington System Center

S/390 zSeries Crypto Hardware, ICSF, and TKE
allmond@us.ibm.com

# Trademarks

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

APPN*
DB2*
e-business logo*
Enterprise Storage Systems
ESCON*
FICON
GDPS
Geographically Dispersed Parallel Sysplex
HiperSockets
IBM*

IBM logo*
IMS
Magstar*
MVS
Netfinity*
OS/390*
Parallel Sysplex*
Processor Resource/Systems Managers
PR/SM
RACF

S/390*
S/390 Parallel Enterprise Server
Virtual Image Facility
VM/ESA*
VSE/ESA
VTAM*
WebSphere
z/Architecture
z/OS
z/VM
zSeries

* Registered trademarks of IBM Corporation

Lotus, Notes, and Domino are trademarks or registered trademarks of Lotus Development Corporation
Tivoli is a trademark of Tivoli Systems Inc.
UNIX is a registered trademark of The Open Group in the United States and other countries.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.
RSA and BSAFE are trademarks owned by RSA Data Systems
Atalla is a U.S. registered trademark of Atalla Corporation.
Racal

Acknowledgements: Some foils used in this presentation are from Patrick Kappeler and Linwood Robinson.

**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.

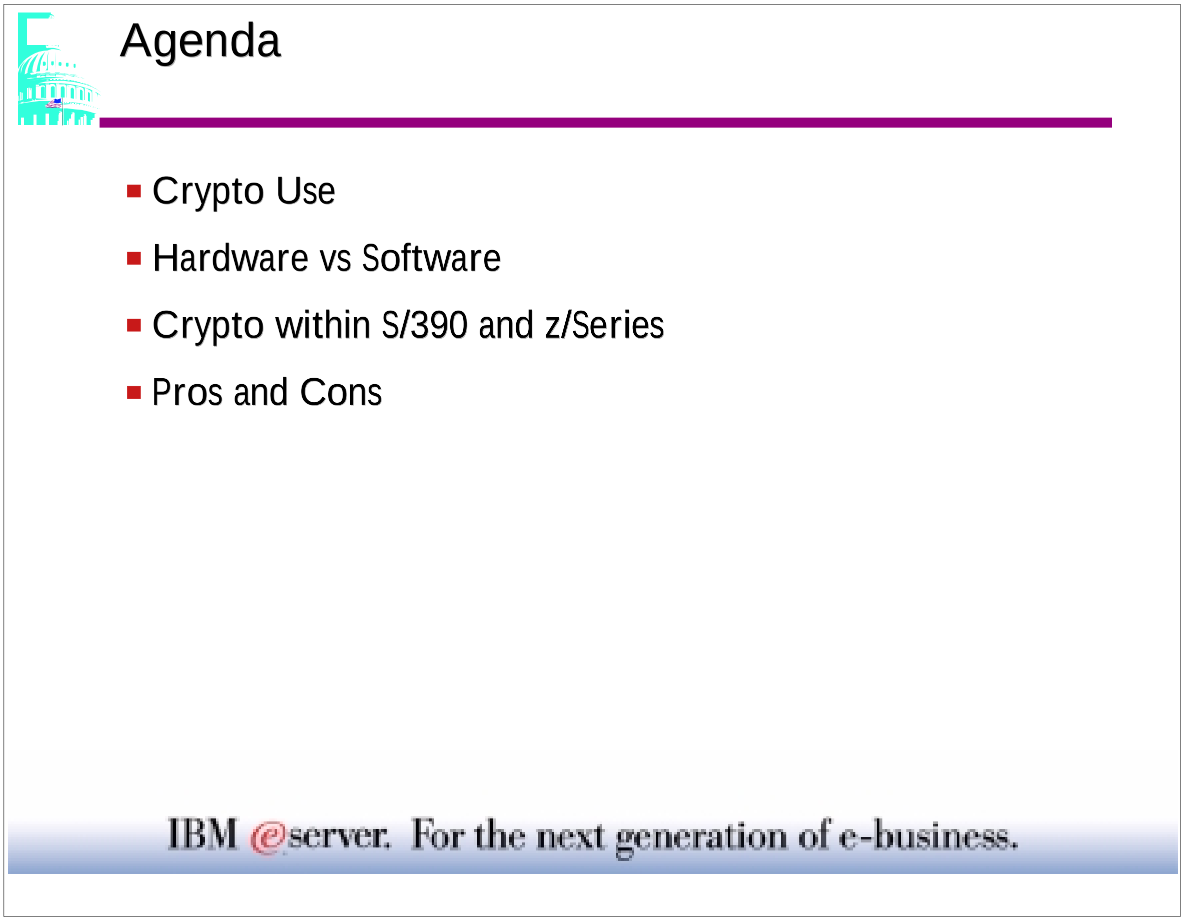
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

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.

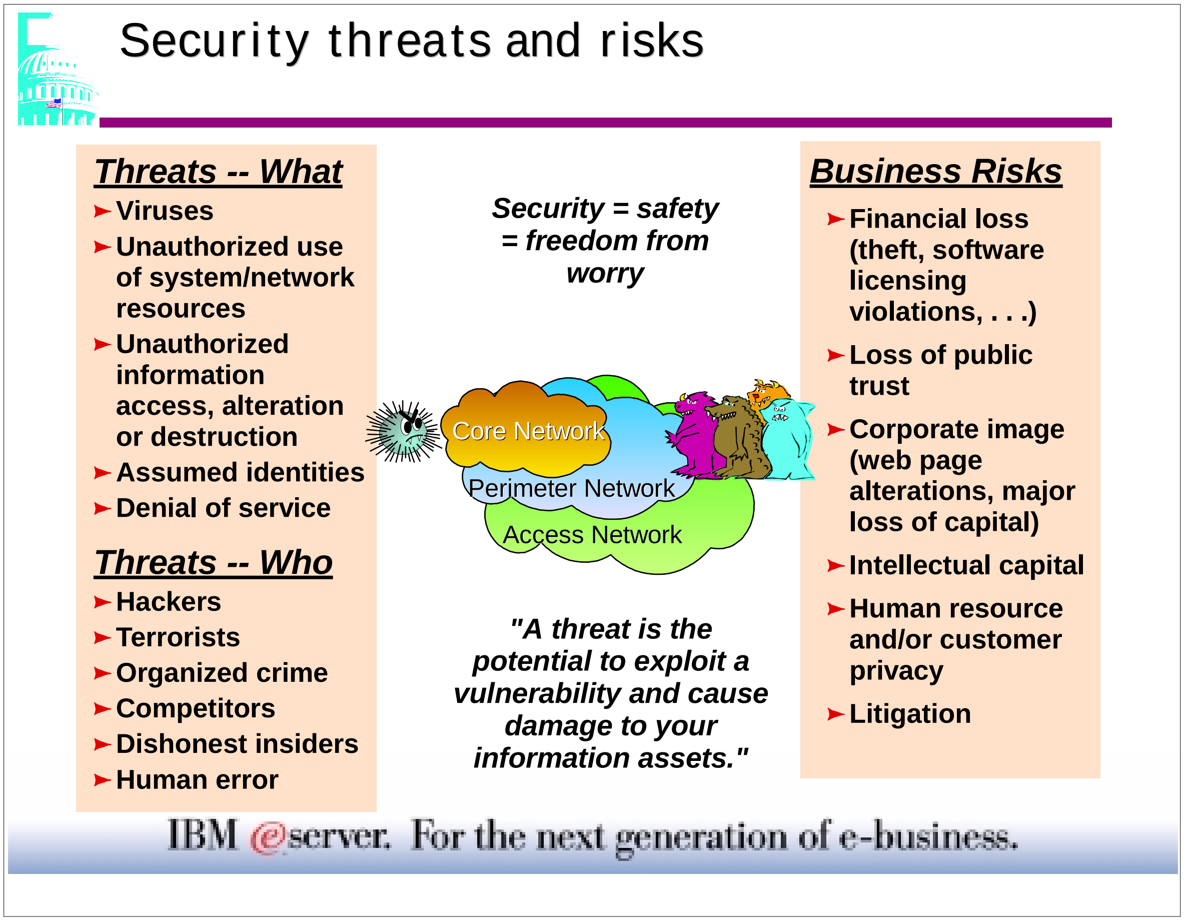
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products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



# Agenda

- Crypto Use
- Hardware vs Software
- Crypto within S/390 and z/Series
- Pros and Cons

IBM @server. For the next generation of e-business.



# Security threats and risks

## Threats -- What

- Viruses
- Unauthorized use of system/network resources
- Unauthorized information access, alteration or destruction
- Assumed identities
- Denial of service

## Threats -- Who

- Hackers
- Terrorists
- Organized crime
- Competitors
- Dishonest insiders
- Human error

***Security = safety = freedom from worry***

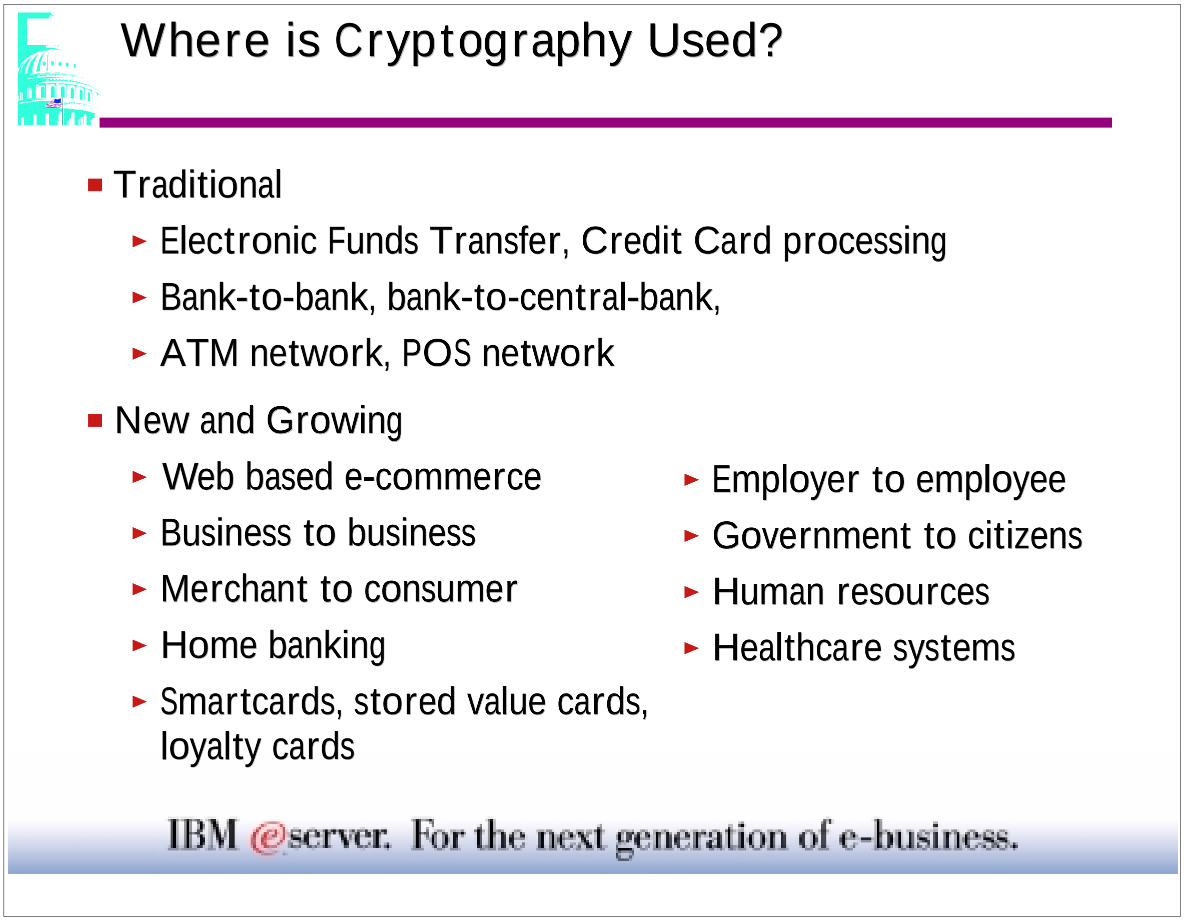
Core Network
Perimeter Network
Access Network

***"A threat is the potential to exploit a vulnerability and cause damage to your information assets."***

## Business Risks

- Financial loss (theft, software licensing violations, . . .)
- Loss of public trust
- Corporate image (web page alterations, major loss of capital)
- Intellectual capital
- Human resource and/or customer privacy
- Litigation

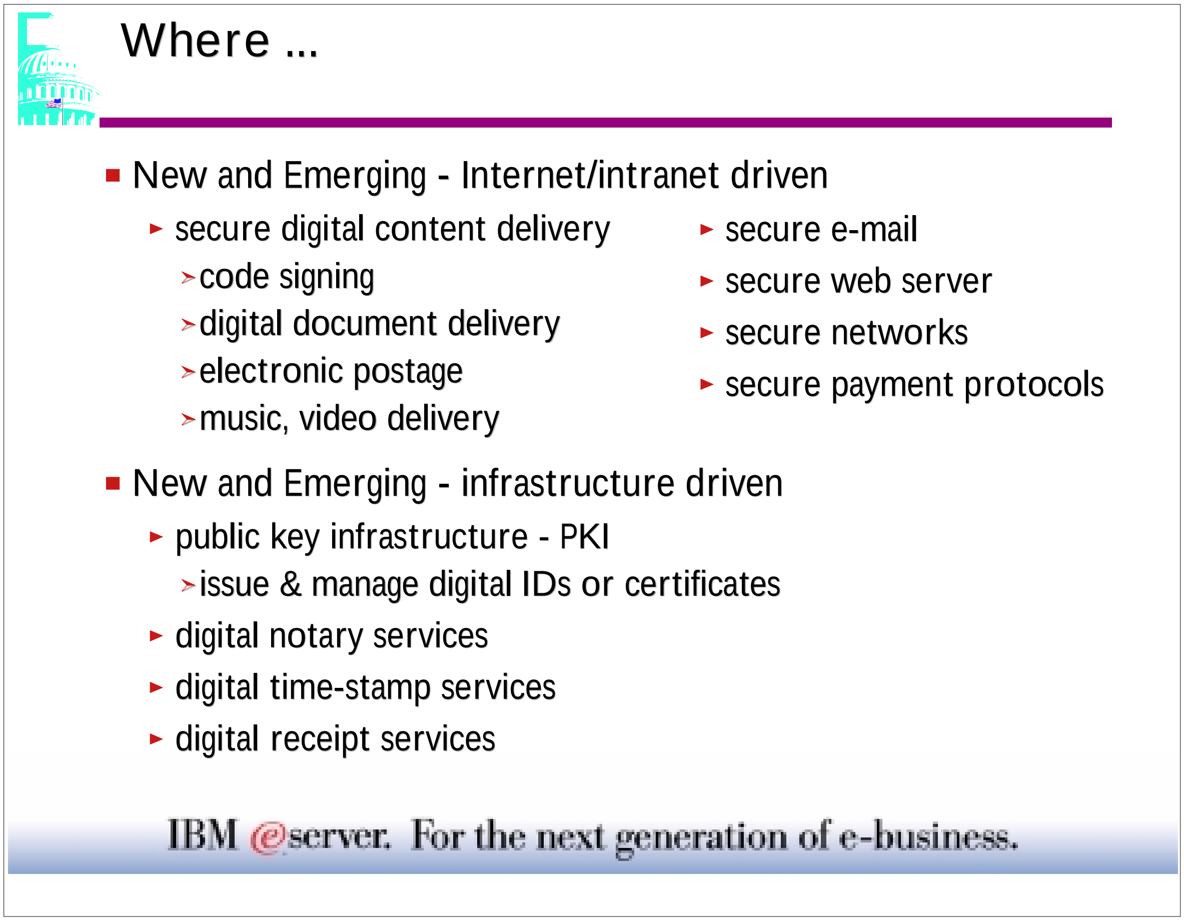
IBM @server. For the next generation of e-business.



## Where is Cryptography Used?

- Traditional
  - Electronic Funds Transfer, Credit Card processing
  - Bank-to-bank, bank-to-central-bank,
  - ATM network, POS network
- New and Growing
  - Web based e-commerce
  - Business to business
  - Merchant to consumer
  - Home banking
  - Smartcards, stored value cards, loyalty cards
  - Employer to employee
  - Government to citizens
  - Human resources
  - Healthcare systems

IBM @server. For the next generation of e-business.



## Where ...

- New and Emerging - Internet/intranet driven
  - secure digital content delivery
    - code signing
    - digital document delivery
    - electronic postage
    - music, video delivery
  - secure e-mail
  - secure web server
  - secure networks
  - secure payment protocols
- New and Emerging - infrastructure driven
  - public key infrastructure - PKI
    - issue & manage digital IDs or certificates
  - digital notary services
  - digital time-stamp services
  - digital receipt services

IBM @server. For the next generation of e-business.

## Why Hardware Cryptography?

- Emerging e-business workloads place new demands on high performing servers
  - Internet access to business data must have confidentiality
  - Software cryptographic solutions can perform poorly
  - Software cryptographic solutions cannot protect sensitive encryption keys
- e-business absolutely demands cryptography
  - Protect sensitive data from unauthorized viewing
  - Provide identification and/or authentication to otherwise "masked" partner

## Hardware vs Software

- Both environments provide cryptographic engines and support programming language interfaces so requests can be directed to the hardware.
- Key Security is one area where the environments differ
  - Key Storage can be a sensitive topic whether it is DES or RSA key storage
  - Keys used for highly critical functions, whether legal and/or financial will require appropriate levels of security
- Performance is the other area
  - Dependency on high transaction rates and data throughput may require more load on a system than can be tolerated
  - Hardware Crypto Engines assist by off-loading the workload from software to hardware

## Cryptographic Key Storage

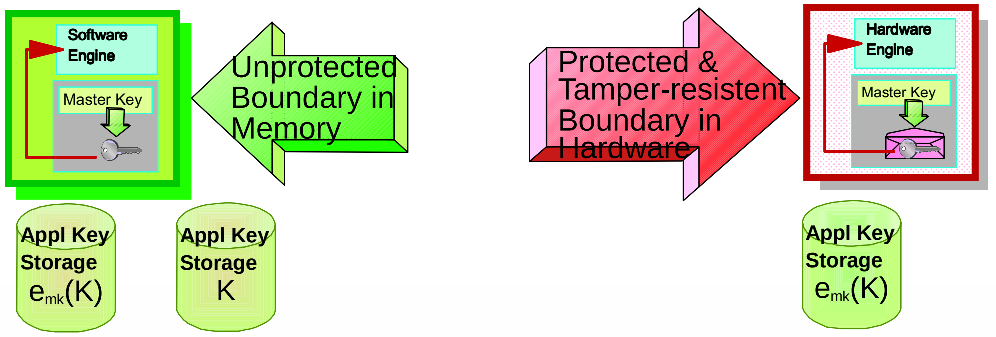
- Keys are nothing more than random strings of hexadecimal digits.
  - 2 digits per byte, 8 byte key = 16 digits, etc.
  - Example:

  1AEF 880B D622 9AB4   7CCF 0CD7 32E4 48DB

- The keys used by applications affect an algorithm's output and is critical to the production of the desired result
- Both DES and RSA key values then must be kept for application use, thus the protection of the values is paramount.

## DES Master Key Storage

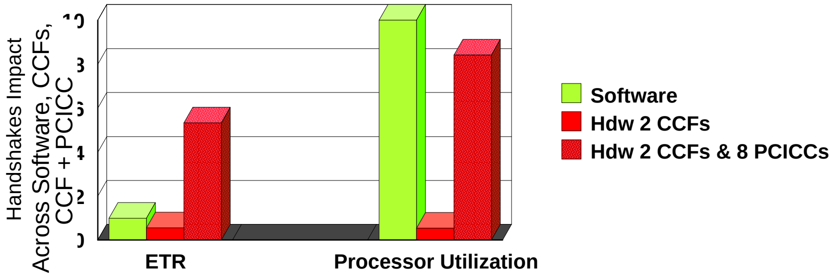
- Where
  - in software cryptographic implementations must be in clear software storage or at most masked via some reversible process in software storage
  - in hardware cryptographic implementation is within the boundary of the hardware cryptographic module


Software Engine
Master Key
Unprotected Boundary in Memory
Protected & Tamper-resistent Boundary in Hardware
Hardware Engine
Master Key
Appl Key Storage $e_{mk}(K)$
Appl Key Storage K
Appl Key Storage $e_{mk}(K)$

# What Drives Overhead

- Public Key Algorithm (PKA) encryption/decryption, for instance, cause lots of processing due to the large numbers required for the modular exponentiation or factoring

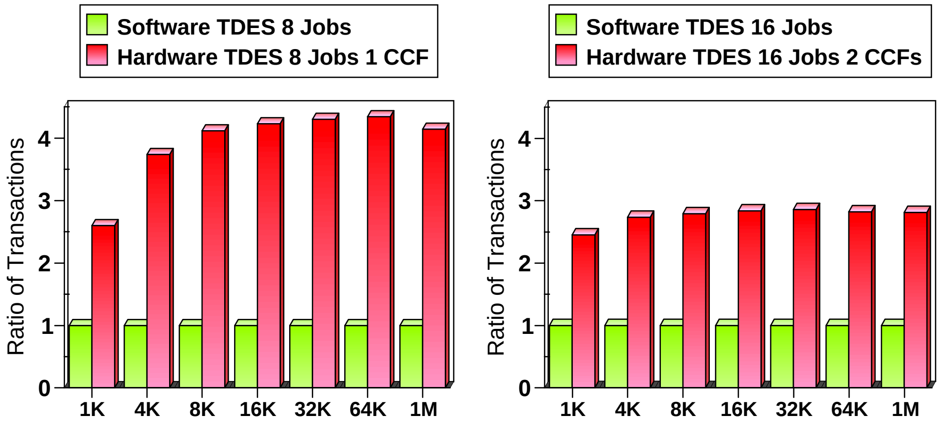
**System SSL - RC4 MD5 (Data Encryption n/a)**
**9672-XZ7 with z/OS V1R1**
**and APAR Support for ICSF & System SSL**



Comparison of SSL Handshake Impact
8 Jobs on 9672-XZ7 with z/OS V1R1

# What Drives Overhead . . .

- Large amounts of data encryption/decryption using symmetric keys impact CPU processes due to the data size

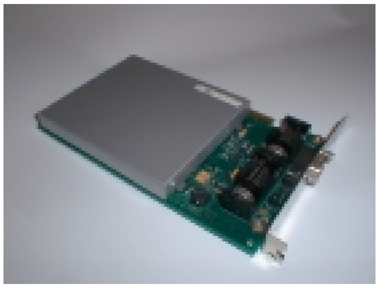


**8 Jobs on 9672-X47 with z/OS V1R1**
TDES Processing Comparison
**using 1 CCF**

**16 Jobs on 9672-XZ7 with z/OS V1R**
TDES Processing Comparison
**using 2 CCFs**

# IBM Crypto Hardware

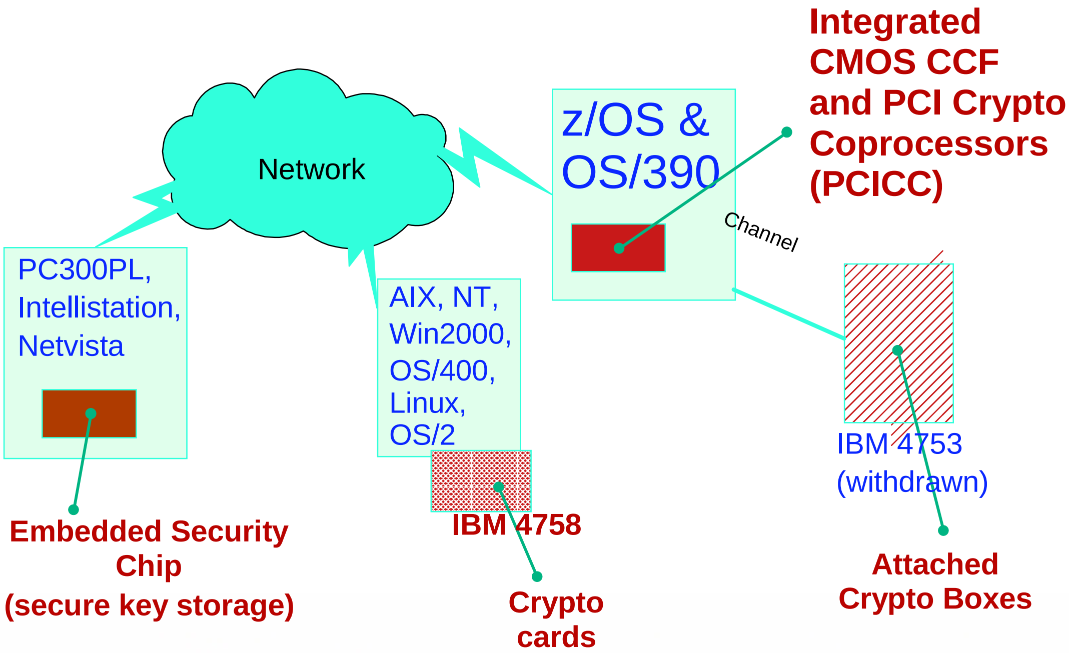
CCF



PCICC

Support a common cryptographic architecture, CCA.

# IBM Hardware Cryptography



Integrated CMOS CCF and PCI Crypto Coprocessors (PCICC)

Network

z/OS & OS/390

Channel

PC300PL, Intellistation, Netvista

AIX, NT, Win2000, OS/400, Linux, OS/2

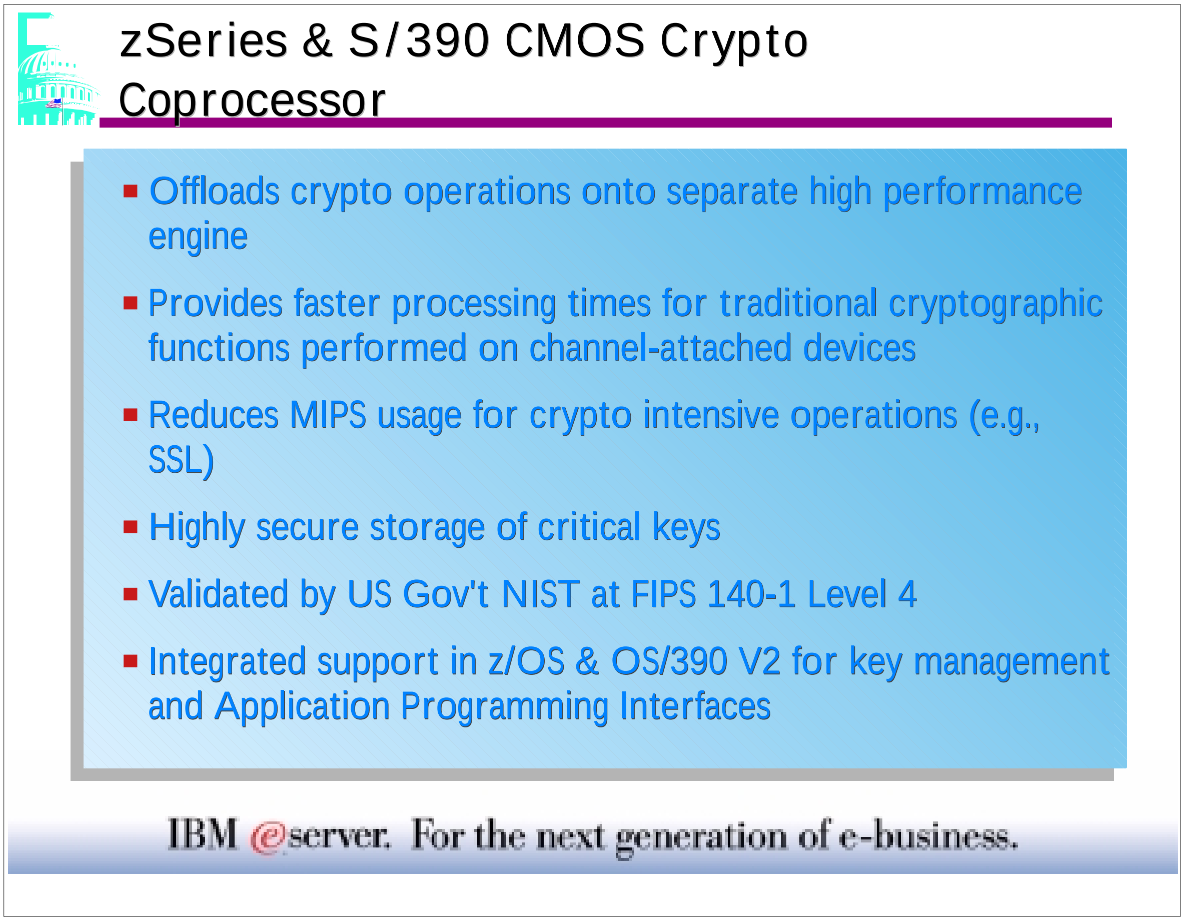
IBM 4753 (withdrawn)

IBM 4758

Embedded Security Chip (secure key storage)

Crypto cards

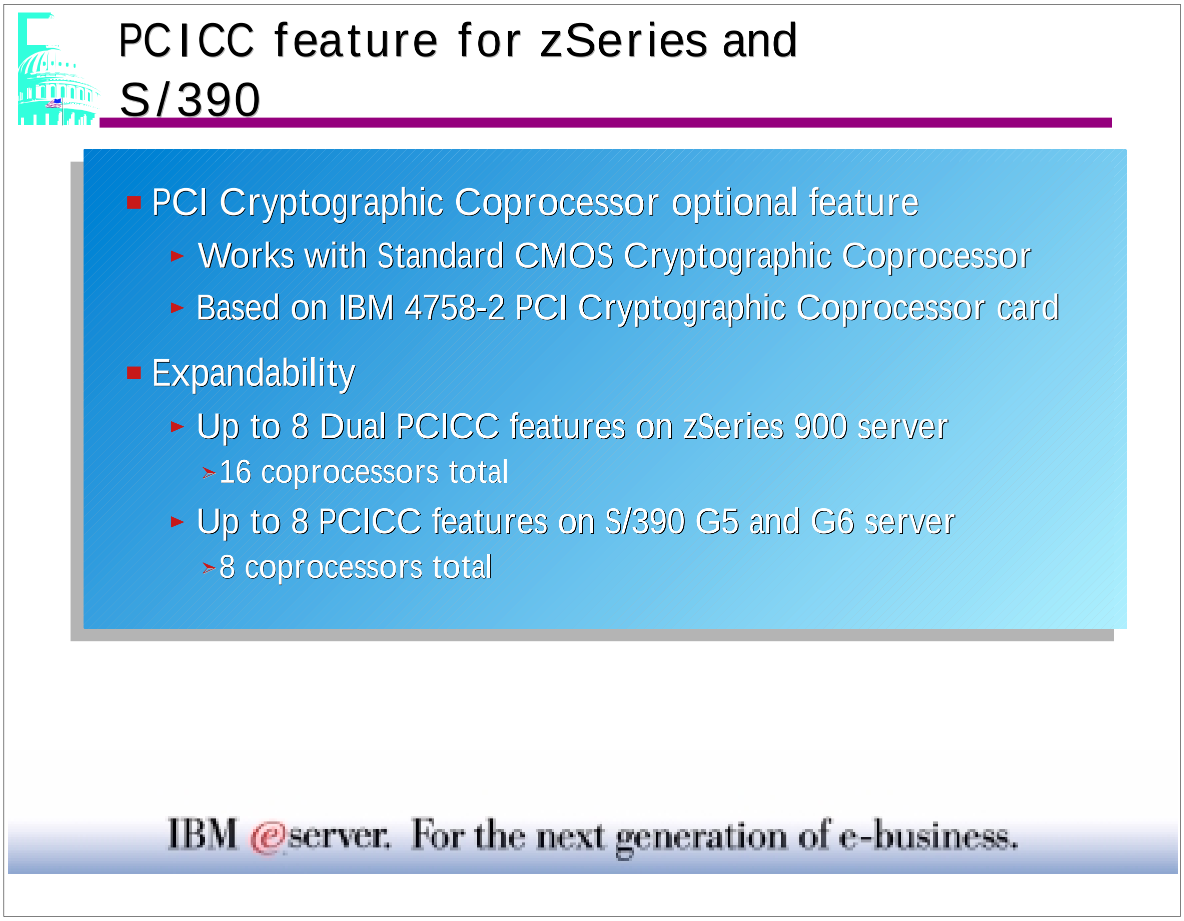
Attached Crypto Boxes



## zSeries & S/390 CMOS Crypto Coprocessor

- Offloads crypto operations onto separate high performance engine
- Provides faster processing times for traditional cryptographic functions performed on channel-attached devices
- Reduces MIPS usage for crypto intensive operations (e.g., SSL)
- Highly secure storage of critical keys
- Validated by US Gov't NIST at FIPS 140-1 Level 4
- Integrated support in z/OS & OS/390 V2 for key management and Application Programming Interfaces

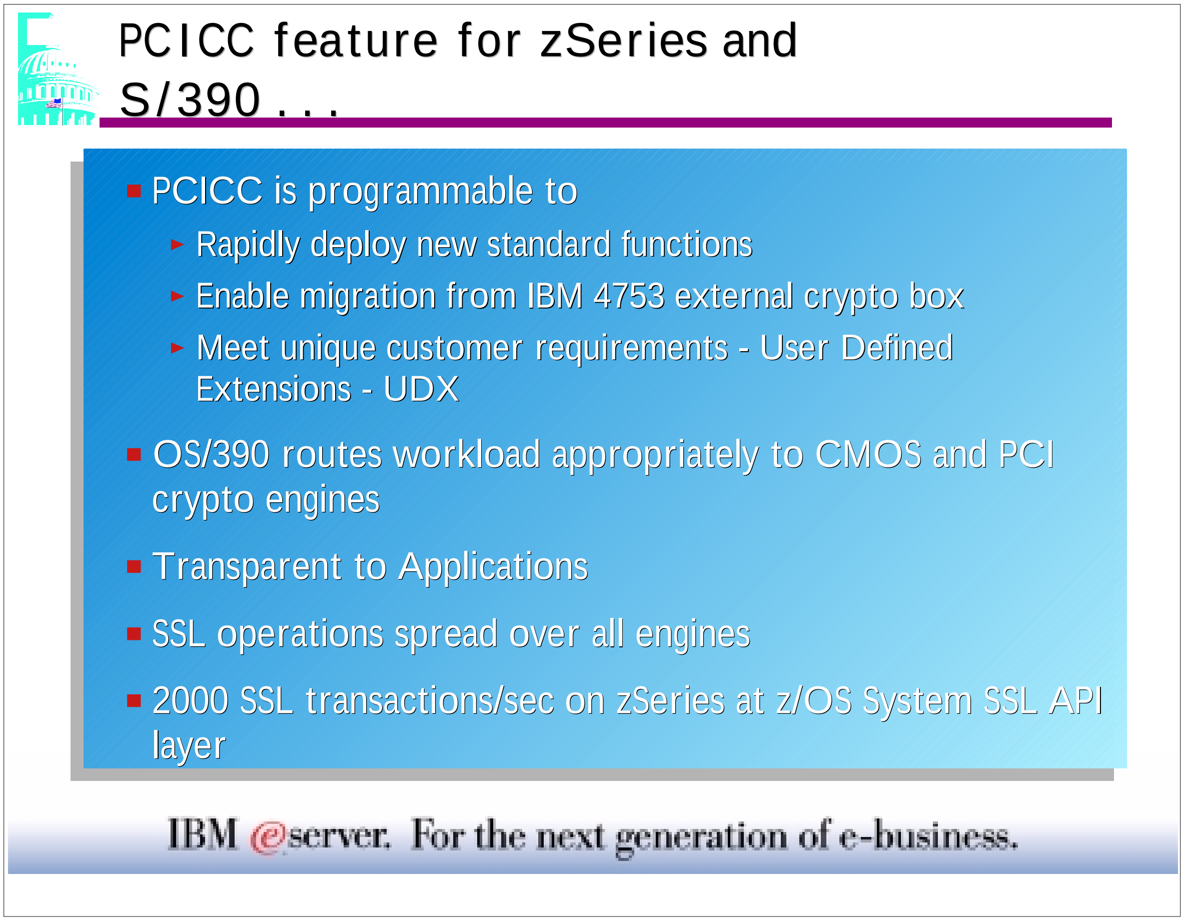
IBM @server. For the next generation of e-business.



## PCICC feature for zSeries and S/390

- PCI Cryptographic Coprocessor optional feature
  - Works with Standard CMOS Cryptographic Coprocessor
  - Based on IBM 4758-2 PCI Cryptographic Coprocessor card
- Expandability
  - Up to 8 Dual PCICC features on zSeries 900 server
    - 16 coprocessors total
  - Up to 8 PCICC features on S/390 G5 and G6 server
    - 8 coprocessors total

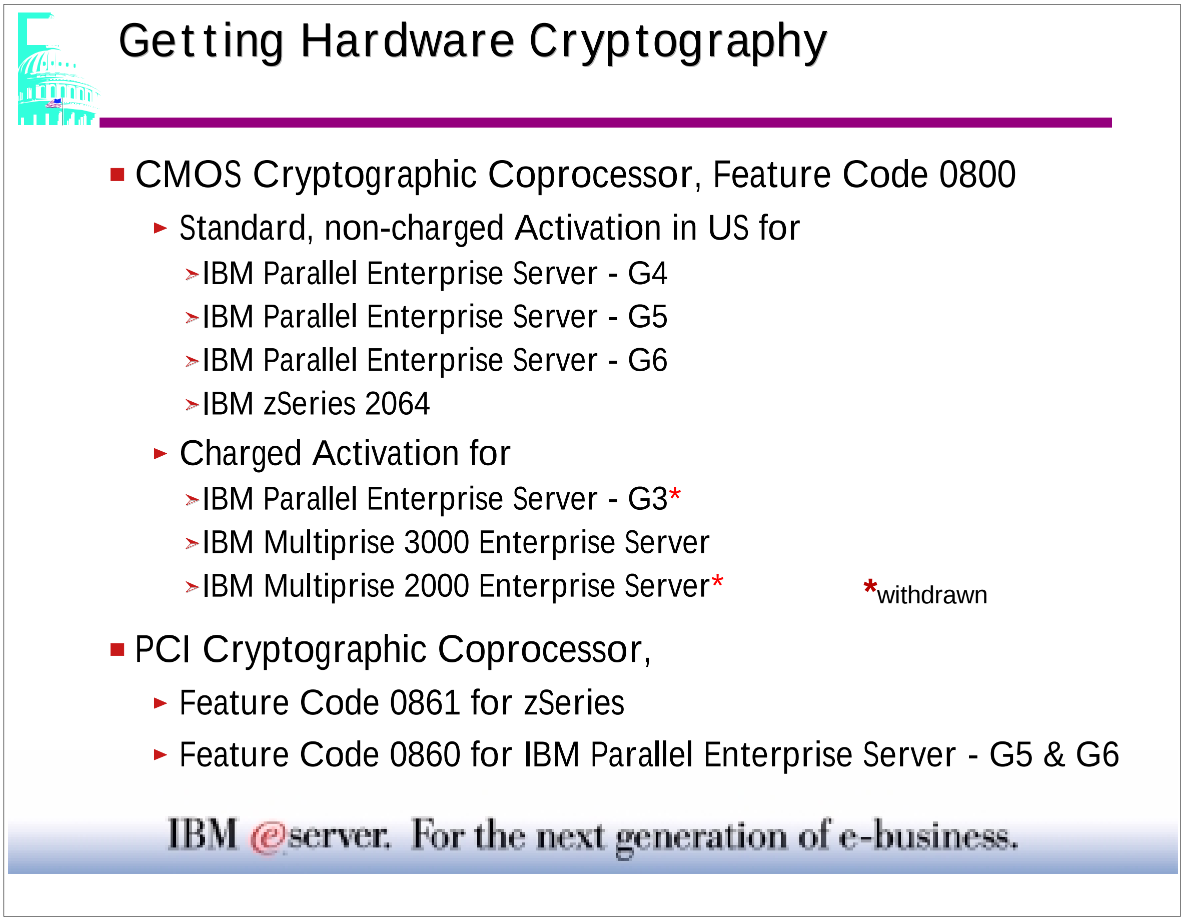
IBM @server. For the next generation of e-business.



## PCICC feature for zSeries and S/390 . . .

- PCICC is programmable to
  - Rapidly deploy new standard functions
  - Enable migration from IBM 4753 external crypto box
  - Meet unique customer requirements - User Defined Extensions - UDX
- OS/390 routes workload appropriately to CMOS and PCI crypto engines
- Transparent to Applications
- SSL operations spread over all engines
- 2000 SSL transactions/sec on zSeries at z/OS System SSL API layer

IBM @server. For the next generation of e-business.



## Getting Hardware Cryptography

- CMOS Cryptographic Coprocessor, Feature Code 0800
  - Standard, non-charged Activation in US for
    - IBM Parallel Enterprise Server - G4
    - IBM Parallel Enterprise Server - G5
    - IBM Parallel Enterprise Server - G6
    - IBM zSeries 2064
  - Charged Activation for
    - IBM Parallel Enterprise Server - G3*
    - IBM Multiprise 3000 Enterprise Server
    - IBM Multiprise 2000 Enterprise Server*

*withdrawn

- PCI Cryptographic Coprocessor,
  - Feature Code 0861 for zSeries
  - Feature Code 0860 for IBM Parallel Enterprise Server - G5 & G6

IBM @server. For the next generation of e-business.

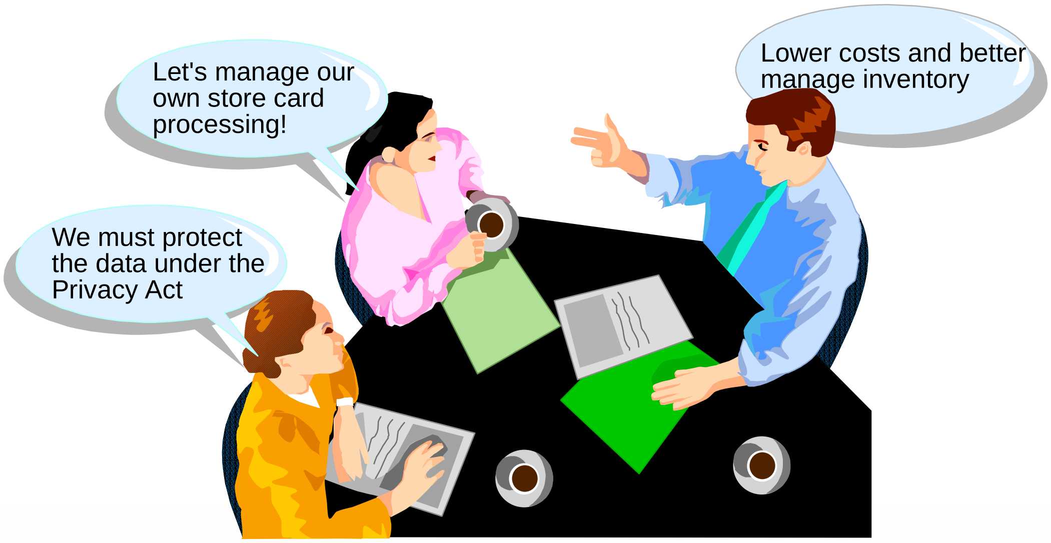
## Getting Hardware Cryptography . . .

This chart has been modified since SecureWorld 2001.

- Hardware is built into IBM Servers with Activation requiring specific actions
  - Ordering and Loading of the LIC to Enable the hardware with configuration data;
    - LIC for CCFs is 0824/0825 for M3000, 0834/0835 for all other CMOS servers, and 0874/0875 for zSeries
    - LIC or FCV for PCICCs is sent with order
    - A disruptive function for CCFs
  - Activation of the OS/390 or z/OS Base component, ICSF
  - Master Key Entry of DES and PKA key values
- Keeping the hardware crypto available for use by applications means managing the crypto such that no unexpected loss of Master Keys occurs

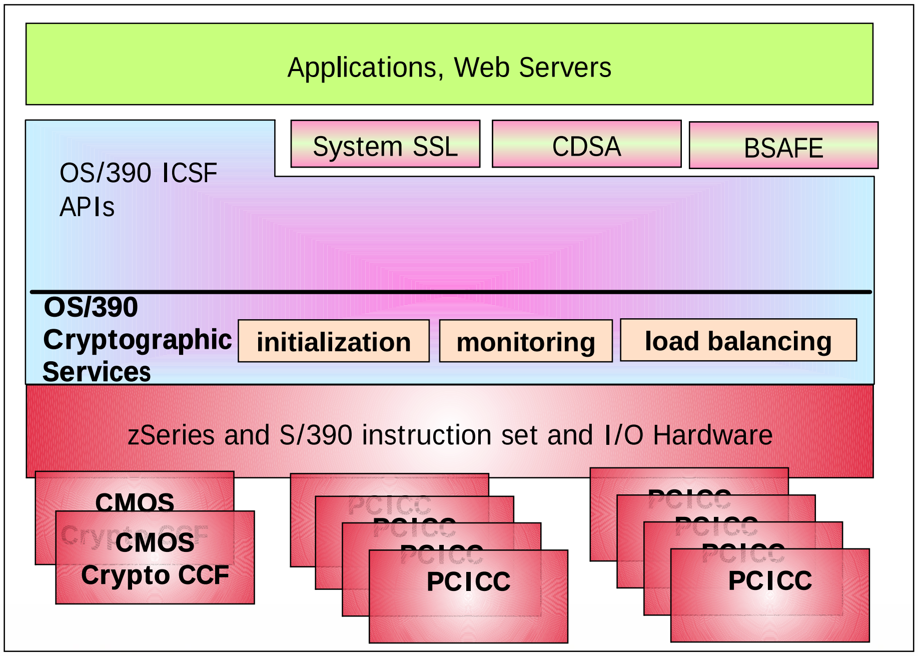
IBM @server. For the next generation of e-business.

## IBM Crypto : The Software Side


Let's manage our own store card processing!
Lower costs and better manage inventory
We must protect the data under the Privacy Act

IBM @server. For the next generation of e-business.

# IBM zSeries and IBM S/390



Applications, Web Servers

System SSL

CDSA

BSAFE

OS/390 ICSF APIs

OS/390 Cryptographic Services

initialization

monitoring

load balancing

zSeries and S/390 instruction set and I/O Hardware

CMOS Crypto CCF

CMOS Crypto CCF

PCICC

PCICC

PCICC

PCICC

PCICC

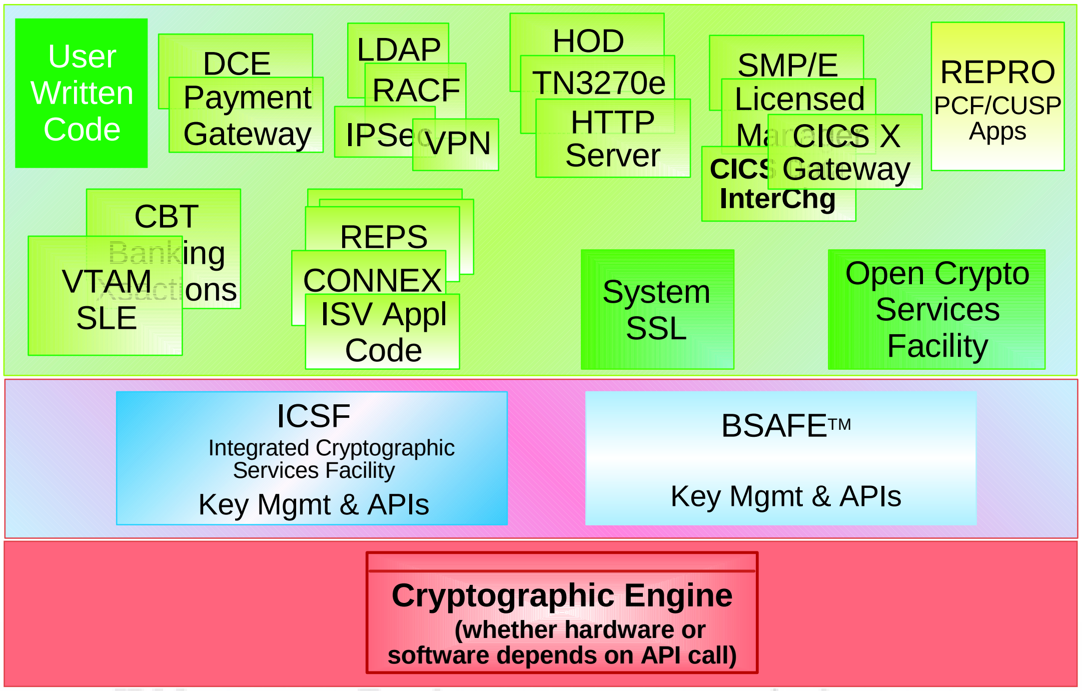
PCICC

PCICC

PCICC

IBM @server. For the next generation of e-business.

# IBM Crypto Software



User Written Code

DCE Payment Gateway

LDAP

RACF

IPSec VPN

HOD

TN3270e

HTTP Server

SMP/E

Licensed Marketing

CICS X Gateway

CICS InterChg

REPRO PCF/CUSP Apps

CBT Banking Transactions

VTAM SLE

REPS

CONNEX

ISV Appl Code

System SSL

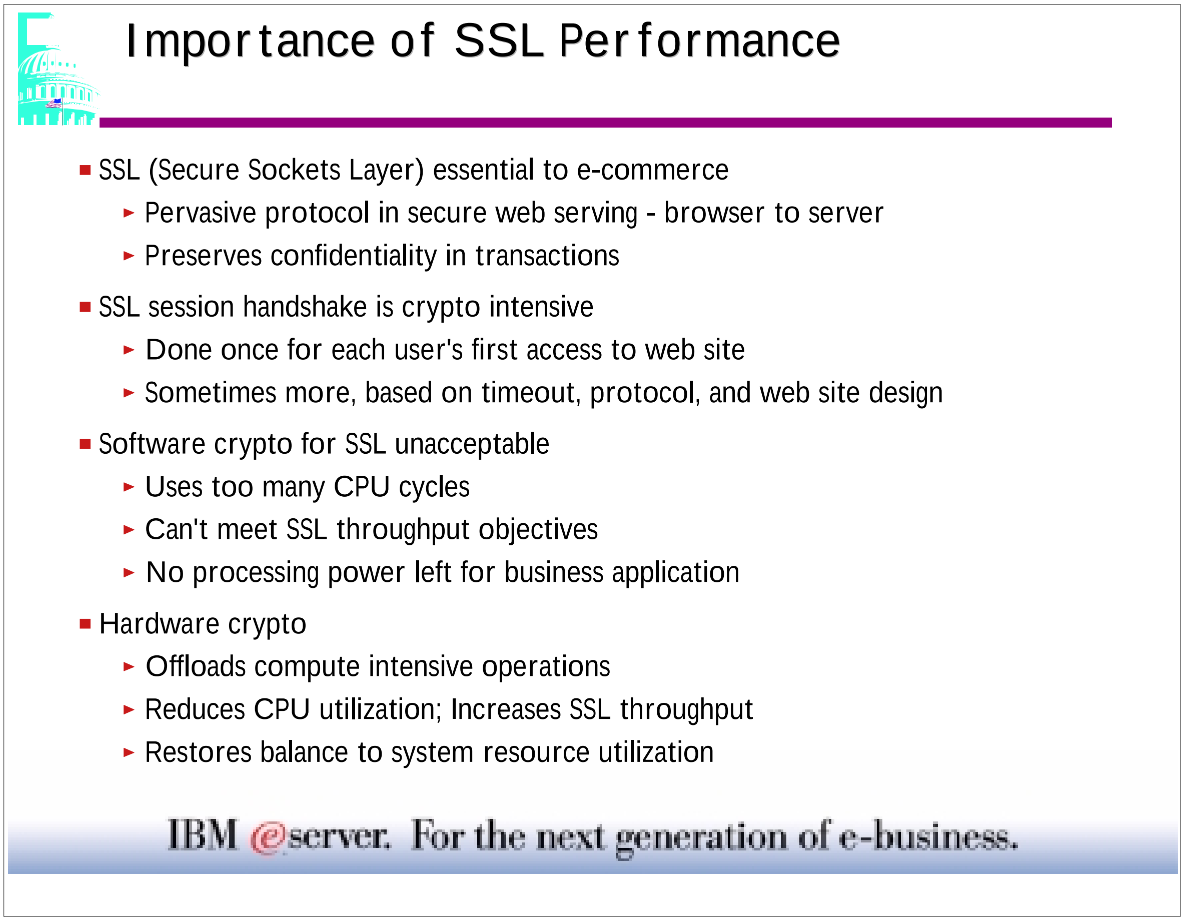
Open Crypto Services Facility

ICSF Integrated Cryptographic Services Facility Key Mgmt & APIs

BSAFE™ Key Mgmt & APIs

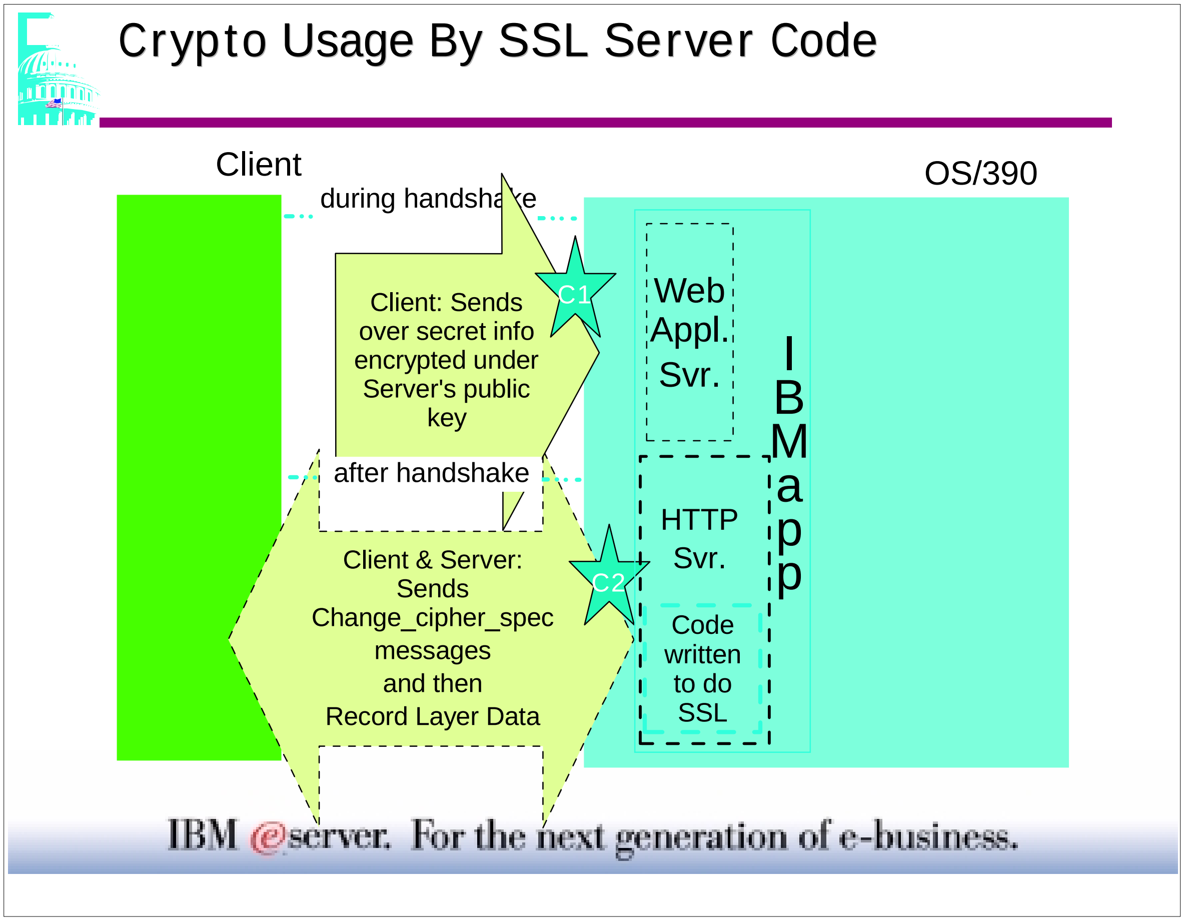
**Cryptographic Engine** (whether hardware or software depends on API call)

IBM @server. For the next generation of e-business.



## Importance of SSL Performance

- SSL (Secure Sockets Layer) essential to e-commerce
  - Pervasive protocol in secure web serving - browser to server
  - Preserves confidentiality in transactions
- SSL session handshake is crypto intensive
  - Done once for each user's first access to web site
  - Sometimes more, based on timeout, protocol, and web site design
- Software crypto for SSL unacceptable
  - Uses too many CPU cycles
  - Can't meet SSL throughput objectives
  - No processing power left for business application
- Hardware crypto
  - Offloads compute intensive operations
  - Reduces CPU utilization; Increases SSL throughput
  - Restores balance to system resource utilization



## Crypto Usage By SSL Server Code

Client

OS/390

during handshake

Client: Sends over secret info encrypted under Server's public key

C1

Web Appl. Svr.

IBM app

after handshake

Client & Server: Sends Change_cipher_spec messages and then Record Layer Data

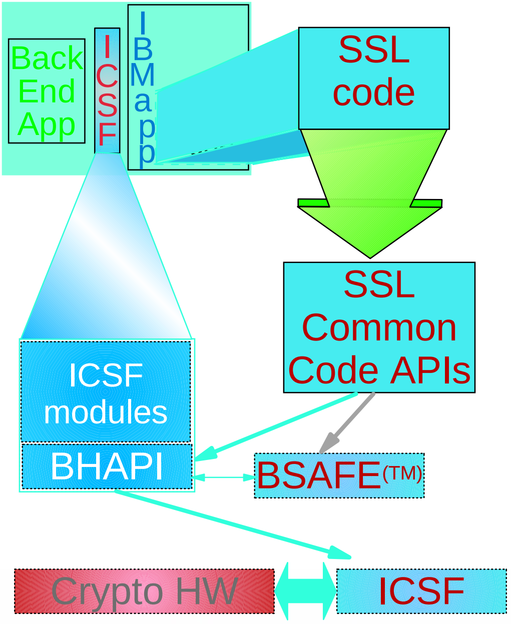
C2

HTTP Svr.

Code written to do SSL

# SSL Usage & Crypto Hardware

OS/390 and z/OS



Back End App

ICSF

IBM app

SSL code

SSL Common Code APIs

ICSF modules

BHAPI

BSAFE(TM)

Crypto HW

ICSF

Is Crypto Hardware valid and ICSF active?

Yes

Send certain requests to the IBM CCA APIs ICSF for processing on Crypto hardware

- decrypt data from under the server's public key
- is negotiated cipherspec DES or TDES?

YES

- encrypt/decrypt using the negotiated session key

No

Send requests to BSAFE for processing on software engine.

# General Crypto Interoperability

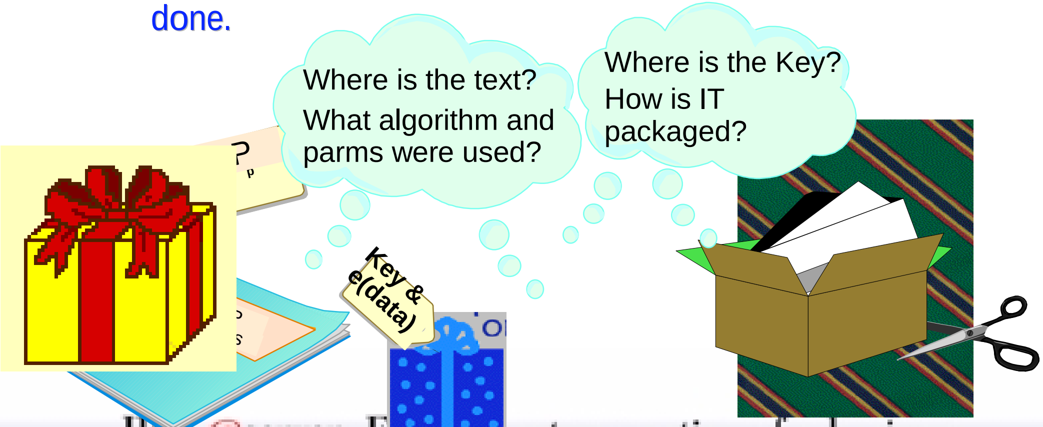
- Same type algorithm? Same processing method?
  - DES => DES? yes
  - DES => IDEA? no
  - RSA => RSA? yes
  - RSA => Elliptic Curve? no
- Same key association? Same length capability?
  - DES key value (a) = DES key value (a+n)? no
  - DES key value (a) = DES key value (a)? yes
  - RSA key value ($b_{len1024}$) = RSA key value ($b_{len512}$)? no
  - RSA key value ($b_{len1024}$) = RSA key value ($b_{len1024}$)? yes
  - RSA key ($e_{joe's\ public\ key}$(msg)) => RSA key ($d_{bob's\ private\ key}$(msg)) no

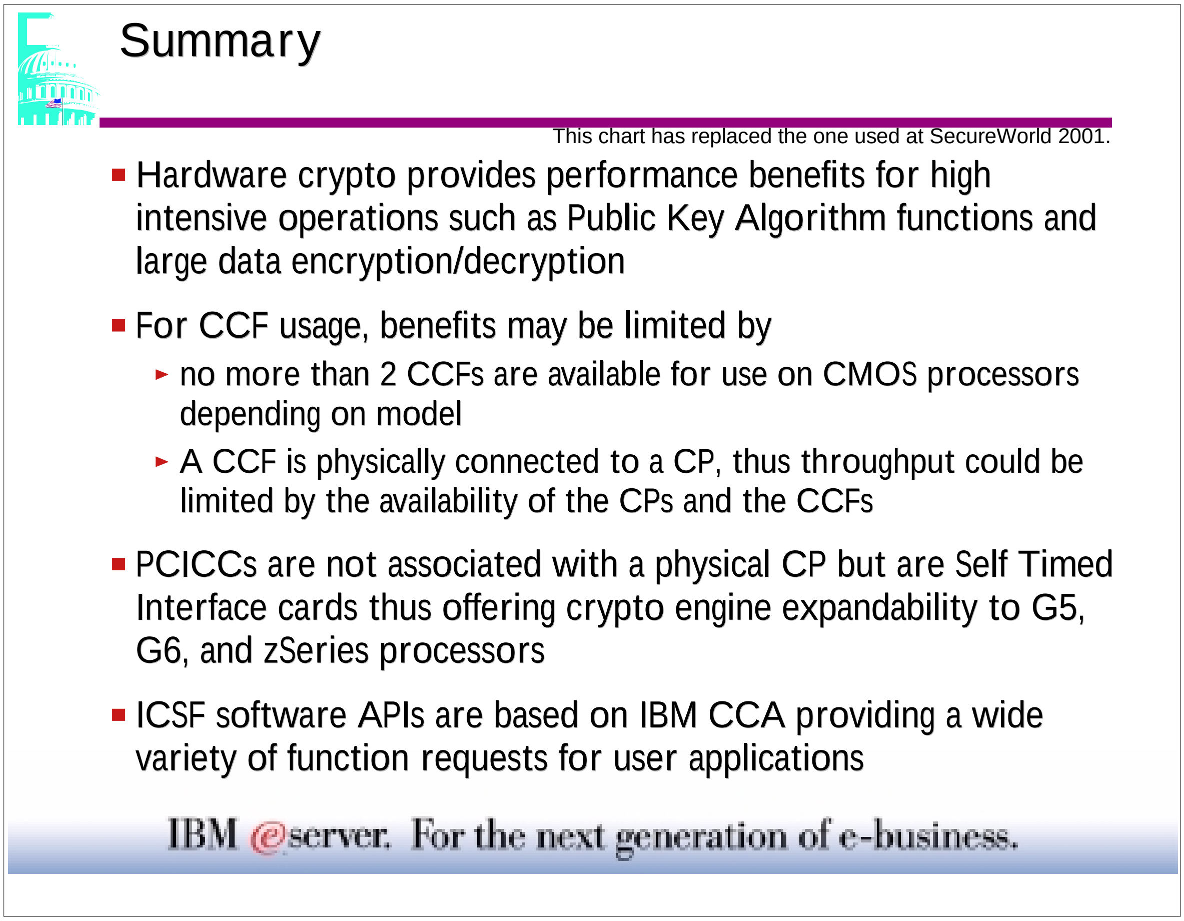
# General Crypto Interoperability . . .

- Applications vs Enablers
  - Some products provide a mechanism for doing cryptographic functions with some configuration or no external requirements.
  - These products are applications which use cryptographic functions in a predetermined manner.
- PGP - Pretty Good Privacy
  - Provides specific function based on GUI selection
  - Application code manages the creation of the "packaged" text and key information
- BSAFE, ICSF
  - Provide coding mechanisms for application selection of function
  - User written code must use those Application Programming Interfaces to create their desired "packaging"

# General Crypto Interoperability . . .

- In English....
  - Unless you want to write your own application to conform to an application's "package", you must always use the application at both ends of the transmission.
  - Packages may not be well documented as to all that must be done.



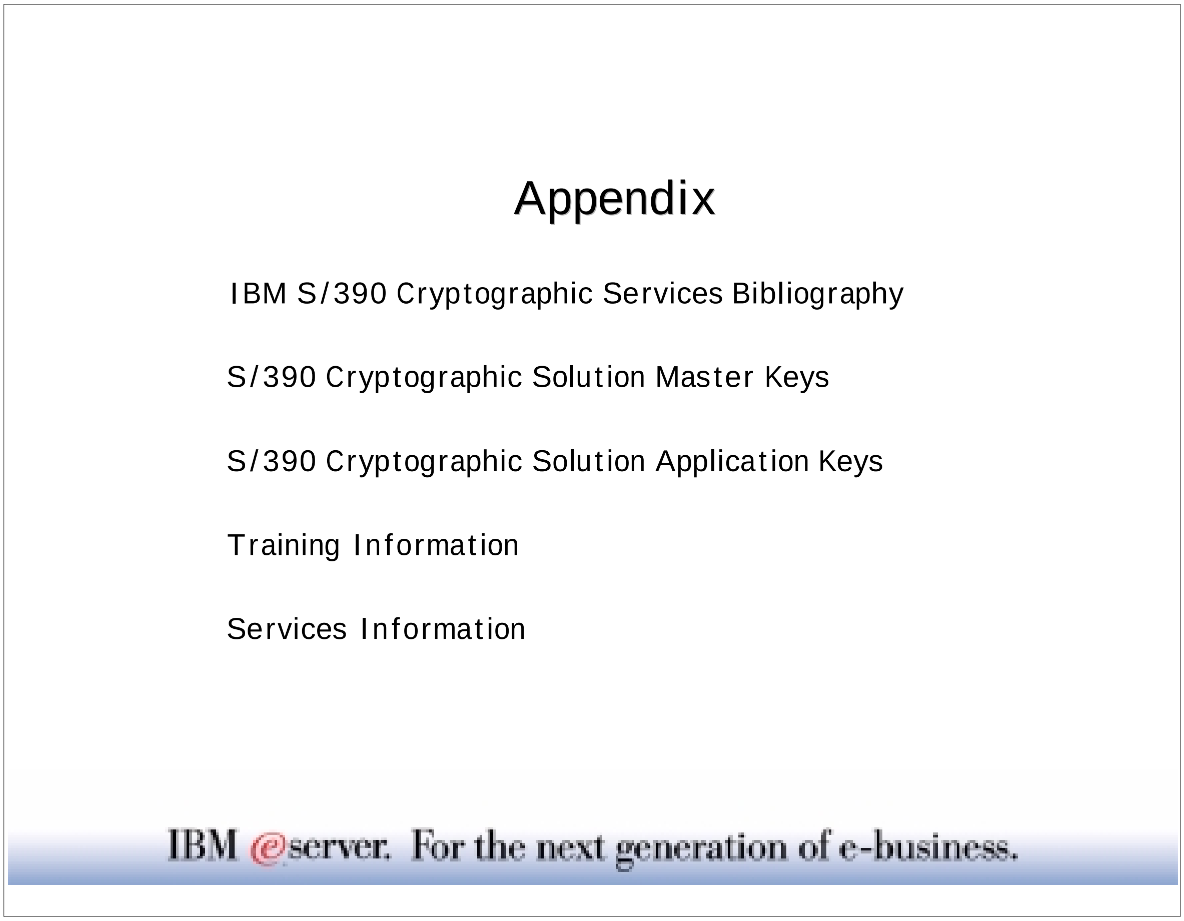


## Summary

This chart has replaced the one used at SecureWorld 2001.

- Hardware crypto provides performance benefits for high intensive operations such as Public Key Algorithm functions and large data encryption/decryption
- For CCF usage, benefits may be limited by
  - no more than 2 CCFs are available for use on CMOS processors depending on model
  - A CCF is physically connected to a CP, thus throughput could be limited by the availability of the CPs and the CCFs
- PCICCs are not associated with a physical CP but are Self Timed Interface cards thus offering crypto engine expandability to G5, G6, and zSeries processors
- ICSF software APIs are based on IBM CCA providing a wide variety of function requests for user applications

IBM @server. For the next generation of e-business.



## Appendix

IBM S/390 Cryptographic Services Bibliography

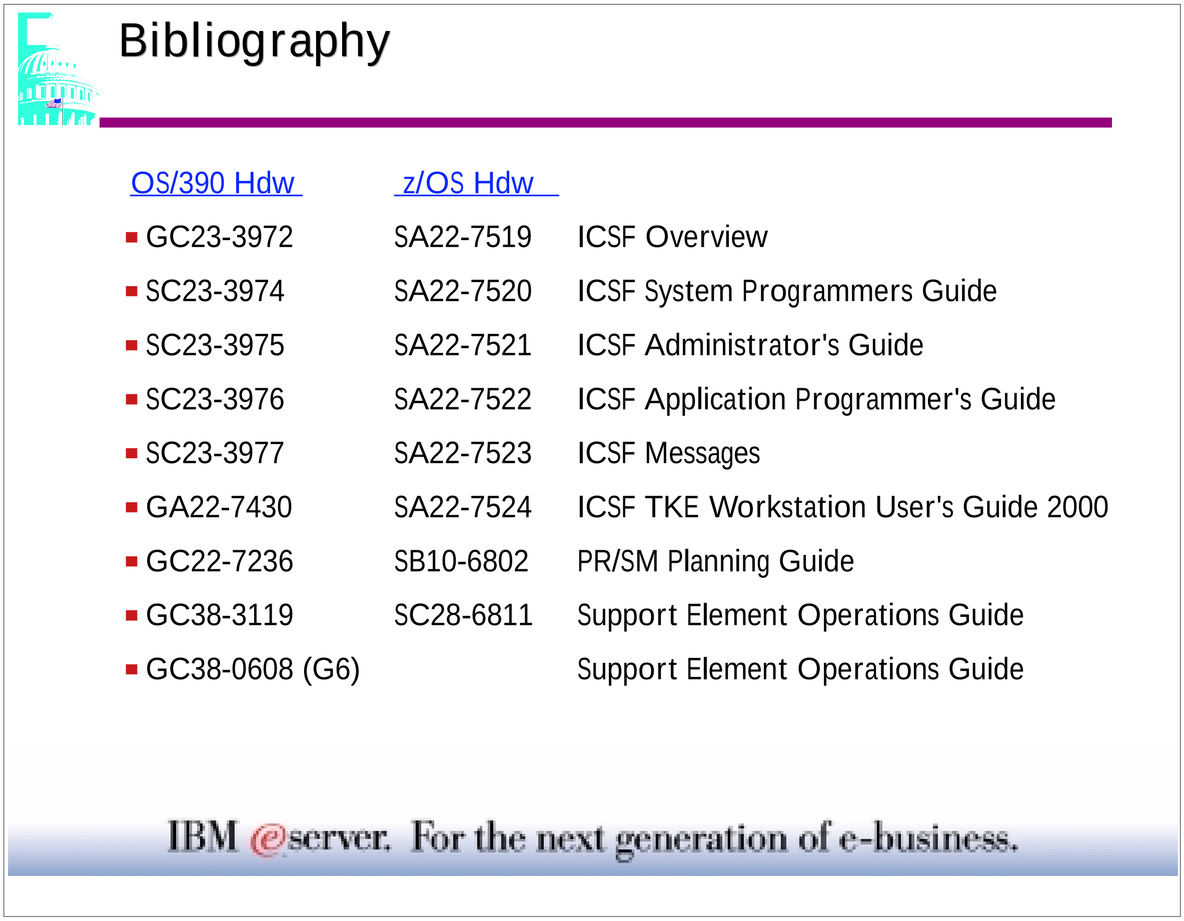
S/390 Cryptographic Solution Master Keys

S/390 Cryptographic Solution Application Keys

Training Information

Services Information

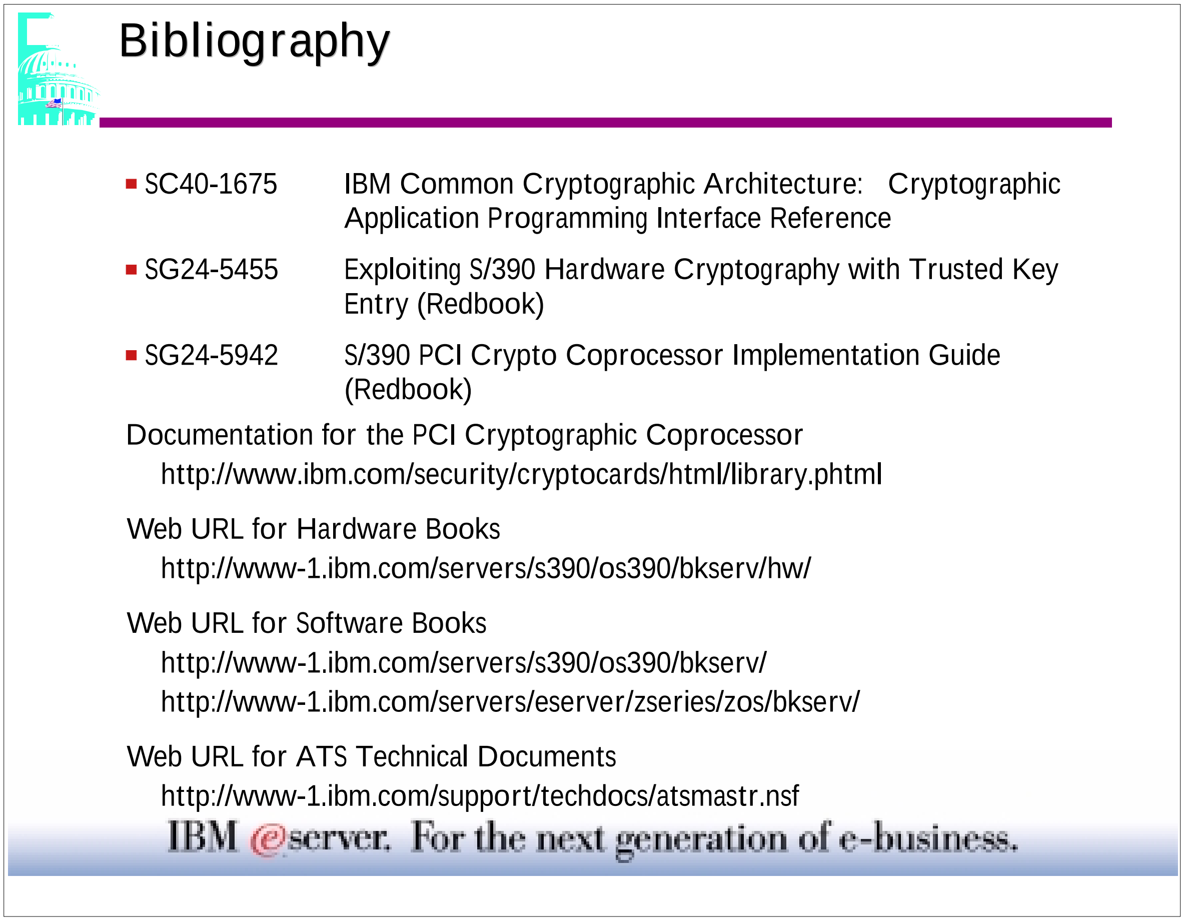
IBM @server. For the next generation of e-business.



## Bibliography

| OS/390 Hdw | z/OS Hdw | |
|---|---|---|
| GC23-3972 | SA22-7519 | ICSF Overview |
| SC23-3974 | SA22-7520 | ICSF System Programmers Guide |
| SC23-3975 | SA22-7521 | ICSF Administrator's Guide |
| SC23-3976 | SA22-7522 | ICSF Application Programmer's Guide |
| SC23-3977 | SA22-7523 | ICSF Messages |
| GA22-7430 | SA22-7524 | ICSF TKE Workstation User's Guide 2000 |
| GC22-7236 | SB10-6802 | PR/SM Planning Guide |
| GC38-3119 | SC28-6811 | Support Element Operations Guide |
| GC38-0608 (G6) | | Support Element Operations Guide |

IBM @server. For the next generation of e-business.



## Bibliography

| | |
|---|---|
| SC40-1675 | IBM Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference |
| SG24-5455 | Exploiting S/390 Hardware Cryptography with Trusted Key Entry (Redbook) |
| SG24-5942 | S/390 PCI Crypto Coprocessor Implementation Guide (Redbook) |

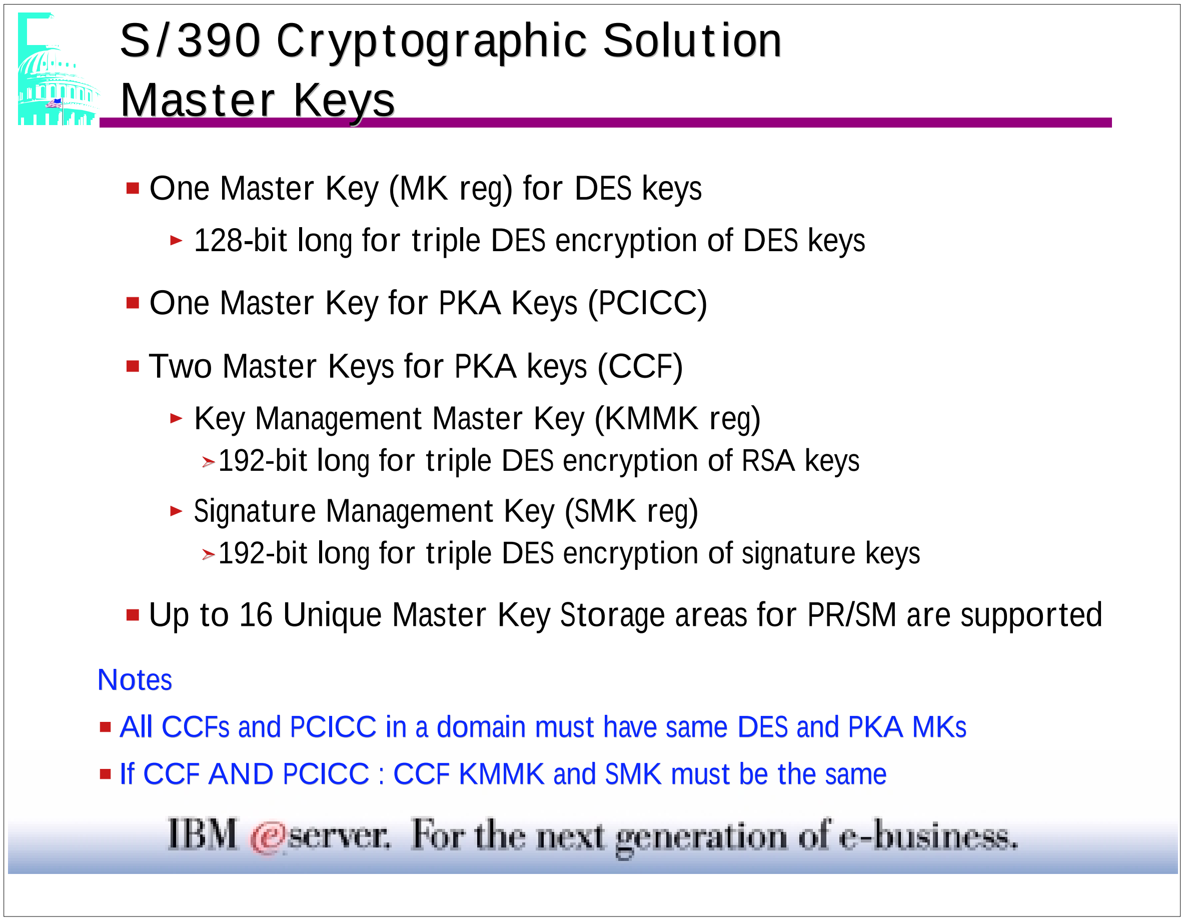
Documentation for the PCI Cryptographic Coprocessor
http://www.ibm.com/security/cryptocards/html/library.phtml

Web URL for Hardware Books
http://www-1.ibm.com/servers/s390/os390/bkserv/hw/

Web URL for Software Books
http://www-1.ibm.com/servers/s390/os390/bkserv/
http://www-1.ibm.com/servers/eserver/zseries/zos/bkserv/

Web URL for ATS Technical Documents
http://www-1.ibm.com/support/techdocs/atsmastr.nsf

IBM @server. For the next generation of e-business.



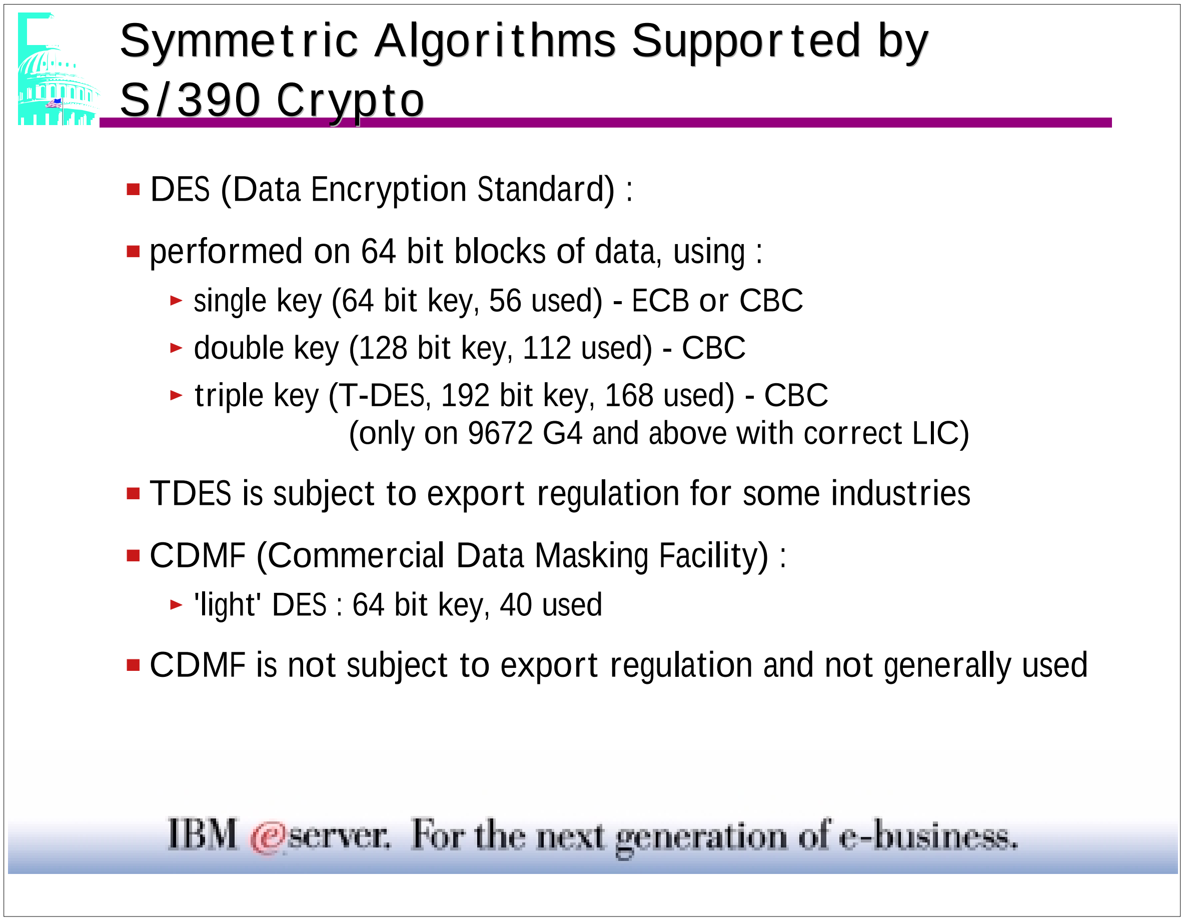
## S/390 Cryptographic Solution Master Keys

- One Master Key (MK reg) for DES keys
  - 128-bit long for triple DES encryption of DES keys
- One Master Key for PKA Keys (PCICC)
- Two Master Keys for PKA keys (CCF)
  - Key Management Master Key (KMMK reg)
    - 192-bit long for triple DES encryption of RSA keys
  - Signature Management Key (SMK reg)
    - 192-bit long for triple DES encryption of signature keys
- Up to 16 Unique Master Key Storage areas for PR/SM are supported

Notes

- All CCFs and PCICC in a domain must have same DES and PKA MKs
- If CCF AND PCICC : CCF KMMK and SMK must be the same

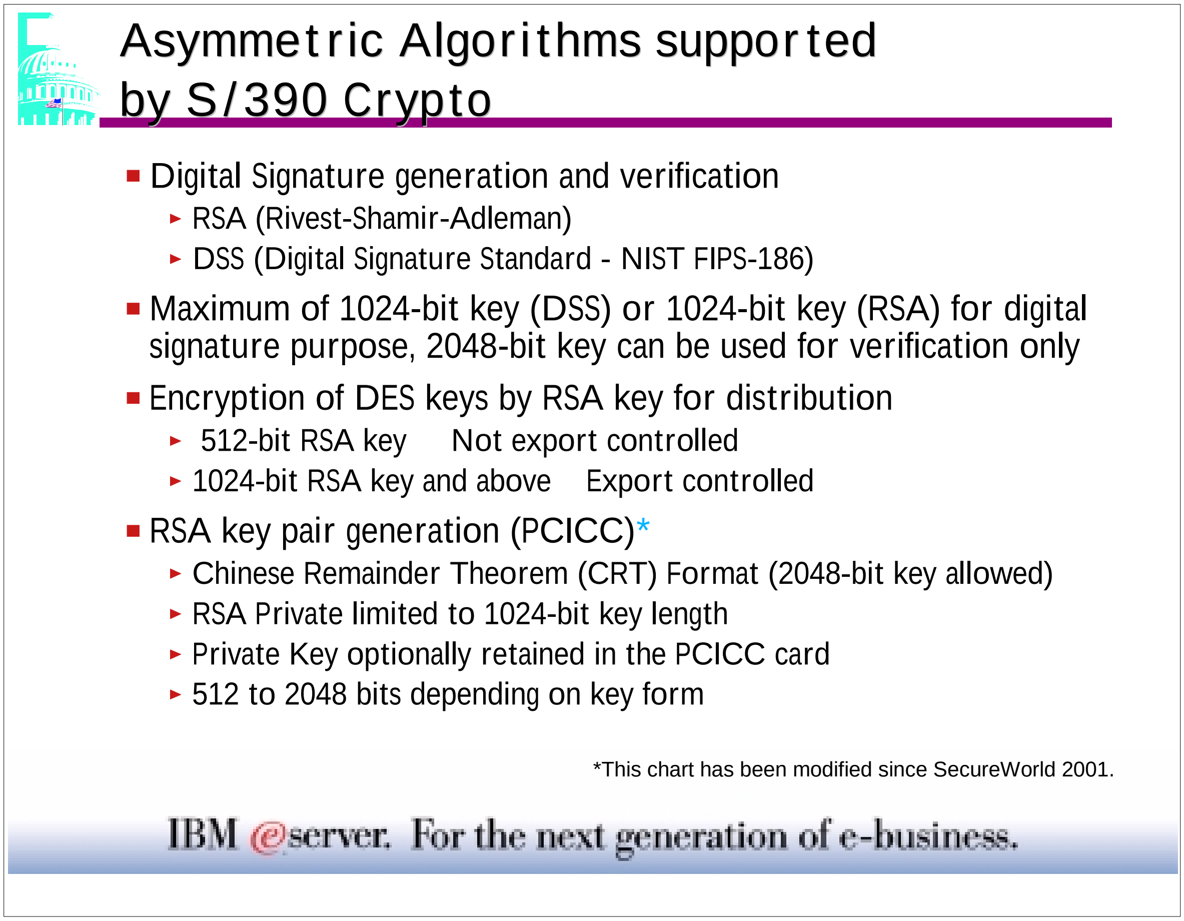
IBM @server. For the next generation of e-business.



## Symmetric Algorithms Supported by S/390 Crypto

- DES (Data Encryption Standard) :
- performed on 64 bit blocks of data, using :
  - single key (64 bit key, 56 used) - ECB or CBC
  - double key (128 bit key, 112 used) - CBC
  - triple key (T-DES, 192 bit key, 168 used) - CBC
    (only on 9672 G4 and above with correct LIC)
- TDES is subject to export regulation for some industries
- CDMF (Commercial Data Masking Facility) :
  - 'light' DES : 64 bit key, 40 used
- CDMF is not subject to export regulation and not generally used

IBM @server. For the next generation of e-business.

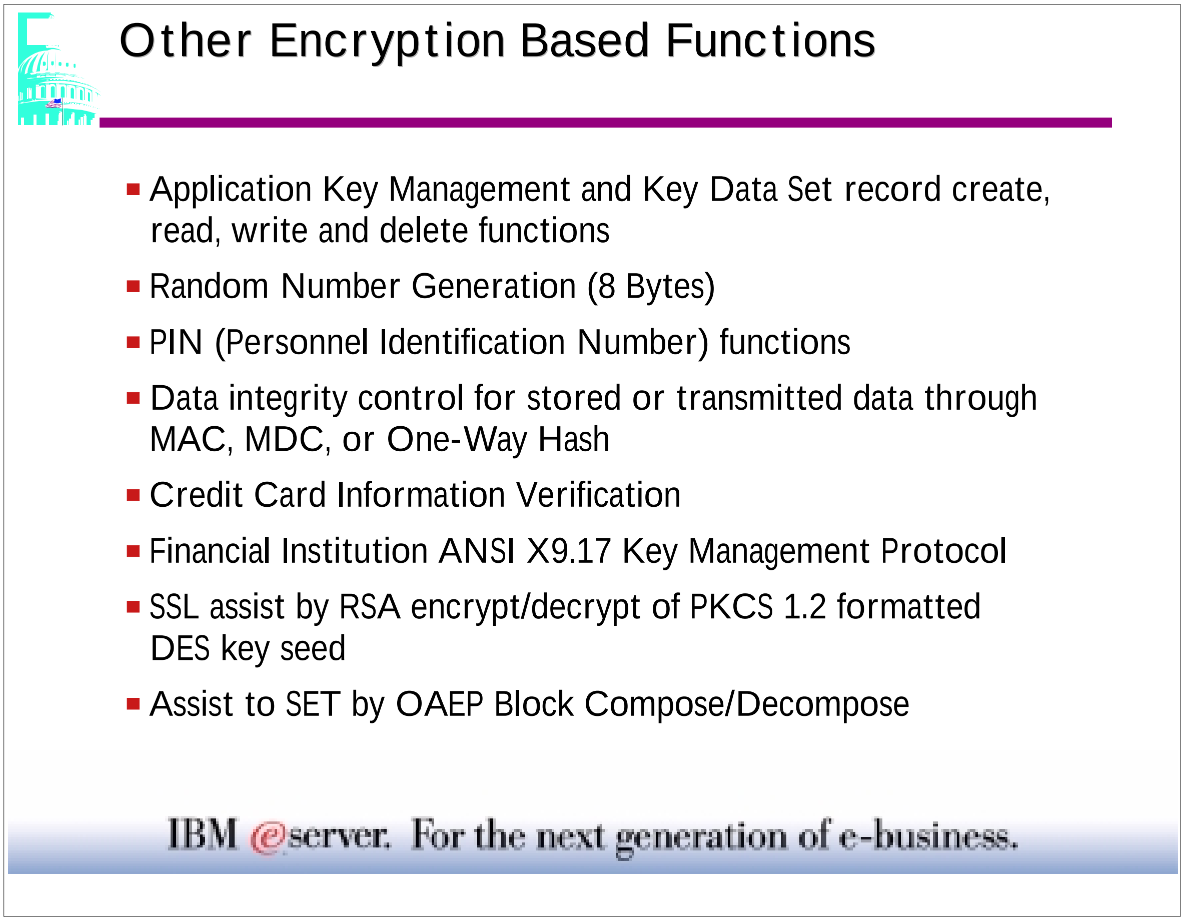


## Asymmetric Algorithms supported by S/390 Crypto

- Digital Signature generation and verification
  - RSA (Rivest-Shamir-Adleman)
  - DSS (Digital Signature Standard - NIST FIPS-186)
- Maximum of 1024-bit key (DSS) or 1024-bit key (RSA) for digital signature purpose, 2048-bit key can be used for verification only
- Encryption of DES keys by RSA key for distribution
  - 512-bit RSA key     Not export controlled
  - 1024-bit RSA key and above     Export controlled
- RSA key pair generation (PCICC)*
  - Chinese Remainder Theorem (CRT) Format (2048-bit key allowed)
  - RSA Private limited to 1024-bit key length
  - Private Key optionally retained in the PCICC card
  - 512 to 2048 bits depending on key form

*This chart has been modified since SecureWorld 2001.

IBM @server. For the next generation of e-business.



## Other Encryption Based Functions

- Application Key Management and Key Data Set record create, read, write and delete functions
- Random Number Generation (8 Bytes)
- PIN (Personnel Identification Number) functions
- Data integrity control for stored or transmitted data through MAC, MDC, or One-Way Hash
- Credit Card Information Verification
- Financial Institution ANSI X9.17 Key Management Protocol
- SSL assist by RSA encrypt/decrypt of PKCS 1.2 formatted DES key seed
- Assist to SET by OAEP Block Compose/Decompose

IBM @server. For the next generation of e-business.

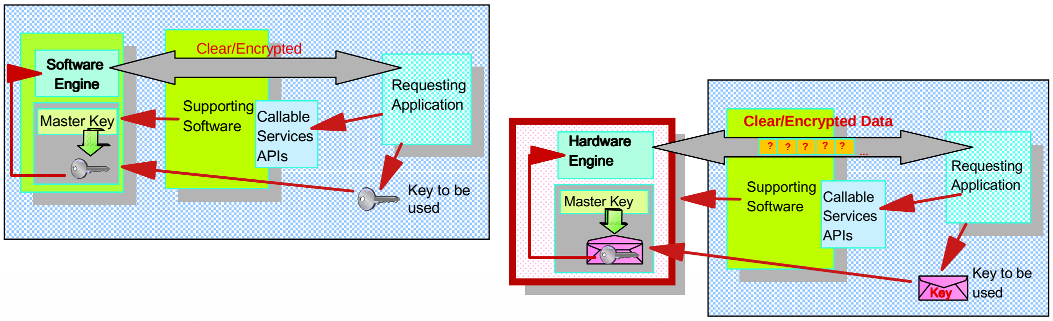
# Symmetric (DES) Key Storage

- DES Key protection is performed by use of a system Master Key
  - Master Key is clear string data, unencrypted, and unusable by direct application programming interfaces
  - Application Keys are protected under encipherment of the system Master Key
- Keys are nothing more than random strings of hexadecimal digits.
  - 2 digits per byte, 8 byte key = 16 digits, etc.
  - Example:

1AEF 880B D622 9AB4   7CCF 0CD7 32E4 48DB

# Application Key Storage

- DES Application Keys that have associations beyond a session must be stored within the system in some DASD data set.
- These application keys need to be
  - Protected from viewing
  - Converted to their clear form prior to processing a request



# Asymmetric Key Storage

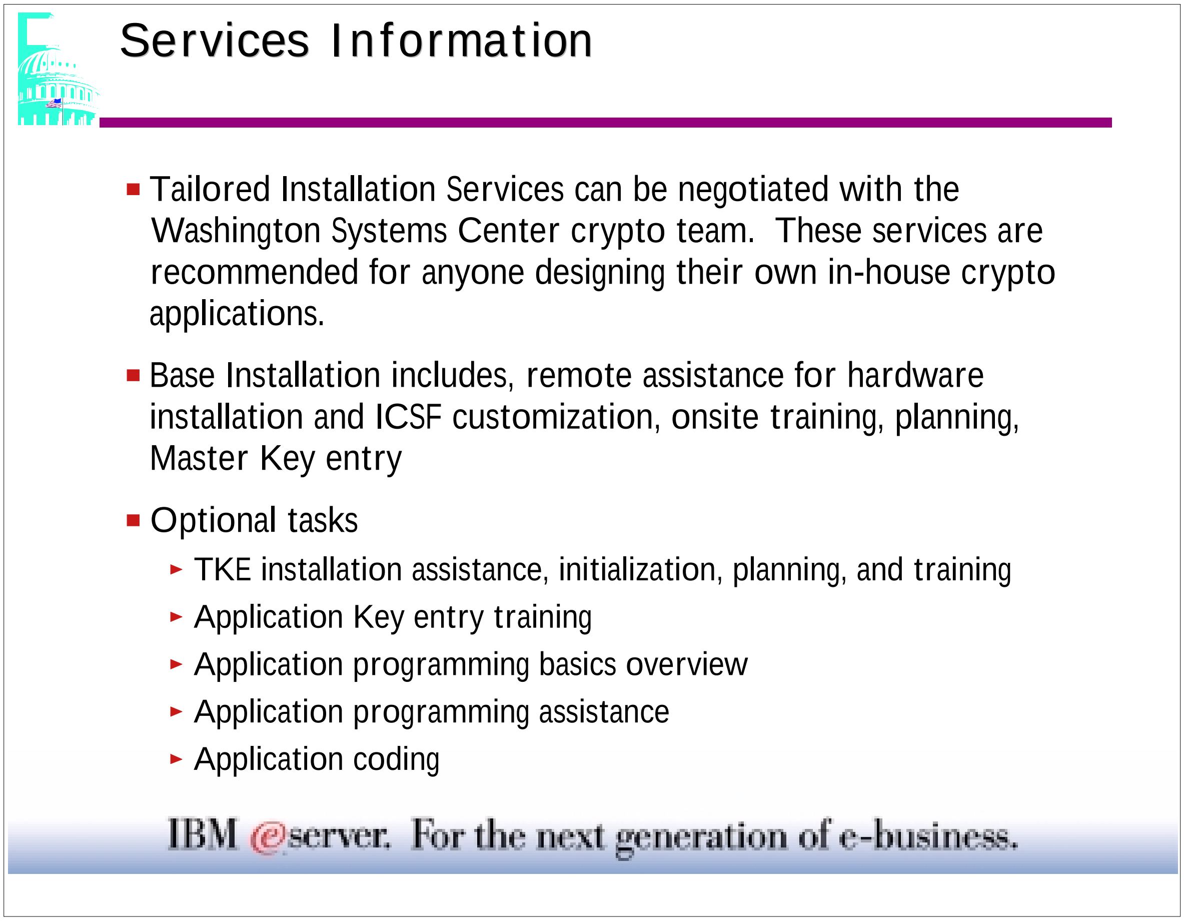
- Asymmetric Key protection is also needed since private key values should remain private and secret without access by other than the owner.
- In OS/390 and z/OS asymmetric keys, RSA keys, can be stored in ICSF's public key data set (PKDS) either
  - By use of RACF's RACDCERT command support, or
  - By application code which performs the work necessary to import the key into the ICSF key format
- In software implementation RSA keys are generally stored in UNIX keyrings or some file structure. The key may or may not be protected by some password mechanism.

IBM @server. For the next generation of e-business.

# Training Information

- Training classes are taught in Gaithersburg, MD USA and Markham, Ontario Canada periodically, check Learning Services catalogue for country specific schedules
  - ES80A*, Crypto Hardware, ICSF, and TKE Installation and Overview
    - *This course is in the process of being updated and will be given a new course code, CRY30
    - It is a lecture-only workshop.
  - CRY80, ICSF/CCA Programming Workshop
    - This workshop is hands-on lab advanced training requiring prerequisites to have been met for the most beneficial experience. No coding language knowledge is required. Application programmers and ICSF Administrators gain the greatest benefit when attending together.
- Technical Documentation created by Washington Systems Center crypto team is placed on the ATS TechDocs Website

IBM @server. For the next generation of e-business.



# Services Information

- Tailored Installation Services can be negotiated with the Washington Systems Center crypto team. These services are recommended for anyone designing their own in-house crypto applications.
- Base Installation includes, remote assistance for hardware installation and ICSF customization, onsite training, planning, Master Key entry
- Optional tasks
  - TKE installation assistance, initialization, planning, and training
  - Application Key entry training
  - Application programming basics overview
  - Application programming assistance
  - Application coding

IBM @server. For the next generation of e-business.