Rex Johnson
johnsore@us.ibm.com

# 11390: Crypto Services For the VMWare Cloud

SHARE Anaheim
August 8, 2012

# 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.

# Agenda

- Background References
- 4765 Crypto Chipset Overview
- Advanced Cryptographic Service Provider Overview
- Basic VMWare Usage Pattern
- Distributed Key Management System Overview
- Advanced VMWare Usage Pattern

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

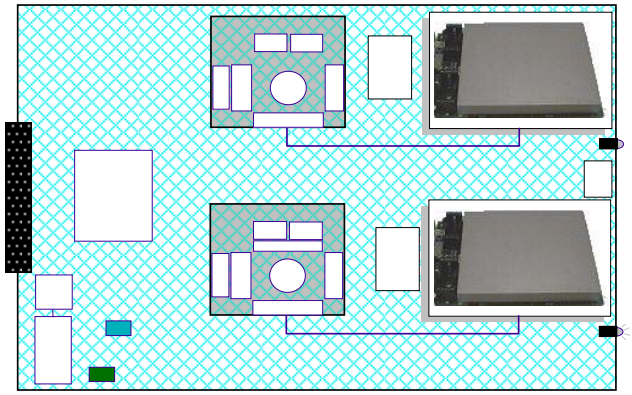
- Share Webcast, *Mainframe Data Encryption: Maximizing Efficiency,* by Paul Spicer from PKWare, presented on 7/26/2012, at http://www.share.org/p/cm/ld/fid=208

- 11484: 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.

- 11622: Digital Certificate Demystified – Ross Cooper (IBM Corporation)
  This is a beginner's guide to digital certificates. After the session, the participants will have a basic understanding on what a certificate is and how it works based on the public key cryptography technology, why there are different types certificates like SSL certificates, code signing certificates, EV (Extended Validation) certificates... and what differentiates them, how long should a certificate be renewed, how to decide if they need to be issued by a commercial certificate authority (CA) or issued internally.

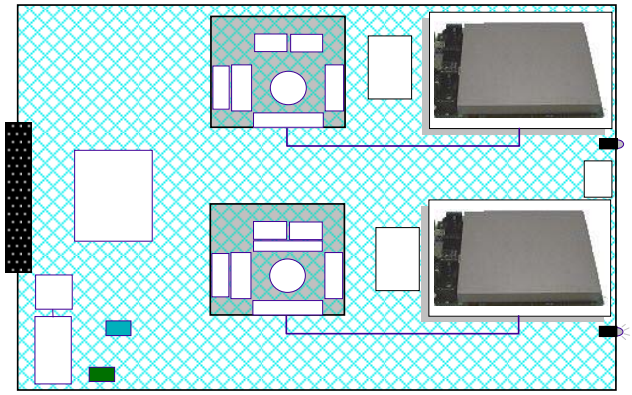
# IBM PCIe Cryptographic Coprocessor
# IBM 4765 Cryptographic Security Module

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

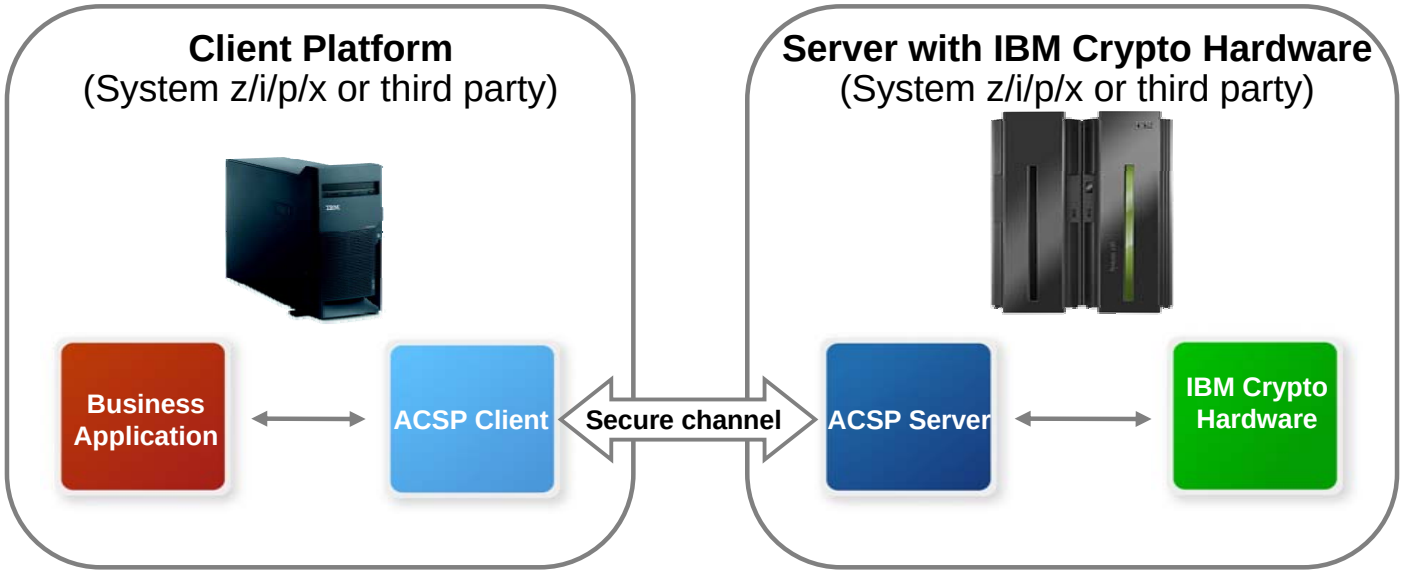
- Common APIs – IBM Common Cryptographic Architecture (CCA) – across all platforms
- POWER – i5OS: Native to OS
- POWER – AIX: CCA Download
- x86 / x64 Windows: CCA Download
- x86 / x64 Linux: CCA Download
- System z – z/VM: Native to OS
- System z – Linux for System z: OS extensions from distributors
- 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 – coming 2H2012
- IBM system x with Linux and IBM 4765 Crypto HW

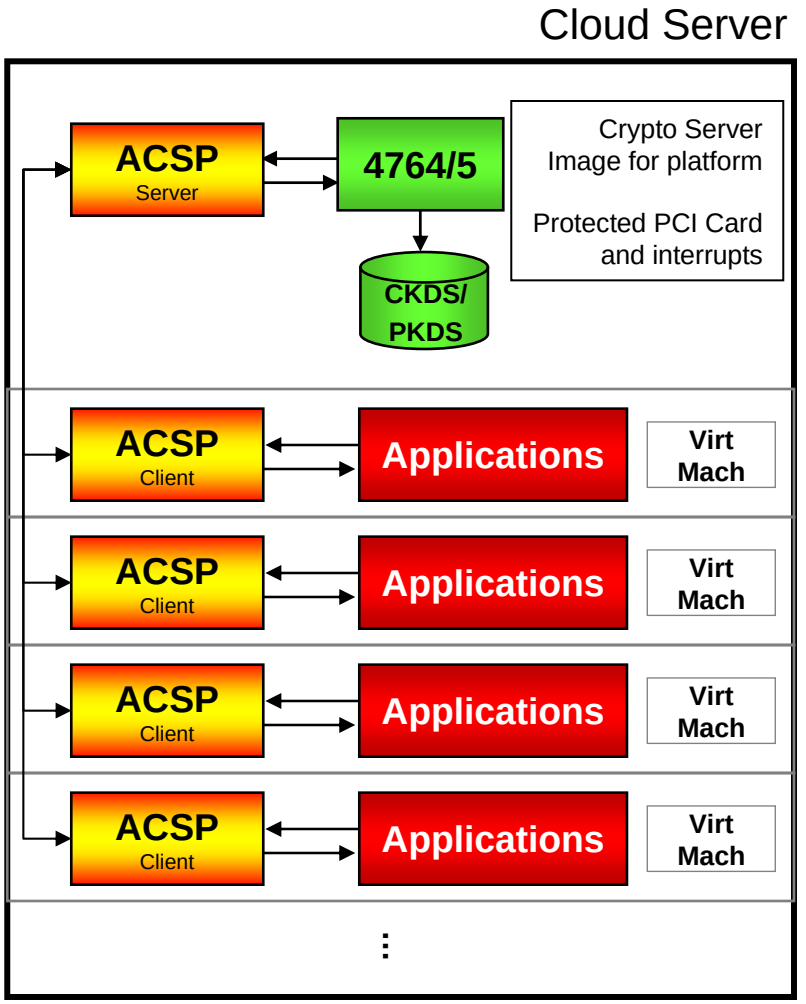


# Advanced Crypto Service Provider (ACSP)
# Virtualization Enables More Platforms

- x86/x64 VMWare with ACSP Linux server guest
- x86/x64 Linux with ACSP server guest
- Power/VM with ACSP server guest (2H2012)
- PureFlex / PureApplication
  - Multiple PCI Slots
  - POWER or x86/x64 environments
  - Both environments support ACSP server guest (x86/x64 now; POWER 2H2012)
- 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



# 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

# Distributed Key Management System (DKMS)
# Centralized Management of Key Material

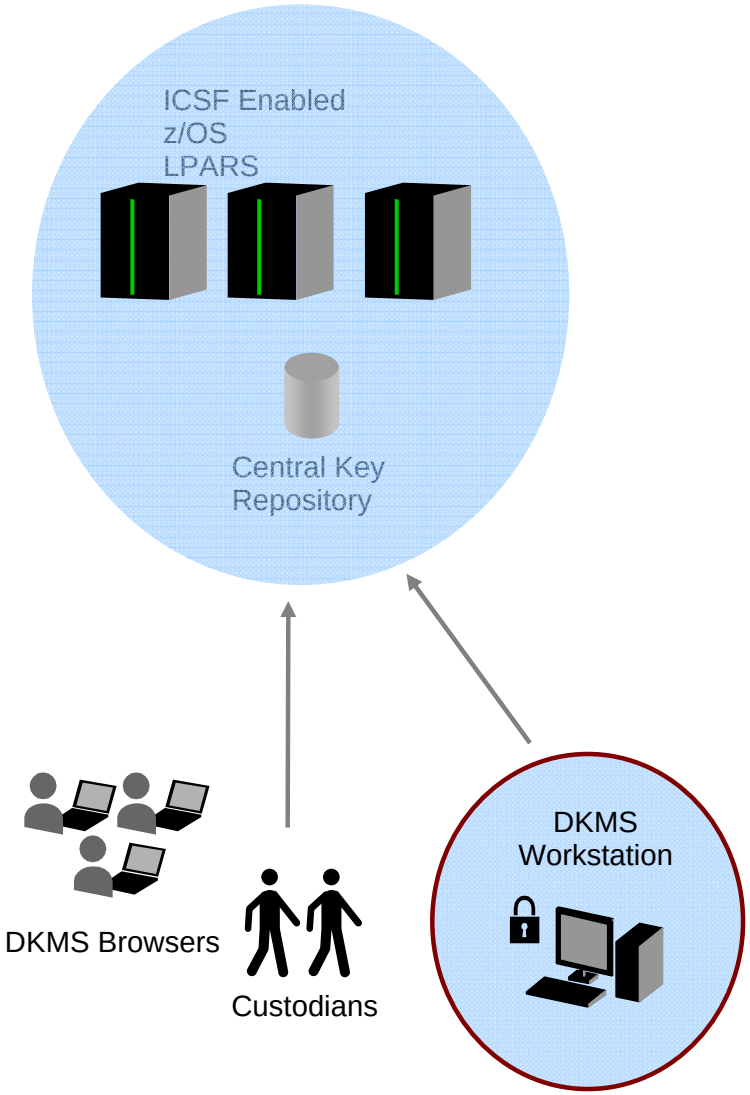
- One central system for managing all keys
- On-line management of large systems, both System z and distributed servers – A Push model for key management
- Central key repository for archive and backup - enabling key restore and reporting
- Monitoring expiry of keys
- Semi-automated operations support rotation of keys and multiple key generation
- Split knowledge and dual control can be enforced

# Distributed Key Management System (DKMS)
# 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

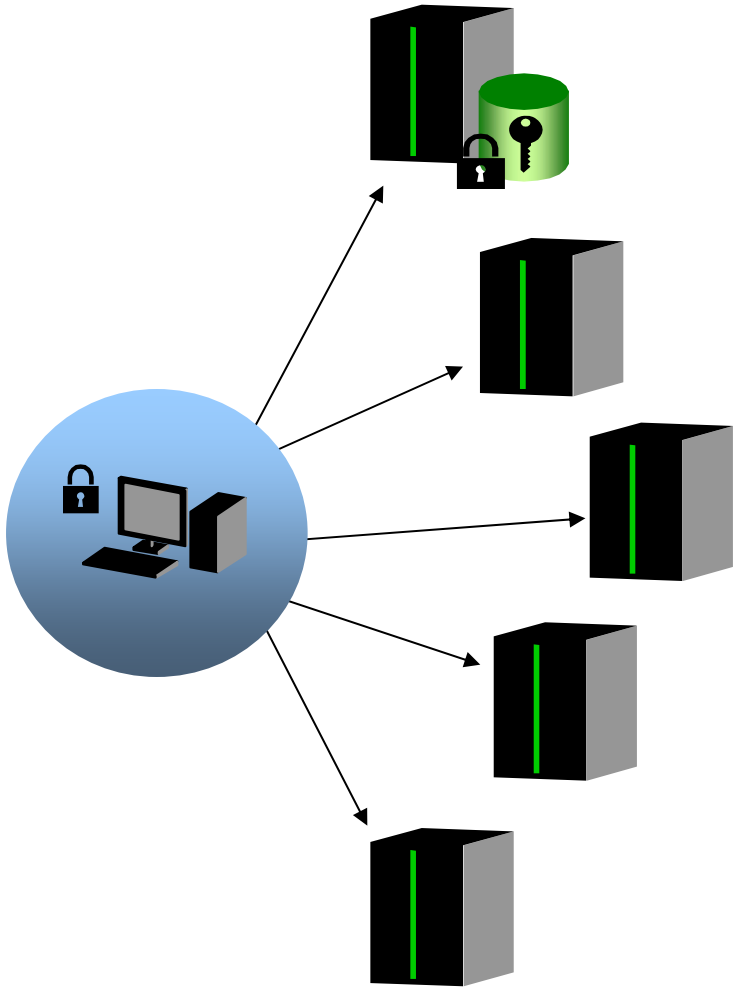
# Distributed Key Management System (DKMS) Overview

- The IBM DKMS 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 DKMS workstation. This enables easy backup and recovery of key material in case of a disaster.
- All key generations take place on the DKMS Workstation which is based on a the IBM 4765, in a physically secure location



# Distributed Key Management System (DKMS) Architecture and Components

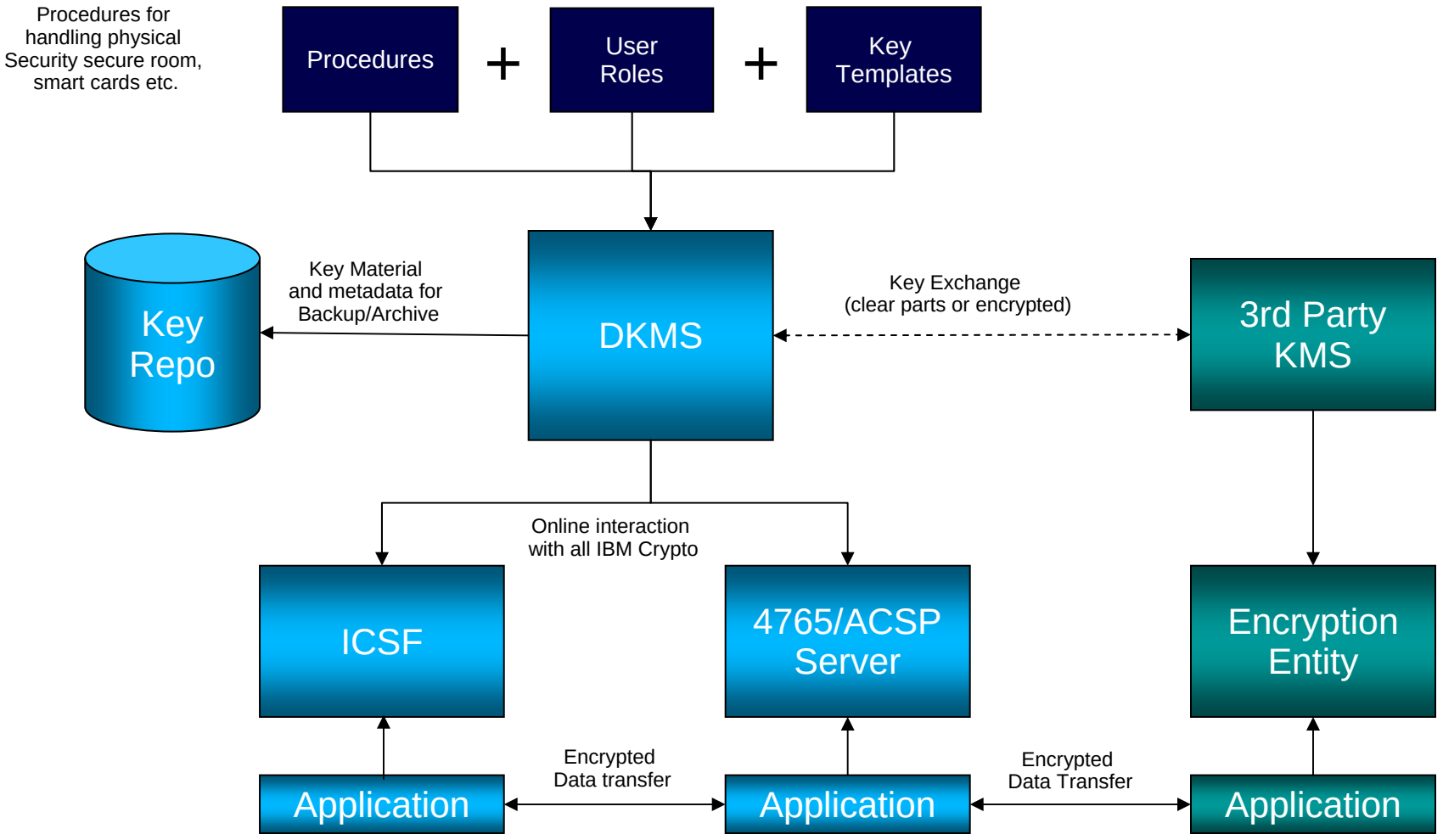
- DKMS Workstation is online with all crypto servers in the system
  - ALL connections are secure, encrypted and protected
  - Manages the keys in ICSF/4765 module key stores
  - Support for several workstations for disaster recovery and business continuity
- One DB2 server is hosting the DKMS Repository
  - containing keys and metadata
  - for easy backup and recovery
  - DB2 Queue Replication can maintain a mirror of the DKMS Repository at an alternate, or disaster recovery, location



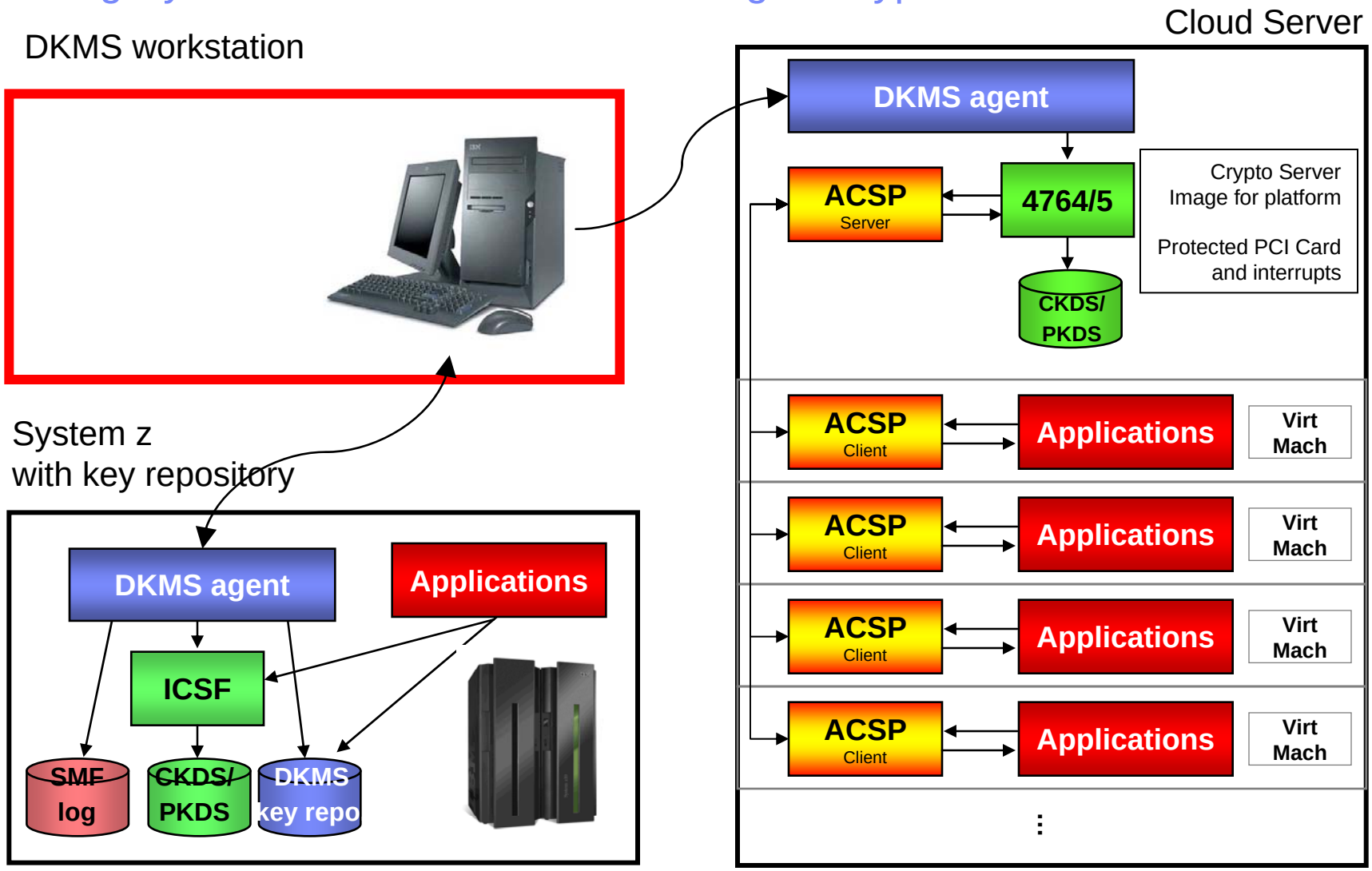
# Distributed Key Management System (DKMS)
# Key Management Model

- 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 DKMS 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

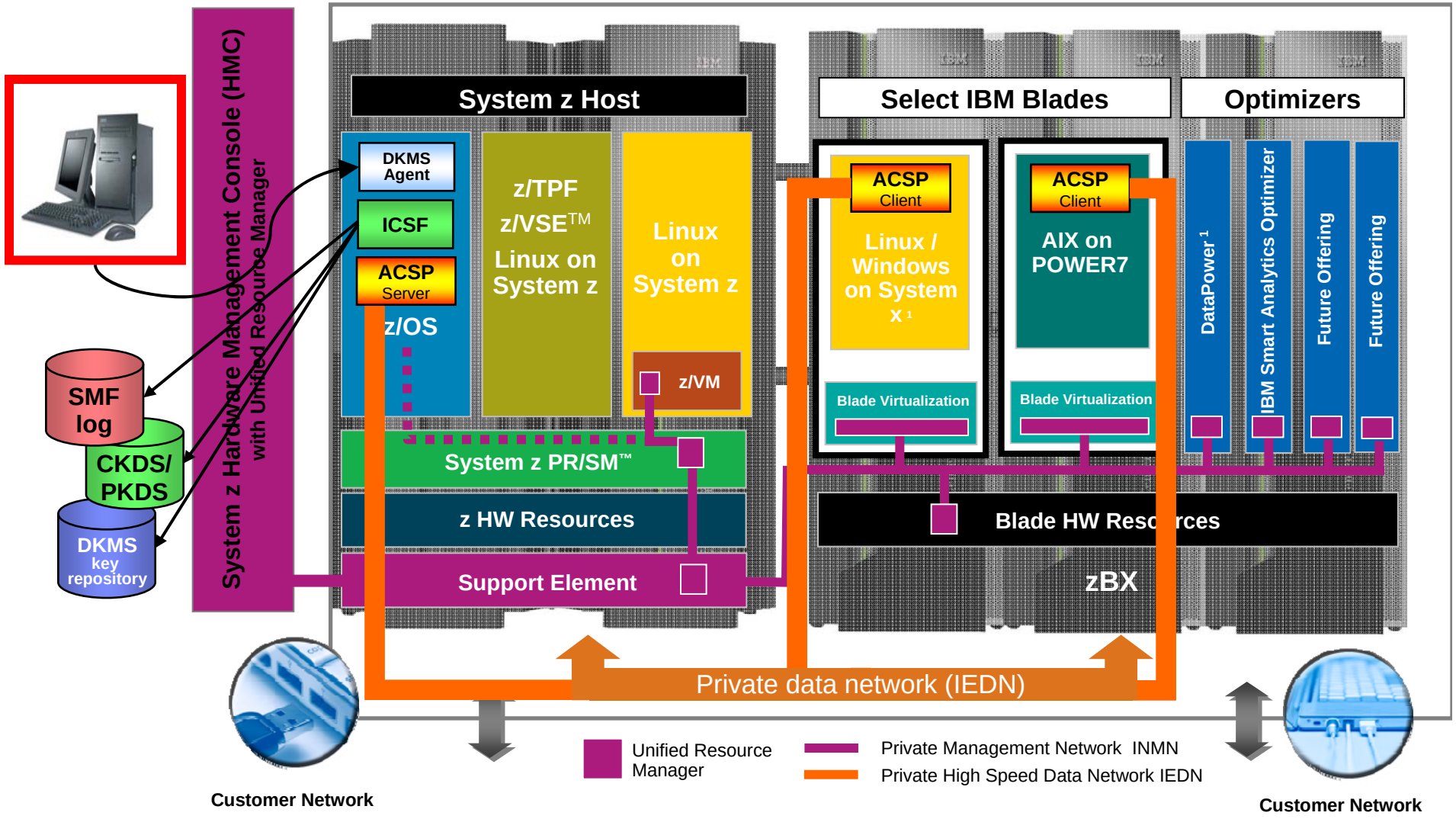
# Key Management Model



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



# zEnterprise Pattern




[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)
- Distributed Key Management System (DKMS) 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…)

# Thank You
# From Your Key Security Contacts

- Rich Skinner – rcs@us.ibm.com – Americas Security Solution Sales
- 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 DKMS (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?