Vanguard Security and Compliance 2012

Session: AST2
Encryption Evolution: z196/z114

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.

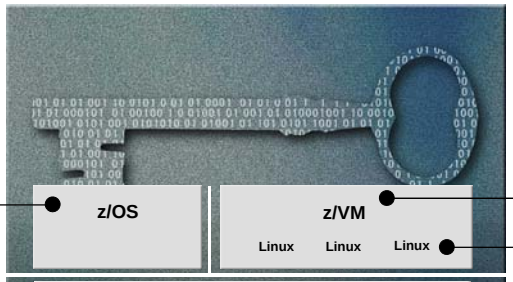
Agenda

- z10/z196/z114 System Overview
- z10/z196/z114 Cryptographic Hardware
- z10/z196/z114 Cryptographic Functionality
- Uses/Extensions

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)
    - z/OS 1.12: EAL5
- IdenTrust™ certification for z/OS as a Digital Certificate Authority (PKI Services)
- System Integrity Statement



System z9 EC and z9 BC

System z10 EC and z10 BC

zEnterprise: z196

- Common Criteria EAL5+ for Logical partitions
- FIPS 140-2 level 4 for Crypto Express 3

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

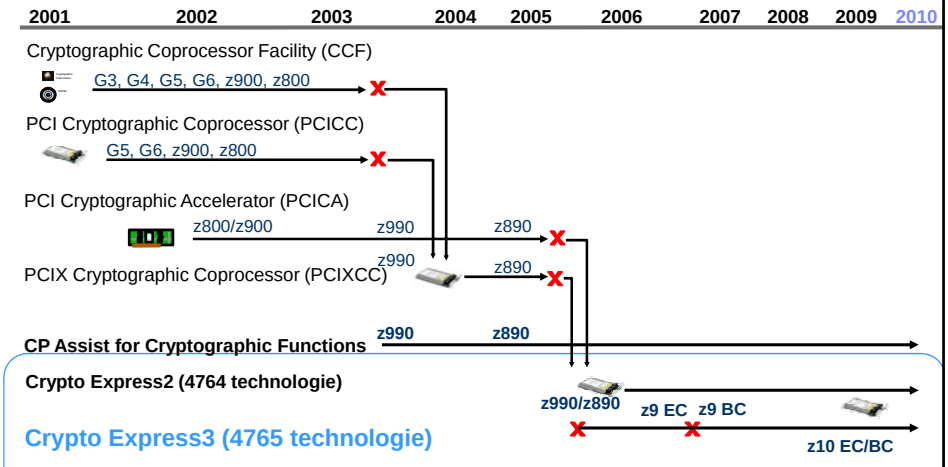
Linux on System z
- Common Criteria
- SUSE LES10 certified at EAL4+ with CAPP
- Red Hat EL5 EAL4+ with CAPP and LSPP

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

Recent 2012 System z Certifications

- IBM RACF for z/OS 1.12 has achieved Common Criteria certification at Evaluation Assurance Level 5 (EAL5)
- IBM's® z/OS® Version 1 R. 13 System ICSF PKCS#11 Cryptographic Module Receives FIPS 140-2 Certification – February 23, 2012
- IBM's® z/OS® Version 1 Release 13 System SSL Cryptographic Module Receives FIPS 140-2 Certification – March 20, 2012

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

z10/z196/z14 Overview

z ESAME Crypto Solution

FC3863 CPACF clear key
(protected key with CEX3C)

CEX3C
encrypted key

Support Element

Trusted Key Entry

What's New for ICSF V1 R11 --- HCR7751/HCR7770

- 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

What's New for ICSF V1 R11 --- HCR7770 (Nov 2009)

- PKCS #11 enhancements
  - DSA
  - Diffie-Hellman
  - Elliptic Curve cryptography
  - HMAC
  - Blowfish
  - RC4
  - AES GCM (Galois/Counter Mode)
- Path length Improvements
- ICSF Non-cancelable, non-swapable
  - CSFMMAIN becomes CSFINIT
- New Query services calls to enhance CSFIQF
- **Protected key**

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

- 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

What's New for ICSF V1 R12 HCR7790 (Sept 2011)

- TR-31 key block import/export
- CVV Key combine
  - CVV double length key
- Co-ordinated and dynamic CKDS update
- ECC-DH symmetric key generate
- Stored DECIMALIZATION table

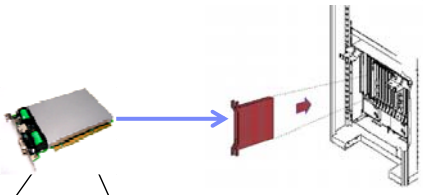
z10 Hardware Cryptography Implementation

CP Assist for Cryptographic Functions (CPACF)

- A facility integrated in each PU
- Standard orderable feature
- Clear Key & Protected Key only
- Symmetric, hash, …

Crypto Express 2/3 (CEX2C, CEX3C)

- Priced feature
- 0 to 8 features in a system
- 2 secure **4764/4765 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** Certified (As Coprocessor only)



Accelerator *FIPS140-2 = NO*

Coprocessor *FIPS140-2 = YES*

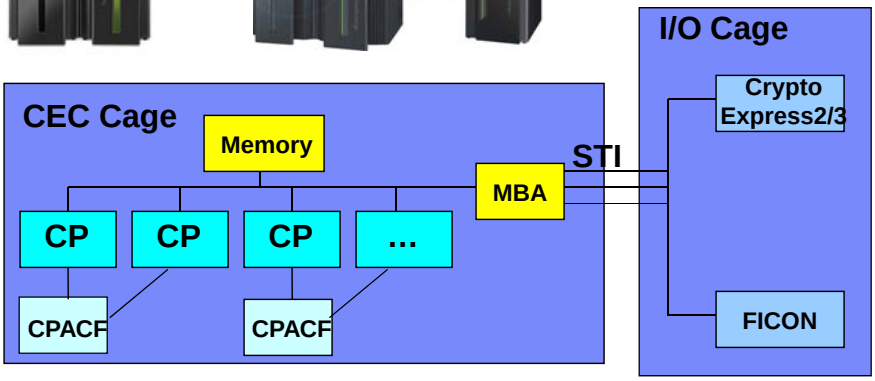
Details next slide

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

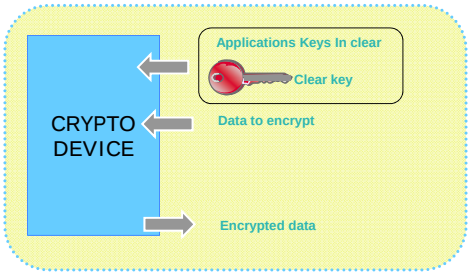
z10/z196/z114 Crypto HW



Clear Key

CPACF, CEX2A, CEX3A

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

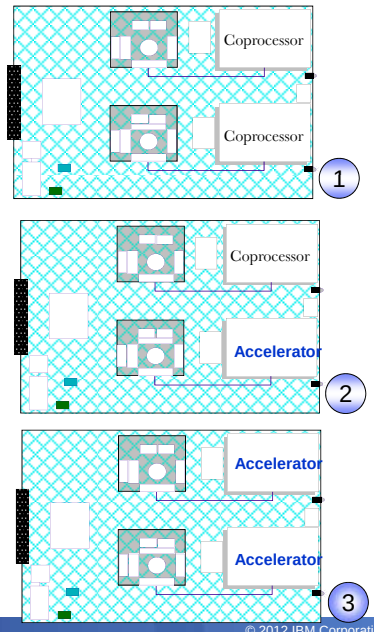


Database Encryption

- 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

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

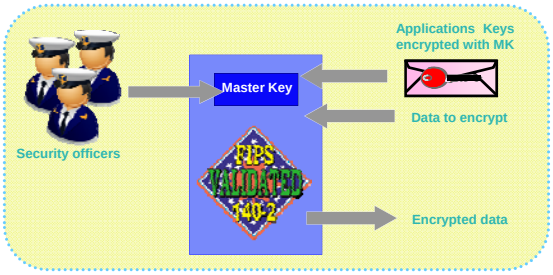


Secure Coprocessor

Secure Coprocessor (e.g. CEX2C, CEX3C)

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

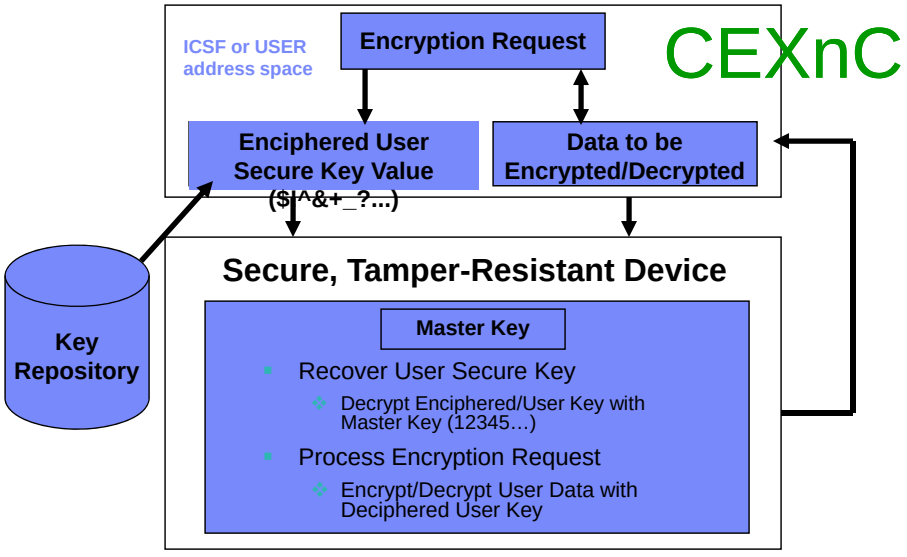
Fort Knox



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

+ Master Key zeroization in case of tampering attempt

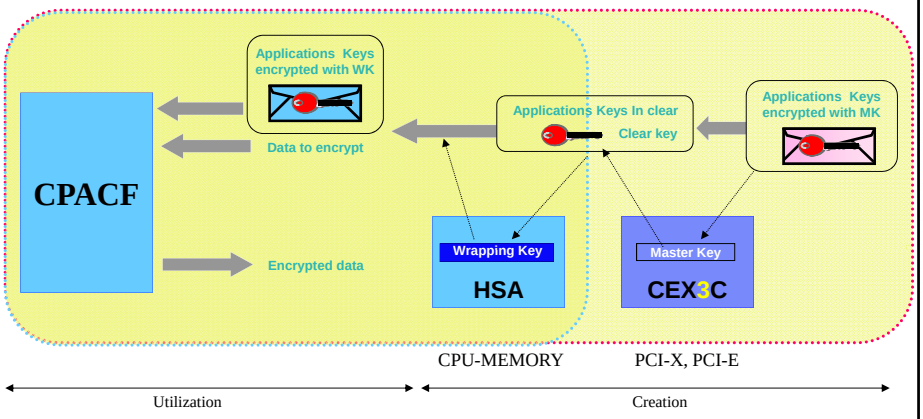
Secure Key Processing



Protected Key

CPACF (CEX3C required)

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

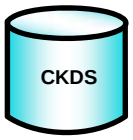


ICSF CEXnC Functions

- 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

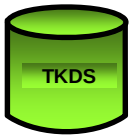
Master Keys . . .

- DES Master Key
  - DES-MK protects secure DES Keys stored in Cryptographic Key Data Set
  - 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



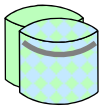
Master Keys . . .

- PKA
  - 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
  - Called ECC-MK
  - Protect Application Keys stored in Public Key Data Set (PKDS)
  - Stored in CEXnC, not PKDS
- 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**

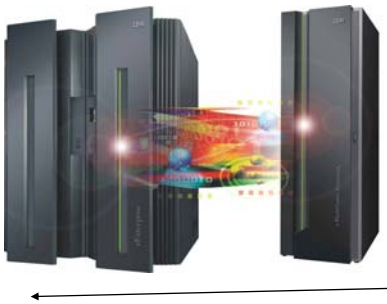
Usage Domain of 5

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

Crypto System

Secure Crypto HW



z/OS

ICSF

CKDS

Trusted Key Entry

Crypto Card

TCP/IP

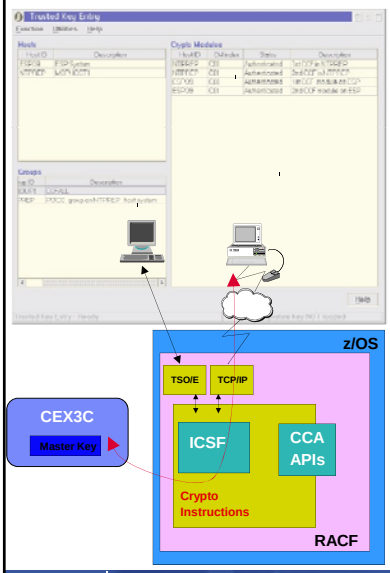
Cmd[e_{DHK}(key part value)]signed^{An}

PKDS

CKDS

TKDS

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

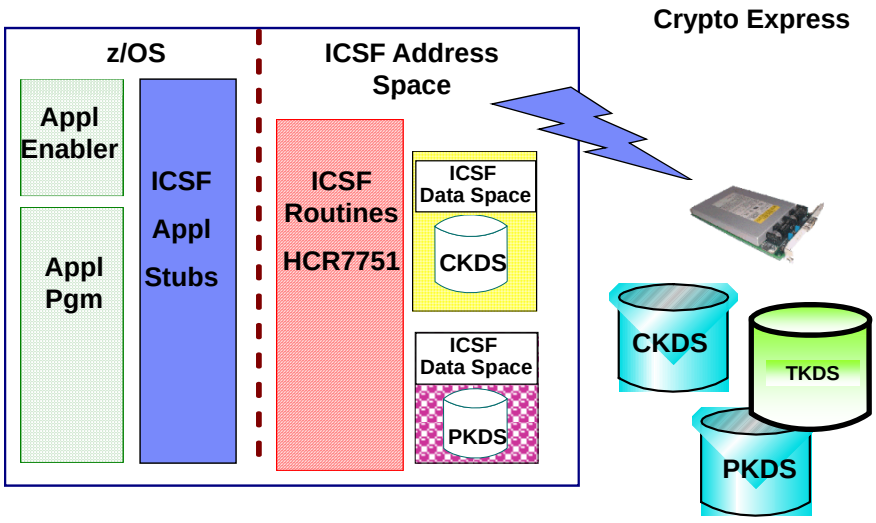
Master Keys . . .

All stored	DES-MK	AES-MK	PKA-MK	ECC-MK
In the	New DES-MK	New AES-MK	New PKA-MK	New ECC-MK
CEXnC None in CEXnA or CPACF	Old DES-MK	Old PKA-MK	Old PKA-MK	OLD ECC-MK

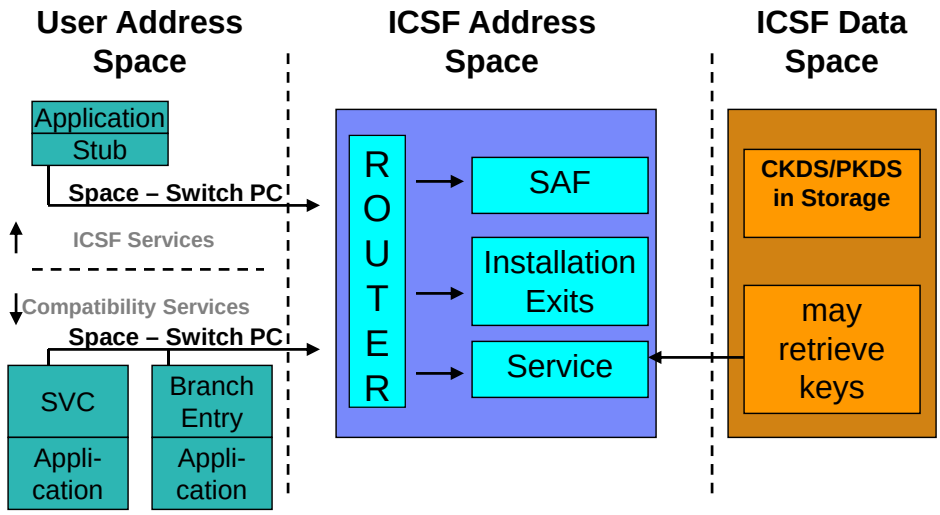
ICSF

- 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



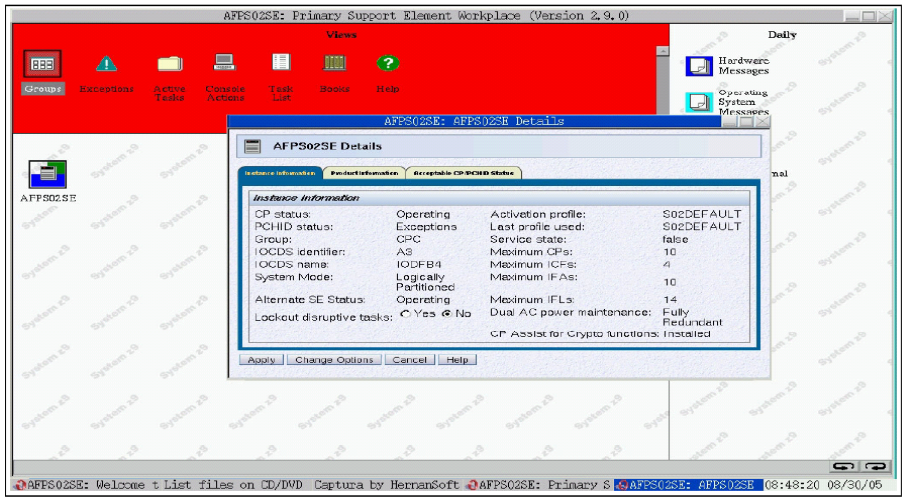
ICSF Internals



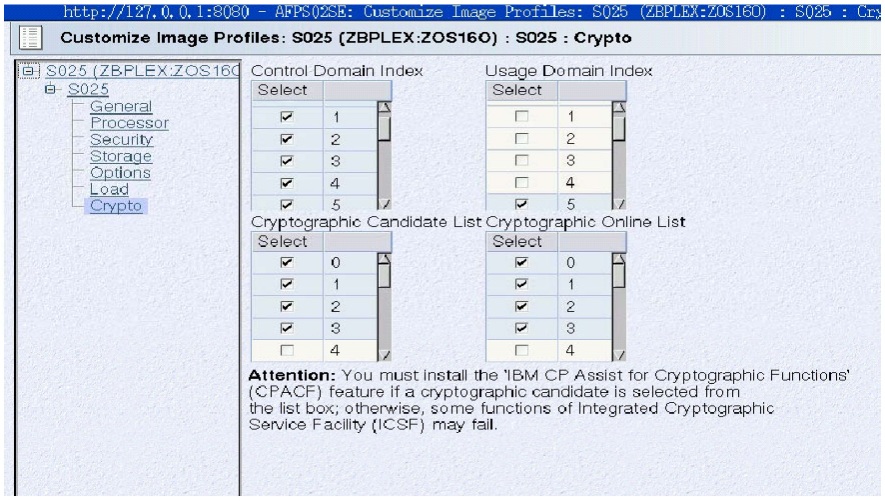
Hardware (SE) Functions

- Add feature 3863
- Configure LPAR crypto domains
- Configure CEXnC/ CEXnA

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
- 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

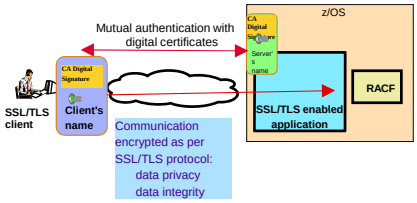
- z/OS
- z/VM & Linux on z
- z/VSE

Cryptographic Exploiters

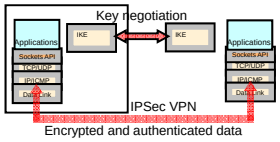
- Exploitation Examples
  - Network
  - Java
  - Database
  - Tape

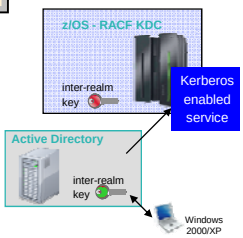
z/OS Exploitation Of Hardware Crypto - Examples

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



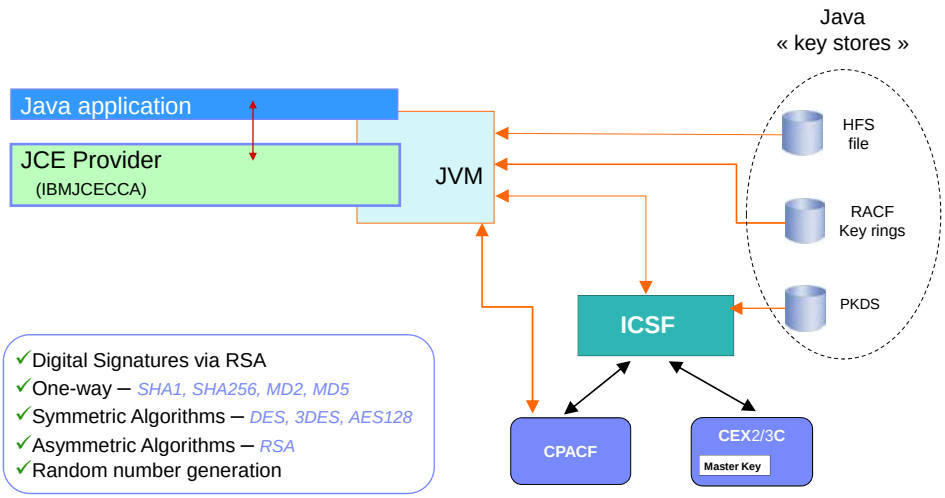
z/OS Communications Server – IPSec VPNs
- CEX2/3C for Key Server authentication via ICSF
- CPACF for DES, T-DES or AES128 data encryption via ICSF





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)

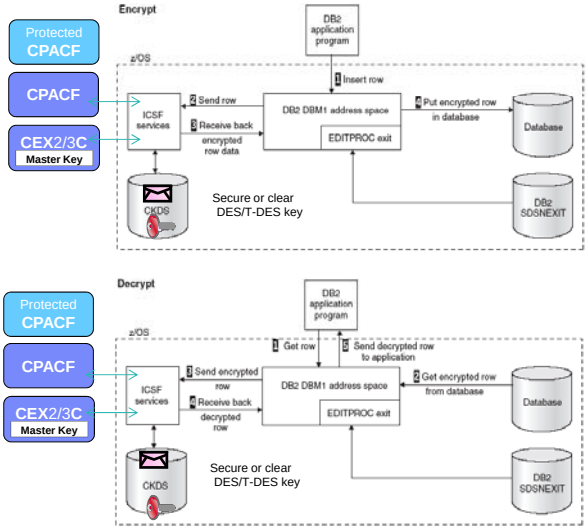
EDITPROC exits
IMS Segment Edit/Compression exit
- DECENC00 – Secure key
- DECENA00 – Clear key

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

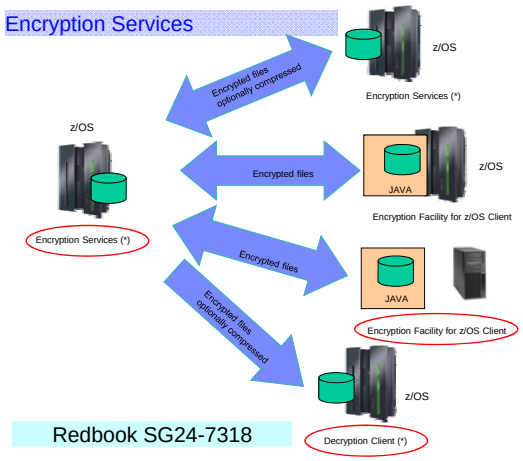
NOTE:
+ *Indexes will NOT be encrypted*
+ *Row level Encryption (All row will be encrypted)*
+ *Data encrypted in DB2 Bufferpool*



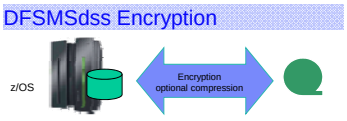
Similar implementation for IMS DB encryption

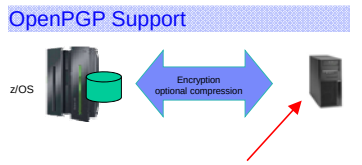
Encryption Facility For z/OS V1.2

(Program Product 5655-P97)



Redbook SG24-7318



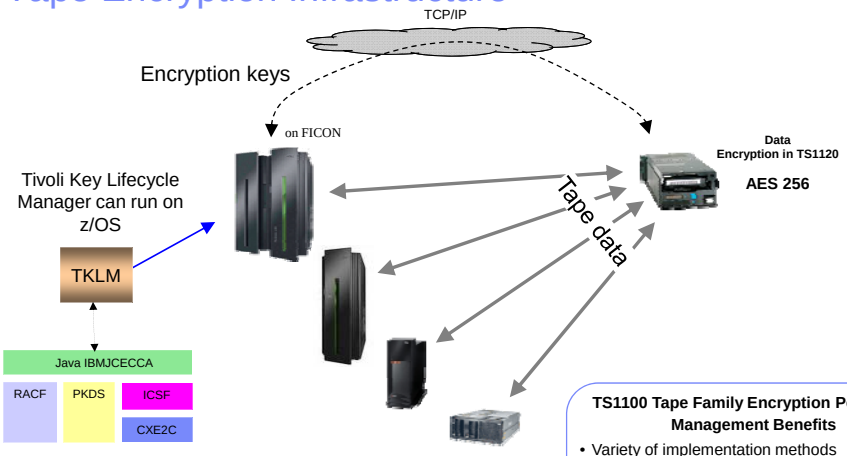


Redbook SG24-7434

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



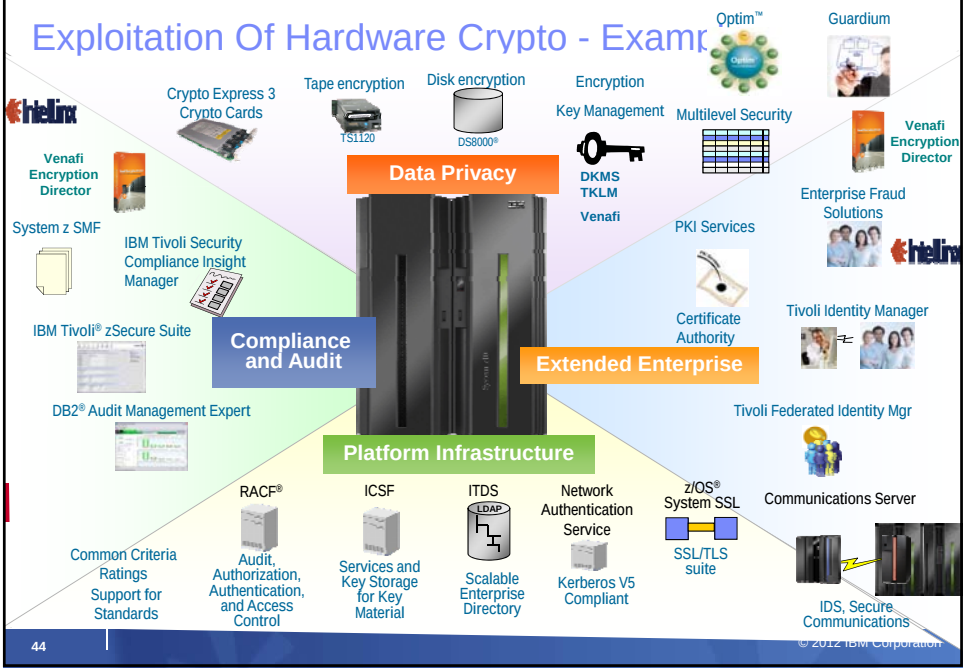
- ✓ Symmetric key generation
- ✓ Symmetric key RSA wrapping/unwrapping
- ✓ RSA keys repository

Redbook SG24-7320

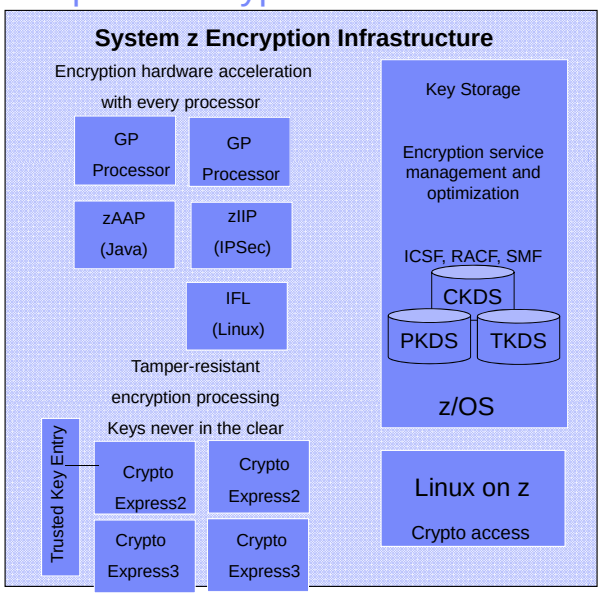
TS1100 Tape Family Encryption Potential Management Benefits

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

Exploitation Of Hardware Crypto - Examp



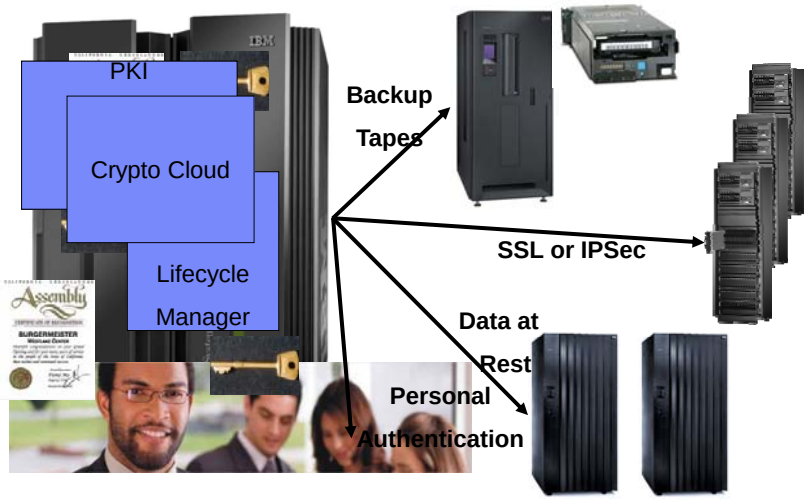
Enterprise Encryption Solutions



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)
- ISKLM - Encryption Key Lifecycle Mgr

Encryption Management & Controls



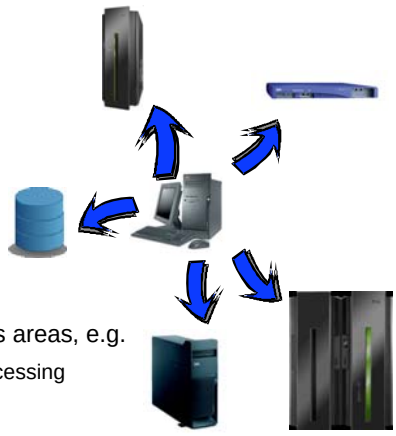
IBM DKMS Key Management System

- IBM's enterprise key management system

  for System z and other IBM platforms

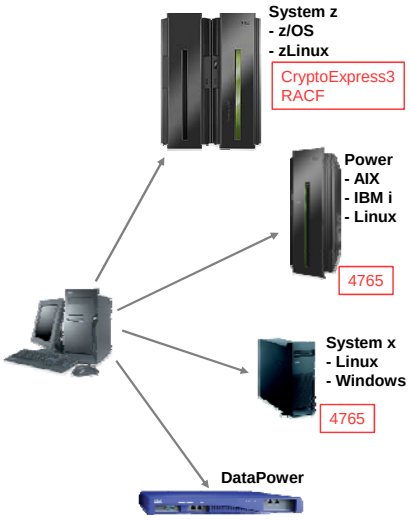
DKMS in a Nutshell

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



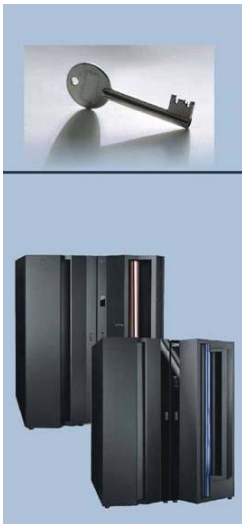
DKMS Key Features

- On-line management of large, heterogeneous environments – from mainframes to distributed servers
- Symmetric and asymmetric keys as well as certificates
- Continuous operation ensured by secure backup and restore of keys
- Automated monitoring of expiry of keys and certificates
- Semi-automated operations enable easy rotation of keys and renewal of certificates



DKMS Supported Systems and Keys

- Supported key types and lengths
  - DES, TDES
  - RSA (up to 4096 bit keys)
  - AES (128, 192, 256 bit keys)
- IBM
  - CryptoExpress2 and 3 on z/OS and zLinux
  - RACF on z/OS (private keys in ICSF)
  - DataPower (private keys and certificates)
  - IBM 4764/5 on AIX, OS/400, IBM i, Windows
- Thales
- Off-line
  - PKCS#11
  - SSL server key stores
    - PKCS#12, JKS, KDB



Monitoring Service

- Monitors expiration of keys and certificates in DKMS key repository
- Monitoring and reports are customizable
- Alerts key managers / application owners by e-mail
- Report available on DKMS workstation as a list of tasks to perform

EMV

Chip card issuing and transaction acquiring

EMVco specifications

.

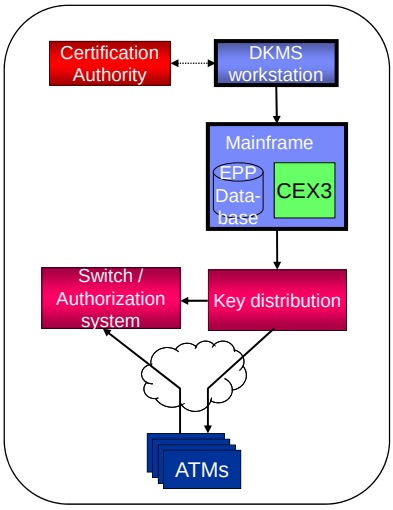
DKMS supports EMV chip cards in several areas

- EMV chip card issuing
  - creating the key material to be loaded to the card
- EMV transactions acquiring
  - authenticating transactions
- EMV root CA
  - DKMS EMV CA used by AMEX and Visa
  - create your own CA based on EMV standards

Implementation of the specifications developed by EMVco and compliance with the procedures required by AMEX, JBC, MasterCard, and Visa

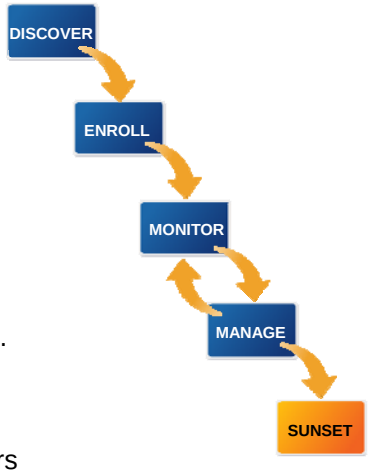
ATM Remote Key Loading

- Electronic distribution of Terminal Master Keys (TMKs)
- Replaces manual handling of TMK key parts
  - saves cost
  - eliminates errors
- Described in ANSI X9.24 part 2
- Is supported by the major ATM vendors Diebold, NCR, and Wincor Nixdorf



Certificate Management

- Centralized management of certificates
- Expiry monitored and managed: Avoid certificate expiry
- Efficient work flow
  - certificate managers takes care of monitoring reports and request certs
  - System administrators install certs and restart service
- Focused on z/OS cert management
  - RACF Key Ring, MQ, System SSL...
  - Tight interaction with z/OS PKI Services
  - off-line support for distributed servers



Advanced Cryptographic Service Provider

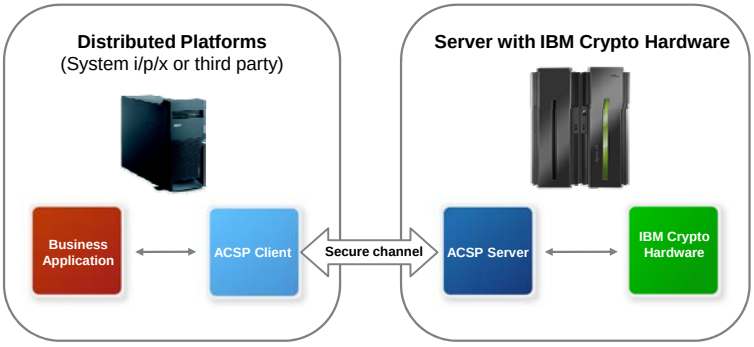
Remote encryption for System z and other platforms

.

The ACSP Concept

- Replace HSMs installed in distributed servers with a Net HSM
  - Utilize mainframe crypto capacity as the Net HSM
    Other servers like Linux servers supported as well
  - Expose crypto functions to client applications
- Benefits
  - Cost effective use of available crypto capacity
  - Reduced administration and simpler key management
  - Crypto support for platforms with no native IBM crypto HW support
  - High scalability, reliability, and availability

ACSP Components



- ACSP client platforms
  - AIX, Linux, Windows
  - (in reality any platform that supports Java)
- ACSP client APIs
  - CCA in Java and C
  - PKCS#11 basic set
- Transport network
  - TCP
  - MQ
  - SSL/TLS protected server/client authentication
- ACSP server platform
  - z/OS, zLinux, Linux
  - CEX2, CEX3, 4764, 4765

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