Pervasive Encryption Demo:

Guided Tour of Policy-Based Data Set Encryption

Eysha S. Powers
IBM, Enterprise Cryptography

November 2018
Session FF

About me ☺

IBM Career (~15 years)

2004: z/OS Resource Access Control Facility (RACF)

2006: z/OS Java Cryptography Extension (JCE)

2008: z/OS Integrated Cryptographic Services Facility (ICSF)

- A few cool projects:
  - Elliptic Curve Cryptography (ECC)
  - Enterprise PKCS #11 (EP11)
  - Crypto-as-a-service (ACSP-REST)
  - Regional Cryptographic Enablement (RCE)
  - Field Level Encipher (FLE) for secure key tokens
  - Crypto Usage Statistics (STATS)

"Crypto Nerd"

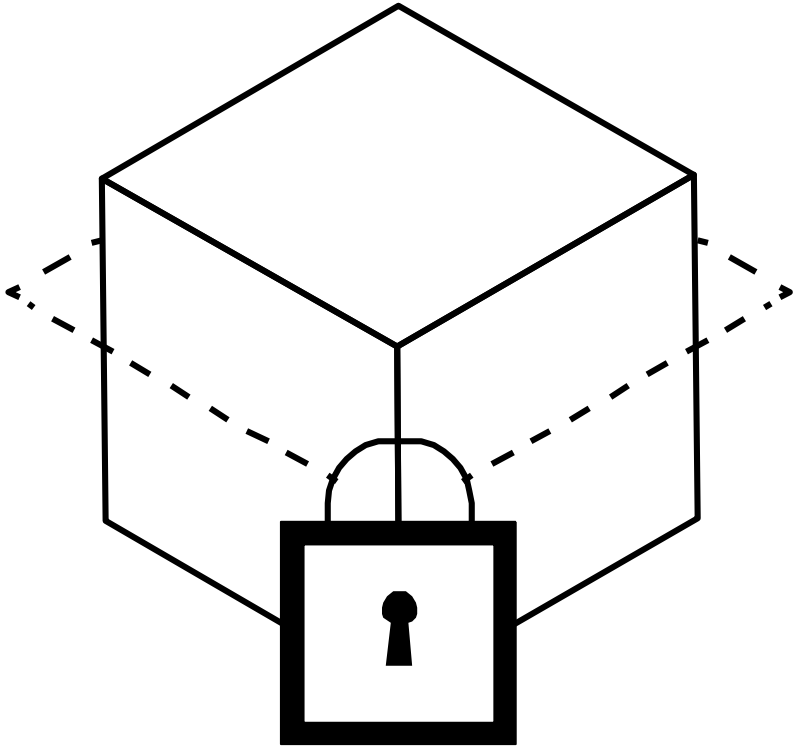
Current Role: z/OS Crypto SME, z/OS ICSF Developer

Responsibilities: Crypto Software Design & Development, Crypto Code Samples, Crypto Education

Founded the IBM Crypto Education community:
https://www.ibm.com/developerworks/community/groups/community/crypto

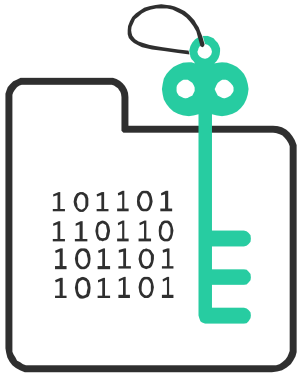
Getting Started…

1. Configure Crypto Express Cards
2. Configure ICSF
3. Start ICSF
4. Load AES MK
5. Initialize CKDS
6. Generate a Secure AES Data Key
7. Protect Data Sets with Secure Keys
8. Authorize Key Users
9. Allocate Data Sets
10. Write & Print the Encrypted Data Set



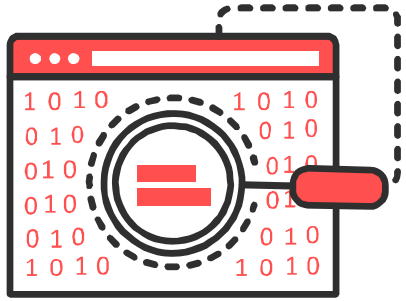
For REXX, CLIST and JCL Samples see
IBM Crypto Education: https://ibm.biz/BdiAah

Three Perspectives…



ICSF View

- ICSF Configuration & Auditing
- Master Key Generation & Loading
- Master Key Life Cycle
- Operational Key Generation
- Operational Key Life Cycle
- Operational Key Label Naming Conventions



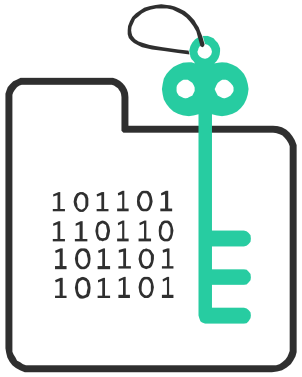
DFSMS View

- Data Set Naming Conventions
- Data Set Allocation
- Data Set Read & Write
- Data Set Management

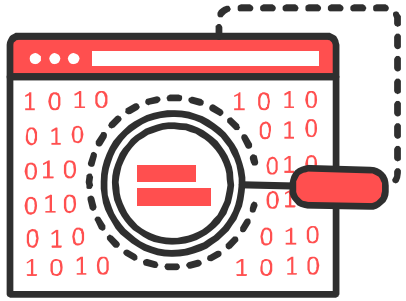
RACF View

- CSFSERV Authorization
- CSFKEYS Authorization
- FACILITY Authorization
- DATASET Authorization

Step 1: Configuring Crypto Express Cards



ICSF View



DFSMS View

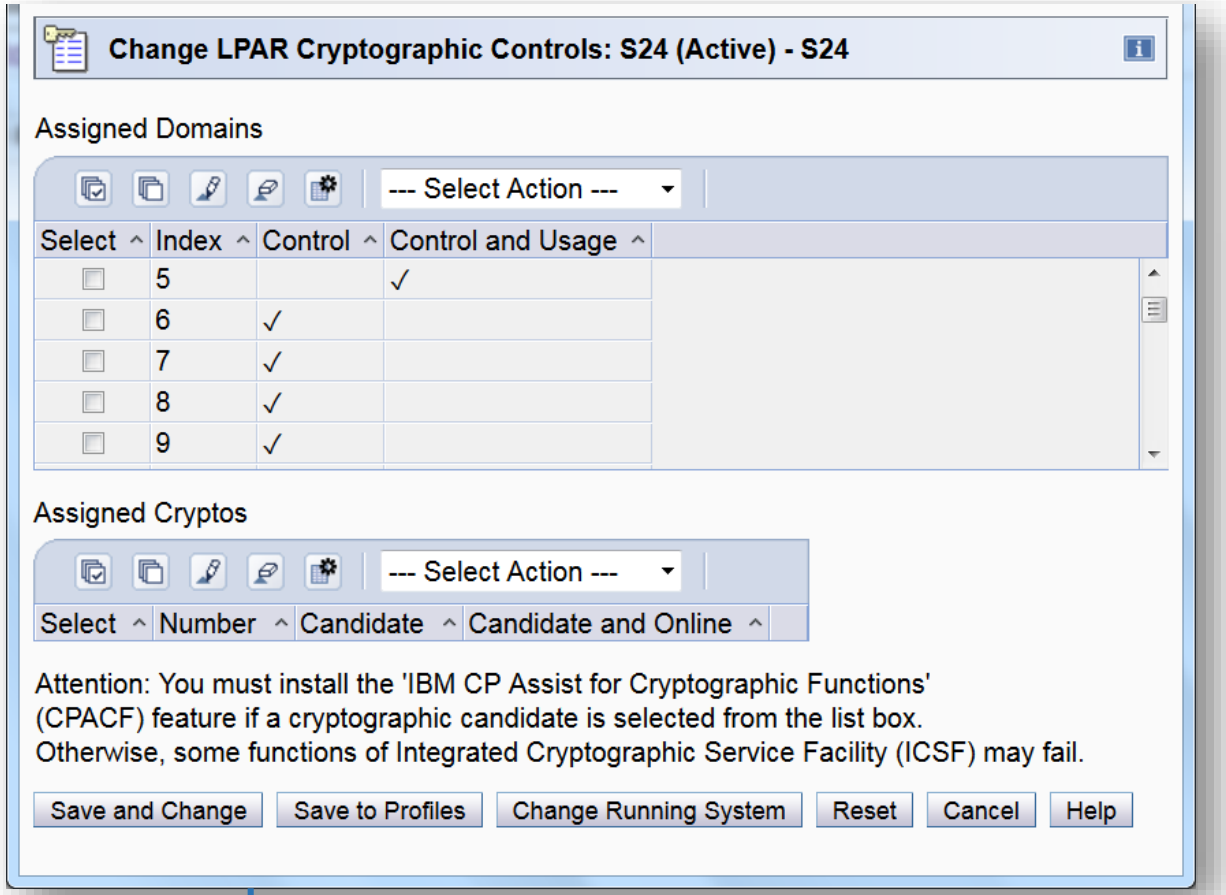
RACF View

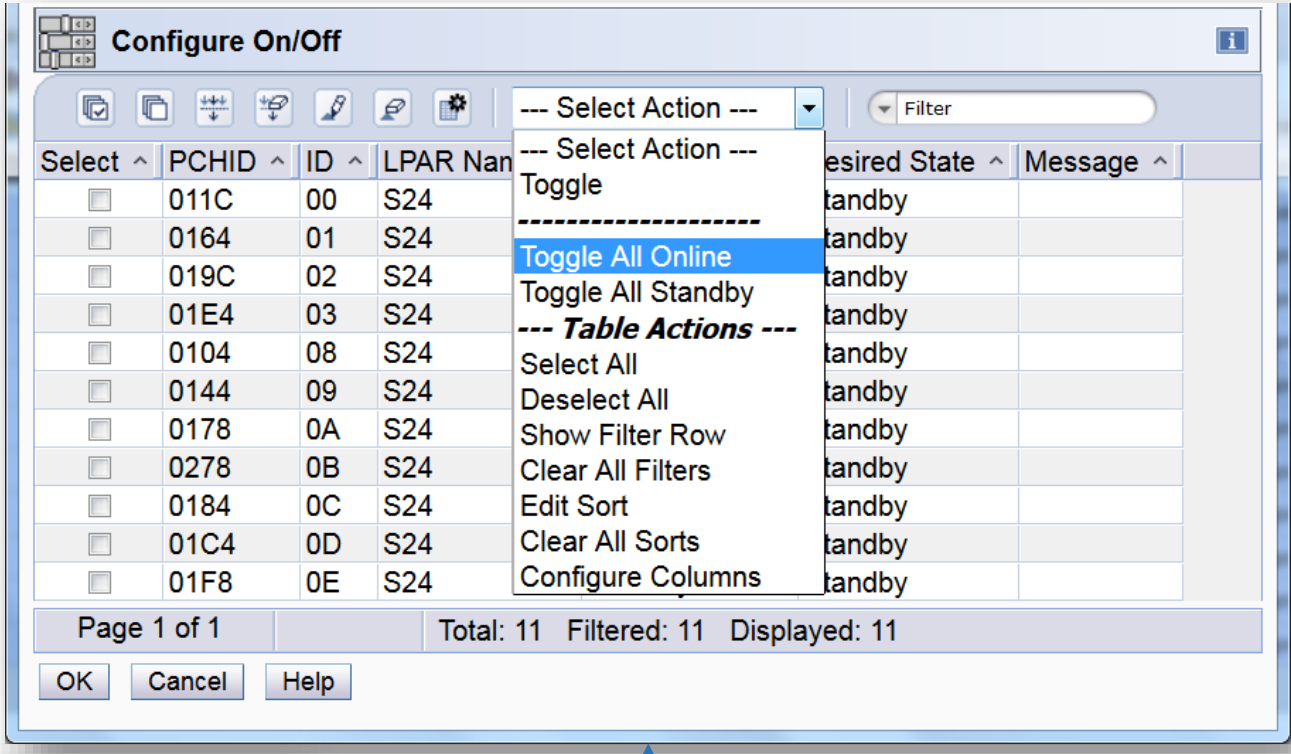
- How many Crypto Express adapter will be needed?
- Which Crypto Express adapters will be assigned to which LPARs?
- Which modes will be configured?
- Is a TKE Workstation needed?

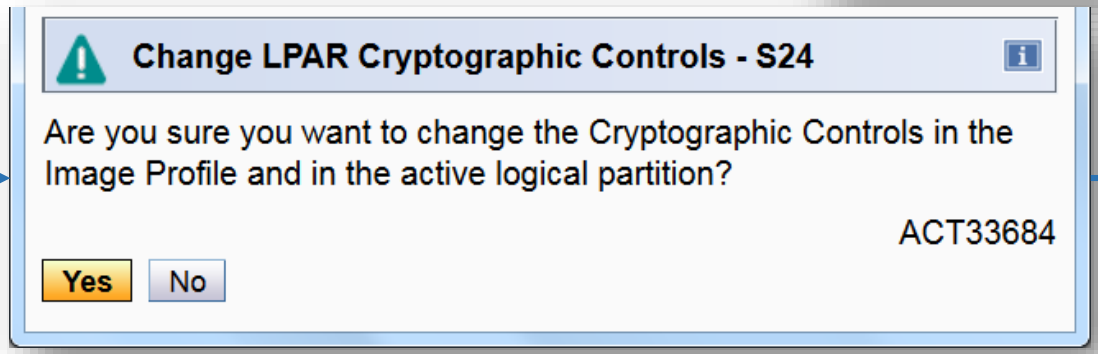
N/A

N/A

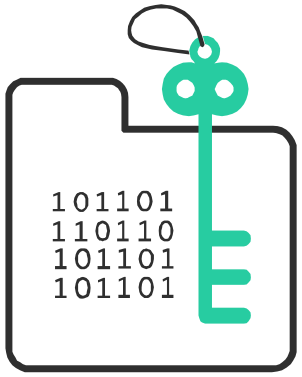
Crypto Card Capacity Planning:
https://www.ibm.com/developerworks/community/blogs/79c1eec4-00c4-48ef-ae2b-01bd8448dd6c/entry/Crypto_Express_Card_Capacity_Planning


Change LPAR Cryptographic Controls: S24 (Active) - S24
Assigned Domains
--- Select Action ---
Select
Index
Control
Control and Usage
5
6
7
8
9
Assigned Cryptos
--- Select Action ---
Select
Number
Candidate
Candidate and Online
Attention: You must install the 'IBM CP Assist for Cryptographic Functions' (CPACF) feature if a cryptographic candidate is selected from the list box. Otherwise, some functions of Integrated Cryptographic Service Facility (ICSF) may fail.
Save and Change
Save to Profiles
Change Running System
Reset
Cancel
Help


Configure On/Off
--- Select Action ---
Filter
Select
PCHID
ID
LPAR Nan
esired State
Message
011C 00 S24 tandby
0164 01 S24 tandby
019C 02 S24 tandby
01E4 03 S24 tandby
0104 08 S24 tandby
0144 09 S24 tandby
0178 0A S24 tandby
0278 0B S24 tandby
0184 0C S24 tandby
01C4 0D S24 tandby
01F8 0E S24 tandby
--- Select Action ---
Toggle
Toggle All Online
Toggle All Standby
--- Table Actions ---
Select All
Deselect All
Show Filter Row
Clear All Filters
Edit Sort
Clear All Sorts
Configure Columns
Page 1 of 1
Total: 11 Filtered: 11 Displayed: 11
OK
Cancel
Help

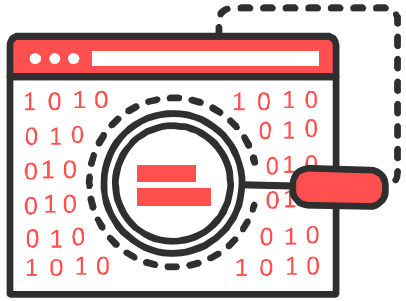

Change LPAR Cryptographic Controls - S24
Are you sure you want to change the Cryptographic Controls in the Image Profile and in the active logical partition?
ACT33684
Yes
No

Step 2: Configure ICSF



ICSF View

- Which Key Data Sets (KDSs) are needed?
- Will the KDS use the Common Record Format?
- Will any KDSs be shared in a sysplex with a common Master Key?
- Should key usage auditing be enabled?
- Should key life cycle auditing be enabled?
- Should crypto usage statistics be enabled?



DFSMS View

N/A

RACF View

- Does the ICSF admin have authority to update the CSFPRMxx PARMLIB member?
- Are the CSFSERV and CSFKEYS classes ACTIVE and RACLISTed?
- Do the CSFSERV and CSFKEYS classes have a generic resource defined with UACC(NONE)?

CKDS Allocation Job

```
//*************************************************************
//***         CREATE CKDSR
//*************************************************************
//STEP2    EXEC PGM=IDCAMS,REGION=4M
//SYSPRINT DD  SYSOUT=*
//SYSIN DD *
  DEFINE CLUSTER (NAME(EYSHA.ICSF.CSF77C1.CKDSR) -
                  VOLUME(CSFDR7) -
                  RECORDS(100 50) -
                  RECSZ(332,2048) -
                  KEYS(72 0) -
                  FSPC(10,10) -
                  SHR(2,3)) -
           DATA (NAME(EYSHA.ICSF.CSF77C1.CKDSR.DATA) -
                 BUFFERSPACE(100000)                 -
                 ERASE                               -
                 WRITECHECK)                         -
          INDEX (NAME(EYSHA.ICSF.CSF77C1.CKDSR.INDEX))
//*
```

The CKDS must be in Common Record Format (i.e. LRECL = 2048) in order to perform key archival, set key validity dates, track key reference dates and add custom metadata to key records. These features require ICSF HCR77B0 or later.

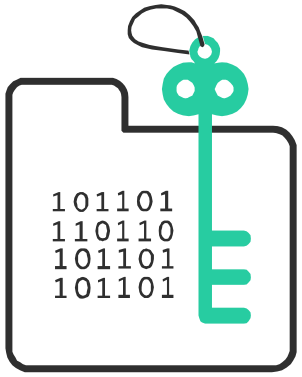
ICSF Installation Options Data Set (IODS) in CSFPRMxx

```
CKDSN(EYSHA.ICSF.CSF77C1.CKDSR)
SYSPLEXCKDS(YES,FAIL(YES))
CHECKAUTH(NO)
DOMAIN(0)
SSM(YES)
DUMPTKT(YES)
KDSREFDAYS(1)
STATS(ENG,SRV,ALG)
AUDITKEYLIFECKDS(TOKEN(YES),LABEL(YES))
AUDITKEYUSGCKDS(TOKEN(YES),LABEL(YES),INTERVAL(1))
```

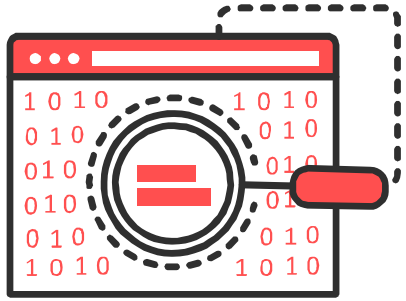
z/OS data set encryption requires the use of a CKDS to store operational keys.

If you plan to share the CKDS with other LPARs, enable SYSPLEXCKDS.

Step 3: Start ICSF



ICSF View



DFSMS View

RACF View

- Are the Crypto Express adapters correctly displayed at ICSF startup?
- Are the Key Data Sets correctly displayed at ICSF startup?
- Are the ICSF options correctly displayed at ICSF startup?

N/A

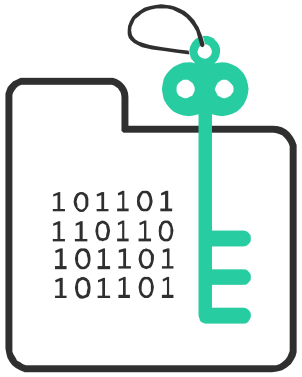
N/A

ICSF Started Task

```
//* This is the start proc for loading ICSF HCR77C1
//CSFEPC1 PROC
V=CSFDR7,CSFPRM='EYSHA.ICSF.Z14.ENCRYPT.STEP2.CONFIG'
//CSFSTEP EXEC PGM=CSFINIT,REGION=0M,TIME=1440
//CSFPARM DD DISP=SHR,DSN=&CSFPRM,VOL=SER=&V,UNIT=3390
```

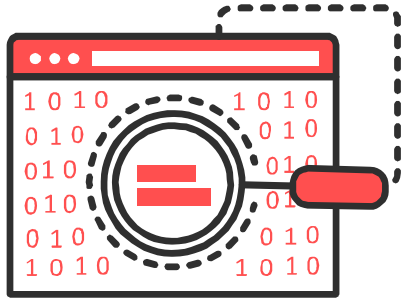
```
SY1 S0000055  CSFM111I CRYPTOGRAPHIC FEATURE IS ACTIVE. CRYPTO EXPRESS5
 COPROCESSOR 5C33, SERIAL NUMBER 99EA6076.
SY1 S0000055  CSFM100E CRYPTOGRAPHIC KEY DATA SET,
 EYSHA.ICSF.CSF77C1.CKDSR IS NOT INITIALIZED.
SY1 S0000055  CSFM508I CRYPTOGRAPHY - THERE ARE NO CRYPTOGRAPHIC
 ACCELERATORS ONLINE.
SY1 S0000055  CSFM015I FIPS 140 SELF CHECKS FOR PKCS11 SERVICES
 SUCCESSFUL.
SY1 S0000055  CSFM126I CRYPTOGRAPHY - FULL CPU-BASED SERVICES ARE
 AVAILABLE.
SY1 S0000055  CSFM001I ICSF INITIALIZATION COMPLETE
SY1 S0000055  CSFM640I ICSF RELEASE FMID=HCR77C1.
```

Step 4: Load AES Master Key



ICSF View

- How will Master Keys be loaded? TKE, Master Key Entry panels or PPINIT?
- How many key officers will have master key parts?
- How will master key parts be securely stored for future re-entry for disaster recovery or loading new adapters?



DFSMS View

N/A

RACF View

- Does the ICSF Admin have authorization to the ICSF panels for Master Key Entry which are protected by the CSFSERV class?

How do you generate, maintain and manage Master Keys?

Using the Trusted Key Entry (TKE) Workstation

- Applicable for initialization of ICSF Key Data Sets (i.e. key stores) and Crypto Express adapters
- Applicable for master key change operations
- Required for EP11 Master Key management & PCI-HSM Master Key management
- Separate, priced product

Trusted Key Entry (TKE) Workstation

Smart Cards

Smart Card Readers

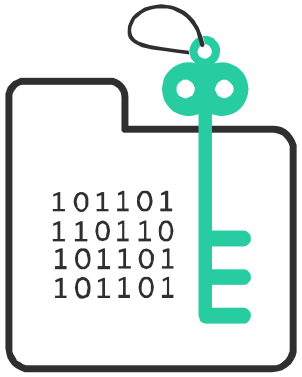
Using the ICSF Master Key Entry Panels

- Applicable for initialization of ICSF Key Data Sets (i.e. key stores) and Crypto Express adapters
- Applicable for master key change operations
- Included with z/OS and ICSF

Using the Pass Phrase Initialization (PPINIT) Panel

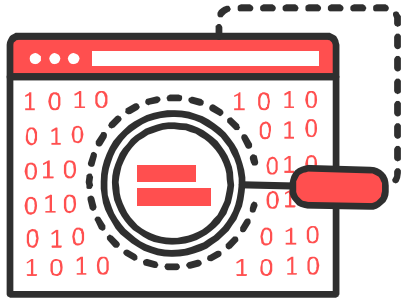
- Applicable for initialization of ICSF Key Data Sets (i.e. key stores) and Crypto Express adapters
- **NOT** applicable for master key change operations
- Included with z/OS and ICSF

Step 5: Initialize CKDS



ICSF View

- Is the CKDS empty?
- Are all Master Keys parts loaded?



DFSMS View

N/A

RACF View

- Does the ICSF Admin have authorization to the ICSF panels for CKDS Initialization which is protected by the CSFSERV class?

```
--------------------------- ICSF - CKDS Operations ---------------------------
COMMAND ===> 1

Enter the number of the desired option.

  1  Initialize an empty CKDS and activate master keys
  2  REFRESH  - Activate an updated CKDS
  3  Update an existing CKDS
  4  Update an existing CKDS and activate master keys
  5  Refresh and activate master keys


Enter the name of the CKDS below.

  CKDS ===> 'TST1.CKDS1'



Press ENTER to execute your option.
Press END   to exit to the previous menu.
```

ICSF Panel 2.1.1

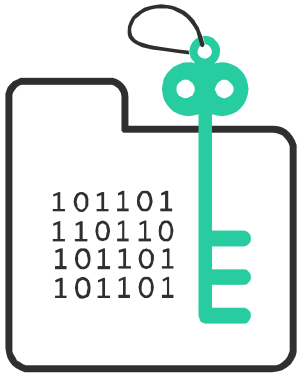
```
--------------------------- ICSF - CKDS Operations - INITIALIZATION COMPLETE
COMMAND ===>

Enter the number of the desired option.

  1  Initialize an empty CKDS and activate master keys
  2  REFRESH  - Activate an updated CKDS
  3  Update an existing CKDS
  4  Update an existing CKDS and activate master keys
  5  Refresh and activate master keys


Enter the name of the CKDS below.

  CKDS ===> 'TST1.CKDS1'



Press ENTE
Press END
```

Success

MVS Console

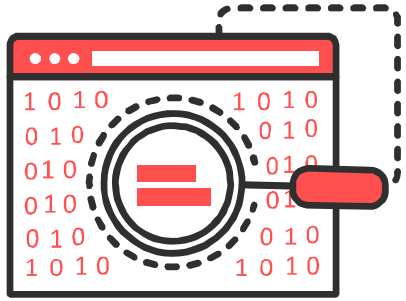
```
SY1 S0000040  CSFM129I MASTER KEY AES ON CRYPTO EXPRESS5 COPROCESSOR 5C35,
  SERIAL NUMBER 99EA6076, IS CORRECT.
SY1 S0000040  CSFM129I MASTER KEY AES ON CRYPTO EXPRESS5 COPROCESSOR 5C36,
  SERIAL NUMBER 99EA6096, IS CORRECT.
SY1 S0000040  CSFM127I CRYPTOGRAPHY - AES SERVICES ARE AVAILABLE.
```

Step 6: Generate a Secure AES DATA Key



ICSF View

- What naming convention should I use for the data set keys? Will it include the generic data set resource covering the data sets?
- How long should the encryption key be active?
- What tool, utility or application will be used to generate the key?



DFSMS View

- Will each data set have its own encryption key?
- Which data sets should be grouped and encrypted with the same key?
- Does the ICSF Admin know how many keys to generate?
- Does the ICSF Admin know the proper naming convention?

RACF View

- Does the ICSF Admin have authorization to the ICSF panels and/or callable services (APIs) for key generation?

```
aes_key_label = ,
   left('DATASET.EYSHA.ICSF.ENCRYPT.ME.ENCRKEY.00000001',64);
kgn_key_form            = 'OP   ';
kgn_key_length          = 'KEYLN32 ';
kgn_key_type_1          = 'AESDATA ';
kgn_key_type_2          = '';
kgn_kek_identifier_1    = copies('00'x,64);
kgn_kek_identifier_2    = '';
kgn_generated_key_identifier_1 = copies('00'x,64);
kgn_generated_key_identifier_2 = '';
Call CSNBKGN;

krc2_label = aes_key_label;
krc2_token_length = '00000040'x;
krc2_token = kgn_generated_key_identifier_1;
Call CSNBKRC2;
```

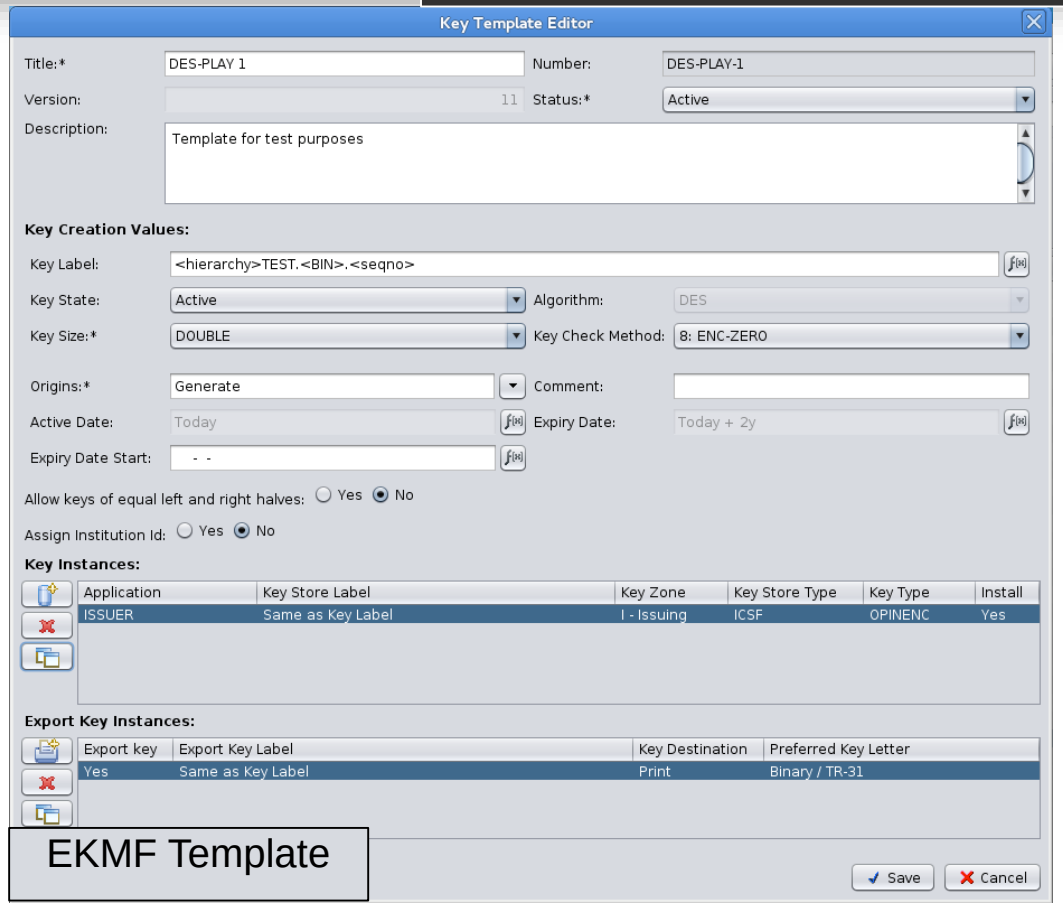
ICSF API

```
------------------------- ICSF - CKDS Generate Key -------------------------
COMMAND ===>

Active CKDS: EYSHA.ICSF.CSF77C1.CKDSR

Enter the CKDS record label for the new AES DATA key
==> DATASET.EYSHA.ICSF.ENCRYPT.ME.ENCRKEY.00000001

AES key bit length:   _ 128   _ 192   s 256
```

ICSF CKDS KEYS Panel (HCR77C1)

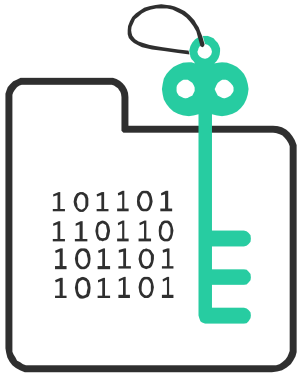
```
------------- ICSF - Create ADD, UPDATE, or DELETE Key Statement -------------
Specify control statement information below

   Function  ===> ADD___     ADD, UPDATE, or DELETE
   Algorithm ===> AES        DES or AES
   Key Type  ===> DATA____    Outtype ===> ________    (Optional)
   Label ===> ____________________________________________________________
    Group Labels  ===> NO_   NO or YES
 or Range:
   Start ===> DATASET.EYSHA.ICSF.ENCRYPT.ME.ENCRKEY.0005_____________________
   End   ===> DATASET.EYSHA.ICSF.ENCRYPT.ME.ENCRKEY.0010_____________________

    Transport Key Label(s)
         ===> ____________________________________________________________
         ===> ____________________________________________________________
 or Clear Key              ===> NO_      NO or YES
   Control Vector ===> YES  NO or YES
   Length of Key  ===> ___  For DES: 8, 16 or 24   For AES: 16, 24, or 32
   Key Values     ===>
    ________________ , ________________ , ____
COMMAND ===>
```

ICSF KGUP

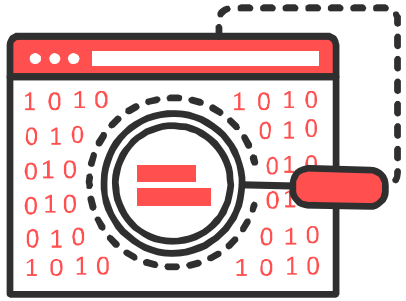


EKMF Template

Step 7: Protect Data Sets with Secure Keys



ICSF View



DFSMS View

RACF View

- Does the Security Admin have the key label names to use for the generic data set profile?

- Does the Security Admin have the mapping of the key label names to the data set names to be covered by generic data set profiles?

- Should data set encryption be limited to security admins only? Should data set owners and/or storage admins be able to add key labels at dataset allocation?
- What key labels should be assigned to which dataset profiles?
- Which users should have access to the dataset profiles? What access level?

```
RDEFINE FACILITY STGADMIN.SMS.ALLOW.DATASET.ENCRYPT UACC(NONE)

SETROPTS RACLIST(FACILITY) REFRESH
```

Restrict data set encryption to security administrators using SAF profiles.

Use generic profiles to control access to subsets of data sets.

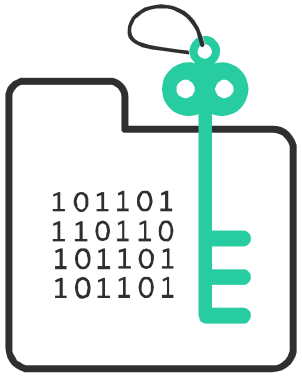
```
ADDSD 'EYSHA.ICSF.ENCRYPT.ME.*' UACC(NONE)

ALTDSD 'EYSHA.ICSF.ENCRYPT.ME.*'                                    +
  DFP(DATAKEY(DATASET.EYSHA.ICSF.ENCRYPT.ME.ENCRKEY.00000001))

/* SETROPTS GENERIC(DATASET) REFRESH */
```

Specify a DFP segment with the DATAKEY set to the key label in the CKDS where the encryption key resides.

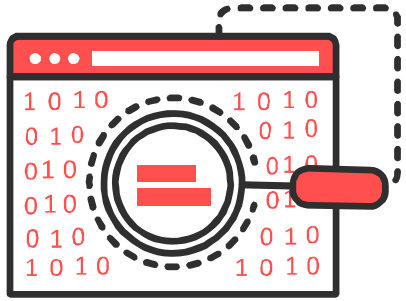
```
ADDUSER DATAOWN PASSWORD(change-me) TSO(ACCTNUM(123) PROC(TST77C1))
ADDUSER STORADM PASSWORD(change-me) TSO(ACCTNUM(123) PROC(TST77C1))

PERMIT 'EYSHA.ICSF.ENCRYPT.ME.*' ID(DATAOWN) ACCESS(UPDATE)
PERMIT 'EYSHA.ICSF.ENCRYPT.ME.*' ID(STORADM) ACCESS(ALTER)
```

Permit access to the data set as usual.

Step 8: Authorize Key Users



ICSF View



DFSMS View

RACF View

- Does the Security Admin have the key label naming conventions to grant access to data set encryption keys?

- Which users should be able to view the data set contents?

- What CSFKEYS resources should be created to protect the dataset key labels?
- Which users should have READ access to those CSFKEYS profiles?

The class that protects ICSF keys in the CKDS and PKDS

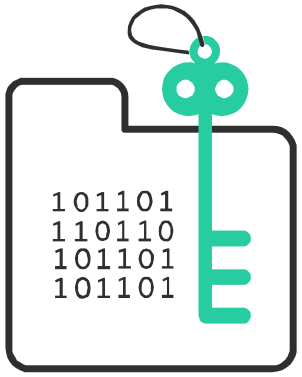
The resource protecting all key labels that match the pattern

```
RDEFINE CSFKEYS DATASET.EYSHA.ICSF.ENCRYPT.ME.* UACC(NONE)

RALTER CSFKEYS DATASET.EYSHA.ICSF.ENCRYPT.ME.*                    +
  ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES))

PERMIT DATASET.EYSHA.ICSF.ENCRYPT.ME.* CLASS(CSFKEYS) ID(DATAOWN)  +
   ACCESS(READ) WHEN(CRITERIA(SMS(DSENCRYPTION)))

SETROPTS RACLIST(CSFKEYS) REFRESH
```

New segment that indicates the user is permit access to the key label only for data set encryption.

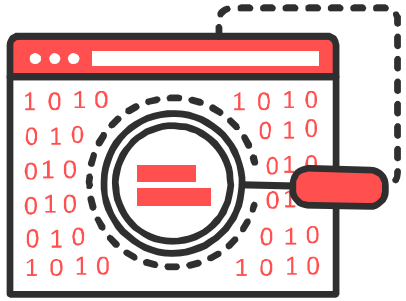
Fields that enable the use of protected keys and the ability to return protected keys to authorized callers such as DFSMS.

Step 9: Allocate Data Sets



ICSF View

N/A



DFSMS View

- Do data classes exist for extended format (DSNTYPE=EXTR or EXTP)?
- Are the ACS routines modified to select these data classes for the data sets?
- Are there data classes that also have compressed format (COMPACTION=)?
- Are zEDC features installed for use with zEDC compression?

RACF View

N/A

Allocate a data set using TSO Allocate or JCL.

```
ALLOCATE DATASET('EYSHA.ICSF.ENCRYPT.ME.DATA') STORCLAS(NOSPACE)        +
  RECFM(F,B) BLOCK(80) DSNTYPE(EXTREQ) NEW

FREE DATASET('EYSHA.ICSF.ENCRYPT.ME.DATA')
```

The data set to be encrypted must be:

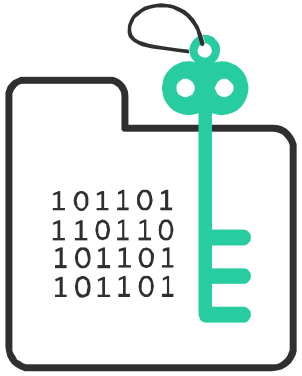
- SMS Managed
- Extended Format
  - Data class DSNTYPE=EXTR or EXTP
  - JCL DSNTYPE=EXTREQ or EXTPREF
- QSAM or BSAM
  - Sequential Data Sets
- VSAM or VSAM/RLS
  - KSDS, ESDS, RRDS, VRRDS, LDS
- Stored on Device Type 3390

The data set to be encrypted must NOT be:

- A system data set (such as Catalogs, SHCDS, HSM data sets)
- A data set used before ICSF is started:
  - RACF database
- The ICSF Key Data Set
- Basic and Large format sequential
- PDS/PDSE
- BDAM

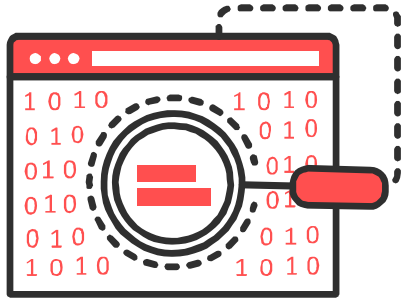
Data must be compressed prior to encryption!

Step 10: Write & Print Cipher Text



ICSF View

N/A



DFSMS View

- Are authorized users able to view dataset content?
- Are unauthorized user able to manage the data set without viewing the data set?

RACF View

- Are unauthorized users prevented from viewing dataset content?
- Are audit records produced showing crypto usage?
- Are audit records produced showing key usage?

Write (or copy) data to the data set

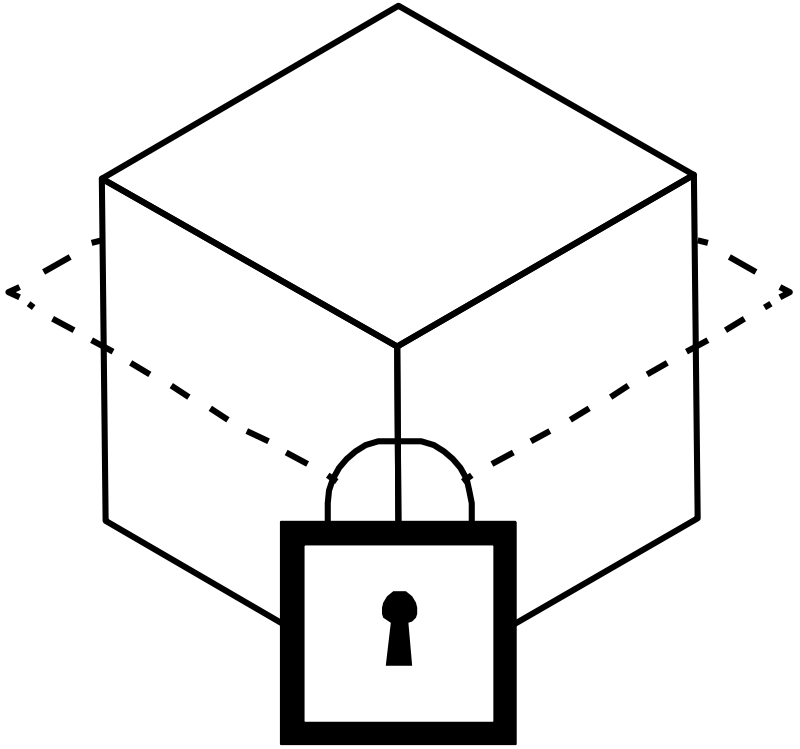
```
//UPDATE   EXEC PGM=IEBDG
//SYSPRINT DD  SYSOUT=*
//OUTDATA  DD  DSNAME=EYSHA.ICSF.ENCRYPT.ME.DATA,UNIT=3390
,
//            DISP=(OLD,KEEP),VOLUME=SER=SMSVL1,
//            DCB=(RECFM=FB,LRECL=80,BLKSIZE=80)
//SYSIN    DD  *
   DSD     OUTPUT=(OUTDATA)
   FD      NAME=HELLO,LENGTH=11,PICTURE=11,'hello world'
   CREATE  QUANTITY=1,NAME=(HELLO)
   END
```

Print the data on the track

```
//PRINT    EXEC PGM=ADRDSSU
//SYSPRINT DD   SYSOUT=*
//SYSIN    DD   *
   PRINT DATASET(EYSHA.ICSF.ENCRYPT.ME.DATA)
INDYNAM(SMSVL1)
/*
```

Live Demo…

1. Configure Crypto Express Cards
2. Configure ICSF
3. Start ICSF
4. Load AES MK
5. Initialize CKDS
6. Generate a Secure AES Data Key
7. Protect Data Sets with Secure Keys
8. Authorize Key Users
9. Allocate Data Sets
10. Write & Print the Encrypted Data Set



Recorded Demonstration:
http://www.newera-info.com/EP1.html

Additional Resources

Pervasive Encryption Wiki
http://ibm.biz/zos-pervasive-encryption-wiki

IBM Crypto Education Community
https://www.ibm.com/developerworks/community/groups/community/crypto

Getting Started with z/OS Data Set Encryption Redbook
http://www.redbooks.ibm.com/redpieces/abstracts/sg248410.html?Ope

We want your feedback!

Please submit your feedback online at ….

- http://conferences.gse.org.uk/2018/feedback/ff

Paper feedback forms are also available from the Chair person

This session is FF