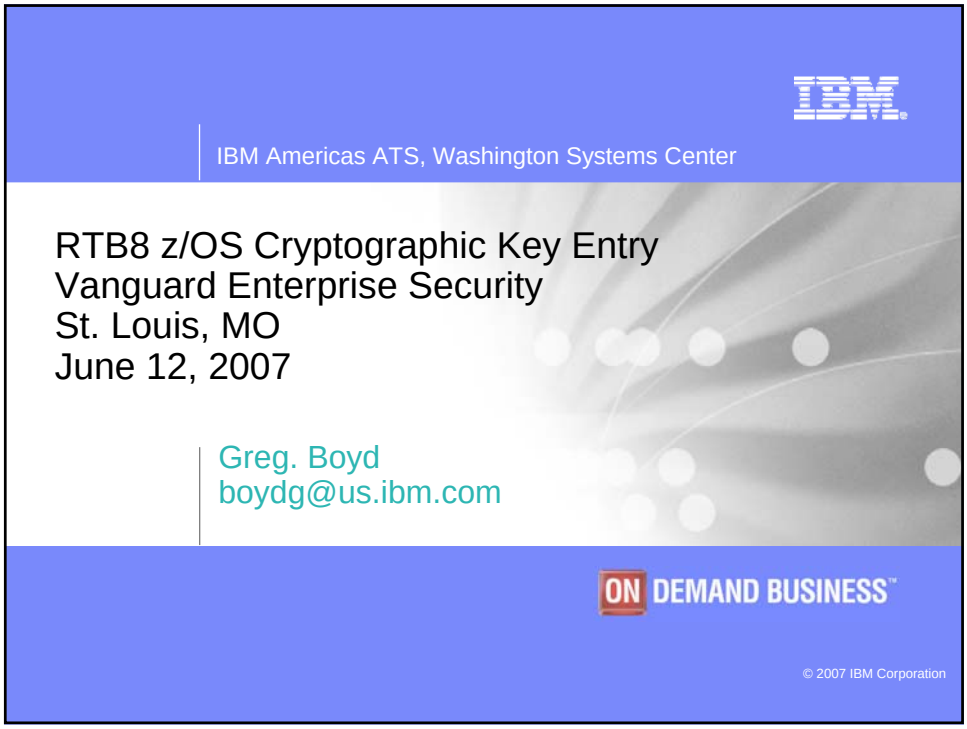


Disclaimer

The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation **of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.**

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

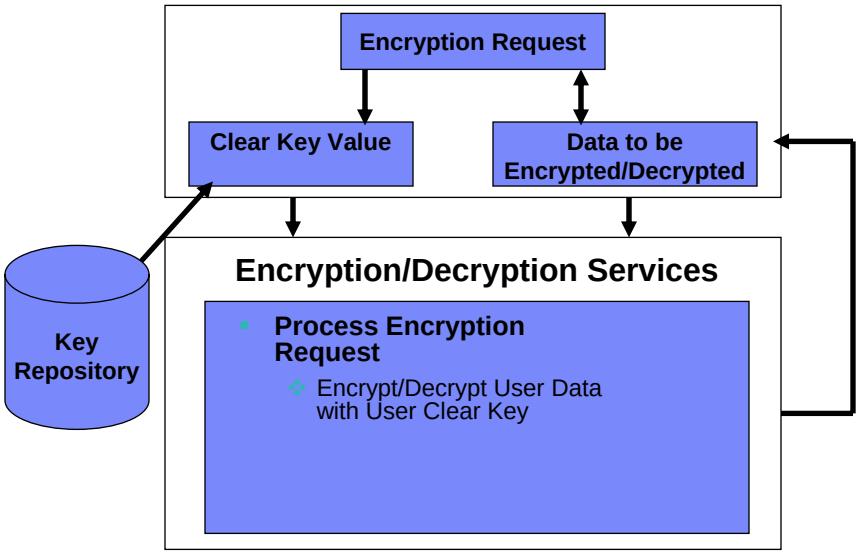
It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.

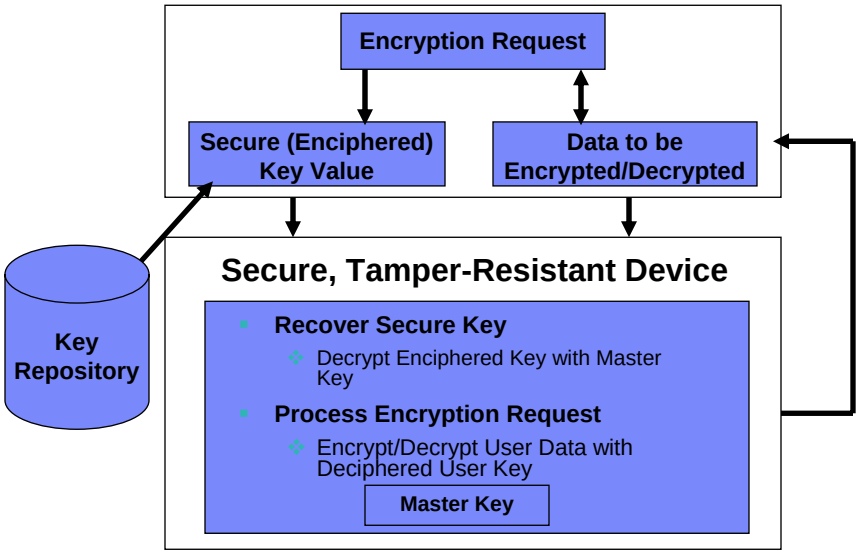
Agenda

- **Some Basics (Secure/Clear Keys, Crypto Hardware)**
- **Creating and Managing Master Keys**
- **Key Management Considerations**

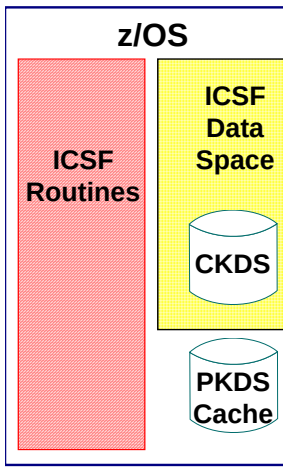
Clear Key Processing

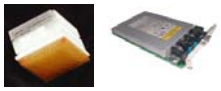


Secure Key Processing

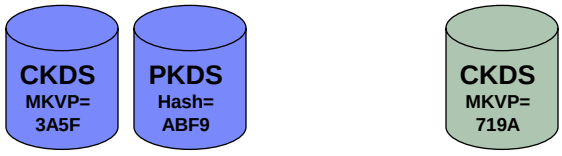


Keep In Sync – Hardware, ICSF Software, Storage





LPAR & Domain	DES Master Key			PKA Master key		
	Current	New	Old	Current	New	Old
LP1 UD1	ABC (MKVP=3A5F)			PKAMstKy (Hash=ABF9)		
LP15 UD9	LP15K (MKVP=719A)					



Key Entry

- **Master Keys**
  - Passphrase Initialization, PPINIT (Master Key Only)
  - ISPF Panels for ICSF (Master Key Only)
  - Trusted Key Entry Workstation
- **Operational Keys**
  - Trusted Key Entry Workstation
  - Key Generation Utility Program (KGUP)
  - APIs

ICSF Main Menu

```
HCR7730 ------------------ Integrated Cryptographic Service Facility ----------------------
OPTION ===>
 Enter the number of the desired option.
  1 COPROCESSOR MGMT  – Management of Cryptographic Processors
  2 Master Key        -- 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/CKDS 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.
```


Pass Phrase Initialization

```
----- ICSF - Pass Phrase MK/KDS Initialization -----
COMMAND ===>
 Enter your pass phrase and the names of the CKDS and PKDS:
   Pass Phrase (16 to 64 characters)
   ===>
   CKDS
   ===>
   PKDS
   ===>
   Initialize the CKDS and PKDS? (Y/N) ===> Y
   Initialize new PCIXCCs only ? (Y/N) ===> N
Press ENTER to process.
Press END   to exit to the previous menu.
```


ICSF Main Menu

```
HCR7730 ------------------ Integrated Cryptographic Service Facility ----------------
OPTION ===>
 Enter the number of the desired option.
  1 COPROCESSOR MGMT  – Management of Cryptographic Processors
  2 Master Key        -- 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/CKDS 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.
```


ICSF Coprocessor Management Screen

```
------------------------- 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.
  COPROCESSOR          SERIAL NUMBER          STATUS
  --------------------  ----------------------  ------------
  .  A0                                        ACTIVE
  .  A1                                        ACTIVE
  .  A2                                        ACTIVE
  .  A3                                        ACTIVE
 S  X04                 93001166               ACTIVE
 S  X05                 93001449               ACTIVE
```


ICSF Panels – Display Hardware Status

```
------------------------------------------- ICSF – Coprocessor Hardware Status -------------------------------------------
COMMAND ===>                                                          Crypto Domain:  3
REGISTER STATUS                    COPROCESSOR X04          COPROCESSOR X05
Crypto Serial Number          :    93001166                 93001449
Status                        :    ACTIVE                   ACTIVE
Symmetric-Keys 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      :    B0070E6F8F31B3C2         B0070E6F8F31B3C2
    Hash pattern              :    4181A04120413B35         4181A04120413B35
              ...

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


ICSF Panels – Display Hardware Status (cont.)

```
------------------------------------- ICSF – Coprocessor Hardware Status -------------------------------------
COMMAND ===>                                                          Crypto Domain:  3
REGISTER STATUS                COPROCESSOR X04          COPROCESSOR X05

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            :  69723AECF26FAA80         69723AECF26FAA80
                              :  CE8771914F05D03A         CE8771914F05D03A

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


ICSF Main Menu

```
HCR7730 ------------------- Integrated Cryptographic Service Facility --------------------
OPTION ===>
 Enter the number of the desired option.
  1 COPROCESSOR MGMT  – Management of Cryptographic Processors
  2 Master Key        -- 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/CKDS 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.
```


ICSF Utility Menu

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

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


ICSF Panels – Random Number Generator

```
------------ ICSF – Random Number Generator ------------
COMMAND ===>
Enter data below:

  Parity Option     ===> RANDOM                 ODD, EVEN, RANDOM
  Random Number1   :  7AD08F3EC17940B3          Random Number 1
  Random Number2   :  76EFE59438982A08          Random Number 2
  Random Number3   :  26041F0DFBF19D83          Random Number 3




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


ICSF Panels – Checksum Calculation

```
------------ ICSF – Checksum and Verification and Hash Pattern ------------
COMMAND ===>
Enter data below:
  Key Type   ===>                          (Selection panel displayed if blank)
  Key Value  ===> 7AD08F3EC17490B3         Input key value 0 - 7
             ===> 76EFE59438982A08         Input key value 8 - 15
             ===> 26041F0DFBF19D83         Input key value 16 – 23 (PKA 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

```
------------ ICSF – Checksum and Verification and Hash Pattern ------------
COMMAND ===>
Enter data below:
  Key Type   ===> MASTER                   (Selection panel displayed if blank)
  Key Value  ===> 7AD08F3EC17490B3         Input key value 0 - 7
             ===> 76EFE59438982A08         Input key value 8 - 15
             ===> 0000000000000000         Input key value 16 – 23 (PKA Keys only)

Checksum         : 2D                     Check digit for key value
Key Part VP      : 8809D948E06CED41       Verification Pattern
Key Part HP      : 5ACDE16BE799E722       Hash Pattern
                 : 95C92A87A6612955

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


ICSF Main Menu

```
HCR7730 ------------------- Integrated Cryptographic Service Facility ---------------------
OPTION ===>
 Enter the number of the desired option.
  1 COPROCESSOR MGMT  – Management of Cryptographic Processors
  2 Master Key        -- 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/CKDS 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.
```


ICSF Coprocessor Management Screen

```
------------------------- 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.
  COPROCESSOR          SERIAL NUMBER          STATUS
  --------------------  ----------------------  ------------
  .  A0                                        ACTIVE
  .  A1                                        ACTIVE
  .  A2                                        ACTIVE
  .  A3                                        ACTIVE
  e  X04                93001166               ACTIVE
  e  X05                93001449               ACTIVE
```


ICSF Panels – 1st Key Part

```
------------ ICSF – Clear Master Key Entry -----------
COMMAND ===>
          Symmetric-keys new master key register      : EMPTY
          Asymmetric-keys new master key register     : EMPTY
Specify information below
   Key Type       ===>              (SYM-MK, ASYM-MK)
   Part           ===>              (RESET, FIRST, MIDDLE, FINAL)
   Checksum       ===>    00
   Key Value      ===>    0000000000000000
                  ===>    0000000000000000
                  ===>    0000000000000000          (ASYM-MK only)


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


ICSF Panels – 1st Key Part (Before)

```
------------ ICSF – Clear Master Key Entry -----------
COMMAND ===>
          Symmetric-keys new master key register      : EMPTY
          Asymmetric-keys new master key register     : EMPTY
Specify information below
   Key Type       ===>    SYM-MK  (SYM-MK, ASYM-MK)
   Part           ===>    FIRST   (RESET, FIRST, MIDDLE, FINAL)
   Checksum       ===>    2D
   Key Value      ===>    7AD08F3EC17940B3
                  ===>    76EFE59438982A08
                  ===>    0000000000000000          (ASYM-MK only)


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


ICSF Panels – 1st Key Part (After)

```
------------ ICSF – Clear Master Key Entry -----------
COMMAND ===>
          Symmetric-keys new master key register      : PART FULL
          Asymmetric-keys new master key register     : EMPTY
Specify information below
   Key Type        ===>    SYM-MK  (SYM-MK, ASYM-MK)
   Part            ===>    FIRST     (RESET, FIRST, MIDDLE, FINAL)
   Checksum        ===>    00
   Key Value       ===>    0000000000000000
                   ===>    0000000000000000
                   ===>    0000000000000000          (ASYM-MK only)
Entered key part   VP:  8809D948E06CED41
                   HP:  5ACDE16BE799E722  95C92A87A6612955
                            (Record and secure these patterns)
Press ENTER to process.
Press END   to exit to the previous menu.
```


ICSF Panels – 2nd Key Part (Before)

```
------------ ICSF – Clear Master Key Entry -----------
COMMAND ===>
          Symmetric-keys new master key register      : PART FULL
          Asymmetric-keys new master key register     : EMPTY
Specify information below
   Key Type        ===>    SYM-MK  (SYM-MK, ASYM-MK)
   Part            ===>    MIDDLE  (RESET, FIRST, MIDDLE, FINAL)
   Checksum        ===>    FF
   Key Value       ===>    CE548C08EAA42A89
                   ===>    0EBF346B9408258A
                   ===>    0000000000000000          (ASYM-MK only)




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


ICSF Panels – 2nd Key Part (After)

```
------------ ICSF – Clear Master Key Entry -----------
COMMAND ===>
          Symmetric-keys new master key register      : PART FULL
          Asymmetric-keys new master key register     : EMPTY
Specify information below
   Key Type        ===>    SYM-MK  (SYM-MK, ASYM-MK)
   Part            ===>    MIDDLE  (RESET, FIRST, MIDDLE, FINAL)
   Checksum        ===>    00
   Key Value       ===>    0000000000000000
                   ===>    0000000000000000
                   ===>    0000000000000000          (ASYM-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)

```
------------ ICSF – Clear Master Key Entry -----------
COMMAND ===>
          Symmetric-keys new master key register      : PART FULL
          Asymmetric-keys new master key register     : EMPTY
Specify information below
   Key Type        ===>    SYM-MK  (SYM-MK, ASYM-MK)
   Part            ===>    FINAL   (RESET, FIRST, MIDDLE, FINAL)
   Checksum        ===>    64
   Key Value       ===>    BF57AD3D94CEAD62
                   ===>    C73491832638F7EF
                   ===>    0000000000000000          (ASYM-MK only)
Press ENTER to process.
Press END   to exit to the previous menu.
```


ICSF Panels – 3rd Key Part (After)

```
----------- ICSF – Clear Master Key Entry -----------
COMMAND ===>
            Symmetric-keys new master key register   : FULL
            Asymmetric-keys new master key register  : EMPTY
Specify information below
   Key Type          ===>     SYM-MK   (SYM-MK, ASYM-MK)
   Part              ===>     FINAL    (RESET, FIRST, MIDDLE, FINAL)
   Checksum          ===>     00
   Key Value         ===>     0000000000000000
                     ===>     0000000000000000
                     ===>     0000000000000000              (ASYM-MK only)
Entered key part   VP:  3FFEAC6F32912B2F   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

```
------------------------- 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.
  COPROCESSOR          SERIAL NUMBER          STATUS
  --------------------  ----------------------  ------------
 .  A0                                         ACTIVE
 .  A1                                         ACTIVE
 .  A2                                         ACTIVE
 .  A3                                         ACTIVE
 S  X04                 93001166               ACTIVE
 S  X05                 93001449               ACTIVE
```


ICSF Panels – Display Hardware Status

```
------------------------------------------------- ICSF – Coprocessor Hardware Status ----------------------------
COMMAND ===>                                                                          Crypto Domain: 3
REGISTER STATUS                    COPROCESSOR X04                 COPROCESSOR X05
Crypto Serial Number          :           93001166                        93001449
Status                        :    ACTIVE                          ACTIVE
Symmetric-Keys Master Key
  New Master Key register     :    FULL                            FULL
    Verification pattern      :     3FFEAC6F32912B2F                3FFEAC6F32912B2F
    Hash pattern              :     1FC752887DA6ED24                1FC752887DA6ED24
  Old Master Key register     :    EMPTY                           EMPTY
    Verification pattern      :
    Hash pattern              :
                              :
  Current Master Key  register:    VALID                           VALID
    Verification pattern      :    B0070E6F8F31B3C2                 B0070E6F8F31B3C2
    Hash pattern              :    4181A04120413B35                4181A04120413B35
              ...

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


ICSF Main Menu

```
HCR7730 ------------------- Integrated Cryptographic Service Facility --------------------
OPTION ===>
 Enter the number of the desired option.
  1 COPROCESSOR MGMT  – Management of Cryptographic Processors
  2 Master Key        -- 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/CKDS 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.
```


ICSF Panels – CKDS/PKDS Access

```
------------ ICSF – Administrative Control Functions ------------  Row 1 to 4
COMMAND ===>

  Active CKDS:        hlq.YOUR.CKDS
  Active PKDS:        hlq.YOUR.PKDS

  To change the status of a control, enter the appropriate character
  (E – Enable, D – Disable)  and press Enter.

    FUNCTION                                  STATUS
    --------------                            -----------
d   Dynamic CKDS Access                       ENABLED
_   PKA Callable Services                     ENABLED
_   PKDS Read Access                          ENABLED
_   PKDS Write, Create, and Delete Access     ENABLED

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


ICSF Main Menu

```
HCR7730 ------------------- Integrated Cryptographic Service Facility ---------------------
OPTION ===>
 Enter the number of the desired option.
  1 COPROCESSOR MGMT  – Management of Cryptographic Processors
  2 Master Key        -- 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/CKDS 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.
```


ICSF Master Key Management

```
---------------------------------- ICSF – Master Key Management ----------------------------------
OPTION ===>
 Enter the number of the desired option.
  1 INIT/REFRESH CKDS     – Initialize a Cryptographic Key Data Set or activate
                            an updated Cryptographic Key Data Set
  2 SET MK                - Set a DES/symmetric-keys master key
  3 REENCIPHER CKDS       - Reencipher the CKDS prior to changing the
                            DES/symmetric-keys  master key
  4 CHANGE MK             - Change the DES/symmetric-keys master key  and
                            activate the reenciphered CKDS
  5 INITIALIZE PKDS       - Initialize or update a PKDS Cryptographic Key Data
                            Set header record
  6 REENCIPHER PKDS       - Reencipher the PKA Cryptographic Key Data Set
  7 ACTIVATE PKDS         - Activate the PKDS after it has been enciphered
  8 REFRESH CACHE         - Refresh the PKDS cache if enabled
Press ENTER to go to the selected option.
Press END   to exit to the previous menu.
```


ICSF Reencipher CKDS

```
-------------------------------- ICSF – Reencipher CKDS --------------------------------
COMMAND ===>

To reencipher all CKDS entries from encryption under the current
DES/symmetric-master keys master key to encryption under the new
master key enter the CKDS names below

   Input   CKDS ===>
  Output CKDS ===>

Press ENTER to reencipher the CKDS.
Press END   to exit to the previous menu.
```


ICSF Change Master Key

```
------------------------------ ICSF – Change Master Key ------------------------------
COMMAND ===>

Enter the name of the new CKDS below.

   New CKDS ===>

   When the master key is changed, the new CKDS will become active.



Press ENTER to change the master key.
Press END   to exit to the previous menu.
```


ICSF Master Key Management

```
--------------------------------- ICSF – Master Key Management ---------------------------------
OPTION ===>
 Enter the number of the desired option.
  1 INIT/REFRESH CKDS     – Initialize a Cryptographic Key Data Set or activate
                            an updated Cryptographic Key Data Set
  2 SET MK                - Set a DES/symmetric-keys master key
  3 REENCIPHER CKDS       - Reencipher the CKDS prior to changing the
                            DES/symmetric-keys  master key
  4 CHANGE MK             - Change the DES/symmetric-keys master key  and
                            activate the reenciphered CKDS
  5 INITIALIZE PKDS       - Initialize or update a PKDS Cryptographic Key Data
                            Set header record
  6 REENCIPHER PKDS       - Reencipher the PKA Cryptographic Key Data Set
  7 ACTIVATE PKDS         - Activate the PKDS after it has been enciphered
  8 REFRESH CACHE         - Refresh the PKDS cache if enabled
Press ENTER to go to the selected option.
Press END   to exit to the previous menu.
```


ICSF Initialize a CKDS

```
--------------------------------- ICSF – Initialize a CKDS ---------------------------------
COMMAND ===>
 Enter the number of the desired option.
    1 Initialize and empty CKDS (creates the header and system keys)
    2 REFRESH   -  Activate an updated CKDS

 Enter the name of the CKDS below.

    CKDS ===>

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


Steps for Changing the SYM-MK

From the ICSF Admin Guide:

1. **Enter the SYM-MK key parts**
2. **Disable CKDS Access**
3. **Re-encipher the CKDS under the new master key**
4. **Change the Master Key and Activate the Reenciphered CKDS**
5. **Enable CKDS Access**
6. **Change the ICSF Options data set to point to the new CKDS**

ICSF Master Key Management

```
---------------------------------- ICSF – Master Key Management ----------------------------------
OPTION ===>
 Enter the number of the desired option.
  1 INIT/REFRESH CKDS     – Initialize a Cryptographic Key Data Set or activate
                            an updated Cryptographic Key Data Set
  2 SET MK                - Set a DES/symmetric-keys master key
  3 REENCIPHER CKDS       - Reencipher the CKDS prior to changing the
                            DES/symmetric-keys  master key
  4 CHANGE MK             - Change the DES/symmetric-keys master key  and
                            activate the reenciphered CKDS
  5 INITIALIZE PKDS       - Initialize or update a PKDS Cryptographic Key Data
                            Set header record
  6 REENCIPHER PKDS       - Reencipher the PKA Cryptographic Key Data Set
  7 ACTIVATE PKDS         - Activate the PKDS after it has been enciphered
  8 REFRESH CACHE         - Refresh the PKDS cache if enabled
Press ENTER to go to the selected option.
Press END   to exit to the previous menu.
```


ICSF Initialize a PKDS

```
------------------ ICSF – Initialize PKA Cryptographic Key Data Set -----------
COMMAND ===>

Enter the name of the new PKDS below.

   PKDS ===>




Press ENTER to initialize the PKDS.
Press END   to exit to the previous menu.
```


ICSF Panels – CKDS/PKDS Access

```
----------- ICSF – Administrative Control Functions -----------  Row 1 to 4
COMMAND ===>

  Active CKDS:        hlq.YOUR.CKDS
  Active PKDS:        hlq.YOUR.PKDS

  To change the status of a control, enter the appropriate character
  (E – Enable, D – Disable)  and press Enter.

    FUNCTION                                  STATUS
    --------------                            -----------
_   Dynamic CKDS Access                       ENABLED
d   PKA Callable Services                     ENABLED
d   PKDS Read Access                          ENABLED
d   PKDS Write, Create, and Delete Access     ENABLED

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


ICSF Reencipher a PKDS

```
---------------------------- ICSF – Reencipher PKDS -------------------------
COMMAND ===>


To reencipher all PKDS entries from encryption under the old
   signature/asymmetric master key to encryption under the
   current master key enter the PKDS names below.


   Input   PKDS ===>

   Output PKDS ===>


Press ENTER to reencipher the PKDS.

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


ICSF Activate a PKDS

---------- ICSF – Activate PKA Cryptographic Key Data Set --------

COMMAND ===>

Enter the name of the new PKDS below.

New PKDS ===>

Press ENTER to activate the PKDS.

Press END to exit to the previous menu.

ICSF Master Key Management

---------- ICSF – Master Key Management ----------

OPTION ===>

Enter the number of the desired option.

1 INIT/REFRESH CKDS	**– Initialize a Cryptographic Key Data Set or activate an updated Cryptographic Key Data Set**
2 SET MK	**- Set a DES/symmetric-keys master key**
3 REENCIPHER CKDS	**- Reencipher the CKDS prior to changing the DES/symmetric-keys master key**
4 CHANGE MK	**- Change the DES/symmetric-keys master key and activate the reenciphered CKDS**
5 INITIALIZE PKDS	**- Initialize or update a PKDS Cryptographic Key Data Set header record**
6 REENCIPHER PKDS	**- Reencipher the PKA Cryptographic Key Data Set**
7 ACTIVATE PKDS	**- Activate the PKDS after it has been enciphered**
8 REFRESH CACHE	**- Refresh the PKDS cache if enabled**

Press ENTER to go to the selected option.

Press END to exit to the previous menu.

Steps for Changing the ASYM-MK

From the ICSF Admin Guide:

1. **Disable PKA Services**
2. **Enter the ASYM-MK key parts**
3. **Re-encipher the PKDS under the new master key**
4. **Activate the PKDS**
5. **Enable PKA Services**
6. **Enable PKA read, write, create and delete access**

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 SYM-MK changed? The ASYM-MK?**
- **How Often are Application Keys changed?**
- **Is crypto a part of change management?**
- **How are changes implemented/coordinated across the SYSPLEX?**

References

- **Publications**
  - ICSF System Programmer's Guide SA22-7520
  - ICSF Administration Guide, SA22-7521
  - ICSF Application Programmer's Guide SA22-7522
  - ICSF TKE Workstatoin User's Guide, SA22-7524
- **ATS TechDocs Web Site**
  www.ibm.com/support/techdocs
  - SEARCH ALL DOCUMENTS, keyword of Crypto
    - TD101580 Implications of Cryptographic Key Pass Phrase Initialization
    - WP100647 A Clear Key / Secure Key Primer
    - A number of documents on Application Keys

Questions …

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

APPN*
CICS*
DB2*
e-business logo*
Enterprise Storage Server*
ESCON*
FICON
FICON Express
GDPS*
HiperSockets
HiperSpace
IBM*
IBM eServer
IBM logo*
IMS
Multiprise*
MVS
On demand business logo
OS/390*
Parallel Sysplex*
Performance Toolkit for z/VM
PR/SM
pSeries*
RACF*
Redbook
Resource Link
RMF
S/390*
Sysplex Timer*
TotalStorage*
Virtual Image Facility
VM/ESA*
VSE/ESA
VTAM*
WebSphere*
z/Architecture
z/OS*
z/VM*
zSeries*
zSeries Entry License Charge

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries or both.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.