Vanguard Security Conference

May 31 – June 4 2009 – Jacksonville Florida

Session Title: Customization of Crypto on z

Session ID: CRP-3

Speaker Name: Ernest Nachtigall **CISSP;CISA**

THE Open GROUP
Master
Certified IT Specialist

Trademarks

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

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer , FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* 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.

Agenda

- z9 z10 Hardware Setup
- z9 z10 ICFS Setup
  - Cautions, Recommendations
- z9 z10 Master Key Entry

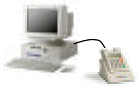
What's New for ICSF V1 R10 --- HCR7751

- HCR7751 requires new LIC and some functions are only available on z10
  - z10 Driver 76D (Nov 2008)
  - z9 Driver 67L (Nov 2008)
- Secure AES keys
  - New Master Key Register for AES (32-byte master key)
  - New callable services to use encrypted AES keys
- Key Store Policy which works in conjuction with CSFKEYS
  - New authorization checks
  - New SAF general resource classes
  - New utility for detection of duplicate tokens
- Support for CKDS on System z without CEX2C
  - Caution - CKDS not uniquely identified from secure CKDS
- Support of PAN-14, -15, -17, -18
- New Query services calls to enhance CSFIQF

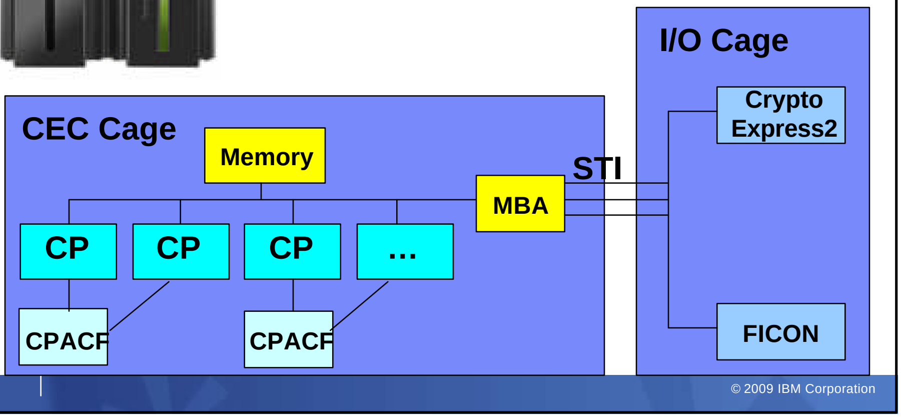
Hardware Setup

- Order and install Feature Code 3863
  - Base code, book 0
    - Required for any crypto functions (export control)

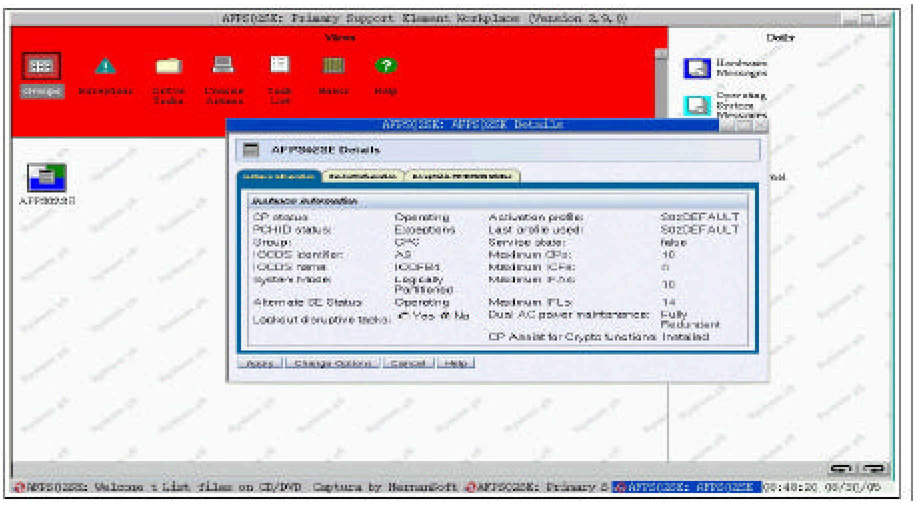
- Evaluate need for secure key crypto
  - **Usually required**
    - Provides traditional banking, retail, PCI-DSS functions
    - Feature Code 0863 on z10-EC, 0870 on z10-BC
- Evaluate need for TKE
  - Secure key injection
  - Possible PCI requirement



z10 Crypto HW



FC 3863 Installed



APPS02SE: Primary Support Element Workplace (Version 2.9.0)

APPS02SE: APPS02SE Details

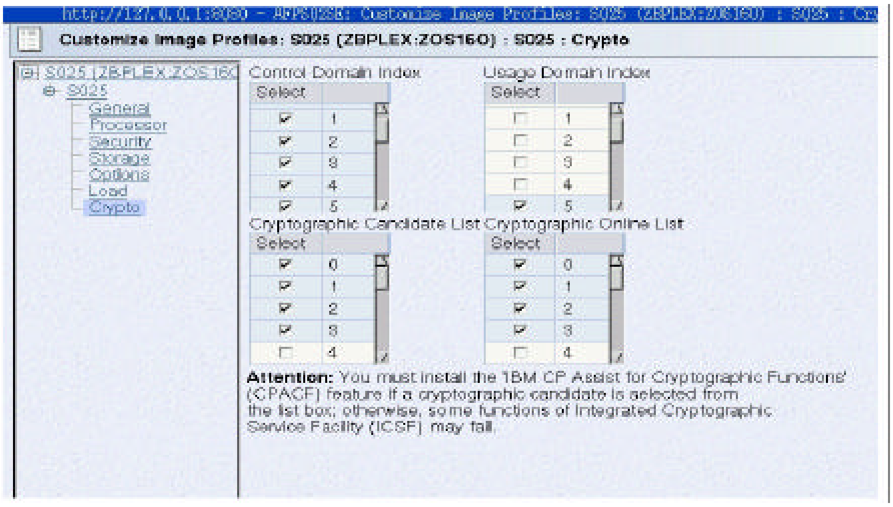
APPS02SE Details

Instance Information

CP status:	Operating	Activation profile:	S02DEFAULT
PCHID status:	Exceptions	Last profile used:	S02DEFAULT
Group:	CPC	Service state:	false
IOCDS identifier:	A2	Maximum CPs:	10
IOCDS name:	IOCF01	Maximum ICFs:	0
System Mode:	Logically Partitioned	Maximum IFAs:	10
Alternate SE Status:	Operating	Maximum IFLs:	14
Lockout disruptive tasks:	○ Yes ● No	Dual AC power maintenance:	Fully Redundant
		CP Assist for Crypto functions:	Installed

APPS02SE: Welcome | List files on CD/DVD | Capture by HarmanSoft | APPS02SE: Primary S | APPS02SE: APPS02SE | 08:48:20 08/20/05

Crypto Definitions



http://127.0.0.1:8080 - APPS02SE: Customize Image Profiles: S025 (ZBPLEX:ZOS160) : S025 : Cry

Customize Image Profiles: S025 (ZBPLEX:ZOS160) : S025 : Crypto

Control Domain Index

Select	
☑	1
☑	2
☑	3
☑	4
☑	5

Usage Domain Index

Select	
□	1
□	2
□	3
□	4
☑	5

Cryptographic Candidate List

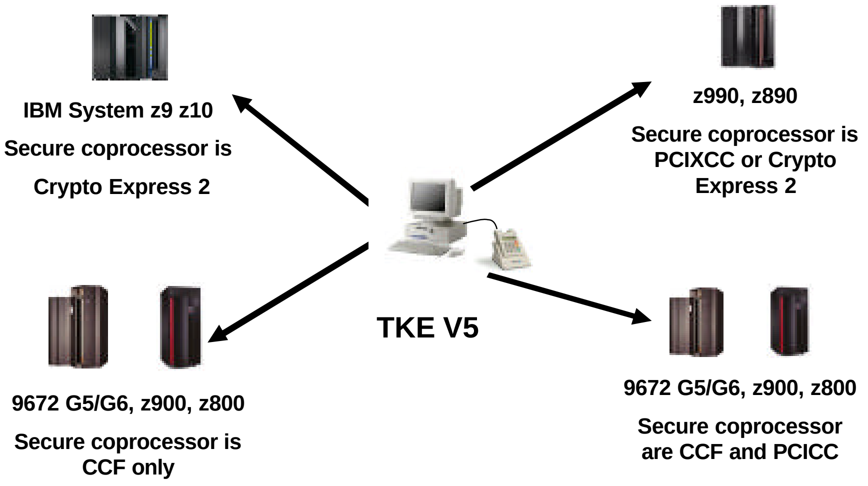
Select	
☑	0
☑	1
☑	2
☑	3
□	4

Cryptographic Online List

Select	
☑	0
☑	1
☑	2
☑	3
□	4

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.

TKE Support



IBM System z9 z10

Secure coprocessor is

Crypto Express 2

z990, z890

Secure coprocessor is PCIXCC or Crypto Express 2

TKE V5

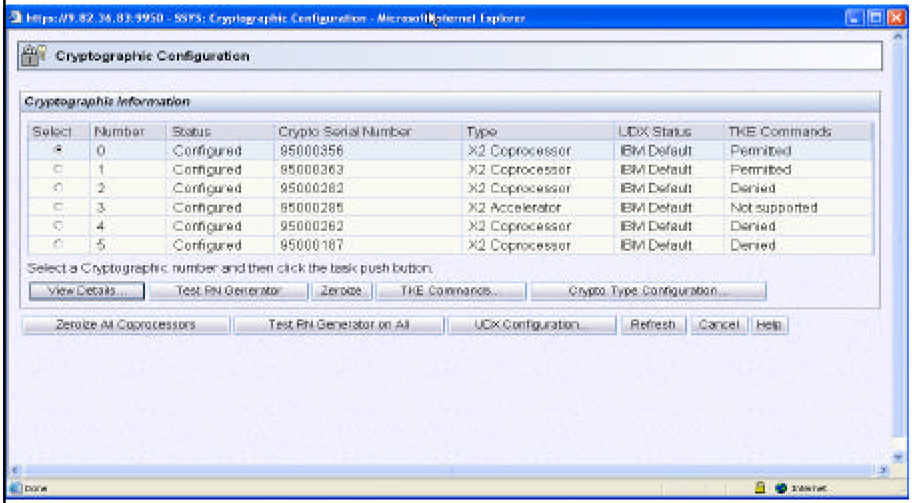
9672 G5/G6, z900, z800

Secure coprocessor is CCF only

9672 G5/G6, z900, z800

Secure coprocessor are CCF and PCICC

z9/z10 Cryptographic Configuration



https://9.82.36.83:9950 - SSYS: Cryptographic Configuration - Microsoft Internet Explorer

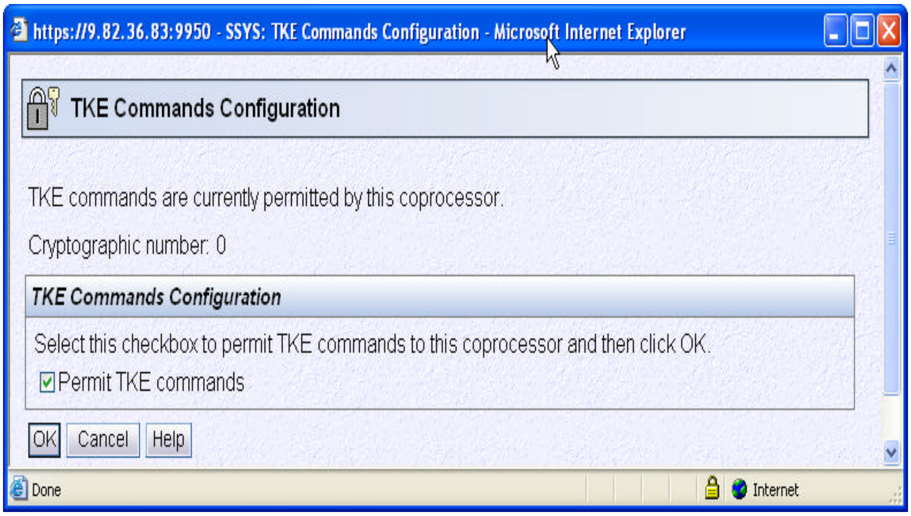
Cryptographic Configuration

Cryptographic Information

Select	Number	Status	Crypto Serial Number	Type	UDX Status	TKE Commands
●	0	Configured	95000356	X2 Coprocessor	IBM Default	Permitted
○	1	Configured	95000363	X2 Coprocessor	IBM Default	Permitted
○	2	Configured	95000282	X2 Coprocessor	IBM Default	Denied
○	3	Configured	95000285	X2 Accelerator	IBM Default	Not supported
○	4	Configured	95000262	X2 Coprocessor	IBM Default	Denied
○	5	Configured	95000187	X2 Coprocessor	IBM Default	Denied

Select a Cryptographic number and then click the task push button.

Permit TKE Commands



https://9.82.36.83:9950 - SSYS: TKE Commands Configuration - Microsoft Internet Explorer

TKE Commands Configuration

TKE commands are currently permitted by this coprocessor.

Cryptographic number: 0

TKE Commands Configuration

Select this checkbox to permit TKE commands to this coprocessor and then click OK.

☑ Permit TKE commands

System Programmer Tasks

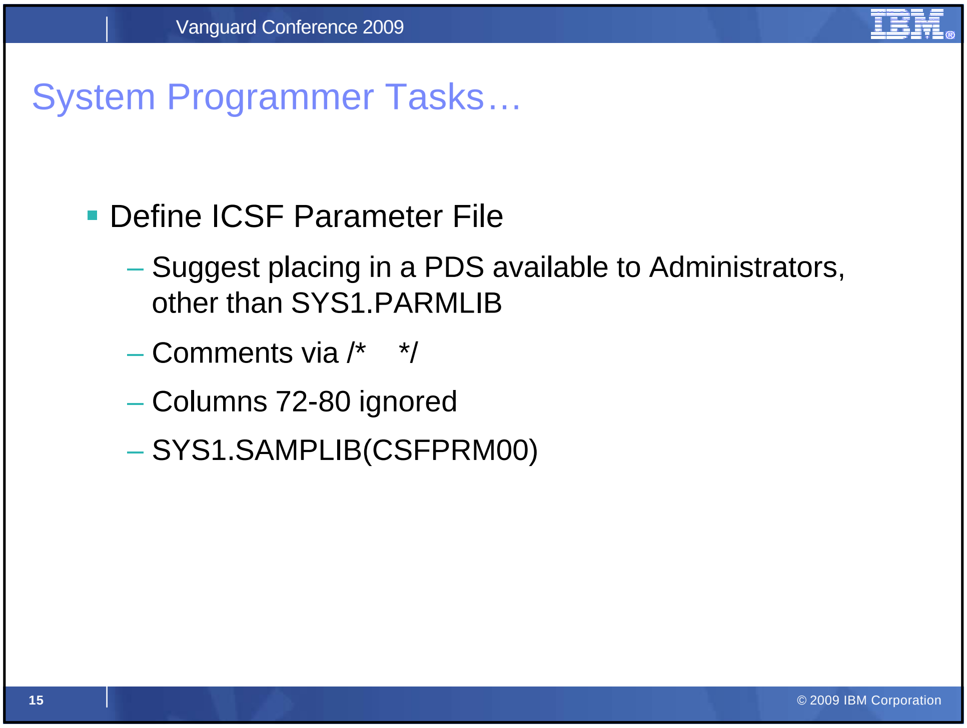
- Install ICSF FMID (HCR7751)
- Add authorizations
- Define Data Sets
- Define ICSF Parameter File
- Add ISPF panels
- Define System Task
- Start ICSF

System Programmer Tasks…

- Add authorizations
  - – Add CEE.SCEERUN and CSF.SCSFMOD0 to LNKLST
  - – APF authorize CSF.SCSFMOD0,
  - – In IKJTSOxx, add CSFDAUTH and CSFDPKDS in the AUTHPGM and the AUTHTSF parameter lists.
  - – Add CSFTTKE in the AUTHCMD

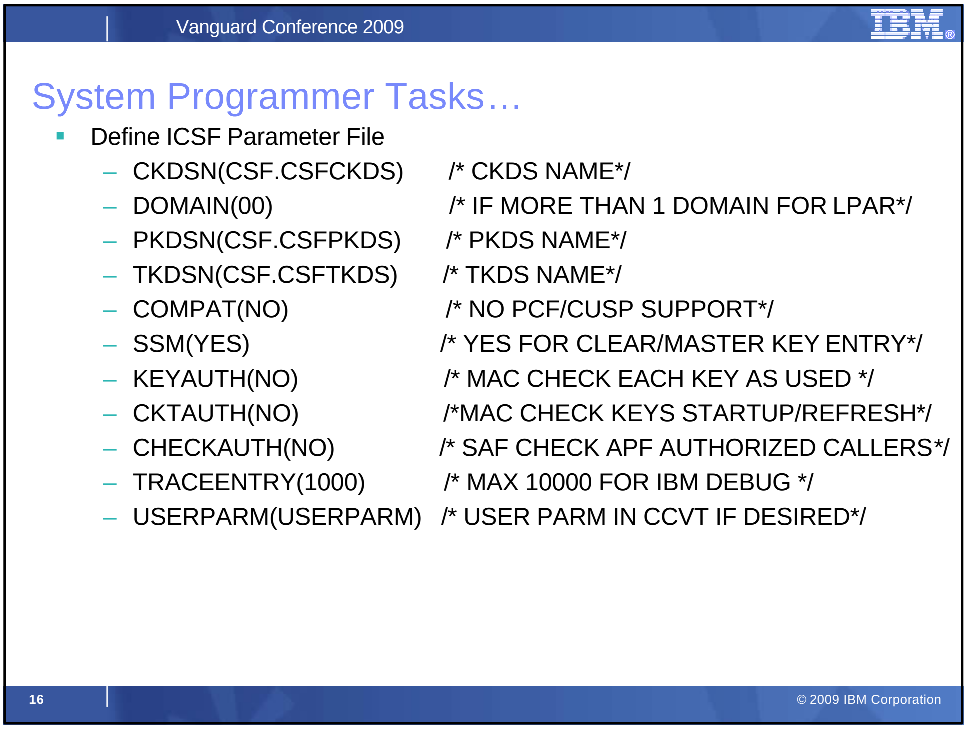
System Programmer Tasks…

- Define Data Sets
  - – Use SYS1.SAMPLIB members CSFCKDS (symmetric keys), CSFPKDS (RSA keys), CSFTKDS (PKCS#11 keys)
    - Toleration support APAR for backlevel systems for a **larger PKDS LRECL (4096 bit keys)**
  - – SAF protect these datasets. Only backup/archive jobs need access. Application code does not directly address/use these files.



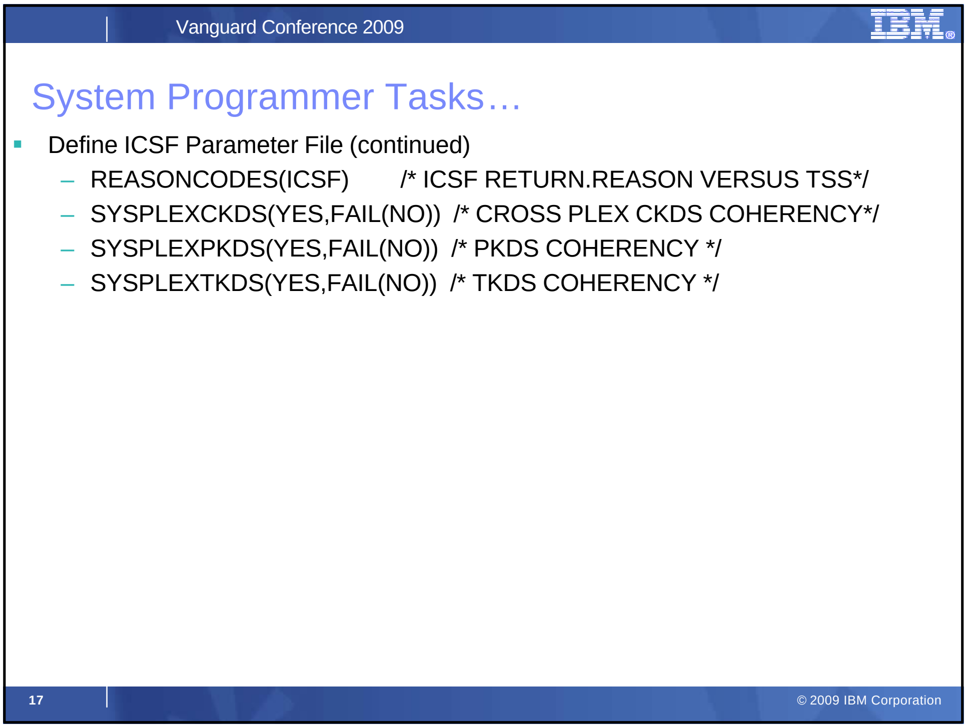
System Programmer Tasks…

- Define ICSF Parameter File
  - Suggest placing in a PDS available to Administrators, other than SYS1.PARMLIB
  - Comments via /*   */
  - Columns 72-80 ignored
  - SYS1.SAMPLIB(CSFPRM00)



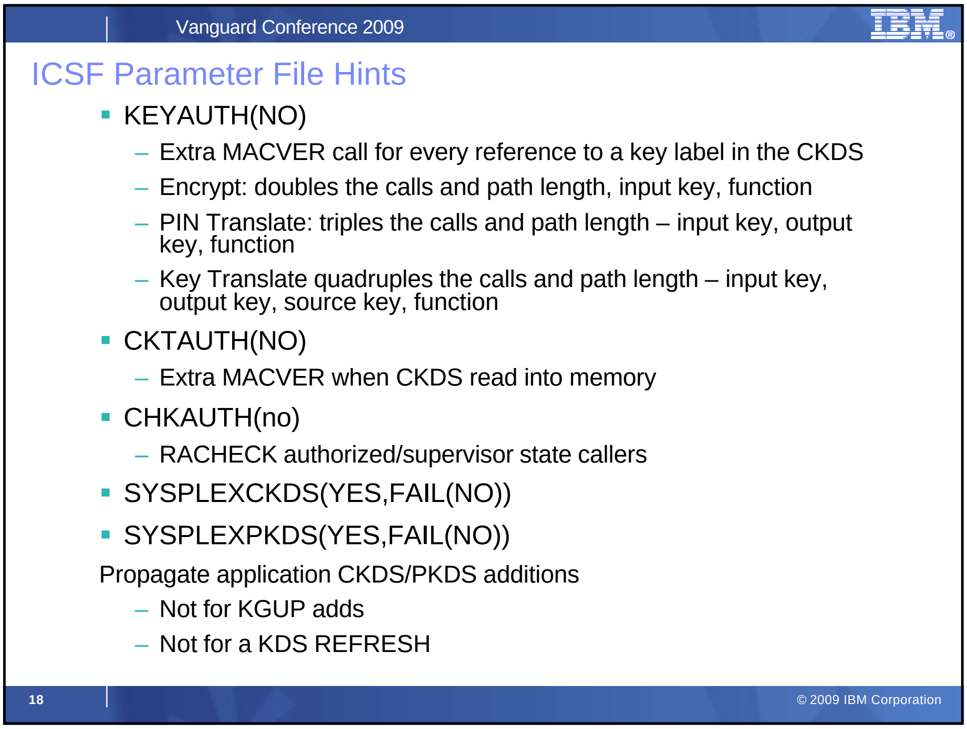
System Programmer Tasks…

- Define ICSF Parameter File
  - CKDSN(CSF.CSFCKDS)   /* CKDS NAME*/
  - DOMAIN(00)   /* IF MORE THAN 1 DOMAIN FOR LPAR*/
  - PKDSN(CSF.CSFPKDS)   /* PKDS NAME*/
  - TKDSN(CSF.CSFTKDS)   /* TKDS NAME*/
  - COMPAT(NO)   /* NO PCF/CUSP SUPPORT*/
  - SSM(YES)   /* YES FOR CLEAR/MASTER KEY ENTRY*/
  - KEYAUTH(NO)   /* MAC CHECK EACH KEY AS USED */
  - CKTAUTH(NO)   /*MAC CHECK KEYS STARTUP/REFRESH*/
  - CHECKAUTH(NO)   /* SAF CHECK APF AUTHORIZED CALLERS*/
  - TRACEENTRY(1000)   /* MAX 10000 FOR IBM DEBUG */
  - USERPARM(USERPARM)   /* USER PARM IN CCVT IF DESIRED*/



System Programmer Tasks…

- Define ICSF Parameter File (continued)
  - REASONCODES(ICSF)   /* ICSF RETURN.REASON VERSUS TSS*/
  - SYSPLEXCKDS(YES,FAIL(NO)) /* CROSS PLEX CKDS COHERENCY*/
  - SYSPLEXPKDS(YES,FAIL(NO)) /* PKDS COHERENCY */
  - SYSPLEXTKDS(YES,FAIL(NO)) /* TKDS COHERENCY */



ICSF Parameter File Hints

- KEYAUTH(NO)
  - Extra MACVER call for every reference to a key label in the CKDS
  - Encrypt: doubles the calls and path length, input key, function
  - PIN Translate: triples the calls and path length – input key, output key, function
  - Key Translate quadruples the calls and path length – input key, output key, source key, function
- CKTAUTH(NO)
  - Extra MACVER when CKDS read into memory
- CHKAUTH(no)
  - RACHECK authorized/supervisor state callers
- SYSPLEXCKDS(YES,FAIL(NO))
- SYSPLEXPKDS(YES,FAIL(NO))

Propagate application CKDS/PKDS additions

- Not for KGUP adds
- Not for a KDS REFRESH

System Programmer Tasks…

- Define System Task
  - //CSF PROC M=CSFPRM00
  - //CSF EXEC PGM=CSFMMAIN,REGION=6M,TIME=1440
  - //CSFLIST DD SYSOUT=A,LRECL=132,BLKSIZE=132
  - //CSFPARM DD DSN=ICSF.PARMLIB(&M),DISP=SHR

System Programmer Tasks…

- update the RACF Started Procedure Table if you define a new started task:
  - Add the new started task name
  - Add a RACF userid to associate with the started task. This userid requires READ access to the data set to which the CSFPARM JCL DD statement refers

System Programmer Tasks…

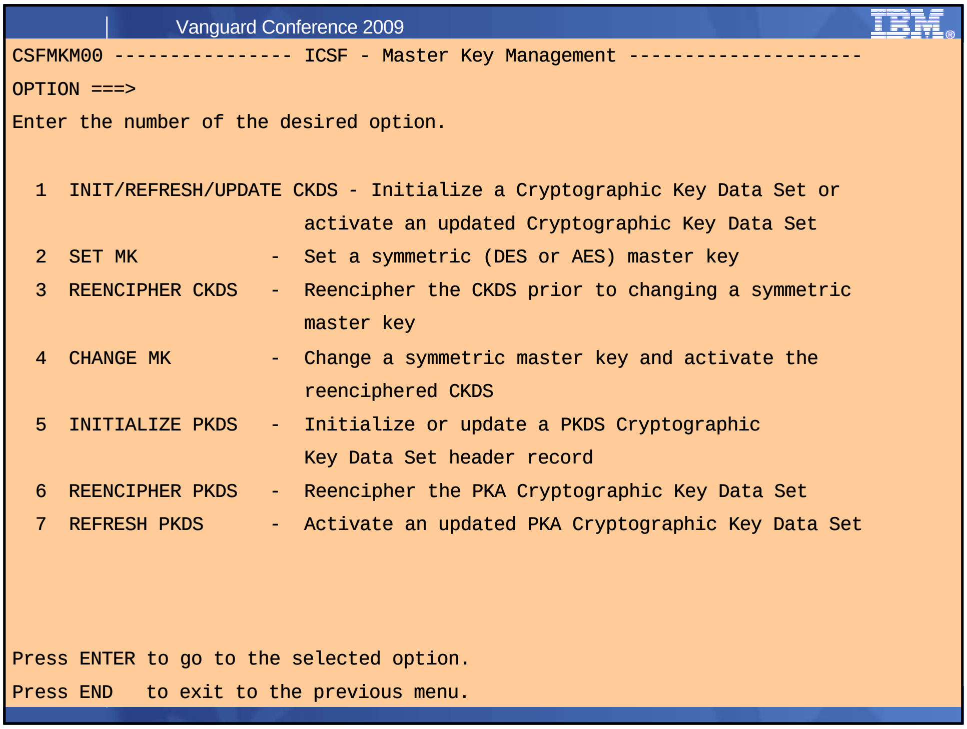
- Add ISPF panels
  - Access the code for the ISPF Primary Option Menu panel body and perform these steps:
  - Under the % OPTION ===> _ZCMD line, add this line: % <option value> - ICSF Panels
  - You can specify either a letter or number for the option value. Do not use an option value that already exists in the menu.
  - On the &ZSEL= TRANS(&ZQ line, add this information: <option value>,’PANEL(CSF@PRIM)’

Administrator Tasks

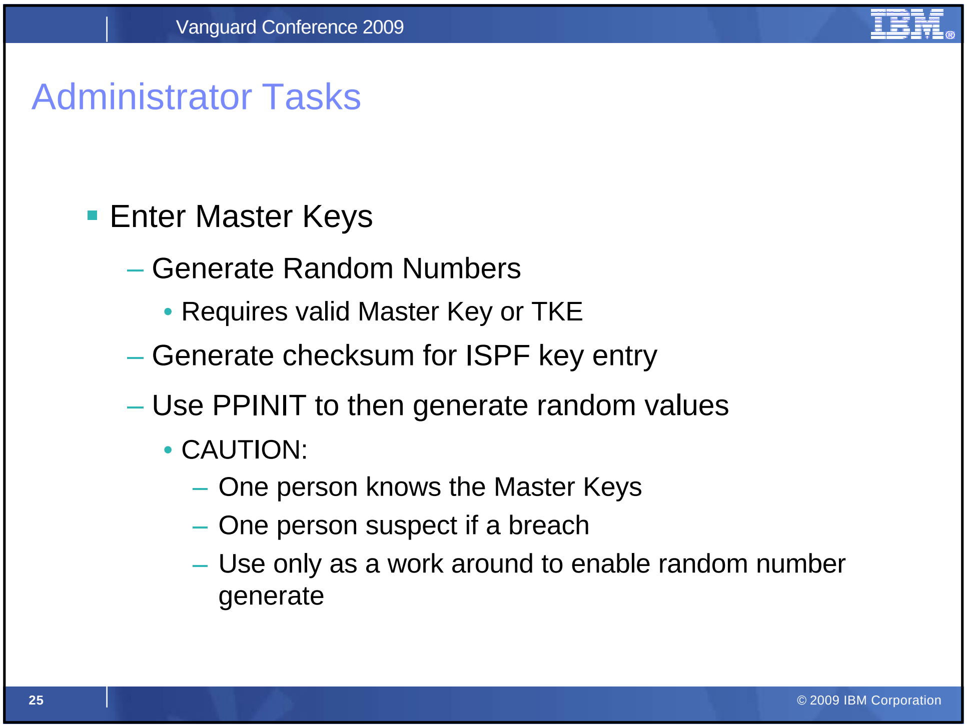
- Define SAF rules CSFSERV, CSFKEYS
  - Optionally XFACLIT XCSFKEY
- Initialize data sets
- Allocate Key Administrators (CEX2C)
  - Master Key parts
  - Application Key parts
  - Backups
  - DR
- Enter Master Keys

Administrator Tasks

- Initialize Data Sets
  - Only done once on a new set of data sets for a first time install
    - CKDS will not allow initialize of an already initialized CKDS
  - CAUTION
    - PKDS used to allow, but should not be used on an active PKDS (changes hash pattern but does not re-encipher the keys)
  - INITIALIZE is designed to prepare a PLEX for a first time install ONLY

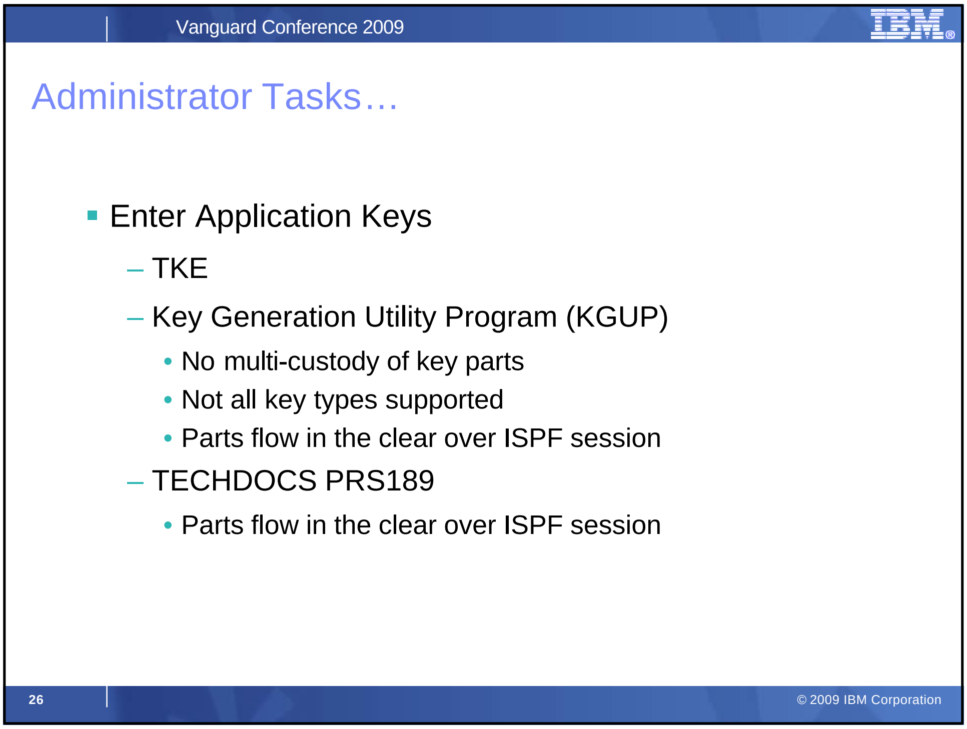


```
CSFMKM00 ---------------- ICSF - Master Key Management --------------------
OPTION ===>
Enter the number of the desired option.

  1  INIT/REFRESH/UPDATE CKDS - Initialize a Cryptographic Key Data Set or
                            activate an updated Cryptographic Key Data Set
  2  SET MK               -  Set a symmetric (DES or AES) master key
  3  REENCIPHER CKDS      -  Reencipher the CKDS prior to changing a symmetric
                            master key
  4  CHANGE MK            -  Change a symmetric 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  REFRESH PKDS         -  Activate an updated PKA Cryptographic Key Data Set



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



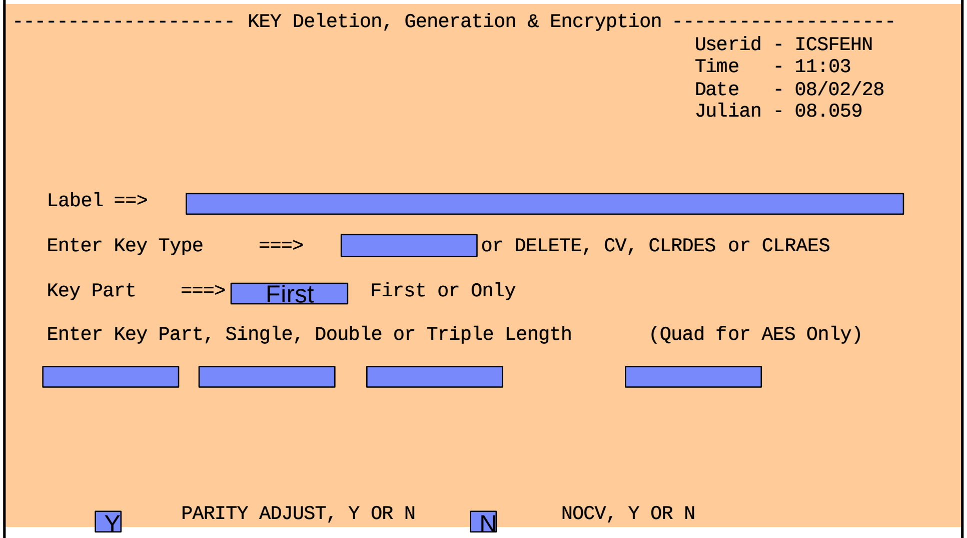
Administrator Tasks

- Enter Master Keys
  - Generate Random Numbers
    - Requires valid Master Key or TKE
  - Generate checksum for ISPF key entry
  - Use PPINIT to then generate random values
    - CAUTION:
      - One person knows the Master Keys
      - One person suspect if a breach
      - Use only as a work around to enable random number generate



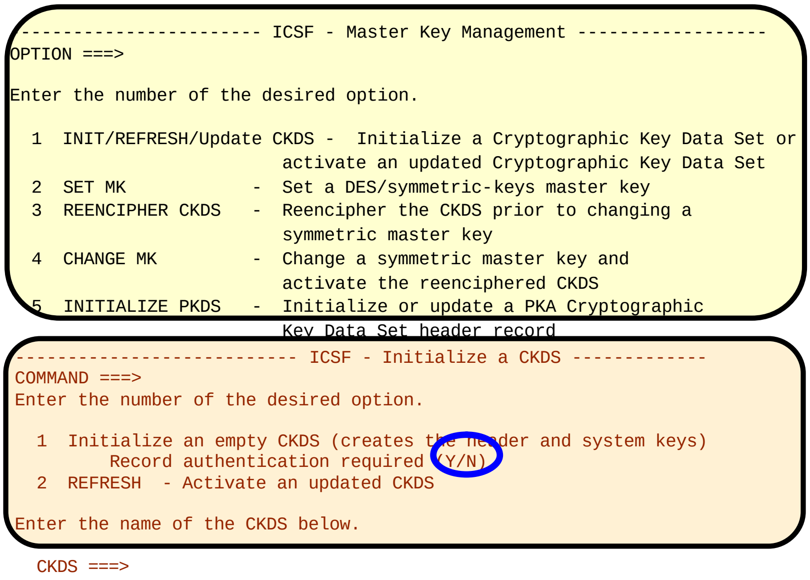
Administrator Tasks…

- Enter Application Keys
  - TKE
  - Key Generation Utility Program (KGUP)
    - No multi-custody of key parts
    - Not all key types supported
    - Parts flow in the clear over ISPF session
  - TECHDOCS PRS189
    - Parts flow in the clear over ISPF session



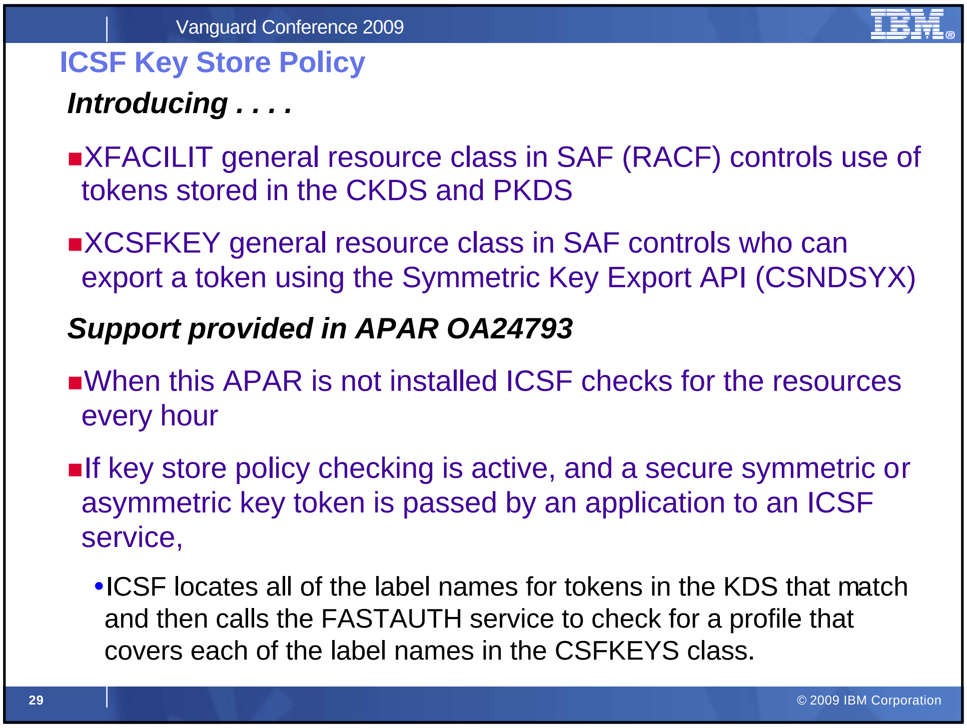
```
-------------------- KEY Deletion, Generation & Encryption --------------------
                                                             Userid - ICSFEHN
                                                             Time   - 11:03
                                                             Date   - 08/02/28
                                                             Julian - 08.059


   Label ==>

   Enter Key Type     ===>              or DELETE, CV, CLRDES or CLRAES

   Key Part    ===>   First      First or Only

   Enter Key Part, Single, Double or Triple Length       (Quad for AES Only)




        Y      PARITY ADJUST, Y OR N      N      NOCV, Y OR N
```

Now, Update the CKDS as Needed . . .



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

Enter the number of the desired option.

  1  INIT/REFRESH/Update CKDS -  Initialize a Cryptographic Key Data Set or
                                 activate an updated Cryptographic Key Data Set
  2  SET MK                  -   Set a DES/symmetric-keys master key
  3  REENCIPHER CKDS         -   Reencipher the CKDS prior to changing a
                                 symmetric master key
  4  CHANGE MK               -   Change a symmetric master key and
                                 activate the reenciphered CKDS
  5  INITIALIZE PKDS         -   Initialize or update a PKA Cryptographic
                                 Key Data Set header record
```

```
-------------------------- ICSF - Initialize a CKDS -------------
COMMAND ===>
Enter the number of the desired option.

  1  Initialize an empty CKDS (creates the header and system keys)
         Record authentication required (Y/N)
  2  REFRESH  - Activate an updated CKDS

Enter the name of the CKDS below.

  CKDS ===>
```



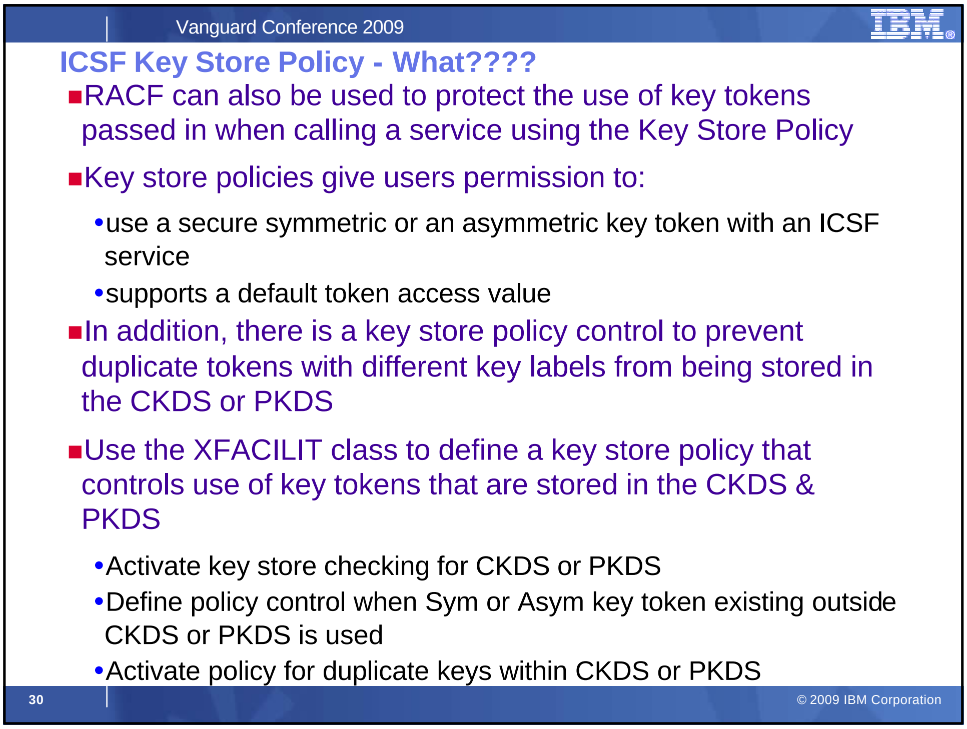
ICSF Key Store Policy

Introducing . . . .

- XFACILIT general resource class in SAF (RACF) controls use of tokens stored in the CKDS and PKDS
- XCSFKEY general resource class in SAF controls who can export a token using the Symmetric Key Export API (CSNDSYX)

Support provided in APAR OA24793

- When this APAR is not installed ICSF checks for the resources every hour
- If key store policy checking is active, and a secure symmetric or asymmetric key token is passed by an application to an ICSF service,
  - ICSF locates all of the label names for tokens in the KDS that match and then calls the FASTAUTH service to check for a profile that covers each of the label names in the CSFKEYS class.



ICSF Key Store Policy - What????

- RACF can also be used to protect the use of key tokens passed in when calling a service using the Key Store Policy
- Key store policies give users permission to:
  - use a secure symmetric or an asymmetric key token with an ICSF service
  - supports a default token access value
- In addition, there is a key store policy control to prevent duplicate tokens with different key labels from being stored in the CKDS or PKDS
- Use the XFACILIT class to define a key store policy that controls use of key tokens that are stored in the CKDS & PKDS
  - Activate key store checking for CKDS or PKDS
  - Define policy control when Sym or Asym key token existing outside CKDS or PKDS is used
  - Activate policy for duplicate keys within CKDS or PKDS

ICSF Key Store Policy - What???? . . .

- Key Store Policy for KDS Label Checking
  - CSF.CKDS.TOKEN.CHECK.LABEL.WARN or CSF.CKDS.TOKEN.CHECK.LABEL.FAIL
  - CSF.PKDS.TOKEN.CHECK.LABEL.WARN or CSF.PKDS.TOKEN.CHECK.LABEL.FAIL
- Key Store Policy options for KDS
  - Key Store Policy supports both WARN and FAIL mode via profile name definition rather than by the SETROPTS setting
    - When the profile activing keystore policy checking ends with WARN, ICSF writes an 82 type SMF record containing an indictor that the key store policy checking is in WARN mode. The application result would have been success or failure and a list of all the labels that matched the token the application used is provided. The application is granted access to use the key token.
    - When the key store policy checking ends with FAIL, 80 type SMF records are written by RACF and the application is denied access. The resource name in the RACF SMF record is the first label that failed the check.

ICSF Key Store Policy - XCSFKEY

- The XCSKEY class profiles expands the protection against keys being sent outside of system

  CSF.XCSFKEY.ENABLE.AES

  CSF.XCSFKEY.ENABLE.DES
- Currently only the CSNBKEX API allowing export of DES/TDES keys has the capability of SAF protection of use
- XCSFKEY class only protects keys associated with CSNDSYX API meaning this profile allows protection of AES or DES keys exported by a RSA public key
- Those users or applications sending AES or DES keys outside of the system should have the appropriate authority under the XCSFKEY class appropriate profile
  - Applications that use SSL/TLS are examples of those that would need access to XCSFKEY if defined

ICSF Key Store Policy - XCSFKEY How ???

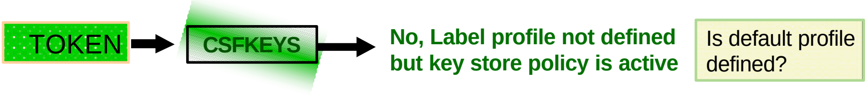
- The XCSKEY class profiles are

  RDEFINE XFACILIT CSF.XCSFKEY.ENABLE.AES

  RDEFINE XFACILIT CSF.XCSFKEY.ENABLE.DES
- XCSFKEY class controls who can export a token using the Symmetric Key Export callable service (CSNDSYX)
- Key policy control profiles in the XFACILIT class do not have to be active or RACLISTed

ICSF Key Store Policy - How????

- Key Store Policy for key tokens not in KDS
  - Key tokens that do not have a label due to being stored outside the KDS' can now have SAF protection
    - No profile would exist in CSFKEYS so only CSFSERV would provide protection for function but not for key value use
    - ICSF services will look for a DEFAULT.LABEL profile in the CSFKEYS class to determine application access for key use
- Define key store policy when a secure symmetric or an asymmetric key token not in a KDS is used
  - CSF.CKDS.TOKEN.CHECK.DEFAULT.LABEL CSF.PKDS.TOKEN.CHECK.DEFAULT.LABEL


TOKEN
CSFKEYS
No, Label profile not defined but key store policy is active
Is default profile defined?

ICSF Key Store Policy - How???? . . .

■Key Store Policy for key duplicates

- Key tokens whose key value when in the clear matches any other key token's key value when in the clear will be determined
  - ƒ If duplicate key checking active, applications attempting to write keys to the KDS with a value that exist will be prevented from writing the record
  - ƒ Key Duplicate checks both the 64-byte label and the control vectors associated with the key that represent the 8-byte key type for DES/TDES symmetric keys only (AES and RSA keys have no keytype)

■Define key store policy profile for key duplicates

- CSF.CKDS.TOKEN.NODUPLICATES
  CSF.PKDS.TOKEN.NODUPLICATES
- Applications will be prevented from using ICSF services to write a key token containing a duplicate key value to the the KDS
- This policy profile denies applications from doing what can be done via KGUP, ICSF's Key Generation Utility Program, with the "group label" option

ICSF Key Store Policy - How???? . . .

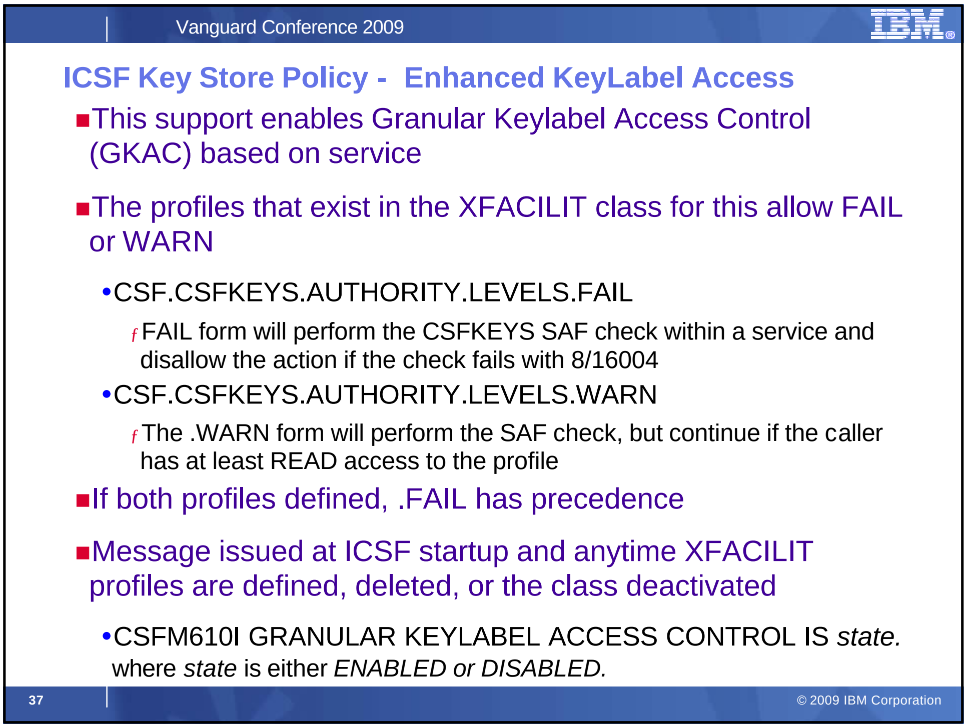
■New Batch Utility - CSFDUTIL to find duplicates

```
//STEP     EXEC PGM=CSFDUTIL,PARM='kdsname'
//DUTIL    EXEC PGM=CSFDUTIL
//SYSOUT  DD SYSOUT=A
//SYSIN      DD *
      CKDSN(ckds.name)
/*
```

- May wish to disable dynamic KDS services

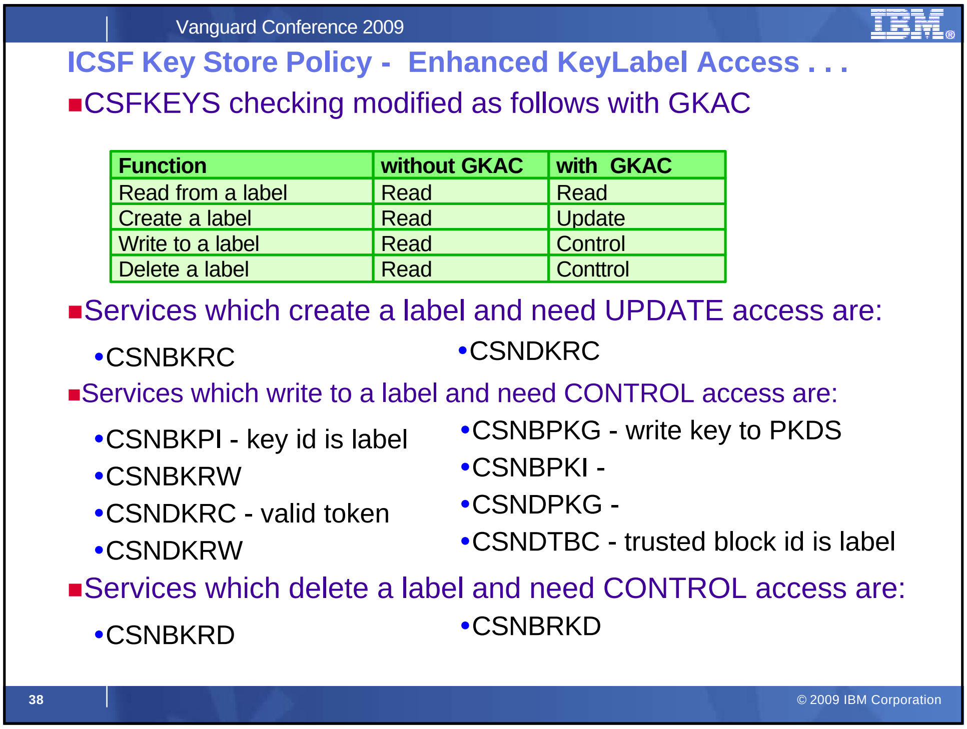
■Output from CSFDUTIL about any duplicates found

CKDS		PKDS	
Column	**Value**	**Column**	**Value**
1-62	Key label	1-62	Key label
67-74	Key type from KDS record	67-74	Create date
77-84	Create date	77-84	Create time
87-94	Create time	87-94	Last update date
97-104	Last update date	97-104	Last update time
107-114	Last update time		



ICSF Key Store Policy - Enhanced KeyLabel Access

- This support enables Granular Keylabel Access Control (GKAC) based on service
- The profiles that exist in the XFACILIT class for this allow FAIL or WARN
  - CSF.CSFKEYS.AUTHORITY.LEVELS.FAIL
    - FAIL form will perform the CSFKEYS SAF check within a service and disallow the action if the check fails with 8/16004
  - CSF.CSFKEYS.AUTHORITY.LEVELS.WARN
    - The .WARN form will perform the SAF check, but continue if the caller has at least READ access to the profile
- If both profiles defined, .FAIL has precedence
- Message issued at ICSF startup and anytime XFACILIT profiles are defined, deleted, or the class deactivated
  - CSFM610I GRANULAR KEYLABEL ACCESS CONTROL IS *state.* where *state* is either *ENABLED or DISABLED.*



ICSF Key Store Policy - Enhanced KeyLabel Access . . .

- CSFKEYS checking modified as follows with GKAC

Function	without GKAC	with GKAC
Read from a label	Read	Read
Create a label	Read	Update
Write to a label	Read	Control
Delete a label	Read	Conttrol

- Services which create a label and need UPDATE access are:
  - CSNBKRC
  - CSNDKRC
- Services which write to a label and need CONTROL access are:
  - CSNBKPI - key id is label
  - CSNBKRW
  - CSNDKRC - valid token
  - CSNDKRW
  - CSNBPKG - write key to PKDS
  - CSNBPKI -
  - CSNDPKG -
  - CSNDTBC - trusted block id is label
- Services which delete a label and need CONTROL access are:
  - CSNBKRD
  - CSNBRKD

ICSF Key Store Policy - Enhanced KeyLabel Access . . .

- XFACILIT class must be ACTIVE, but it does not have to be RACLISTed for granular keylabel access control to take effect.

- For more details see Chapter 2 in the V1.10 ICSF Administrator's Guide at URL

  http://publibz.boulder.ibm.com/epubs/pdf/csfb3z90.pdf

Questions

Programming can be fun, so can cryptography; however they should not be combined.

--Kreitzberg and Shneiderman

The Pause That Refreshes