Vanguard Security & Compliance 2011 *Las Vegas June 22*

Session LSC10:
Cryptography and the zEnterprise

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. Fa ilure of a mark to appear does not mean that IBM does not use th e 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 State s.

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 e ither 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 c ountries.
UNIX is a registered trademark of The Open Group in the United S tates 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 Centr al 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 a mount 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 ar e presented as illustrations of the manner in which some custom ers 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 docu ment in other countries, and the information may be subject to c hange 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 s ubject 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 yo urgeography.

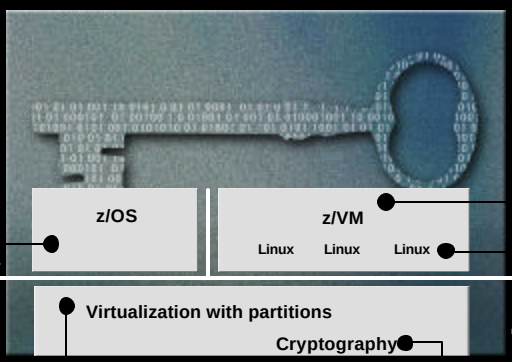
Agenda

- z196 System Overview
- z196 Cryptographic Hardware
- z196 Cryptographic Functionality

zEnterprise z196 and zBX Blade Center

System z Certification & System Integrity Statement

The Common Criteria program establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles



z/OS

- **Common Criteria EAL4+**
  - with CAPP and LSPP
  - z/OS 1.8 + RACF
  - z/OS 1.9 + RACF
  - Z/OS 1.10+ RACF with OSPP
  - z/OS 1.11+ RACF (OSPP)
- **IdenTrust™ certification** for z/OS as a Digital Certificate Authority (PKI Services)
- System Integrity Statement

z/VM

- **Common Criteria**
  - **z/VM 5.3**
  - **EAL 4+ for CAPP/LSPP**
  - **System Integrity Statement**

Linux on System z

- **Common Criteria**
  - **SUSE LES10 certified at EAL4+ with CAPP**
  - **Red Hat EL5 EAL4+ with CAPP and LSPP**

System z9 EC and z9 BC

System z10 EC and z10 BC

- **Common Criteria** EAL5 for Logical partitions
- **FIPS 140-2 level 4** for Crypto Express 2
- FIPS 140-2 Level 1
  - System SSL R10/R11
  - ICSF WD#9

See: **www.ibm.com/security/standards/st_evaluations.shtml**

z Enterprise Crypto Solution

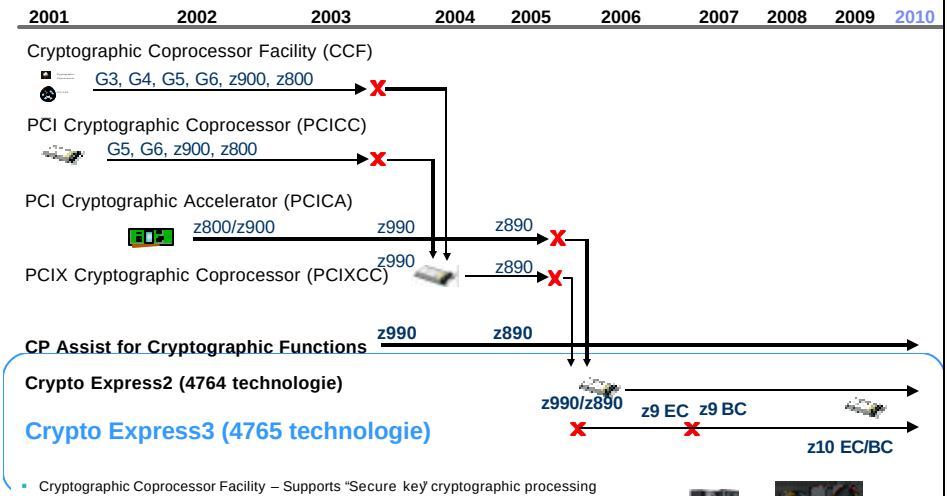
FC3863 CPACF clear key (protected key with CEX3C)

CEX3C encrypted key

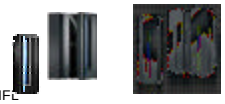
Support Element

Trusted Key Entry

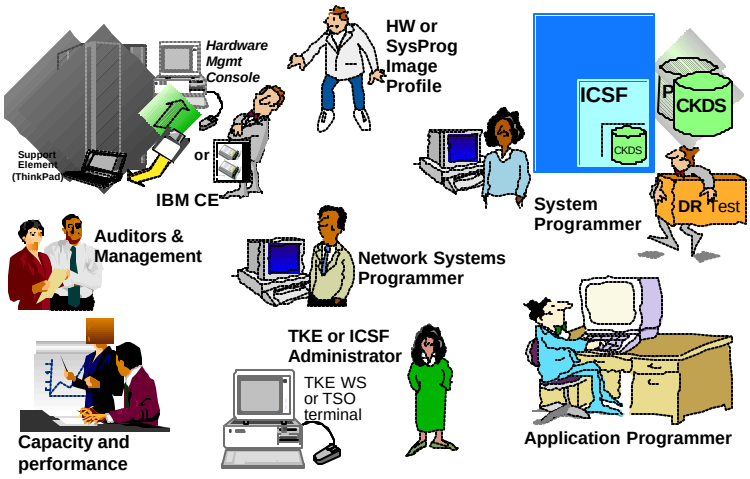
System z Crypto History Support



- Cryptographic Coprocessor Facility – Supports "Secure key" cryptographic processing
- PCICC Feature – Supports "Secure key" cryptographic processing
- PCICA Feature – Supports "Clear key" SSL acceleration
- PCIXCC Feature – Supports "Secure key" cryptographic processing
- CP Assist for Cryptographic Function allows limited "Clear key" crypto functions from any CP/IFL



Welcome to the Party



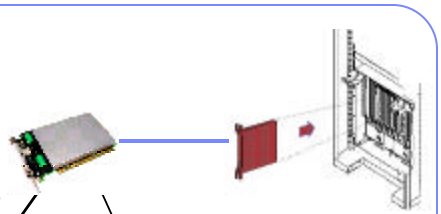
What's New for ICSF V1 R11 --- HCR7780 (Oct 2010)

- Secure AES (HCR7751)
- Protected Key (HCR7770)
- Elliptic Curve cryptography
- z196 Support (MSA-4 instructions)
- Enhancements to ANSI X9.8 support
- Enhancements to ANSI X9.24 support
- Keyed-Hash Message Authentication Code
- Enhanced logging for PCI Audit requirements
- CKDS Constraint Relief
- 64-bit APIs
- TKE 7.0
  - New Platform
  - Migration Wizard and new Smart Card Types
  - Audit Offload Utility

z196 Hardware Cryptography Implementation

CP Assist for Cryptographic Functions (CPACF)
- A facility integrated in each PU
- Standard orderable feature
- Clear Key & Protected Key only
- Symmetric, hash, …

Crypto Express 3 (CEX3C)
- Priced feature
- 0 to 8 features in a system
- 2 secure **4765 coprocessors** per feature
- Secure keys symmetric (DES, T-DES) and asymmetric (RSA)
- PR/SM sharable
- Manually configurable into an RSA accelerator (CEX2A, CEX3A)
- **FIPS140-2** (As Coprocessor only)



Coprocessor
FIPS140-2 = YES

Details next slide

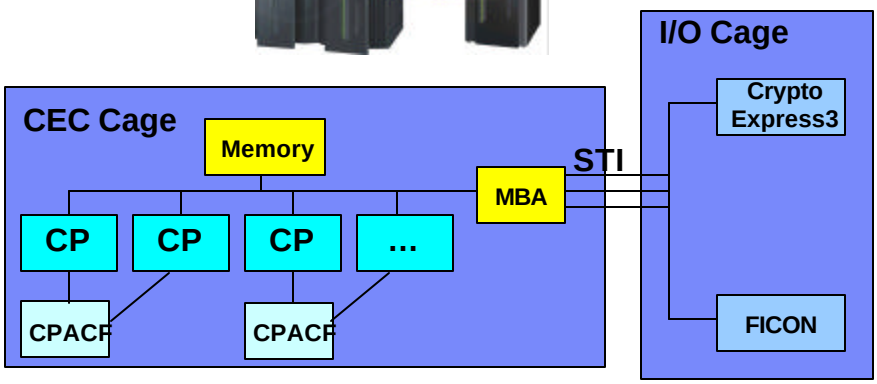
Clear Key / Secure Key / Protected Key

- Clear Key – key may be in the clear, at least briefly, somewhere in the environment
- Secure Key – key value does not exist in the clear outside of the HSM (secure, tamper-resistant boundary of the card)
- Protected Key – key value does not exist outside of physical hardware, although the hardware may not be tamper-resistant




Fort Knox

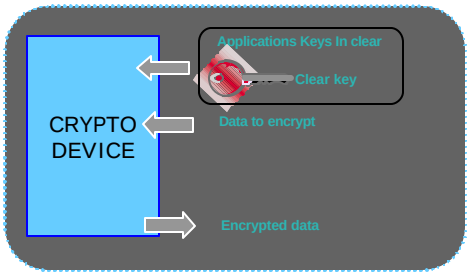

z196 Crypto HW



Clear Key

CPACF, CEX2A, CEX3A

"Clear Key – key <u>may</u> be in the clear, at least briefly, somewhere in the environment"



- Performance VS. Security
  - 10 – 100 times faster

Database Encryption

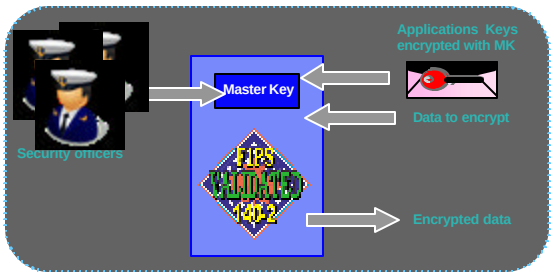
- Data Encryption for IMS and DB2 Databases

  NOW ***IBM*** InfoSphere Guardium Data ***Encryption*** for ***DB2*** and ***IMS*** 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/z196 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 (TDES) algorithm and also supports the replacement AES algorithm.
- Works at and is customizable at the IMS segment level or DB2 table level
- Optimized CPACF processing

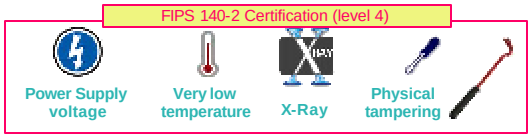
Secure Coprocessor

"Secure Key – key value does not exist in the clear outside of the HSM (secure, tamper-resistant boundary of the card)"

Fort Knox



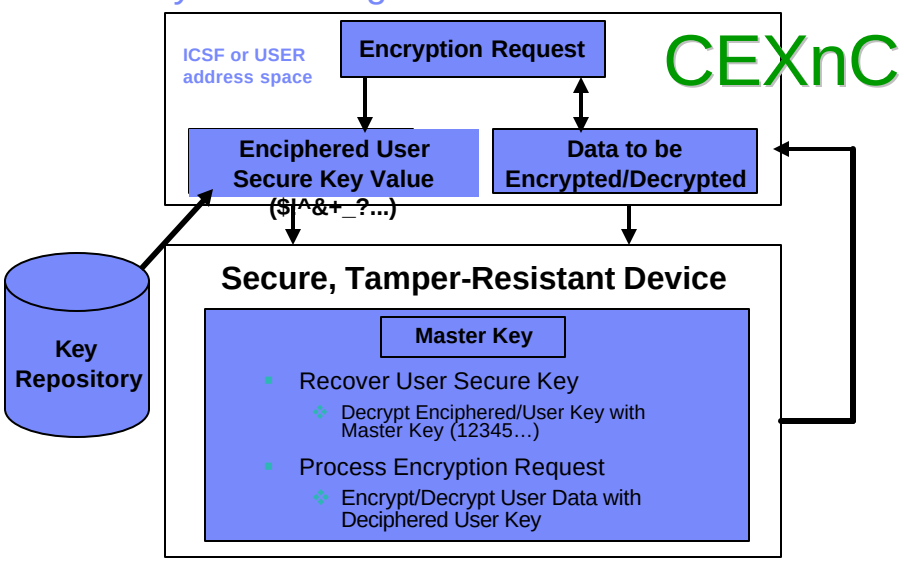
FIPS 140-2 Certification (level 4)



http://csrc.nist.gov/cryptval/140-1/1401val2006.htm look for certificate #661

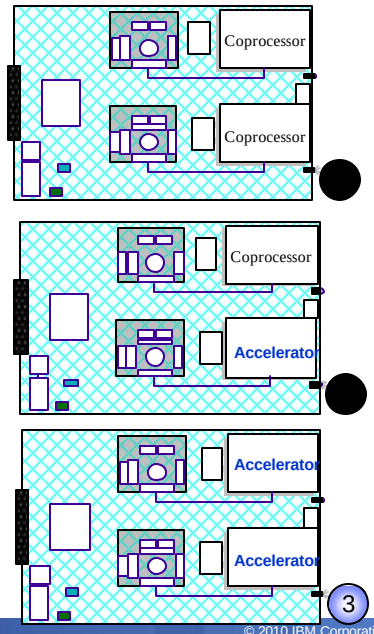
+ Master Key zeroization in case of tampering attempt

Secure Key Processing



zCrypto Express2/3 Configuration

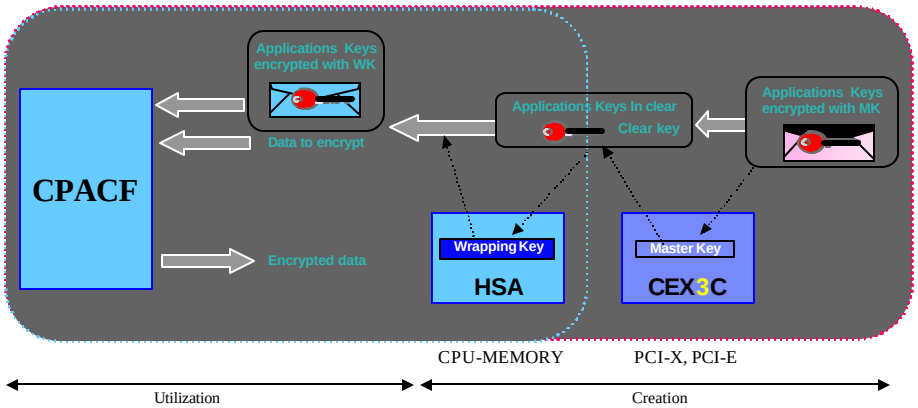
- Secure Coprocessor **(default)**
  - Provides both Secure key" and "Public key" functionality
  - "Secure key" improved performance compared to PCIXCC on z990 (requires multitasking)
  - "Public key" equivalent performance to PCICA on z990
  - No action required (default configuration)
  - SSL at 1000-2000/second
- Accelerator
  - Provides only 3 "Public key" functions with enhanced performance
  - Must be configured using the HMC
  - SSL at 3000-6000/second



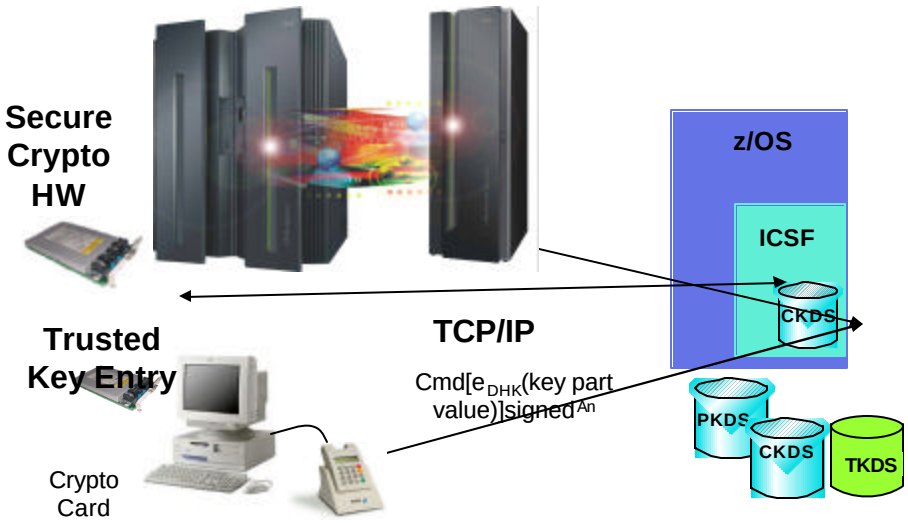
Protected Key

CPACF (CEX3C required)

"Protected Key – key value does not exist outside of physical hardware, although the hardware may not be tamper-resistant"



Crypto System

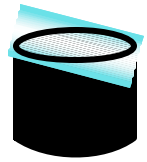


ICSF CEXnC Functions

- 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

Master Keys . . .

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



Domain Association Across CEXnC, ICSF, and TKE

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

Look in

5 nia D o m

MK VP

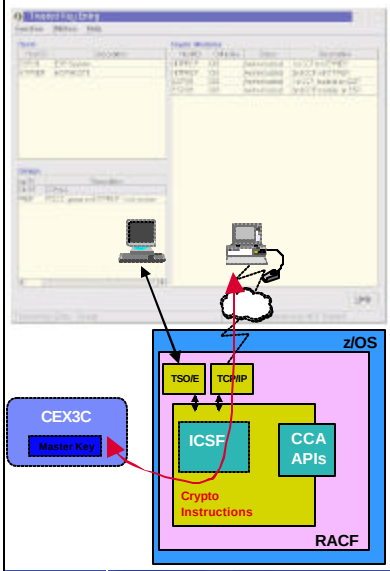
Current Mkeys
New Mkeys
Old Mkeys

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

The Trusted Key Entry Workstation

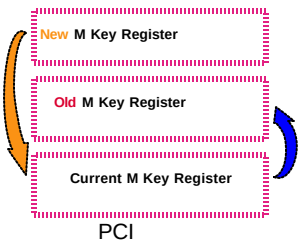


- **Priced optional feature** - A highly secure alternative
- TSO/E for the management of secure coprocessors Master Keys and operational keys
- Encrypted and signed communications over TCP/IP
  - Listener in ICSF
  - End point is the coprocessor
- Increased security for
  - Access to secure cryptographic coprocessors
  - Authorities (security officers) identified by their password and digital signature
  - Option to require multiple signatures before performing a crypto function
  - smart card support
- Coprocessors can be administered as groups

Can be used on Linux with secure keys

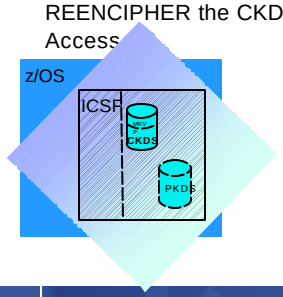
First Time DESAES Master Key Entry Process

- 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

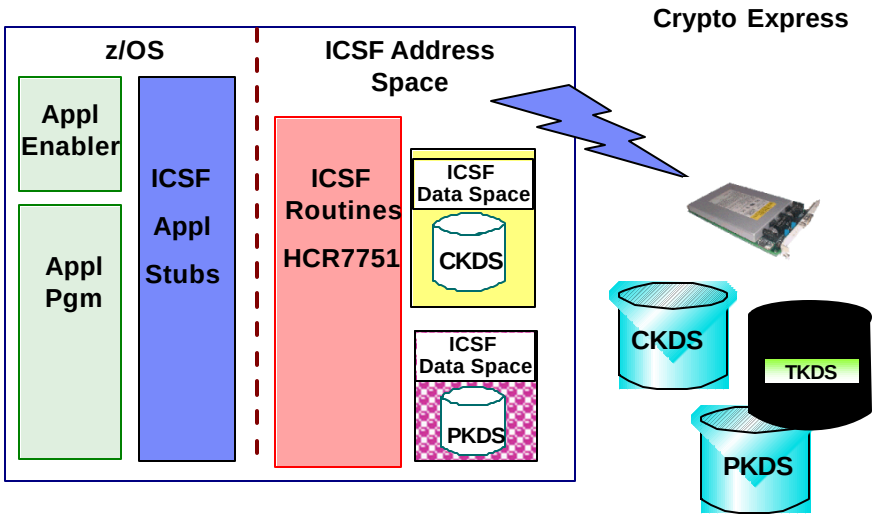


PCI

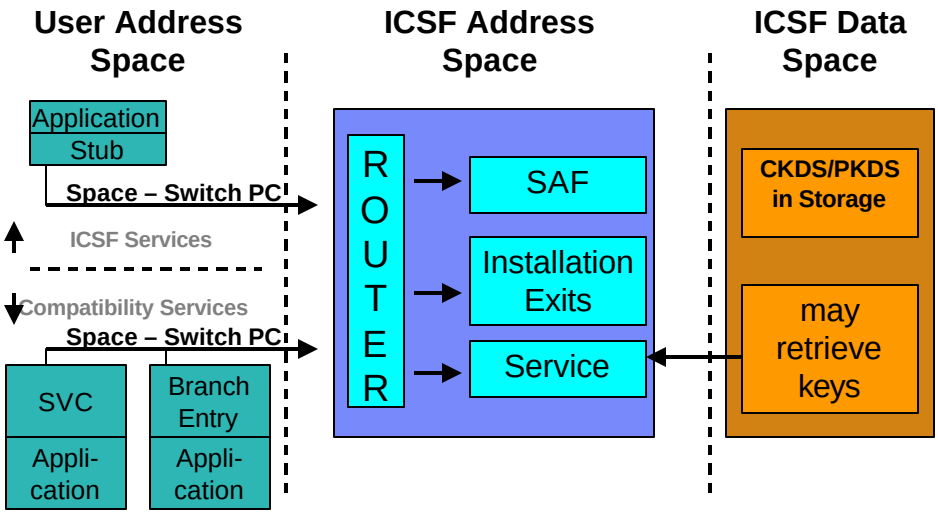
ICSF

- 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 (CEXnC)
- 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



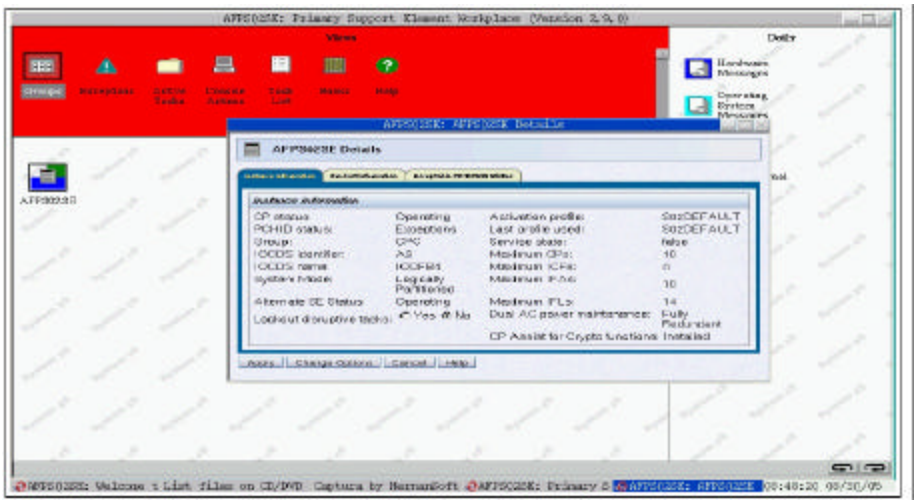
ICSF Internals



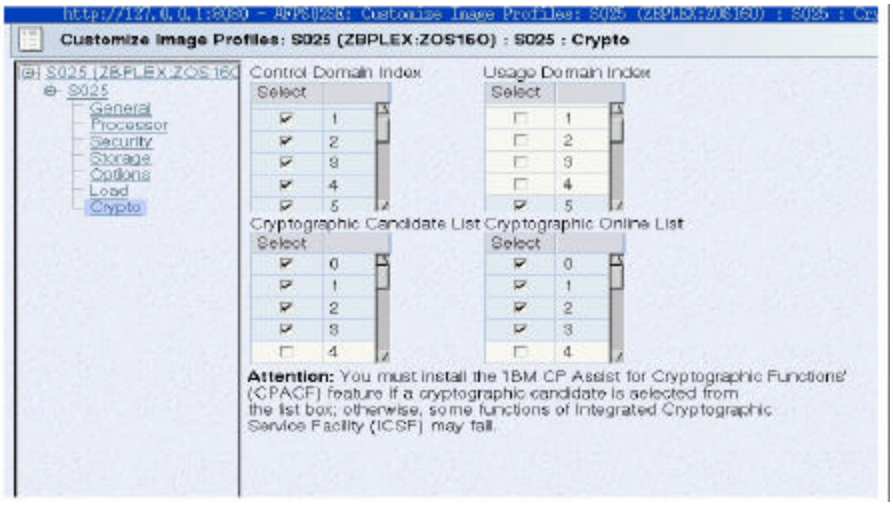
Hardware (SE) Functions

- Add feature 3863
- Configure LPAR crypto domains
- Configure CEX3C/ CEX3A

FC 3863 Installed



Crypto Definitions (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
- XFACILIT general 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)

ICSF Parameter File Hints

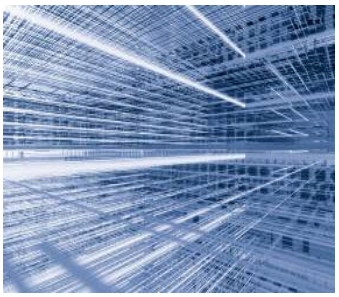
- KEYAUTH(NO)
  - Extra MACVER call for every reference to a key label in the CKDS
  - Encrypt: doubles the calls and path length, input key, function
  - PIN Translate: triples the calls and path length – input key, output key, function
  - Key Translate quadruples the calls and path length – input key, output key, source key, function
- CKTAUTH(NO)
  - Extra MACVER when CKDS read into memory
- CHKAUTH(no)
  - RACHECK authorized/supervisor state callers
- SYSPLEXCKDS(YES,FAIL(NO))
- SYSPLEXPKDS(YES,FAIL(NO))

Propagate application CKDS/PKDS additions

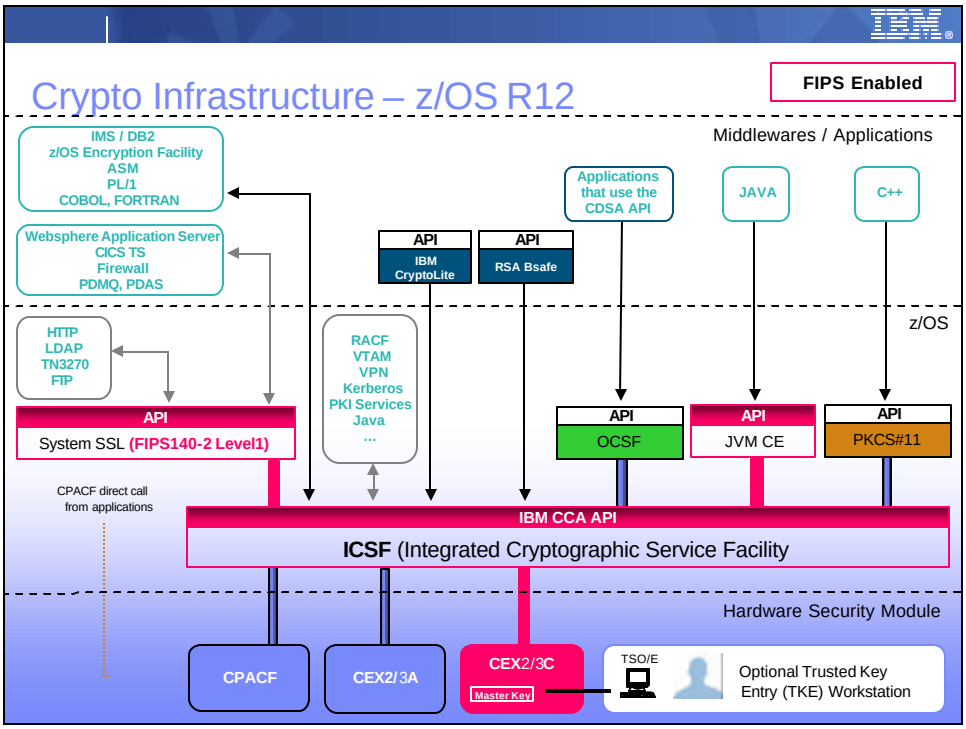
- Not for KGUP adds
- Not for a KDS REFRESH

IBM System z Cryptographic Implementation

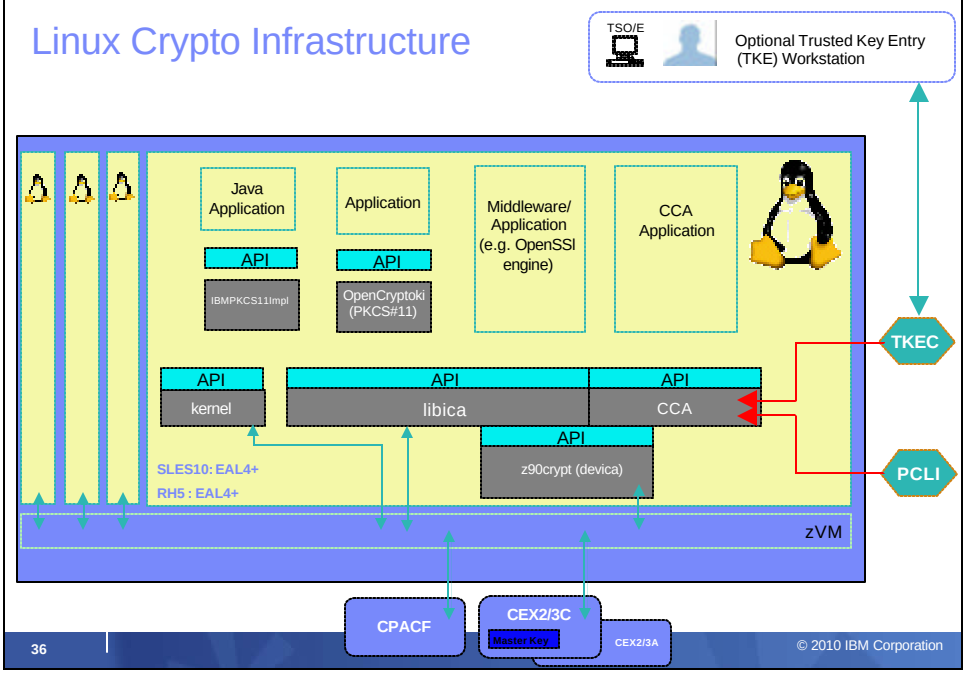
- z/OS
- z/VM & Linux on z
- z/VSE



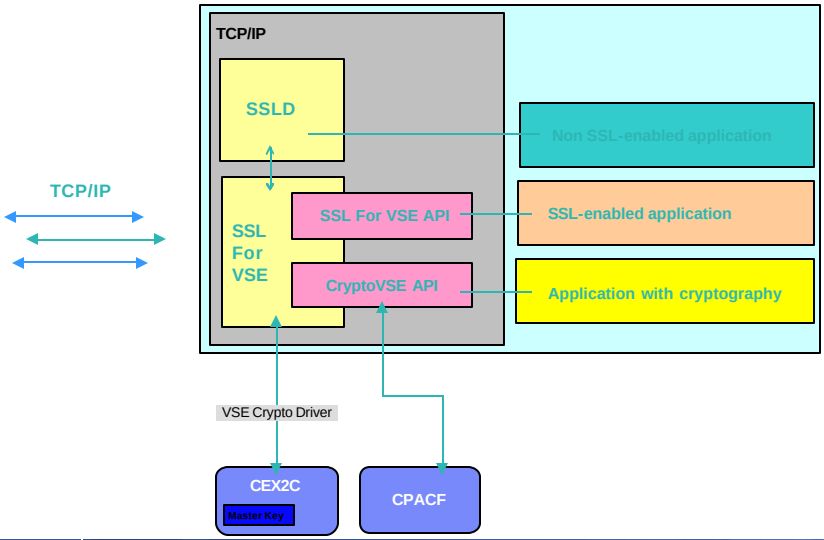
Crypto Infrastructure – z/OS R12



Linux Crypto Infrastructure



z/VSE Crypto Infrastructure



Clear RSA key only

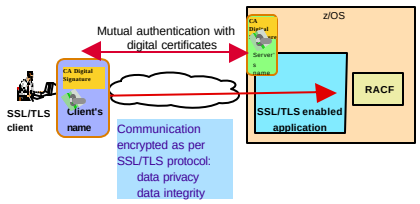
Cryptographic Exploiters

- Exploitation Examples
  - Network
  - Java
  - Database
  - Tape

z/OS Exploitation Of Hardware Crypto - Examples

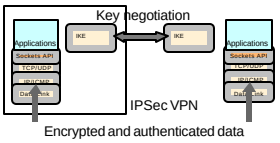
z/OS System SSL – SSL/TLS

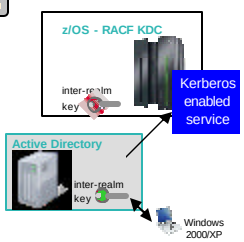
- z/OS System SSL provides the API to applications
- z/OS System SSL calls
  - CEX2/3C for handshake (RSA) – via ICSF
  - CPACF for data transfer (DES or T-DES) - direct call via instructions



z/OS Communications Server – IPSec VPNs

- CEX2/3C for Key Server authentication via ICSF
- CPACF for DES, T-DES or AES128 data encryption via ICSF

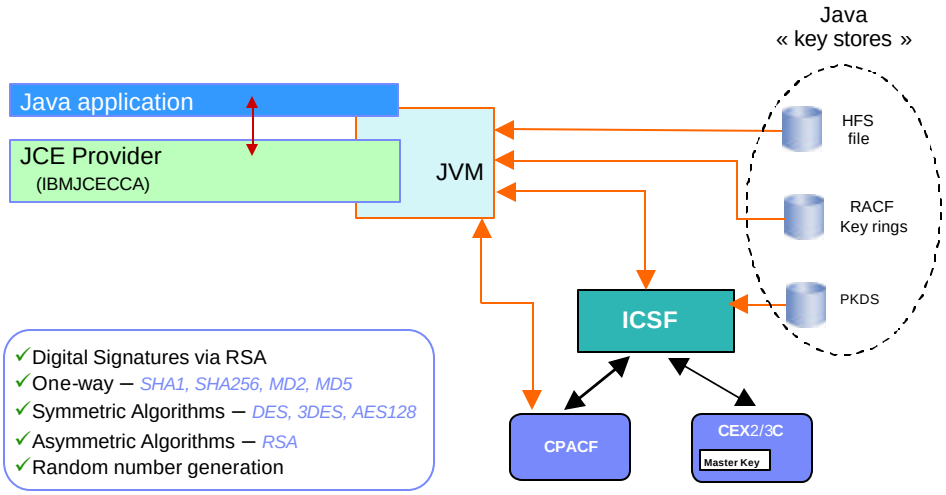




Kerberos (z/OS Network Authentication Service)

- CPACF for AES128
- CEX2/3C for DES or T-DES authentication and data encryption via ICSF

z/OS Exploitation Of Hardware Crypto - Java



- ✓Digital Signatures via RSA
- ✓One-way – *SHA1, SHA256, MD2, MD5*
- ✓Symmetric Algorithms – *DES, 3DES, AES128*
- ✓Asymmetric Algorithms – *RSA*
- ✓Random number generation

IBM Data Encryption for DB2 Database

(Product number 5655-P03)

EDITPROC exits

IMS Segment Edit/Compression exit

- DECENC00 – Secure key
- DECENA00 – Clear key

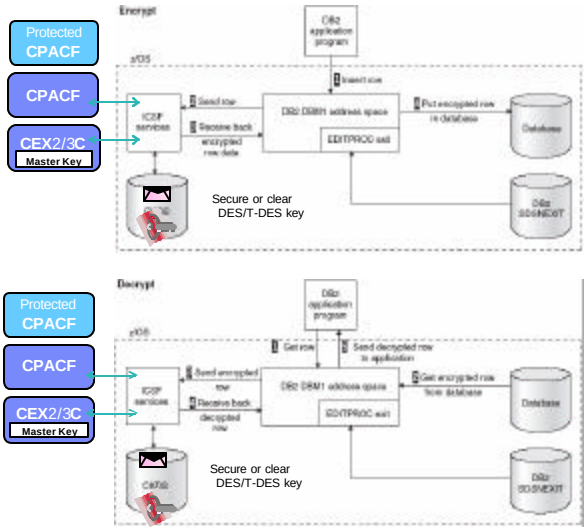
Specified in the EDITPROC clause of the SQL CREATE TABLE statement

Keys installed with the KGUP (Key Generation Utility Program) in the CKDS with a label

One different key per table if desired

NOTE:

+ *Indexes will NOT be encrypted*
+ *Row level Encryption (All row will be encrypted)*
+ *Data encrypted in DB2 Bufferpool*

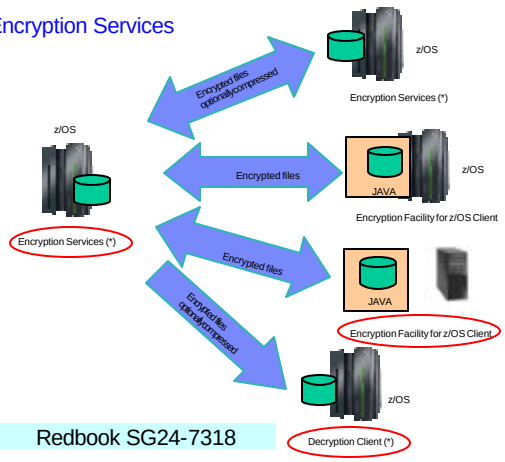


Similar implementation for IMS DB encryption

Encryption Facility For z/OS V1.2

(Program Product 5655-P97)

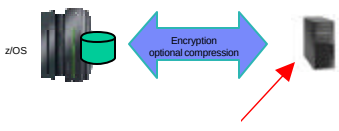
Encryption Services



Redbook SG24-7318

DFSMSdss Encryption

OpenPGP Support



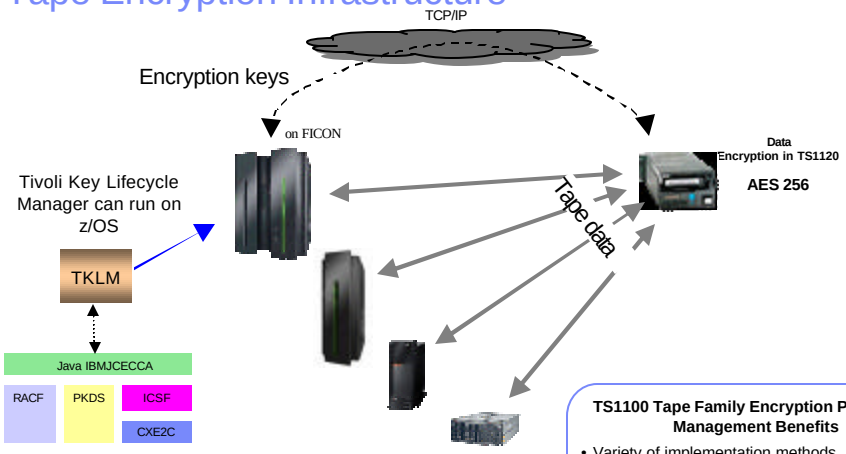
Any platform that supports OpenPGP (RFC 2440)

Redbook SG24-7434

Sizing services at
http://w3-03.ibm.com/support/techdocs/atsmastr.nsf/84279f6ed9ffde6f86256ccf00653ad3/5dd1cd0d735d3e23862570af0048710f?OpenDocument

Encryption Facility for z/VSE now available in VSE Central Functions V8.1 (5686-CF8)

Tape Encryption Infrastructure



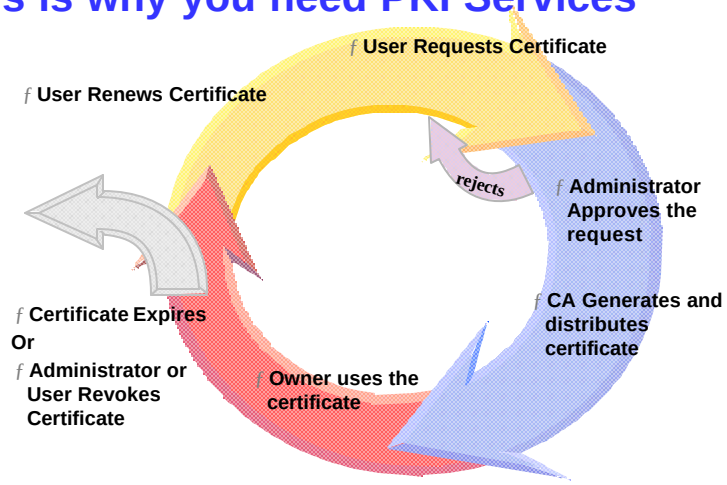
- ✓ Symmetric key generation
- ✓ Symmetric key RSA wrapping/unwrapping
- ✓ RSA keys repository

Redbook SG24-7320

TS1100 Tape Family Encryption Potential Management Benefits

- Variety of implementation methods
- Heterogeneous server support
- Avoid host MIPS encryption overhead
- Minimize impact to existing processes and applications

Certificate Life Cycle – This is why you need PKI Services



Overview

- A component on z/OS since V1R3
- Closely tied to RACF
  - The CA cert must be installed in RACF's key ring
  - Authority checking goes through RACF's callable service
- **Supports more functions than RACDCERT**
  - Full certificate life cycle management: request, create, renew, revoke
  - Generation and administration of certificates via customizable web pages
  - Support automatic or administrator approval process
  - Support multiple revocation checking mechanisms
    - Certificate Revocation List (CRL)
    - Online Certificate Status Protocol (OCSP)
  - Certificates and CRLs can be posted to LDAP

Overview (contd)

- Provides email notification
  - to notify end user for completed certificate request and expiration warnings
  - to notify administrator for pending requests
  - to send the automatic renewed certificate
- Provides Trust Policy Plug-in for certificate validation

DKMS in a Nutshell

- Centralized management of keys and certificates
- Managing keys and certificates for many platforms and devices
- Efficient operations
  - key and certificate expiry monitoring
  - semi-automated functions
- Highly secure operations
- Supports PCI-DSS compliance
  - Enforcement of operational procedures
  - Audit trail
- Dedicated functions for selected business areas, e.g.
  - EMV chip card issuing and acquiring processing
  - ATM remote key loading

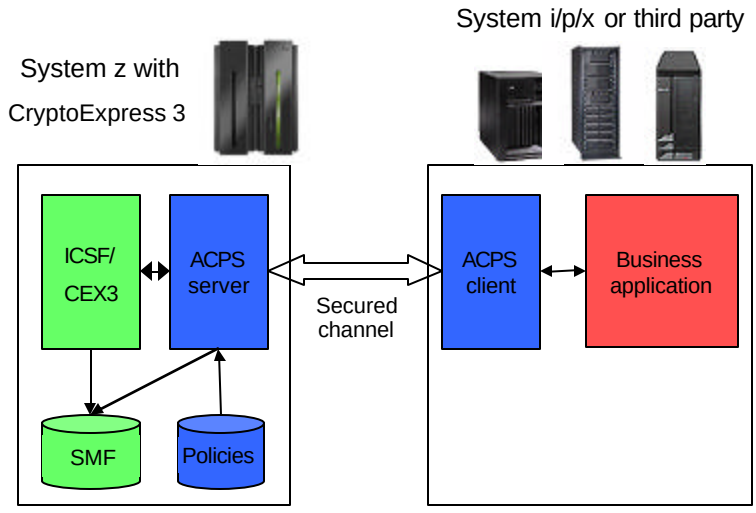
DKMS Key Features

- Secure management of keys by throughout use of crypto HW
- On-line management of large, heterogeneous environments – mainframes and distributed servers
- Continuous operation ensured by secure backup and restore of keys
- Access control and audit trail enables PCI-DSS compliance
- Automated monitoring of expiry of keys and certificates
- Semi-automated operations enable easy rotation of keys

Advanced Crypto Service Provider

- Replace HSMs installed in distributed servers with a Net HSM
- Utilize mainframe crypto capacity as the Net HSM
- Expose crypto functions on clients
- Aggregate crypto commands
- Load balancing
  - multiple servers (clients do balancing)
  - multiple crypto coprocessors (server does balancing)

ACSP Overview



Enterprise Encryption Solutions

System z Encryption Infrastructure

Encryption hardware acceleration with every processor

GP Processor

GP Processor

zAAP (Java)

zIIP (IPSec)

IFL (Linux)

Tamper-resistant encryption processing
Keys never in the clear

Trusted Key Entry

Crypto Express3

Crypto Express3

Key Storage

Encryption service management and optimization

ICSF, RACF, SMF

CKDS

PKDS

TKDS

z/OS

Linux on z

Crypto access

Encryption Solutions

- Tape
- Disk Encryption
- Internet Access
- Web applications
- Java Applications
- Certificate Authority
- Encryption Facility File Exchange
- Databases
- Smart Cards
- POS / ATM
- zBX (zEnterprise Blades)
- Distributed Key Mgmt System (DKMS)
- Encryption Key Lifecycle Mgr

Exploitation Of Hardware Crypto - Examples

Protect Data in Transit

Protect privacy of customer & employee information

Encryption with key management

Highly secure data transfer

Information Integrity

Ensure integrity of information, SoD for encryption of data at rest

Encryption of data for archival

Encryption

z/OS key management capabilities

Long-term key management

The Secured Business Environment

Protect your Communications

Enabling non-z/OS servers to communicate securely with z/OS

FTP, FTPs
OpenSSL, OpenSSH

IPsec

z/OS

Linux

CPACF | Crypto Express 3

secure key

Secure exchange of business critical information

Highly secure transfers across the Internet

Trusted exchange with open standards & support for **IP encryption**

Digital Certificates

Trusted business transactions

PKI and Digital Certificates

Identrus compliant Certificates

Directory Services

Managing identity across enterprise

Security Administration

Data Security

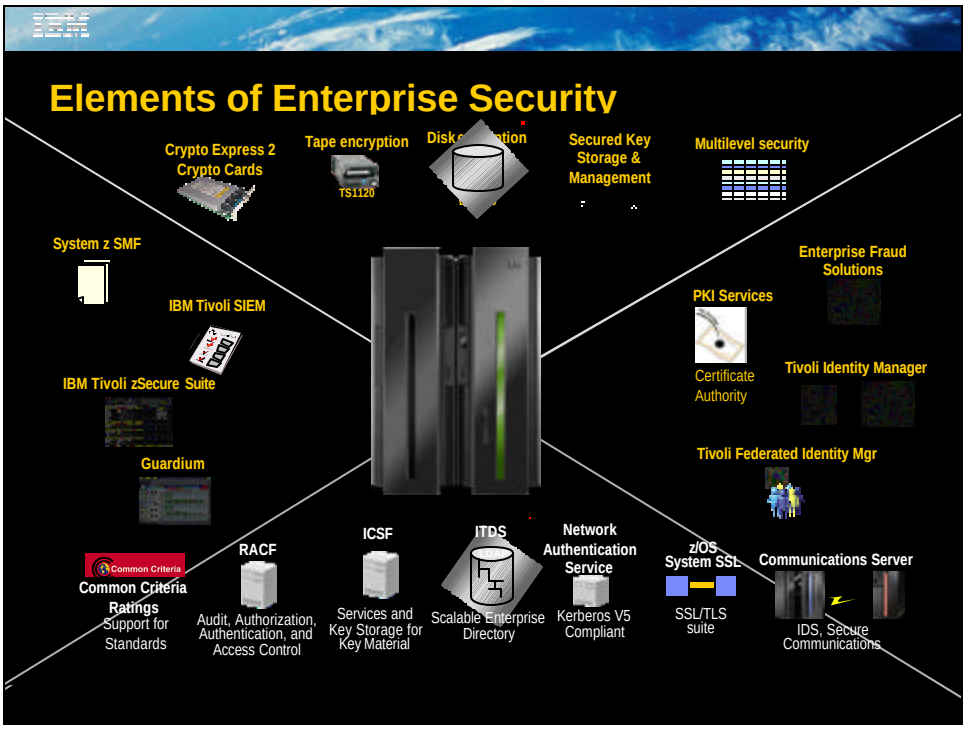
Single repository of data with various levels of security

Distributed directory services

LDAP
Directory tree

RACF
Kerberos
Digital Certificates

DB2
Multi-Level Security



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

Crypto Class 1.5 + 3.5 Days

- ICSF Install and Crypto Components (lecture)
- ICSF Crypto Application Programming (TSO calling to ICSF)

- NO CHARGE!
- enachtig@ca.ibm.com

Questions

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

--Kreitzberg and Shneiderman

The Pause That Refreshes