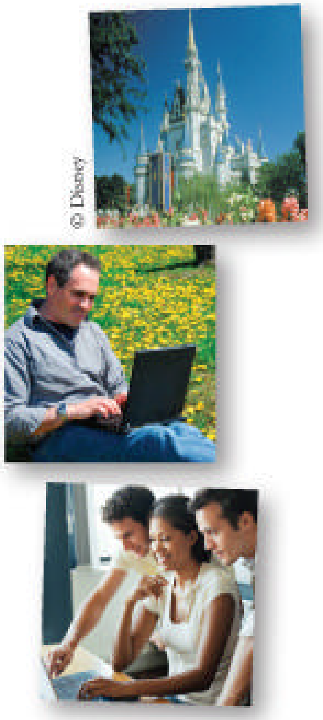
SHARE
Technology • Connections • Results

Integrated Cryptographic Services Facility (ICSF) Installation, Setup, and Customization

Jessica Bonner
IBM

February 26, 2007
Session Number 5523



Trademarks

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

- IBM
- RACF
- s/390
- z/OS
- zSeries
- z9

The following are trademarks or registered trademarks of other companies.

- American Express
- MasterCard
- RSA
- SET
- VISA

Other company, product, and service names may be trademarks or service marks of others.

Objective

To give an overview of zSeries Crypto Hardware and of ICSF software

- cryptographic hardware
- customize and initialize software

SHARE
Technology · Connections · Results

Cryptographic Hardware

Cryptographic Coprocessors

Model	Installed Coprocessors	Optional Coprocessors
z900 z800	CCF	PCICC PCICA
Z990 Z890	None	PCIXCC CEX2C PCICA
Z9	None	CEX2C CEX2A

z900/z800 Cryptographic Hardware

- **Cryptographic Coprocessor Feature (CCF)**
  - up to two CCFs are standard with most z900/z800 servers
  - enablement requires a Power On Reset
  - symmetric and asymmetric functions supported
  - certified at FIPS 140-1 level 4
- **PCI Cryptographic Coprocessor (PCICC)**
  - optional feature with CCF systems
  - non-disruptive enablement
  - symmetric and asymmetric functions supported
  - User Defined Extensions (UDX) support
  - certified at FIPS 140-1 level 4

z990/z890 Cryptographic Hardware

- **PCI Cryptographic Accelerator (PCICA)**
  - optional feature with zSeries only
  - no enablement feature
  - can be shared across 16 LPARs
  - clear key SSL en/decryption only
- **PCI X Cryptographic Coprocessor (PCIXCC) / Crypto Express2 Coprocessor (CEX2C)**
  - optional feature with z990/z890 only
  - non-disruptive enablement
  - replacement for the CCF and PCICC
  - symmetric and asymmetric functions supported
  - UDX support
  - can be shared across 16 LPARs
  - designed for FIPS 140-2 level 4 certification

z9 EC/z9 BC Cryptographic Hardware

- Crypto Express2
  - optional feature with z9 EC/z9 BC only
  - can be shared across 16 LPARs
  - CEX2 can be configured as either CEX2C or CEX2A.

  - Configured as an Accelerator
    - Accelerator performs RSA acceleration only.
    - Used for RSA clear key operations in CSNDDSV, CSNDPKD, and CSNDPKE.

  - Configured as a coprocessor
    - non-disruptive enablement
    - replacement for the CCF and PCICC
    - symmetric and asymmetric functions supported
    - UDX support
    - designed for FIPS 140-2 level 4 certification

CP Assist for Cryptographic Functions

CP Assist for Cryptographic Functions (CPACF) is available on every CP of a z9 BC, z9 EC, z990 or z890.

CPACF does not contain master key and CAN NOT do secure operations.

CPACF functions include:

- SHA-1 hashing
- Modification detection code (MDC) message authentication*
- Clear key DES/TDES encryption/decryption*
- AES supported in software only by ICSF

Additional CPACF functions on z9

- AES-128
- SHA-256

Implemented via new problem state instructions published in z/Architecture Principles of Operations

*Requires CPACF enablement feature 3863 for export control

Cryptographic Features

Maximum number of allowable features by model

Coprocessor (number of coprocessors per feature)	z900 z800	z990 z890	z9 EC z9 BC
PCICC(2)	8	-	-
PCICA(2)	6	6	-
PCIXCC(1)	-	8	-
CEX2C(2)	-	8	-
CEX2C/A(2)	-	-	8

Maximum number of installed features is 8

Crypto Domain

- The cryptographic coprocessor uses virtualization to share the card with 16 logical partitions.
  - up to 16 logical partitions can concurrently access a cryptographic coprocessor
- Secure coprocessors have 16 physical domains
  - each domain has its own set of master key registers
- Appears as a dedicated coprocessor to the partition

Trusted Key Entry update?

- TKE is an optional feature on zSeries processors.
- TKE workstation consists of an application on xSeries machine with a 4764 card.
- Provides secure remote administration of all cryptographic coprocessors.
  - one TKE workstation can manage multiple systems
- Features include:
  - TCP/IP connection between workstation and host
  - authentication between host and administrators
  - master key and operational key entry in parts
  - storage of key parts on smart cards
  - key parts are encrypted when sent to host
  - enabling/disabling cryptographic functions
  - protection against replay attacks
  - SMF audit trail of activity

Hardware Setup

Hardware Setup

Hardware setup from the hardware master console (HMC) requires three basic steps:

- **Hardware installation (done by IBM)**
  - installation of CPACF feature 3863
  - installation of PCICA/PCIXCC/CEX2C
- **LPAR definition (done by customer)**
  - assign domain to partition
  - assign cryptographic coprocessor to the partition
- **TKE enablement**
  - enable TKE access to secure cryptographic coprocessor

Cryptographic Software

Integrated Cryptographic Service Facility

- ICSF is the software interface to the cryptographic hardware.
- ICSF is part of the cryptographic server component of z/OS.
- ICSF provides TSO panel interfaces to
  - Enter keys into the tamper-resistant hardware
  - Create and manage keys for application use
  - Display status and manage cryptographic hardware
- ICSF maintains three VSAM data sets for application cryptographic keys.
  - Cryptographic Key Data Set (CKDS) for symmetric keys
  - Public Key Data Set (PKDS) for asymmetric keys
  - Token Key Data Set (TKDS) for PKCS#11 tokens
- ICSF provides application interfaces to 70+ callable services.

Enhancements - HCR7720

Web deliverable – z/OS V1R6 and z/OS V1R7

- Support for 64 – bit virtual for selected services.
- As security enhancement for CPACF use, support for clear DES keys in CKDS via KGUP and CKDS I/O services, to be passed by label in CSNBSYE and CSNBSYD
- Support for 19 digit PAN in CVV_Generate and CVV_Verify services.
- Support for CEX2C coprocessor.

Enhancements – HCR7731

Web Deliverable – Available on z/OS V1R6, z/OS V1R7, and z/SO V1R8.

- Support for Remote Key Loading – z9 Only
  - Public key based ATM key management compliant with ANSI x9.24-2.
  - New verbs: Trusted Block Create (CSNDTBC) and Remote Key Export (CSNDKRX).
  - PKCS support for trusted blocks.
  - Additional enhancements in CSNDPKI, CSNDDSV, and CSNDKTC.
- Support for ICSO 16609 CBC TDES MAC in MAC_generation and MAC_verification services.

Enhancements – HCR7740

Available only on z/OS V1R9 and only on zSeries hardware

- ICSF now supports PKCS#11 on z/OS
  - ICSF has implemented virtual PKCS#11 tokens to support multi-user environments
  - NEW Token Key Dataset (TKDS) for storing PKCS#11 objects
- Random Number Generate – Added that on a Cryptographic Coprocessor Feature only SMK-MK set is required.

Enhancements – HCR7750

Web Deliverable – Available on z/OS V1R7, z/OS V1R8, and z/SO V1R9.

- 4096-bit RSA key support on the Crypto Express2 Coprocessor card
  - 17 API were updated
- Support for ISO-3 PIN block format was added to 6 callable services
- New callable service Random Number Generate Long (CSFNBRNGL and CSNERNGL), now allows a user to specify the length when generating a random number
- Limited the retained key functionality

ICSF Setup

ICSF Setup

Refer to the z/OS Program Directory for installation instructions.

The following steps are detailed in the z/OS ICSF System Programmer’s Guide, SA22-7520.

- Customize SYS1.PARMLIB
- Allocate the CKDS, PKDS, and optionally the TKDS
- Create the installation options data set
- Provide access to the ICSF panels
- Create the ICSF startup procedure
- Start ICSF

Customize SYS1.PARMLIB

- Add CEE.SCEERUN and CSF.SCSFMOD0 to the LNKLST concatenation.
- APF authorize CSF.SCSFMOD0, if LNKAUTH=APFTAB.
- In the IKJTSOxx member, add CSFDAUTH and CSFDPKDS in the AUTHPGM and AUTHTSF parameter lists.
- If using TKE V3.0 or later, add CSFTTKE to the AUTHCMD parameter list.

Allocate the CKDS, PKDS, & TKDS

- The CKDS, PKDS, and TKDS are VSAM data sets. Use the AMS DEFINE CLUSTER command to define the data sets.
- Sample jobs are documented in z/OS ICSF System Programmer's Guide.
- Sample jobs are provided in SYS1.SAMPLIB. The JCL to allocate the CKDS, PKDS, and TKDS are different.
  - Sample job CSFCKDS to allocate the CKDS
  - Sample job CSFPKDS to allocate the PKDS
  - Sample job CSFTKDS to allocate the TKDS
- Allocate the data sets on a permanently resident volume.
- Ensure this volume is not subject to data set migration.
- Use RACF profiles to protect these data sets.

JCL to allocate a CKDS/PKDS

SYS1.SAMPLIB(CSFCKDS)

```
//CSFCKDS   JOB <JOB CARD PARAMETERS>
//DEFINE  EXEC PGM=IDCAMS,REGION=4M
//SYSPRINT DD  SYSOUT=*
//SYSIN DD *
 DEFINE CLUSTER (NAME(CSF.CSFCKDS)        -
           VOLUMES(XXXXXX)         -
           RECORDS(100 50)         -
           RECORDSIZE(252,252)     -
           KEYS(72 0)              -
           FREESPACE(10,10)        -
           SHAREOPTIONS(2)         -
           UNIQUE)                 -
       DATA (NAME(CSF.CSFCKDS.DATA)  -
           BUFFERSPACE(100000)     -
           ERASE                   -
           WRITECHECK)             -
      INDEX (NAME(CSF.CSFCKDS.INDEX))
/*
```

SYS1.SAMPLIB(CSFPKDS)

```
//CSFPKDS   JOB <JOB CARD PARAMETERS>
//DEFINE  EXEC PGM=IDCAMS,REGION=4M
//SYSPRINT DD  SYSOUT=*
//SYSIN DD *
 DEFINE CLUSTER (NAME(CSF.CSFPKDS)        -
           VOLUMES(XXXXXX)         -
           RECORDS(100,50)         -
           RECORDSIZE(350,2800)    -
           KEYS(72 0)              -
           FREESPACE(0,0)          -
           SHAREOPTIONS(2,3)       -
           UNIQUE)                 -
       DATA (NAME(CSF.CSFPKDS.DATA)  -
           BUFFERSPACE(100000)     -
           ERASE                   -
           CISZ(8192)              -
           WRITECHECK)             -
      INDEX (NAME(CSF.CSFPKDS.INDEX))
/*
```

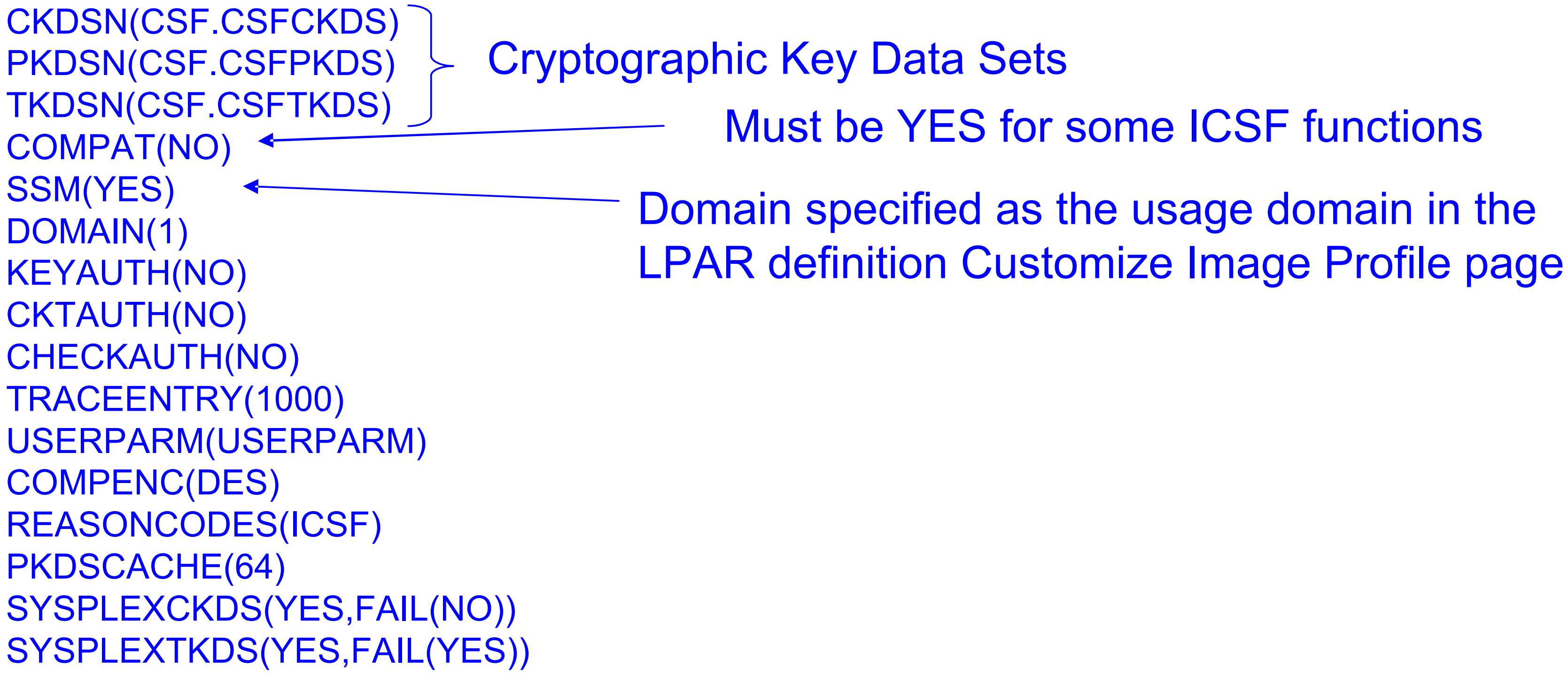
JCL to allocate a TKDS

SYS1.SAMPLIB(CSFTKDS)

```
//CSFCKDS   JOB <JOB CARD PARAMETERS>
//DEFINE  EXEC PGM=IDCAMS,REGION=4M
//SYSPRINT DD  SYSOUT=*
//SYSIN DD *
  DEFINE CLUSTER (NAME(CSF.CSFTKDS)         -
                 VOLUMES(XXXXXX)            -
                 RECORDS(100 50)            -
                 RECORDSIZE(2200 32756)     -
                 KEYS(72 0)                 -
                 FREESPACE(0 0)             -
                 SPANNED                    -
                 SHAREOPTIONS(2 3)          -
                 UNIQUE)                    -
           DATA (NAME(CSF.CSFTKDS.DATA)    -
                 BUFFERSPACE(100000)        -
                 ERASE                      -
                 WRITECHECK)                -
          INDEX (NAME(CSF.CSFTKDS.INDEX))
/*
```

Installation Options Data Set

- Defines the run time options for ICSF.
- Becomes active when ICSF is started.
- Samples are provided in z/OS ICSF System Programmer’s Guide and in SYS1.SAMPLIB(CSFPRM00).
- System symbols are supported.
- Should be stored in SYS1.PARMLIB.



```
CKDSN(CSF.CSFCKDS)
PKDSN(CSF.CSFPKDS)
TKDSN(CSF.CSFTKDS)
COMPAT(NO)
SSM(YES)
DOMAIN(1)
KEYAUTH(NO)
CKTAUTH(NO)
CHECKAUTH(NO)
TRACEENTRY(1000)
USERPARM(USERPARM)
COMPENC(DES)
REASONCODES(ICSF)
PKDSCACHE(64)
SYSPLEXCKDS(YES,FAIL(NO))
SYSPLEXTKDS(YES,FAIL(YES))
```

Cryptographic Key Data Sets

Must be YES for some ICSF functions

Domain specified as the usage domain in the LPAR definition Customize Image Profile page

Options Performance Guidance

- On a z/890 and above with secure coprocessors, code KEYAUTH(NO)!
- KEYAUTH(YES) causes a MAC_verification to be performed on the instorage CKDS record.
  - The function drives to the card, and can be devastating to performance.
  - For example, and CSNBPTR call with IPINENC and OPINENC keys in the CKDS would need three trips to the crypto card – two to verify the two CKDS key records, and one to do the real CSNBPTR work. So what could be 1000 calls / second without the MAC_verification drops to perhaps 400 with verification of both records.
  - We could afford to do this on the CCFs (although we believe it had no real value) but the cost on a CEX2C is too high.

Options Performance Guidance Cont.

- CKTAUTH is new, and controls if CKDS records are to be MAC_verified as they are read into storage during ICSF startup.
- For very large CKDS, performance cost of a MAC_verify in the coprocessor could significantly impact time to start ICSF.
- CKTAUTH(NO) bypasses the MAC_verify.
- MAC_verify still performed during REFRESH and REENCIPHER processing, no matter how CKTAUTH is coded.

Access to ICSF Panels

- Create an ICSF option on the ISPF Primary Option Menu.
- Update TSO logon procedure
  - //SYSPROC DD …
    - add CSF.SCSFCLI0
  - //ISPPLIB DD …
    - add CSF.SCSFPNL0
  - //ISPMLIB DD …
    - add CSF.SCSFMSG0
  - //ISPSLIB DD …
    - add CSF.SCSFSKL0
  - //ISPTLIB DD …
    - add CSF.SCSFTLIB

ICSF Startup Procedure

```
//CSF PROC
//CSF EXEC PGM=CSFMMAIN,REGION=6M,TIME=1440
//CSFLIST DD SYSOUT=A,LRECL=132,BLKSIZE=132,HOLD=YES
//CSFPARM DD DSN=SYS1.PARMLIB(CSFPRM00),DISP=SHR
```

- CSFLIST data set contains messages pertaining to ICSF startup.
  - Messages are documented in z/OS ICSF Messages, SA22-7523.
- CSFPARM points to the installation options data set member.

ICSF First Time Startup Messages

```
S CSF
$HASP373 CSF    STARTED
IEF403I CSF - STARTED - TIME=14.12.39
CSFM507I CRYPTOGRAPHY - THERE ARE NO CRYPTOGRAPHIC COPROCESSORS
      ONLINE.
CSFM508I CRYPTOGRAPHY - THERE ARE NO CRYPTOGRAPHIC ACCELERATORS
      ONLINE.
CSFM122I PKA SERVICES WERE NOT ENABLED DURING ICSF INITIALIZATION.
CSFM001I ICSF INITIALIZATION COMPLETE
CSFM400I CRYPTOGRAPHY - SERVICES ARE NOW AVAILABLE.
```

CPACF only

```
S CSF
$HASP100 CSF    ON STCINRDR
$HASP373 CSF    STARTED
IEF403I CSF - STARTED - TIME=09.35.52
CSFM411I PCI CRYPTOGRAPHIC ACCELERATOR A00 IS ACTIVE
CSFM507I CRYPTOGRAPHY - THERE ARE NO CRYPTOGRAPHIC COPROCESSORS
      ONLINE.
CSFM122I PKA SERVICES WERE NOT ENABLED DURING ICSF INITIALIZATION.
CSFM001I ICSF INITIALIZATION COMPLETE
CSFM400I CRYPTOGRAPHY - SERVICES ARE NOW AVAILABLE.
```

CPACF and PCICA

ICSF First Time Startup Messages

With PCIXCC or CEX2C, master keys must be loaded and CKDS/PKDS must be initialized.

```
S CSF
$HASP373 CSF    STARTED
IEF403I CSF - STARTED - TIME=17.59.05
CSFM101E PKA KEY DATA SET, CSF.CSFPKDS IS NOT INITIALIZED.
CSFM419E INCORRECT MASTER KEY (SYM) ON PCI X CRYPTOGRAPHIC COPROCESSOR
X01, SERIAL NUMBER 93006015.
CSFM434E INCORRECT MASTER KEY (SYM) ON CRYPTO EXPRESS2 COPROCESSOR E02,
SERIAL NUMBER 94006004.
CSFM434E INCORRECT MASTER KEY (SYM) ON CRYPTO EXPRESS2 COPROCESSOR E03,
SERIAL NUMBER 94006026.
CSFM411I PCI CRYPTOGRAPHIC ACCELERATOR A00 IS ACTIVE
CSFM100E CRYPTOGRAPHIC KEY DATA SET, CSF.CSFCKDS IS NOT INITIALIZED.
CSFM122I PKA SERVICES WERE NOT ENABLED DURING ICSF INITIALIZATION.
CSFM001I ICSF INITIALIZATION COMPLETE
CSFM400I CRYPTOGRAPHY - SERVICES ARE NOW AVAILABLE.
```

Master Keys

ICSF uses two master keys to protect application keys:

- Symmetric-keys master key (SYM-MK)
  - 128 bit key
  - protects DES (or symmetric) application keys
- Asymmetric-keys master key (ASYM-MK)
  - 192 bit key
  - protects RSA (or asymmetric) private keys

Stored within the secure hardware boundary of the cryptographic coprocessor

Master Key Entry

There are three methods for ICSF master key entry:

- **Pass Phrase Initialization**
  - master key values derived from a character string 16 to 64 characters long
  - limited to initializing ICSF only
- **Clear master key entry from ICSF panels**
  - can be used to initialize or change master keys
  - keys can be entered in parts
  - key values can be generated using the random number generator utility
- **Trusted Key Entry (TKE) workstation**
  - can manage all cryptographic coprocessors from one TKE workstation
  - keys can be entered in parts
  - key values can be generated and saved to binary files or smart cards

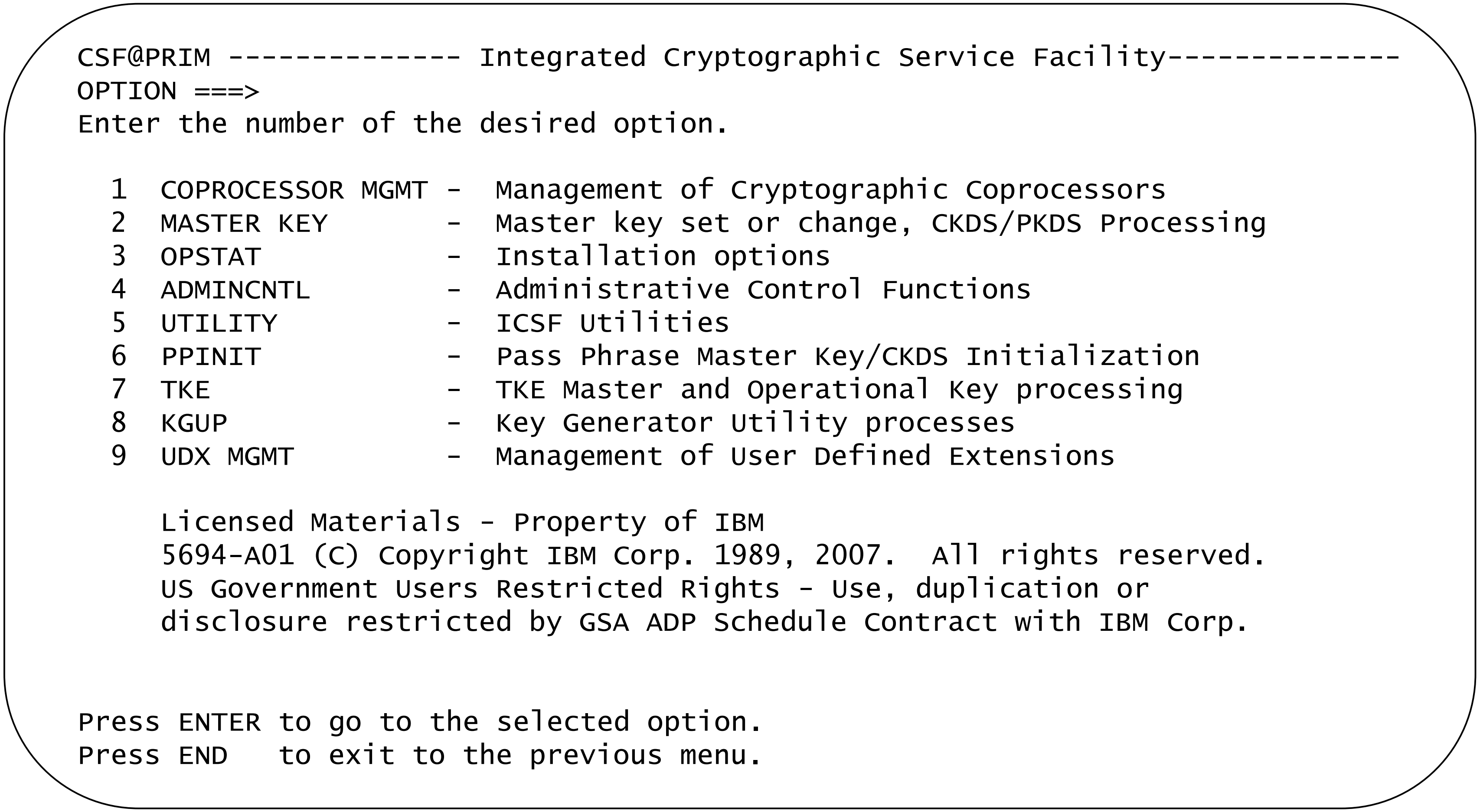
Recommendation for ICSF Initialization

1. Use Pass Phrase to initialize ICSF quickly with minimal effort.
2. Change the master keys using ICSF Clear Master Key entry panels.

Reasons:

- Random number generate is not active until ICSF has been initialized.
- Entering master keys in parts is more secure
  - key parts can be assigned to different people

ICSF Main Panel



```
CSF@PRIM -------------- Integrated Cryptographic Service Facility--------------
OPTION ===>
Enter the number of the desired option.

  1  COPROCESSOR MGMT -  Management of Cryptographic Coprocessors
  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

     Licensed Materials - Property of IBM
     5694-A01 (C) Copyright IBM Corp. 1989, 2007.  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 Panel Functions

TSO panels are provided to perform the following functions:

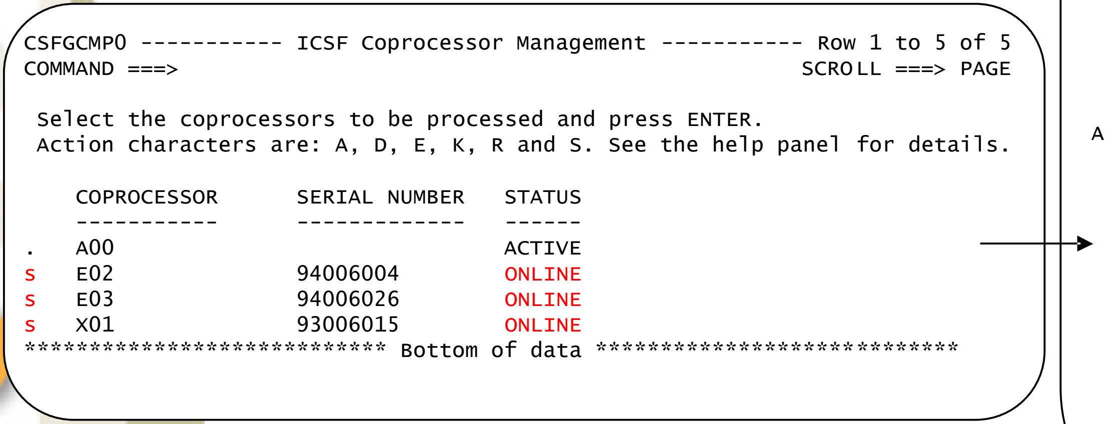
- display coprocessor hardware status
- deactivate/activate coprocessors
- load master keys
- initialize or reencipher the CKDS/PKDS
- refresh the CKDS, refresh the PKDS cache
- set or change the symmetric-keys master key
- activate a reenciphered PKDS
- pass phrase initialization
- manage application cryptographic keys in the CKDS using KGUP
- generate random numbers
- calculate checksum
- enable/disable PKA callable services
- enable/disable CKDS/PKDS create, write, delete access
- complete TKE load operations

PF1 from any panel will display HELP panels.

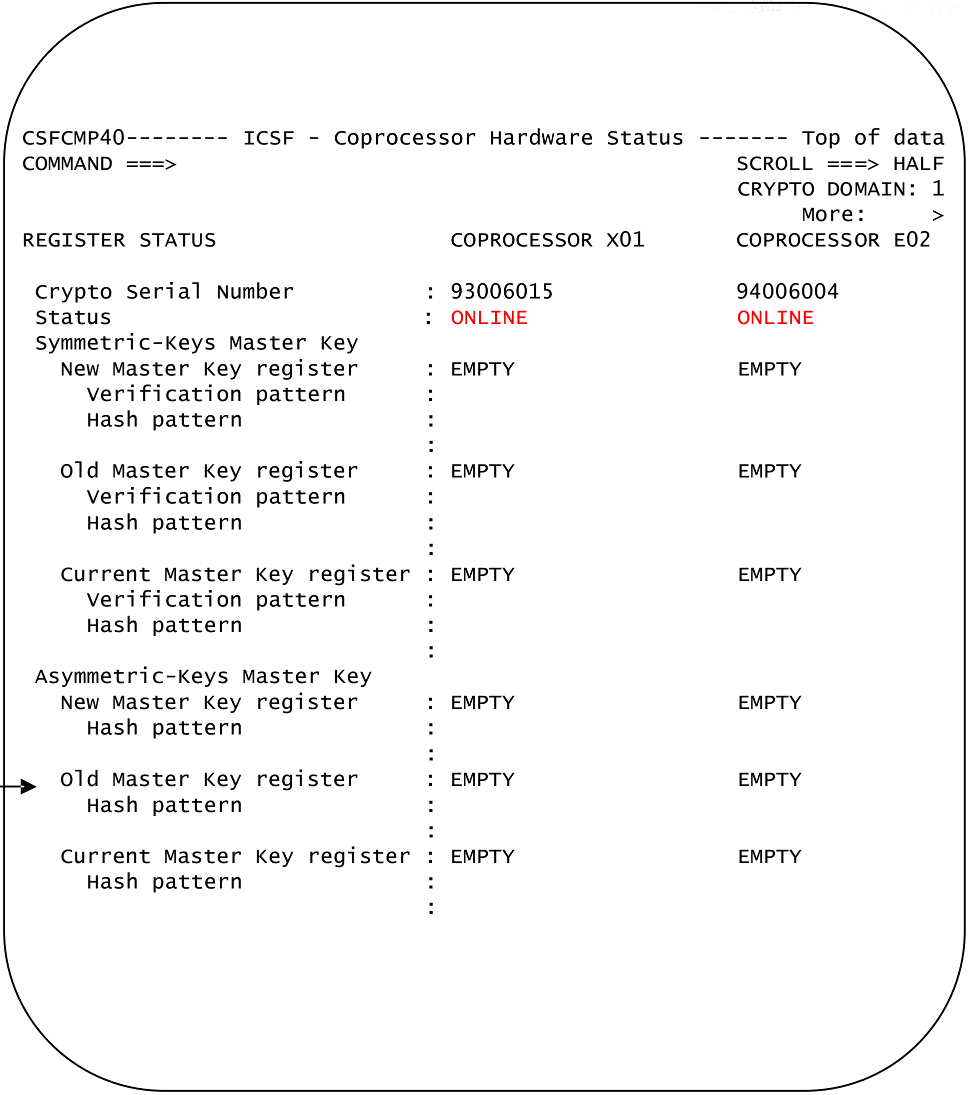
Coprocessor Hardware Status

At first time startup, the status of the secure cryptographic coprocessors is ONLINE and all the master key registers are empty.

Select option 1 COPROCESSOR MGMT from ICSF Main Panel.



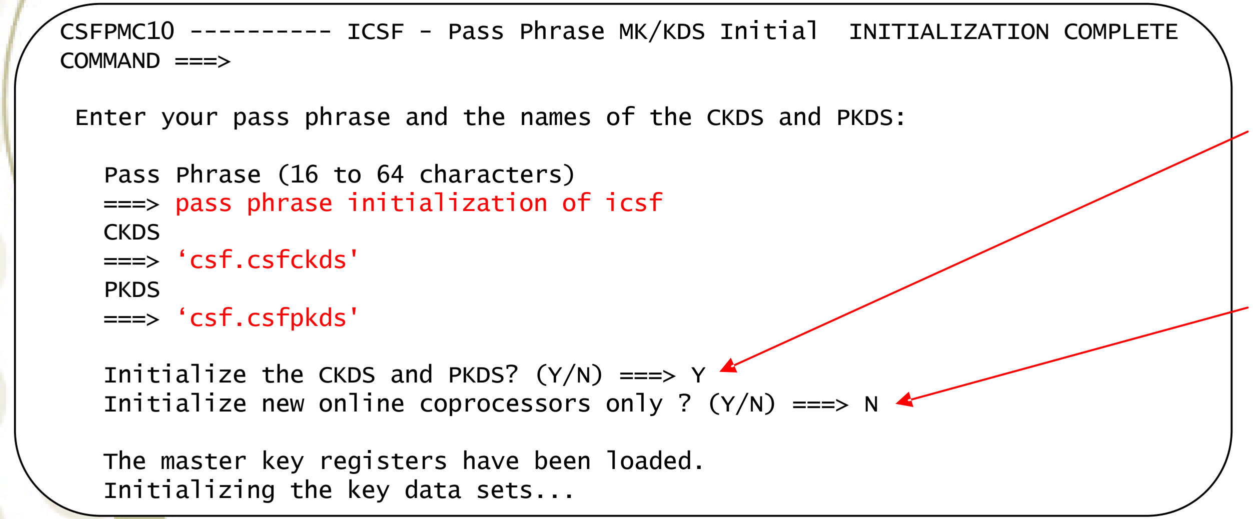
```
CSFGCMP0 ----------- ICSF Coprocessor Management ----------- Row 1 to 5 of 5
COMMAND ===>                                                 SCROLL ===> PAGE

 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
    -----------      -------------   ------
.   A00                              ACTIVE
s   E02              94006004        ONLINE
s   E03              94006026        ONLINE
s   X01              93006015        ONLINE
**************************** Bottom of data ****************************
```



```
CSFCMP40-------- ICSF - Coprocessor Hardware Status ------- Top of data
COMMAND ===>                                                SCROLL ===> HALF
                                                        CRYPTO DOMAIN: 1
                                                             More:     >
REGISTER STATUS                  COPROCESSOR X01       COPROCESSOR E02

 Crypto Serial Number          : 93006015              94006004
 Status                        : ONLINE                ONLINE
 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 : EMPTY                 EMPTY
     Verification pattern      :
     Hash pattern              :
                               :
 Asymmetric-Keys Master Key
   New Master Key register     : EMPTY                 EMPTY
     Hash pattern              :
                               :
   Old Master Key register     : EMPTY                 EMPTY
     Hash pattern              :
                               :
   Current Master Key register : EMPTY                 EMPTY
     Hash pattern              :
                               :
```

Pass Phrase Initialization

Select option 6 PPINIT from ICSF Main Panel.

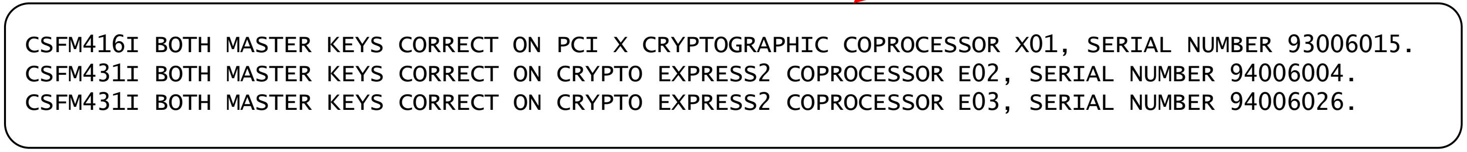


```
CSFPMC10 ---------- ICSF - Pass Phrase MK/KDS Initial  INITIALIZATION COMPLETE
COMMAND ===>

 Enter your pass phrase and the names of the CKDS and PKDS:

   Pass Phrase (16 to 64 characters)
   ===> pass phrase initialization of icsf
   CKDS
   ===> ‘csf.csfckds'
   PKDS
   ===> ‘csf.csfpkds'

   Initialize the CKDS and PKDS? (Y/N) ===> Y
   Initialize new online coprocessors only ? (Y/N) ===> N

   The master key registers have been loaded.
   Initializing the key data sets...
```

must be ‘Y’ if CKDS/PKDS are empty

useful if synchronizing master key values in newly plugged PCIXCC or CEX2C

operator console messages indicating that master keys have been successfully loaded

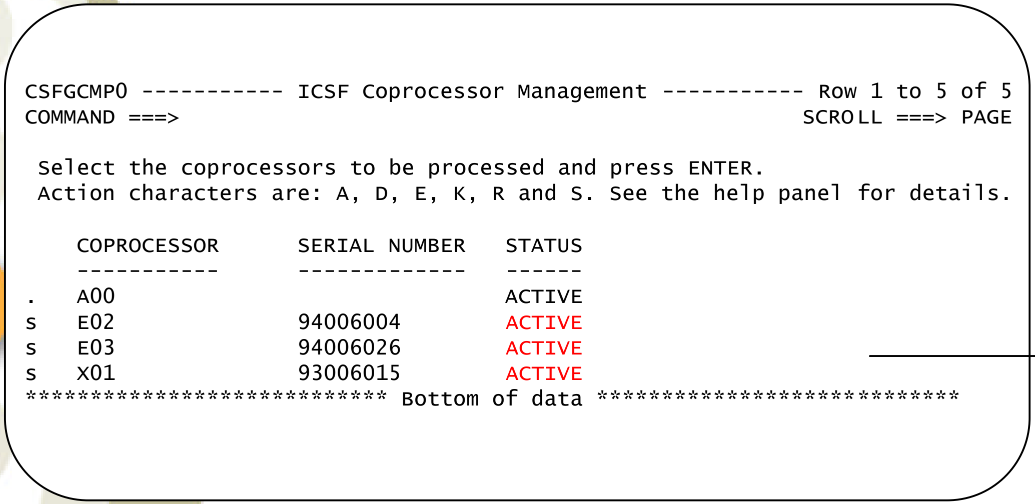


```
CSFM416I BOTH MASTER KEYS CORRECT ON PCI X CRYPTOGRAPHIC COPROCESSOR X01, SERIAL NUMBER 93006015.
CSFM431I BOTH MASTER KEYS CORRECT ON CRYPTO EXPRESS2 COPROCESSOR E02, SERIAL NUMBER 94006004.
CSFM431I BOTH MASTER KEYS CORRECT ON CRYPTO EXPRESS2 COPROCESSOR E03, SERIAL NUMBER 94006026.
```

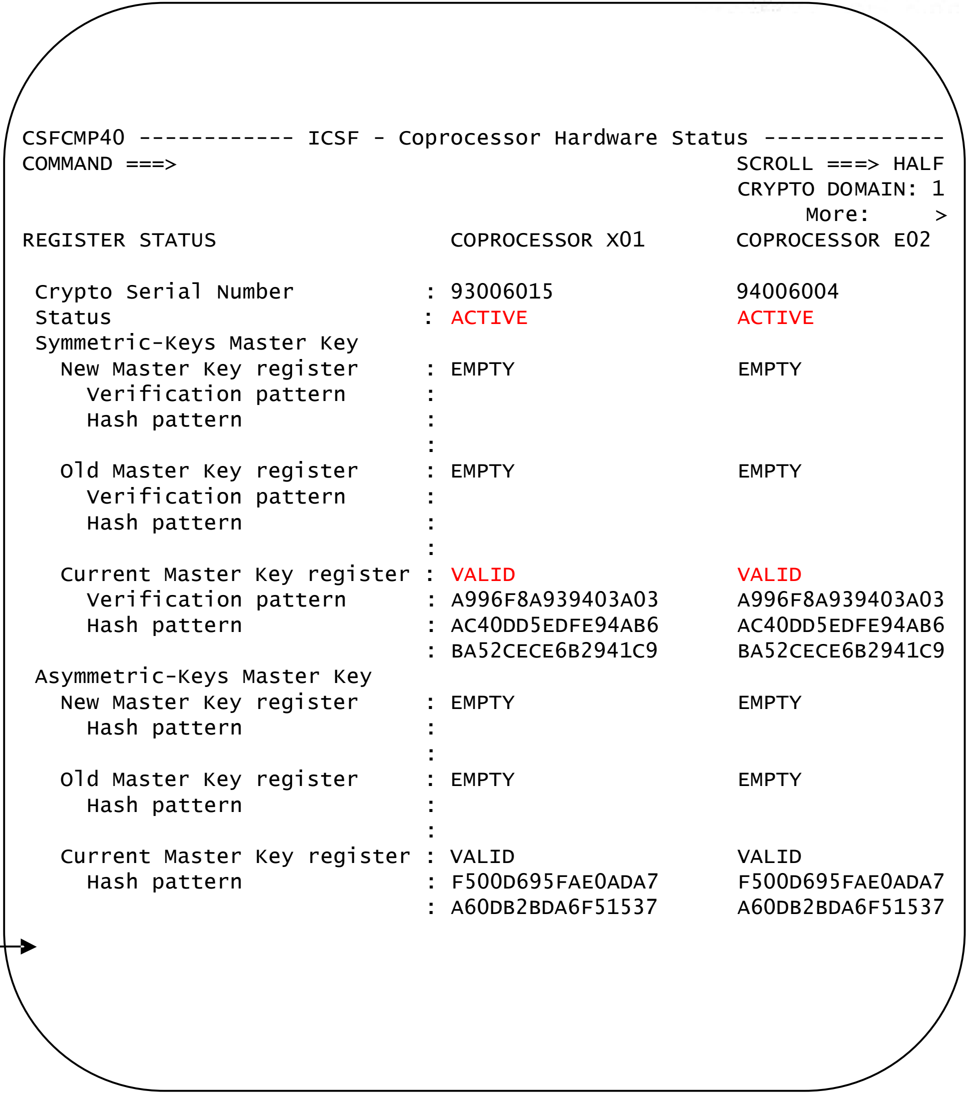
Coprocessor Hardware Status

The status of the secure coprocessors is now ACTIVE and the current master key registers are VALID.

Select option 1 COPROCESSOR MGMT from the ICSF Main Panel.



```
CSFGCMP0 ----------- ICSF Coprocessor Management ----------- Row 1 to 5 of 5
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
    -----------       -------------    ------
.   A00                                ACTIVE
s   E02               94006004         ACTIVE
s   E03               94006026         ACTIVE
s   X01               93006015         ACTIVE
**************************** Bottom of data ****************************
```



```
CSFCMP40 ------------ ICSF - Coprocessor Hardware Status --------------
COMMAND ===>                                           SCROLL ===> HALF
                                                       CRYPTO DOMAIN: 1
                                                            More:     >
REGISTER STATUS                  COPROCESSOR X01       COPROCESSOR E02

 Crypto Serial Number          : 93006015              94006004
 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      : A996F8A939403A03      A996F8A939403A03
     Hash pattern              : AC40DD5EDFE94AB6      AC40DD5EDFE94AB6
                               : BA52CECE6B2941C9      BA52CECE6B2941C9
 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              : F500D695FAE0ADA7      F500D695FAE0ADA7
                               : A60DB2BDA6F51537      A60DB2BDA6F51537
```

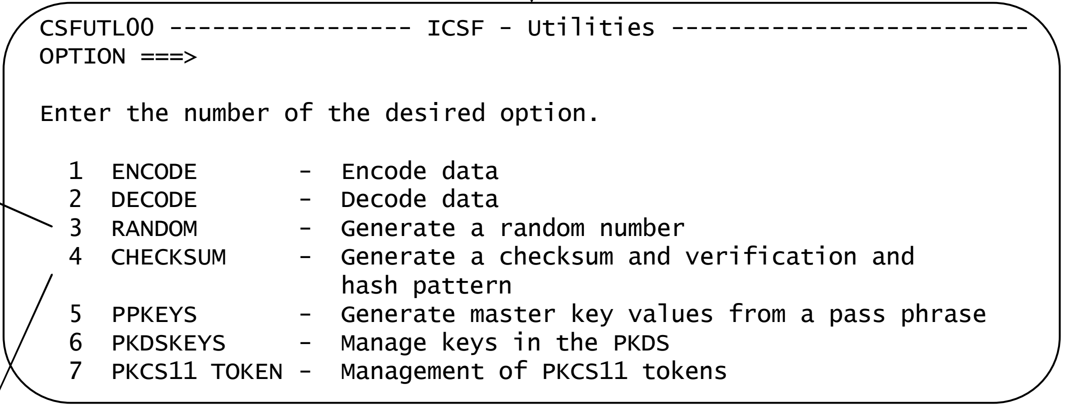
Steps to Change the Master Keys

1. Define empty CKDS/PKDS.
2. **Generate key values using Random Number Generator utility.**
3. **Calculate checksum for key value using checksum utility.**
4. Disable PKA callable services.
5. Enter master key in parts.
6. Reencipher CKDS.
7. Change the SYM-MK master key.
8. Reencipher PKDS.
9. Activate the new PKDS.
10. Enable PKA callable services, PKDS read and write access.

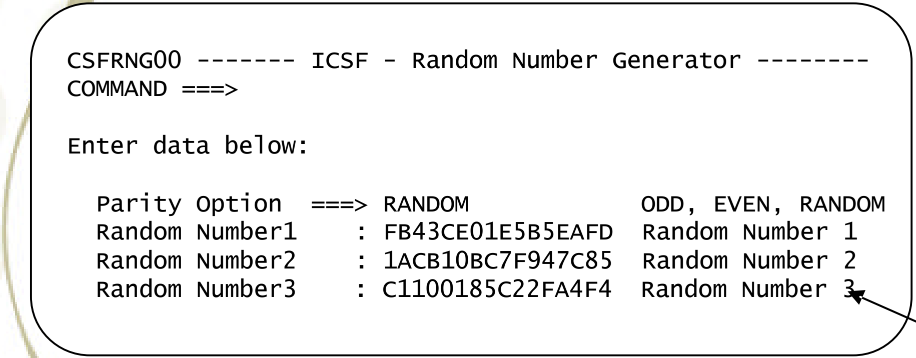
Detailed information on master key entry can be found in the z/OS ICSF Administrator’s Guide, SA22-7521.

Random Number Generator and Checksum Utilities

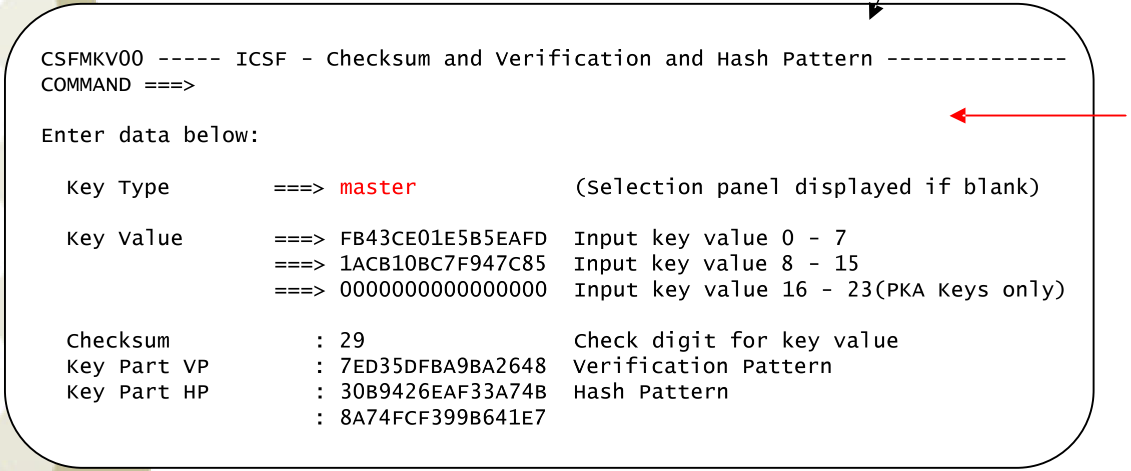
Select option 5 UTILITY from ICSF Main Panel



```
CSFUTL00 ----------------- 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
  6  PKDSKEYS      -  Manage keys in the PKDS
  7  PKCS11 TOKEN  -  Management of PKCS11 tokens
```



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

Enter data below:

  Parity Option  ===> RANDOM            ODD, EVEN, RANDOM
  Random Number1    : FB43CE01E5B5EAFD  Random Number 1
  Random Number2    : 1ACB10BC7F947C85  Random Number 2
  Random Number3    : C1100185C22FA4F4  Random Number 3
```



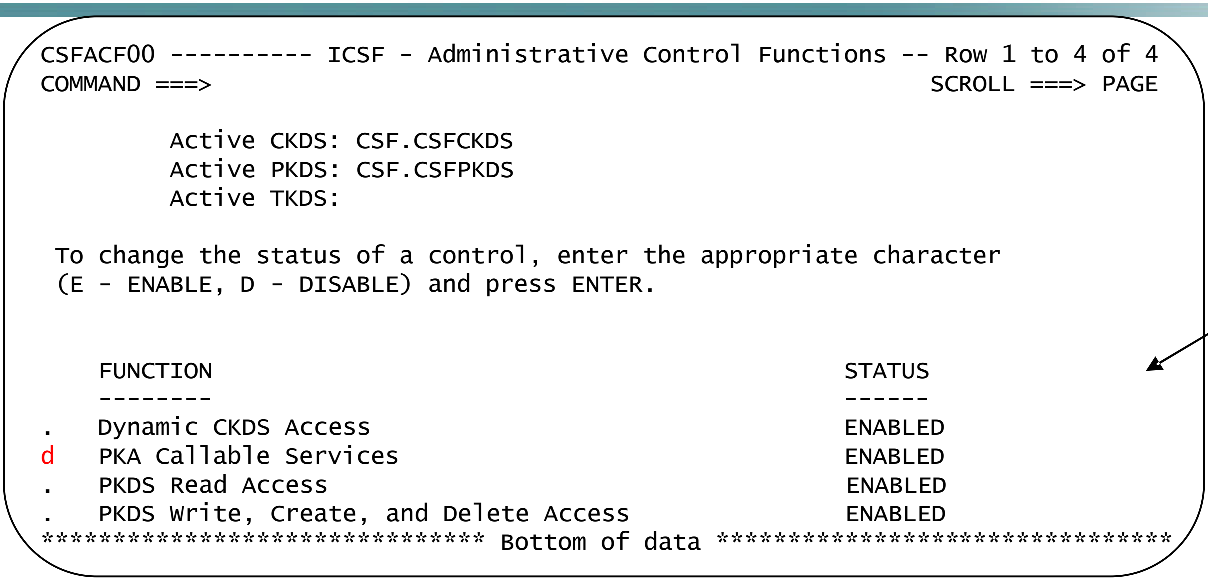
```
CSFMKV00 ----- ICSF - Checksum and Verification and Hash Pattern -------------
COMMAND ===>

Enter data below:

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

  Key Value       ===> FB43CE01E5B5EAFD  Input key value 0 - 7
                  ===> 1ACB10BC7F947C85  Input key value 8 - 15
                  ===> 0000000000000000  Input key value 16 - 23(PKA Keys only)

  Checksum           : 29                Check digit for key value
  Key Part VP        : 7ED35DFBA9BA2648  Verification Pattern
  Key Part HP        : 30B9426EAF33A74B  Hash Pattern
                     : 8A74FCF399B641E7
```

Enter MASTER for SYM-MK,
enter PKAMSTR for ASYM-MK,
or leave blank for key type selection panel

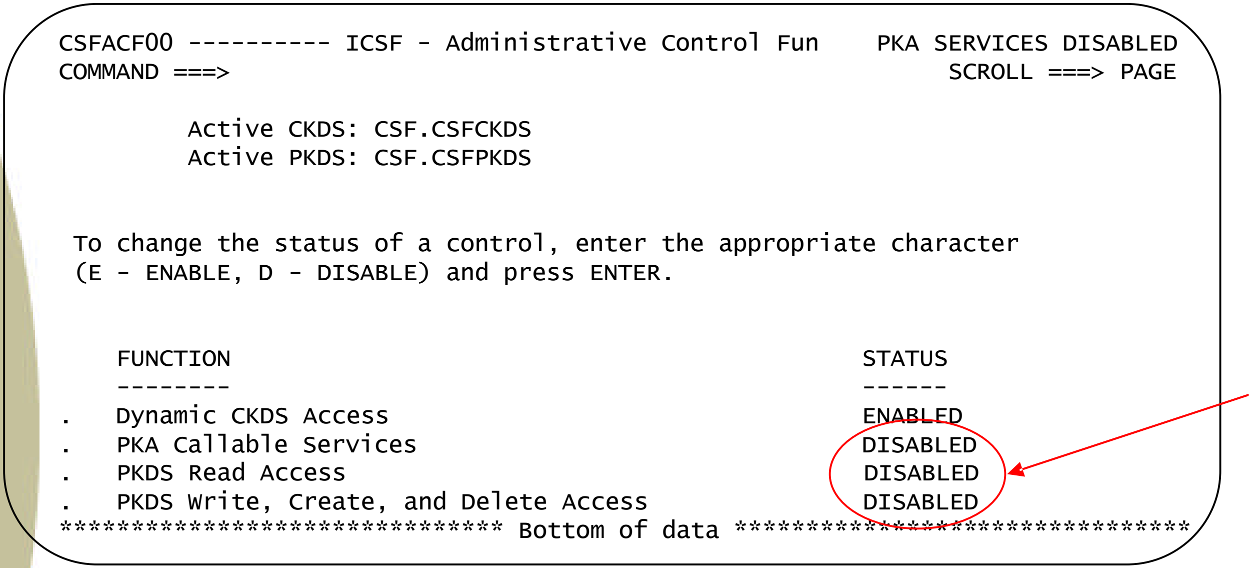
Steps to Change the Master Keys

1. Define empty CKDS/PKDS.
2. Generate key values using Random Number Generator utility.
3. Calculate checksum for key value using checksum utility.
4. **Disable PKA callable services.**
5. Enter master key in parts.
6. Reencipher CKDS.
7. Change the SYM-MK master key.
8. Reencipher PKDS.
9. Activate the new PKDS.
10. Enable PKA callable services, PKDS read and write access.

Disable PKA Callable Services



```
CSFACF00 ---------- ICSF - Administrative Control Functions -- Row 1 to 4 of 4
COMMAND ===>                                                   SCROLL ===> PAGE

         Active CKDS: CSF.CSFCKDS
         Active PKDS: CSF.CSFPKDS
         Active TKDS:

 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
.   PKDS Read Access                                     ENABLED
.   PKDS Write, Create, and Delete Access                ENABLED
******************************* Bottom of data ********************************
```



```
CSFACF00 ---------- ICSF - Administrative Control Fun    PKA SERVICES DISABLED
COMMAND ===>                                                   SCROLL ===> PAGE

         Active CKDS: CSF.CSFCKDS
         Active PKDS: CSF.CSFPKDS


 To change the status of a control, enter the appropriate character
 (E - ENABLE, D - DISABLE) and press ENTER.


    FUNCTION                                             STATUS
    --------                                             ------
.   Dynamic CKDS Access                                  ENABLED
.   PKA Callable Services                                DISABLED
.   PKDS Read Access                                     DISABLED
.   PKDS Write, Create, and Delete Access                DISABLED
******************************* Bottom of data ********************************
```

PKA callable services must be disabled before entering the ASYM-MK.

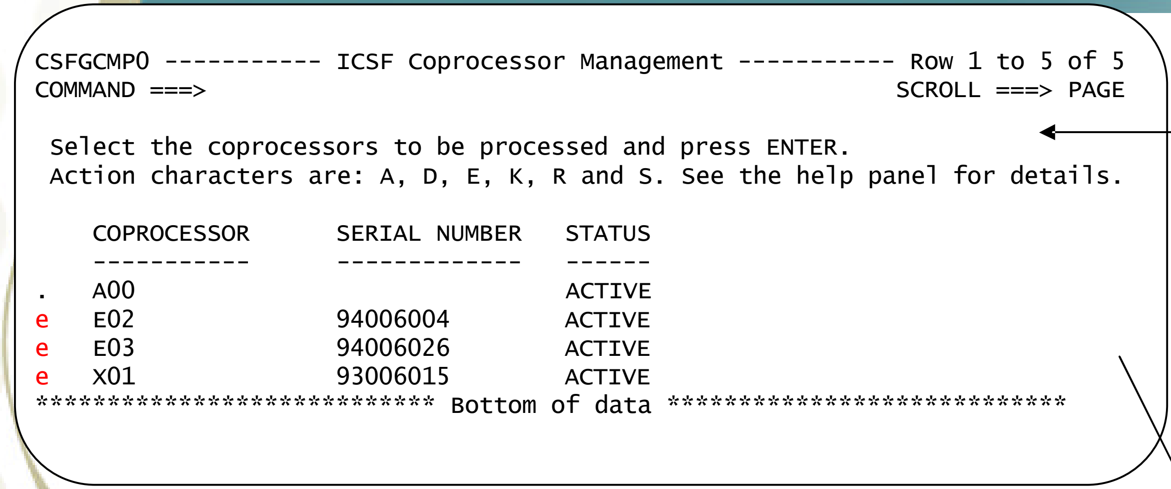
Select option 4 ADMINCNTL from the ICSF Main Panel.

Note: Disabling PKA Callable Services also disables PKDS Read Access and PKDS Write, Create, and Delete Access.

Steps to Change the Master Keys

1. Define empty CKDS/PKDS.
2. Generate key values using Random Number Generator utility.
3. Calculate checksum for key value using checksum utility.
4. Disable PKA callable services.
5. **Enter master key in parts.**
6. Reencipher CKDS.
7. Change the SYM-MK master key.
8. Reencipher PKDS.
9. Activate the new PKDS.
10. Enable PKA callable services, PKDS read and write access.

Clear Master Key Entry

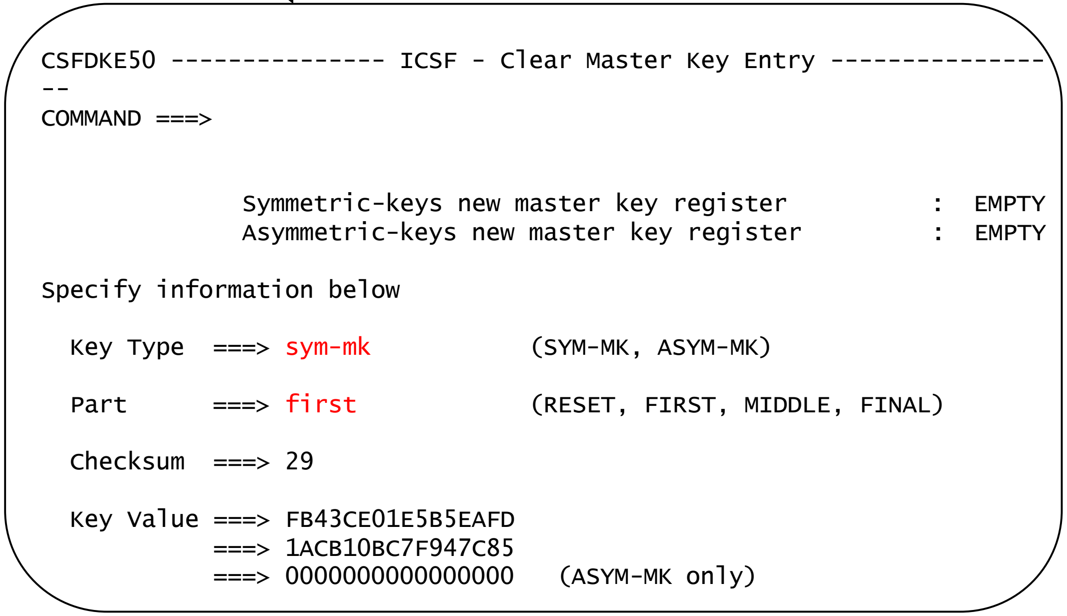


```
CSFGCMP0 ----------- ICSF Coprocessor Management ----------- Row 1 to 5 of 5
COMMAND ===>                                                  SCROLL ===> PAGE

 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
    -----------      -------------   ------
.   A00                              ACTIVE
e   E02              94006004        ACTIVE
e   E03              94006026        ACTIVE
e   X01              93006015        ACTIVE
**************************** Bottom of data ****************************
```

Select option 1 COPROCESSOR MGMT

from ICSF Main Panel.

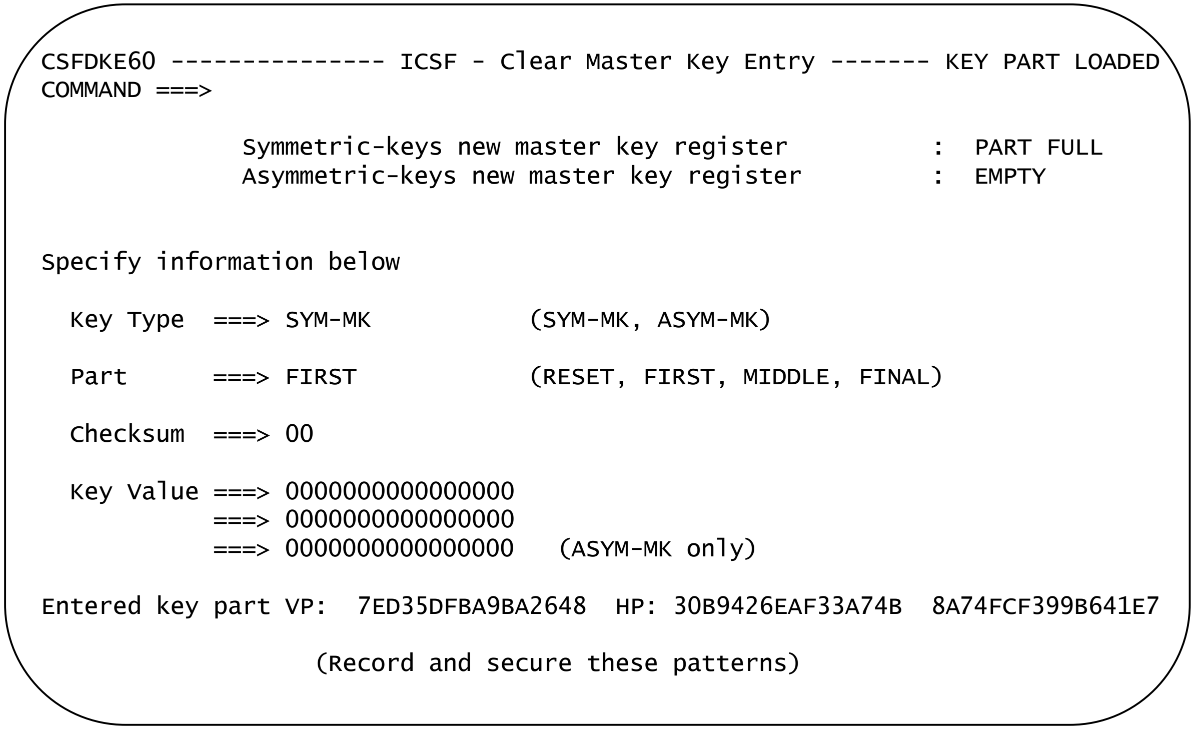
- Checksum and key value are copied from the random number generate and checksum panel.
- Enter SYM-MK or ASYM-MK for key type.
- Enter the key part – FIRST, MIDDLE, or FINAL.
  - FIRST and FINAL key parts are required.
  - MIDDLE key parts are optional. Multiple MIDDLE key parts are allowed.
  - Enter RESET to clear the master key register to restart the key entry process. Must reload FIRST key part.



```
CSFDKE50 --------------- 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  ===> 29

  Key Value ===> FB43CE01E5B5EAFD
            ===> 1ACB10BC7F947C85
            ===> 0000000000000000   (ASYM-MK only)
```

Clear Master Key Entry…cont

- Checksum and key value fields are cleared when the key part is loaded.
- Each key part is exclusive or-ed with the contents in the register
- Status of the new master key register is updated.
  - Status of SYM-MK new master key register changes from EMPTY-PART FULL-FULL
  - Status of ASYM-MK new master key register changes from EMPTY-PART FULL-EMPTY. The new ASYM-MK is set when the final key part is entered.



```
CSFDKE60 --------------- ICSF - Clear Master Key Entry ------- KEY PART LOADED
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:  7ED35DFBA9BA2648  HP: 30B9426EAF33A74B  8A74FCF399B641E7

                   (Record and secure these patterns)
```

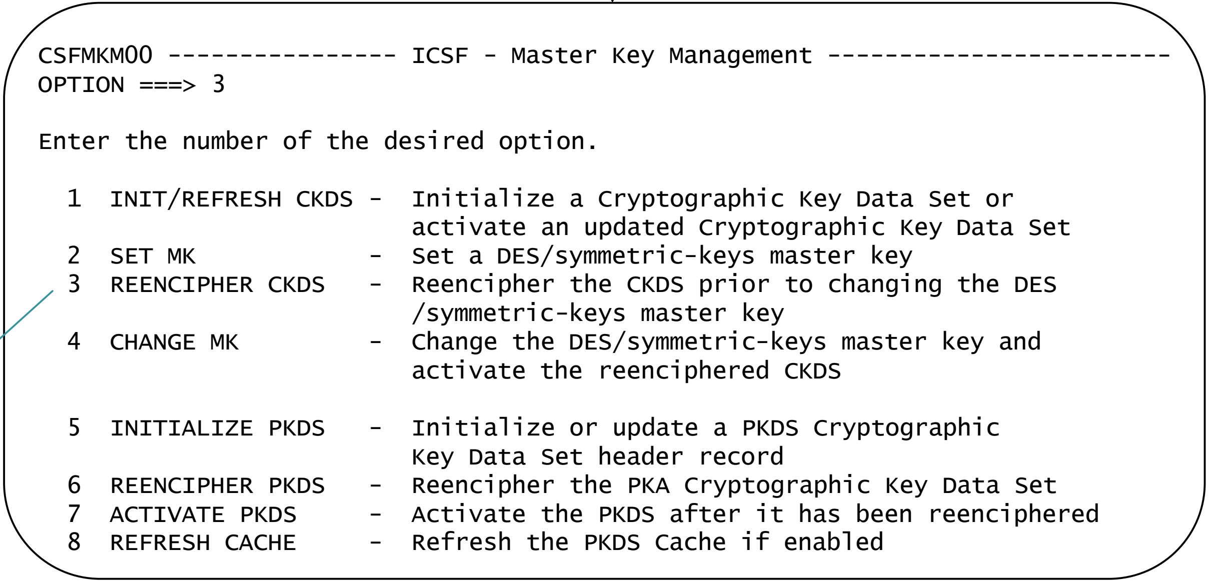
- VP and/or HP of entered key part are displayed at bottom of panel. Record these for verification.
- VP and/or HP of master key register are displayed after the final key part is entered. Record these for verification.

Steps to Change the Master Keys

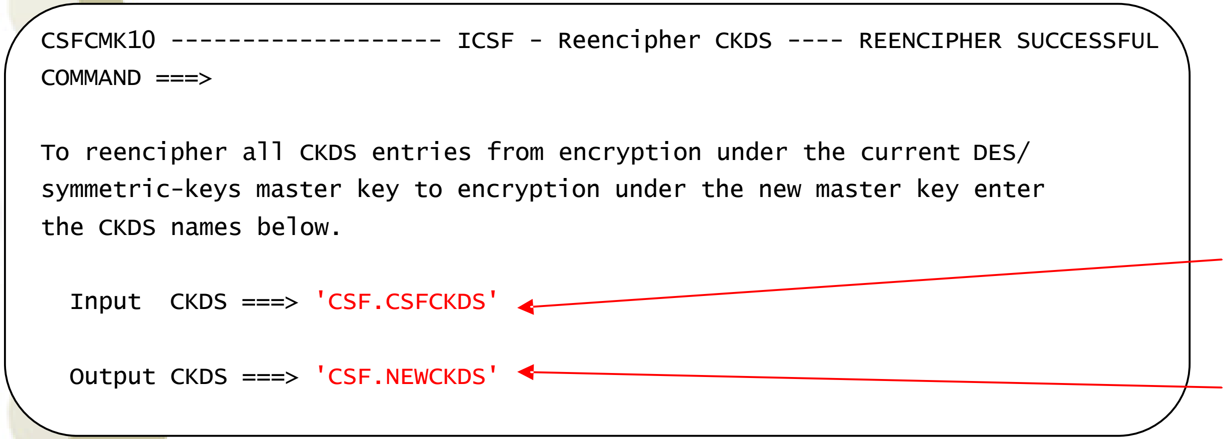
1. Define empty CKDS/PKDS.
2. Generate key values using Random Number Generator utility.
3. Calculate checksum for key value using checksum utility.
4. Disable PKA callable services.
5. Enter master key in parts.
6. **Reencipher CKDS.**
7. Change the SYM-MK master key.
8. Reencipher PKDS.
9. Activate the new PKDS.
10. Enable PKA callable services, PKDS read and write access.

Reencipher the CKDS

Select option 2 MASTER KEY from ICSF Main Panel



```
CSFMKM00 ---------------- ICSF - Master Key Management ------------------------
OPTION ===> 3

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 reenciphered
  8  REFRESH CACHE     -  Refresh the PKDS Cache if enabled
```



```
CSFCMK10 ------------------- ICSF - Reencipher CKDS ---- REENCIPHER SUCCESSFUL
COMMAND ===>

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

  Input  CKDS ===> 'CSF.CSFCKDS'

  Output CKDS ===> 'CSF.NEWCKDS'
```

input CKDS is the current active CKDS

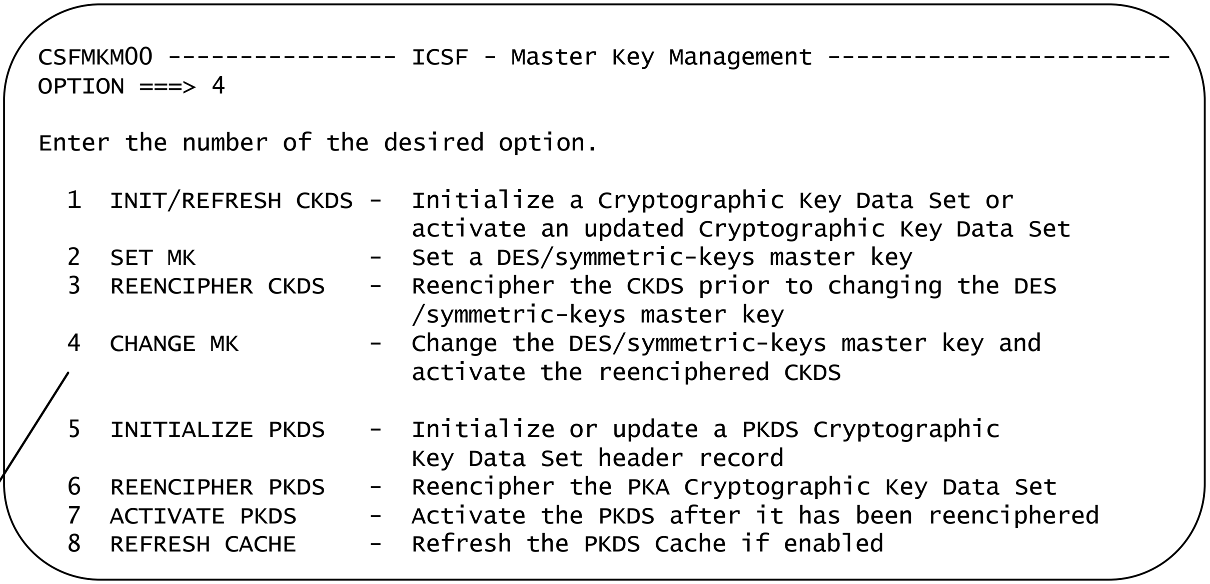
output CKDS must be an empty CKDS

Steps to Change the Master Keys

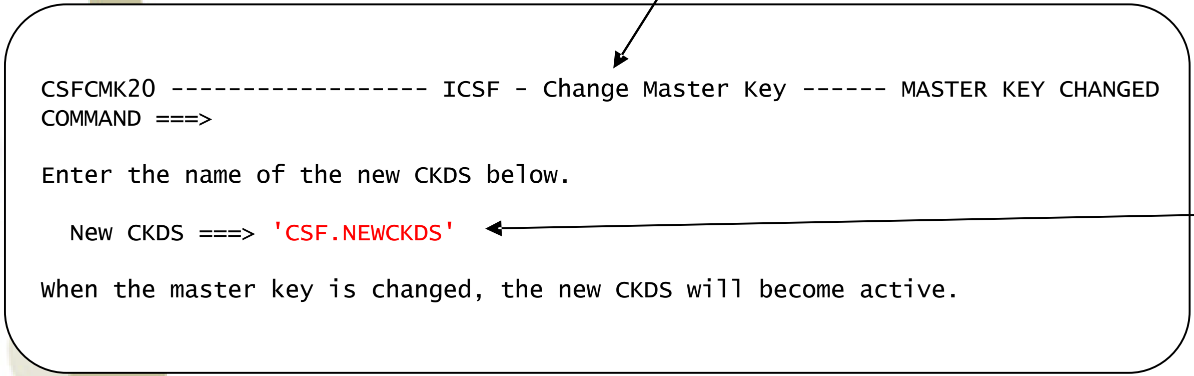
1. Define empty CKDS/PKDS.
2. Generate key values using Random Number Generator utility.
3. Calculate checksum for key value using checksum utility.
4. Disable PKA callable services.
5. Enter master key in parts.
6. Reencipher CKDS.
7. **Change the SYM-MK master key.**
8. Reencipher PKDS.
9. Activate the new PKDS.
10. Enable PKA callable services, PKDS read and write access.

Change the SYM-MK

Select option 2 MASTER KEY from ICSF Main Panel



```
CSFMKM00 ---------------- ICSF - Master Key Management ------------------------
OPTION ===> 4

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 reenciphered
  8  REFRESH CACHE     -  Refresh the PKDS Cache if enabled
```



```
CSFCMK20 ------------------ ICSF - Change Master Key ------ MASTER KEY CHANGED
COMMAND ===>

Enter the name of the new CKDS below.

  New CKDS ===> 'CSF.NEWCKDS'

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

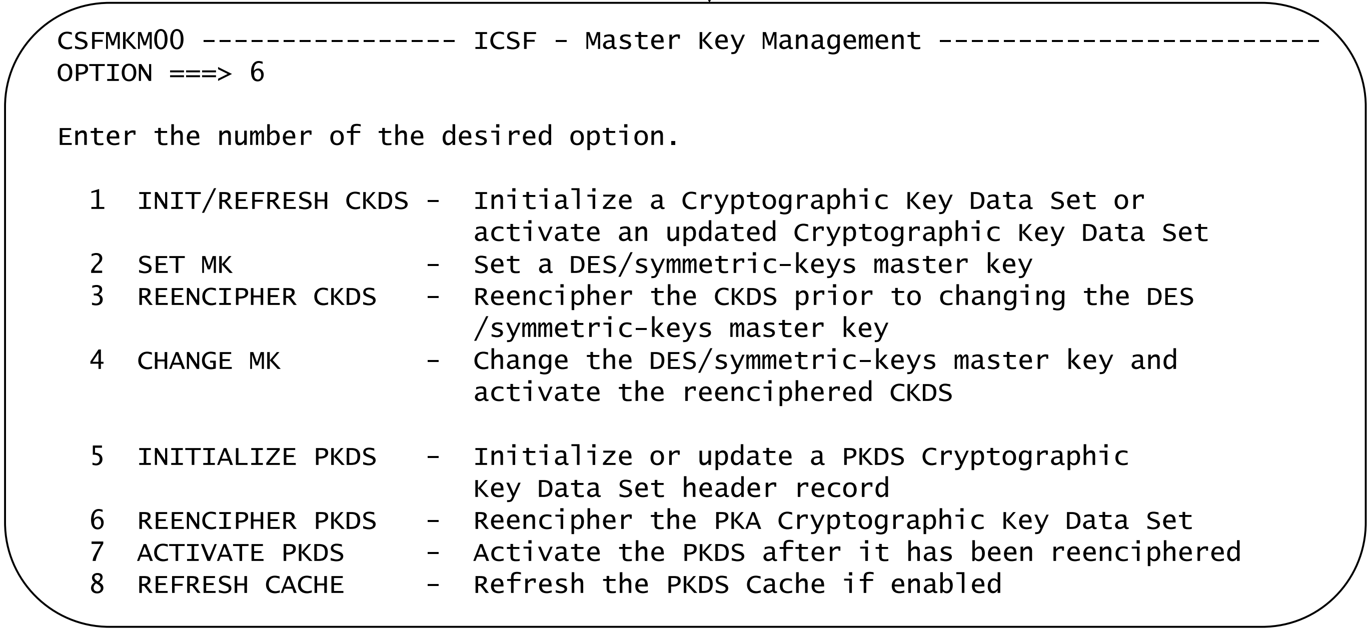
This is the output CKDS from CKDS Reencipher.

Steps to Change the Master Keys

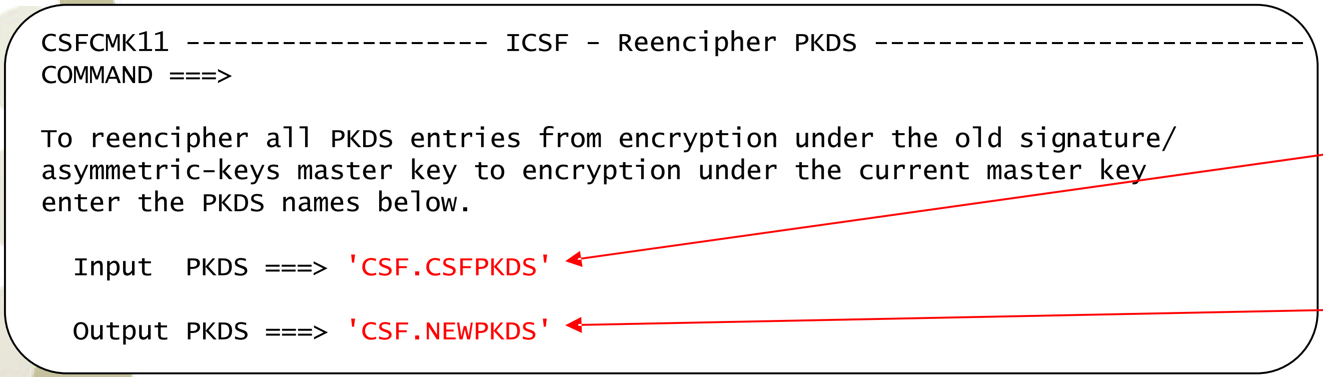
1. Define empty CKDS/PKDS.
2. Generate key values using Random Number Generator utility.
3. Calculate checksum for key value using checksum utility.
4. Disable PKA callable services.
5. Enter master key in parts.
6. Reencipher CKDS.
7. Change the SYM-MK master key.
8. **Reencipher PKDS.**
9. Activate the new PKDS.
10. Enable PKA callable services, PKDS read and write access.

Reencipher the PKDS

Select option 2 MASTER KEY from ICSF Main Panel



```
CSFMKM00 ---------------- ICSF - Master Key Management ------------------------
OPTION ===> 6

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 reenciphered
  8  REFRESH CACHE     -  Refresh the PKDS Cache if enabled
```



```
CSFCMK11 ------------------- ICSF - Reencipher PKDS --------------------------
COMMAND ===>

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

  Input  PKDS ===> 'CSF.CSFPKDS'

  Output PKDS ===> 'CSF.NEWPKDS'
```

input PKDS is the current active PKDS

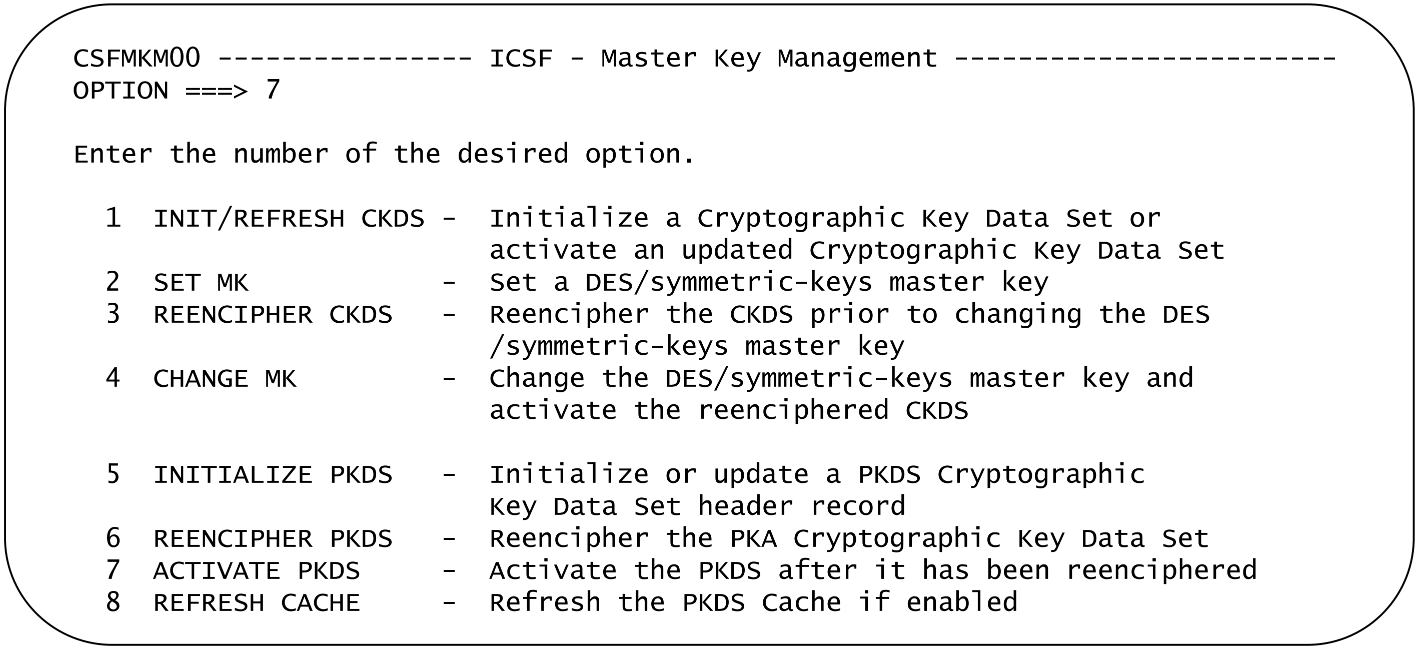
output PKDS must be an empty PKDS

Steps to Change the Master Keys

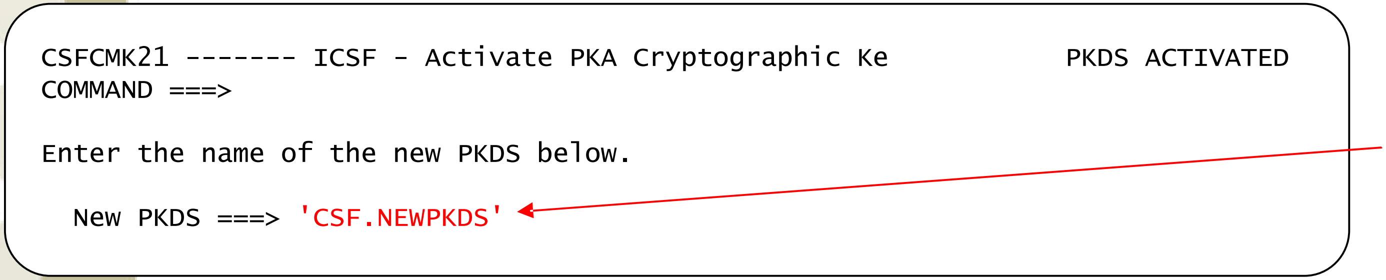
1. Define empty CKDS/PKDS.
2. Generate key values using Random Number Generator utility.
3. Calculate checksum for key value using checksum utility.
4. Disable PKA callable services.
5. Enter master key in parts.
6. Reencipher CKDS.
7. Change the SYM-MK master key.
8. Reencipher PKDS.
9. **Activate the new PKDS.**
10. Enable PKA callable services, PKDS read and write access.

Activate the PKDS

Select option 2 MASTER KEY from the ICSF Main Panel.



```
CSFMKM00 ---------------- ICSF - Master Key Management ------------------------
OPTION ===> 7

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 reenciphered
  8  REFRESH CACHE     -  Refresh the PKDS Cache if enabled
```



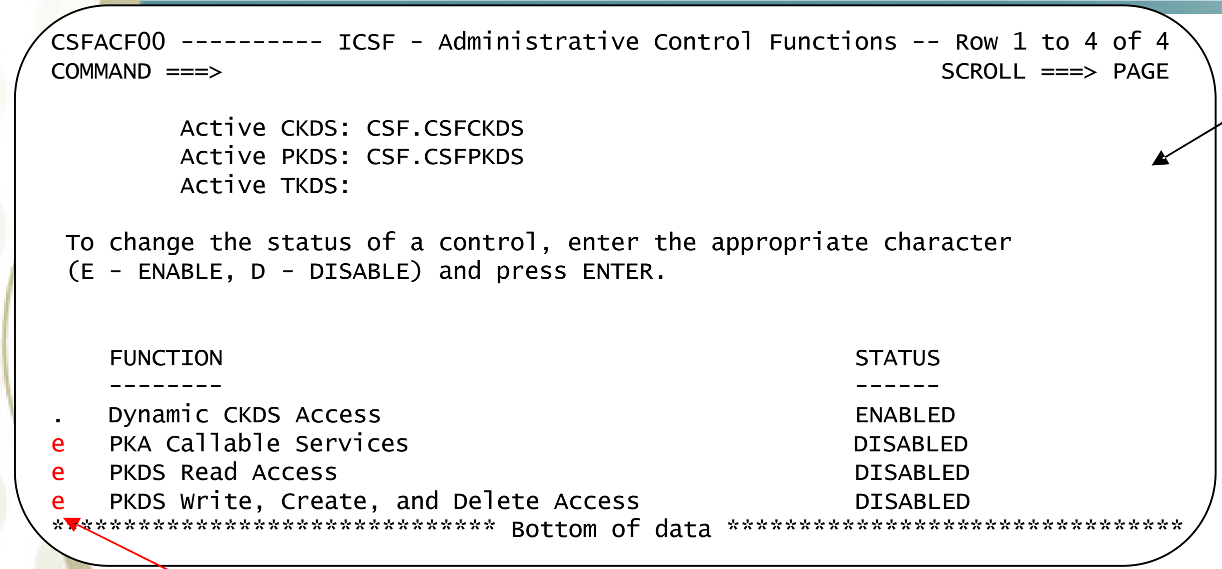
```
CSFCMK21 ------- ICSF - Activate PKA Cryptographic Ke           PKDS ACTIVATED
COMMAND ===>

Enter the name of the new PKDS below.

  New PKDS ===> 'CSF.NEWPKDS'
```

This is the output PKDS from PKDS reencipher.

Steps to Change the Master Keys

1. Define empty CKDS/PKDS.
2. Generate key values using Random Number Generator utility.
3. Calculate checksum for key value using checksum utility.
4. Disable PKA callable services.
5. Enter master key in parts.
6. Reencipher CKDS.
7. Change the SYM-MK master key.
8. Reencipher PKDS.
9. Activate the new PKDS.
10. **Enable PKA callable services, PKDS read and write access.**

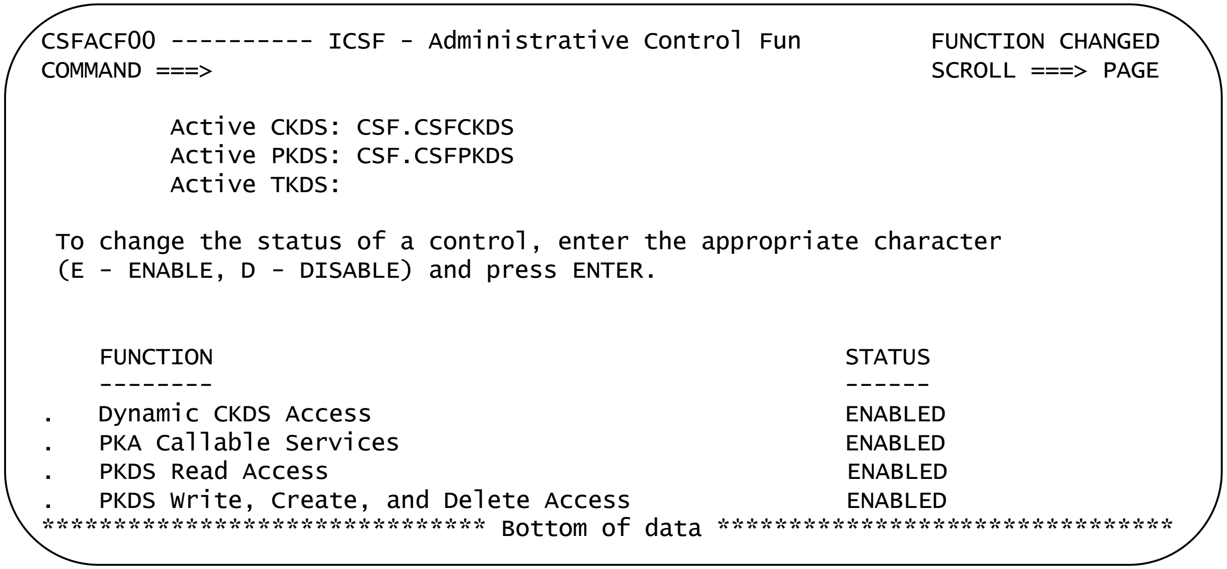
Enable PKA Callable Services



```
CSFACF00 ---------- ICSF - Administrative Control Functions -- Row 1 to 4 of 4
COMMAND ===>                                                   SCROLL ===> PAGE

         Active CKDS: CSF.CSFCKDS
         Active PKDS: CSF.CSFPKDS
         Active TKDS:

 To change the status of a control, enter the appropriate character
 (E - ENABLE, D - DISABLE) and press ENTER.


    FUNCTION                                              STATUS
    --------                                              ------
.   Dynamic CKDS Access                                   ENABLED
e   PKA Callable Services                                 DISABLED
e   PKDS Read Access                                      DISABLED
e   PKDS Write, Create, and Delete Access                 DISABLED
******************************* Bottom of data ********************************
```

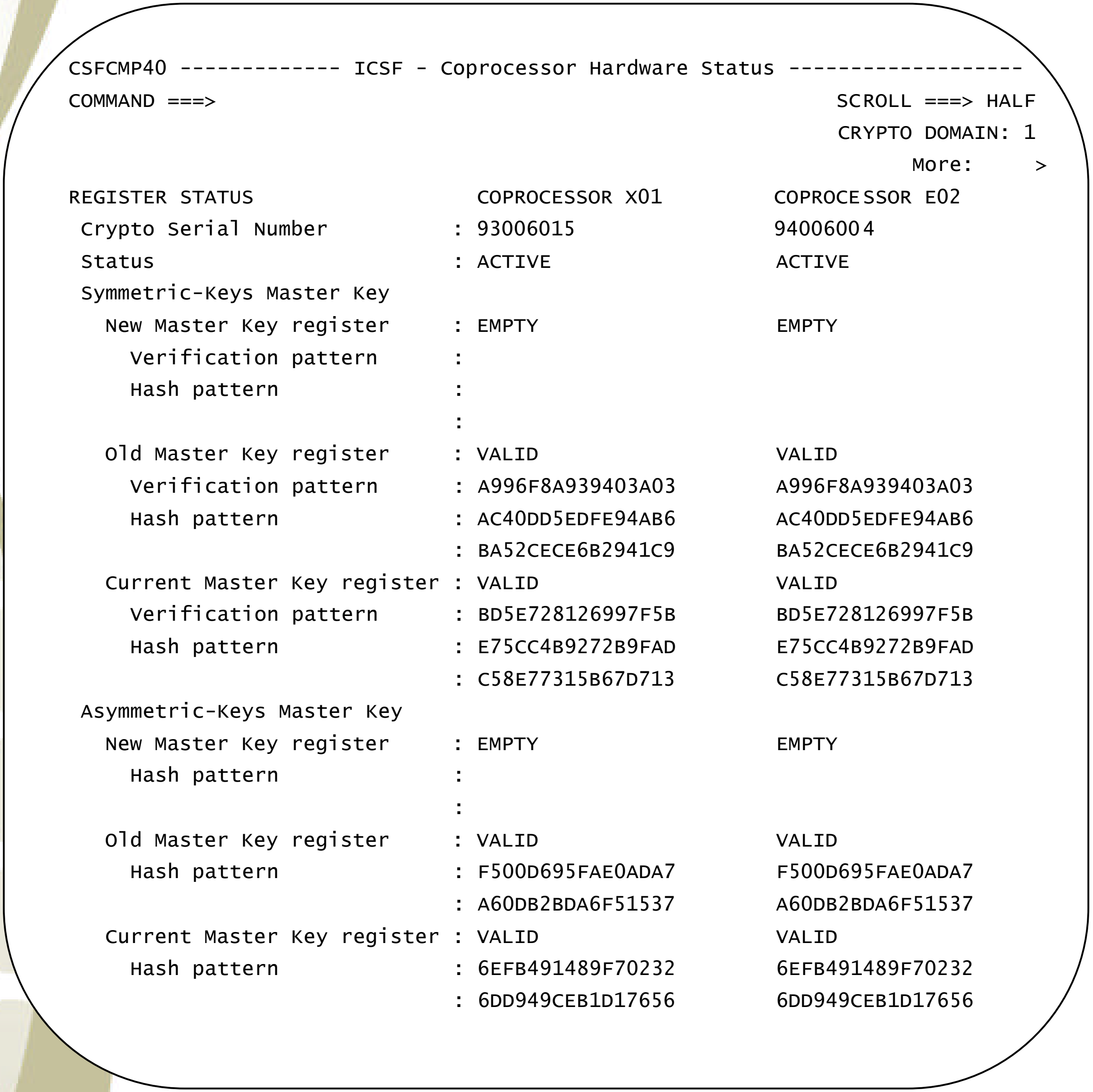
Select option 4 ADMINCNTL from the ICSF Main Panel.

- Enable PKA Callable Services
- Enable PKDS Read Access
- Enable PKDS Write, Create, and Delete Access



```
CSFACF00 ---------- ICSF - Administrative Control Fun         FUNCTION CHANGED
COMMAND ===>                                                   SCROLL ===> PAGE

         Active CKDS: CSF.CSFCKDS
         Active PKDS: CSF.CSFPKDS
         Active TKDS:

 To change the status of a control, enter the appropriate character
 (E - ENABLE, D - DISABLE) and press ENTER.


    FUNCTION                                              STATUS
    --------                                              ------
.   Dynamic CKDS Access                                   ENABLED
.   PKA Callable Services                                 ENABLED
.   PKDS Read Access                                      ENABLED
.   PKDS Write, Create, and Delete Access                 ENABLED
******************************* Bottom of data ********************************
```

Current Hardware Status



```
CSFCMP40 ------------- ICSF - Coprocessor Hardware Status -------------------
COMMAND ===>                                                  SCROLL ===> HALF
                                                              CRYPTO DOMAIN: 1
                                                                   More:     >
REGISTER STATUS                  COPROCESSOR X01        COPROCESSOR E02
 Crypto Serial Number          : 93006015               94006004
 Status                        : ACTIVE                 ACTIVE
 Symmetric-Keys Master Key
   New Master Key register     : EMPTY                  EMPTY
     Verification pattern      :
     Hash pattern              :
                               :
   Old Master Key register     : VALID                  VALID
     Verification pattern      : A996F8A939403A03       A996F8A939403A03
     Hash pattern              : AC40DD5EDFE94AB6       AC40DD5EDFE94AB6
                               : BA52CECE6B2941C9       BA52CECE6B2941C9
   Current Master Key register : VALID                  VALID
     Verification pattern      : BD5E728126997F5B       BD5E728126997F5B
     Hash pattern              : E75CC4B9272B9FAD       E75CC4B9272B9FAD
                               : C58E77315B67D713       C58E77315B67D713
 Asymmetric-Keys Master Key
   New Master Key register     : EMPTY                  EMPTY
     Hash pattern              :
                               :
   Old Master Key register     : VALID                  VALID
     Hash pattern              : F500D695FAE0ADA7       F500D695FAE0ADA7
                               : A60DB2BDA6F51537       A60DB2BDA6F51537
   Current Master Key register : VALID                  VALID
     Hash pattern              : 6EFB491489F70232       6EFB491489F70232
                               : 6DD949CEB1D17656       6DD949CEB1D17656
```

- At first time startup, all master key registers were empty.
- After Pass Phrase, the current master key register is valid.
- Key parts are loaded to the new master key register.
- After changing the master keys, the content of the current master key register is moved to the old master key register, the content of the new master key register is moved to the current master key register, and the new master key register is cleared.

Update Installation Options Data Set

Change your installation options data set to point to your new CKDS and PKDS for next start up of ICSF.

- Change CKDSN and PKDSN parameters

Otherwise ICSF error messages are written to MVS console and status of secure coprocessors is ONLINE, not ACTIVE.

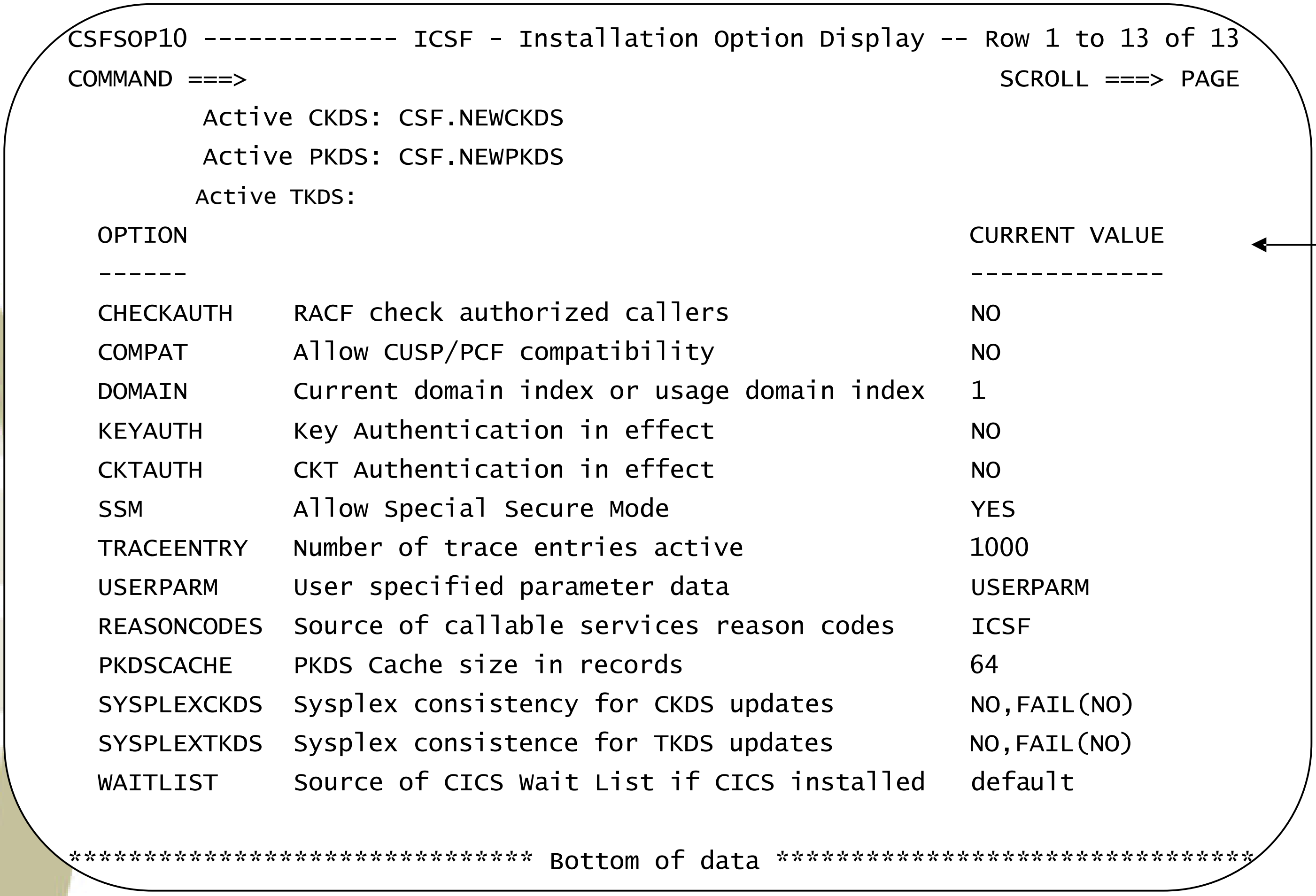
```
CSFM419E INCORRECT MASTER KEY (SYM) ON PCI X CRYPTOGRAPHIC COPROCESSOR
X01,SERIAL NUMBER 93006015.
CSFM434E INCORRECT MASTER KEY (SYM) ON CRYPTO EXPRESS2 COPROCESSOR E02,
SERIAL NUMBER 94006004.
CSFM434E INCORRECT MASTER KEY (SYM) ON CRYPTO EXPRESS2 COPROCESSOR E03,
SERIAL NUMBER 94006026.
```

Installation Options Display

- Displays the installation options that are active since the last start of ICSF.
- Some options have defaults.

Select option 3 OPSTAT from ICSF Main Panel.

Select option 1 OPTIONS to display installation options.



```
CSFSOP10 ------------- ICSF - Installation Option Display -- Row 1 to 13 of 13
COMMAND ===>                                                   SCROLL ===> PAGE
         Active CKDS: CSF.NEWCKDS
         Active PKDS: CSF.NEWPKDS
        Active TKDS:
  OPTION                                                     CURRENT VALUE
  ------                                                     -------------
  CHECKAUTH    RACF check authorized callers                 NO
  COMPAT       Allow CUSP/PCF compatibility                  NO
  DOMAIN       Current domain index or usage domain index    1
  KEYAUTH      Key Authentication in effect                  NO
  CKTAUTH      CKT Authentication in effect                  NO
  SSM          Allow Special Secure Mode                     YES
  TRACEENTRY   Number of trace entries active                1000
  USERPARM     User specified parameter data                 USERPARM
  REASONCODES  Source of callable services reason codes      ICSF
  PKDSCACHE    PKDS Cache size in records                    64
  SYSPLEXCKDS  Sysplex consistency for CKDS updates          NO,FAIL(NO)
  SYSPLEXTKDS  Sysplex consistence for TKDS updates          NO,FAIL(NO)
  WAITLIST     Source of CICS Wait List if CICS installed    default

******************************* Bottom of data ********************************
```

RACF Protection of Keys and Services

Use RACF to control which applications can use specific keys and services.

- Protect key labels using CSFKEYS general resource class.
- Protect ICSF callable services and TSO panels using CSFSERV general resource class.

```
RDEFINE CSFKEYS label UACC(NONE)
RDEFINE CSFSERV service_name UACC(NONE)
PERMIT label CLASS(CSFKEYS) ID(userid) ACCESS(READ)
PERMIT service_name CLASS(CSFSERV) ID(userid) ACCESS(READ)
```

Refer to the z/OS ICSF Administrator's Guide for a list of *service_names*

that can be protected.

Refer to the z/OS Security Server RACF Command Language Reference, SA22-7686 for RACF commands.

CKDS/PKDS Sharing Considerations

- CKDS must have been initialized on a CCF (z900/z800) system.
  - can not share a z990/z890/z9 EC/z9 BC initialized CKDS with a CCF system.
- Master keys *must* match.
  - the CCF DES master key must match the PCIXCC/CEX2C symmetric-keys master key (SYM-MK)
  - the CCF Signature Master Key (SMK) must match the PCIXCC/CEX2C asymmetric-keys master key (ASYM-MK)
  - the CCF Key Management Master Key (KMMK) must match the SMK
- Detailed information about CKDS/PKDS sharing can be found in the z/OS ICSF Administrator’s Guide.

Callable Service APIs

ICSF Callable Services

ICSF provides over 70 application callable services.

Symmetric Algorithm Services

- Encryption/Decryption using DES, TDES, AES
- Hashing – SHA-1, MDC-2, MDC-4, MD5
- Message Authentication Code Generation/Verification

Symmetric Key Management

- Key generation
- Key distribution via DES and RSA, including SSL handshakes

Financial Services

- PIN generation/verification/translation
- CVV generation/verification
- SET processing
- EMV support
- ATM Remote Key Load suport.

Asymmetric Algorithm Services

- RSA key generation
- Digital signature generation/verification

CKDS/PKDS key management services

PKCS#11 services

Callable Service API

```
CALL CSNBENC (
                 return_code,
                 reason code,
                 exit_data_length,
                 exit_data,
                 key_identifier,
                 text_length,
                 clear_text,
                 initialization_vector,
                 rule_array_count,
                 rule_array,
                 pad_character,
                 chaining_vector,
                 cipher_text       )
```

Languages supported:

- Assembler H
- C
- COBOL
- Fortran
- PL/1

Refer to the z/OS ICSF Application Programmer's Guide for a list of the callable services supported.

Cryptographic Support Performance Hints - CICS TRUE

- ICSF has implemented a CICS Task Related User Exit (TRUE).
- Intended to offload CICS transactions to a separate MVS subtask when processing would deliberately give up control during crypto processing.
- On z900 machines with CCFs use of the TRUE was optional and the intended environment was limited to the following:
  - Use of PKA functions on the CCFs. OS WAITS would be issued and latch suspensions were possible..
  - Any work which would go to the PCICC card. OS WAITS would be issued and latch suspensions were possible.
  - Callers of CSNBKRC, CSNBKRW and CSNBKRD.Multiple OS WAITS issued and ENQUEUE suspensions were possible.
  - Callers of analogous PKDS I/O functions including CSNDKRR. OS WAITS certain and latch suspensions possible.
- Outside of this intended environment use of the TRUE likely hurt performance.

Cryptographic Support Performance Hints - CICS TRUE

- On Z990 use of the TRUE is strongly recommended for functions that use the PCICA or the PCIXCC features.
  - Use of either feature causes application to give up control via OS WAIT, PAUSE invocation, or latch suspension.
- ICSF use of TRUE, by service name, is controlled by the ICSF WAITLIST option in the options dataset.
  - Data set specifies service names that will use the TRUE.
  - In HCR770A, default WAITLIST is correct for z990 users but...
  - The default for z900 users has a bias towards users of the PCICC vs the CCF.
    - Services that could conceivably go to the PCICC will use the TRUE, even if they in fact only use the CCF.
  - So, for HCR770A on a z900, it might be useful for customers to supply their own customized WAITLIST, specifying only those services that go to the PCICC, do CKDS/PKDS I/O, or do PKA operations on the CCFs.
  - On the z990, use the default WAITLIST..
  - Note that a UDX service name can be added to a customized WAITLIST.

Migration Considerations

If migrating from a CCF system the following are no longer supported on z990/z890/z9 EC/z9 BC:

DSA signatures and key generation

- Cipher Text Translate callable service (CSNBCTT)
- CDMF (40 bit encryption)
- German Bank Pool PIN Offset (GBP-PINO)
- ANSI x9.17 services and key type
- CSFUDK callable service (replaced with CSNBDKG)

Migrating to HCR7750 from a lower release, the PKDS record size is now larger to accommodate 4096 bit RSA keys. The PKDS needs to be recreated to this larger size.

Refer to the z/OS ICSF System Programmer's Guide for detailedinformation about migration.

Hardware Cryptography Exploiters

- BSAFE Toolkit 3.1 (or later)
- z/OS System SSL
- z/OS Open Cryptographic Services Facility (OCSF)
- IBM HTTP Server for z/OS
- z/OS LDAP server and client
- CICS Transaction Server and CICS Transaction Gateway
- z/OS TN3270 server
- z/OS Firewall Technologies
- z/OS DCE
- Payment processing products
- VTAM Session Level Encryption
- RACF
- Crypto Based Transactions (CBT) banking solution
- Java cryptography
- z/OS Public Key Infrastructure (PKI) services
- z/OS Network Authentication Service (Kerberos)

Related Publications

z/OS ICSF Overview	SA22-7519
z/OS ICSF System Programmer's Guide	SA22-7520
z/OS ICSF Administrator's Guide	SA22-7521
z/OS ICSF Application Programmer's Guide	SA22-7522
z/OS ICSF Messages	SA22-7523
z/OS TKE Workstation User's Guide	SA22-7524
Program Directory for ICSF – FMID HCR7720	GI11-2845
z/OS Security Server RACF Command Language Reference	SA22-7686
Support Element Operations Guide	SC28-6831
PR/SM Planning Guide	SB10-7036
IBM eServer zSeries 990 (z990) Cryptography Implementation	SG24-7070

Acronyms

AES	Advanced Encryption Standard
ASYM-MK	Asymmetric-keys Master Key
CCA	Common Cryptographic Architecture
CCF	Cryptographic Coprocessor Feature
CDMF	Commercial Data Masking Facility
CEX2C	Crypto Express2 Coprocessor
CKDS	Cryptographic Key Data set
CP	Central Processor
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
EMV	Europay, MasterCard and VISA
FIPS	Federal Information Processing Standards
HMC	Hardware Master Console
ICSF	Integrated Cryptographic Service Facility
LIC	Licensed internal code
MD5	Message Digest 5

Acronyms…cont

PAN	Personal Account Number
PCI	Peripheral Component Interconnect
PCICA	PCI Cryptographic Accelerator
PCICC	PCI Cryptographic Coprocessor
PCIXCC	PCI Extended Cryptographic Coprocessor
PKA	Public Key Algorithm
PKDS	PKA Key Data Set
PPINIT	Pass Phrase Initialization
RACF	Resource Access Control Facility
RSA	Rivest-Shamir-Adelman
SET	Secure Electronic Transaction
SHA-1	Secure Hash Algorithm 1
SSL	Secure Sockets Layer
SYM-MK	Symmetric-Keys Master Key
TDES	Triple key DES
TKDS	Token Key Data Set
TKE	Trusted Key Entry
VSAM	Virtual Storage Access Method