z/OS 2.4 IBM Education Assistant (IEA)

Solution (Epic) Name: ICSF WD18 (HCR77D0) Enhancements

Element(s)/Component(s): ICSF

Agenda

- Trademarks
- Session Objectives
- Epics
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Session Objectives

- 239895: Expanded Triple-Length DES Key Support
- 196559: PKDS Keys, PKCS11 Token Utilities
- 196539: SAF Profile Prefix
- 196529: KGUP Security Enhancements
- 196334: Dynamic Service Update
- 196321: ICSF Early Availability

Overview: Expanded Triple-Length DES Key Support

- Who (Audience)
  - ICSF Application Programmers, Administrators
- What (Solution)
  - non-DATA 3KDES keys
- Wow (Benefit / Value, Need Addressed)
  - 3KDES keys provide better data protection vs 2KDES keys
  - 2KDES keys aren’t strong enough to protect 3KDES keys
  - NIST only allows the use of 2KDES for legacy purposes

Expanded Triple-Length DES Key Support

- Currently, triple-length DES key support is limited to DATA keys which can perform encipherment and MACing
- Triple-length DES key support is being expanded to the following key types
  - Data operation keys: CIPHER, ENCIPHER, DECIPHER, MAC, MACVER
  - PIN processing keys: PINGEN, PINVER, IPINENC, OPINENC
  - Key encrypting keys: IMPORTER, EXPORTER
- Services capable of producing keys accept a new TRIPLE or TRIPLE-O keyword or triple-length skeleton token
  - A triple-length skeleton token can be built using the Key Token Build (CSNBKTB) service
- KGUP can be used to generate 3KDES keys via the $TRIPLE and $TRIPLEO keywords

Expanded Triple-Length DES Key Support (contd)

- Services which support the key types but don’t support 3KDES keys
  - Remote Key Export (CSNDRKX and CSNFRKX)
  - Unique Key Derive (CSNBUKD and CSNEUKD)

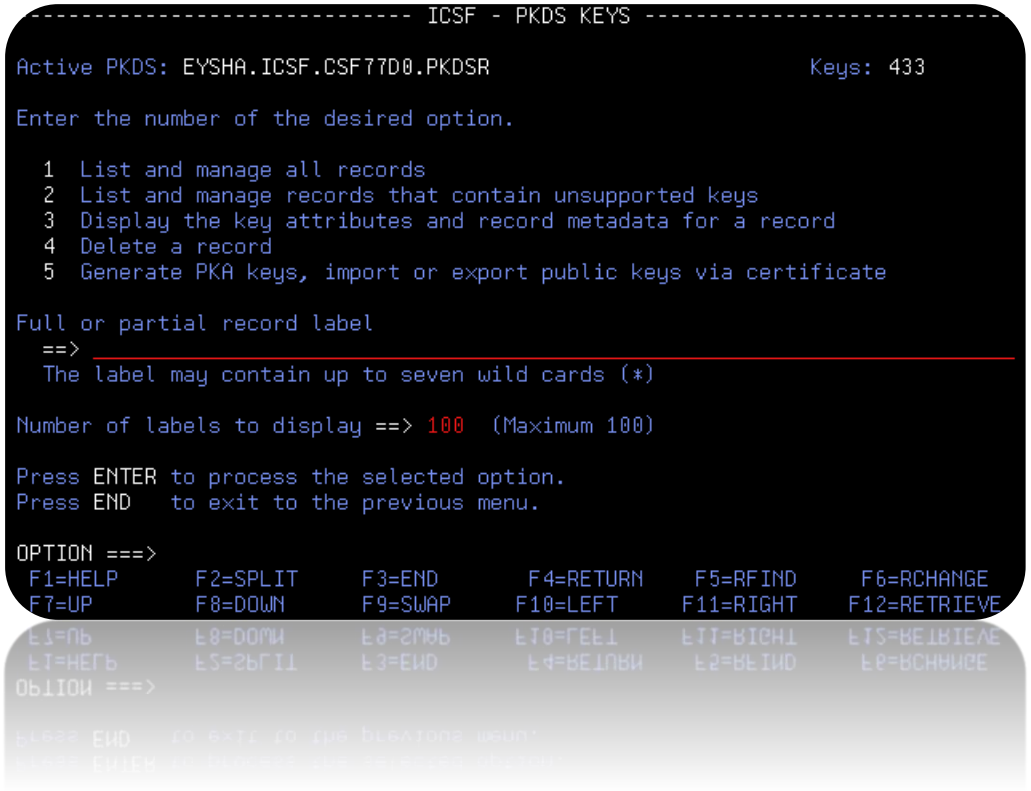
Notes:

- A CEX5C with CCA 5.4 or CEX6C with CCA 6.2 is required to exploit this function

Overview: PKDS Keys, PKCS11 Token Utilities

- Who (Audience)
  - ICSF Administrators
- What (Solution)
  - Panel-based PKDS, PKCS#11 Key Management
- Wow (Benefit / Value, Need Addressed)
  - Ability to view, update, delete PKDS keys without coding ICSF services
  - Ability to update the metadata attributes of PKCS#11 keys without coding ICSF services

PKDS Keys, PKCS11 Token Utilities



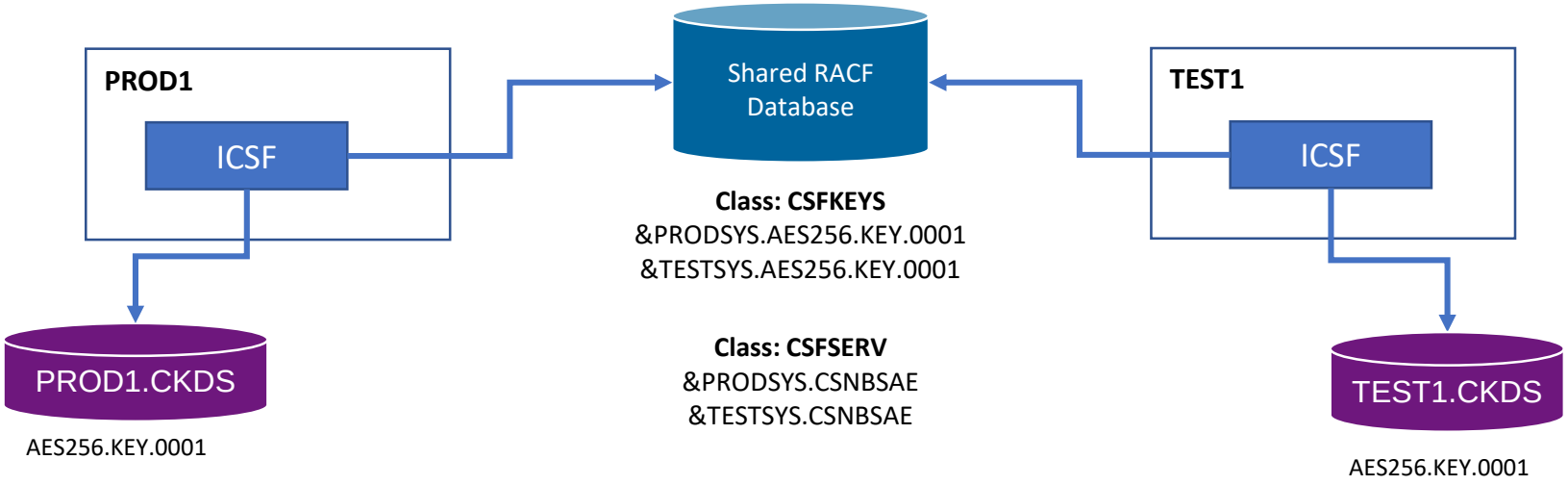
- The existing PKDS KEYS utility has been enhanced with functionality similar to the CKDS KEYS utility to manage records in the active PKDS.
- You may view, create, update, and delete keys in your PKDS. Some information you may view include:
  - state of the record (i.e. active, pre-active, deactivated, archived)
  - key attributes and record metadata
- The existing PKCS #11 Token Utility is being updated to support management of TKDS metadata when the TKDS is in KDSR format
- Both utilities are under ICSF Option 5. UTILITY

Overview: SAF Profile Prefix

- Who (Audience)
  - ICSF Administrators
- What (Solution)
  - Adds a system prefix to SAF profiles in the CSFKEYS, CSFSERV classes
- Wow (Benefit / Value, Need Addressed)
  - The ability to share a SAF database among different systems but have separate access controls to ICSF resources (keys, services,) eg. production vs test systems

SAF Profile Prefix

- There is currently no way to share a RACF database between different systems and have different authorizations to ICSF resources
- When the **CSF.PREFIX.CSFKEYS.ENABLED** resource is defined in the XFACILIT class, ICSF will allow users to split their **CSFKEYS** resources across multiple LPARs.
- When the **CSF.PREFIX.CSFSERV.ENABLED** resource is defined in the XFACILIT class, ICSF will allow users to split their **CSFSERV** resources across multiple LPARs.
- The system name will be prepended to the resource being authorization checked.



SAF Profile Prefix (contd)

- The maximum length of CSFKEYS and CSFSERV profiles is increasing to 246
- The state of conditional access control can be queried via the ICSF Query Facility (CSFIQF) service
- The state of conditional access control is reported by message CSFM699I
  - SAF PROFILE PREFIXNG FOR *CSFKEYS*|*CSFSERV* IS *ENABLED*|*DISABLED*.

SAF Profile Prefix (contd)

1. Define RACF variables

```
RDEFINE RACFVARS &PRODSYS ADDMEM(PROD1 PROD2 PROD3)
RDEFINE RACFVARS &TESTSYS ADDMEM(TEST1 TEST2)
```

2. Define prefixed CSFKEYS / CSFSERV profiles

```
RDEFINE CSFSERV &PRODSYS.CSFKGN UACC(NONE)
RDEFINE CSFKEYS &TESTSYS.AES256.KEY.0001 UACC(NONE)
```

3. Enable the prefixed profiles

```
SETROPTS RACLIST(RACFVARS) REFRESH
SETROPTS RACLIST(CSFSERV) REFRESH
SETROPTS RACLIST(CSFKEYS) REFRESH
```

4. Enable prefixing

```
RDEFINE XFACILIT CSF.PREFIX.CSFSERV.ENABLED UACC(NONE)
RDEFINE XFACILIT CSF.PREFIX.CSFKEYS.ENABLED UACC(NONE)
SETROPTS RACLIST(XFACILIT) REFRESH
```

Note: Enabling this feature will supersede non-prefixed CSFKEYS and CSFSERV profiles. Authorization checks will no longer be performed against the non-prefixed profiles. Be sure to define prefixed profiles before enabling.

Note: This function requires the following APARs: zSecure (OA56463), DFSMS (OA56500, OA56501, OA56502, OA56578), DB2 (PH05032).

Overview: KGUP Security Enhancements

- Who (Audience)
  - ICSF Administrators, System Programmers
- What (Solution)
  - Granular KGUP Security Controls
- Wow (Benefit / Value, Need Addressed)
  - The ability to differentiate between users who can create keys vs users who can update/delete keys
  - The ability to limit a users access to only keys they have been authorized to manage

KGUP Security Enhancements - Verbs

- Currently, Key Generator Utility Program (KGUP) only performs a SAF check against the CSFKGUP profile in the CSFSERV class. Users must have READ authority, which is the default authority when no profile exists.
- When the **CSF.KGUP.VERB.AUTHORITY.CHECK** resource in the XFACILIT class is defined, KGUP will require higher authorization levels to the CSFKGUP profile to perform certain operations.
- The state of KGUP Verb Access Control can be queried via the ICSF Query Facility (CSFIQF) service
- The state of KGUP Verb Access Control is reported by message CSFM697I
  - KGUP *CSFKEYS*|*VERB* AUTHORITY CONTROL IS *ENABLED*|*DISABLED*

Verbs	Authority
ADD, RENAME, OPKYLOAD	READ (default authority)
DELETE, UPDATE	UPDATE

KGUP Security Enhancements – Key Labels

- When the **CSF.KGUP.CSFKEYS.AUTHORITY.CHECK** resource in the XFACILIT class is defined, KGUP will issue a SAF check against the CSFKEYS class for each key label .
- SAF Profile Prefixing is supported
- The key store policy granular key label access control setting is honored
  - CSF.CSFKEYS.AUTHORITY.LEVELS.WARN
  - CSF.CSFKEYS.AUTHORITY.LEVELS.FAIL
- The state of KGUP CSFKEYS Authority Control can be queried via the ICSF Query Facility (CSFIQF) service
- The state of KGUP Verb Access Control is reported by message CSFM697I
  - KGUP *CSFKEYS|VERB* AUTHORITY CONTROL IS *ENABLED|DISABLED*

Verbs	Keywords	Authority (default)	Authority when granular key access is enabled.
Source of Label in KGUP Statement			
ADD	LABEL or RANGE	READ	UPDATE
UPDATE	LABEL or RANGE	READ	CONTROL
DELETE, RENAME	LABEL	READ	CONTROL
OPKYLOAD	LABEL	READ	UPDATE
ADD, UPDATE	TRANSKEY	READ	READ

Overview: Dynamic Service Update

- Who (Audience)
  - ICSF System Programmers
- What (Solution)
  - Activate ICSF service without restart or IPL
- Wow (Benefit / Value, Need Addressed)
  - As encryption becomes more pervasive, allows crypto capability to always be available

Dynamic Service Update

- Currently, to apply most service to ICSF requires a stop and restart of the ICSF started task in order for service updates to be picked up and activated.
- A smaller set of ICSF service updates requires an IPL in order to be picked up and activated.
- Neither of these is desirable in an environment where ICSF always needs to be available

Dynamic Service Update (contd)

New Installation Options Dataset Parameters

- The following new parameters identify datasets where ICSF will check for service versions of modules to load.
  - SERVSCSFMOD0(dsname[,volser])
  - SERVSIEALNKE(dsname[,volser])
- New SERVICELIBS(YES|NO) parameter will control whether the above service data sets are used.

Dynamic Service Update (contd)

- You will use the SETICSF PAUSE command to pick up ICSF Service without disrupting workloads
  - SERVICELIBS(YES) will use the SERV* libraries specified in the options data set
  - SERVICELIBS(NO) will use the normal search order and ignore the service libraries.
  - The processing is as follows:
    - Pauses new requests coming into ICSF
    - Waits until all active requests exit ICSF
    - Terminates ICSF (New requests continue to be paused)
    - ICSF auto restarts via ARM or customer automation
    - ICSF wakes up paused clients which proceed with their ICSF request

Dynamic Service Update (contd)

- SETICSF PAUSE command may now be used to:
  - Recycle ICSF with minimal disruption
  - Pick up ICSF service without disrupting workloads
  - Change ICSF options not supported via SETICSF OPTIONS,REFRESH

Dynamic Service Update (contd)

- DISPLAY ICSF,SERVICELIBS command lists the current and next settings for
  - SERVSCSFMOD0
  - SERVSIEALNKE

Note: This function requires the following APARs: OA56604, OA56605.

Overview: ICSF Early Availability

- Who (Audience)
  - ICSF System Programmers
- What (Solution)
  - Start ICSF early during IPL process as a system address space
- Wow (Benefit / Value, Need Addressed)
  - As encryption becomes more pervasive, allows crypto capability to be available earlier

ICSF Early Availability

- Currently, ICSF is typically initialized as a started task after IPL
- This does not allow core components of z/OS to utilize ICSF for crypto early in IPL
- ICSF will now be able to be started in one of two ways
  - With the START command as it is today, or
  - Using the IEASYSxx system parameter

ICSF Early Availability (contd)

- IEASYSxx
  - ICSF=xx where xx is passed to the ICSF PROC
  - ICSFPROC=procname specifies the name of the PROC to start or NONE
- ICSF gets started as a system address space during IPL
- Calls to ICSF before it completes initialization will be paused until ICSF is available.
- Choice of options definition allows options to be shared with older releases of ICSF
  - Options can come from PARMLIB concatenation (CSFPRMxx)
  - Options can come from CSFPARM DD as before

Notes:

- When ICSF is started early, the LIST option of the DISPLAY [JOBS|A] command does not include ICSF eg. DISPLAY A,L. Use the ALL option instead eg. DISPLAY A,ALL.
- Automatic Restart Manager (ARM) may not be used to restart ICSF when it is started early

Usage & Invocation

- Already covered

Interactions & Dependencies

- To exploit this item, all systems in the Plex must be at the new z/OS level: No
- Software Dependencies
  - The following APARs are required before starting ICSF: PH04377, OA56421
  - The following APARs are required before exploiting SAF Profile Prefix: OA56463, OA56500, OA56501, OA56502, OA56578, PH05032.
  - The following APARs are required before exploiting Dynamic Service Update: OA56604, OA56605
- Hardware Dependencies
  - 3KDES exploitation requires a CEX5C w/CCA 5.4 or CEX6C w/CCA 6.2
- Exploiters
  - None

Migration & Coexistence Considerations

- Migration
  - The ICSF installation option dataset may not be a sequential dataset
- Coexistence
  - APAR OA55906 is required on systems running HCR77C0 or earlier
  - APAR OA55906 or OA55184 is required on systems running HCR77C1
- Toleration
  - On systems running HCR77C0 or earlier, APAR OA55906 must be installed and active before upgrading to a CEX5C with CCA 5.4 or CEX6C with CCA 6.2
  - On systems running HCR77C1, APAR OA55906 or OA55184 must be installed and active before upgrading to a CEX5C with CCA 5.4 or CEX6C with CCA 6.2

Installation

- None

Bonus

- 196549: Restrict which services a key can be used in
- 207093: PKCS#11 algorithms: ChaCha20 and Poly1305
- 196582: D ICSF,MKVPS console command to help diagnose issues with coprocessor master keys
- 207042: BSI 2017 compliance mode support for the EP11 coprocessor
- 232457: DES CIPHER keys as protected keys (requires APAR OA56265 and CEX6C w/CCA 6.2 for exploitation)

Session Summary

- 239895: Expanded Triple-Length DES Key Support
- 196559: PKDS Keys, PKCS11 Token Utilities
- 196539: SAF Profile Prefix
- 196529: KGUP Security Enhancements
- 196334: Dynamic Service Update
- 196321: ICSF Early Availability

Appendix

- z/OS Cryptographic Services ICSF System Programmer's Guide
- z/OS Cryptographic Services ICSF Administrator's Guide
- z/OS Cryptographic Services ICSF Application Programmer's Guide

Questions?

End of Section