MAINFRAME CRYPTO

Master Key Entry on z Systems

Greg Boyd

www.mainframecrypto.com

October 2015

Copyrights and Trademarks

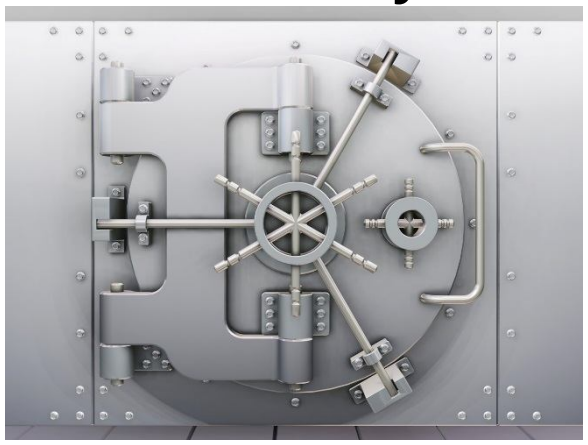
- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 10 years

Agenda

- Some Basics
  - Secure/Clear/Protected Keys
  - Why/when we need master keys
- Creating and Managing Master Keys
- Key Management Considerations

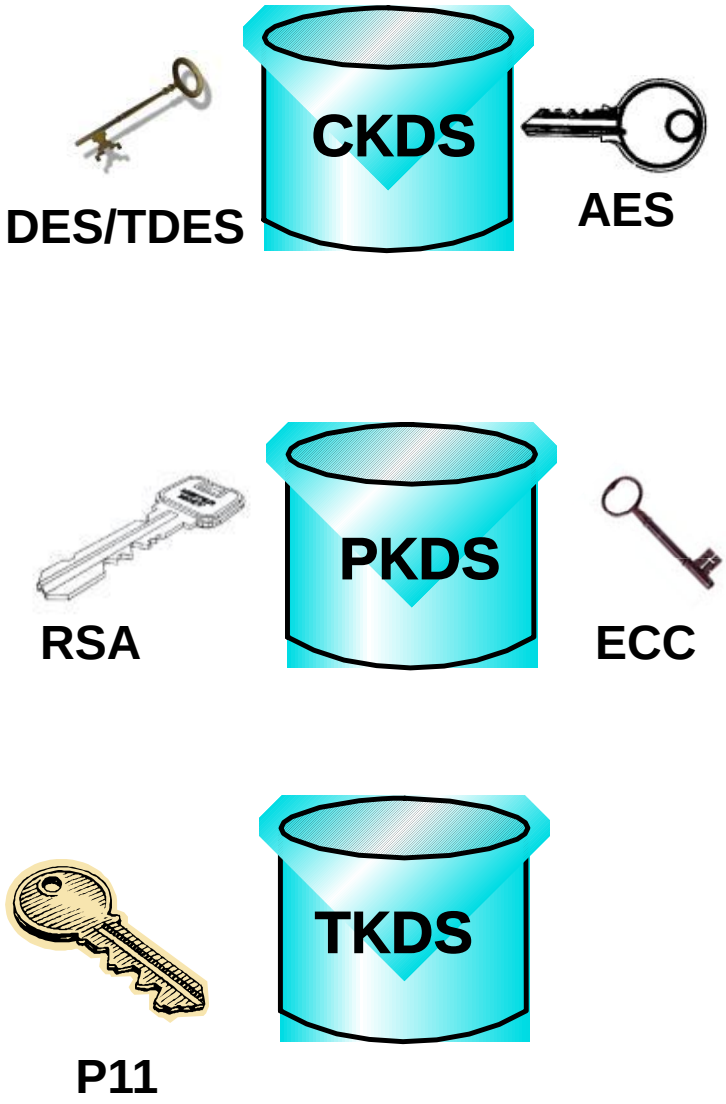
Clear Key / Secure Key / Protected Key

- Clear Key – key may be in the clear, at least briefly, somewhere in the environment
- Secure Key – key value does not exist in the clear outside of the HSM (secure, tamper-resistant boundary of the card)
- Protected Key – key value does not exist outside of physical hardware, although the hardware may not be tamper-resistant



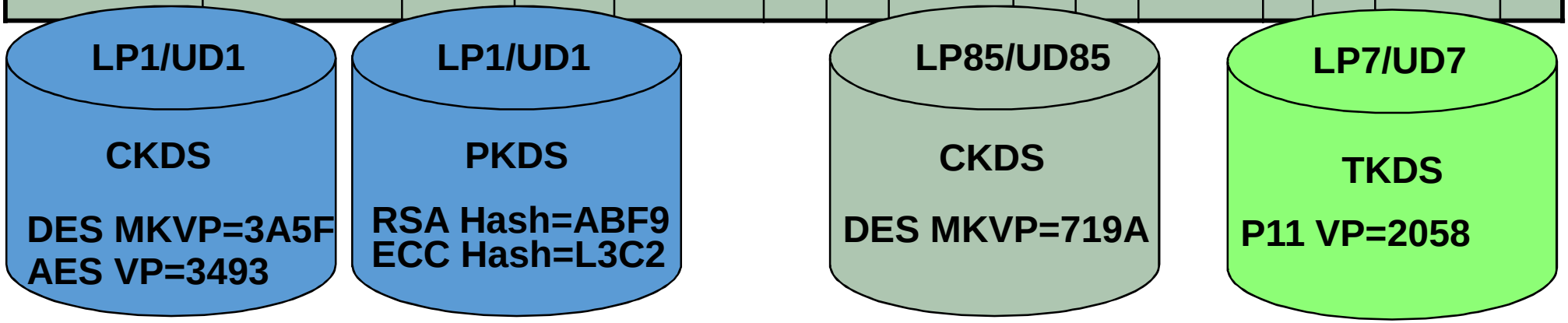
ICSF Keystores

- CKDS – Cryptographic Key Data Set
  - Symmetric DES/TDES keys
  - Symmetric AES keys
  - PIN keys
  - Importer/Exporter keys
  - Other symmetric keys
- PKDS – PKA Key Data Set
  - RSA (Public/Private keys)
  - ECC (Public/Private keys)
  - Trusted PIN Blocks
- TKDS – Token Key Data Set
  - Cryptographic Objects



Keys in Sync in Hardware and Storage

LPAR & Domain	DES-MK			AES-MK			RSA-MK			ECC-MK			P11-MK	
	Current	New	Old	Current	N	O	Current	N	O	Current	N	O	Current	N
LP1 UD1	ABC (MKVP= 3A5F)			IKJ (VP=3493)			PQR (Hash= ABF9)			XYZ (Hash= L3C2)				
LP6 UD6	EFG (MKVP = 719A)													
LP7 UD7													TUV (VP= 2058)	
LP85 UD9	EFG (MKVP = 719A)													



Key Entry

- Master Keys
  - Passphrase Initialization (aka PPINIT)
  - Via the ISPF Panels for ICSF
  - From the Trusted Key Entry Workstation

When do you need to load master keys?

- First time start-up
- At Disaster Recovery site
- When installing new hardware or replacing hardware
- Whenever your security policy calls for key change
- Suspected compromise / Personnel change

ICSF Main Menu

```
HCR77B0 ------------------ Integrated Cryptographic Service Facility ------------------
OPTION ===> 6

Enter the number of the desired option.
  1  COPROCESSOR MGMT  – Management of Cryptographic Coprocessors
  2  MASTER KEY MGMT    -- 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

          Licensed Materials - Property of IBM
          5668-ZOS (C) Copyright IBM Corp. 1989, 2015. All rights reserved.
          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.
```

Pass Phrase Initialization

CSFPMC40 ----------ICSF – Pass Phrase MK/CKDS/PKDS Initialization----------
COMMAND ===>

Enter your pass phrase (16 to 64 characters)
===> _**CRYPTO on System z Rocks**_____

Select one of the initialization actions then press ENTER to process.
S Initialize system – Load the AES, DES, ECC, and RSA master keys to all coprocessors and initialize the CKDS and PKDS, making them the active key data sets.
KDSR format (Y/N) ===> Y
CKDS ===> **'CSF.TEST.CKDS'**
PKDS ===> **'CSF.TEST.PKDS'**
_ Reinitialize system – Load the AES, DES, ECC, and RSA master keys to all coprocessors and make the specified CKDS and PKDS the active key data sets.
CKDS ===>
PKDS ===>
_ Add coprocessors – Initialize additional inactive (Master key incorrect) coprocessors with the same AES, DES, ECC, and RSA master keys.
_ Add missing MKs – Load missing AES and/or ECC master keys on each active coprocessor. Update the currently active CKDS and/or PKDS to include the MKVP of the loaded MK(s).

Press ENTER to process.
Press END to exit to the previous menu

Pass Phrase Initialization (cont.)

CSFPMC40 --- ICSF – Pass Phrase MK/CKDS/PKDS Initialization--- INITIALIZATION COMPLETE
COMMAND ===>
Enter your pass phrase (16 to 64 characters)
===> _____
Select one of the initialization actions then press ENTER to process.
_ Initialize system – Load the AES, DES, ECC, and RSA master keys to all coprocessors and initialize the CKDS and PKDS, making them the active key data sets.
KDSR format (Y/N) ===> Y
CKDS ===>
PKDS ===>
_ Reinitialize system – Load the AES, DES, ECC, and RSA master keys to all coprocessors and make the specified CKDS and PKDS the active key data sets.
CKDS ===>
PKDS ===>
_ Add coprocessors – Initialize additional inactive (Master key incorrect) coprocessors with the same AES, DES, ECC, and RSA master keys.
_ Add missing MKs – Load missing AES and/or ECC master keys on each active coprocessor. Update the currently active CKDS and/or PKDS to include the MKVP of the loaded MK(s).
The master key registers have been loaded.
Processing of the key data sets is complete.
Pass phrase initialization has completed.
Press ENTER to process.

The problem with PPINIT

- Only works for loading master keys the first time
- Anyone and everyone that knows your passphrase knows your master key
- Only the hardware needs to know the master key

The ICSF panels or the TKE provide better security for the master keys

ICSF Main Menu

```
HCR77B0 ------------------ Integrated Cryptographic Service Facility ------------------
OPTION ===> 1

Enter the number of the desired option.
  1  COPROCESSOR MGMT  – Management of Cryptographic Coprocessors
  2  MASTER KEY MGMT    -- 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

          Licensed Materials - Property of IBM
          5668-ZOS (C) Copyright IBM Corp. 1989, 2015. All rights reserved.
          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.
```

ICSF Coprocessor Management Screen

CSFGCMP0 ---------- ICSF Coprocessor Management ---------- Row 1 to 2 of 2
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.

COPROCESSOR	SERIAL NUMBER	STATUS	AES	DES	ECC	RSA	P11
_**S**_ G06	90004543	ACTIVE	A	A	A	A	U
_**S**_ G07	90004529	ACTIVE	A	A	A	A	U

ICSF Panels – Display Hardware Status (AES-MK)

```
CSFCMP40 ---------- ICSF Coprocessor Hardware Status ----------------------
COMMAND ===>                                              Crypto Domain:  3
REGISTER STATUS                 COPROCESSOR G06     COPROCESSOR G07     More +
Crypto Serial Number        :   97007637            97007663
Status                      :   ACTIVE              ACTIVE
AES Master Key
  New Master Key register   :   EMPTY               EMPTY
    Verification pattern    :

 Old Master Key register    :   EMPTY               EMPTY
    Verification pattern    :

 Current Master Key register :  VALID               VALID
    Verification pattern    :   F03CF42DB933BF1E    F03CF42DB933BF1E



Press ENTER to refresh the hardware status display.
Press END     to exit the previous menu.
```

ICSF Panels – Display Hardware Status (DES-MK)

```
CSFCMP40 ---------- ICSF Coprocessor Hardware Status ----------------------
COMMAND ===>                                              Crypto Domain:  3
REGISTER STATUS                 COPROCESSOR G06     COPROCESSOR G07     More +
Crypto Serial Number        :   97007637            97007663
Status                      :   ACTIVE              ACTIVE
DES Master Key
  New Master Key register   :   EMPTY               EMPTY
    Verification pattern    :
    Hash pattern            :
  Old Master Key register   :   EMPTY               EMPTY
    Verification pattern    :
    Hash pattern            :
  Current Master Key register:  VALID               VALID
    Verification pattern    :   E9572EFFDAA14AA8    E9572EFFDAA14AA8
    Hash pattern            :   DD20A717C842FC0C    DD20A717C842FC0C
                            :   5D018950FEB7F9B4    5D018950FEB7F9B4

Press ENTER to refresh the hardware status display.
Press END     to exit the previous menu.
```

ICSF Panels – Display Hardware Status (ECC-MK)

```
CSFCMP40 ---------- ICSF Coprocessor Hardware Status ----------------------
COMMAND ===>                                              Crypto Domain:  3
REGISTER STATUS                 COPROCESSOR G06     COPROCESSOR G07     More +
Crypto Serial Number        :   97007637            97007663
Status                      :   ACTIVE              ACTIVE
ECC Master Key
  New Master Key register   :   EMPTY               EMPTY
    Verification pattern    :

Old Master Key register     :   EMPTY               EMPTY
    Verification pattern    :

Current Master Key register :   VALID               VALID
    Verification pattern    :   CDB26CD88EC37699    CDB26CD88EC37699

Press ENTER to refresh the hardware status display.
Press END     to exit the previous menu.
```

ICSF Panels – Display Hardware Status (RSA-MK)

```
CSFCMP40 ---------- ICSF Coprocessor Hardware Status ----------------------
COMMAND ===>                                              Crypto Domain:  3
REGISTER STATUS                 COPROCESSOR G06     COPROCESSOR G07     More +
Crypto Serial Number         :  97007637            97007663
Status                       :  ACTIVE              ACTIVE
Asymmetric-Keys Master Key
  New Master Key register    :  EMPTY               EMPTY
    Hash pattern             :

Old Master Key register      :  EMPTY               EMPTY
    Hash pattern             :

Current Master Key register  :  VALID               VALID
    Hash pattern             :  15D7602B7CD493BC    15D7602B7CD493BC
                             :  A7709D4956FEFEEB    A7709D4956FEFEEB

Press ENTER to refresh the hardware status display.
Press END   to exit the previous menu.
```

Dilbert Understands Random Numbers

http://dilbert.com/strips/comic/2001-10-25/

ICSF Main Menu

```
HCR77B0 ----------------- Integrated Cryptographic Service Facility ------------------
OPTION ===>  5

Enter the number of the desired option.
  1  COPROCESSOR MGMT – Management of Cryptographic Coprocessors
  2  MASTER KEY MGMT    -- 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

          Licensed Materials - Property of IBM
          5668-ZOS (C) Copyright IBM Corp. 1989, 2015. All rights reserved.
          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.
```

ICSF Utility Menu

```
CSFUTL00 ---------------------- ICSF – Utilities --------------------------------
OPTION ===> 3

Enter the number of the desired option.

  1  ENCODE          – Encode data
  2  DECODE          – Decode data
  3  RANDOM          – Generate a random number
  4  CHECKSUM        – Generate a checksum and verification and hash pattern
  5  PPKEYS          – Generate master key values from a pass phrase
  6  PKDSKEYS        – Manage keys in the PKDS

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

ICSF Panels – Random Number Generator

```
CSFRNG00  ---------- ICSF –  Random Number Generator  ------------------------
COMMAND ===>

Enter data below:

 Parity Option  ===> RANDOM                ODD, EVEN, RANDOM
 Random Number 1  :  0000000000000000     Random Number 1
 Random Number 2  :  0000000000000000     Random Number 2
 Random Number 3  :  0000000000000000     Random Number 3
 Random Number 4  :  0000000000000000     Random Number 4


Press ENTER to process.
Press END      to exit to the previous menu.
```

ICSF Panels – Random Number Generator

```
CSFRNG00  ------------- ICSF –  Random Number Generator  -------------------------
COMMAND ===>

Enter data below:

 Parity Option  ===>                              ODD, EVEN, RANDOM
 Random Number 1  :  02AC7633C1951F0A  Random Number 1
 Random Number 2  :  5916A7A3DF8718DB  Random Number 2
 Random Number 3  :  7E1EEB82B27969CA  Random Number 3
 Random Number 4  :  A7D6ECF77E91DAAC  Random Number 4


Press ENTER to process.
Press END      to exit to the previous menu.
```

ICSF Panels – Checksum Calculation

```
CSFMKV00  ---------- ICSF –  Checksum and Verification and Hash Pattern ----------
COMMAND ===>

Enter data below:
  Key Type  ===>  DES-MK                (Selection panel displayed if blank)
  Key Value ===>  02AC7633C1951F0A      Input key value 1
            ===>  5916A7A3DF8718DB      Input key value 2
            ===>  7E1EEB82B27969CA      Input key value 3 (AES, ECC & RSA Keys)
            ===>  A7D6ECF77E91DAAC      Input key value 4 (AES, ECC Keys only)

  Checksum        : 00                  Check digit for key value
  Key Part VP     : 0000000000000000    Verification Pattern
  Key Part HP     : 0000000000000000    Hash pattern
                  : 0000000000000000

Press ENTER to process.
Press END     to exit to the previous menu.
```

ICSF Panels – Checksum Calculation (cont.)

```
CSFMKV00  ---------- ICSF –  Checksum and Verification and Hash Pattern ----------
COMMAND ===>

Enter data below:
  Key Type  ===>                                (Selection panel displayed if blank)
  Key Value ===>  02AC7633C1951F0A             Input key value 1
            ===>  5916A7A3DF8718DB             Input key value 2
            ===>  0000000000000000             Input key value 3 (AES, ECC & RSA Keys)
            ===>  0000000000000000             Input key value 4 (AES, ECC Keys only)

  Checksum        : DD                         Check digit for key value
  Key Part VP     : A7518C6F9C65FB02           Verification Pattern
  Key Part HP     : D8C18ADC8F01E6D9           Hash pattern
                  : 307C31F4CC1CB2F2

Press ENTER to process.
Press END     to exit to the previous menu.
```

ICSF Coprocessor Management Screen

CSFGCMP0 ---------- ICSF Coprocessor Management ---------- Row 1 to 2 of 2
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.

COPROCESSOR	SERIAL NUMBER	STATUS	AES	DES	ECC	RSA	P11
_**E**_ G06	90004543	ACTIVE	A	A	A	A	U
_**E**_ G07	90004529	ACTIVE	A	A	A	A	U

ICSF Panels – 1st Key Part

```
CSFDKE50 ------------------- ICSF – Clear Master Key Entry  -------------------------
COMMAND  ===>
                    AES new master key register          :        EMPTY
                    DES new master key register          :        EMPTY
                    ECC new master key register          :        EMPTY
                    RSA new master key register          :        EMPTY

 Specify information below
    Key Type        ===>                                 (AES-MK, DES-MK, ECC-MK, RSA-MK)
    Part            ===>                                 (RESET, FIRST, MIDDLE, FINAL)
    Checksum        ===>  DD
    Key Value       ===>  02AC7633C1951F0A
                    ===>  5916A7A3DF8718DB
                    ===>  0000000000000000               (AES-MK, ECC-MK, and RSA-MK only)
                    ===>  0000000000000000               (AES-MK, ECC-MK only)



Press ENTER to process.
Press END      to exit to the previous menu.
```

ICSF Panels – 1st Key Part (Before)

```
CSFDKE50 ------------------- ICSF – Clear Master Key Entry  -------------------------
COMMAND  ===>
                    AES new master key register          :        EMPTY
                    DES new master key register          :        EMPTY
                    ECC new master key register          :        EMPTY
                    RSA new master key register          :        EMPTY

 Specify information below
    Key Type        ===>  DES-MK                (AES-MK, DES-MK, ECC-MK, RSA-MK)
    Part            ===>  FIRST                 (RESET, FIRST, MIDDLE, FINAL)
    Checksum        ===>  DD
    Key Value       ===>  02AC7633C1951F0A
                    ===>  5916A7A3DF8718DB
                    ===>  0000000000000000      (AES-MK, ECC-MK, and RSA-MK only)
                    ===>  0000000000000000      (AES-MK, ECC-MK only)

Press ENTER to process.
Press END      to exit to the previous menu.
```

ICSF Panels – 1st Key Part (After)

```
CSFDKE50 -------------------- ICSF – Clear Master Key Entry  ----------------- KEY PART LOADED
COMMAND  ===>
                    AES new master key register          :        EMPTY
                    DES new master key register          :        PART FULL
                    ECC new master key register          :        EMPTY
                    RSA new master key register          :        EMPTY

 Specify information below
   Key Type        ===>  DES-MK                    (AES-MK, DES-MK, ECC-MK, RSA-MK)
   Part            ===>  FIRST                     (RESET, FIRST, MIDDLE, FINAL)
   Checksum        ===>  00
   Key Value       ===>  0000000000000000
                   ===>  0000000000000000
                   ===>  0000000000000000          (AES-MK, ECC-MK, and RSA-MK only)
                   ===>  0000000000000000          (AES-MK, ECC-MK only)

Entered key part VP: A7518C6F9C65FB02   HP: D8C18ADC8F01E6D9 307C31F4CC1CB2F2
                                        (Record and secure these patterns)

 Press ENTER to process.
 Press END     to exit to the previous menu.
```

ICSF Panels – 2nd Key Part (Before)

```
CSFDKE50 ------------------- ICSF – Clear Master Key Entry  -------------------------
COMMAND  ===>
                    AES new master key register          :        EMPTY
                    DES new master key register          :        PART FULL
                    ECC new master key register          :        EMPTY
                    RSA new master key register          :        EMPTY

Specify information below
   Key Type       ===>  DES-MK                  (AES-MK, DES-MK, ECC-MK, RSA-MK)
   Part           ===>  MIDDLE                  (RESET, FIRST, MIDDLE, FINAL)
   Checksum       ===>  FF
   Key Value      ===>  CE548C08EAA42A89
                  ===>  0EBF346B9408258A
                  ===>  0000000000000000        (AES-MK, ECC-MK, and RSA-MK only)
                  ===>  0000000000000000        (AES-MK, ECC-MK only)

Press ENTER to process.
Press END      to exit to the previous menu.
```

ICSF Panels – 2nd Key Part (After)

```
CSFDKE50 ------------------- ICSF – Clear Master Key Entry  ---------------- KEY PART LOADED
COMMAND  ===>
                    AES new master key register          :        EMPTY
                    DES new master key register          :        PART FULL
                    ECC new master key register          :        EMPTY
                    RSA new master key register          :        EMPTY

Specify information below
   Key Type       ===>  DES-MK                  (AES-MK, DES-MK, ECC-MK, RSA-MK)
   Part           ===>  MIDDLE                  (RESET, FIRST, MIDDLE, FINAL)
   Checksum       ===>  00
   Key Value      ===>  0000000000000000
                  ===>  0000000000000000
                  ===>  0000000000000000        (AES-MK, ECC-MK, and RSA-MK only)
                  ===>  0000000000000000        (AES-MK, ECC-MK only)

 Entered key part VP: 8E86E485545AA669   HP: 1D29966EBEC2BD11 AD540801821039D0
                              (Record and secure these patterns)

Press ENTER to process.
Press END     to exit to the previous menu.
```

ICSF Panels – 3rd Key Part (Before)

```
CSFDKE50 ------------------- ICSF – Clear Master Key Entry  -------------------------
COMMAND  ===>
                    AES new master key register          :        EMPTY
                    DES new master key register          :        PART FULL
                    ECC new master key register          :        EMPTY
                    RSA new master key register          :        EMPTY

Specify information below
   Key Type       ===>  DES-MK                (AES-MK, DES-MK, ECC-MK, RSA-MK)
   Part           ===>  FINAL                 (RESET, FIRST, MIDDLE, FINAL)
   Checksum       ===>  64
   Key Value      ===>  BF57AD3D94CEAD62
                  ===>  C73491832638F7EF
                  ===>  0000000000000000      (AES-MK, ECC-MK, and RSA-MK only)
                  ===>  0000000000000000      (AES-MK, ECC-MK only)

Press ENTER to process.
Press END      to exit to the previous menu.
```

ICSF Panels – 3rd Key Part (After)

```
CSFDKE50 ------------------- ICSF – Clear Master Key Entry  ---------------- KEY PART LOADED
COMMAND  ===>
                    AES new master key register          :        EMPTY
                    DES new master key register          :        FULL
                    ECC new master key register          :        EMPTY
                    RSA new master key register          :        EMPTY

Specify information below
   Key Type       ===>  DES-MK                  (AES-MK, DES-MK, ECC-MK, RSA-MK)
   Part           ===>  FINAL                   (RESET, FIRST, MIDDLE, FINAL)
   Checksum       ===>  00
   Key Value      ===>  0000000000000000
                  ===>  0000000000000000
                  ===>  0000000000000000        (AES-MK, ECC-MK, and RSA-MK only)
                  ===>  0000000000000000        (AES-MK, ECC-MK only)

 Entered key part VP: 3FFEAC6F32918B2F   HP: 1FC752887DA6ED24 F339F8321FF99FF4
 Master Key       VP: B0070E6F8F31B3C2   HP: 4181A04120413B35  D389DE6FC7DF75A7
                            (Record and secure these patterns)
Press ENTER to process.
Press END      to exit to the previous menu.
```

ICSF Coprocessor Management Screen

CSFGCMP0 ---------- ICSF Coprocessor Management ---------- Row 1 to 2 of 2
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.

COPROCESSOR	SERIAL NUMBER	STATUS	AES	DES	ECC	RSA	P11
_s_ G06	90004543	ACTIVE	A	A	U	A	U
_s_ G07	90004529	ACTIVE	A	A	U	A	U

ICSF Panels – Display Hardware Status (DES-MK)

```
CSFCMP40 ---------- ICSF Coprocessor Hardware Status ----------------------
COMMAND ===>                                              Crypto Domain:  3
REGISTER STATUS                 COPROCESSOR G06    COPROCESSOR G07     More +
Crypto Serial Number         :  97007637           97007663
Status                       :  ACTIVE             ACTIVE
DES Master Key
  New Master Key register    :  FULL               FULL
    Verification pattern     :  B0070E6F8F31B3C2   B0070E6F8F31B3C2
    Hash pattern             :  4181A04120413B35   4181A04120413B35
  Old Master Key register    :  EMPTY              EMPTY
    Verification pattern     :
    Hash pattern             :
  Current Master Key register:  VALID              VALID
    Verification pattern     :  E9572EFFDAA14AA8   E9572EFFDAA14AA8
    Hash pattern             :  DD20A717C842FC0C   DD20A717C842FC0C
                             :  5D018950FEB7F9B4   5D018950FEB7F9B4

Press ENTER to refresh the hardware status display.
Press END     to exit the previous menu.
```

ICSF Main Menu

HCR77B0 ---------- Integrated Cryptographic Service Facility ----------
OPTION ===> **2**

Enter the number of the desired option.

1	COPROCESSOR MGMT	– Management of Cryptographic Coprocessors
2	MASTER KEY MGMT	-- 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.

Master Key Management

```
CSFMKM10  ---------------------- ICSF – Master Key Management -----------------------
OPTION ===> 1

Enter the number of the desired option.

  1  CKDS MK MANAGEMENT  -       Perform Cryptographic Key Data Set (CKDS)
                                 functions including master key management
  2  PKDS MK MANAGEMENT -        Perform Public Key Data Set (PKDS)
                                  functions including master key management
  3  TKDS MK MANAGEMENT -        Perform PKCS #11 Token Data Set (TKDS)
                                  functions including master key management
  4  SET MK                 -    Set master key




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

Coordinated Key Admin - Prereqs

- All members of the CSFplex must be running HCR77A0 or higher
- All members of the CSFplex must be pointing to the same CKDS/PKDS
- All members of the CSFplex must have the same master key loaded
- All members of the CSFplex must have the same new master key loaded
- Cannot be running with COMPAT(YES) mode

Master Key Management - CKDS

CSFMKM20 ---------- ICSF – Master Key Management ----------
OPTION ===> **5**

Enter the number of the desired option.

1 CKDS OPERATIONS	-- Initialize a CKDS, activate a different CKDS, (Refresh), or update the header of a CKDS and make it active
2 REENCIPHER CKDS	-- Reencipher the CKDS prior to changing a symmetric master key
3 CHANGE SYM MK	-- Change a symmetric master key and activate the reenciphered CKDS
4 COORDINATED CKDS REFRESH	-- Perform a coordinated CKDS refresh
5 COORDINATED CKDS CHANGE MK	-- Perform a coordinated CKDS change master key
6 COORDINATED CKDS CONVERSION	– Convert the CKDS to use KDSR record format
7 CKDS KEY CHECK	-- Check keys in the active CKDS for format errors

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

Coordinated KDS Change Master Key

CSFCRC20 ---------- ICSF – Coordinated KDS change master key ----------
COMMAND ===>

To perform a coordinated KDS change master key, enter the KDS names below and optionally select the rename option.

KDS Type ===> CKDS
Active KDS ===> **'PLEX.TEST.CKDS'**
New KDS ===> **'PLEX.NEW.CKDS'**

Rename Active to Archived and New to Active (Y/N) ===> N

Archived KDS ===>

Create a backup of the reenciphered KDS (Y/N) ===> N

Backup KDS ===>

Press ENTER to perform a coordinated KDS refresh.
Press END to exit to the previous menu.

Steps for Changing the DES or AES Master Key

- Generate key parts and calculate checksums
- Enter the DES-MK/AES-MK key parts
- Disable CKDS Access*
- Re-encipher the CKDS under the new master key
- Change the Master Key and Activate the Reenciphered CKDS
- Enable CKDS Access*
- Change the ICSF Options data set to point to the new CKDS*

Key Management Policies/Procedures

- How Many Key Officers/Key Parts?
- How Are the Key Parts Generated? Who Generates them?
- Where are the Keys Stored for Emergencies?
- How Often is the DES-MK changed? The AES-MK? The RSA-MK? The ECC-MK? The P11-MK?
- How Often are Application Keys changed?
- How are changes implemented/coordinated across the SYSPLEX?
- Is crypto a part of change management?

Summary

- Master Key Change is not hard, but it can be intimidating
- You should have a security policy that defines when master keys are changed
- You should be using the ICSF panels or the TKE, not PPINIT
- You should have a documented process for changing the master keys
- The master key parts must be available for recovery purposes

References

- ICSF Administrator's Guide
  - SC14-7506 (HCR77A1 & later)
  - SA22-7521 (prior versions of ICSF & z/OS)

- TechDocs - www.ibm.com/support/techdocs
  - TD106095 So, you LOST your MASTER Keys
  - PRS5120 dhppkeys exec to Display PassPhrase Generated Master Key Values

- Enterprise Tech Journal – To Passphrase or Not To Passphrase
  - http://enterprisesystemsmedia.com/article/to-passphrase-or-not-to-passphrase#sr=g&m=o&cp=or&ct=-tmc&st=(opu%20qspwjefe)&ts=1402433213 (or look for the link under Articles at www.mainframecrypto.com)


Questions