The z Exchange

ICSF

Greg Boyd

www.mainframecrypto.com
Copyrights and Trademarks

• Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 10 years

• Copyright © 2015 Greg Boyd, Mainframe Crypto, LLC. All rights reserved.

• 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

• What is ICSF
• Key repositories & Verification Patterns
• ICSF Setup &Parms
• Other ICSF ‘stuff’ (Panels, Healthchecks & SMF)
• Keys, Control Vectors & Tokens
• APIs
• SAF and Security Policies
ICSF Install

• New Install? Or upgrade?
• Are there any keys in the keystores? If so, is there any data encrypted under those keys?
• If so, do you know what the master keys are? Do you have the Passphrase? Or the key parts?
ICSF Setup and Usage

1) Check ICSF Versions; Check for APARs
2) PARMLIB Authorizations
3) Define Keystore Data Sets
4) Define the Started Task
5) Specify Options
6) Panel Access
7) Security Access
8) Start ICSF & Master Key Entry
9) Post-Install Adjustments

More specifically We are here
5) Create the Options data set

- Must specify CKDS & PKDS, TKDS is optional
  - CKDS(ckds), PKDS(pkds)
  - TKDS(tkds)
- May require Usage Domain, depending on the LPAR Activation profile
  - DOMAIN(n)
- Must specify SSM(YES), COMPAT(NO) for first-time start-up
  - SSM(YES) – for first time start-up
  - COMPAT(NO)
- Can use System Variables
5) Options - SYPSLEX KDS Sharing

- SYSPLEXCKDS(YES/NO,FAIL(YES/NO))
- SYSPLEXPKDS(YES/NO,FAIL(YES/NO))
- SYSPLEXTKDS(YES/NO,FAIL(YES/NO))

If you are sharing the keystore, then you must tell ICSF via the Options, so he can coordinate changes.

Caution when sharing a keystore between multiple levels of ICSF – Compatibility APARs may be required
5) Options – Performance

- **CHECKAUTH(YES/NO)** – Bypass SAF checks for supervisor state/system key callers
- **HDRDATE(YES/NO)** – control frequency of updates to timestamp in header record
- **RNGCACHE(YES/NO)** – tells ICSF whether to maintain a cache of random numbers
- **KDSREFDAYS(n)** – control frequency of key reference date in individual key records
  - 0 – no updates
  - 1-30
- **KEYAUTH(YES/NO)** – Check MAC on read from dataspace
  - Deprecated in HCR77A1
- **CKTAUTH(YES/NO)** – Check MAC on read from keystore
  - Deprecated in HCR77A1
5) Options - Other

- EXIT(ICSF Name, Load Module Name, FAIL(option))
- SERVICE(Service Number, Load Module Name, FAIL(option))
- UDX(UDX ID, Service Number, ‘Comment’, Fail(option))
- KEYARCHMSG(YES/NO) – tells ICSF to generate a message if an app references an archived key record
- UDX(UDX ID, Service Number, load module name, ‘Comment’, Fail(YES/NO)) – defines the UDX to ICSF
- WAITLIST(data set name) – list of APIs that are executed on the CEX card
- FIPSMODE(YES/NO/COMPAT,FAIL(YES/NO))
5) Options - CTRACE PARMLIB member

- New with HCR77A1, there is the ability to customize trace data that ICSF captures
- The trace options are defined in CTICSF00 which is installed in SYS1.PARMLIB as part of the HCR77A1 install
- Either customize CTICSF00 (the defaults are acceptable to start) or point to CTRACE(CTICSFxx) in the Options data set
- The old TRACEENTRY option has been deprecated and will be ignored after generating CSFO0212 message
Displaying the options

<table>
<thead>
<tr>
<th>OPTION</th>
<th>CURRENT VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHECKAUTH</td>
<td>RACF check authorized callers</td>
</tr>
<tr>
<td>COMPAT</td>
<td>Allow CUSP/PCF compatibility</td>
</tr>
<tr>
<td>CTRACE</td>
<td>CTRACE parmlib used at ICSF startup</td>
</tr>
<tr>
<td>DEFAULTWRAP</td>
<td>Default symmetric key wrapping – internal</td>
</tr>
<tr>
<td>DEFAULTWRAP</td>
<td>Default symmetric key wrapping – external</td>
</tr>
<tr>
<td>DOMAIN</td>
<td>Current domain index or usage domain index</td>
</tr>
<tr>
<td>FIPSMODE</td>
<td>Operate PKCS #11 in FIPS 140-2 mode</td>
</tr>
<tr>
<td>HDRDATE</td>
<td>Update the header record for all I/O ops</td>
</tr>
<tr>
<td>KDSREFDAYS</td>
<td>Number of days between reference updates</td>
</tr>
<tr>
<td>KEYARCHMSG</td>
<td>Message for archived KDS record reference</td>
</tr>
<tr>
<td>MAXSESSOBJECTS</td>
<td>Max non-authpgm PKCS #11 session objects</td>
</tr>
<tr>
<td>REASONCODES</td>
<td>Source of callable service reason codes</td>
</tr>
<tr>
<td>RNGCACHE</td>
<td>Random Number Generate cache enabled</td>
</tr>
<tr>
<td>SSM</td>
<td>Allow Special Secure Mode</td>
</tr>
<tr>
<td>SYSPLEXCKDS</td>
<td>SYSPLEX Consistency for CKDS Updates</td>
</tr>
<tr>
<td>SYSPLEXPKDS</td>
<td>SYSPLEX Consistency for PKDS updates</td>
</tr>
<tr>
<td>SYSPLEXTKDS</td>
<td>SYSPLEX Consistency for TKDS Updates</td>
</tr>
<tr>
<td>USERPARM</td>
<td>User specified parameter data</td>
</tr>
<tr>
<td>WAITLIST</td>
<td>Source of CICS Wait List if CICS installed</td>
</tr>
</tbody>
</table>

Select ICSF option 3, OPSTAT from Main Panel.
Select option 1 OPTIONS, to display installation options.

Active CKDS: CSF.PROD.CKDS
Active PKDS: CSF.PROD.PKDS
Active TKDS: CSF.PROD.TKDS
6) ISPF Access to ICSF Libraries

• Add ISPF Libraries in TSO Logon PROC or provide a REXX EXEC/CLIST or LIBDEF to allocate them dynamically

• ISPF Panel access (add panel option or REXX/CLIST)
7) SAF Authorization

• Protect the ICSF Libraries (including the keystores)
• Protect Keys
• Protect Services (APIs) including KGUP
• Protect ISPF panels
8) Start ICSF and Load the Master Keys

- On first time start-up of ICSF on new hardware, the master keys will not be loaded, and ICSF will tell you so via CSFM124I
  - Loading the master keys will initialize the keystores
- On first time start-up of a new version of ICSF on current hardware (with master keys loaded) you should see CSFM129I; if you see CSFM123E then the master key in the hardware does not match the master key that was used to initialize the keystore
  - Either point to the correct keystores or
  - Load the master keys that match the keystores
8) Start up messages

CSFM124I MASTER KEY P11 ON CRYPTO EXPRESS4 COPROCESSOR SPxx, SERIAL NUMBER nnnnnnnnn, IS CORRECT.

CSFM129I MASTER KEY DES ON CRYPTO EXPRESS4 COPROCESSOR SCxx, SERIAL NUMBER nnnnnnnnn, IS CORRECT.

CSFM129I MASTER KEY AES ON CRYPTO EXPRESS4 COPROCESSOR SCxx, SERIAL NUMBER nnnnnnnnn, IS CORRECT.

CSFM129I MASTER KEY RSA ON CRYPTO EXPRESS4 COPROCESSOR SCxx, SERIAL NUMBER nnnnnnnnn, IS CORRECT.

CSFM129I MASTER KEY ECC ON CRYPTO EXPRESS4 COPROCESSOR SCxx, SERIAL NUMBER nnnnnnnnn, IS CORRECT.

CSFM111I CRYPTOGRAPHIC FEATURE IS ACTIVE. CRYPTO EXPRESS4 COPROCESSOR SCxx, SERIAL NUMBER nnnnnnnnn.

CSFM111I CRYPTOGRAPHIC FEATURE IS ACTIVE. CRYPTO EXPRESS4 COPROCESSOR SPxx, SERIAL NUMBER nnnnnnnnn.

CSFM132I SECURE KEY PKCS11 SERVICES AVAILABLE.

CSFM400I CRYPTOGRAPHY - SERVICES ARE NOW AVAILABLE.

CSFM130I CRYPTOGRAPHY - RSA SERVICES ARE AVAILABLE.

CSFM130I CRYPTOGRAPHY - ECC SERVICES ARE AVAILABLE.
9) Post install customization

• Change Options if appropriate
  • SSM MODE
    • It might be appropriate to run SSM(NO) in production and SSM(YES) in test and development environments
  • COMPAT MODE
    • Only if you need to support old PCF/CUSP environments should you switch to COMPAT(YES)
ICSF Main Panel

HCR77B0 --------------- Integrated Cryptographic Service Facility-----------
OPTION ===> 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 Master and Operational Key processing
8. KGUP - Key Generator Utility processes
9. UDX MGMT - Management of User Defined Extensions

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
Master Key Entry

• Passphrase Initialization
  • PPINIT (Option 6) on the ICSF Main Menu
  • Provide a 16 to 64 character Passphrase which is used to calculate master key material
  • Only used for ICSF initialization, can’t be used to ‘change’ master keys

• ICSF Panel Entry
  • Coprocessor Management (Option 1) on the ICSF Main Menu
  • Forces split knowledge (minimum of two key parts)
  • Can be used to initialize the environment or to ‘change’ master keys

• Trusted Key Entry Workstation
  • Most secure way to load master key material
  • Still requires using the panels to finish the process – ICSF Option 7
ICSF Coprocessor Management Panel – HCR77B0

**CSFCMP00**  -------------------  ICSF Coprocessor Management  -------------------

**COMMAND =>**

Select the coprocessors to be processed and press ENTER.

Action characters are: A, D, E, K, R, and S. See the help panel for details.

<table>
<thead>
<tr>
<th>Crypto Feature</th>
<th>Serial Number</th>
<th>Status</th>
<th>AES</th>
<th>DES</th>
<th>ECC</th>
<th>RSA</th>
<th>P11</th>
</tr>
</thead>
<tbody>
<tr>
<td>__5A01</td>
<td>__</td>
<td>ACTIVE</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>__5C02</td>
<td>24778902</td>
<td>ACTIVE</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>__5C05</td>
<td>98001236</td>
<td>ACTIVE</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>__5C06</td>
<td>97006090</td>
<td>Master key incorrect</td>
<td>U</td>
<td>C</td>
<td>U</td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>__5C12</td>
<td>97006094</td>
<td>ACTIVE</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>__5A13</td>
<td>__</td>
<td>OFFLINE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>__5P14</td>
<td>97006062</td>
<td>ACTIVE</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Master Key Status

- A Active
- U Uninitialized
- C Correct
- E Error
- I Ignored
- - Not supported
## Coprocessor Hardware Status

### CSFCMP40 - ICSF - Coprocessor Hardware Status

<table>
<thead>
<tr>
<th>Command</th>
<th>SCROLL</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAGE</td>
<td></td>
</tr>
</tbody>
</table>

**CRYPTO DOMAIN: 2**

<table>
<thead>
<tr>
<th>REGISTER STATUS</th>
<th>COPROCESSOR 5C05</th>
<th>COPROCESSOR 5C06</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Crypto Serial Number</strong></td>
<td>98001236</td>
<td>97006090</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>ACTIVE</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

**AES Master Key**

- **New Master Key register**: EMPTY
- **Verification pattern**: 
- **Old Master Key register**: EMPTY
- **Verification pattern**: 

**Current Master Key register**: VALID

- **Verification pattern**: F03CF42DB933BF1E
### Coprocessor Hardware Status

**CSFCMP40 **

<table>
<thead>
<tr>
<th>REGISTER STATUS</th>
<th>COPROCESSOR 5C05</th>
<th>COPROCESSOR 5C06</th>
</tr>
</thead>
</table>

**DES Master Key**

- **New Master Key register**: EMPTY
- **Verification pattern**: :
- **Hash pattern**: :
- **Old Master Key register**: EMPTY
- **Verification pattern**: :
- **Hash pattern**: :
- **Current Master Key register**: VALID
- **Verification pattern**: E9572EFFDAA14AA8
- **Hash pattern**: DD20A717C842FC0C
  - 5D018950FEB7F9B4
### Coprocessor Hardware Status (cont.)

<table>
<thead>
<tr>
<th>CSFCMP40</th>
<th>ICSF – Coprocessor Hardware Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMAND</td>
<td>SCROLL ==&gt; PAGE</td>
</tr>
</tbody>
</table>

**REGISTER STATUS**

<table>
<thead>
<tr>
<th>COPROCESSOR 5C05</th>
<th>COPROCESSOR 5C06</th>
</tr>
</thead>
</table>

**ECC Master Key**

- **New Master Key register**: EMPTY
  - Verification pattern: 
  - Hash pattern: 
- **Old Master Key register**: EMPTY
  - Verification pattern: 
  - Hash pattern: 
- **Current Master Key register**: EMPTY
  - Verification pattern: 
  - Hash pattern: 

---

*Page 24, July 2015*
### Coprocessor Hardware Status (Option 1, Show ... cont.)

<table>
<thead>
<tr>
<th>REGISTER STATUS</th>
<th>COPROCESSOR 5C05</th>
<th>COPROCESSOR 5C06</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA Master Key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Master Key register</td>
<td>EMPTY</td>
<td>EMPTY</td>
</tr>
<tr>
<td>Verification pattern</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash pattern</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Old Master Key register</td>
<td>EMPTY</td>
<td>EMPTY</td>
</tr>
<tr>
<td>Verification pattern</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash pattern</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current Master Key register</td>
<td>VALID</td>
<td>VALID</td>
</tr>
<tr>
<td>Verification pattern</td>
<td>15D7602B7CD493BC</td>
<td>15D7602B7CD493BC</td>
</tr>
<tr>
<td>Hash pattern</td>
<td>A7709D4956FEFEEB</td>
<td>A7709D4956FEFEEB</td>
</tr>
</tbody>
</table>
HealthChecks

- ICSFMIG7731_ICSF_RETAINED_RSAKEY
- ICSFMIG_DEPRECATED_SERV_WARNINGS
- ICSFMIG77A1_CCA_COPROCESSOR_ACTIVE
- ICSFMIG77A1_UNSUPPORTED_HW
- ICSFMIG77A1_TKDS_OBJECT
- ICSF_COPROCESSOR_STATE_NEGCHANGE
- ICSF_MASTER_KEY_CONSISTENCY
SMF Type 82

- Subtype 1 – ICSF Initialization
- Subtype 3 – change in number of available processors
- Subtype 4 – when ICSF handles error conditions for crypto feature failure or tampering
- Subtype 5 – change in SSM
- Subtype 6 & 7 – when a key part is entered via Key Entry Unit (KEU)
- Subtype 7 – Key Part Entry Section
- Subtype 8 – Cryptographic Key Data Set Refresh Section
- Subtype 9 – Dynamic CKDS Update
- Subtype 10 – when clear key part entered for PKA-MK
- Subtype 11 – when clear key part entered for DES-MK
- Subtype 12 – for each request and reply from calls to CSFSPKSC service by TKE
- Subtype 13 – Dynamic PKDS Update
- Subtype 14 – Cryptographic Coprocessor Master Key Entry
- Subtype 15 – PCI Cryptographic Coprocessor Retained Key Create/Delete

Subtypes in light gray are deprecated in HCR77A1
SMF Type 82 (cont.)

• Subtype 16 – PCI Cryptographic Coprocessor TKE
• Subtype 17 – periodically to provide some indication of PCI Cryptographic Coprocessor usage
• Subtype 18 – Cryptographic Processor Configuration
• Subtype 19 – PCI X Cryptographic Coprocessor Timing
• Subtype 20 – Cryptographic Processor Processing Times
• Subtype 21 – ICSF Sysplex Group Change Section
• Subtype 22 – Trusted Block Create Callable Services Section
• Subtype 23 – Token Data Set Update
• Subtype 24 – Duplicate Tokens Found
• Subtype 25 – Key Store Policy
• 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

Subtypes in light gray are deprecated in HCR77A1
CSFSMFR REXX EXEC / CSFSMFJ
Sample JCL

- CSFSMFR Reads the Type 82 record and generates a ‘meaningful’ report
- CSFSMFJ Captures Type 82, sorts and executes CSFSMFR
- Forensics, not performance
- Output may be large (multiple lines per Type 82 record)

Subtype=0014 Cryptographic Coprocessor Timing
Written periodically to provide some indication of coprocessor and accelerator

Nov 2011 0:00:19.26
TME... 00000786 DTE... 0111305F SID... SYSC   SSI... 00000000 STY... 0014
TFL... 10000000
  TFL 10 Coprocessor is a CEX3C
TNQ... C89B5841F5841AB1 TDQ... C89B5841F59D39B1 TWT...
C89B5841F59D5AB1
TQU... 00000000 TSF... áä TIX... 00
TSN... 91008705 TDM... 02 TRN... 40

Subtype=0012 Cryptographic Processor Timing
Written periodically to provide some indication of coprocessor and accelerator

Nov 2011 0:00:19.26
TME... 00000786 DTE... 0111305F SID... SYSC   SSI... 00000000 STY... 0012
TFL... 10000000
  TFL 10 Coprocessor is a CEX3C
TNQ... C89B5841F5841AB1 TDQ... C89B5841F59D39B1 TWT...
C89B5841F59D5AB1
TQU... 00000000 TSF... áä TIX... 00
TSN... 91008705 TDM... 02 TRN... 40

CSFSMFR REXX EXEC / CSFSMFJ
Sample JCL
ICSF Publications

- ICSF Overview
  - SC14-7505 z/OS 2.1
  - SA22-7519 z/OS 1.13
- ICSF Administrator’s Guide
  - SC14-7506 z/OS 2.1
  - z/OS 1.13 SA22-7521 z/OS 1.13
- ICSF Application Programmer’s Guide
  - SC14-7508 z/OS 2.1
  - z/OS 1.13 SA22-7522 z/OS 1.13
- ICSF Systems Programmer’s Guide
  - SC14-7507 z/OS 2.1
  - SA22-7520 z/OS 1.13

z/OS Web Download Site
Agenda

• What is ICSF
• Key repositories & Verification Patterns
• ICSF Setup &Parms
• Other ICSF ‘stuff’ (Panels, Healthchecks & SMF)
• Keys, Control Vectors & Tokens
• APIs
• SAF and Security Policies

And now, We are here
Questions