MAINFRAME CRYPTO

Unscrambling the Complexity of Crypto!

ICSF

Part 1 of 2

Greg Boyd

www.mainframecrypto.com

THE Z EXCHANGE

February 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

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

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

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

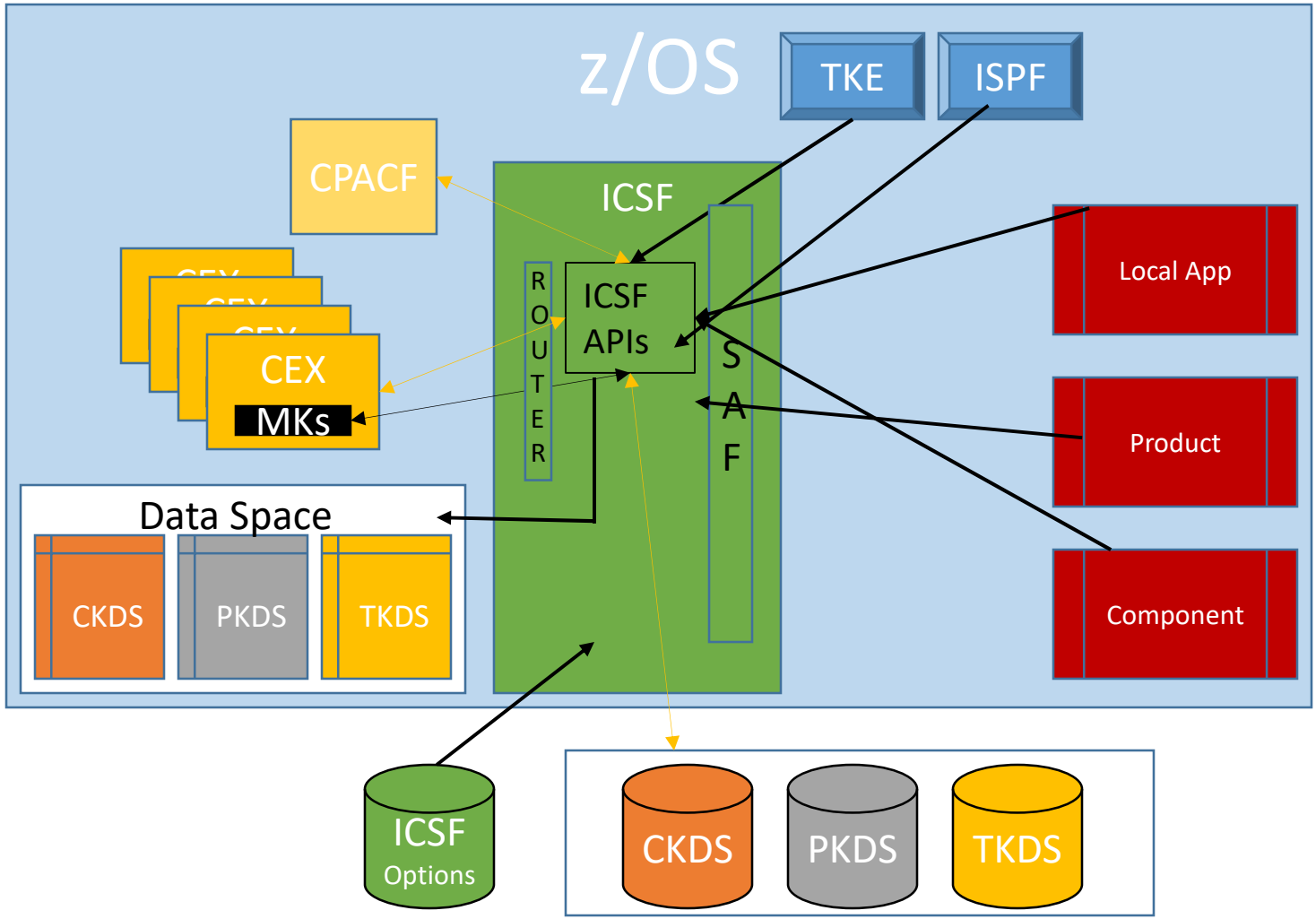
ICSF Levels

- HCR77D1
  - z15 and CEX7S Exploitation, including Quantum Safe algorithms
  - ANSI TR-34 support
  - New health check for Probabilistic Signature Scheme (PSS) support
  - New PIN services for DK support
- HCR77D0
  - Dynamic maintenance
  - ICSF start-up early in IPL
  - Dynamic Browser for PKDS
  - New triple-length key types
  - DK Key Diversification
  - ChaCHa20 & Poly1305 algorithms
  - ISO-4 PIN block support

ICSF Levels

- HCR77C1
  - z14 and CEX6S exploitation, including SHA-3 hashing, a True Random Number Generator and AES-GCM performance improvements
  - PCI-HSM Compliance
  - ICSF Counters
  - CKDS Keys Browser
- HCR77C0
  - More auditing
  - Options Data set refresh
  - GA2 support for CEX5S

ICSF Started Task



SYS1.SAMPLIB(CSF)

```
//CSF PROC
//CSF EXEC PGM=CSFINIT,REGION=0M,TIME=1440,MEMLIMIT=NOLIMIT
//* When using CSFPARM DD, the installation options data set must be
//* a partitioned data set on systems running HCR77D0 or later.
//CSFPARM DD DSN=USER.PARMLIB(CSFPRM00),DISP=SHR
```

- 'S CSF' from the console or in COMMNDxx or Auto Operations
- 'S CSF,SUB=MSTR' (to start it before JES)
- 'START CSF,SUB=MSTR,REUSASID=YES' (to reuse the ASID)

- P CSF or FORCE CSF,ARM to stop the ICSF address space
  - After omvs is stopped (to allow update to an encrypted file system to complete)
  - After JES is shutdown, if encrypting JES spool data sets

ICSF Always Up – CSF Proc w/OA55378

- OA55378 (for z/OS 2.3) introduced support to start ICSF via a RIM
- 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
- SYS1.SAMPLIB(CSF)

```
//CSF PROC PRM=00
 …
//CSFPARM DD DSN=USER.PARMLIB(CSFPRM&PRM),DISP=SHR
```

  - AUTOR policy for BCF005A and BCF006A
  - See http://www.ibm.com/support/docview.wss?uid=isg1OA55378
  - Don't forget to disable current auto start (COMMNDxx or AutoOps)

SYS1.SAMPLIB(CSF2) (HCR77D0)

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

- CSFPARM2 DD is used internally
- Options data set must be a CSFPRMxx member of the PARMLIB concatenation
- ICSFPROC=CSF2 in IEASYSxx

CSF Started Task

- SAF access to the Options data set and the keystores (if specified)
  - Assign a userid via the Started-procedures table (ICHRIN03)
  - Assign an omvs segment, IF using Regional Cryptographic Servers

- ARM Policy

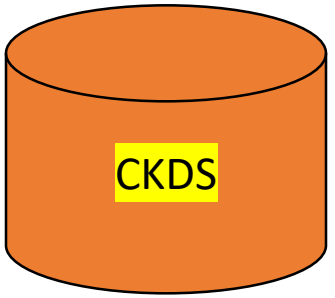
  DATA TYPE(ARM)
  DEFINE POLICY NAME(CSFPOL) REPLACE(YES)
  RESTART_GROUP(ICSFGROUP)
  TARGET_SYSTEM(*)
  ELEMENT(**SYSICSF_***)
  RESTART_METHOD(BOTH,PERSIST)

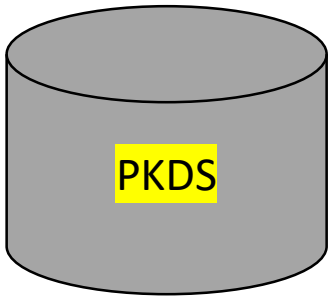
ICSF Options

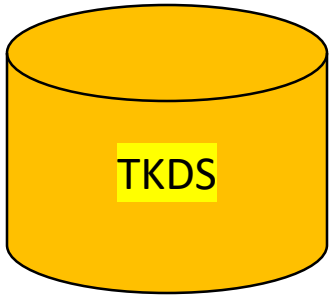
- Data set
  - PARMLIB, PDS or Sequential file
  - PARMLIB (only with HCR77D0)
  - System Variables
- Contents
  - CKDSN, PKDSN, TKDSN
    - SAF protect them!
  - DOMAIN(n)
  - First time start-up
    - SSM(YES)
    - COMPAT(NO)

Key Stores

- CKDS – Cryptographic Key Data Set
  - AES keys
  - DES/TDES keys
- PKDS – PKA Key Data Set
  - ECC keys
  - RSA keys
  - Trusted PIN Blocks
- TKDS – Token Key Data Set
  - Cryptographic Objects (AES, DES/TDES, ECC, RSA keys in a PKCS #11 format or architecture)







Keystore Data Set Definitions

- CKDS – Cryptographic Key Data Set
  - RECORDSIZE(252,252) – pre HCR7780
  - RECORDSIZE(332,1024) – optional beginning with HCR7780 for HMAC variable length keys
  - RECORDSIZE(372,2048) – optional beginning with HCR77A1 (KDSR format)
- PKDS – PKA Key Data Set
  - RECORDSIZE(350,2800) – pre HCR7750*
  - RECORDSIZE(350,3800) – HCR7750 to HCR77A0 (longer RSA keys)
  - RECORDSIZE(800,3800) – HCR77A1 and later (KDSR format)
- TKDS – Token Key Data Set
  - RECORDSIZE(2200,32756)

*HCR77B1 and earlier versions are no longer supported

KDSR Format (HCR77A1)

- Metadata (up to 250 bytes)
  - REFDATE STCKE – Store Clock Extended Timestamp
  - REFDATE - yyyymmdd
  - Additional metadata (w/HCR77B0)
    - Validity Dates - yyyymmdd
      - Start Date - Key material can't be used before the start date
      - End Date - Key material can't be used after the end date
      - **Last reference date**
      - Archive & Recall dates
    - IBM & installation metadata blocks
- CSFKDSL Key Data Set List API can search for records based on the metadata
- SMF Type 82 Subtype 30 Keystore Policy Archived and Inactive Checking
- KEYARCHMSG ICSF Option – generate a message when an archived key is referenced

Key Labels – VSAM KSDS Index

- CKDS
  - Key label (64 characters*)
  - Key type (8 bytes)**
    - DATA, CIPHER, PINGEN/PINVER, OPINENC/IPINENC, EXPORTER/IMPORTER, MAC …
- PKDS
  - Key label (64 characters*)
  - Reserved (8 bytes)
- TKDS
  - Token name (32 characters)
  - Sequence number (8 bytes, in EBCDIC)
  - Category (1 byte) - ‘T’ for clear, ‘Y’ for secure, blank for token, … || 3 blanks
  - 28 bytes of binary 0s

- * - 1 Alphabetic or National and Up to 63 Alphanumeric, national or period; Left-justified, padded with blanks
- ** - Left-justified, padded with blanks

Always Up - Dynamic Service Update
(HCR77D0)

- Without stopping ICSF
  - Activate new service
    - SCSFMOD0 – ICSF modules
    - SIEALNKE – CSFINPV2 (validates integrity for FIPS 140-2 compliance)
  - Recycle – restart without shutting down
  - Pick up Options (those that aren't picked up by SETICSF OPTIONS,REFRESH)
- 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 (HCR77D0)

- Update ICSF Options data set
  - SERVICELIBS(YES/**NO**)
  - SERVSCSFMOD0(dsn, volser)
  - SERVSIEALNKE(dsn, volser)
- 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
  - After CSFM401I CRYPTOGRAPHY - SERVICES ARE NO LONGER AVAILABLE message

STATS & STATSFILTER (HCR77C1)

- ICSF Options
  - STATS(ENG,SRV,ALG)
    - ENG – track cryptographic engines
    - SRV – track cryptographic services
    - ALG – track cryptographic algorithms
  - STATSFILTER – level of aggregation (for high volume apps)
- SMF Type 82 Subtype 31
  - The jobs and tasks that are using the various cryptographic engines.
  - The cryptographic card types that are getting the most requests.
  - If any cryptographic requests are being handled in software.
  - The peak periods of cryptographic usage.
  - The ICSF services that are being started by other z/OS components.
  - The jobs and tasks that are using out-of-date algorithms or key sizes.

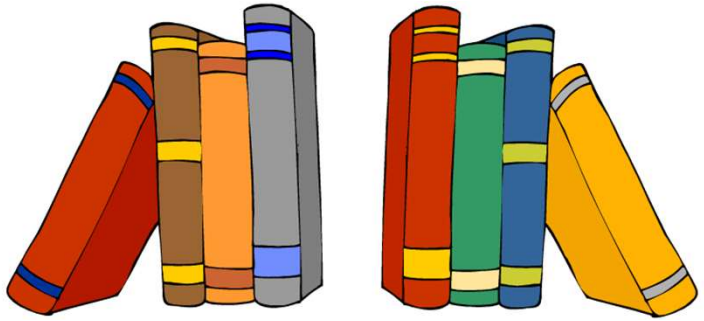
Cryptographic Key Usage Statistics

Subtype=001F Crypto Usage Statistics
Written periodically to record crypto usage counts
7 Mar 2018 11:30:30.00
TME... 003F3798 DTE... 0118066F SID... MFC1 SSI... 00000000 STY... 001F
INTVAL_START.. 03/07/2018 16:20:30.000330
INTVAL_END.... 03/07/2018 16:30:30.000548
USERID_AS..... GBOYD
USERID_TK.....
JOBID..... TSU13812
JOBNAME..... BOYDG
JOBNAME2.....
PLEXNAME..... MFCPLEX
DOMAIN..... 12
ENG...CARD...5C01/DV53K342... 50
ENG...CARD...5C03/DV53G424... 50
ENG...CPACF... 100
ALG...AES256..... 200
SRV...CSFSYE..... 100
SRV...CSFSAD..... 100

Performance Monitoring

- RMF
  - Crypto Hardware Activity Report
    - RMF Processor Activity (SMF Type 70, Subtype 2)
  - RMF Monitor III
    - CRYOVW – Crypto hardware overview (CRO)
    - CRYACC – Crypto accelerator activity (CRA)
    - CRYPKC – Crypto PKCS11 coprocessor activity (CRP)
  - RMF Overview Report (Type 70, Subtype 1)
    - OVW(ENCRMSU(LACSCR))
  - Workload Activity (SMF Type 72, Subtype 3)
    - Samples the TCBs executing and waiting on Crypto APs
- CPU Measurement Facility
- ICSF STATS

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