Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

IBM

IBM Americas ATS, Washington Systems Center

10195 Crypto And Disaster Recovery

SHARE

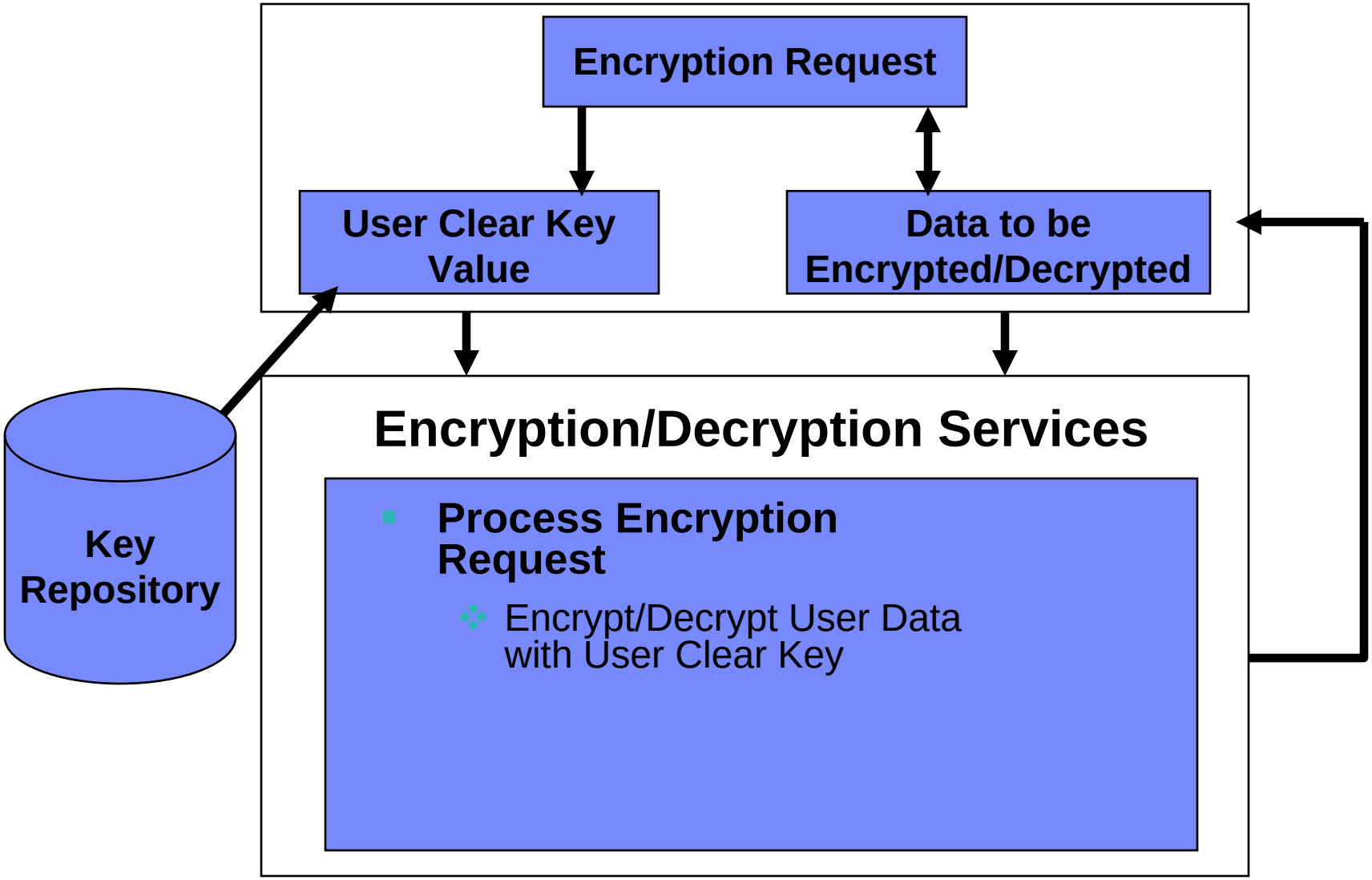
Greg Boyd (boydg@us.ibm.com)
March 16, 2012
Atlanta, GA

ON DEMAND BUSINESS™

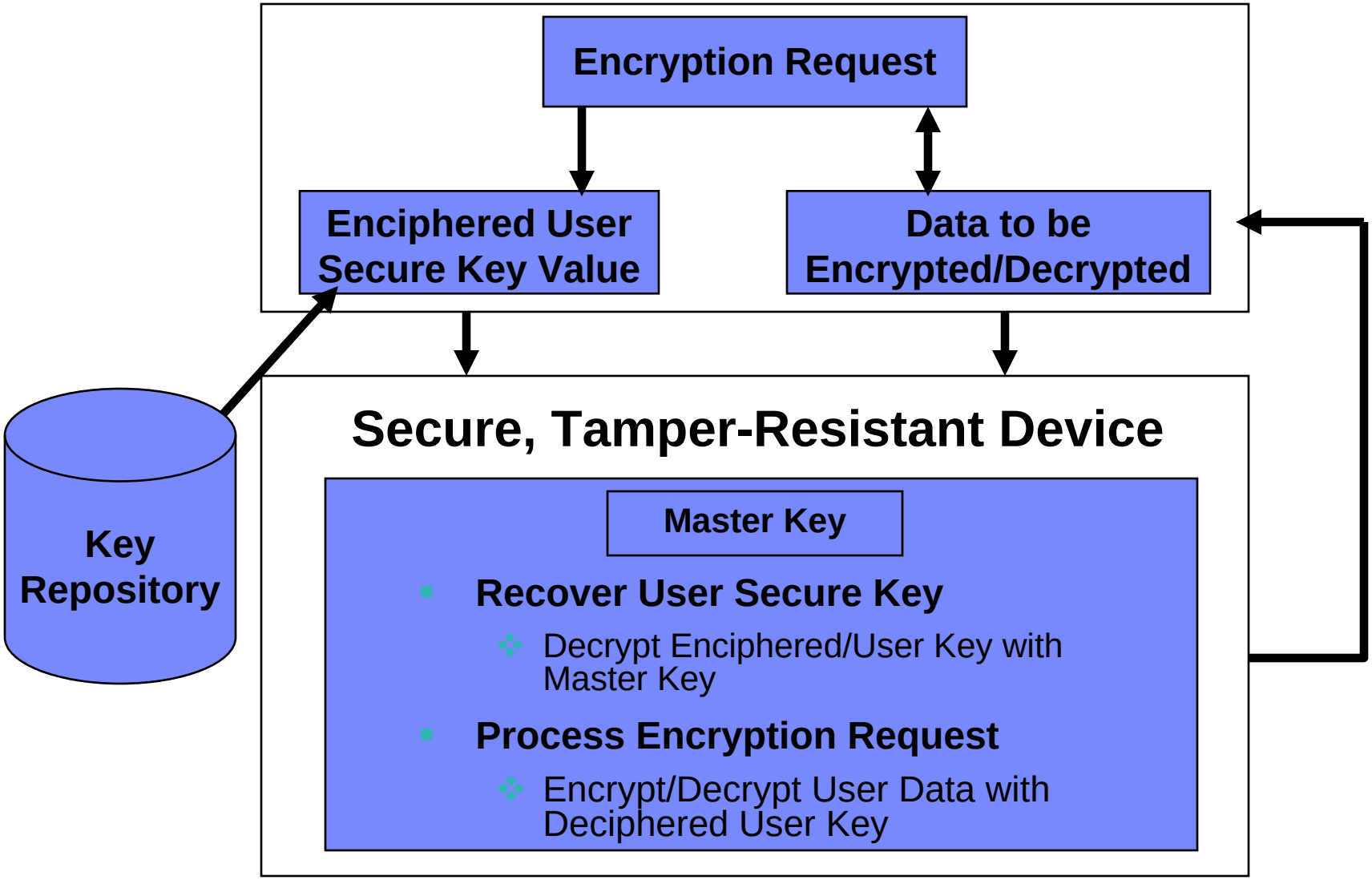
Agenda

- **Clear key / Secure key / Protected key**
- **Hardware**
  - CCF/CPACF/PCI
  - Usage Domains
  - Implications of Different Architectures
- **How are you (What products are) using the crypto infrastructure?**
- **Restoring the DR environment**
  - Encrypting tape drives
  - Encryption Facility
  - Master Keys
- **TKE**

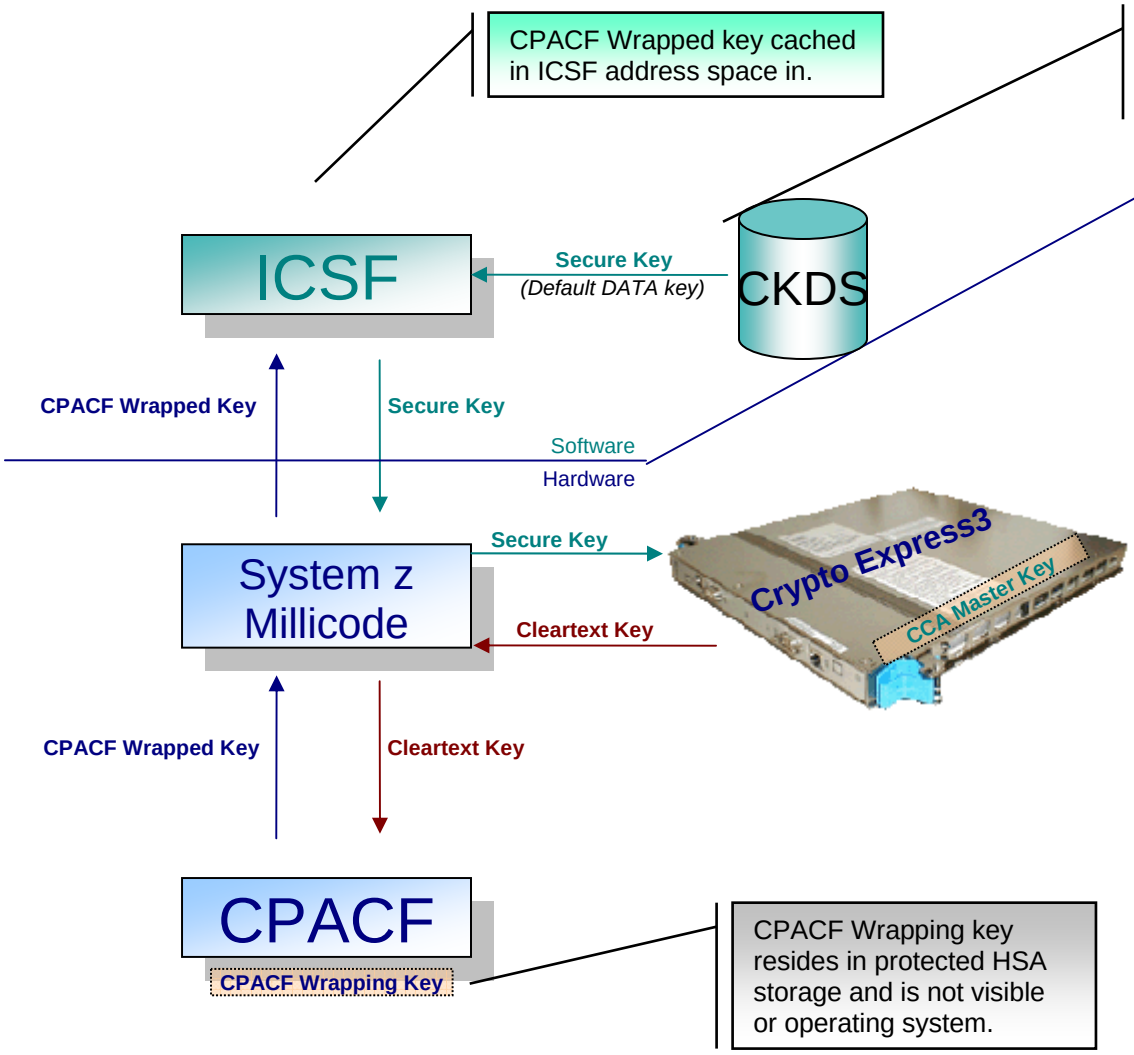
Clear Key Processing



Secure Key Processing



CPACF Protected Key - Key Wrapping



- **Create a key 'ABCD', store as secure key (i.e. encrypted under Master Key, MK)**
  - E_{MK}(x'ABCD') => x'4A!2'
- **Execute CSNBSYE (clear key API) with that key and text to be encrypted of 'MY MSG '**
- **ICSF will pass key value x'4A!2' to CEX3, recover original key value, then wrap it using wrapping key**
  - D_{MK}(x' 4A!2') => x' ABCD'
  - E_{WK}(x'ABCD') => x'*94E'
- **ICSF will pass wrapped key value to CPACF, along with message to be encrypted**
- **In CPACF, unwrap key and perform encryption**
  - D_{wk}(x' *94E') => x' ABCD'
  - $E_{x'ABCD'}$('MY MSG ') => ciphertext of x' 81FF18019717D183'

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**

TechDoc WP100647 – A Clear Key / Secure Key / Protected Key Primer

System z Clear Key Cryptographic Hardware – z890/z990, **z9 (EC & BC),** z10 (EC (GA3) & BC (GA2)), z196/z114

- **CP Assist for Cryptographic Function (CPACF)**
  - DES (56-, 112-, 168-bit), **new chaining options**
  - **AES (128-, -192, 256-bit), new chaining options**
  - SHA-1, **SHA-256, SHA-512 (SHA-2)**
  - **PRNG**
  - **Protected Key**

TechDoc WP100810 – A Synopsis of System z Crypto Hardware

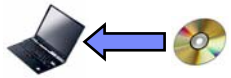
System z Secure Key Crypto Hardware

PCIXCC/PCICA

Crypto Express2 (CEX2) / Crypto Express2-1P (CEX2-1P)

Crypto Express3 (CEX3) / Crypto Express3-1P (CEX3-1P)

- **Secure Key DES/TDES**
- ***Secure Key AES***
- ***Financial (PIN) Functions*****
- ***Key Generate/Key Management*****
- ***Random Number Generate / Generate Long***
- ***SSL Handshakes (2048-, 4096- bit keys)***
- ***Protected Key Support***
- ***ECC*** ***(z196/z114 only)***



TechDoc WP100810 – A Synopsis of System z Crypto Hardware

***** Add'l functionality on later machines***

Must Production Hardware = DR Hardware?

- **Platform**
  - Microcode installed
  - LPAR Activation Profilez
  - z/OS Toleration Support
  - ICSF Version
  - Native instructions

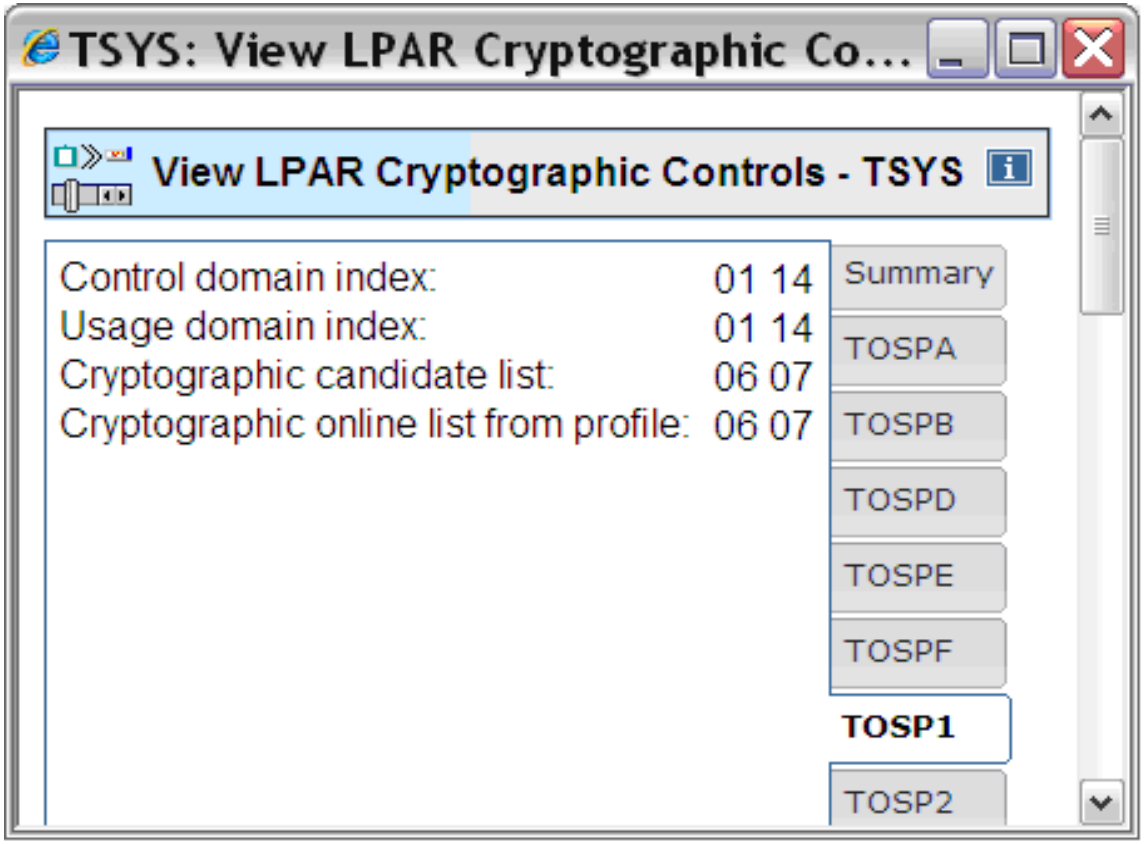
?=?

- **Crypto Function**
  - Equivalent Function
  - Crypto Products/Apps that can adapt
    - System SSL – the App that Adapts!
  - Performance Expectations

Secure key on production site will require secure key HW at DR site

Clear key on production site may require clear key HW at DR site

LPAR Activation Profile

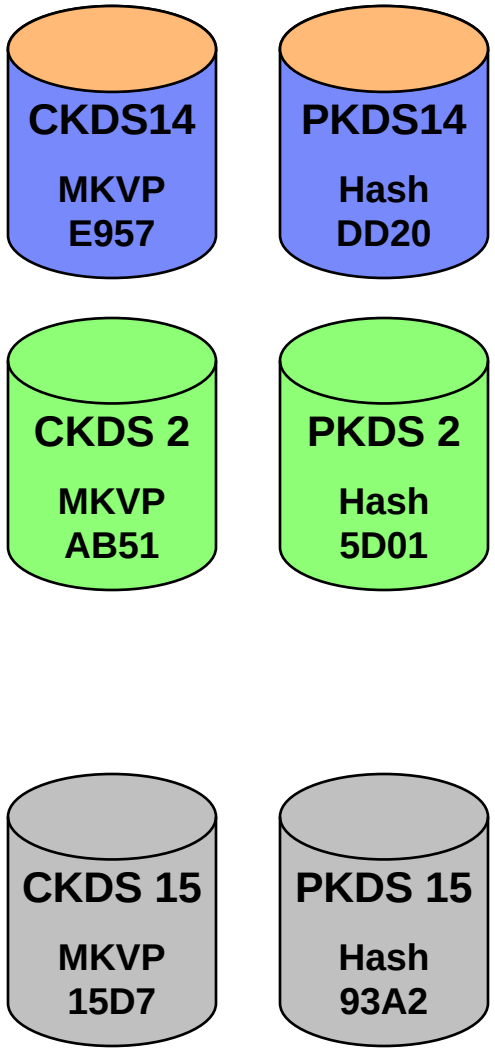


- **From CPC Operational Customization, click on View LPAR Cryptographic Controls**

Usage Domains

Options => DOMAIN=n

LPAR & Domain	DES Master Key	PKA Master Key	AES MK	ECC MK
LP1 UD1	ABC (MKVP=E957)	XYZ (Hash=DD20)	…	…
LP2 UD2	LP2KEY (MKVP=AB51)	PKAMST (Hash=5D01)	…	…
LP3				
LP4 UD4	ABC (MKVP=E957)	XYZ (Hash=DD20)	…	…
LP5				
…				
LP15 UD9	LP15KY (MKVP=15D7)	AKEY (MKVP=93A2)	…	…



Crypto Support in the VM Directory

- **CRYPTO – authorizes guest machine to use crypto**
  - APVIRTual – provides access to clear key devices (PCICA, CEX2A, CEX3A) – for Linux and VSE Guests
  - APDEDicated ap, ap … – assigns specific secure key devices
  - DOMAIN n – assigns a domain(s) to the guest
  - *CSU 0,1,* – assigns zero, one or both CCFs*
  - *KEYENTRY – PCCF functions*
  - *SPECIAL – Enable Special Secure Mode*
  - *MODIFY – provides access to a TKE from this guest*
- **OPTION CRYMeasure – authorizes access to crypto measurement data on the crypto hardware**

System Keys – Where was the CKDS Initialized?

- **CKDS System keys are not required in a PCIXCC/CEX2C environment**
  - NOCV-enablement keys
  - ANSI System keys
  - Extended System keys (ESYS)

IDCAMS => PRINT INDATASET('ckds dsn') COUNT(20)

TechDoc PRS1953 – Utility to allow migration from a CPACF/PCI based CKDS back to a CCF (9672/z800/z900) system

Where was the PKDS Initiailized?

- **CCF => Signature Master Key (SMK) & Key Management Master Key (KMMK)**
- **PCICC/PCIXCC/CEX2C => Asymmetric Master Key (ASYM-MK)**

The PKDS Header Record contains the hash pattern of the KMMK at +108 and the hash pattern of the SMK at +124

See ICSF Admin Guide 'Steps for setting the SMK equal to the KMMK'

Consider your crypto users

- **DB2 BIF**
- **Data Encryption Tool for IMS and DB2**
- **System SSL**
- **Encryption Facility**
- **Encryption Key Manager (EKM)**
- **OEM products**
- **Applications**

TEST!

Master Keys on the DR System

- **Hot-site (DASD mirroring)**
  - CKDS/PKDS are mirrored, master key changes are made on the production system and DR system
- **Warm/Cold-site (Tapes restored)**
  - System Volumes Encrypted - If the keys are stored on the z/OS system, then the driver system that restores the tapes, must have access to those keys
  - Application Data Encrypted – DR system may be used to recover data

Recovering Master Keys

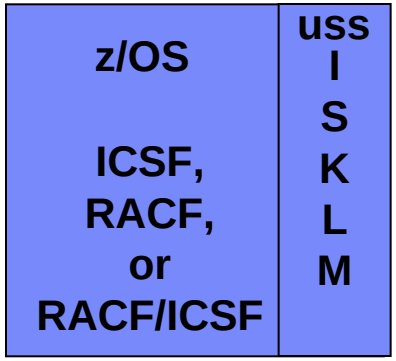
- **Master Keys**
  - Passphrase Initialization, PPINIT (Master Key Only)
  - ISPF Panels for ICSF (Master Key Only)
  - Trusted Key Entry Workstation

- **Master keys are installed into secure hardware**
  - Once loaded, no way to retrieve them!
  - Master keys must be available to the DR hardware

- **Use the MKVP (SYM-MK/CKDS) and the Hash Pattern (ASYM-MK/PKDS) to ensure you're loading the right keys**
- **Weak keys cannot be loaded in a PCICC/PCIXCC/CEX2C (see the Admin Guide)**

Restoring the DR environment – Encrypted Tape Drives

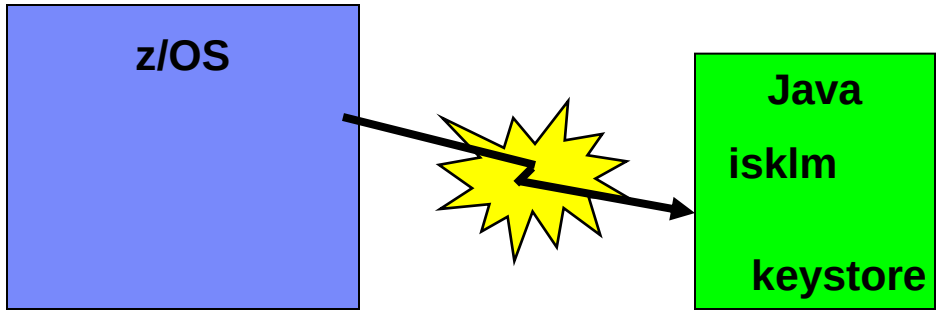
- **If your backups are encrypted – where is your key repository?**
  - IBM Security Key LifeCycle Manager (ISKLM) under Unix System Services (USS) and key repository using RACF, or ICSF or RACF and ICSF
    - Plus – key security provided by RACF, ICSF and secure key hardware
    - Minus – must make the RSA keys available on the driver system, where the tapes are restored



If the RSA keys are stored in ICSF, then the PKDS must be available to the driver system, which means the driver system must have secure hardware and the associated ASYM-MK must be loaded

Restoring Tapes – Encrypted Tape Drives (cont.)

- **If your backups are encrypted – where is your key repository?**
  - ISKLM on a remote system (z/OS or not)
    - Plus – driver system can connect to the production ISKLM and key repository
    - Minus – key protection provided by the non-z/OS platform



Restoring tapes – Encryption Facility

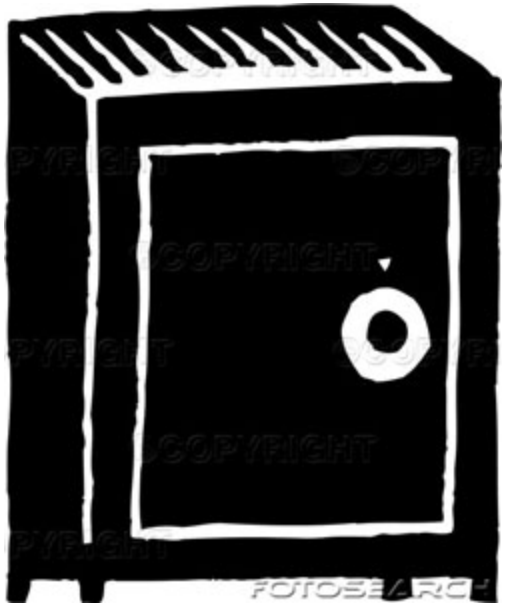
- **Password option – the password must be provided to the restore job on the driver system**
- **RSA Option – RSA keys in the PKDS must be available on the driver system, along with the ASYM-MK that is associated with that PKDS**

AND

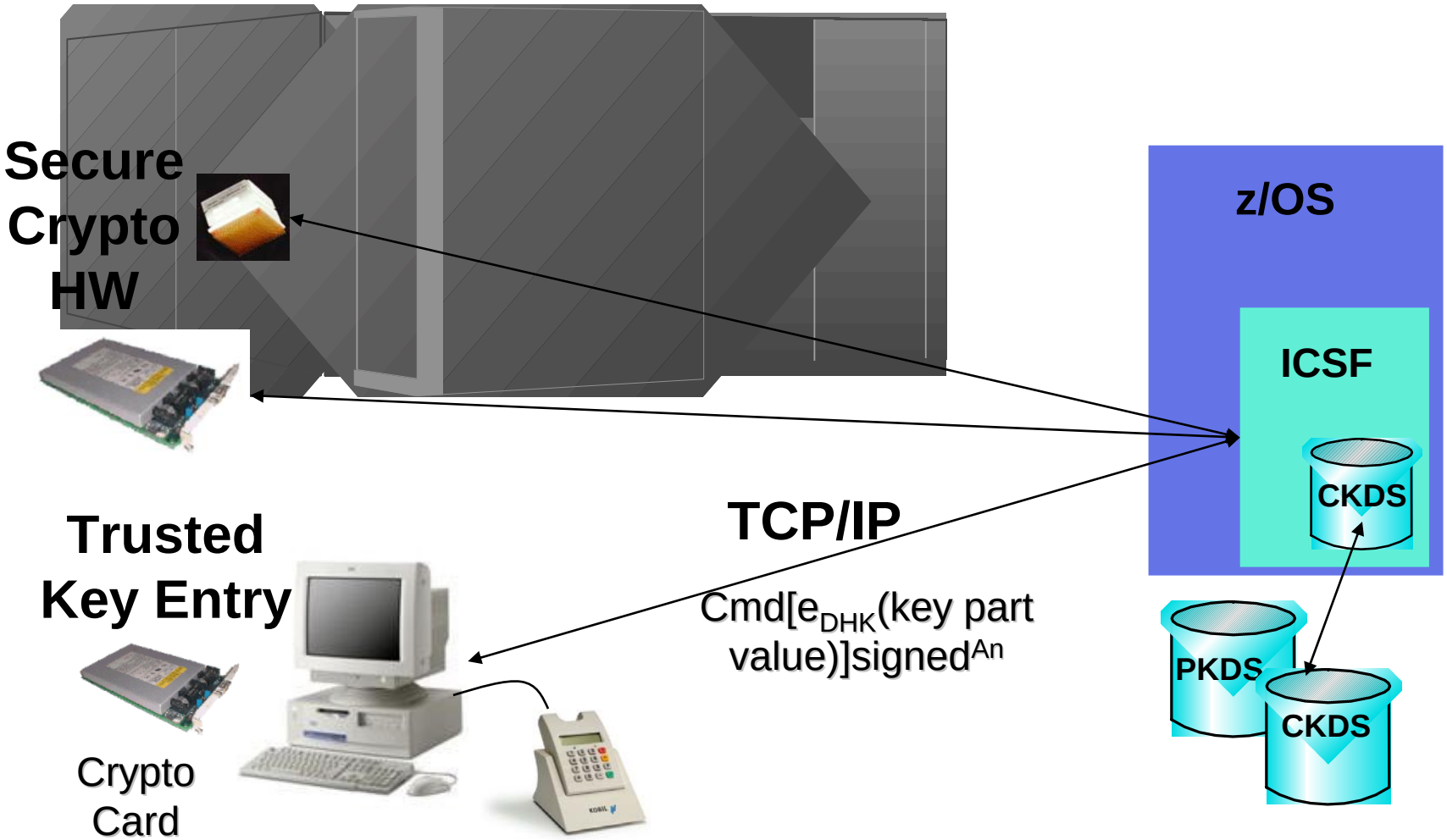
- **Specific hardware may be required**
  - microcode must be installed
  - CLRAES – potential performance issues if the driver system doesn't provide AES hardware
  - ENCTDES – driver system must have secure hardware
  - RSA Keys > 1048-bits in length require PCICC, PCIXCC or CEX2C

Restoring tapes – OEM Products

- **Where is the key repository?** If it uses the CKDS or PKDS, then the CKDS and/or PKDS must be available on the driver system



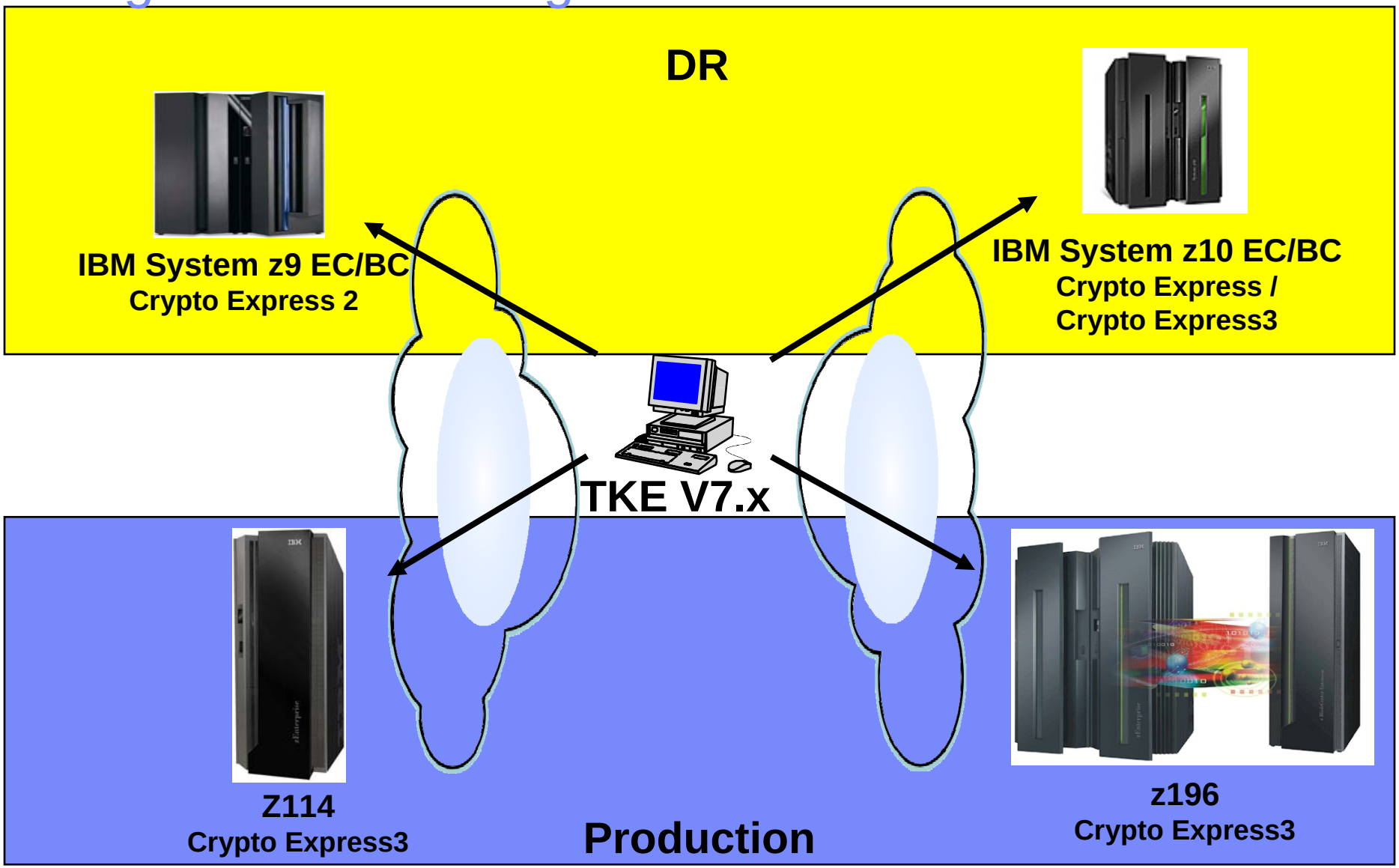
TKE – Trusted Key Entry Workstation



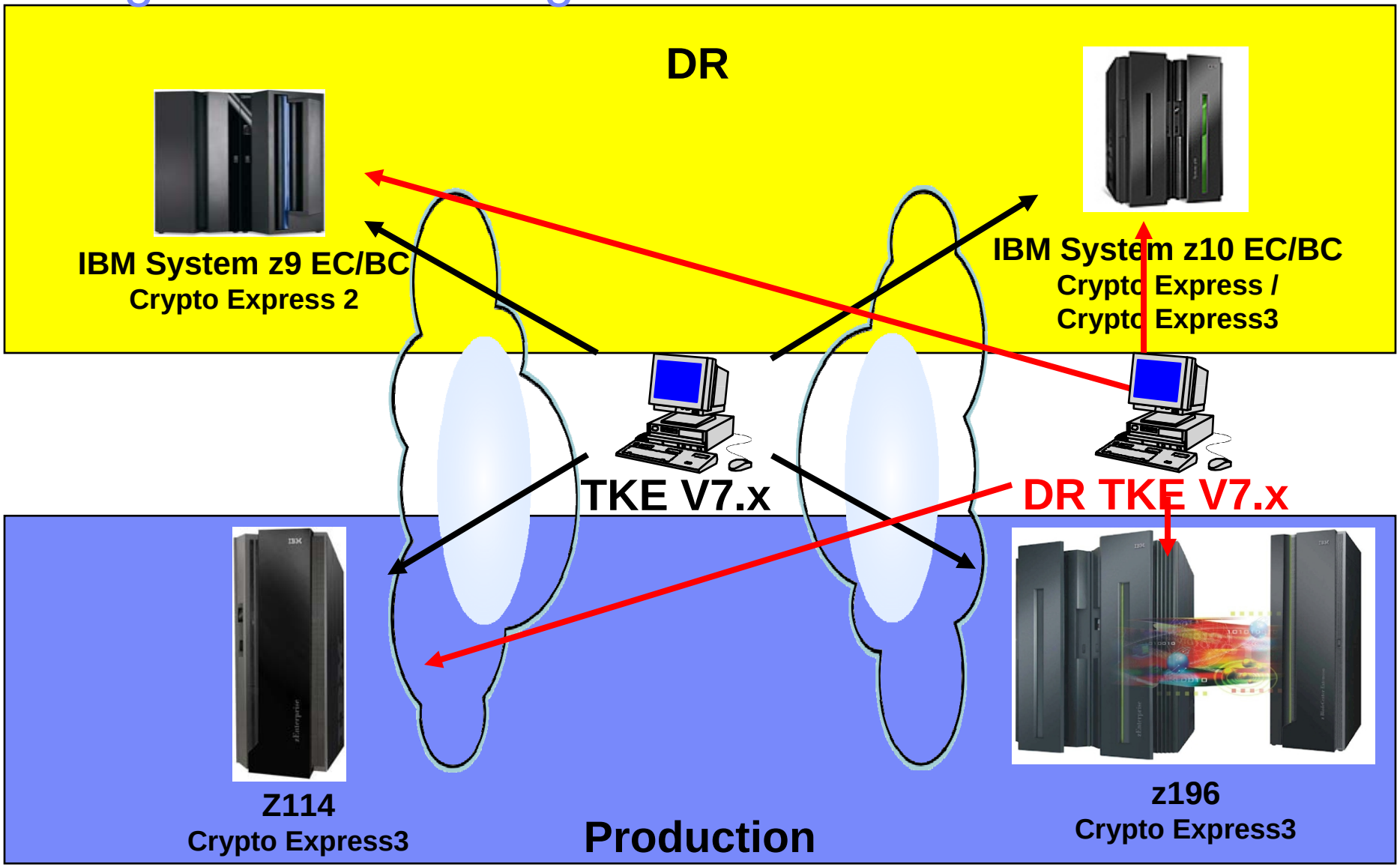
TKE Configuration for Backup and Recovery

- **TKE Workstation Crypto Adapter**
  - Profiles
  - Roles
- **Host Crypto Adapter**
  - User/Authority
  - Roles

Using a TKE to manage the DR site



Using a TKE to manage the DR site



TKE Migration Wizard

Wizard is the implementation of a

secure protocol

for collecting, saving, and installing data

from one cryptographic adapter to another.

Data includes Key Material!

TKE Backup/Recovery for Host Files

- **TKECM – Crypto Module Data set defined to the Host Transaction Program**
  - Contains info about TKE application windows
  - Crypto module notebooks (descriptions, domain descriptions, authority information)
  - Backup for recovery purposes, but may need to be recreated at a DR site if the crypto modules and configuration are not identical
- **Host Configuration – IP Addresses configured properly**

TKE Backup/Recovery for Workstation Files

- **Backup Critical Console Data**
  - intended for protecting from a failed harddrive, applicable for DR **IF** the TKEs are identical
- **Backup Utility (TKE Prior to V5)**
- **TKE File Management Utility (TKE V5 and later)**

Workstation Files

- **host.dat – definitions for host sessions and related data, includes CMID and public modulus for each crypto module**
- **group.dat – group definitions**
- ***.rol & *.pro – smart card and passphrase roles and profiles**
  - Changes to the defaults and
  - New ones, unique to the customer
- **desstore.dat & desstore.NDX**
- **pkastore.dat & pkastore.NDX**

TKE Backup/Recovery of Keys

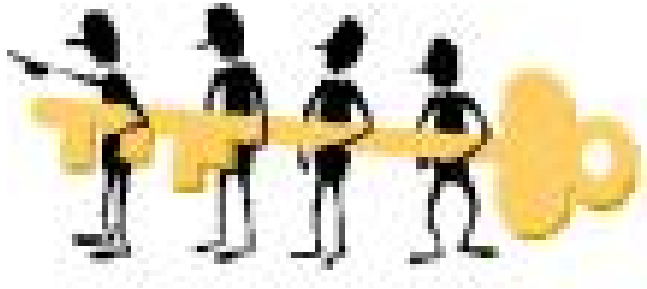
- **Keys**
  - Master Keys
  - Operational Keys
  - Signature Keys
- **Storage**
  - Smart Card
  - Floppy
  - Keystore
  - Print

One final note

- **After a DR – exercise or the real thing**
  - Clear your master keys at the DR site

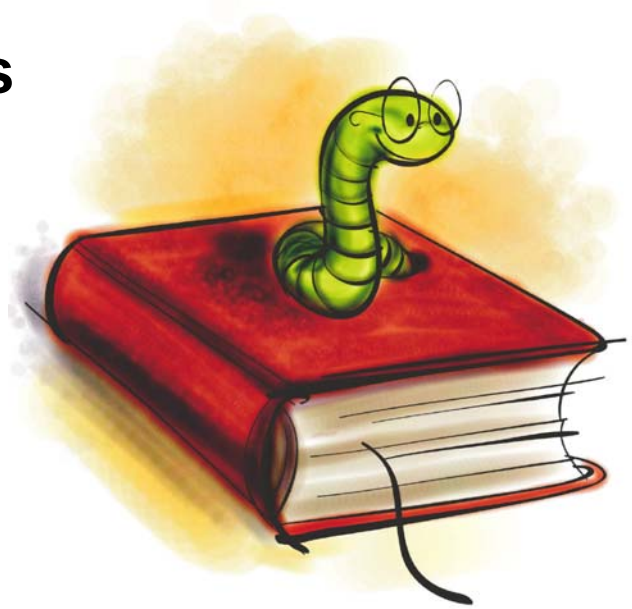
OR

- Change your master keys



IBM Pubs

- **ICSF Overview, SA22-7519**
- **ICSF Administrator's Guide, SA22-7521**
- **ICSF Application Programmer's Guide, SA22-7522**
- **ICSF System Programmer's Guide, SA22-7520**



IBM Resources (on the web)

- **ATS TechDocs Web Site www.ibm.com/support/techdocs (Search All Documents for keyword of 'Crypto')**
  - WP100647 – A Clear Key / Secure Key / Protected Key Primer
  - WP100810 – A Synopsis of Systme z Crypto Hardware
  - WP100700 – Encryption Facility for z/OS – Performance and Sizing
- **Redbooks – www.redbooks.ibm.com on 'Crypto'**
  - System z Crypto and TKE Update, SG24-7848
  - IBM zEnterprise System Technical Introduction, SG24-7832
  - IBM zEnterprise System Technical Guide, SG24-7833
  - IBM zEnterprise 196 Configuration Setup, SG24-7834
- **'How to Setup TKE for Disaster Recovery' in Hot Topics Aug. 2007 Issue 17**
  - http://publibz.boulder.ibm.com/epubs/pdf/e0z2n180.pdf

Questions?

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml: AS/400, DBE, e-business logo, ESCON, eServer, FICON, IBM, IBM Logo, iSeries, MVS, OS/390, pSeries, RS/6000, S/390, VM/ESA, VSE/ESA, Websphere, xSeries, z/OS, zSeries, z/VM

The following are trademarks or registered trademarks of other companies

Lotus, Notes, and Domino are trademarks or registered trademarks of Lotus Development Corporation
Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
LINUX is a registered trademark of Linux Torvalds
UNIX is a registered trademark of The Open Group in the United States and other countries.
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.
Intel is a registered trademark of Intel Corporation
* 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.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Any proposed use of claims in this presentation outside of the United States must be reviewed by local IBM country counsel prior to such use.

The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.