Rex Johnson
johnsore@us.ibm.com

IBM

12485: Crypto Services For the VMWare Cloud

SHARE 120 San Francisco
February 6, 2013

Trademarks

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

IBM*	FICON*	System z*
IBM (logo)*	IMS	System z10
ibm.com*	Lotus*	Tivoli*
AIX*	POWER7	WebSphere*
BladeCenter*	ProtecTIER*	XIV*
DataPower*	RACF*	zEnterprise
CICS*	Rational*	z/OS*
DB2*	System Storage	z/VM*
DS4000*	System x*	

* Registered trademarks of IBM Corporation

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 there from.
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.
InfiniBand is a trademark and service mark of the InfiniBand Trade Association.
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.

QR Code

Agenda

- Background References

- What's New for SHARE 120 – 2/5/13 Announcements

- 4765 Crypto Chipset Overview

- Advanced Cryptographic Service Provider Overview

- Basic VMWare Usage Pattern

- Enterprise Key Management Foundation Overview

- Crypto Hardware Initialization & Management Overview

- Advanced VMWare Usage Pattern

On the shoulders of giants…
…please refer to these sessions for basic cryptography concepts

- Share Webcast, *Mainframe Data Encryption: Maximizing Efficiency,* by Paul Spicer from PKWare, presented on 7/26/2012, at http://www.share.org/p/cm/ld/fid=208

- 12687: Intro To Crypto – Greg Boyd (IBM Corporation)
  This session will introduce basic concepts of encryption. We'll talk about the crypto related functions that are supported on System z.

- 12793: CYA with NIST Security Standards on System z – Brian Marshall (Vanguard Integrity Professionals)
  This session will help you keep current with the rapidly-changing landscape of security standards enabling you to provide the utmost levels of protection and compliance for your enterprise. Make sure you are **C**overing **Y**our **A**sssets!

What's New for SHARE 120 San Francisco Announcements 2/5/2013

- **Enterprise Key Management Facility (EKMF)**
  - "IBM Enterprise Key Management Foundation, a comprehensive highly secure key management system, which is ideal for banks and payment card processors that must comply with industry standards and manage keys and certificates"

- **Advanced Crypto Service Provider (ACSP)**
  - "By making cryptography-as-a-service available to Linux clients, including those not running on the zEC12, z/OS extends the strength of centralized and secured key management to more enterprise applications."

- **Crypto Hardware Initialization & Maintenance (CHIM)**
  - ICSF equivalent management functionality for IBM 4765 devices in non-zEnterprise systems

- **Announcement Letter 213-013 2/5/13 at:**
  http://www.ibm.com/common/ssi/cgi-bin/ssialias?infotype=AN&subtype=CA&appname=gpateam&supplier=897&letternum=ENUS213-013&pdf=yes

IBM PCIe Cryptographic Coprocessor
IBM 4765 Cryptographic Security Module

- Three form factors
  - PCIe local-bus-compatible interface
  - System z I/O cage carrier (two modules)
  - zEnterprise I/O drawer

- Onboard Key Store in battery backed up memory

- Tamper-responsive module design

- Elliptical Curve Cryptography (ECC) support

- Offloads AES, DES, TDES, RSA, SHA-1, SHA-224 to SHA-512 from main processor(s) on non-CPACF systems

- Functions
  - Asymmetric / RSA Key Generation
  - Symmetric Key Generation
  - CIPHER / DECIPHER
  - Financial PIN Generation and Verification
  - CVV / CVC Generation and Verification
  - …and more…

- High Performance – on System z a single 4765 module has been tested to 6,000 SSL handshakes per second

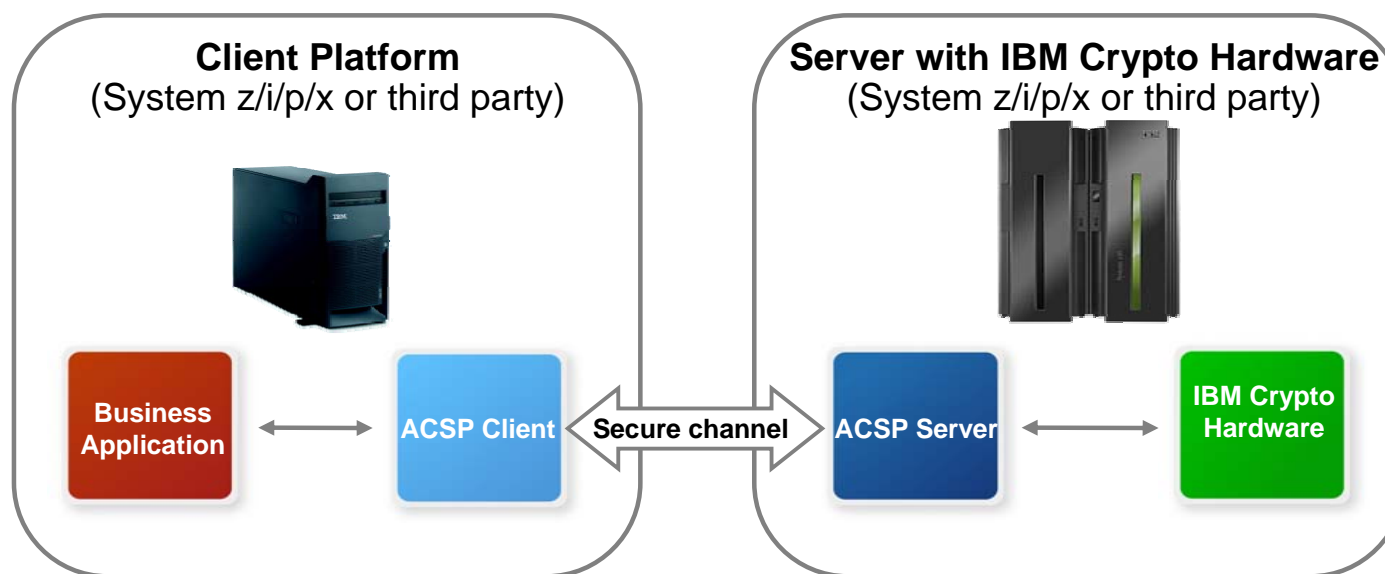- Visit: http://www-03.ibm.com/security/cryptocards/pciecc/overview.shtml
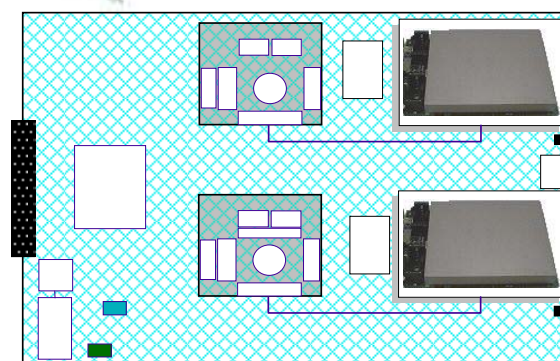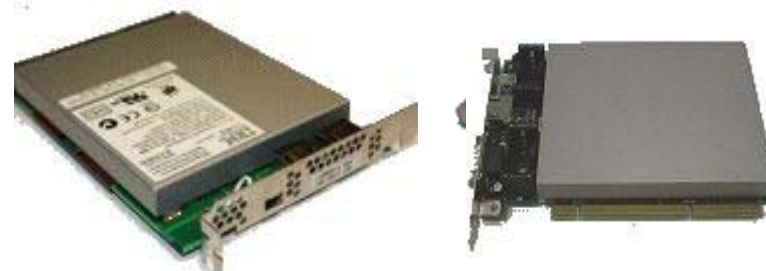
IBM PCIe Cryptographic Coprocessor Run-Time Support / Management

- Common APIs – IBM Common Cryptographic Architecture (CCA) – across all platforms

- POWER – i5OS: Native to OS

- POWER – AIX: CCA Download

- x86 / x64 Windows: CCA Download

- x86 / x64 Linux: CCA Download

- System z – z/VM: Native to OS

- System z – Linux for System z: OS extensions from distributors

- System z – z/OS: Integrated Cryptographic Services Facility (ICSF)

- Major Functions
  - Setup and environmental configuration of device
  - Manage secure material in key store
  - Debugging tools for development (included on z/OS, z/VM and i5OS)
  - Provide high and low level programmatic APIs for application development and exploitation
  - Load balancing across modules for high performance and availability
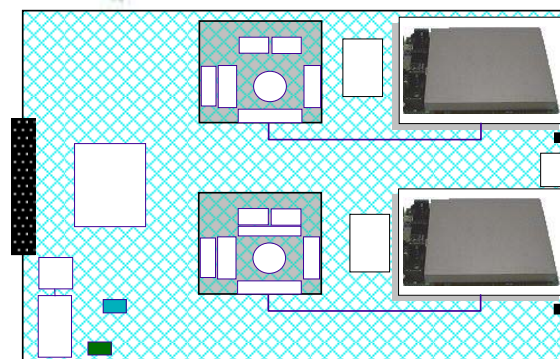
Advanced Crypto Service Provider (ACSP)
Exposing The API Services

- The ACSP Client exposes the standard IBM CCA interface, a PKCS#11 interface and a JCE provider to the business applications. The IBM CCA interface is available as a Java and C interface: IBM CCA in Java and C, PKCS#11 basic set (mapped to CCA) and a Java JCE Provider (basic set mapped to CCA)

- ACSP client platforms: AIX, Linux, Windows (in reality any Java platform)

- ACSP client APIs: Access to UDFs & UDXs are also supported

- The ACSP server schedules and performs the operation in the hardware, subsequently the response is transferred back to the requesting application via ACSP. All operations coming through the server are monitored so statistics can be collected and acted upon. The server runs on all platforms supporting IBM cryptographic hardware

- IBM system z with ICSF on z/OS and CEX3C Crypto HW

- IBM System p with AIX and IBM 4765 Crypto HW – *** Now Available ***

- IBM system x with Linux and IBM 4765 Crypto HW

Client Platform
(System z/i/p/x or third party)

Server with IBM Crypto Hardware
(System z/i/p/x or third party)

Business Application ←→ ACSP Client **Secure channel** ACSP Server ←→ **IBM Crypto Hardware**

Advanced Crypto Service Provider (ACSP)
Virtualization Enables More Platforms

- x86/x64 VMWare with ACSP Linux server guest

- x86/x64 Linux with ACSP server guest

- POWER/VM with ACSP server guest

- PureFlex / PureApplication
  - Multiple PCI Slots
  - POWER or x86/x64 environments
  - Both environments support ACSP Server guests (x86/x64 NOW; POWER NOW)

- z/OS with ACSP provides services to all zBX supported OS images

- z/VM manages guest OS access to hardware on z
  - Linux for System z with ACSP server guest
  - z/OS with ACSP server guest

- ACSP makes the Crypto hardware "Cloud Ready"
  - Wide variety of ACSP Server platforms
  - All cloud OS images can be provisioned with ACSP Client empowering them with a full range of sophisticated crypto functionality

Advanced Crypto Service Provider (ACSP)
The VMWare Pattern

- One image manages Crypto HW
  - Key Store secure
  - Request load automatically balanced over multiple modules
  - Crypto HW access limited to image

- Client virtual machines provisioned with ACSP Server address on the platform

- ACSP Client and Server communicate with each other securely over TCP or MQ protected by SSL/TLS

- Functionally tested with VMWare in 1Q2012 at the IBM Cryptographic Competency Center in Copenhagen, Denmark (CCCC)

- Contact Mark Barnkob at CCCC for test, process, and configuration details
  BARNKOB@dk.ibm.com

Cloud Server
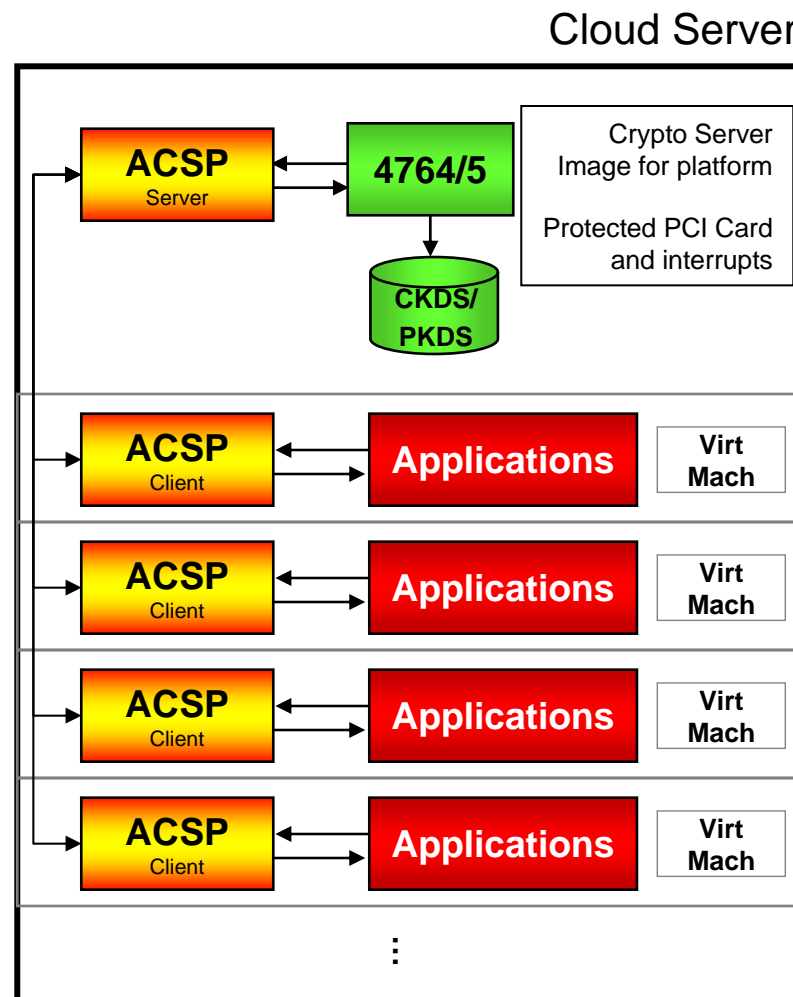
Outcomes

- **Good**
  - Cloud Secured
  - High performance, complex cryptography ubiquitous
  - Crypto message traffic can be managed at any point in the network by locating an additional inexpensive module at strategic points
  - Expense reduced
    - 4765 Module roughly 25-33% of the price of competitive HSMs
    - Test, Development, and QA can make use of excess production crypto capacity

- **Not So Good**
  - Lots of 4765 modules => lots of key stores
  - Manual key store loading (modules and z/OS ICSF images)
    - Error prone
    - Time & Labor consuming
    - Manual processes frowned on by auditors and regulators
  - Key Store consumption – To prevent errors, some may choose to put all keys in every key store

Enterprise Key Management Foundation (EKMF)
Centralized Management of Key Material

- Clients asked for it – IBM listened

- One central system for managing all keys

- On-line management of large systems, both System z and distributed servers – A Push model for key management

- Central key repository for archive and backup - enabling key restore and reporting

- Monitoring expiry of keys

- Semi-automated operations support rotation of keys and multiple key generation

- Split knowledge and dual control can be enforced

- Services Offering like GDPS

  – Deploy only functionality you need

  – Fit your policies, processes, and procedures

  – Solution – Not a checklist of products to order

Enterprise Key Management Foundation (EKMF)
Key Benefits (Pun Intended)

- Remove sources of error by
  - Implementation of strict and efficient processes
  - Key templates making it possible to test processes thoroughly before moving to production

- Provide a higher quality of service by
  - Automated distribution of keys to key stores at time of generation
  - Recovery of keys removed from key stores by accident or disaster

- Effective due to
  - Monitoring key expiry
  - Semi-automated generation and multiple key generation
  - Work flow support

- Enable PCI-DSS compliance
  - Access control system
  - Audit log
  - Compliant with NIST Key Management standard - NIST SP800-57

Enterprise Key Management Foundation (EKMF) Overview

- The IBM EKMF solution comprises a central repository, a highly secured workstation and a browser application.

- All new keys are generated on the workstation by users authenticated with smart cards.

- The browser application features monitoring capabilities and enables planning of future key handling session to be executed on the workstation.

- The central repository contains keys and metadata for all cryptographic keys produced by the EKMF workstation. This enables easy backup and recovery of key material in case of a disaster.

- All key generations take place on the EKMF Workstation which is based on a the IBM 4765, in a physically secure location

ICSF Enabled z/OS LPARS

Central Key Repository

EKMF Browsers

Custodians
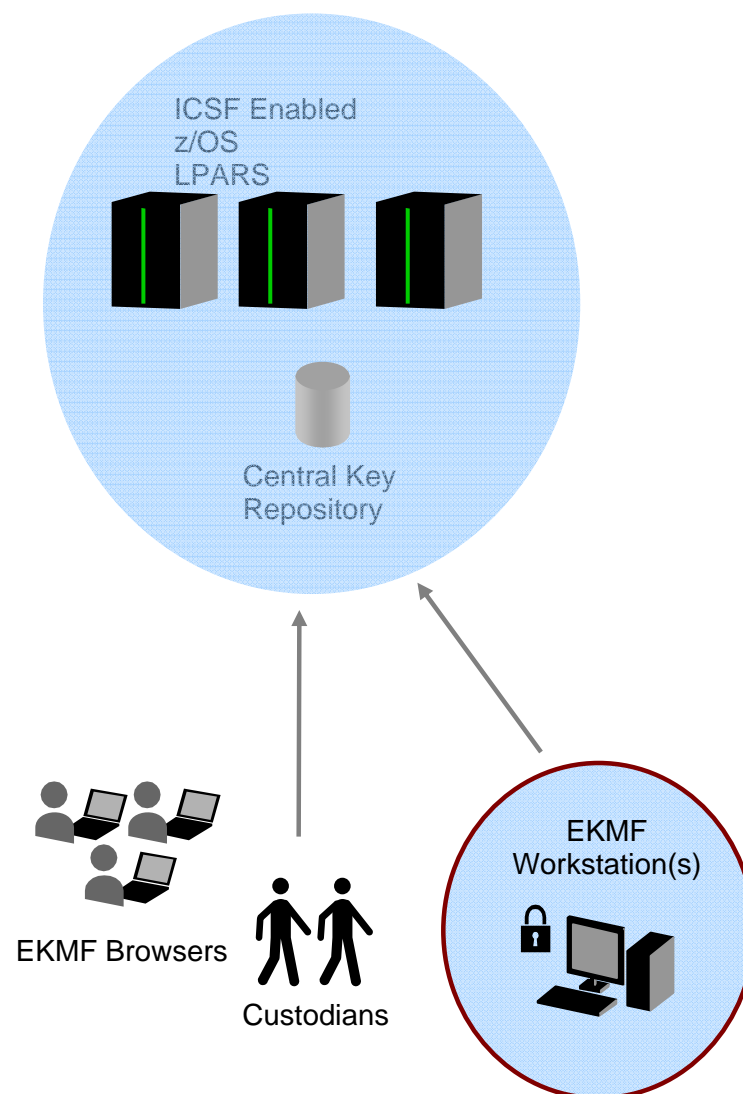
EKMF Workstation(s)

Enterprise Key Managment Foundation (EKMF) Architecture and Components

- EKMS Workstation is online with all crypto servers in the system

  - ALL connections are secure, encrypted and protected
  - Manages the keys in ICSF/4765 module key stores
  - Support for several workstations for disaster recovery and business continuity

- One DB2 server is hosting the EKMF Repository

  - containing keys and metadata
  - for easy backup and recovery
  - DB2 Queue Replication can maintain a mirror of the EKMF Repository at an alternate, or disaster recovery, location
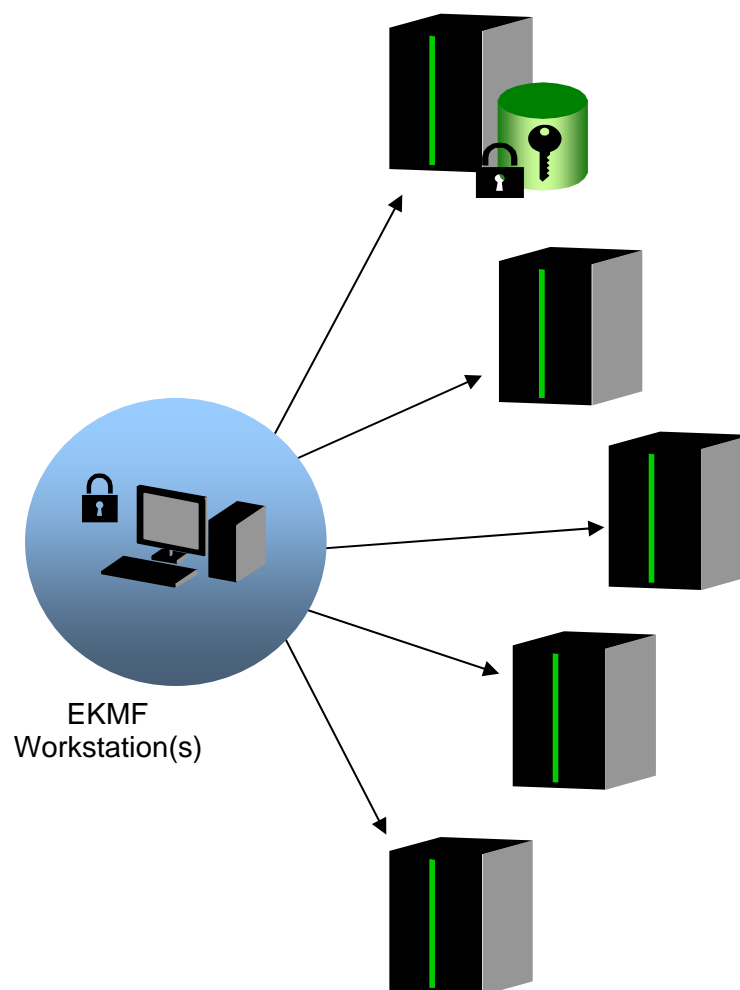
EKMF
Workstation(s)

Enterprise Key Managment Foundation (EKMF)
Key Management Model

- Different user roles for segregation of duties
  - Administrators for system configuration and planning of key ceremonies
  - Custodians for key generations and handling of cryptographic variables

- Key Templates for efficient key design and handling
  - All keys in EKMF are based on a key template.
  - Enables designing and testing before generating keys in production
  - Comprises the properties of a key – such as:
    - key labels, (de)activation dates, key state etc.
    - origin of the key (generation, import or translation)
    - where it must be placed after entering the system

- Push model
  - Keys are pushed to the keys stores

- Secure audit log for reliable review by auditors

- Compliant with NIST Key Management standard - NIST SP800-57

Key Management Model

Procedures for handling physical Security secure room, smart cards etc.

Procedures + **User Roles** + **Key Templates**

Key Material and metadata for Backup/Archive

Key Repo

EKMF

Key Exchange (clear parts or encrypted)

3rd Party KMS

Online interaction with all IBM Crypto

ICSF

ACSP/CHIM Server

Encryption Entity

Application

Encrypted Data transfer

Application

Encrypted Data Transfer

Application

SHARE 120 San Francisco 12485: Crypto Services For the VMWare Cloud

EKMF addresses System z; Gaps Exist

- Secure enrollment of IBM 4765 devices for IBM System x, PureFlex and POWER, as well as IBM devices installed in non-IBM servers

- Central "crypto" management of multiple servers with multiple IBM 4765 devices
    - Centralized overview
    - Personalization (device key, polices)
    - Generate/load Masterkeys
    - Load user credentials
    - Manage UDXs (based on new UDX development process)

- Monitor servers and devices (status, warnings, errors, performance, capacity, response time)

Crypto Hardware Initialization & Management (CHIM)
Basic Concepts

- CryptoNodeManager (System x, PureFlex, POWER) / TKE (z) / EKMF CryptoServerManagement like functions for CHIM manager, including smart card access

- TKE like securely protected end-to-end commands

- RACF like access control of keys and functions

- MoteRunner (IBM virtual machine) for UDX development and runtime

- Graphical user interface based on Eclipse

- Prerequisites

  - ACSP
    - ACSP for transport and access to the IBM 4765
    - ACSP logging and monitoring
    - ACSP Server for easy enablement of ACSP services to applications
  - EKMF
    - Device Configuration Integration
    - Application Deployment Profile Integration

Crypto Hardware Initialization & Management (CHIM) Vision

Vision: Provide from a central location, the ability to securely enroll, initialize and configure IBM crypto devices on IBM System x, PureFlex and POWER, and manage these using best practices.

Cluster x with 2 x System p+IBM 4765

Central CHIM management system

Cluster 1 with 2 x System p +IBM 4765

CHIM Management

Secure channel

CHIM Agent

IBM Crypto Hardware (UDX)
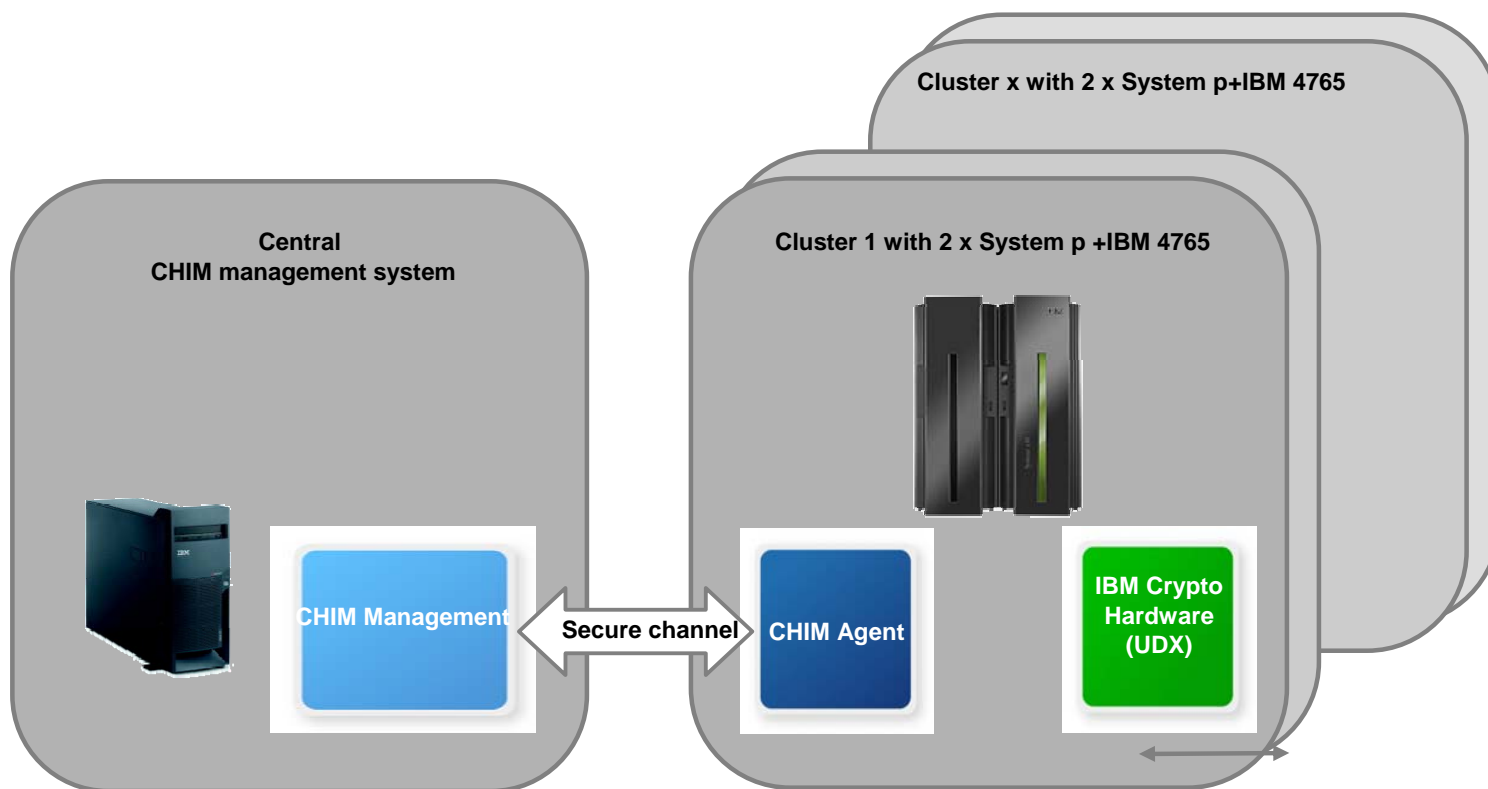
Crypto Hardware Initialization & Management (CHIM) Manager controls multiple CHIM Agents

CHIM Manager:

Manage IBM 4765 devices (enroll, intialize, configure)

Manage UDXs in IBM 4765 device
Monitor IBM 4765 devices

CHIM Agent and Firmware:

CHIM firmware in 4765 provides end-to-end security

Cluster x with 2 x System p+IBM 4765

Cluster 1 with 2 x System p +IBM 4765

Central
CHIM management system

CHIM Management

Secure
channel

CHIM Agent

IBM Crypto
Hardware
(UDX)

Secure Channel
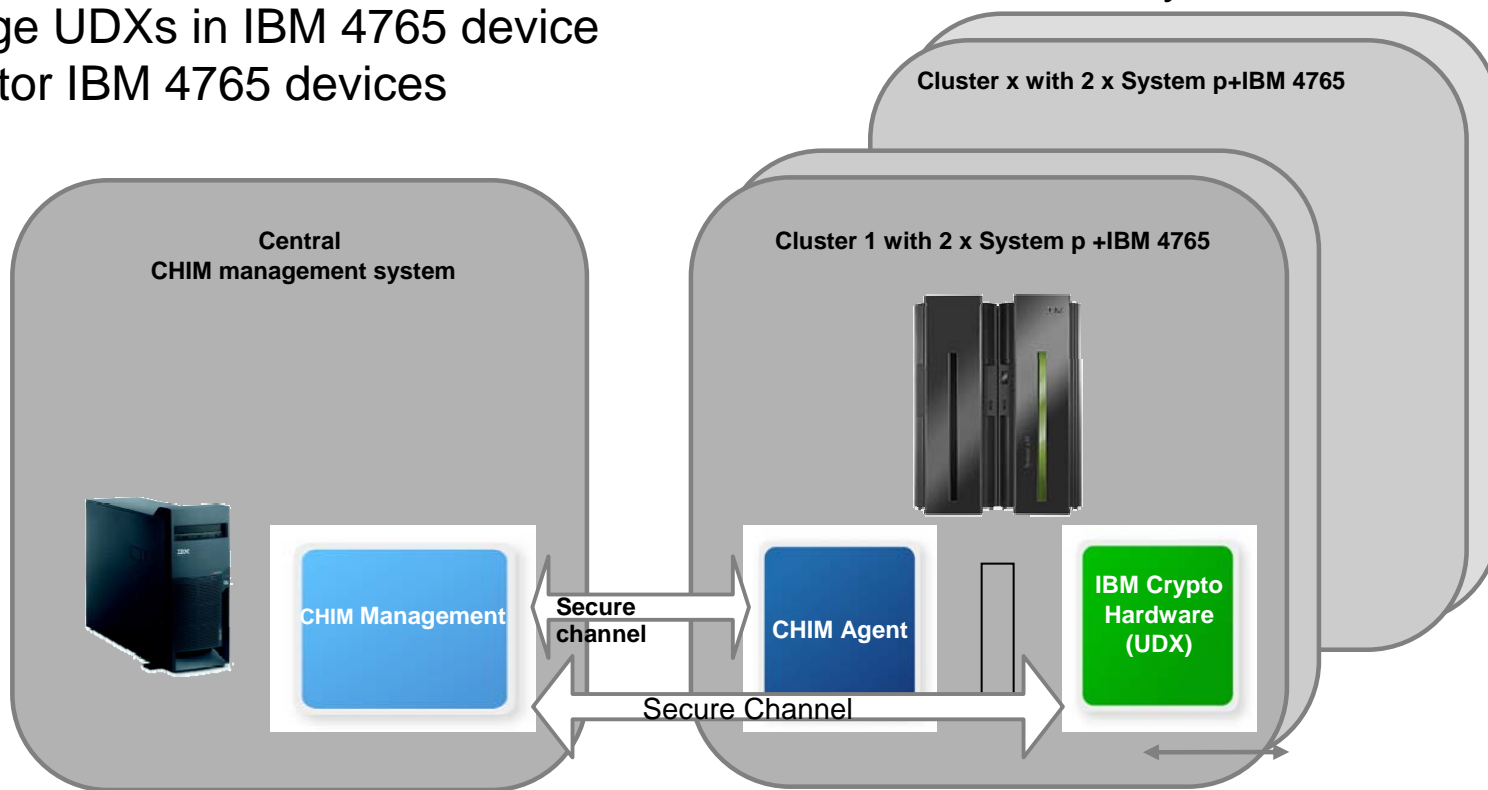
Crypto Hardware Initialization & Management (CHIM)
Agent can be enabled for business application interaction

On the client side:

IBM CCA (C, Java),

UDF and UDX supported

On the server side:

IBM CCA w. UDX/UDF

Application servers

IBM System x, p with IBM 4765

Business Application

ACSP Client (UDF,UDX)

Secure channel

CHIM Agent ACSP Server

IBM Crypto Hardware (UDX)
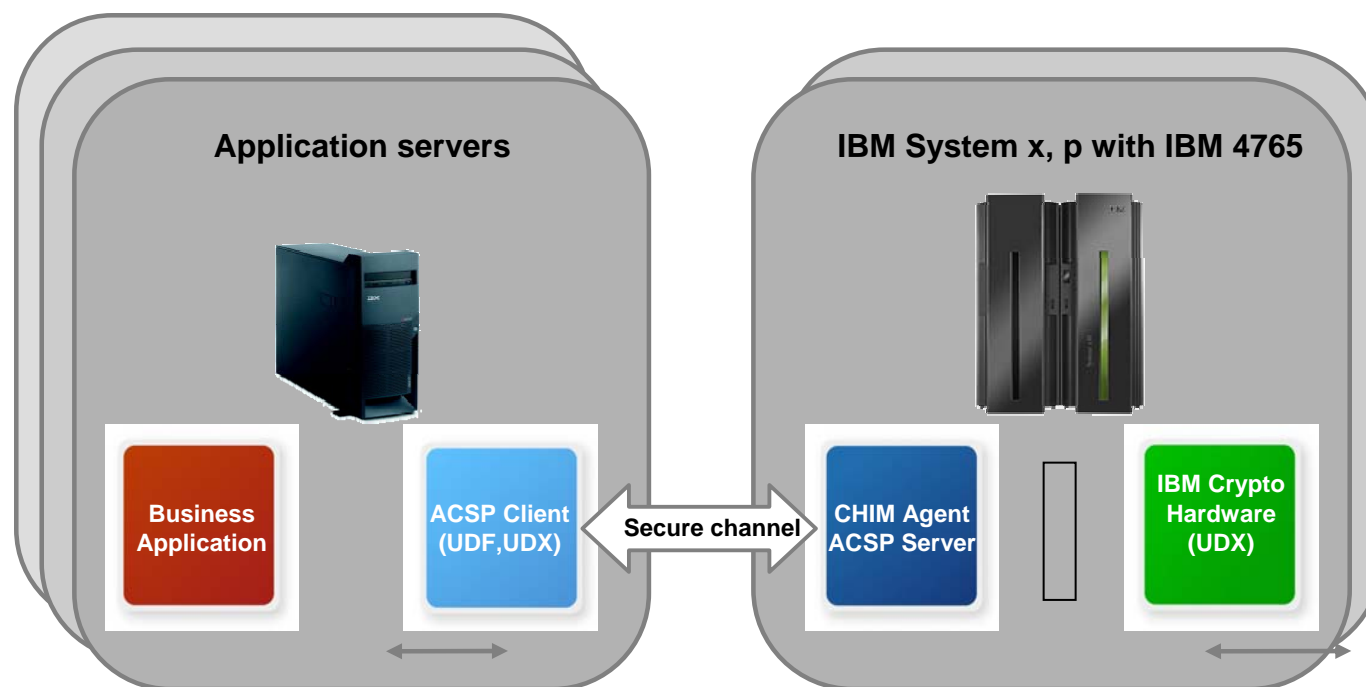
CHIM/ACSP Monitoring – aggregated from all servers with crypto devices

IBM CCCC Server Monitor

CccAcsp | CccNet | Runtime Info | Thread Info

Card Stats | CCA Verb Stats | UDF Call Stats | CCA Throughput Stats | CCA Alert logging

Name	Calls	Failed
ALLCARDS	202,752	0
HSM_1	202,752	0

IBM EKMF ACSP Server Monitor

CccAcsp | CccNet | Runtime Info | Thread Info

Card Stats | CCA Verb Stats | UDF Call Stats | CCA Throughput Stats | CCA Alert logging

VerbName	Total Calls	Direct Calls	Client Calls	Failed	Recv.Time	T.Recv.Time	Resp.Time	T.Resp.Time	Avg. Exec Ti...	Total Exec.T...
CSNBKEX	2	0	2	2	75.82 ms	0.152 s	0.737 ms	0.001 s	0.406 ms	0.001 s
CSNBKGN	34,236	33,283	953	2	65.903 ms	62.805 s	0.053 ms	0.051 s	1.514 ms	51.835 s
CSNBKIM	2	0	2	2	67.816 ms	0.136 s	0.73 ms	0.001 s	0.796 ms	0.002 s
CSNBKPI	2	0	2	2	66.31 ms	0.133 s	0.78 ms	0.002 s	0.39 ms	0.001 s
CSNBKRC	2	0	2	2	66.424 ms	0.133 s	0.789 ms	0.002 s	0.076 ms	0 s
CSNBKRD	2	0	2	2	71.37 ms	0.143 s	0.686 ms	0.001 s	0.081 ms	0 s
CSNBKRR	4	0	4	2	122.563 ms	0.49 s	0.369 ms	0.001 s	0.306 ms	0.001 s
CSNBKRW	2	0	2	2	70.082 ms	0.14 s	0.624 ms	0.001 s	0.076 ms	0 s
CSNBKTB	7,515	6,562	953	2	65.127 ms	62.066 s	0.044 ms	0.042 s	0.035 ms	0.263 s

Crypto Hardware Initialization & Management (CHIM) Summary

- IBM 4765 card is loaded with firmware in a trusted environment – typically at a physically secure central site

- Each server is registered with type, serial number, OS version, CHIM Agent version, CCA version

- Each crypto device is registered with type, serial number, firmware version

- Manage Master Keys in devices (secure load, enroll in zone) – load in multiple devices (group)

- Manage Roles and Profiles in devices (secure load)

- Manage UDXes (secure load)

- Manage keystores

- Backup / Restore / Clone configuration data

- Scalable solution – multiple servers, multiple devices per server

- CHIM uses the ACSP management UI

Crypto Hardware Initialization & Management (CHIM) Benefits

- Central management – enables efficient operations and consistent policy compliance

- CHIM management program supports smartcard for authentication and loading key parts, and entry of key parts via the cardreader

- IBM EKMF can manage the keys and certificates and provide DR capability (shares device config data)

- Flexible logging of events

- Monitors, creates, and can forward events to multiple locations, processes, or higher-level service monitors

- Discrete levels of monitoring detail
  - Overview, Create, Update, Delete
  - Proactive configuration health (status, warnings, errors, performance, capacity, response time)

The VMWare Pattern
Including System z and VMWare as Managed Crypto Servers

EKMF workstation

CHIM
Manager

System z
with key repository

EKMF Agent   Applications

ICSF

SMF log   CKDS/ PKDS   EKMF key repo

Cloud Server

EKMF Agent

ACSP Server   4764/5

CHIM Agent   CKDS/ PKDS

Crypto Server Image for platform

Protected PCI Card and interrupts

ACSP Client   Applications   Virt Mach

ACSP Client   Applications   Virt Mach

ACSP Client   Applications   Virt Mach

ACSP Client   Applications   Virt Mach

zEnterprise Pattern

| Unified Resource Manager | | Private Management Network INMN |
| Private High Speed Data Network IEDN |

System z Host

Select IBM Blades

Optimizers

EKMF Agent

ICSF

ACSP Server

z/OS

z/TPF z/VSE™ Linux on System z

Linux on System z

ACSP Client

Linux / Windows on System X [1]

ACSP Client

AIX on POWER7

DataPower [1]

IBM Smart Analytics Optimizer

Future Offering

Future Offering

z/VM

Blade Virtualization

Blade Virtualization

System z PR/SM™

z HW Resources

Blade HW Resources

Support Element

zBX

System z Hardware Management Console (HMC), with Unified Resource Manager

SMF log

CKDS/ PKDS

EKMF key repository

Private data network (IEDN)

Customer Network

Customer Network

[1] All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represents goals and objectives only.

The Bottom Line
or Some Things I Learned at SHARE

- IBM has a complete, end-to-end, multi-platform cryptography enablement and management system in support of data security with common APIs across platforms

- The 4765 Crypto module offloads complex algorithms from our CPUs, is fast, powerful, tamper-responsive, FIPS 140-2 certified, and runs at bus speeds inside of ALL IBM systems, including System z and the new PureFlex family (Hmmm…Bus speed is way faster than our network or channel attached devices…And it is around 70% less expensive)

- Advanced Cryptographic Service Provider (ACSP) exposes the hardware function to any client system image (That means at its slowest, IBM's solution has the same latency delays as our network attached devices)

- Crypto Hardware Initialization & Management (CHIM) provides central management of master keys (like the TKE) on distributed systems equipped with 4765 Crypto cards.

- Enterprise Key Management Foundation (EKMF) provides a central repository on DB2 for storing all the key materials we need, encrypted, in both a local and remote database, as well as pushing all requisite key material to all crypto modules anywhere in our enterprise with audit trails (We could do it by hand, typing into ICSF or the individual servers, but how would we audit that? I wonder if our Security folks have a backup of our keys and certs at the DR site? Hope so…)

![IBM]

Thank You
From Your Key Security Contacts

- John Dayka – dayka@us.ibm.com – Security Hardware and Strategy

- Leo Moesgard – lemo@dk.ibm.com – Crypto Solutions Sales Manager (CCCC)

- Mark Barnkob – BARNKOB@dk.ibm.com – Crypto Solutions Architect (CCCC)

- Carsten Frehr – CDF@dk.ibm.com – Lead Architect Crypto Solutions (CCCC)

- Greg Boyd – boydg@us.ibm.com – ATS System z Security Team

- Rex Johnson – johnsore@us.ibm.com – Solutions Client Architect

- Please visit the CCCC website for additional details
  http://www-03.ibm.com/security/cccc/products/dkms.shtml

- Explore IBM PCIe Cryptographic Coprocessor hardware at
  http://www-03.ibm.com/security/cryptocards/pciecc/overview.shtml

Questions?

CHIM Backup

UDX development

- The UDX functionality is developed in Java and converted to special byte code

- A Mote Runner virtual machine is implemented in segment 3 as an old fashioned UDX and signed as today.
  The Mote Runner VM is enhanced to support CCA.

- UDX code is signed during the conversion - with dual control and integrity check mechanisms (hash on source and load)

- UDXes are loaded and activated via the CHIM Manager

- A generic UDX API is available through the normal application interface and that API maps to the UDX functions loaded

CHIM Version 1 – plan 1Q13

V.R	CHIM Manager Platform	CHIM Agent Platform	Features
1.0	System x SLES 11 IBM 4765	System x SLES 11 / RHEL 6 IBM 4765 ACSP 1.3	Secure enrollment Secure configuration load Secure MasterKey load Monitoring Logging

CHIM V1.0
- basics for secure enrollment and initialization of remote IBM 4765 devices
- backup/restore/clone

CHIM V1.1
- UDX load and management from CHIM Manager
- new UDX development process

CHIM V1.2
- EKMF integration (device configuration, agent to use ACSP)
- enhanced monitoring capabilites
- enhanced logging capabilities

Stories / Use cases

- **As a Crypto HW manager**
    - Load IBM 4765 firmware at a trusted site
    - Securely enroll an IBM crypto device on x and p from a remote management center
    - Securely load authorities and policies (users, access controls) - remote

- **As a Key manager**
    - Generate and load Master keys into the device – remote
    - Load applications keys into the device - remote

- **As a System operator**
    - Overview of all managed devices and keystores - remote
    - Monitor status, load, problems on devices – remote
    - Monitor Logs on managed devices - remote