Vanguard Security Conference

May 31 – June 4 2009 – Jacksonville Florida

Session Title: Overview of Crypto on z

Session ID: CRP-2

Speaker Name: Ernest Nachtigall **CISSP;CISA**

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

- z9 z10 System Overview
- z9 z10 Cryptographic Hardware
- z9 z10 Cryptographic Functionality
- Data Encryption
- SAF Implications

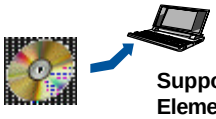
z9 z10 Overview

z ESAME Crypto Solution

z9 z10

FC3863 CPACF clear key

CEX2C encrypted key



Support Element

Trusted Key Entry

What's New for ICSF V1 R10 --- HCR7751

- HCR7751 requires new LIC and some functions are only available on z10
  - z10 Driver 76D (Nov 2008)
  - z9 Driver 67L (Nov 2008)
- Secure AES keys
  - New Master Key Register for AES (32-byte master key)
  - New callable services to use encrypted AES keys
- Key Store Policy which works in conjuction with CSFKEYS
  - New authorization checks
  - New SAF general resource classes
  - New utility for detection of duplicate tokens
- Support for CKDS on System z without CEX2C
  - Caution - CKDS not uniquely identified from secure CKDS
- Support of PAN-14, -15, -17, -18
- New Query services calls to enhance CSFIQF

CPACF *z9 z10*

- DES (56, 112, 168 bit)
- SHA-1, *SHA-256*
- *AES-128*
- *PRNG*

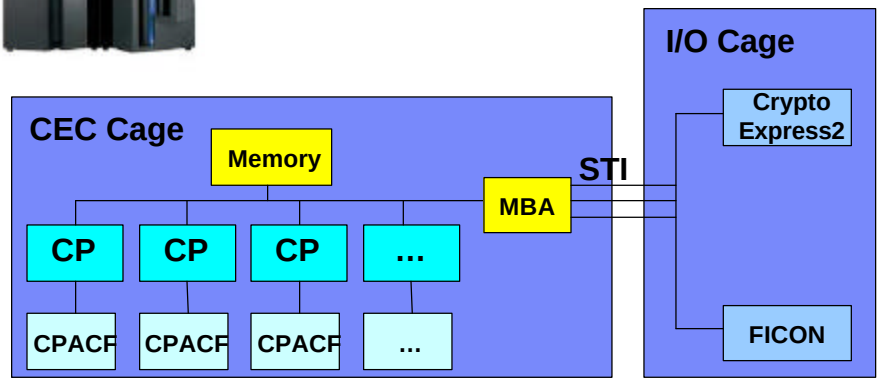
z10

- AES-192, AES-256
- SHA-224, SHA-384, SHA-512

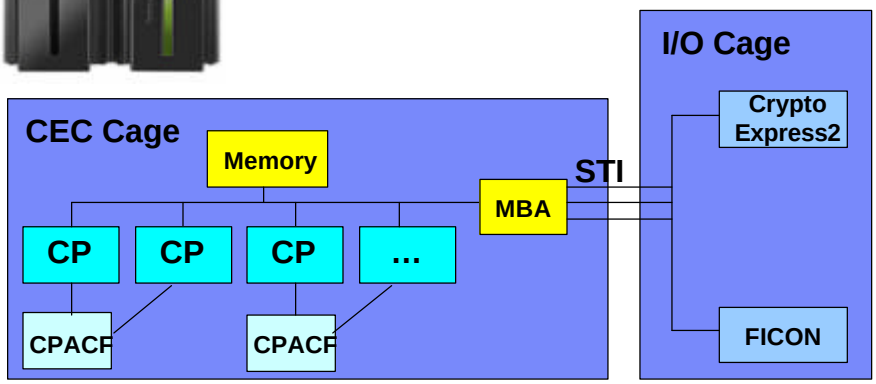
z10 SHA-2

- SHA-224 Initialization value
  - C1059ED8 367CD507 3070DD17 F70E5939 FFC00B31 68581511 64F98FA7 BEFA4FA4
- SHA-256 Initialization value
  - 6A09E667 BB67AE85 3C6EF372 A54FF53A 510E527F 9B05688C 1F83D9AB 5BE0CD19
- SHA-384 Initialization value
  - CBBB9D5DC1059ED8 629A292A367CD507 9159015A3070DD17 152FECD8F70E5939 67332667FFC00B31 8EB44A8768581511 DB0C2E0D64F98FA7 47B5481DBEFA4FA4
- SHA-512 Initialization value
  - 6A09E667F3BCC908 BB67AE8584CAA73B 3C6EF372FE94F82B A54FF53A5F1D36F1 510E527FADE682D1 9B05688C2B3E6C1F 1F83D9ABFB41BD6B 5BE0CD19137E2179

z9 Crypto HW



z10 Crypto HW



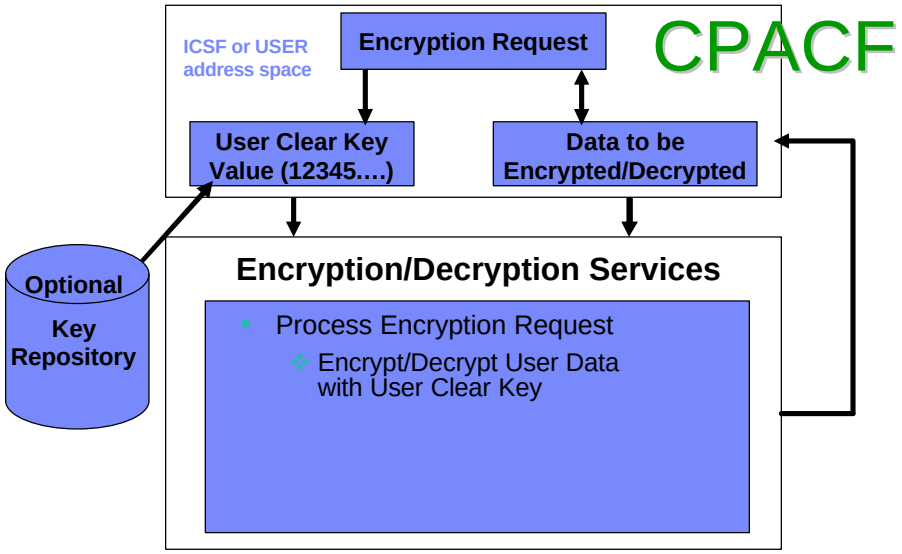
New OP CODES

5 New Machine Instructions
Documented in z/OS™ 1.5+ Principles of Operation (POP)
Never before have crypto instructions been documented
Problem state instructions, as such, can be used directly in applications without going through ICSF.
Instruction Names and Mnemonics
Cipher Message (KM)
Cipher Message with Chaining (KMC)
Compute Intermediate Message Digest (KIMD)
Compute Last Message Digest (KLMD)
Compute Message Authentication Code (KMAC)
Generate Pseudo Random Number

Clear Key Crypto (CPACF)

High Speed Symmetric Algorithms imbedded in each CP
available via ICSF as API's (CSNBSYD/CSNBSYE) or as new operation codes (OP CODES)
"SOFTWARE ENCRYPTION" with algorithm code in hardware
DES TDES SHA-1 AES-128 on z9 (MD5 and AES-192/256 via ICSF)
AES-192 AES-256 SHA-192 SHA-224 SHA-384 on z10
Encryption/Decryption keys are clear (not encrypted) in user address space
typically not appropriate or allowed for sensitive processing such as VISA, MasterCard, INTERAC, LINK
can be mitigated to offer certain in-house functions
file archive to tape (IBM Encryption Facility)
ICSF user defined functions, keys in clear in the ICSF address space only
Specifically designed for WEB (SSL/TLS/TN3270/FIREWALL) type applications, short duration applications, throw-away key values or semi-protected key values (IMS DB2 Data Encryption tool)

Clear Key Processing



CPACF Functions (ASM)

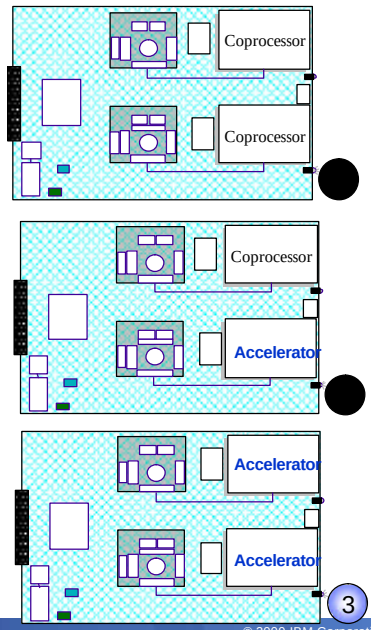
- MSA Instructions
- Clear key
  - Cipher message AES-128/TDES (KM). AES-256 on z10
    - ICSF (CSNBSYE/CSNBSYD)
  - Cipher message with chaining (KMC)
    - ICSF CSNBSYE/CSNBSYD
  - Compute intermediate message digest SHA-1 SHA-256 (KIMD). SHA-224 SHA-384 SHA-512 on z10
    - ICSF CSNBOWH
  - Compute last message digest (KLMD)
    - ICSF CSNBOWH
  - Compute MAC (KMAC)
  - Generate random numbers

Database Encryption

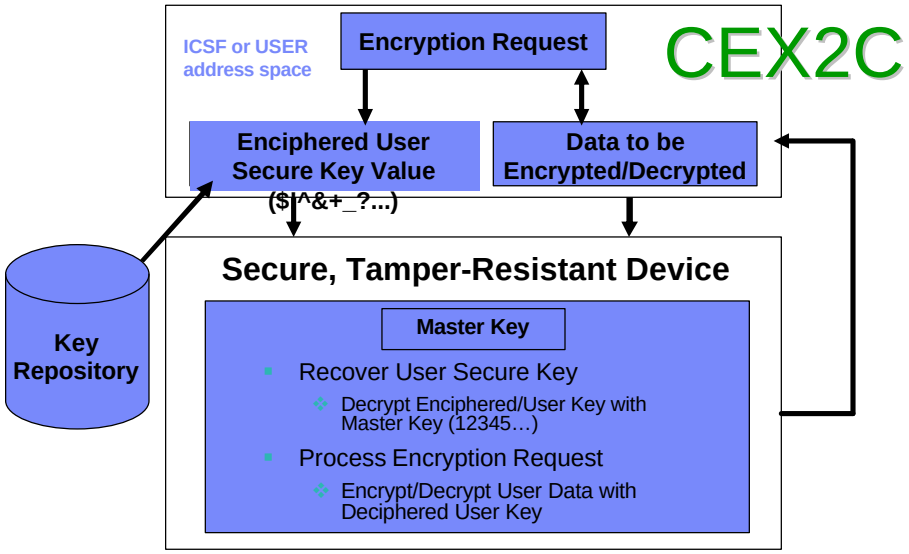
- Data Encryption for IMS and DB2 Databases
- Row level encryption
- No application changes
- Uses EDITPROC
- Provides user-customizable, pre-coded exits for encrypting IMS and DB2 data
- Exploits zSeries and z9/z10 Crypto Hardware features, which results in low overhead encryption/decryption
- Uses the ANSI Data Encryption Algorithm (DEA), also known as the U.S. National Institute of Science and Technology (NIST) Data Encryption Standard (DES) algorithm
- Works at and is customizable at the IMS segment level or DB2 table level
- Conforms to the existing OS/390 and z/OS security model
- Optimized CPACF or CCF processing

z9 z10 Crypto Express2 Configuration

- Secure Coprocessor **(default)**
  - Provides both Secure key" and "Public key" functionality and performance equivalent to PCIXCC/Crypto Express2 features on z990
  - "Secure key" improved performance compared to PCIXCC on z990 (requires multitasking)
  - "Public key" equivalent performance to PCICA on z990
  - No action required (default configuration)
  - SSL at 1000/second
- Accelerator
  - Provides only 3 "Public key" functions with enhanced performance
  - Must be configured using the HMC
  - SSL at 3000/second



Secure Key Processing



ICSF CEX2C Functions

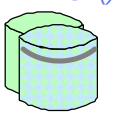
- Encipher/Decipher
  - ICSF CSNBENC/CSNBDEC
- PIN
- MAC
  - X9.9, X9-19
  - ISO16609 CBC TDES MAC
    - Strengthen data integrity
- Random Number Generate
- Key Generate
- Key Management
- Remote key loading for ATM's and POS
  - More flexible key management and privacy

Encryption Options by Machine Type

	z800 z900	z890 z990	z9
CLRTDES	CCF Hardware (25MB second)	CPACF Instruction (150MB second)	CPACF instruction (200MB second)
ENCTDES	CCF Hardware (25MB second)	PCI Hardware (5MB second. Longer path length)	PCI Hardware (5MB second. Longer path length)
CLRAES	General purpose CP (CPU intensive)	General purpose CP (CPU intensive)	CPACF (250-290MB second)

Domain Association Across CEX2C, ICSF, and TKE

LPAR PRD1
ICSF Options Data Set
Domain(5)
CKDSN()
PKDSN()



Look in

5 nia D o m

MK VP

Current Mkeys
New Mkeys
Old Mkeys

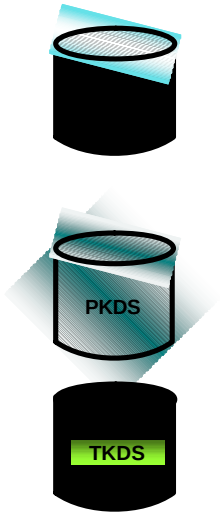
LPAR PRD1 **Support Element**

Usage Domain of 5

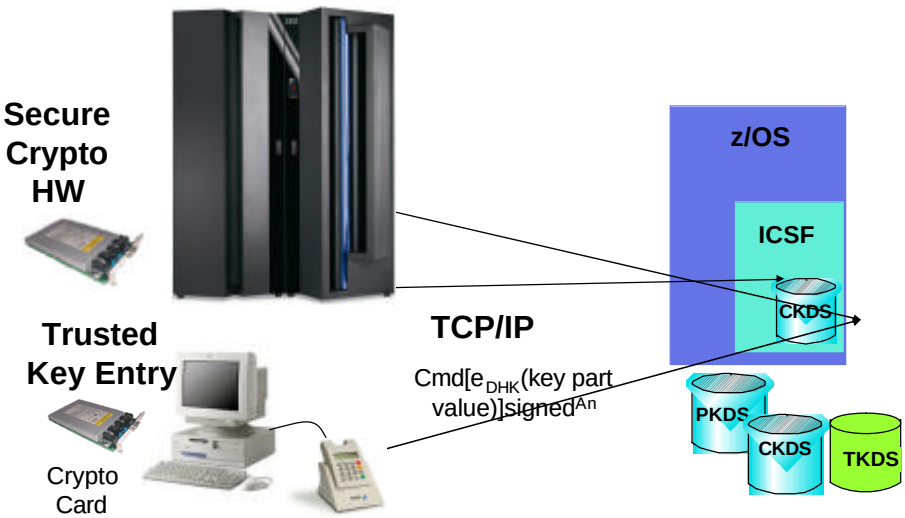
Domain	DES-MK	Old DES-MK	New DES-MK	AES-MK	Old AES-MK	New AES-MK	ASYM-MK	Old ASYM-MK	New ASYM-MK	TKE Controls
0										
5										
.										
15	DES-MK	Old DES-MK	New DES-MK	AES-MK	Old AES-MK	New AES-MK	ASYM-MK	Old ASYM-MK	New ASYM-MK	TKE Controls

Master Keys . . .

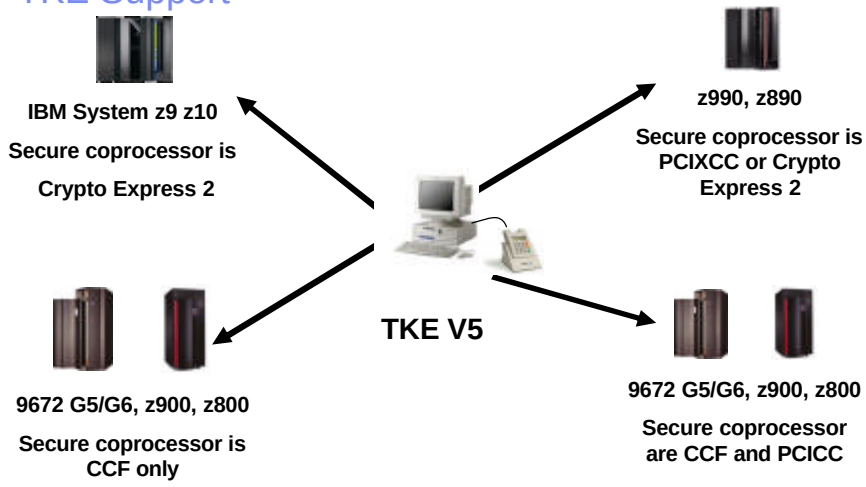
- DES Master Key
  - DES-MK protects secure DES Keys stored in Cryptographic Key Data Set
  - Can change dynamically in native mode
  - Stored in CEX2C, not CKDS
- AES Master Key
  - AES-MK protects AES secure keys stored in the CKDS
  - Can change dynamically
  - Stored in CEX2C, not CKDS
- PKA
  - Called ASYM-MK
  - Protect Application Keys stored in Public Key Data Set (PKDS)
  - Stored in CEX2C, not PKDS
    - PKDS contains ASYM-MK HASH for CEX2C/ICSF verification
- PKCS#11
  - Clear keys



Crypto System



TKE Support

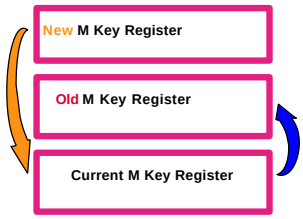


Master Keys . . .

	DES Master Key Storage	AES Master Key Storage	PKA Master Key Storage Areas
CEX2C Not CPACF	DES-MK	AES-MK	ASYM-MK
	New DES-MK	New AES-MK	New ASYM-MK
	Old DES-MK	Old AES-MK	Old ASYM-MK

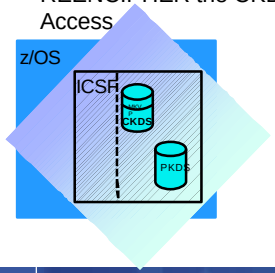
First Time DESAES Master Key Entry Process

- Must be in Special Secure Mode
- Enter (PPINIT) or process key part values
- Set the Master Key registers
- CKDS
  - For first-time, empty CKDS (IDCAMS DEFINE)
  - Initialize CKDS/PKDS
  - Perform SET of Master Key, system keys added automatically,



Later DES Master Key Entry Process (New LPAR/DR)

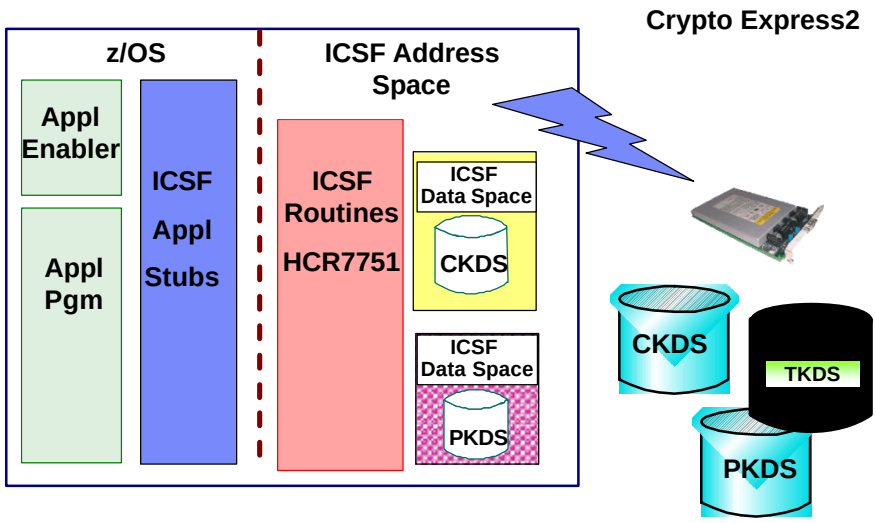
- Must be in Special Secure Mode
- Must run COMPAT(NO)
- Enter key part values into New Master Key (NMK) Register
- Based on Status of CKDS activate the New Master Key, if CKDS header record contains MKVP
  - Matching MKVP of contents in NMK, do SET
  - Different than MKVP of contents in NMK, do CHANGE and REENCIPHER the CKDS first, perhaps Disable Dynamic CKDS Access



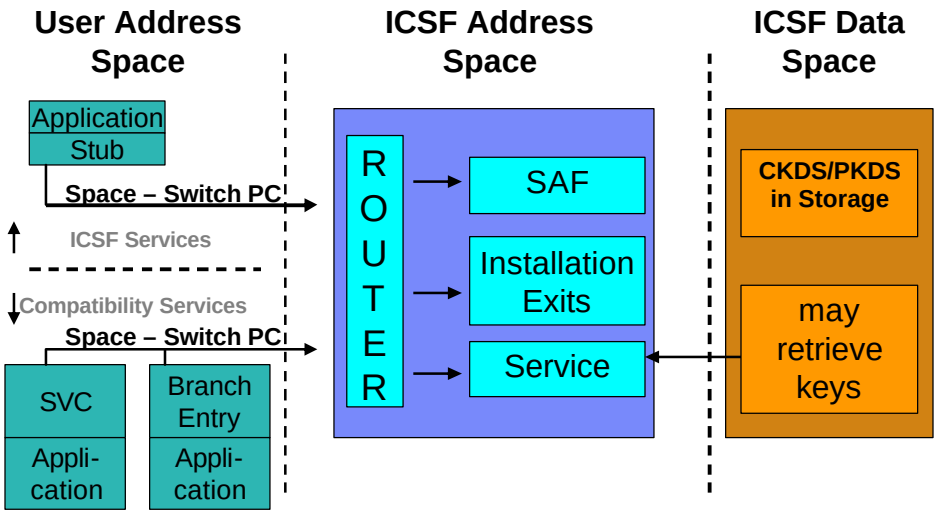
ICSF

- ICSF is a no charge system task that provides a tool kit for application access to cryptographic functions
- ICSF provides load balancing across cryptographic hardware (CEX2C)
- ICSF provides a secure storage for cryptographic keys (CKDS, PKDS)
- ICSF checks SAF access to functions and keys that it stores for you
- ICSF is not in itself a full key management system

ICSF – Interface to the Hardware



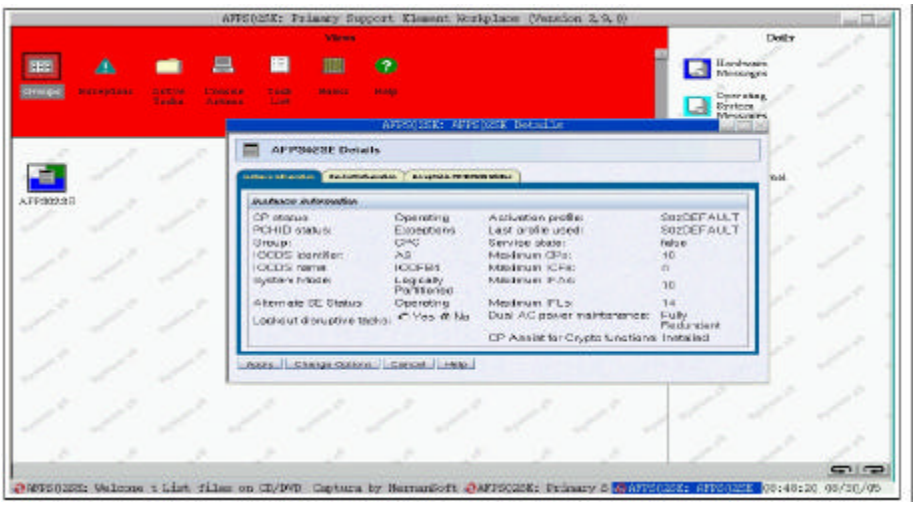
ICSF Internals



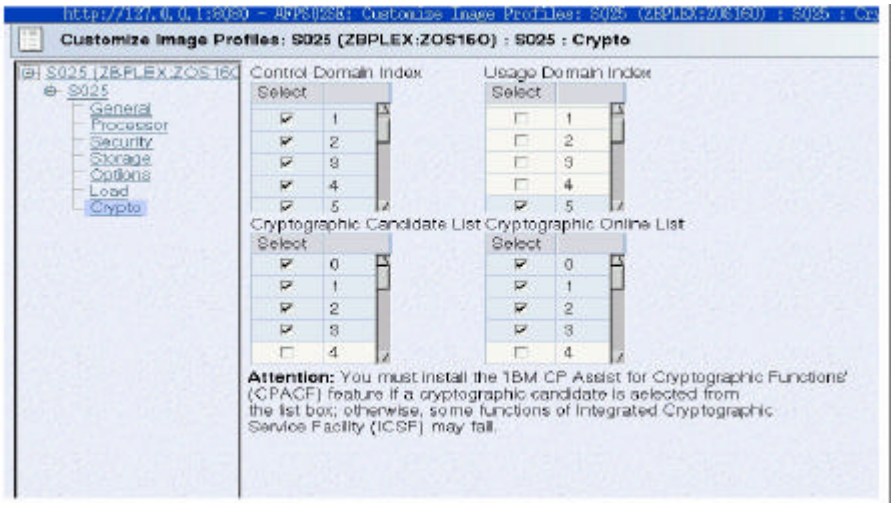
Hardware (SE) Functions

- Add feature 3863
- Configure LPAR crypto domains
- Configure CEX2C/ CEX2A

FC 3863 Installed



Crypto Definitions (z10 Dynamic)



SAF (RACF/ACF2/TopSecret)

- ICSF Issues SAF calls to two resources
  - CSFSERV
    - What service is requested
      - Not done for non-crypto based calls such as ASCII-EBCDIC translation or Clear Key Encrypt/Decrypt (CSNBSYE/CSNBSYD)
    - I can encrypt, but not decrypt (secure key)
  - CSFKEYS
    - What key label is requested form the xKDS
    - I can encrypt, but not with production keys (based on label)
  - ICSF Administrator's Guide Chapter 3
  - ICSF is also a user subject to SAF rules for internal functions
- XFACILITgeneral resource class in SAF (RACF) controls use of tokens stored in the CKDS and PKDS
- XCSFKEY general resource class in SAF controls who can export a token using the Symmetric Key Export API (CSNDSYX)

RACF

- RACDCERT
  - RACF certificate support
    - GENCERT
    - ADD
    - ADDRING
    - CONNECT
    - EXPORT
    -
    -
    -

References

- ATS TechDocs Web Site
  - http://www-1.ibm.com/support/techdocs/atsmastr.nsf
    - search on CRYPTO
- IBM Web Libraries
  - http://www-1.ibm.com/servers/eserver/zseries/zos/bkserv/
  - http://www-1.ibm.com/servers/eserver/zseries/library/online_pubs.html
  - http://www-1.ibm.com/servers/eserver/zseries/library/whitepapers/
  - http://app-06.www.ibm.com/servers/resourcelink
  - http://publib-b.boulder.ibm.com/Redbooks.nsf/RedpaperAbstracts/redp3747.html?Open
- 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.schneier.com/crypto-gram.html

Questions

Programming can be fun, so can cryptography; however they should not be combined.

--Kreitzberg and Shneiderman

The Pause That Refreshes