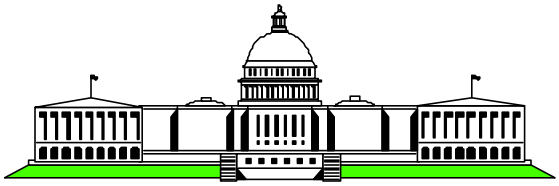
Session 82

Crypto on S/390 and zSeries Overview



IBM WSC: S/390 and zSeries Security

Vanguard's 16th Annual Enterprise Security Expo 2002June 23-28, 2002

Marilyn Frazier Allmond (301) 240-8858 allmond@us.ibm.com

Disclaimer

WSC Advanced Technical Support

The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

Trademarks

WSC Advanced Technical Support

IBM @server zSeries

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

eNetwork	DFSMS/MVS	IMS/ESA	RAMAC
geoManager	DFSMSdfp	IP PrintWay	RMF
AD/Cycle	DFSMSdss	IPDS	RS/6000
ADSTAR	DFSMShsm	Language Environment	S/390
AFP	DFSMSrmm	Multiprise	S/390 Parallel
APL2	DFSORT	MQSeries	Enterprise Server
APPN	Enterprise System/3090	MVS/DFP	SecureWay
BookManager	Enterprise System/4381	MVS/ESA	
BookMaster	Enterprise System/9000	Network Station	Sysplex Timer
C/370	ES/3090	NetSpool	System/390
CallPath	ES/4381	OfficeVision/MVS	SystemView
CallPath CICS/MVS	ES/9000	Open Class	SOM
CICS*	ESA/390	OpenEdition	SOMobjects
CICS/ESA	ESCON	OS/2	SP
CICS/MVS	First Failure	OS/390	VisualAge
CICSPlex	Support Technology	Parallel Sysplex*	VisualGen*
COBOL/370	FlowMark	Print Services	VisualLift*
DataPropagator	FFST	Facility	VM/ESA*
DisplayWrite	GDDM	PrintWay	VTAM
DB2*	ImagePlus	ProductPac	WebSphere*
DB2 Universal	Intelligent Miner	PR/SM	3090
Database	IBM*, IBM logo*	QMF	3890/XP
DFSMS	IMS	RACF	
z/Architecture	z/OS	zSeries	z/VM

* Registered trademarks of IBM Corporation

Trademarks

WSC Advanced Technical Support

IBM @server zSeries

The following are trademarks or registered trademarks of other companies.

DFS is a trademark of Transarc Corporation
Lotus, Notes, and Domino are trademarks or registered trademarks of Lotus Development Corporation
LINUX is a registered trademark of Linus Torvalds
Penguin (Tux) complements of Larry Ewing
Tivoli is a trademark of Tivoli Systems Inc.
Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
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.
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.

Discussion Agenda

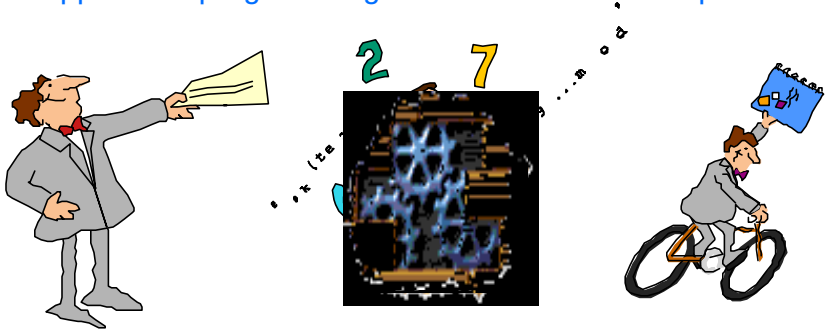
WSC Advanced Technical Support

- What is the IBM Crypto
- How is Crypto used
- What is it used for
- Benefits of using
- Other Good Stuff for Reference
  - New, Changed Function
  - Order Snapshot
  - Install HiLevel Checklist
  - Common things that can go wrong
  - Reference List for pubs, training, resources

What is Crypto?

WSC Advanced Technical Support

- Cryptography is the science of transforming text into some unintelligible code.
  - Today cryptography is done using mathematical algorithms.
  - Cryptographic systems use
    - Cryptographic engines; hardware or software
    - Keys
    - Application programming interface to make a request



What is Crypto on IBM Mainframes?

WSC Advanced Technical Support

- **Cryptography on zSeries and z/OS**
  - **Hardware engines that can be exploited for performance and function using a software interface**
  - **Standalone software programming enablers that are provided either as separate requirement or as an integrated part of a product**
    - Integrated Cryptographic Services Facility (ICSF)
    - Open Cryptographic Services Facility (OCSF)
    - System SSL
    - Using a software engine, such as, BSAFE(tm), a RSA(tm) toolkit
- **Most Software crypto exploiters in the "z/OS" family allow exploitation of the hardware engines**

Mainframe Crypto Hardware

WSC Advanced Technical Support

- **Standard Cryptographic Coprocessor Facility, 0800**
  - **Serves as the base hardware for the other crypto hardware features in a OS/390 and z/OS operating environment**
  - **Physically attached to CP, limit of 2 CCFs per machine**
  - **Available on 9672 G3, G4, G5, G6, Multiprise 2000/3000, z900 and z800**
- **PCI Cryptographic Coprocessor, 0860 on G5/G6 and 0861**
  - **Serves as a growth platform for new function, algorithms, etc.**
  - **Attached via STI, limit of 8 PCICCs per machine**
  - **Only available on 9672 G5/G6 and z900/z800**
- **PCI Cryptographic Accelerator, 0862 on zSeries only**
  - **Serves as an accelerator for SSL handshakes where clear keys are used**
  - **Attached via STI, limit of 6 PCICAs per machine**
  - **Only available on zSeries**
- **Trusted Key Entry Workstation**

Mainframe Crypto Hardware - z990 only

WSC Advanced Technical Support

- **Standard CP for Cryptographic Functions (no feature code)**
  - Serves as the base hardware for the other crypto hardware features on z990
  - Physical associated with each PU hardware, no limitation
- **PCI Cryptographic Accelerator, 0862**
  - same as on z900/z800
- **PCI XCryptographic Coprocessor, 0868 (10/31/03)**
  - Provides the secure key function available with CCF and PCICC
  - Attached via STI, limit of 4 PCIxCCs per machine
- **All Crypto Hardware Must Be ENABLED Prior to Use (except PCICA)**
- **Software Application Programming Interface**
  - For CCF, PCICC, PCICA, and PCIXCC this is provided by ICSF, Integrated Cryptographic Service Facility, a part of the z/OS and OS/390 base element Cryptographic Services

9672, Multiprise, z900/z800 Crypto Hardware

WSC Advanced Technical Support

	CCF	PCICC	PCICA
Available on Multiprise and 9672	x		
Available on G5/G6		x	
Available on z900/z800		x	x
# of Processor Cards/Modules per Feature	1	1 on G5/G6 2 on z900/z800	2
Charged Feature US	Multiprise, G3, and z800	x	x
Hardware Feature Code	0800	0860 on G5/6 0861 on z900/z800	0862
Requires Enablement prior to use (FC)	x (0825, 0835, or 0875 depending on server)	x (0865)	

9672, Multiprise, z900/z800 Crypto Hardware . . .

WSC Advanced Technical Support

	CCF	PCICC	PCICA
Requires LPAR Definitions prior to use using Image Profile	x Processor and Crypto Pages	x PCI Page	x PCI Page
Requires Use of CHPID		x	x
Assists SSL Handshake Performance	x	x	x
Assists SSL Client Authent'n Performance	x	x	
Assists SSL Record Layer Performance	x **(DES, TDES only)**		
Supported in Linux OS		x, not used if PCICA installed and available	x

z990 Crypto Hardware

WSC Advanced Technical Support

	CPACF	PCIXCC	PCICA
Available on z990	x	x	x
Available on G5/G6			
Available on z900/z800			x
# of Processor Cards/Modules per Feature	na - with each PU	1	2
Charged Feature US	x	x	x
Hardware Feature Code	na	0868	0862
Requires Enablement prior to use (FC)	x **(3863)**	(using CPACF data)	

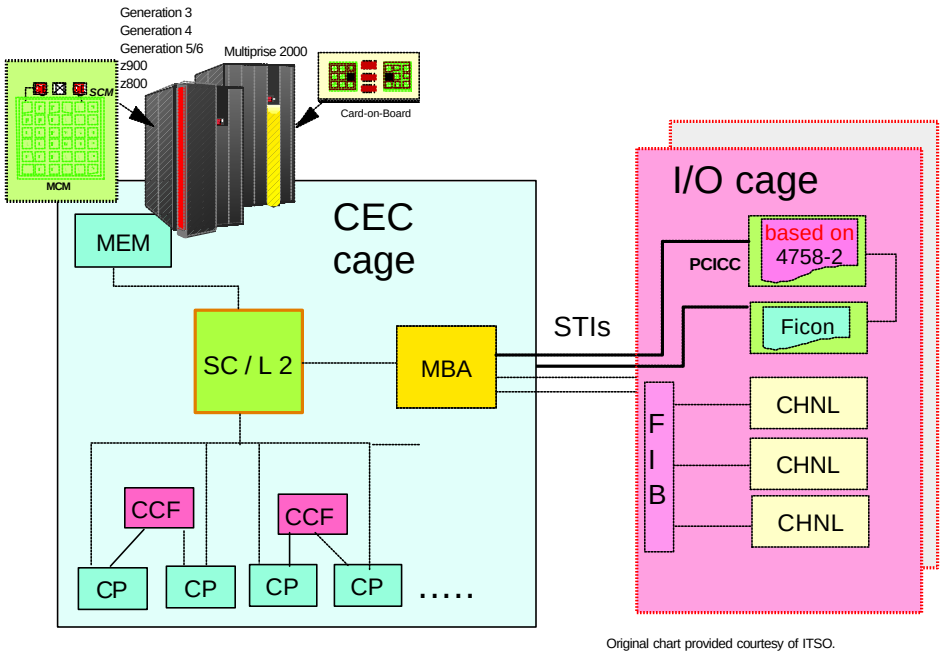
z990 Crypto Hardware . . .

WSC Advanced Technical Support

	CPACF	PCIXCC	PCICA
Requires LPAR Definitions prior to use using Image Profile	x PCI Page	x PCI Page	x PCI Page
Requires Use of CHPID	intentionally left blank		
Assists SSL Handshake Performance			x
Assists SSL Client Authent'n Performance		x	
Assists SSL Record Layer Performance	x **(DES, TDES only)**		
Supported in Linux OS		SOD	x

Crypto Hardware Connectivity

WSC Advanced Technical Support



Original chart provided courtesy of ITSO.

OS/390 and z/OS and Crypto Hardware

WSC Advanced Technical Support

Integrated Cryptographic Services Facility, ICSF

- **Interface to the Crypto Hardware for**
  - **Key Entry for both system master keys and application use keys**
  - **Application Programming Interfaces (APIs) that pass requests to the crypto hardware**
- **Started Task**
- **Runs in its own address space**
- **Has associated data space**
- **Has system level data sets that must be available to become active**
- **Must be active in OS/390 and z/OS environments to have access to hardware**
- **IS NOT a cryptographic engine**

Linux and Crypto Hardware

WSC Advanced Technical Support

Linux Operating System

- **Hardware support is for SSL handshakes**
- **Application Programming Interface is via software driver which is part of Linux code**
  - **Primary requests will be RSA encrypt/decrypt of DES key data**
- **Both PCICC and PCICA hardware features support requests within a Linux OS**
  - **When both PCICC and PCICA are present, only PCICA is used**
  - **Since only clear keys are used in this environment, PCICA is the better high speed performer so PCICC is not needed. Routing is not a user controllable function**
  - **PCICA only available on zSeries**

How is Crypto Invoked?

WSC Advanced Technical Support

- Application must request function of the crypto hardware
- This is done by
  - APIs being issued to ICSF and ICSF passing the request
    - User written code
    - IBM product code
  - requests made via crypto driver interface to PCI crypto
- Application must request function of software crypto
- This is done by
  - APIs being issued
    - OCSF
    - System SSL
    - BSAFE
    - etc.

What is Crypto Used For?

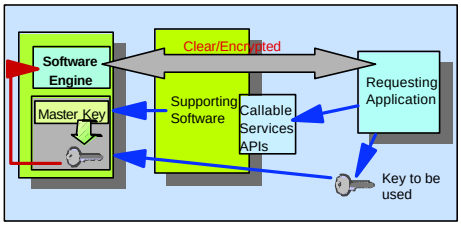
WSC Advanced Technical Support

- Privacy
  - Providing Confidentiality
- Data Integrity
  - Providing notice of change to original
- Authentication
  - Verification of who, what via presentation of something
- Generally, a part of some overall security task involving multiple activities and perhaps multiple crypto functions/products/etc.

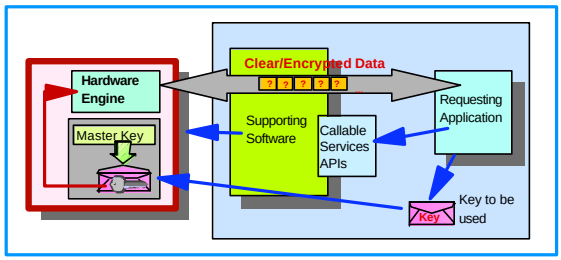
Advantages

WSC Advanced Technical Support

- **Hardware Crypto devices are more secure than software crypto engines**
  - **DES algorithms usually have a system master key than is stored in clear text**
- **More secure key storage than software**
  - **Multiple encipherment of application keys**
  - **Ability of using optional PCICC for retained key support**



Software Engine
Key is stored in Control Block



Hardware Engine : Key stored in Tamper-resistant area

Security for Crypto

WSC Advanced Technical Support

- **Hardware allows you to erase ("zeroize") system master key data via a process that overwrites the storage area with binary zeroes.**
- **System Master Keys used to protect application keys via multiple encipherment once imported into ICSF**
  - **Multiple key parts entered to comprise a final key value**
  - **Key part is same length as final key**
    - 16-bytes, 128-bit for DES Master Key
    - 24-bytes, 192-bit for PKA Master Keys
  - **Strong security begins with management practice for key entry**
  - **Dual key officers at minimum with job separation**
  - **Secure key parts in tamper-evident/resistant envelopes in lock box that has management controls and logs as dictated by site policy**

Security for Crypto . . .

WSC Advanced Technical Support

- ICSF datasets require protection to prevent denial of service and loss of data integrity
- ICSF Key Generation Utility datasets require protection to prevent possible DES application key value exposure
- Use of coax-connected terminal in secure area will provide connectivity security for key entry from ICSF Panels
- Application keys cannot be entered in parts from the ICSF product panels. However, there is a sample application for entering application key parts via ISPF panels on the ATS TechDocs website

Security for Crypto . . .

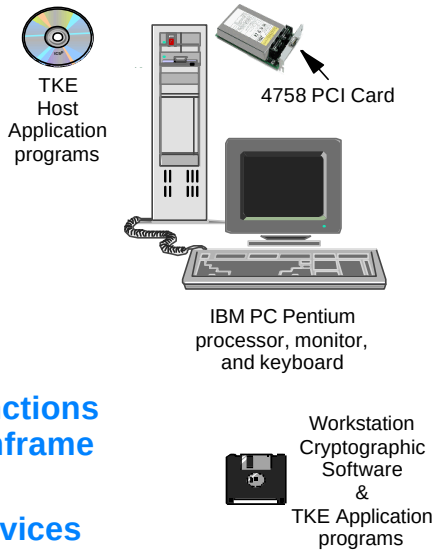
WSC Advanced Technical Support

- For Application Keys, ICSF has 2 general resource classes defined for SAF access control
  - CSFSERV for protection and control of application programming interfaces and selective hardware functions
  - CSFKEYS for protection and control of application keys based on the key label
- Recommend protecting functions that may cause disruptions or potential exposure of sensitive information
- For really secure entry of application key values, might consider TKE workstation

Trusted Key Entry Workstation

WSC Advanced Technical Support

- Charged Feature
- TCP/IP connection on TKE V3
- Includes cryptographic hardware
  - 4758 PCI Card
  - Workstation software
  - TKE Application software
- TKE provides ability for
  - granular control over functions
  - approval requirement prior to functions being performed by the IBM mainframe CCA hardware
  - remote management of crypto devices
  - management of multiple servers and/or multiple IBM mainframe crypto devices from a single TKE

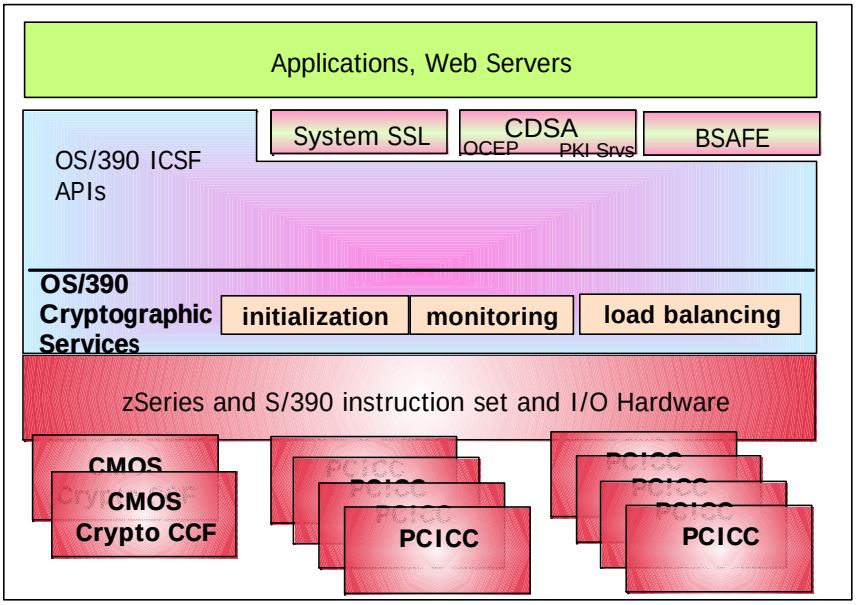


TKE Workstation . . .

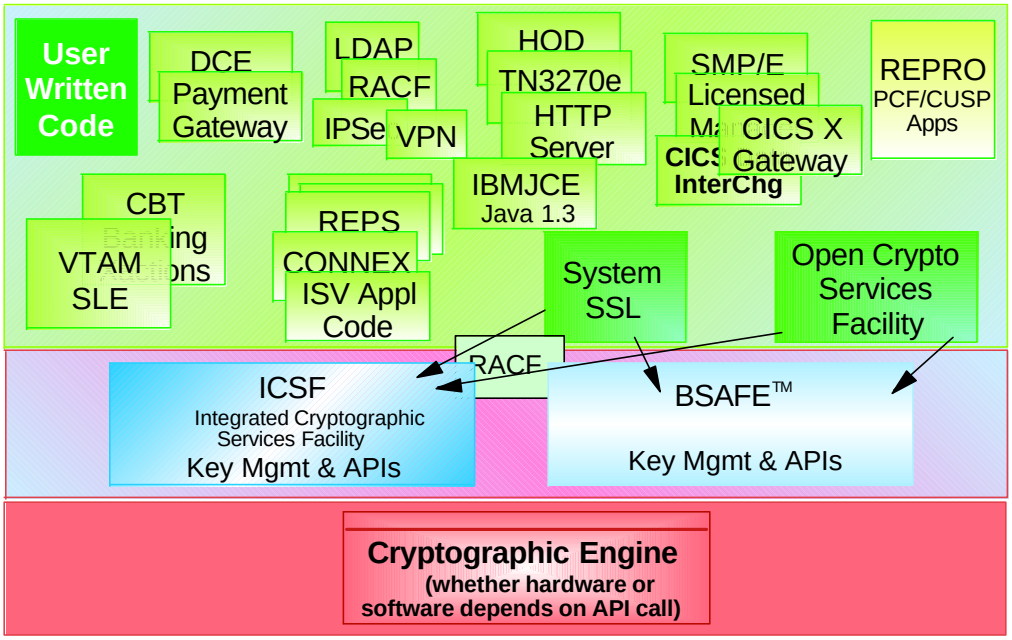
WSC Advanced Technical Support

- Provides more secure key entry via
  - Authentication to host and recognition of host crypto
  - Digital Signatures are used for authentication
  - Key parts protected with a Diffie-Hellman generated transport key
- Use of TKE provides much more secure key entry and key part entry for all but DATA key types
- Allows flexibility in control via
  - Multiple administrative levels
  - Management of host control capabilities from TKE
- TKE requires secure physical protection
- Management procedures are required to provide and ensure the level of security required by site policy

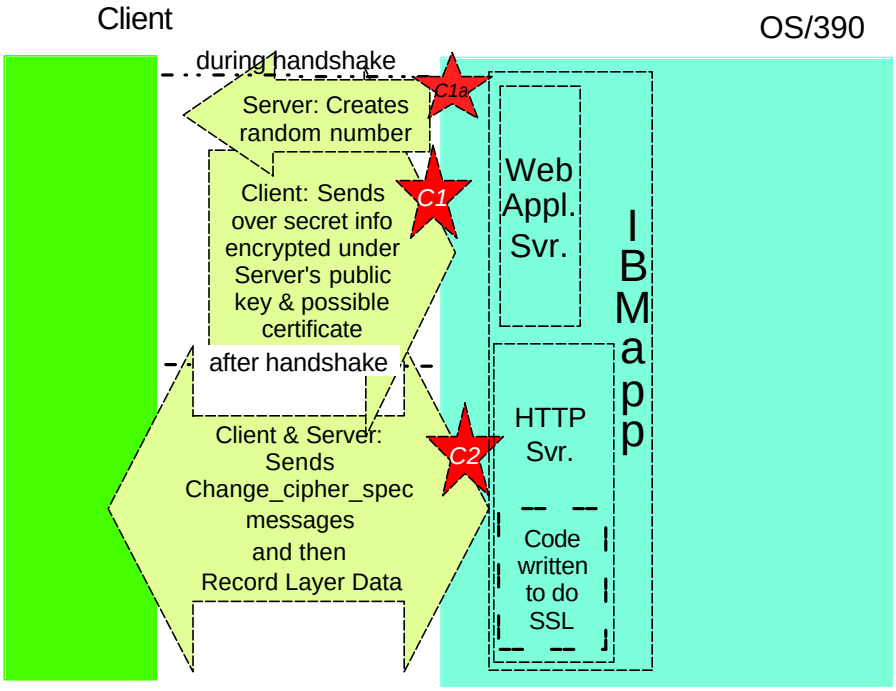
IBM zSeries and IBM S/390



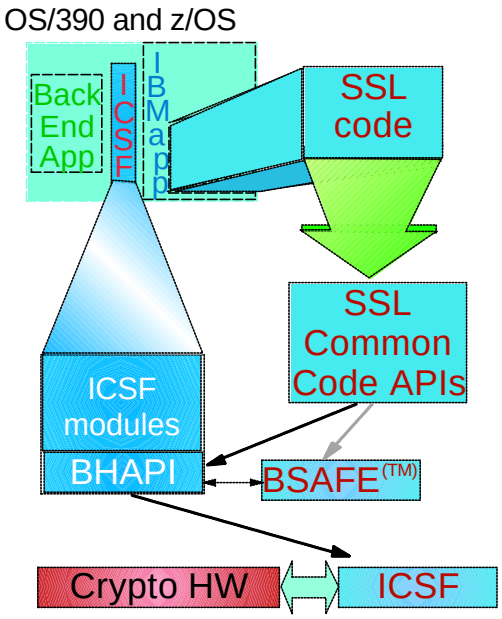
IBM Crypto Software



Crypto Usage By SSL Server Code



SSL Usage & Crypto Hardware



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.

Similar flows occur for IPSec Crypto requests.

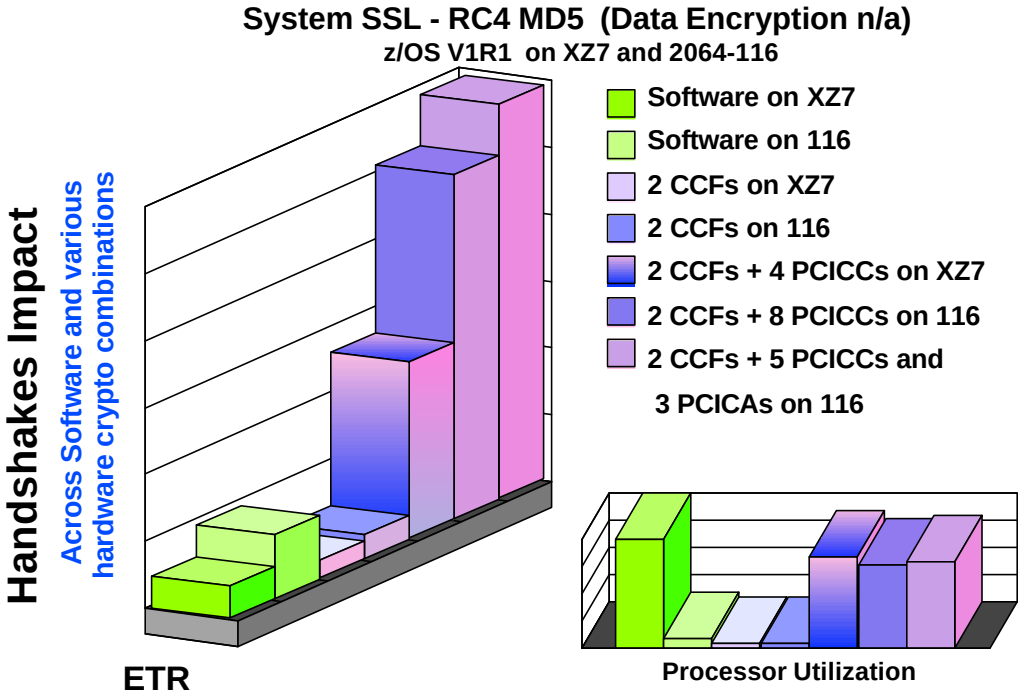
Performance Advantages

WSC Advanced Technical Support

- **Performance improvements for certain operations**
  - **Less CPU utilization**
  - **More throughput**
- **Rough Interpretation of Benchmark Data* For SSL Server transactions is that**
  - **2 CCFs will outperform software on X47 but not XZ7**
  - **Adding 4 PCICC features increases throughput**
    - 850% over that of a single (1) CCF on X47 and
    - slightly over 600% over 2 CCFs on XZ7
  - **100% Caching will outperform 0% caching even with crypto hardware**
  - **Client Authentication will decrease transaction throughput anywhere from 55% to 75% depending on software release and hardware**

Performance Advantages: For SSL Server transactions

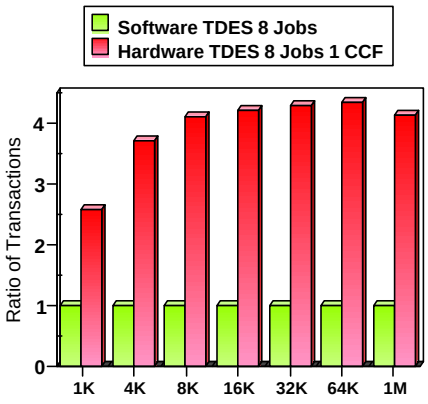
WSC Advanced Technical Support



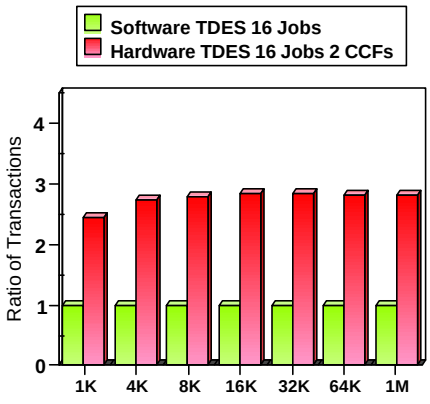
Performance Advantages: For Encryption . . .

WSC Advanced Technical Support

- 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 V1R1
TDES Processing Comparison
using 2 CCFs

Performance Advantages . . .

WSC Advanced Technical Support

- Rough Rule of Thumb for Crypto Hardware Features
  - Order based on functions Required
  - If Application coding using ICSF APIs, then PCICC may be required for functions only available on that feature
  - If SSL support only

Feature	SSL Handshakes	Comment
0800 1 CCF	70	
0800 2 CCFs	140	
0860 PCICC on G5/G6	130	Note: Handshake growth is not exponential per additional feature.
0861 PCICC on zSeries	260	
0862 PCICA on zSeries	2140	

Other Good Stuff
Reference Pages
(So much to tell and not enough time)

New Function Summary

WSC
Advanced Technical Support

API CSNDKTC	PKA Key Token Change	Changes PKA internal key tokens (RSA and DSS) from encipherment with the old PCICC asym-MK to encipherment under the current PCICC asym-MK
API CSNBSKY	Secure Messaging for Keys	Encrypts a text block, including a clear key value decrypted from an internal or external DES token.
API CSNBSPN	Secure Msging for PINs	Encrypts a text block, including a clear PIN block recovered from an encrypted PIN block
Install Options DS	PKDSCACHE	Defines the size of PKDS cache records. Performance improvement for frequently used records
PCICA	Support for	Clear RSA key processes in CSFDPKD service routed to PCICA
PKDS	Reencipher & Activate	Support added to ICSF MK Mgmt Panels and a new utility, CSFPUTIL, added.
UDX	User support	Added support for user written UDXs.
CSNBSYD CSNBSYE	AES Support	2 new API calls added. Clear keys only

Changed Function Summary

WSC Advanced Technical Support

- **DOMAIN in Installation Options becomes an optional parameter unless more than 1 domain is specified on the Usage Domain window in the Image profile or if running in native mode.**
  - **CSFM409E Multiple Domains Available, Select One in the Options Data Set**
- **MAXLEN parm checking eliminated for**
  - **Encipher/Decipher and compatibility CIPHER service**
  - **MAC generate/verify**
  - **Ciphertext Translate**
  - **MDC generate**
- **Pass Phrase Initialization allows uninitialized PCICC to be initialized without processing all CCFs.**

Deleted Function Summary

WSC Advanced Technical Support

- **IEC161I eliminated during first time startup of ICSF**
- **X'18F' eliminates reason codes below, replacing each with a message**
  - **RC x'3C' replaced by CSFM105E**
  - **RC x'48' replaced by CSFM120E**
  - **RC x'1B' replaced by CSFM410E**
  - **RC x'4B' replaced by CSFM107E**
  - **RC x'106' if no configuration X'18F' RC '4A', otherwise CSFM113E**

Ordering

WSC Advanced Technical Support

- **Security - Enablement Diskette Configuration data for CCFs**
  - **0874/0875 for z900**
  - **~~0865~~ 0875 for z800**
  - **0834/0835 for G6, G5, G4**
  - **0824/0825 for Multiprise 3000**
    - Note: Not all server models have or allow access to 2 CCFs
- **TKE Workstation based on connectivity**
  - **Token-Ring 0866, newer workstation models - 0876**
  - **Ethernet 0869, newer workstation models - 0879**
    - Note: TKE is for more secure key entry only! It is only needed, if security requirements mandate that no key part or value may exist in clear even for an extremely short time.

Ordering . . .

WSC Advanced Technical Support

- **PCICC**
  - **0860 on G6/G5 1 engine per feature**
  - **0861 on zSeries 2 engines per feature**
  - **Total of 8 max**
  - **FCV - configuration data - 0864or 0865**
- **PCICA 0862 5 engines ~~per feature~~**
  - **Total of 6 max**
- **Note that any combination of PCI features may not exceed a total of 8**

Installation

WSC Advanced Technical Support

- **Check PSP Bucket and EC levels for latest APARs and requirements**
- **Hardware Install**
  - **Order Configuration Data for hardware features to be used**
  - **Enablement done by IBM CSR**
    - Load Configuration Data
    - Select for Next Activation
  - **Requires Power On Reset for enablement to be complete for CCFs**
- **Associate LPARs with crypto hardware**
  - **Identify CCFs to each logical partition**
  - **Define the crypto characteristics to be associated with the image**
  - **Identify any PCI features to each logical partition**

Installation . . .

WSC Advanced Technical Support

- **ICSF Software Activation**
  - **ICSF modules APF and LNKLST**
  - **Key Data Sets defined**
  - **STC defined**
  - **ICSF ISPF data sets concatenations added**

  Reference the ICSF System Programmer's Guide
- **Master Key Entry for DES and PKA**
  - **If PPINIT used, change MKs to known values**
  - **For security purposes, dual custody of key values**

  Reference the ICSF Administrator's Guide and/or the TKE Workstation 2000 User's Guide
- **If crypto applications planned, consider attending a workshop for training on how the hardware and software work together to be able to anticipate impacts to operations.**

Best Practices for Crypto Hw & ICSF

WSC Advanced Technical Support

- Master Key values kept and enter under dual custody
- Change Process updated to include Crypto impact
- Weigh risk for key parts with clear key value entry from TSO
- Define Policy for Master Key changes and Transport Key changes
- Understand application design impacts BEFORE application coding started
- If using TKE, Backup before you start and test settings before changing Authority 1
- Get training

Common Problems for Crypto Hw & ICSF

WSC Advanced Technical Support

HW Setup

- Check for configuration loaded AND selected - otherwise, POR
  - If configuration exists, must specify FORCE to obtain new one, if desired. Reentry of master key values required.
- If TKE, check for PKSC Initialized
- Check domain specifications and crypto characteristics for Image
  - Usage # must be one used by ICSF on that LPAR
  - If TKE, control must have all # listed for all LPAR crypto areas to be managed when TKE is active on this particular LPAR
  - If TKE, Modify Authority must be active (dynamic change)

Common Problems for Crypto Hw & ICSF . . .

WSC Advanced Technical Support

ICSF Setup

- Check for correct allocation of key data sets
- Check for correct name of key data sets
- DELETE, PURGE, and ERASE CKDS/PKDS, if redefining
- Use correct domain number
- Verify ICSF Initialization of CKDS completed correctly - CKDS should have a minimum of 5 records
- ICSF cannot be used until Master Keys defined

Common Problems for Crypto Hw & ICSF . . .

WSC Advanced Technical Support

ICSF Usage Tips

- Check for correct name of key data sets
- If verification pattern error for CKDS, your CKDS name is incorrect. Fix by
  - Either refreshing the CKDS and specifying the correct name
  - Or, reentering the master key values that were valid when the CKDS was last used.
- ICSF will initialize even if crypto modules do not come online!
  - Means error in setup
  - ICSF provides you chance to correct
- If Master Key values lost, CHANGE MASTER KEY before DR required
- Deletion of CKDS or PKDS may render data unrecoverable

Reference: Training

WSC Advanced Technical Support

- **Training**
  - **ICSF Programming Workshop**
    (Course Code CRY80 for US and ES80P for Canada)
    Gaithersburg, Maryland, USA
    ~~July 9 - 12, 2002~~
    October 1 - 4, 2002
    Toronto, Canada
    November 5 - 8, 2002
  - **S/390 & zSeries Crypto Hardware, ICSF, TKE Installation and Overview Workshop**
    - (Course Code ES801 for US and ES800 for Canada)
      Gaithersburg, Maryland, USA
      September 16 - 20, 2002
      Toronto, Canada
      October 21 - 25, 2002

Reference: Publications

WSC Advanced Technical Support

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	TKE Workstation User's Guide 2000
GC22-7236	SB10-6802	PR/SM Planning Guide
GC38-3119	SC28-6811	Support Element (SE) Operations Guide
GC38 -0608	(G6)	SE Operations Guide
SC28-6811	(zSeries)	SE Operations Guide

Reference: Publications

WSC Advanced Technical Support

- 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/

Reference: Resources

WSC Advanced Technical Support

- ATS TechDocs Web Site
  - http://www-1.ibm.com/support/techdocs/atsmastr.nsf
  - Choose SEARCH ALL DOCUMENTS use keyword crypto
- More IBM Web Libraries
  - http://www-1.ibm.com/servers/eserver/zseries/library/online_pubs.html
  - http://www-1.ibm.com/servers/eserver/zseries/library/whitepapers/
  - http://www-1.ibm.com/servers/s390/os390/bkserv/redbooks.html
- Standards
  - http://www.ietf.org/
  - http://csrc.nist.gov/cryptval/140-1/1401val.htm
  - http://www.rsasecurity.com/rsalabs/standards/
- Free Stuff
  - http://www.infosecuritymag.com/
  - http://www.scmagazine.com/index2.html
  - http://www.counterpane.com/crypto-gram.html

Acronyms Used

WSC
Advanced
Technical Support

- AES Advanced Encryption Standard
- API Application Programming Interface
- ATS Advanced Technical Support
- CCA Common Crypto Architecture
- CCF Crypto Coprocessor Facility
- CEC Central Electronics Complex
- DES Data Encryption Standard
- FIB Fast Internal Bus
- ICSF Integrated Crypto Services Facility
- MBA Memory Bus Adapter
- OCEP Open Crypto Enhanced Plugins
- OCSF Open Crypto Services Facility
- PCI Peripheral Component Interconnect
- PCICC PCI Crypto Coprocessor
- PCICA PCI Crypto Accelerator
- PKA Public Key Algorithm
- SAF System Authorization Facility
- SSL Secure Sockets Layer
- TKE Trusted Key Entry Workstation
- TLS Transport Layer Security