MAINFRAME CRYPTO

Unscrambling the Complexity of Crypto!

HCR77D0
(aka Cryptographic Support for z/OS V2R2 – z/OS V2R3)

Greg Boyd

gregboyd@mainframecrypto.com

THE Z EXCHANGE

March 2019

. . . And Trademarks

-
- 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

- Announcement, Installation & Operations
- ICSF Always Up
  - New Started Task
  - Dynamic Service
- Triple-length DES Keys
- Key Utilities
  - CKDS Utility Enhanced
  - New PKDS Utility
  - New TKDS Utility
- Security
  - SAF Prefixes
  - Conditional Access List
  - KGUP SAF Checking

z/OS: ICSF Version and FMID Cross Reference (TD103782)

FMID	External Name	Applicable z/OS Releases	Availa-bility	Planned EoS	Supported Servers
HCR77B0	Enhanced Cryptographic Support for z/OS V1R13-z/OS V2R1	z/OS 1.13; z/OS 2.1	Feb 2015	TBD	z890/z990; z9; z10; z196/z114; zEC12/zBC12; z13/z13s**, z14/z14R1**
	z/OS 2.2	z/OS 2.2	Sep 2015	TBD	
HCR77B1	Cryptographic Support for z/OS V1R13-z/OS V2R2	z/OS 1.13; z/OS 2.1; z/OS 2.2	Nov 2015	TBD	z890/z990; z9; z10; z196/z114; zEC12/zBC12; z13/z13s**, z14/z14R1**
HCR77C0	Cryptographic Support for z/OS V2R1 – z/OS V2R2	z/OS 2.2; z/OS 2.1	Oct 2016	TBD	z9; z10; z196/z114; zEC12/zBC12; z13/z13s; z14/z14R1**
	z/OS 2.3	z/OS 2.3	Sep 2017	TBD	
HCR77C1	Cryptographic Support for z/OS V2R1 – z/OS V2R3	z/OS 2.3; z/OS 2.2; z/OS 2.1	Sep 2017	TBD	z9; z10; z196/z114; zEC12/zBC12; z13; z14
HCR77D0	Cryptographic Support for z/OS V2R2 – z/OS V2R3	z/OS 2.2; z/OS 2.3	Dec. 2018	TBD	z10; z196/z114; zEC12/zBC12; z13; z14

**Older versions of ICSF may need toleration maintenance installed to support newer hardware

TechDoc Highlights for HCR77D0 (and HCR77C1)

- CCA 5.4 & 6.1 (HCR77C1 OA55184)
  - ISO-4 format PIN blocks
  - Triple-length TDES support for more key types
    - CIPHER, ENCIPHER, DECIPHER, EXPORTER, IMPORTER, MAC, MACVER, IPINENC, OPINENC, PINGEN, PINVER
  - DK Key support for new key diversification scheme to generate keys with different attributes
    - KDKGENKY – new key type
    - CSNBDDK – Diversified Directed Key API
  - New Key wrapping support for ISO-20038 to use AES key types
    - TR-31 Export and TR-31 Import APIs

TechDoc Highlights for HCR77D0

- Enhancements for CCA Release 6.2
  - Restrict a key from being used as a symmetric key
  - New tagging to restrict a key to PCI HSM compliance usage
  - CCA redirection for Regional Crypto Enablement
  - CHACHA20 & Poly1305 algorithm support in PKCS #11
  - ICSF always up – apply new service to a running ICSF
  - ICSF early start up
  - KGUP can now check CSFKEYS profiles for access
  - ISPF PKDS Browser
  - Remove restriction on 32-byte CKA Label attribute of PKCS #11 key objects
  - CSNBKYT can now support clear keys
  - Honor MASTERKCVLEN keyword in SMF records after Operational Key Load function
  - Ability to specify key wrapping when importing a key via Operational Key Load
  - New BSI mode, BSI 2017
  - Support AES-GCM key wrapping for secret and private clear keys
  - Display ICSF, MKVP operator command

IBM Announcement Letter 185-075

- CEX6S designed to meet FIPS 140-2 Level 4
- IBM CCA 6.0 is PCI-HSM certified
  (https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices)

COMPANY	APPROVAL NUMBER	VERSION	PRODUCT TYPE	EXPIRY DATE
IBM Corporation				
IBM 4768 Cryptographic Coprocessor Security Module				
Hardware #: L12 01PP165, L11 01KV353 **Firmware #:** CCA 6.0.xz **Applic #:** View Security Policy	4-20333	3.x	HSM	30 Apr 2026 

Toleration & Migration Maintenance

- APAR OA48403 – Support for PKCS #11 objects in the TKDS (HCR77B1)
  - HCR77B0, HCR77A1, HCR77A0
- APAR OA50707 – Key fingerprint in a KDS record (HCR77C0)
  - HCR77B1, HCR77B0, HCR77A1
- APAR OA52388 – CEX6S support (HCR77C1)
  - HCR77C0 , HCR77B1, HCR77B0, HCR77A1, HCR77A0
- APAR OA55906 – Toleration for CCA 5.4 & CCA 6.1: Triple-length DES keys, ISO-4 PIN blocks, New diversified key support (HCR77C1 with OA55184)
  - HCR77C1, HCR77C0, HCR77B1, HCR77B0,

Configuration and Setup Changes

- APF Authorize CSF.SCSFSTUB
- SAF Access to the keystores
  - ICSF STC needs access at start-up and for a Coordinated Change Master Key
  - Non-coordinated operations (Initialize, Change MK, Refresh, Convert)
    - TSO User driving the panels needs access
    - Batch job needs access

ICSF Always Up – CSF Proc

- SYS1.SAMPLIB(CSF)

  //CSF PROC PRM=00 ...

  //CSFPARM DD DSN=MY.ICSF.PARM(CSFPRM&PRM),DISP=SHR

  - New parms in IEASYSxx
    - ICSFPROC – the name of the ICSF started procedure, in PROCLIB
    - ICSF=xx – the suffix for the ICSF Options member that is referenced by CSFPARM in the started task

    - Don’t forget to disable current auto start (COMMNDxx)
    - AUTOR policy for BCF005A and BCF006A

ICSF Always Up – CSF2 Proc

- SYS1.SAMPLIB(CSF2)

```
//CSF2 PROC PRM=00
//CSF2 EXEC PGM=CSFINIT,PARM=&PRM,REGION=0M,TIME=1440,MEMLIMIT=NOLIMIT
```

  - Store this startup PROC in SYS1.PARMLIB (or another suitable library).
  - HCR77D0 only
  - CSFPARM2 DD is used internally
  - Suffix is passed as PARM
  - Options data set must be a CSFPRMxx member of the PARMLIB concatenation

Automatic Restart

- ARM Policy

```
DATA TYPE(ARM)
DEFINE POLICY NAME(CSFPOL) REPLACE(YES)
RESTART_GROUP(ICSFGROUP)
TARGET_SYSTEM(*)
ELEMENT(SYSICSF_*)
RESTART_METHOD(BOTH,PERSIST)
```

Always Up - Dynamic Service Update

- Without stopping ICSF
  - Activate service
    - SCSFMOD0 – ICSF modules
    - SIEALNKE – CSFINPV2 (validates integrity for FIPS 140-2 compliance)
  - Pick up Options (those that aren't picked up by SETICSF OPTIONS,REFRESH)
  - Recycle – restart without shutting down
- Dynamic Service cannot be used to upgrade the ICSF release
- Dynamic Service update discards all PKCS #11 session objects and they need to be recreated

Dynamic Service Update

- Update ICSF Options data set
  - SERVSCSFMOD0(dsn, volser)
  - SERVSIEALNKE(dsn, volser)
  - SERVICELIBS(YES)
- SETICSF PAUSE
  - ICSF will wait for current requests to complete, monitoring the number of active requests. When the number of active requests hasn't changed for 10 seconds, ICSF will terminate
- Restart ICSF

Operations

- MASTERKCVLEN
  - D ICSF,MKVPS displays the Master Key Verification Patterns and honors the truncation length
  - Honors the truncation of the pattern as specified by MASTERKCVLEN in the Options data set
  - SMF Type 82, Subtype 7 (Operational Key Part Entry)

  - DISPLAY ICSF,MKVPS
    - Display MKVPs from the KDS and crypto devices
  - DISPLAY ICSF,MKVPS,ERRORS
    - Limits the display to devices that have no master key loaded, or the master key does not match the keystore

Triple Length Keys – not just DATA keys anymore

- Requires z13 or later, with November 2018 LIC & OA55184
  - Cipher Class
    - CIPHER/DECIPHER/ENCIPHER
  - MAC Class
    - MAC/MACVER
  - PIN Class
    - PINGEN/PINVER
    - IPINENC/OPINENC
  - Key-encrypting key Class
    - EXPORTER/IMPORTER, IMP-PKA

Some implications of Triple Length Keys

- Control Vectors
  - Left and right key parts are the same
- All new triple-length DES keys are wrapped using Enhanced Wrapping2
  - WRAPECB DEFAULTWRAP Original
  - WRAP-ENH DEFAULTWRAP Enhanced
    - CBC Mode w/SHA-1
  - WRAPENH2 DEFAULTWRAP Enhanced
    - CBC Mode w/SHA-256
- Key Token Generate & Key Token Build APIs – Rule array keyword
  - TRIPLE – triple-length key
  - TRIPLE-O – triple-length key with all three key parts unique

Two New APIs

- Diversify Directed Key
  - Used to generate and derive session keys (a pair of associated keys) using the DK direct key diversification key scheme
  - Key type KDKGENKY
- Encrypted PIN Translate2
  - Reencipher a PIN block from one PIN-encrypting key to another and optionally change the PIN block format
  - New and improved Encrypted PIN Translate API
    - ISO-4 PIN blocks & AES PIN-encrypting keys

CKDS Keys Utility

- List function supports more key types
  - CIPHER (DES)
  - CIPHERXI
  - CIPHERXO
  - CVARENC
  - CVARXCVL
  - CVARXCVR
  - DECIPHER
  - DKGENKY (DES)
  - ENCIPHER
  - IKEYXLAT
  - KDKGENKY
  - OKEYXLAT
  - SECMSG (DES)

PKDS Keys Utility

```
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.
```

Action & Status Characters

- Action Character
  - A – Archive a record
  - D – Delete a record
  - K – Display key attributes and metadata
  - M – Display metadata
  - P – Prohibit Archive
  - R - Recall
- Status Character
  - - Active
  - A Archived
  - I Inactive

Metadata

- Record creation date
- Update date
- **Cryptoperiod start date**
- **Cryptoperiod end date**
- **Date the record was last used**
- Service called when last used
- Date the record was recalled
- Date the record was archived
- **Archived flag**
- **Prohibit archive flag**

PKDS CSFSERV profiles

- CSFBRPK Profile
  - List labels
    - Read access to CSFSERV(CSFKDSL & CSFBRPK)
  - Display attributes & record metadata
    - Read access to CSFSERV(CSFBRPK)
  - Modify metadata
    - Update access to CSFSRV(CSFBRPK)
    - Read access to the label via CSFKEYS
  - Delete records
    - Control access to CSFBRPK
    - Read access to the label via CSFKEYS
  - Archive/recall records
    - Update access to CCSFBRPK
    - Read access to the label via CSFKEYS
- CSFBRPK ALTER – trumps all

APIs used by PKDS Keys Utility

- CSFSERV
  - CSNDKRR
  - CSNDKRC
  - CSNDKRD
  - CSNDPKB
  - CSNDPKG
  - CSNDPKX
  - CSNBOWH
  - CSNDDSG
- CSFKEYS

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
- Token – representation of a security device, such as a smart card reader

Listing tokens and objects

- Token Details panel
  - Data Object Details
  - Certificate Object Details
  - Secret Key Object Details
  - Public Key Object Details
  - Private Key Object Details
  - Domain Parameters Object Details
- Token Management Record Metadata

CSFSERV Class Authority

- CSFSERV CSFBRTK
  - Read access to use the utility
  - Update access to modify metadata
- CSFSERV Read access
  - CSF1GAV – Get object attributes
  - CSF1SAV – Update object attributes
  - CSF1TRC – Token or object creation
  - CSF1TRD – Token or object deletion
  - CSF1TRL – Token or object find

CRYPTOZ Class Authority – Access to tokens

USER.token-name		
User R/O	Read & use public and private objects	READ
Weak User*	Plus create/delete/modify public and private objects	UPDATE
User R/W	Plus add/delete/modify certificate authority objects	CONTROL
SO.token-name		
Weak SO*	Read/create/delete/modify & use public objects	READ
SO R/W	Plus create & delete tokens	UPDATE
Strong SO*	Plus read, but not use private objects; create/ delete/modify private objects	CONTROL

Prefixed CSFSERV and CSFKEYS Profiles

- HCR77D0 introduces support for prefixed profiles
  - z/OS 2.3 with APAR OA54350
- New XFACILIT profiles
  - CSF.PREFIX.CSFKEYS.ENABLED
  - CSF.PREFIX.CSFSERV.ENABLED
- Use RACFVARS to define the system name

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

RDEFINE CSFKEYS &TESTSYS.KEY1 UACC(NONE)
RDEFINE CSFSERV &PRODSYS.CSFKGN* UACC(NONE)
```

- Don’t forget to prefix
  - CSF-CKDS-DEFAULT / CSF-PKDS-DEFAULT
  - CSF-PROTECTED-KEY-TOKEN

Conditional Access List (by API) – OA54350

- Access to the Key based on API
- New XFACILIT profiles
  - CSF.CSFKEYS.CONDITIONAL.ACCESS.CONTROL

PERMIT key-label CLASS(CSFKEYS) ID(user) ACCESS(READ)
WHEN(CRITERIA(SERVICE(sericename1, servicename2,....)

Authority within KGUP

- KGUP Verb Authority
  - XFACILIT CSF.KGUP.VERB.AUTHORITY.CHECK
    - ADD, RENAME, OPKYLOAD — Read Authority
    - DELETE, UPDATE — Update Authority
- KGUP CSFKEYS Authority
  - XFACILIT CSF.KGUP.CSFKEYS.AUTHORITY.CHECK
  - CSFKEYS Profile prefixes are honored

KGUP Verb and Keyword	CSFKEYS Class profile	
	Authority (default)	Authority when Granular Key Access enabled
ADD Verb w/LABEL or RANGE keyword	READ	UPDATE
DELETE/UPDAET verb w/LABEL or RANGE keyword	READ	CONTROL
RENAME Verb w//Label keyword	READ	CONTROL
OPKYLOAD verb w/Label keyword	READ	UPDATE
ADD/UPDATE w/TRANSKEY keyword	READ	READ

KGUP Resource Checks

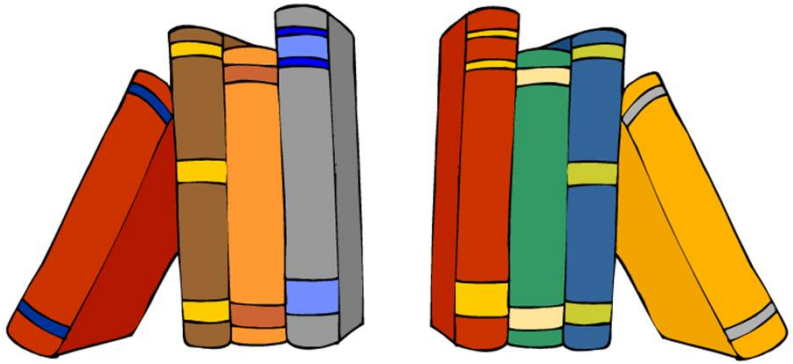
- CSFIQF – ICSF Query Facility
- CSFKIM – Key Import
- CSFKGN – Key Generate
- CSFKGN2 – Key Generate2
- CSFKTR2 – Key Translate2
- CSFRNGL – Random Number Generate Long
- CSFSKI2 – Secure Key Import2
- CSFSKM – Secure Key Import

- CSFOPKL – Operational Key Load (Resource)
- CSFGKF – Generate Key Fingerprint (Resource)

Resource names

Descriptive service name	CCA entry point names		ICSF entry point names		SAF resource name	Callable service exit name
	31-bit	64-bit	31-bit	64-bit		
Authentication Parameter Generate	CSNBAPG	CSNEAPG	CSFAPG	CSFAPG6	CSFAPG	CSFAPG
Ciphertext Translate2	CSNBCTT2	CSNECTT2	CSFCTT2	CSFCTT26	CSFTT2	CSFCTT2
Ciphertext Translate2	CSNBCTT3	CSNECTT3	CSFCTT3	CSFCTT36	CSFCTT3	CSFCTT3
.....						
Clear PIN Encrypt	CSNBCPE	CSNECPE	CSFCPE	CSFCPE6	CSFCPE	CSFCPE
.....						

References



- Announcment Letters
  - 118-075 http://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/5/897/ENUS118-075/index.html&lang=en&request_locale=en
- 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
  - GI11-9478-07 Program Directory for Cryptographic Services for z/OS V2R2 – z/OS V2R3
  - SA23-2211-08 ICSF Trusted Key Entry Workstation User's Guide

On the Web

- Techdocs – www.ibm.com/support/techdocs
  - TD103782 – z/OS: ICSF Version and FMID Cross Reference
  - Or search on 'Crypto'
- z/OS Downloads – Cryptographic Support Downloads
  - https://www.ibm.com/servers/resourcelink/svc00100.nsf/pages/zosDownloads?OpenDocument
- Crypto Cards
  - https://www.ibm.com/security/cryptocards

Questions