MAINFRAME CRYPTO

Unscrambling the Complexity of Crypto!

ICSF

Part 2 of 2

Greg Boyd

www.mainframecrypto.com

THE Z EXCHANGE

May 2021

Copyrights and Trademarks

- Copyright © 2021 Greg Boyd, Mainframe Crypto, LLC. All rights reserved.
- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 30+ years

- All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. IBM, System z, zEnterprise and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.
- **THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY**. Greg Boyd and Mainframe Crypto, LLC assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Greg Boyd or Mainframe Crypto, LLC be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if expressly advised in advance of the possibility of such damages.

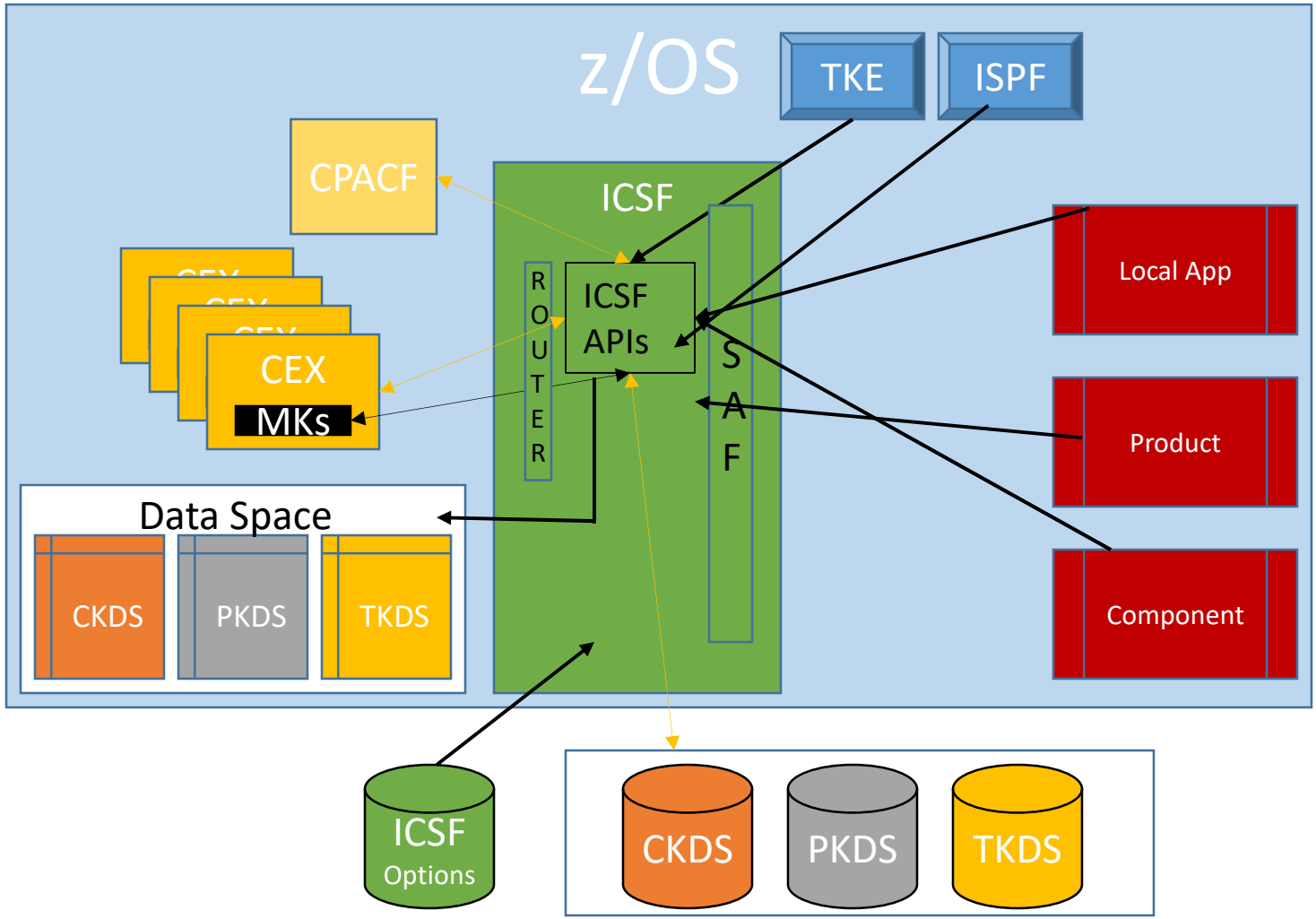
Agenda - ICSF

- ICSF – Part 1 of 2
  - z/OS Component
  - Started Task
  - Always Up!
  - Key stores
  - Options
- ICSF – Part 2 of 2
  - Operator Commands
  - ISPF Panels
    - Master Keys
    - KGUP
    - Keys Panels
  - Security & Key Store Policies
  - SMF
  - HealthChecks
  - APIs

ICSF

- Interface to the hardware
  - CPACF APIs (invoke the native instructions)
  - CEX APIs (the only interface to the CEX cards)
  - Other APIs (query, key definition/management)
- Crypto management
  - ISPF interface (view/manage devices and master keys, manage key repositories, view options, etc.)
  - Operator commands
- Key Security & Integrity
  - Master key loading
  - Invoke KGUP
- SAF
  - Operational Keys
  - APIs
  - Key store policies

ICSF Started Task



SETICSF Command (HCR77B1)

- Activate, deactivate, restart a crypto device
- Add, check, delete a regional crypto device
- Attempt to reopen sockets
- Change selected ICSF installation options
- Enable or disable updates to a key data set
- Pause transactions until ICSF is restarted
- Refresh some ICSF options (from the Options data set)

secured by MVS.SETICSF profile

SETICSF Command (HCR77B1)

- Remotedevice
  - ACTivate (Index, Serial Number, Remote Device)
  - DEACTivate (Index, Serial Number, Remote Device)
  - RESTART (Index, Serial Number, Remote Device)
  - CHECK (Remote Device)
  - DELETE (Remote Device)
- Keystore (CKDS, PKDS, TKDS)
  - ENable
  - DISable
- Options (AUDIT…, MKCVLEN, RISEC, RIPER, STATS)

secured by MVS.SETICSF profile

SETICSF OPTIONS,REFRESH (HCR77C0)

- AUDITKEYLIFECKDS
- AUDITKEYLIFEPKDS
- AUDITKEYLIFETKDS
- AUDITKEYUSGCKDS
- AUDITKEYUSGPKDS
- AUDITPKCS11USG
- BEGIN
- CHECKAUTH
- CICSAUDIT
- COMPLIANCEWARN
- DEFAULTWRAP
- END
- FIPSMODE
- KEYARCHMSG
- KDSREFDAYS
- MASTERKCVLEN
- MAXSESSOBJECTS
- RNGCACHE
- SSM
- USERPARM
- WAITLIST

Display ICSF Command (HCR77B1)

- LIST (members of sysplex)
- CARDS (coprocessors)
- KDS (active keystores)
- MKS (master key info, for each card)
- MKVPS (master key verification patterns)
- OPTIONS
- REMOTEdevice (network attached open cryptographic servers)
- SERVICELIBS

secured by MVS.DISPLAY.ICSF profile

DISPLAY ICSF

D ICSF,CARDS

```
RESPONSE=S1
 CSFM668I 19.14.19 ICSF CARDS 029
   ACTIVE DOMAIN = 013
   CRYPTO EXPRESS6 COPROCESSOR 6C01
     STATUS=Active            SERIAL#=DV795357 LEVEL=6.0.8z
     REQUESTS=0000000250  ACTIVE=0000
   CRYPTO EXPRESS6 COPROCESSOR 6C03
     STATUS=Active            SERIAL#=DV795351 LEVEL=6.0.8z
     REQUESTS=0000000257  ACTIVE=0000
```

D ICSF,MKS

```
RESPONSE=S1
 CSFM668I 19.15.40 ICSF MKS 036
   SYSNAME: S1      DOMAIN: 013 CPC Name: PELCP02
     FEATURE SERIAL#  STATUS          AES DES ECC RSA P11
      6C01   DV795357 Active            A   A   A   A
      6C03   DV795351 Active            A   A   A   A
```

DISPLAY ICSF,OPTIONS ….

D ICSF,OPTIONS
CSFM668I 10.23.21 ICSF OPTIONS 833
SYSNAME = MFCA ICSF LEVEL = HCR77D0
LATEST ICSF CODE CHANGE = 09/25/20
Refdate update interval in Days/HH.MM.SS = 001/00.00.00
Refdate update period in Days/HH.MM.SS = 000/01.00.00
MASTERKCVLEN = display 3 digits
AUDITKEYLIFECKDS: Audit CCA symmetric key lifecycle events
SYSNAME LABEL TOKEN
MFCA Yes Yes
AUDITKEYLIFEPKDS: Audit CCA asymmetric key lifecycle events
SYSNAME LABEL TOKEN
MFCA Yes Yes
AUDITKEYLIFETKDS: Audit PKCS #11 key lifecycle events
SYSNAME TOKOBJ SESSOBJ
MFCA Yes Yes

.... DISPLAY ICSF,OPTIONS

```
AUDITKEYUSGCKDS: Audit CCA symmetric key usage events
   SYSNAME LABEL TOKEN Interval Days/HH.MM.SS
   MFCA        Yes     Yes       000/01.00.00
AUDITKEYUSGPKDS: Audit CCA asymmetric key usage events
   SYSNAME LABEL TOKEN Interval Days/HH.MM.SS
   MFCA        Yes     Yes       000/01.00.00
AUDITPKCS11USG: Audit PKCS #11 usage events
   SYSNAME TOKOBJ SESSOBJ NOKEY Interval Days/HH.MM.SS
   MFCA        Yes       Yes       Yes       000/01.00.00
STATS:
   MFCA      ENG, SRV, ALG
COMPLIANCEWARN: Compliance warning events
   MFCA      PCI-HSM 2016 Yes
```

Display ICSF Operator Command (HCR77D0)

- DISPLAY ICSF,MKVPS
  - Display MKVPs from the KDS and crypto devices

```
RESPONSE=S2
 CSFM668I 17.17.12 ICSF MKVPS 843
  CKDS  MFCPLEX.S2.CSFCKDS
          ID                AES       DES
   KDSMKVPS                  ....     5EB98E   14138E
   MFC1                      6C01     5EB98E   14138E
  PKDS  MFCPLEX.S2.CSFPKDS
          ID                ECC       RSA
   KDSMKVPS                  ....     3ED9AC   B78602
   MFC1                      6C01     3ED9AC   B78602
  No TKDS defined or no EP11 adapters online
```

- DISPLAY ICSF,MKVPS,ERRORS
  - Limits the display to devices that have no master key loaded, or the master key does not match the keystore

ICSF Main Panel

```
HCR77D0 ------------ Integrated Cryptographic Service Facility-------------
OPTION ===>
System name:  S1                                        Crypto Domain:  13

Enter the number of the desired option.
  1  COPROCESSOR MGMT -  Management of Cryptographic Coprocessors
  2  KDS MANAGEMENT   -  Master key set or change, KDS Processing
  3  OPSTAT           -  Installation options
  4  ADMINCNTL        -  Administrative Control Functions
  5  UTILITY          -  ICSF Utilities
  6  PPINIT           -  Pass Phrase Master Key/KDS Initialization
  7  TKE              -  TKE PKA Direct Key Load
  8  KGUP             -  Key Generator Utility processes
  9  UDX MGMT         -  Management of User Defined Extensions


     Licensed Materials - Property of IBM
     5650-ZOS (C) Copyright IBM Corp. 1989, 2018.
     US Government Users Restricted Rights - Use, duplication or
     disclosure restricted by GSA ADP Schedule Contract with IBM Corp.


Press ENTER to go to the selected option.
Press END   to exit to the previous menu.
```

ISPF Panel Functions for ICSF

- Display coprocessor status
- Deactivate/activate coprocessors
- Load/set/change master keys
- Initialize/reencipher keystores
- Refresh/activate keystores
- Passphrase initialization
- Front-end process for Key Generation Utility Program (KGUP)
- Generate random numbers/calculate checksums
- Administrative control for CKDS/PKDS access and PKA callable services
- Complete TKE operations

PF1 from any panel for help

ADMINCNTL (Option 4)

```
CSFACF00 --- ICSF Administrative Control Functions --- Row 1 to 2 of 2
COMMAND ===>
                Active CKDS:  CSF.PROD.CKDS
                Active PKDS:  CSF.PROD.PKDS
                Active TKDS:  CSF.PROD.TKDS

To change the status of a control, enter the appropriate character
(E - ENABLE, D - DISABLE) and press ENTER.

       Function                                STATUS
       --------                                ------
 .  Dynamic CKDS Access                        ENABLED
 .  Dynamic PKDS Access                        ENABLED
```

Master Key Entry

- Passphrase Initialization – ICSF Main Menu Option 6
  - 16 to 64 character Passphrase which is used to calculate master key material
  - Only for first-time initialization of ICSF
- ICSF Panels
  - Coprocessor Management – ICSF Main Menu Option 1 to load key material
  - KDS Management – ICSF Main Menu Option 2 to Initialize the key stores or to change master keys
- Trusted Key Entry Workstation
  - Load key material from the TKE
  - KDS Management – ICSF Main Menu Option 2 to Initialize the key stores or to change master keys

ICSF Coprocessor Management Panel – HCR77D0

```
CSFCMP00  -------- ICSF Coprocessor Management --------------
COMMAND =>
Select the coprocessors to be processed and press ENTER.
Action characters are:  A, D, E, K, R, S and V.  See the help
panel for details.

Crypto  Serial
Feature Number   Status                AES  DES  ECC  RSA  P11
------- -------- -----------           ---  ---  ---  ---  ---
_ 7A01           ACTIVE
_ 7C02  24778902 ACTIVE                 A    A    A    A
_ 7C05  98001236 ACTIVE                 A    A    A    A
_ 7C06  97006090 Master key incorrect   U    C    U    E
_ 7C12  DV795357 ACTIVE                 A    A    A    A
_ 7A13           OFFLINE
_ 7P14  97006062 ACTIVE                                  A
```

Coprocessor Hardware Status (Option 1 – Show)

```
CSFCMP40 ----------- ICSF - Coprocessor Hardware Status --------------
COMMAND ===>                                          SCROLL ===> PAGE
                                                      CRYPTO DOMAIN: 2

REGISTER STATUS                    COPROCESSOR 7C02     COPROCESSOR 7C05
                                                                MORE +
 Crypto Serial Number            : 98001236             97006090
 Status                          : ACTIVE               ACTIVE
 PCI-HSM Compliance Mode         : INACTIVE             INACTIVE
 Compliance Migration Mode       : INACTIVE             INACTIVE
 AES Master Key
   New Master Key register       : EMPTY                EMPTY
     Verification pattern        :
   Old Master Key register       : VALID                VALID
     Verification pattern        : BF494FF74B86343F     BF494FF74B86343F
   Current Master Key register   : VALID                VALID
     Verification pattern        : F03CF42DB933BF1E     F03CF42DB933BF1E
```

Displaying the options

ICSF option 3, OPSTAT from Main Panel, Select option 1, Options

```
CSFSOP10 ------ ICSF - Installation Option Display -- Row  1 to 22 of 34
COMMAND ===>                                              SCROLL ===> PAGE
         Active CKDS: CSF.PROD.CKDS
         Active PKDS: CSF.PROD.PKDS
         Active TKDS: CSF.PROD.TKDS
  OPTION                                                   CURRENT VALUE
  ------                                                    -------------
AUDITKEYLIFECKDS Audit CCA symmetric key lifecycle events   TOKEN(Y),LABEL(Y)
AUDITKEYLIFEPKDS Audit CCA asymmetric key lifecycle events  TOKEN(Y),LABEL(Y)
AUDITKEYLIFETKDS Audit PKCS #11 key lifecycle events        TOKEN(Y),SESSO(Y)
AUDITKEYUSGCKDS  Audit CCA symmetric key usage events       TOK(Y),LAB(Y)
                                                            INT(001,00.00.00)
AUDITKEYUSGPKDS  Audit CCA asymmetric key usage events      TOK(Y),LAB(Y)
                                                            INT(001,00.00.00)
AUDITPKCS11USG   Audit PKCS #11 usage events                TOK(Y),SESSO(Y),
                                                            NOKEY(Y),
                                                            INT(001,00.00.00)
CHECKAUTH        RACF check authorized callers              NO
CICSAUDIT        Audit CICS client identity                 NO
COMPAT           Allow CUSP/PCF compatibility               NO
COMPLIANCEWARN   Compliance Warn Mode                       Not Specified
CTRACE           CTRACE parmlib used at ICSF startup        CTICSF00
DEFAULTWRAP      Default symmetric key wrapping - internal  ORIGINAL
DEFAULTWRAP      Default symmetric key wrapping - external  ORIGINAL
DOMAIN           Current domain index or usage domain index 1
FIPSMODE         Operate PKCS #11 in FIPS 140-2 mode        NO,FAIL(NO)
KDSREFDAYS       Number of days between reference updates   1
KEYARCHMSG       Message for archived KDS record reference  NO
MASTERKCVLEN     Length of master key verification patterns
```

Displaying the options

ICSF option 3, OPSTAT from Main Panel, Select option 1, Options

```
CSFSOP10 ------ ICSF - Installation Option Display -- Row 23 to 34 of 34
COMMAND ===>                                                SCROLL ===> PAGE
         Active CKDS: CSF.PROD.CKDS
         Active PKDS: CSF.PROD.PKDS
         Active TKDS: CSF.PROD.TKDS
  OPTION                                                    CURRENT VALUE
  ------                                                    -------------
MAXSESSOBJECTS  Max non-authpgm PKCS #11 session objects    65535
REASONCODES     Source of callable service reason codes     ICSF
RNGCACHE        Random Number Generate cache enabled        YES
SSM             Allow Special Secure Mode                   YES
STATS           Crypto Usage Statistics                     ENG,SRV,ALG
STATSFILTERS    Crypto Usage Statistics Filters             NOTKUSERID(N)
SYSPLEXCKDS     SYSPLEX Consistency for CKDS Updates        YES,FAIL(YES)
SYSPLEXPKDS     SYSPLEX Consistency for PKDS updates        YES,FAIL(YES)
SYSPLEXTKDS     SYSPLEX Consistency for TKDS Updates        YES,FAIL(YES)
USERPARM        User specified parameter data               USERPARM
WAITLIST        Source of CICS Wait List if CICS installed
                       DSN: SYS1.SAMPLIB(CSFWTL01)
```

Create a KGUP Control Statement

```
CSFCSE10 ---- ICSF - Create ADD, UPDATE, or DELETE Key Statement ----
COMMAND ===>

Specify control statement information below
  Function  ===> ______     ADD, UPDATE, or DELETE
  Algorithm ===> DES         DES or AES
  Key Type  ===> ________    Outtype ===> ________    (Optional)
  Label ===>  ____________________________________________________
   Group Labels  ===> NO_   NO or YES
 or Range:
  Start ===> ____________________________________________________
  End   ===> ____________________________________________________
   Transport Key Label(s)
        ===> ____________________________________________________
        ===> ____________________________________________________
 or Clear Key ===> NO_      NO or YES

  Control Vector ===> YES  NO or YES
  Length of Key  ===> ___  For DES: 8, 16 or 24 For AES: 16, 24, or 32
  Key Values     ===>  _________ , _________ , _________ , _________
   Comment Line   ===> ____________________________________________

Press ENTER to create and store control statement
Press END   to exit to the previous panel without saving
```

CKDS Keys Utility (HCR77C1)

- List and manage all records
- List and manage records by key type
- List and manage records based on status (Active, Inactive, Archived)
- List and manage records with unsupported CCA keys
- Display key attributes
  - Algorithm
  - Key Usage
  - Key Check Value
  - Key Type
  - Key Length
- Display metadata
  - Creation, Update and Validity dates
  - Date and Service Last Used
  - Date archived
  - Archive & Prohibit Archive Flag
  - Date recalled
- Change some metadata
- Delete a record
- Very limited key generation - AES DATA keys

CKDS Keys Panel

```
CSFBRCK0  ------------------ ICSF CKDS KEYS ------------------  CKDS NO RECORDS
OPTION ===>

Active CKDS:  CSF.PROD.CKDS                                    Keys:  0

Enter the number of the desired option.
 1 List and manage all records
 2 List and manage records with label key type ____ leave blank for list, see
help
 3 List and manage records that are __________ (ACTIVE, INACTIVE, ARCHIVED)
 4 List and manage records that contain unsupported CCA keys
 5 Display the key attributes and record metadata for a record
 6 Delete a record
 7 Generate AES DATA keys

Full or partial record label
 ===>  ________________________________________________________________________
  The label may contain up to seven wild cards (*)
Number of labels to dislplay ===>  100    (Maximum 100)


Press ENTER to go to the selected option.
Press END     to exit to the previous menu.
```

PKDS Keys Utility (HCR77D0)

```
CSFBRPK0  ------------ ICSF - PKDS KEYS -----------------------------
OPTION ===>

Active CKDS:  CSF.PROD.PKDS                                  Keys:   149

Enter the number of the desired option.
 1   List and manage all records
 2   List and manage records that are _____________ (ACTIVE, INACTIVE, ARCHIVED)
 3   List and manage records that contain unsupported CCA keys
 4   Display the key attributes and record metadata for a record
 5   Delete a record
 6   Generate PKA keys, import or export public keys via certificate

Full or partial record label
 ===> ________________________________________________________________
  The label may contain up to seven wild cards (*)

Number of labels to dislplay ===>  100    (Maximum 100)

Press ENTER to go to the selected option.
Press END     to exit to the previous menu.
```

PKDS Key Management Panel(pre HCR77D0)

```
CSFPKY00 ---------------- ICSF - PKDS Keys ------------------------
COMMAND ===>
 Enter the RSA record's label for the actions below
  ==>  ________________________________________________
 Select one of the following actions then press ENTER to process:
 - Generate a new RSA or EC key pair record. Select one key type/size.
    RSA key bit length: _ 512 _ 1024 _ 2048 _ 3072 _ 4096
    EC NIST Curve : _ p192 _ p224 _ p256 _ p384 _ p521
    EC Brainpool Curve: _ p160 _ p192 _ p224 _ p256 _ p320 _ p384 _ p512
    Enter Private Key Name (optional)
        ==> ________________________________________________
 - Delete the existing public key or key pair PKDS record
 - Export the PKDS record's public key to a certificate data set
    Enter the DSN ===>  ____________________________________
    Enter desired subject's common name (optional)
      CN= ________________________________________________
 - Create a PKDS public key record from an input certificate.
    Enter the DSN ===> ____________________________________
```

TKDS Keys Utility

- ICSF Utilities Panel, Option 7 PKCS11 Token - Manage PKCS11 tokens
  - Create a new token
  - Delete an existing token
  - Manage an existing token
  - List existing tokens

TKDS Token Management Panel

```
CSFTBR00 ---------- ICSF – Token Management – Main Menu --------------
OPTION ===>
Enter the number of the desired option.
  1  Create a new token
  2  Delete an existing token
  3  Manage an exiting token
  4  List an existing token

  Full or partial token name:  ____________________________________


Press  ENTER to go to the selected option.
Press  END   to exit to the previous menu.
```

RACF Profiles

- CSFKEYS – profiles to protect key material, based on the key label
- XCSFKEY – alternative profiles to protect key material
- CSFSERV – profiles to protect the ICSF APIs, as well as functions from the ISPF panels and KGUP
- CRYPTOZ – profiles to protect PKCS #11 tokens
- XFACILIT - Miscellaneous use profiles, used to implement Key Store Policies

Key Store Policies – XFACILIT Class

By defining a policy, a security administrator can make symmetric and asymmetric keys more secure, without requiring application changes

- Key Token Authorization Checking
- Default Key Label Checking
- Duplicate Key Token Checking
- Granular Key Label Access Control
- Symmetric Key Label Export Control (aka CSNDSYX Export Control)
- PKA Key Management Extension Control
- Key Archive Use Control

SMF Type 82 – ICSF Record

- Subtype 1 – Initialization options
- Subtype 7 – Operational key load
- Subtype 8 – Cryptographic key data set refresh
- Subtype 9 – Dynamic CKDS Update
- Subtype 13 – Dynamic PKDS update
- Subtype 14 – Cryptographic coprocessor master key entry
- Subtype 15 – PCI Crypto coprocessor retained key create/delete
- Subtype 16 – PCI Cryptographic coprocessor TKE
- Subtype 18 – Cryptographic processor configuration
- Subtype 19 – PCI X Cryptographic coprocessor timing
- Subtype 20 – Cryptographic processor processing times

SMF Type 82 – ICSF Record (cont.)

- Subtype 21 – ICSF Sysplex group change
- Subtype 22 – Trusted block create callable services
- Subtype 23 – Token data set update
- Subtype 24 – Duplicate tokens found
- Subtype 25 – Key store policy for key token authorization checking
- Subtype 26 – Public key data set refresh
- Subtype 27 – PKA key management extensions
- Subtype 28 – High performance encrypted key (Protected Key)
- Subtype 29 – TKE workstation audit record

SMF Type 82 – ICSF Record (cont.)

- Subtype 30 – Key store policy archived & inactive KDS records
- Subtype 31 – Cryptographic usage statistics
- Subtype 40 – CCA symmetric key lifecycle event
- Subtype 41 – CCA asymmetric key lifecycle event
- Subtype 42 – PKCS #11 object lifecycle event
- Subtype 43 – Regional cryptographic server configuration
- Subtype 44 – CCA symmetric key usage event
- Subtype 45 –CCA asymmetric key usage event
- Subtype 46 – PKCS #11 key usage event
- Subtype 47 – PKCS #11 no key usage event
- Subtype 48 – Compliance warning event

SMF and Logging

- z/OS System Measurement Facility
  - SYS1.PARMLIB(SMFPRXxx)
    - SYS(TYPE(…,82,…))
  - Dump Started Task/Job

```
//SMFDMP   EXEC PGM=IFASMFDP,REGION=4M
//SMFIN          DD  *
 INDD(DUMPIN,OPTIONS(ALL))
 OUTDD(DUMPOUT,TYPE(000:255)
```

REXX EXEC CSFSMFR

- Formats the SMF Type 82 records into a 'readable' report
  - Sample Job, CSFSMFJ to
    - Capture the Type 82 records (with IFASMFDP)
    - Sort the records
    - Execute CSFMFR, via Batch TSO
  - Output may be large – multiple lines per Type 82 record
  - It's more readable than the raw SMF record, but still a bit complex

TYPE 82, SUBTYPE 1 ICSF Initialization

```
Subtype=0001 Initialization Section
  Written whenever ICSF is started
  6 Jul 2016 8:38:00.12
     TME..002F6CAC DTE..0116188F SID..S1 SSI..00000000 STY..0001 VES..A0000000
       VES 80 SSM enabled
       VES 20 RNG Cache enabled
     VTS... 00 IDO... 0D
     CKD... SHARPLEX.CRYPTO.CKDS
     IML... 0000FFFF USR... USERPARM
     PKD... SHARPLEX.CRYPTO.PKDS
     TKD... SHARPLEX.CRYPTO.TKDS
  ICSF Server Identity...
     USRI.. STCSYS
     GRPN.. STCGRP
     JBN... CSF
     RST... 8:37:52.77
     RSD... 6 Jul 2016
     SUID.. 4040404040404040
```

Health Checks - Status

- Status Check – info on current state of ICSF
  - ICSF_ COPROCESSOR_STATE_NEGCHANGE
  - ICSF_DEPRECATED_SERV_WARNINGS
  - ICSF_KEY_EXPIRATION
  - ICSF_MASTER_KEY_CONSISTENCY
  - ICSF_OPTIONS_CHECK
  - ICSF_PKCS_PSS_SUPPORT
  - ICSF_UNSUPPORTED_CCA_KEYS
  - ICSF_WEAK_CCA_KEYS

Health Checks – Migration

- Migration Check – warns of changes in current or pending ICSF release that could negatively impact usage
  - ICSFMIG_DEPRECATED_SERV_WARNINGS
  - ICSFMIG_MASTER_KEY_CONSISTENCY
  - ICSFMIG7731_ICSF_RETAINED_RSAKEY
  - ICSFMIG77A1_COPROCESSOR_ACTIVE
  - ICSFMIG77A1_TKDS_OBJECT
  - ICSFMIG77A1_UNSUPPORTED_HW

APIs (HCR77D1)

- Symmetric Key Management (51)
- Protecting Data (9)
- Verifying Data Integrity and Authenticating Messages (10)
- Financial Services (25)
- Financial Services for DK PIN Methods (10)
- Using Digital Signatures (2)
- Managing PKA Cryptographic Keys (8)
- Key Data Set Management (16)
- Utilities (7)
- Trusted Interfaces (2)
- Using PKCS #11 Tokens and Objects (19)
- Using the PKCS #11 Key Structure Callable Services (4)

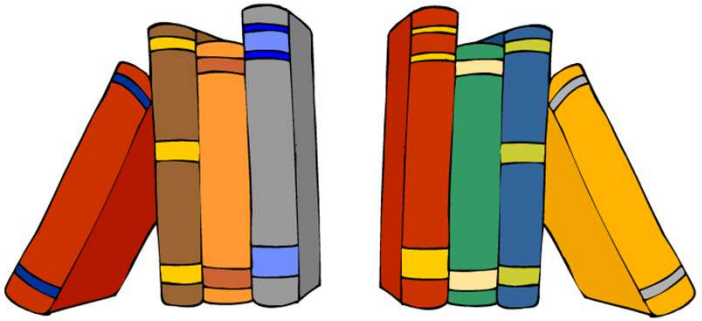
Callable Services

- Dependency on server type
- Dependency on Crypto card
- Languages: C, COBOL, PL/I, Assembler, Fortran (and REXX)
- Problem vs Supervisor State
- Task or SRB Mode
- 64-Bit Access (as of HCR77A0)
- Alternate entry points (ALET-qualified)

API Syntax

- All ICSF APIs start with same 4 parms
  - Return Code — INTEGER, HEX PIC 9(8) COMP
  - Reason Code — INTEGER, HEX PIC 9(8) COMP
  - Exit Data Length — INTEGER, HEX PIC 9(8) COMP
  - Exit Data — STRING, CHAR, PIC X()
- Followed by specific positional parms, unique to the API
- RULE_ARRAY
  - Array of parms, specific to the API
  - 8-byte keywords, left-justified, blank padded

IBM Manuals



- SC14-7505-08 ICSF Overview
- SC14-7506-08 ICSF Administrator's Guide
- SC14-7507-08 ICSF System Programmer's Guide
- SC14-7508-08 ICSF Application Programmer's Guide
- SC14-7509-07 ICSF Messages
- SC14-7510-06 ICSF Writing PKCS #11 Applications
- GI11-9478-08 Program Directory for Cryptographic Services for z/OS V2R2 – z/OS V2R4

ICSF Web References

- ICSF Cross Reference (old TechDoc)
  - https://www.ibm.com/support/pages/node/6354701
    - https://www.ibm.com/support/pages/system/files/inline-files/ICSF%20Version%20and%20FMID%20Cross%20Reference%20Oct2020.pdf
- z/OS Web Download site
  - http://www.ibm.com/systems/z/os/zos/tools/downloads/index.html

Agenda - ICSF

- ICSF – Part 1 of 2
  - z/OS Component
  - Started Task
  - Always Up!
  - Key stores
  - Options
- ICSF – Part 2 of 2
  - Operator Commands
  - ISPF Panels
    - Master Keys
    - KGUP
    - Keys Panels
  - Security & Key Store Policies
  - SMF
  - HealthChecks
  - APIs

Questions