IBM

"So, you LOST your <MASTER> keys?"

New York RACF User's Group

Speaker: Dave Hilliard
ICSF lvl2 Poughkeepsie NY
dhilliar@us.ibm.com

Trademarks

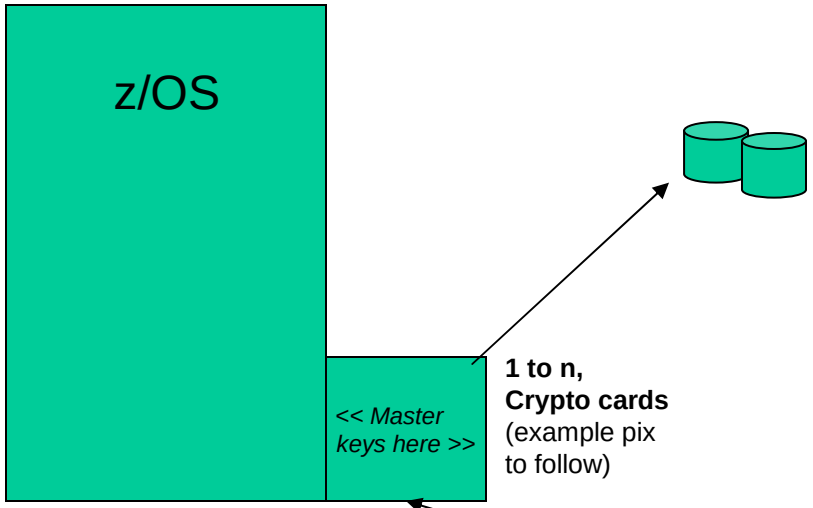
For a list of trademarks see URL :

http://www.ibm.com/legal/copytrade.shtml

Agenda

- ICSF(tm) at 10,000 feet - How master keys FIT in the picture.
- When you do NOT have them **(Setting and knowing your master keys)**
- Key types
- Software changes – what happened ? (as it regards status of Crypto processors)

ICSF at 10,000 feet



1 to n,
Crypto cards
(example pix to follow)

ICSF key stores (for user's keys)

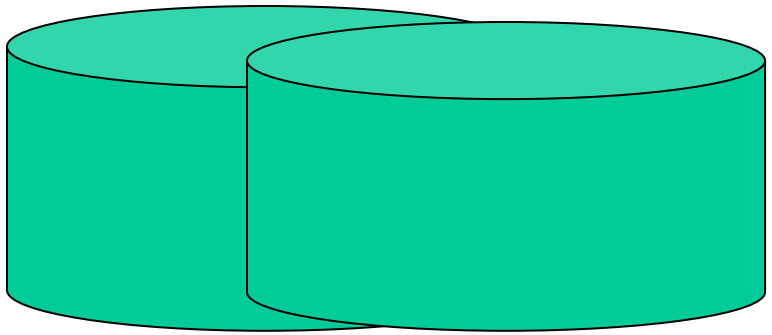
CKDS

PKDS

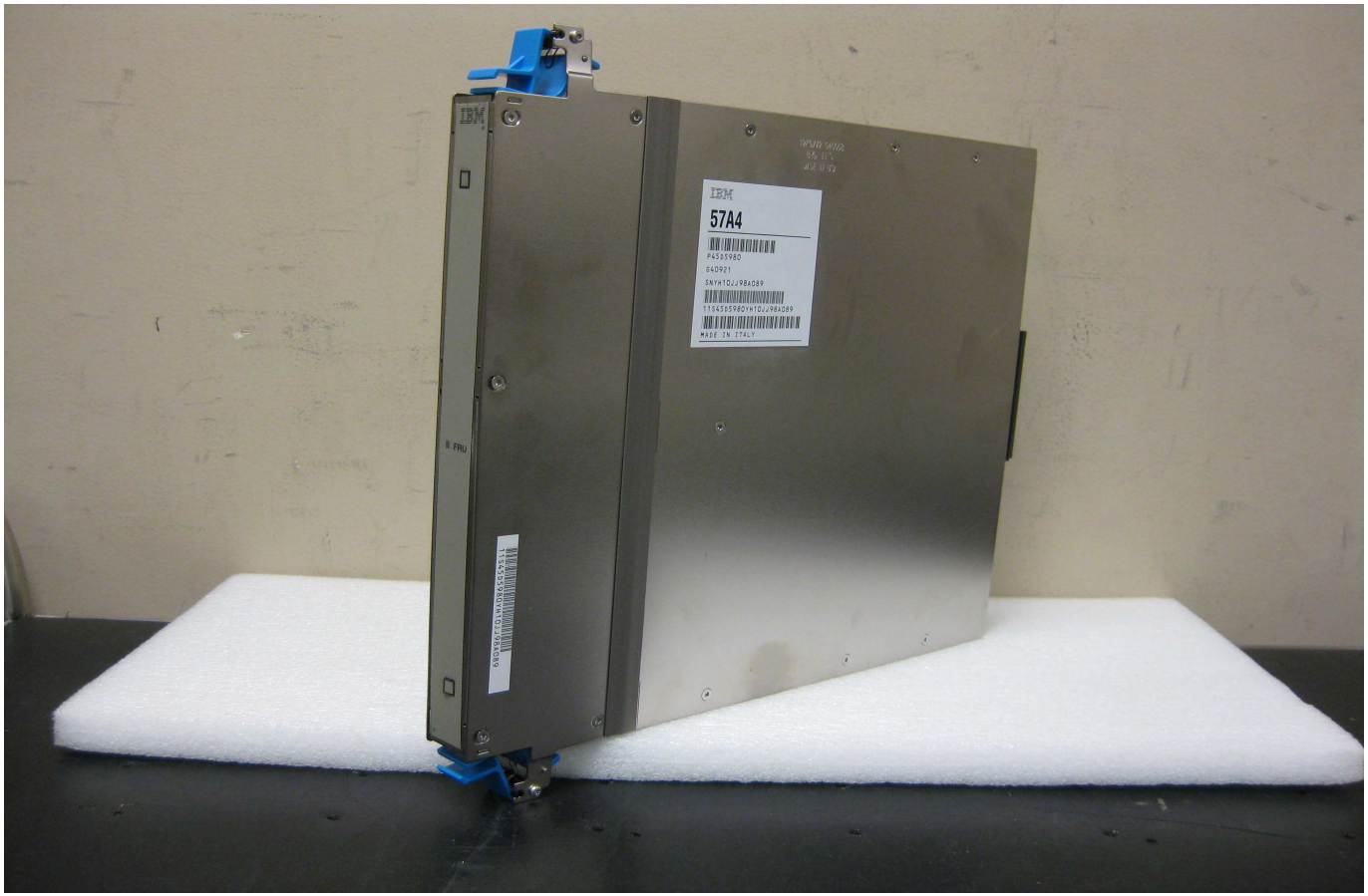
Applications / customers can encrypt their data using keys stored in either of several xKDS VSAM files.

ICSF itself protects (encrypts) these keys with MASTER keys stored in one of their crypto cards.

Changing hardware (new or replacement cards, or whole new frames) require the re-entering of those master keys.



Customer data (encrypted, with keys stored in an xKDS file)



If card is tampered with (especially silver case, upper left of photo) then the keys are inaccessible.

And these cards have LONG length (x years) battery backup. x = 5 or so.

When you do NOT have them?

- No record of them
- Key people have left
- What to do?

- It’s time to change the Master Keys
- Reencipher the CKDS and PKDS
- How do I do that?

Changing (& keeping) your Master keys

Procedure to generate a Random number and to enter it as a first AES Master Key Part.

ICSF main menu, select option 5

```
HCR7780  -------------- 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, CKDS/PKDS 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
     5694-A01 Copyright IBM Corp. 1989, 2010.  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.
```

Changing (& keeping) your Master keys

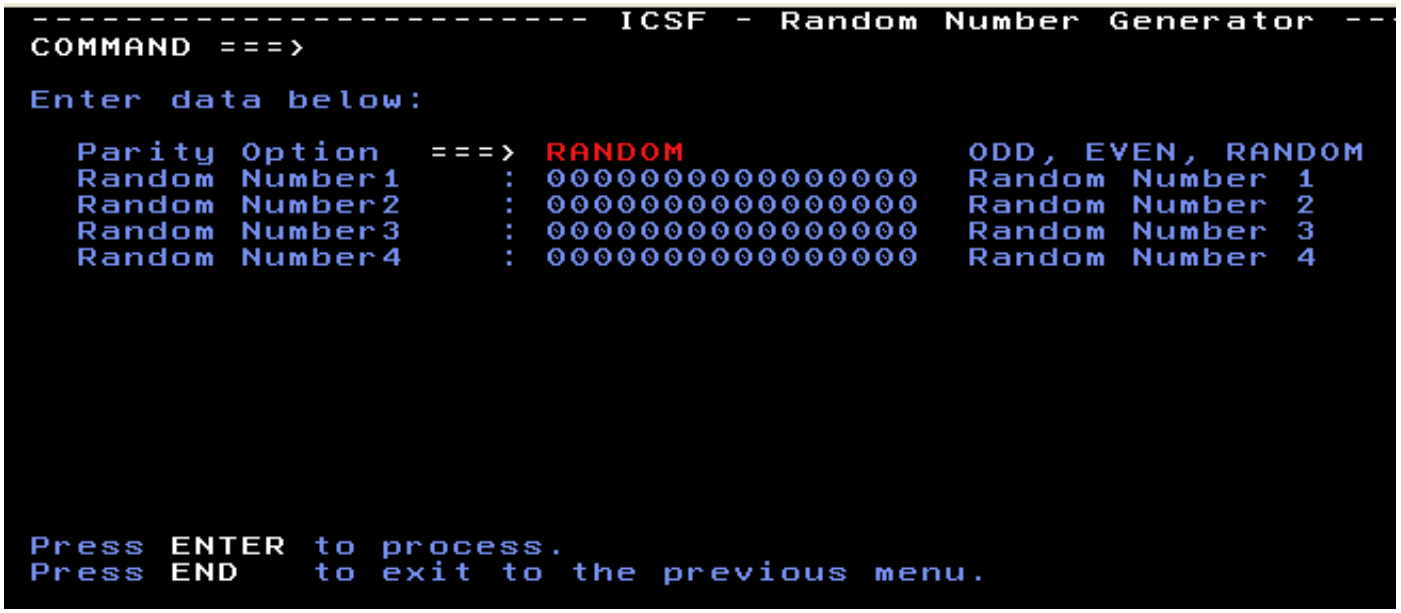
Select option 3 for Random Number

```
------------------------------ 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
  7  PKCS11 TOKEN -  Management of PKCS11 tokens




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

Press Enter to generate the random number

Changing (& keeping) your Master keys

Press Enter to generate the random number



Changing (& keeping) your Master keys

A Random number is generated

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

Enter data below:

  Parity Option   ===> RANDOM              ODD, EVEN, RANDOM
  Random Number1     : ACF62FFF901A50FA     Random Number 1
  Random Number2     : B191F19A5DC193C0     Random Number 2
  Random Number3     : 057F133421FBE488     Random Number 3
  Random Number4     : 002DBB800D0A9366     Random Number 4









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

Changing (& keeping) your Master keys

Select option 4 to get the 1 byte checksum

```
------------------------------ ICSF - Utilities ------------------
OPTION ===> 4

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
  7  PKCS11 TOKEN  -  Management of PKCS11 tokens




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

Changing (& keeping) your Master keys

Press Enter to bring up the Key Type Selection Panel

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

Enter data below:

  Key Type         ===>                    (Selection panel displayed if blank)

  Key Value        ===> ACF62FFF901A50FA   Input key value 1
                   ===> B191F19A5DC193C0   Input key value 2
                   ===> 057F133421FBE488   Input key value 3(AES, ECC & RSA Keys)
                   ===> 002DBB800D0A9366   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.
```

Changing (& keeping) your Master keys

Select the Master Key you want (AES, DES, ECC, or RSA)

```
---------------------- ICSF - Key Type Selection Panel ---- Row 1 to 14 of 14
COMMAND ===>                                                SCROLL ===> PAGE

Select one key type only
    KEY TYPE       DESCRIPTION
s   AES-MK         AES Master Key
    ASYM-MK        Asymmetric Master key
    DES-MK         DES Master key
    ECC-MK         ECC Master key
    EXPORTER       Export key encrypting key
    IMP-PKA        Limited Authority Importer key
    IMPORTER       Import key encrypting key
    IPINENC        Input PIN encrypting key
    MASTER         DES Master key
    OPINENC        Output PIN encrypting key
    PINGEN         PIN generation key
    PINVER         PIN verification key
    PKAMSTR        PKA/Asymmetric Master key
    RSA-MK         RSA Master key
****************************** Bottom of data ********************************
```

Changing (& keeping) your Master keys

Very important - Save the Key Value, Checksum and VP in a secure place!!!

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

Enter data below:

  Key Type         ===> AES-MK             (Selection panel displayed if blank)

  Key Value        ===> ACF62FFF901A50FA   Input key value 1
                   ===> B191F19A5DC193C0   Input key value 2
                   ===> 057F133421FBE488   Input key value 3(AES, ECC & RSA Keys)
                   ===> 002DBB800D0A9366   Input key value 4(AES, ECC Keys only)

  Checksum           : 5A                  Check digit for key value
  Key Part VP        : 17AC2CD031982382    Verification Pattern
  Key Part HP        :                     Hash Pattern
                     :

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

Changing (& keeping) your Master keys

Press F3 twice to get back to the main menu and select option 1

```
HCR7780  ---------------- 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, CKDS/PKDS 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
     5694-A01 Copyright IBM Corp. 1989, 2010.  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.
```

Changing (& keeping) your Master keys

Enter an e next to all coprocessors for Master Key Entry.

```
------------------------ ICSF Coprocessor Management -------- Row 1 to 2 of 2
COMMAND ===>                                                 SCROLL ===> PAGE

 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
  -----------   -------------    ------            ---   ---   ---   ---
e   G33         93X06014         ONLINE             V     V     V     V
e   G34         93X06033         ONLINE             V     V     V     V
******************************** Bottom of data ********************************
```

Changing (& keeping) your Master keys

The first key part is ready to be loaded in the AES New Master Key

```
--------------------------- ICSF - 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  ===> 5A

  Key Value ===> ACF62FFF901A50FA
            ===> B191F19A5DC193C0
            ===> 057F133421FBE488   (AES-MK, ECC-MK, and RSA-MK only)
            ===> 002DBB800D0A9366   (AES-MK, ECC-MK  only)

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

Changing (& keeping) your Master keys

Enter aes-mk for the Key Type and enter first for the

```
--------------------------- ICSF - 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           (AES-MK, DES-MK, ECC-MK, RSA-MK)

  Part       ===> first            (RESET, FIRST, MIDDLE, FINAL)

  Checksum   ===> 5A

  Key Value  ===> ACF62FFF901A50FA
             ===> B191F19A5DC193C0
             ===> 057F133421FBE488   (AES-MK, ECC-MK, and RSA-MK only)
             ===> 002DBB800D0A9366   (AES-MK, ECC-MK  only)

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

Changing (& keeping) your Master keys

Key part has been loaded. Save the Verification pattern with the key

```
--------------------------- ICSF - Master Key Entry ---------- KEY PART LOADED
COMMAND ===>

              AES new master key register       :  PART FULL
              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           (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:  17AC2CD031982382

                    (Record and secure these patterns)
Press ENTER to process.
Press END   to exit to the previous menu.
```

Changing (& keeping) your Master keys

The Coprocessor Hardware Statue panel shows the keypart in the NMK

```
---------------------- ICSF - Coprocessor Hardware Status ----------------------
COMMAND ===>                                                  SCROLL ===>
                                                          CRYPTO DOMAIN: 0

REGISTER STATUS                    COPROCESSOR G33        COPROCESSOR G34
                                                                  More:      +
 Crypto Serial Number            : 93X06014               93X06033
 Status                          : ONLINE                 ONLINE
 AES Master Key
   New Master Key register       : PART FULL              PART FULL
     Verification pattern        : 17AC2CD031982382       17AC2CD031982382
   Old Master Key register       : EMPTY                  EMPTY
     Verification pattern        :
   Current Master Key register   : EMPTY                  EMPTY
     Verification pattern        :
 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   : EMPTY                  EMPTY
     Verification pattern        :
     Hash pattern                :
                                 :
 ECC Master Key
   New Master Key register       : EMPTY                  EMPTY
     Verification pattern        :
   Old Master Key register       : EMPTY                  EMPTY
     Verification pattern        :
   Current Master Key register   : EMPTY                  EMPTY
     Verification pattern        :
 RSA Master Key
   New Master Key register       : EMPTY                  EMPTY
     Verification pattern        :
                                 :

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

Changing (& keeping) your Master keys

Repeat this process for the remaining key parts and for the remaining master keys. ie. DES, RSA and ECC.

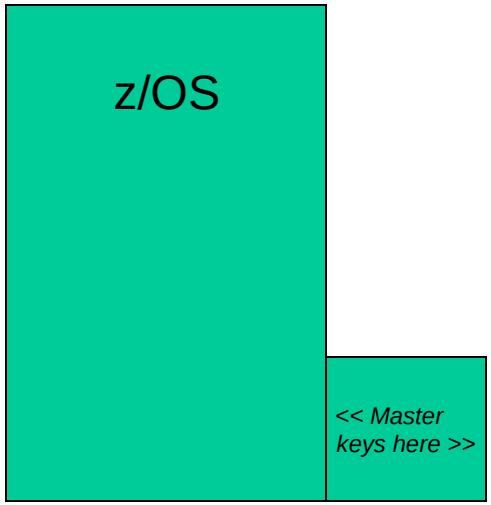
Then reencipher the CKDS and PKDS.

Changing (& keeping) your Master keys

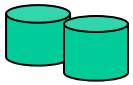
Reenchiper the CKDS then CHANGE SYM MK

Reencipher the PKDS then CHANGE ASYM MK

```
------------------------- ICSF - Master Key Management ----------------------
OPTION ===>

Enter the number of the desired option.

  1  INIT/REFRESH/UPDATE CKDS - Initialize a Cryptographic Key Data Set or
                                activate an updated Cryptographic Key Data Set
  2  SET MK                -   Set a master key (AES, DES, ECC)
  3  REENCIPHER CKDS       -   Reencipher the CKDS prior to changing a symmetric
                                master key
  4  CHANGE SYM MK         -   Change a symmetric master key and activate the
                                reenciphered CKDS
  5  INIT/REFRESH/UPDATE PKDS -  Initialize a Public Key Data Set or
                                activate an updated Public Key Data Set or
                                update the Public Key Data Set header
  6  REENCIPHER PKDS       -   Reencipher the PKDS
  7  CHANGE ASYM MK        -   Change an asymmetric master key and activate the
                                reenciphered PKDS

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



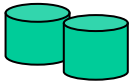
Crypto cards



Current ICSF key stores

CKDS

PKDS



New ICSF key stores

CKDS

PKDS

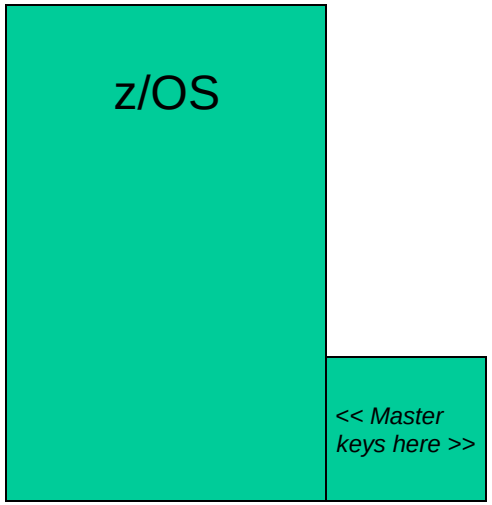
Allocate new key store VSAM files

Enter NEW keys on current hardware

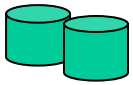
Use new keys and **RE-ENCIPHER** the keys in xKDS (keystore files).

Then use new xKDS files. This or new hardware.

Same customer data, new master KEYS



Crypto cards

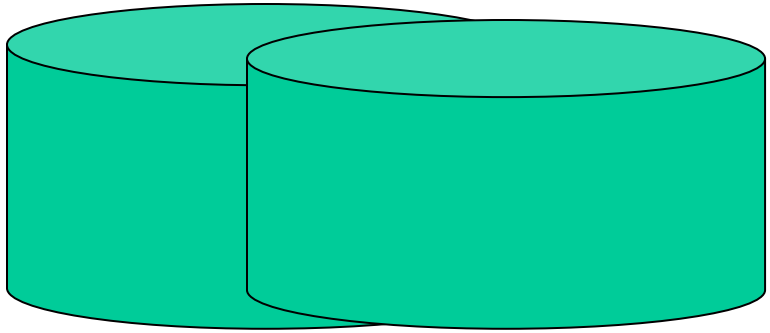


New ICSF key stores (re-enciphered)

CKDS

PKDS

No changes (decrypting and re-encrypting their data) necessary by customers



Customer data (encrypted, with keys stored in an xKDS file)

Key Types

CKDS Symmetric	PKDS Asymmetric
DES	SMK / ALL-PKA \ KMMK
7750 Sym–MK	ASYM – MK
7751 DES AES	ASYM – MK
7770 DES AES	ASYM – MK
7780 DES 7790 AES	RSA ECC

New Activation of Crypto Coprocessors on HCR7780

- Prior to HCR7751, the DES MK needed to be set to make the Coprocessor become Active
- In HCR7751, AES MKs were added. The DES or the AES master key being set would make the Coprocessor become Active
- HCR7780 introduced a new algorithm, Elliptic Curve, and a new master key (ECC-MK)
- There are now four master keys DES-MK, AES-MK, RSA-MK (formally known as ASYM-MK) and ECC-MK
- Loading and setting any one of the Master Keys will make the Coprocessor Active

Coprocessor Activation Logic

- Phase 1 - (coprocessor activation): ICSF determines which algorithm is active on the most coprocessors and then activates only those coprocessors. If there is a tie in the number of engines with a correct master key loaded, DES will take precedence, followed by RSA, then AES and finally ECC.
- Phase 2 - (algorithm activation): From the coprocessor list derived in Phase 1, ICSF will activate the algorithm(s) that are loaded on ALL of those activated coprocessors.

New Activation of Crypto Coprocessors with HCR7780

- **Master Keys loaded on CEX2 Coprocessors (Z10)**
- ==========
- AES DES ECC RSA
- E00 Y Y
- E01
- E02 Y Y
- E03
- When running with HCR7751 or HCR7770, E00 and E02 will be active and DES & RSA work will be routed to both of those coprocessors.

New Activation of Crypto Coprocessors with HCR7780

- **Master Keys loaded on CEX2 Coprocessors (z10)**
- ==========
- AES DES ECC RSA
- E00 Y Y Y
- E01 Y
- E02 Y Y Y
- E03 Y
- When running with HCR7751 or HCR7770, E00 and E02 will be active and DES, AES and RSA work will be routed to both of those coprocessors.

New Activation of Crypto Coprocessors with HCR7780

- **Master Keys loaded on CEX2 Coprocessors (z10)**
- ==========
- AES DES ECC RSA
- E00 Y Y Y
- E01 Y
- E02 Y Y Y
- E03 Y
- User migrated to HCR7780, What coprocessors and algorithms are active? (1am wake up call)

New Activation of Crypto Coprocessors with HCR7780

- **Master Keys loaded on CEX2 Coprocessors (z10)**
- ==========
- AES DES ECC RSA
- E00 Y Y Y
- E01 Y
- E02 Y Y Y
- E03 Y
- Answer E00, E01, E02, E03 and AES ONLY!

New Activation of Crypto Coprocessors with HCR7780

- **Master Keys loaded on CEX2 Coprocessors (z10)**
- ==========
- AES DES ECC RSA
- E00 Y E
- E01 Y E
- E02 Y E
- E03 E
- In this example, the user started ICSF with an existing CKDS and a brand new PKDS. E00, E01 & E02 are Active with DES only as the RSA MK in the coprocessor does not match the PKDS. The user ran some DB2 encryption tests and all was well.
-

New Activation of Crypto Coprocessors with HCR7780

- **Master Keys loaded on CEX2 Coprocessors (z10)**
- ==========
- AES DES ECC RSA
- E00 Y Y
- E01 Y Y
- E02 Y Y
- E03 Y
- Next the user entered new RSA keys and initialized the PKDS. All DB2 jobs began to fail. Why? (2am wake up call)
-

New Activation of Crypto Coprocessors with HCR7780

- **Master Keys loaded on CEX2 Coprocessors (z10)**
- ==========
- AES DES ECC RSA
- E00 Y Y
- E01 Y Y
- E02 Y Y
- E03 Y
- RSA is now Active on all 4 Coprocessors. Since DES is only Active on 3 of them, RSA wins and the DES algorithm is no longer available.
- To correct this, the user loaded the DES MK on E03.

New Activation of Crypto Coprocessors with HCR7780

- **Activation of Cryptographic Coprocessors and Cryptographic Algorithms with ICSF, HCR7780**
- http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/FLASH10749

Session Summary

- ICSF at 10,000 feet - How master keys FIT in the picture.
- When you do NOT have them **(Setting and knowing your master keys)**
- Key types
- Software changes – what happened ? (as it regards status of Crypto processors)

Appendix

- **ICSF Publications for reference:**
  - **SA22-7519-14** - z/OS V1R12.0 ICSF Overview
  - **SA22-7520-13** - z/OS V1R10.0 ICSF System Programmer's Guide
  - **SA22-7521-15** - z/OS V1R12 ICSF Administrator's Guide
  - **SA22-7522-14** - z/OS V1R12 ICSF Application Programmer's Guide
  - **SA23-2231-03** - z/OS V1R12 ICSF Writing PKCS #11 Applications
  - **SA22-7523-14** - z/OS V1R12.0 ICSF Messages
  - **SA23-2211-06** - z/OS V1R12.0 ICSF TKE Workstation User's Guide

Questions,
comments?