MAINFRAME CRYPTO

Unscrambling the Complexity of Crypto!

Crypto Update
An Alternative View

Greg Boyd

gregboyd@mainframecrypto.com

November 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

- HCR77D2
- HCR77D1

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

FMID	External Name	Applicable z/OS Releases	Availa-bility	Planned EoS	Supported Servers
HCR77C0	Cryptographic Support for z/OS V2R1 – z/OS V2R2	z/OS V2.2; z/OS V2.1	Oct 2016	TBD	z9; z10; z196/z114; zEC12/zBC12; z13/z13s; z14/z14R1**,z15**
	z/OS 2.3	z/OS V2.3	Sep 2017	TBD	
HCR77C1	Cryptographic Support for z/OS V2R1 – z/OS V2R3	z/OS V2.3; z/OS V2.2; z/OS V2.1	Sep 2017	TBD	z9; z10; z196/z114; zEC12/zBC12;z13;z14, z15**
HCR77D0	Cryptographic Support for z/OS V2R2 – z/OS V2R3	z/OS 2.2; z/OS V2.3	Dec. 2018	TBD	z10; z196/z114; zEC12/zBC12;z13;z14,z15**
	z/OS 2.4	z/OS 2.4	Oct 2019	TBD	
HCR77D1	Cryptographic Support for z/OS V2R2 – z/OS V2R4	z/OS V2.2; z/OS V2.3	Sept 2019	TBD	z10; z196/z114; zEC12/zBC12;z13;z14,z15
HCR77D2	Cryptographic Support for z/OS V2R5	z/OS 2.5	Sept. 2021	TBD	z13, z13s; z14, z14 ZR1; z15

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

Adapted from: https://www.ibm.com/support/pages/zos-icsf-version-and-fmid-cross-reference

HCR77D2

Common Record Format Large (KDSRL)
Common Record Format (KDSR)

- aka KDSR – Key Data Set Reformat
- Support longer keys
- Metadata fields
  - Fixed-length fields
  - Variable-length fields
    - Tag
    - Length
    - Data
- Conversion to either KDSR or KDSRL
  - ICSF Panels (under KDS Management CSFMKM10 panel)
  - Coordinated KDS Administration (CSFCRC) API

Keystore Data Set Definitions

- CKDS – Cryptographic Key Data Set
  - RECORDSIZE(372,32756) – HCR77D2 KDSRL format
  - RECORDSIZE(372,2048) – HCR77A1 KDSR format
  - RECORDSIZE(332,1024) – HCR7780 support HMAC variable length keys
  - RECORDSIZE(252,252) – pre HCR7780
- PKDS – PKA Key Data Set
  - RECORDSIZE(800,32756); DATA CISZ(32768) – HCR77D2 KDSRL
  - RECORDSIZE(800,3800); DATA CISZ(8192) – HCR77A1 KDSR format
  - RECORDSIZE(350,3800) – HCR7750 support longer RSA 4096-bit keys
  - RECORDSIZE(350,2800) – pre HCR7750*
- TKDS – Token Key Data Set
  - RECORDSIZE(2200,32756); DATA CISZ(32768) – HCR77D2 KDSRL
  - RECORDSIZE(2200,32756)

*HCR77B1 and earlier versions are no longer supported

KDSR Format (HCR77A1)

- Metadata
  - Reference date (STCKE & yyyymmdd format)
  - Additional metadata (w/HCR77B0)
    - Key material validity start date
    - Key material validity end date
    - Record archive flag
    - Record archive date
    - Record recall date
    - Record prohibit archive flag
    - Installation user data
    - Key fingerprint

KDSRL Format (HCR77D2)

- New IBM metadata fields
  - Last used Service Name
  - Last used class reference date
    - Tracked by TrackClassUsage
      - DD - DATADEC
      - DE - DATAENC
- TRACKCLASSUSAGE(class1,class2) – new ICSF Option
  - DATADEC
  - DATAENC
  - Reference day tracking must be enabled (KDSREFDAYS>0)

PKDS support for QSA keys

- APIs
  - PKDS Key Record Create (CSNDKRC and CSNFKRC)
  - PKDS Key Record Delete (CSNDKRD and CSNKFRD)
  - PKDS Key Record Read/ Read2 (CSNDKRR/CSNDKRR2 and CSNFKRR/CSNFKRR2)
  - PKDS Key Record Write (CSNDKRW and CSFNFKRW)
- Requires KDSRL format PKDS
  - RC=8, RS=x'DDF' (3551) if LRECL is too short
- QSA Private key protected by ECC-MK
- PKDS Keys Utility

New Key Store Policy Controls

- Archived key for Data Decryption Use Control
  - XFACILIT profile CSF.KDS.KEY.ARCHIVE.DATA.DECRYPT
    - Allows a key with the ARCHIVE flag on, to be used, but only for decrypt operations
    - CKDS & TKDS; does not apply to PKDS

Control	Encrypt	Decrypt	Key Record Read2
CSF.KDS.KEY.ARCHIVE.USE	RC=8 (RC indicating archived)	RC=8 (RC indicating archived)	RC=8 RS=x'D10' (3344)
CSF.KDS.KEY.ARCHIVE.DATA.DECRYPT	RC=8, RS=x'D5E' (3422)	RC=0	RC=0, RS=x'D5F' (3423)

- CSFKEYS PKA ECC token private-key name checking control
  - XFACILIT profile CSF.CSFKEYS.ECC.PRIVATEKEYNAME.ENABLE

XFACILIT CSF.WRAPENH3.OVERRIDE

- DES Key Wrapping
  - ORIGINAL – WRAP-ECB Mode wrapping
  - ENHANCED – WRAP-ENH
    - HCR7780
    - SHA-1 based derivation key, CBC Mode
    - ANSI X9.24
  - WRAPENH2
    - HCR77C1 with APAR OA55184
    - SHA-256
  - WRAPENH3 -
    - OA60318 (back to z/OS V2.2) per z/OS 2.5 announcement letter
    - SHA-256 HMAC
- CSFCNV2 – utility to convert
- This new XFACILIT profile allows programs that use the WRAP-ENH API rule to default to WRAPENH3, instead of WRAPENH2

Regional Cryptographic Servers

- Removed CCA Support for Regional Cryptographic Servers
  - SOD in Announcement Letter 220-378 z/OS V2.4 3Q 2020 New Functions and Enhancements
  - SOD in Announcement Letter 221-213 z/OS V2.4 2Q 2021 Enhancements
- PKCS #11 Support still available

HCR77D1

z15 Hardware Support

- CPACF
  - New Compute Digital Signature Authentication (KDSA) instruction - Clear key ECC support
  - Protected key support for Elliptic Curve keys
- CEX7S
  - Single Port and Dual Port cards
  - EP11 Mode support for PKCS #11 v2.4 standard
  - QSA Support (PKCS #11 only)
  - Designed for 2X Performance improvement as a CCA card
  - Designed for 3X Performance improvement as an accelerator
  - Protected key support for Elliptic Curve keys

Crystals - Dilithium

- Crystals – Cryptographic Suite for Algebraic Lattices
- A lattice of numbers
  - Start with a list of 5 numbers
  - Add 3 of them together
  - Give you that sum
  - Can you figure out which 5 numbers I used?
- What if the list had a thousand numbers, each with thousands of digits and you have to pick 500?

HCR77D1 (and HCR77D0 via APAR OA57089)

- ANSI TR-34 Remote Key Loading
- PCI-HSM Compliance for AES & RSA keys
- New PIN APIs for DK Customers

New Subtype 49 (SMF Type 82)

- Master key event resulted in a new master key value being promoted to current
  - Name of the system that wrote the record
  - Event flags
  - KDS Name
  - KDS Type
  - Serial Numbers (of Coprocessors) affected
  - MKVPs affected (AES, DES, ECC, RSA, P11)
  - Domain affected
  - TOD (STCKE format)

New Health Checks

- ICSF_PKCS_PSS_Support
  - Detects whether the current hardware config supports PKCS-PSS algorithms
  - RSA-PSS signatures rely on keys that are (must be) protected by the ECC-MK, not the RSA-MK
  - RACDCERT command with RSA(PKDS) will fail for such a key, if the ECC-MK is not loaded
- ICSF_WEAK_CCA_KEYS
  - Lists the labels of records in the PKDS with keys that are cryptographically weak
    - Modulus size < 1024-bits
    - Process all keys (Archived or Inactive as well as Active keys)

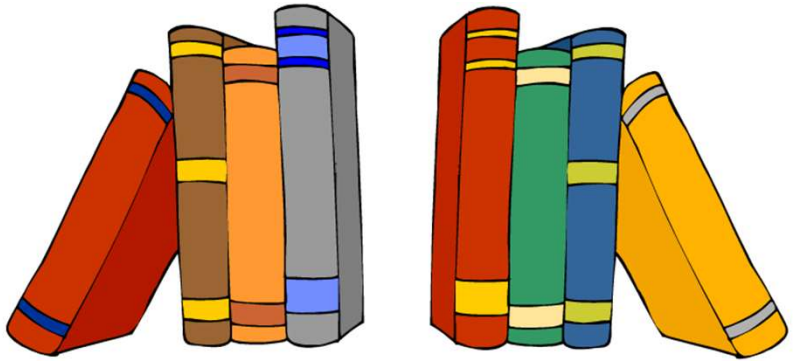
Deprecated callable services

Old API	New API
Clear key Import (CSNBCKI/CSNECKI)	Multiple Clear Key Import (CSNBCKM/CSNECKM)
Key Translate (CSNBKTR/CSNEKTR)	Key Translate2 (CSNBKTR2/CSNEKTR2)
Prohibit Export (CSNBPEX/CSNEPEX)	Restrict Key Attribute (CSNBKRA/CSNEKRA)
Prohibit Export Extended (CSNBPEXX/CSNEPEXX)	Restrict Key Attribute (CSNBKRA/CSNEKRA)
Secure Key Import (CSNBSKI/CSNESKI)	Multiple Secure Key Import (CSNBSKM/CSNESKM)
Decode (CSNBDCO/CSNEDCO)	Symmetric Key Decipher (CSNBSYD/CSNBSYD1/CSNESYD/CSNESYD1)
Encode (CSNBECO/CSNEECO)	Symmetric Key Encipher (CSNBSYE/CSNBSYE1/CSNESYE/CSNESYE1)
Encrypted PIN Translate (CSNBPTR/CSNEPTR)	Encrypted PIN Translate2 (CSNBPTR2/CSNEPTR2)

Announcement Letters

- 121-029 z15
  - https://www.ibm.com/downloads/cas/US-ENUS121-029-CA/name/US-ENUS121-029-CA.PDF
- 118-075 z14
  - https://www.ibm.com/common/ssi/rep_ca/5/897/ENUS118-075/ENUS118-075.PDF
- 221-260 z/OS V2.5
  - https://www.ibm.com/downloads/cas/US-ENUS221-260-CA/name/US-ENUS221-260-CA.PDF
- 221-213 z/OS V2.4 2Q 2021
  - https://www.ibm.com/downloads/cas/US-ENUS221-213-CA/name/US-ENUS221-213-CA.PDF
- 220-378 z/OS V2.4 3Q 2020
  - https://www.ibm.com/downloads/cas/US-ENUS220-378-CA/name/US-ENUS220-378-CA.PDF

References



- IBM Manuals
  - SC14-7505 ICSF Overview
  - SC14-7506 ICSF Administrator's Guide
  - SC14-7507 ICSF System Programmer's Guide
  - SC14-7508 ICSF Application Programmer's Guide
  - SC14-7509 ICSF Messages
  - SC14-7510 ICSF Writing PKCS #11 Applications
  - GI11-9478-08 Program Directory for Cryptographic Services for z/OS V2R2 – z/OS V2R4
  - SA23-2211 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