# z/OS Cryptographic Services - ICSF Best Practices

*Steven R. Hart, CISSP®*
*IBM*

*Thursday, August 7, 2014: 8:30 AM-9:30 AM*
*Session Number 15775*

#SHAREorg

Copyright (c) 2014 by SHARE Inc. Except where otherwise noted, this work is licensed under http://creativecommons.org/licenses/by-nc-sa/3.0/

SHARE in Pittsburgh 2014

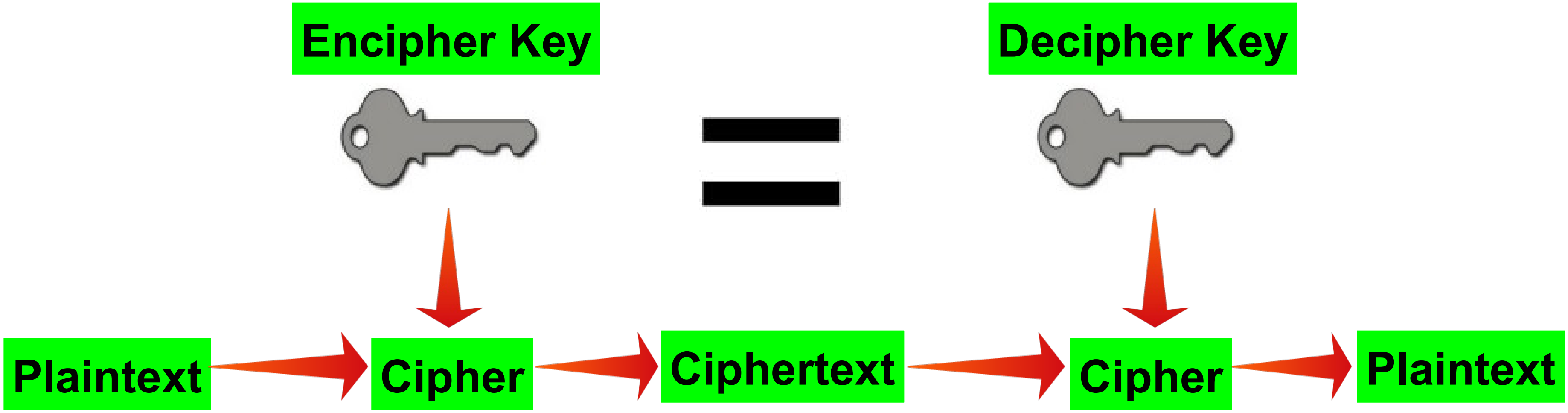
# Topics

- Cryptography Basics
- Cryptographic Hardware
- ICSF Web Deliverables
- ICSF Migration Checks
- Using RACF to Protect Crypto Keys and Services
- ICSF Health Checks
- CCA Access Control Points
- Key Store Policy
- Coordinated KDS Administration
- AP Configuration
- KDS Utilization Statistics
- ICSF Options
- Cryptographic Key Management
- System z Security Portal

# Cryptography

- A set of techniques for scrambling data in such a way that it is only decipherable to authorized entities.
- Cryptography is used to provide the following services:
  - Confidentiality – protecting data from disclosure to unauthorized parties
  - Integrity – protecting data from being modified by unauthorized parties
  - Authentication – confirming the identity of an entity
  - Non-repudiation – provides proof of the origin of data

# Symmetric Cryptography



Encipher Key

=

Decipher Key

Plaintext

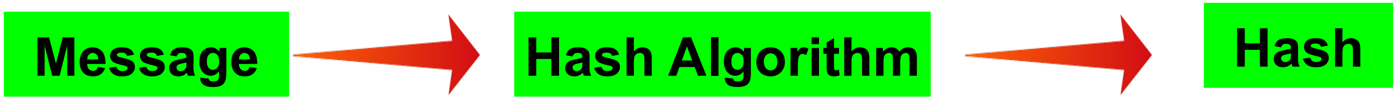
Cipher

Ciphertext

Cipher

Plaintext

# Hash Functions

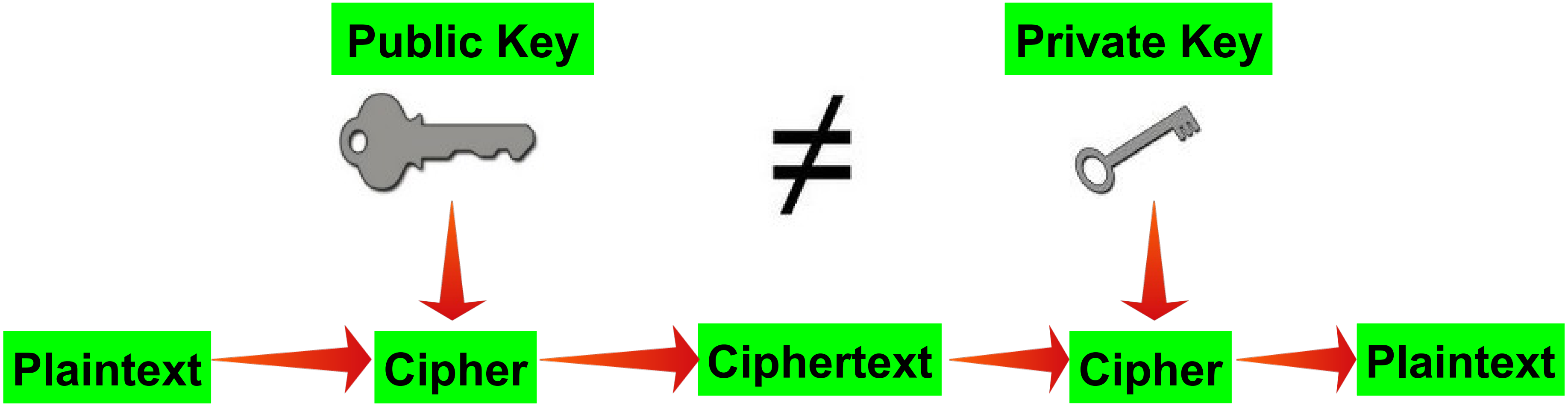


Message

Hash Algorithm

Hash

# Asymmetric Cryptography



Public Key

≠

Private Key

Plaintext

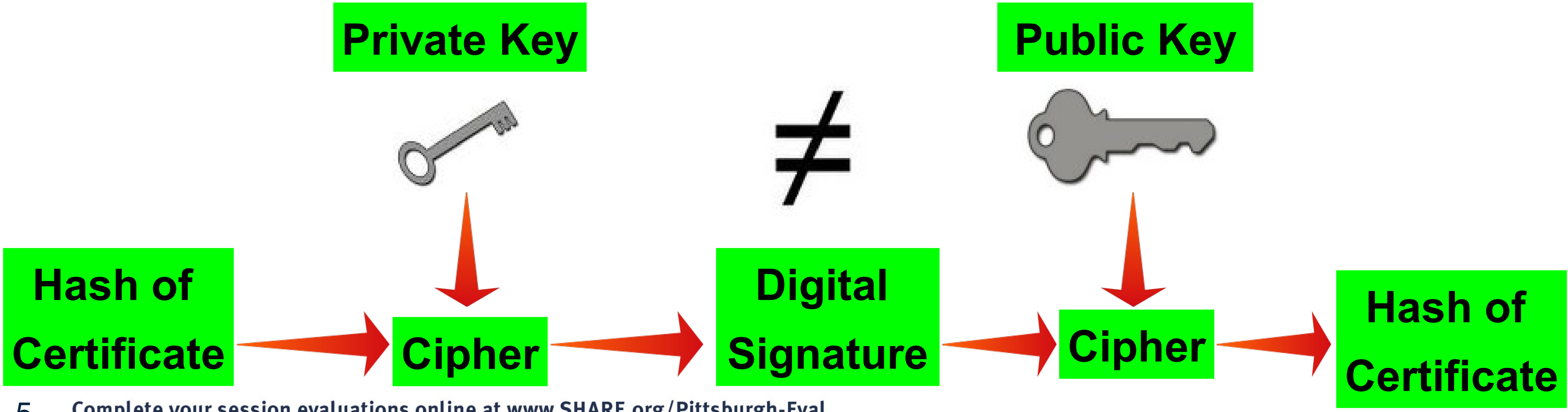
Cipher

Ciphertext

Cipher

Plaintext

# Digital Certificates and Digital Signatures



Private Key

≠

Public Key

Hash of Certificate

Cipher

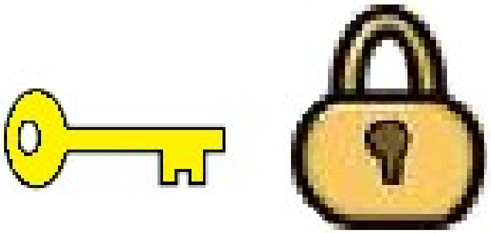
Digital Signature

Cipher

Hash of Certificate

# ICSF

- Integrated Cryptographic Service Facility (ICSF)
- ICSF is a base element of z/OS that provides cryptographic services
- Provides an application programmers interface (API) for applications that need to perform crypto
- Provides basic key management for cryptographic key material
- Provides access to hardware Cryptographic Coprocessors, Cryptographic Accelerators and CP Assist for Cryptographic Function (CPACF)



# ICSF provides a callable interface to perform these tasks:

- Encryption and Decryption of Data
- Key generation and distribution
- Personal Identification Numbers (PINs)
- Message Authentication Codes (MACs)
- Hashing algorithms
- Digital signatures
- Card-verification values
- Translation of data an PINs in networks
- Secure Electronic Transaction
- Secure Sockets Layer
- EMV integrated circuit card specifications
- ATM remote key loading
- PKCS #11

# Cryptographic Coprocessors

- ICSF uses PCIe Cryptographic Coprocessors to perform hardware crypto functions
- These cards provide a high-security, high-throughput cryptographic subsystem.
- The hardware security modules are validated to FIPS 140-2, Overall Level 4 (highest level of security).
- They are tamper responding,

  programmable, cryptographic PCIe cards,

  containing CPU, encryption hardware,

  RAM, persistent memory, a hardware random

  number generator, time of day clock,

  and infrastructure firmware.

# Cryptographic Coprocessors

- New CEX4S Cards can be in three configuration modes
  - Accelerator Mode: Supports RSA clear key and SSL acceleration
  - Coprocessor Mode: IBM Common Cryptographic Architecture
  - Enterprise PKCS#11 (EP11) Mode: PKCS#11 programming interface
- The firmware running in the coprocessor can be customized to meet special requirements
- Custom firmware loads are called User Defined Extensions (UDXs)
- Several algorithms are supported in hardware:
  - DES/TDES w DES/TDES MAC/CMAC
  - AES, AESKW, AES GMAC, AES GCM, AES XTS mode, CMAC
  - MD5, SHA-1, SHA-2 (224,256,384,512), HMAC
  - RSA (512, 1024, 2048, 4096)
  - Montgomery Modular Math Engine
  - RNG (Random Number Generator)
  - Clear Key Fast Path (Symmetric and Asymmetric)

# Cryptographic Accelerators

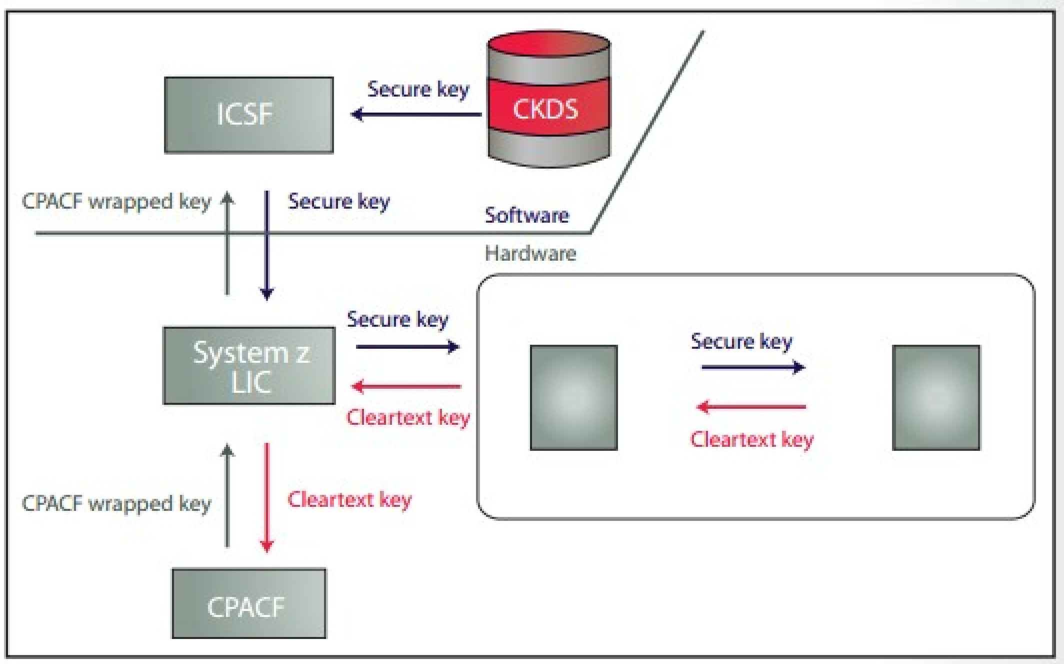
- High performance RSA asymmetric algorithms
- Designed for maximum Secure Socket Layer (SSL) acceleration rather than for specialized financial applications and secure key processing
- Can support over 2000 SSL handshakes per second
- Previously shipped as a separate hardware feature
- Cryptographic Coprocessors can now be configured to become Cryptographic Accelerators

# CP Assist for Cryptographic Function (CPACF)

- Encryption accelerator functionality is provided on a quad-core chip, which is designed to provide the following high-speed cryptography functions:
  - Data Encryption Standard (DES) 56-bit key
  - Triple Data Encryption Standard (TDES) 168-bit keys
  - Advance Encryption Standard (AES) for 128-bit, 192 and 256 bit keys
  - Secure Hash Algorithm (SHA) SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512
  - Pseudo Random Number Generation (PRNG)
  - Protected Key Support

# Secure Key, Clear Key and Protected Key

- Secure Key - provides high security because the key material is protected by the master key within the cryptographic coprocessor and never appears in the clear
- Clear Key - uses the CPACF to provide high performance, however the key material is clear and does appear in application storage and within the keystore
- Protected Key - provides a high performance and high security solution by taking advantage of the high speed CPACF while utilizing keys protected by the cryptographic coprocessor's Master Key



# ICSF Web Deliverables

- As new cryptographic hardware becomes available, ICSF is updated and new functions are delivered via web deliverables outside of the z/OS release cycle
- Web deliverables along with their associated ICSF release publications are available on the z/OS downloads website:
  - http://www.ibm.com/systems/z/os/zos/downloads
- Each new release of z/OS contains a version of ICSF incorporated into its base, however this may not be the latest and greatest level of ICSF
- Check the z/OS downloads website for the latest level of ICSF
- It is recommended to run with the latest level of ICSF to ensure you have all of the latest and greatest features

# In service levels of ICSF

- Cryptographic Support for z/OS V1R9-V1R11 (HCR7770)
  - GA - Nov. 2009
  - Base of z/OS V1.12 – Sept. 2010
  - Highlights – Protected Key CPACF, Crypto Express3, Extended PKCS #11, Elliptic Curve
  - Planned EOS - Sept. 2014
- Cryptographic Support for z/OS V1R10-V1R12 (HCR7780)
  - GA - Sept. 2010
  - Base of z/OS V1.13 – Sept. 2011
  - Highlights – z196 MSA-4 Instructions, CCA Elliptic Curve, ANSI X9.8 & 9.24, HMAC, 64-bit API's, PCI audit logging, CKDS constraint relief
  - Planned EOS - Sept. 2016

# In service levels of ICSF - continued

- Cryptographic Support for z/OS V1R11-V1R13 (HCR7790)
  - GA - Sept. 2011
  - Orphan Release, not in any z/OS base, Web Deliverable only
  - Highlights – Coordinated KDS Administration, Expanded AES CCA support, Enhanced ANSI TR-31, PIN Block dec. table protection, PKA RSA OAEP with SHA-256, Additional ECC functions
  - Planned EOS - Sept. 2016
- Cryptographic Support for z/OS V1R12-V1R13 (HCR77A0)
  - GA - Sept. 2012
  - Base of z/OS V2.1 – Sept. 2013
  - Highlights – CEX4S, EP11, KDS Administration support for PKDS/TKDS, I/O Performance improvements, 24-byte DES MK, Weak key wrapping controls, DUKPT for MAC and Enc keys, FIPS RNG and Cache, Secure Cipher Text Translate, EMV Enhancements
  - Planned EOS Sept. - 2018

# ICSF FMID HCR77A1

- Cryptographic support for z/OS V1R13-V2R1
  - Latest and Greatest Web Deliverable
  - HCR77A0 is in the base of z/OS V2R1
  - GA September 20, 2013
  - Planned EOS Sept. - 2018

# ICSF FMID HCR77A1 – Refresher

## *Hardware Support*

- CCA 4.4 Items:
  - Expanded EMV (EuroPay, MasterCard, Visa) Support
  - Unique Key Derive IPEK Support
  - DESUSECV Support
  - Fixed-Length Payload section for variable-length symmetric key tokens
  - User Defined Extension (UDX) Reduction and Simplification
  - Remote Key Export (RKX) Enhanced Key Wrapping
  - DK AES PIN Support (HCR77A0 and above)

- EP11 Items:
  - Enterprise PKCS #11 Phase 2

- TKE
  - RSA Master Key Set from TKE

# ICSF FMID HCR77A1 – Refresher…

***Software Only Functions:***

- AES MAC Enhancement
- SAF ACEE Selection
- One Way Hash (OWH) and Random Number Generation (RNG) optional SAF checking
- Dynamic Special Secure Mode (SSM)
- AP Configuration Simplification
- Improved ICSF CTRACE Support
- CCF Removal
- KDS Key Utilization Statistics
- New CSFIQF Service (HCR77A0 and above)
- ICSF HCR77A1 Migration Checks

# ICSF HCR77A1 Migration Checks

- The following new migration checks are for users of ICSF FMIDs HCR77A0 and earlier releases who are migrating to FMID HCR77A1 or newer releases of ICSF (APAR OA42011)
  - ICSFMIG77A1_COPROCESSOR_ACTIVE
  - ICSFMIG77A1_UNSUPPORTED_HW
  - ICSFMIG77A1_TKDS_OBJECT

# ICSFMIG77A1_COPROCESSOR_ACTIVE

- The activation of CCA cryptographic coprocessors has changed for HCR77A1 and newer.
- This migration check detects CCA cryptographic coprocessors with master keys that don't match the CKDS and PKDS.
- A coprocessor that has master keys that don't match the CKDS and PKDS will not become active when ICSF FMID HCR77A1 is started.
- This migration check will indicate which coprocessors will not become active when HCR77A1 is started.

# ICSFMIG77A1_UNSUPPORTED_HW

- The HCR77A1 release does not support IBM Eserver zSeries 800 and 900 systems.
- This migration check will indicate if your system is supported or not by HCR77A1 and newer releases.
- Available via APAR OA42011 back to HCR7770.

# ICSFMIG77A1_TKDS_OBJECT

- In the HCR77A1 release, ICSF introduced a common key data set record format for CCA key tokens and PKCS #11 tokens and objects. This new format adds new fields for key utilization and metadata. Because of the size of the new fields, some existing PKCS #11 objects in the TKDS may cause ICSF to fail to start.
- The problem exists for TKDS object records with large objects. The 'User data' field in the existing record can not be stored in the new record format if the object size is greater that 32,520 bytes. The TKDSREC_LEN field in the record has the size of the object. If the 'User data' field is not empty and the size of the object is greater than 32,520 bytes, the TKDS can not be loaded.

# ICSFMIG77A1_TKDS_OBJECT

- This migration check will detect any TKDS object that is too large to allow the TKDS to be loaded when ICSF is started.
- The problem can be corrected by:
  - Modifying the attributes of the object to make it smaller, if possible.
  - Removing the information in the 'User data' field of the object. The 'User data' field must be all zeros for it to be ignored.
  - Copying the object using PKCS #11 services and deleting the old object.
  - Deleting the object.

# Using RACF to Protect Keys and Services

- RACF can be used to protect and audit the use of ICSF keys and services
- The CSFKEYS class controls access to cryptographic keys in the CKDS and PKDS
- Create profiles based on CKDS and PKDS key labels
- The CSFSERV class controls access to ICSF services and ICSF TSO panel utilities
- The XCSFKEY class is used to control the transfer of secure AES and DES keys from encryption under the MK to encryption under an RSA key
  - This is used for authorization checking of the Symmetric Key Export service
- The CRYPTOZ class controls access to, and defines a policy for PKCS #11 tokens which are used by ICSF's PKCS #11 callable services.
- Recommendation: Make sure that access is granted only to the processes and people who need access.

# z/OS ICSF Health Checks (z/OS V1R12 and above)

- z/OS Health Checker is an element of z/OS that provides a common platform for monitoring system operation and implementation of IBM best practices
- New health checks will be available to ensure ICSF services and managed key material are sufficiently protected
  - RACF_CSFSERV_ACTIVE - to verify that the ICSF CSFSERV class is active
  - RACF_CSFKEYS_ACTIVE - to verify that the ICSF CSFKEYS class is active
- The existing RACF_SENSITIVE_RESOURCES check has been updated to report on the status of the ICSF CKDS, PKDS, and TKDS data sets
  - performs the same checking on the ICSF dataset as is performed on all of the other datasets in RACF_SENSITIVE_RESOURCES. **The maximum allowed "general" access (UACC) is NONE.**
  - indicates if ICSF has been started on the system

# CCA Access Control Points

- Access to services that are executed on the CCA coprocessor is through Access Control Points in the ICSF Role.
- To execute services on the coprocessor, access control points must be enabled for each service in the ICSF Role.
- The TKE workstation allows you to enable or disable access control points.
- For systems that do not use the optional TKE Workstation, most access control points (current and new) are enabled in the ICSF Role with the appropriate licensed internal code on the coprocessor.
- See the table in the ICSF Admin Guide for a list of access control points and the default setting of each access control point.
- New TKE users and non-TKE users have the default set of access control points enabled.
- Existing TKE users who have changed the setting of any access control point, any new access control points will not be enabled.
- Recommendation: Only enable ACPs for callable services you use.

# Key Store Policy

- Key Store Policy allows you to control how encrypted key tokens defined in the CKDS and PKDS can be accessed and used.
- Key Store Policy is defined using resource profiles in the XFACILIT class
- Key Store Policy controls allows you to:
  - verify that a user has authority to a secure token when passed to a callable service
  - prevent duplicate tokens in the CKDS and PKDS
  - raise the level of access authority required to create, write, and delete key labels
  - raise the level of access authority required to export a token using the Symmetric Key Export callable service
  - set additional restrictions on how keys can be used

# One Way Hash (OWH) and Random Number Generation (RNG) Access

- CSFSERV SAF checks for OWH and RNG contribute to significant CPU consumption.
- Two new resources were added to the XFACILIT SAF resource class for disabling OWH and RNG SAF checking:

```
CSF.CSFSERV.AUTH.CSFOWH.DISABLE
CSF.CSFSERV.AUTH.CSFRNG.DISABLE
```

# Dynamic Special Secure Mode (SSM)

- Configuring the SSM options data set setting requires an ICSF restart.
- The XFACILIT SAF resource class contains a new resource for dynamically enabling SSM.

CSF.SSM.ENABLE

# IQF Access (HCR77A0 and above)

- CSFIQF is protected by the CSFSERV class because it can call the cryptographic coprocessors.
- CSFIQF2 is a new service that is not SAF protected and does not make calls to cryptographic coprocessors.
- CSFIQF2 returns information from internal ICSF control blocks about which cryptographic hardware is available, the available algorithms, and FIPS mode.

# Coordinated KDS Administration

- In HCR7790, the coordinated KDS administration callable service, CSFCRC, introduced the coordinated CKDS refresh and coordinated CKDS change-mk functions.  In HCR77A0, this callable service has been extended to provide coordinated PKDS refresh, coordinated PKDS change-mk and coordinated TKDS change-mk.

- When used for coordinated change-mk, applications may run KDS update workloads in parallel, and ICSF guarantees that any dynamic updates will be reflected in the target data set.

- For coordinated refresh (CKDS and PKDS only) it is recommended to disable KDS update workloads when refreshing to a target data set that is different from the currently active KDS. Updates occurring to the current active KDS would not be guaranteed to be reflected in the target data set.  ICSF does not enforce that dynamic KDS updates be manually disabled prior to coordinated refresh, and will itself internally suspend such updates until the coordinated refresh operation completes.

- Dynamic KDS updates occurring during a coordinated refresh in place are guaranteed to be accounted in the resulting in-storage KDS when the operation completes.

# Coordinated KDS Administration continued

- In a sysplex environment, the coordinated operations are invoked from a single ICSF instance and processed across all members sharing the same active KDS (sysplex cluster).
- The callable service name for AMODE(64) invocation is CSFCRC6.
- The CRC service may be called from ICSF dialogs.
- This service can be protected with RACF.
- This support additionally includes a new sysplex communication protocol that provides better performance and servicability characteristics.

# AP Configuration Simplification

- Cryptographic Coprocessors are configured online with the Support Element (SE) and then activated on the ICSF Cryptographic Coprocessor Management Panel.
- Cryptographic Coprocessors are reconfigured by deactivating them on the ICSF Cryptographic Coprocessor Management Panel and then configured offline using the SE.
- Prior releases of ICSF may have difficulty communicating with Cryptographic Coprocessors when these steps are not followed in order.
- ICSF's adjust processor (AP) configuration logic has been redesign to improve handling of SE signals when Cryptographic Corprocessors are added, removed, and reconfigured.
- Please still follow the documented process.

# KDS Key Utilization Statistics

- Provides a new key record format (KDSR) for internally saving meta-data and statistics about each cryptographic key.
- The Coordination KDS Administration (CSFCRC and CSFCRC6) callable service has be enhanced to perform a coordinated conversion of an old format *KDS to the new KDSR format.
- Included in this new record format is a section used to track the "last referenced" date for each cryptographic key.

# KDS Key Utilization Statistics

- The reference date is the last time a record was used in a cryptographic operation or read, such that the retrieved key may have been used in a cryptographic operation.  The read is interpreted as a show of interest, so the reference date is updated.
- A new ICSF startup option, KDSREFDAYS(n), has been added that specifies (in days) how often a record should be written for a reference date/time change.
- KDSREFDAYS(0) means that ICSF will not keep track of key reference dates. The default is KDSREFDAYS(1). The maximum value allowed is KDSREFDAYS(30).

# ICSF Options

- HDRDATE(YES or NO) - Indications whether or not an installation should update the data set header record timestamp information when performing CKDS, PKDS, and TKDS I/O update operations.
- KEYAUTH(YES/NO) – check key integrity in memory, this option has been deprecated
- CKTAUTH(YES/NO) – check key integrity on DASD, this option has been deprecated
- CHECKAUTH(YES/NO) – skip SAF checks for Supervisor State or System Key callers
- SYSPLEXCKDS / SYSPLEXPKDS / SYSPLEXTKDS – enables ICSF sysplex support

# Cryptographic Key Management

- ICSF Key Management Services
- ICSF KGUP Utility – remember to refresh your KDS
- PKI (Public Key Infrastructure) - certificate authority, digital certificate hosting and management.
- TKE (Trusted Key Entry) as a secure environment to manage crypto hardware and host master keys.
- Enterprise Key Management Foundation (EKMF) - a centralized key management system to manage key material through their entire life-cycle for cryptographic devices (e.g. CEX3, CEX4S) and key stores (e.g. PKDS, CKDS, TKDS) in an enterprise.
- ISKLM (IBM Security Key Lifecycle Manager) for managing keys that are used to encrypt/decrypt information stored on tape and disk devices.

# System z Security Portal with Automatic notification of Security and Integrity Service

- To help you to maintain rigorous z/OS system security and integrity standards:
  - IBM recommends that you promptly install security and integrity PTFs
  - Sign up for the System z Security Portal
- Can help you stay more current by providing you with advanced automatic notification of SECINT PTFs.
- Provides SMP/E HOLDDATA used to identify fixes before they are marked RSU (Recommended Service Upgrade)
- Also provides associated Common Vulnerability Scoring System (CVSS) V2 ratings for new APARs*
- Delivers information on security and integrity patches more securely!
  - Must register – confidentiality is maintained
  - Avoids widespread communication of the specifics of the potential vulnerability
    - Widespread specifics about a vulnerability could increase the likelihood that an attacker could successfully exploit it
- Visit System z Security Portal site at http://www.vm.ibm.com/security/aparinfo.html to get the information you need to register
- Questions can be directed to: syszsec@us.ibm.com

* Note: According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM provides the CVSS scores :as is" without warranty of any kind, including the implied warranties o merchantability and fitness for a particular purpose. Customers are responsible for assessing the impact of any actual or potential security vulnerability in their specific environment. IBM does not provide a CVSS environment score. The CVSS environment Score is customer environment specific and will impact the overall CVSS score.

# Reference

- SA22-7520 ICSF Systems Programmer’s Guide
- SA22-7521 ICSF Administration Guide
- SA22-7522 ICSF Application Programmer’s Guide