Key Management Solutions

Greg Boyd
boydg@ibm.com
Security Consultant

Agenda – Key Management

- Key Variety
- Key Labels
- Master Keys
- Operational Keys
  - Key Management Tools/Utilities
  - Key Management Products

Many keys

- Master Keys are different than Operational Keys
- Operational Keys
  - Algorithms
    - Symmetric
    - Asymmetric
    - ~~Certificates~~
  - Key Types
    - Symmetric (DATA, CIPHER, ATM PIN, EXPORTER/IMPORTER, etc.)
    - Public keys
    - Public & Private keys

Keystore Labels

- Manage keys both and in terms of
  - Security
  - Lifecycle
- Examples
  - <Environment>.subsystem.application.component.D<yyyymmdd>
  - AES256.<Location>.<Env>.<FileType>.<Appl>.<DateIssued>.<Version>
  - <Environment>.C<Client_ID><Iteration>.Y<YearCreation>.<Sequence#>
  - <Pervasive Encryption>.<Environment>.<CompanyPlatform>.<Version>
- Bad Examples
  - THISISAREALLYLONGKEYLABEL
  - MYKEY
  - X

Loading Master Keys

- Passphrase Initialization (PPINIT)
- ICSF Panels
- Trusted Key Entry Workstation

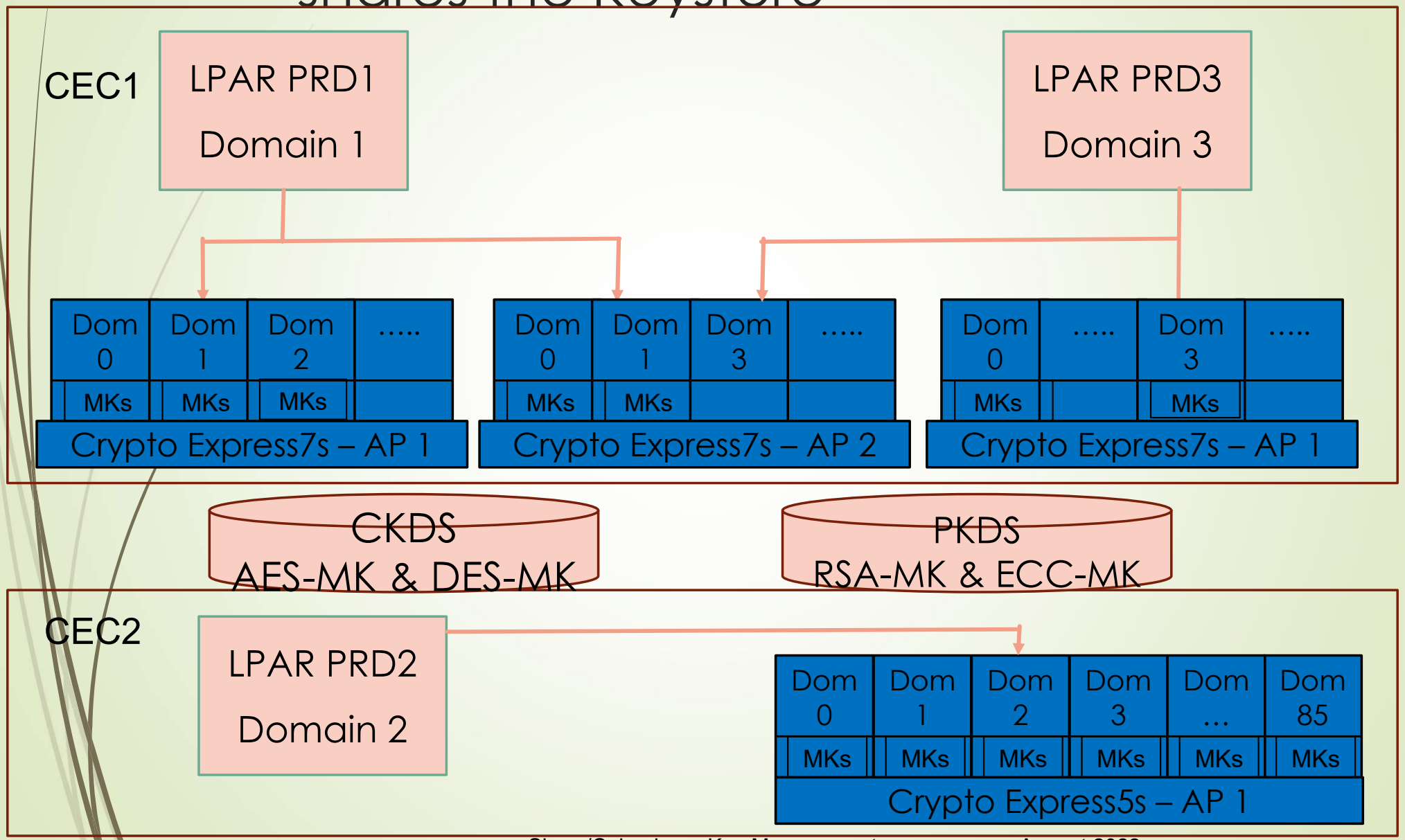
ICSF Panels – Checksum Calculation

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

Enter data below:
Key Type  ==> AES-MK            (Selection panel displayed if blank)
Key Value ==> 02AC7633C1951F0A Input key value 1
          ==> 5916A7A3DF8718DB Input key value 2
          ==> 7E1EEB82B27969CA Input key value 3 (AES-MK, DES24-MK,
                                                  ECC-MK, RSA-MK Only)
          ==> A7D6ECF77E91DAAC Input key value 4 (AES-MK, ECC-MK only)

  Checksum    : BF                 Check digit for key value
  Key Part VP : 1D6924E3F9F69A7A   Verification
  Key Part HP : 0000000000000000   Hash pattern
              : 0000000000000000



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

Loading Key Parts

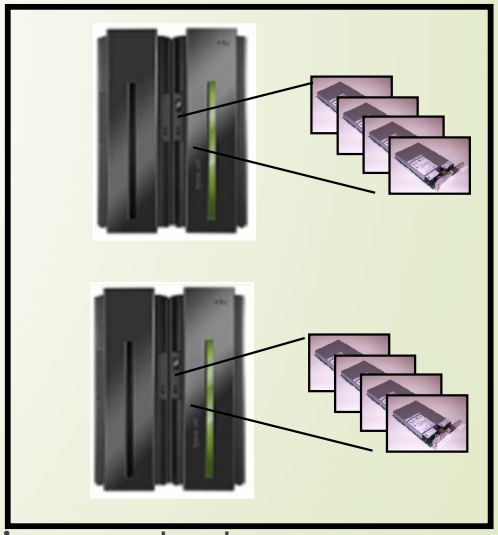
```
CSFDKE50 ---------- ICSF - Master Key Entry   --------------------
COMMAND  ===>
        AES new master key register           :    EMPTY
        DES new master key register           :    EMPTY
        ECC new master key register           :    EMPTY
        RSA new master key register           :    EMPTY

 Specify information below
 Key Type    ===>  AES-MK              (AES-MK, DES-MK, ECC-MK, RSA-MK)
 Part        ===>  FIRST               (RESET, FIRST, MIDDLE, FINAL)
 Checksum    ===>  BF
 Key Value   ===>  02AC7633C1951F0A
             ===>  5916A7A3DF8718DB
             ===>  7E1EEB82B27969CA   (AES-MK, ECC-MK, and RSA-MK only)
             ===>  A7D6ECF77E91DAAC   (AES-MK, ECC-MK only)




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

And repeat … for every system that shares the Keystore

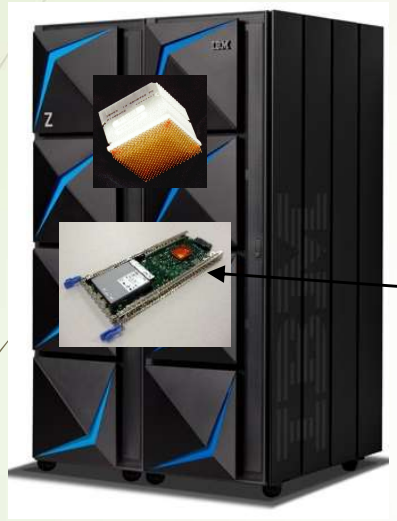


TKE – What does it do?

- Secure Key Loading
  - Master keys or operational keys
  - Key material generated in hardware and never exists in the clear, outside of the tamper-responding hardware
- Two-man (or 4-eyes) rule
  - Issuers & Co-signers
  - Multiple key officers
- Manage host crypto modules
  - As domain groups
  - Across CECs
  - Migration Wizard
  - Wizard like feature for loading master keys in one task



Secure Host Connection



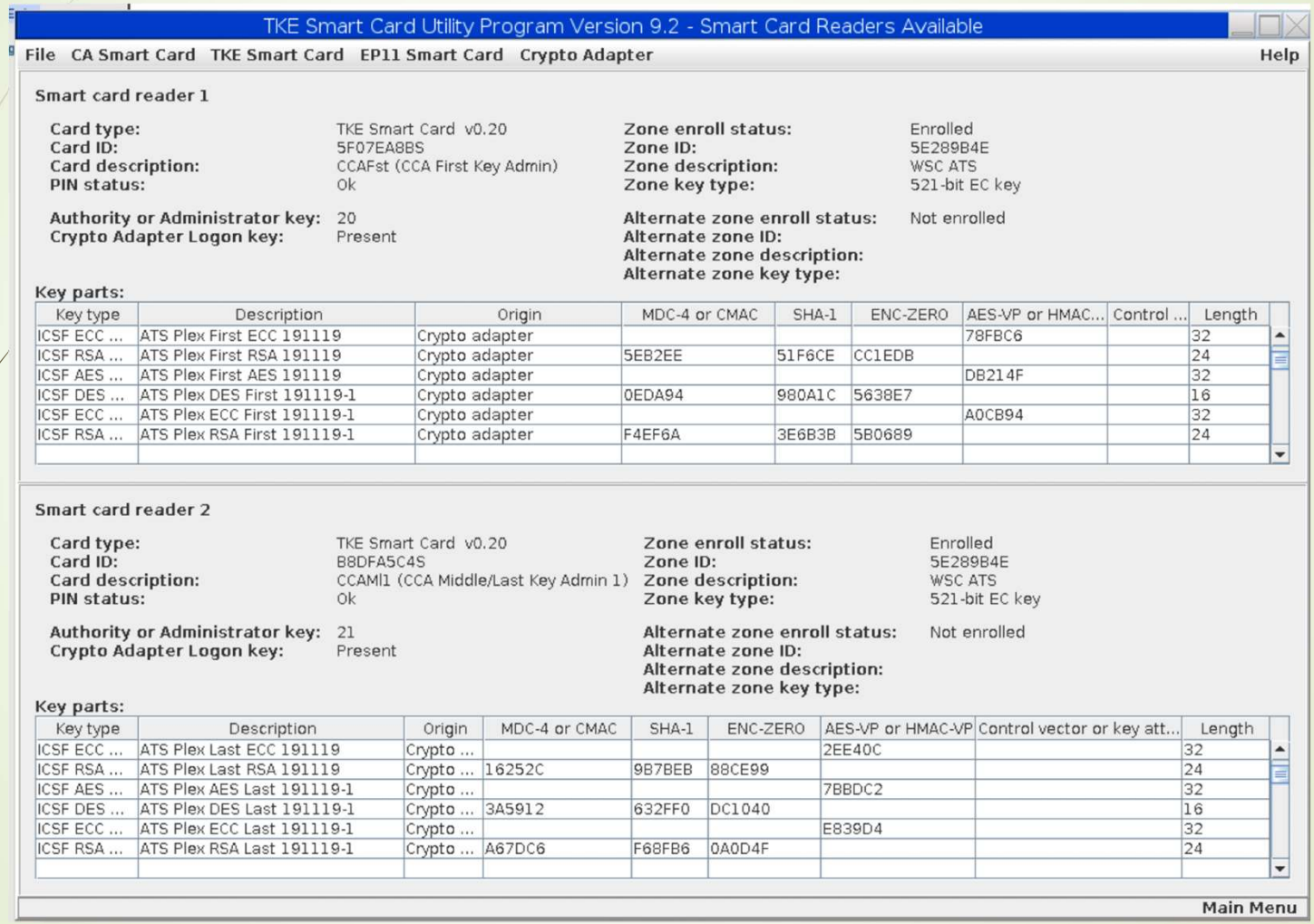
AT/TLS w/TKE 9.2

Cmd[e_{DHK}(key part value)]signed^{An}

z15 w/Crypto Express Card(s)

Trusted Key Entry Workstation

Descriptions (Labels)



TKE Smart Card Utility Program Version 9.2 - Smart Card Readers Available

File CA Smart Card TKE Smart Card EP11 Smart Card Crypto Adapter Help

Smart card reader 1

Card type: TKE Smart Card v0.20
Card ID: 5F07EA8BS
Card description: CCAFst (CCA First Key Admin)
PIN status: Ok

Authority or Administrator key: 20
Crypto Adapter Logon key: Present

Zone enroll status: Enrolled
Zone ID: 5E289B4E
Zone description: WSC ATS
Zone key type: 521-bit EC key

Alternate zone enroll status: Not enrolled
Alternate zone ID:
Alternate zone description:
Alternate zone key type:

Key parts:

Key type	Description	Origin	MDC-4 or CMAC	SHA-1	ENC-ZERO	AES-VP or HMAC...	Control ...	Length
ICSF ECC ...	ATS Plex First ECC 191119	Crypto adapter				78FBC6		32
ICSF RSA ...	ATS Plex First RSA 191119	Crypto adapter	5EB2EE	51F6CE	CC1EDB			24
ICSF AES ...	ATS Plex First AES 191119	Crypto adapter				DB214F		32
ICSF DES ...	ATS Plex DES First 191119-1	Crypto adapter	0EDA94	980A1C	5638E7			16
ICSF ECC ...	ATS Plex ECC First 191119-1	Crypto adapter				A0CB94		32
ICSF RSA ...	ATS Plex RSA First 191119-1	Crypto adapter	F4EF6A	3E6B3B	5B0689			24

Smart card reader 2

Card type: TKE Smart Card v0.20
Card ID: B8DFA5C4S
Card description: CCAMl1 (CCA Middle/Last Key Admin 1)
PIN status: Ok

Authority or Administrator key: 21
Crypto Adapter Logon key: Present

Zone enroll status: Enrolled
Zone ID: 5E289B4E
Zone description: WSC ATS
Zone key type: 521-bit EC key

Alternate zone enroll status: Not enrolled
Alternate zone ID:
Alternate zone description:
Alternate zone key type:

Key parts:

Key type	Description	Origin	MDC-4 or CMAC	SHA-1	ENC-ZERO	AES-VP or HMAC-VP	Control vector or key att...	Length
ICSF ECC ...	ATS Plex Last ECC 191119	Crypto ...				2EE40C		32
ICSF RSA ...	ATS Plex Last RSA 191119	Crypto ...	16252C	9B7BEB	88CE99			24
ICSF AES ...	ATS Plex AES Last 191119-1	Crypto ...				7BBDC2		32
ICSF DES ...	ATS Plex DES Last 191119-1	Crypto ...	3A5912	632FF0	DC1040			16
ICSF ECC ...	ATS Plex ECC Last 191119-1	Crypto ...				E839D4		32
ICSF RSA ...	ATS Plex RSA Last 191119-1	Crypto ...	A67DC6	F68FB6	0A0D4F			24

Main Menu

Control Domains/Domain Groups

CEC2 Dom	AES-MK	DES-MK	RSA-MK	ECC-MK
UD1				
UD11				
UD23				
….				
UD85				

CEC1 Dom	AES-MK	DES-MK	RSA-MK	ECC-MK
UD1				
UD2				
UD7				
UD8				
UD9				
….				
UD85				

TKE Host Transaction Program (aka TKE Listener)

ICSF

z/OS / LPAR 1

Control Domain 1, 11, 23

TKE Host Transaction Program (aka TKE Listener)

ICSF

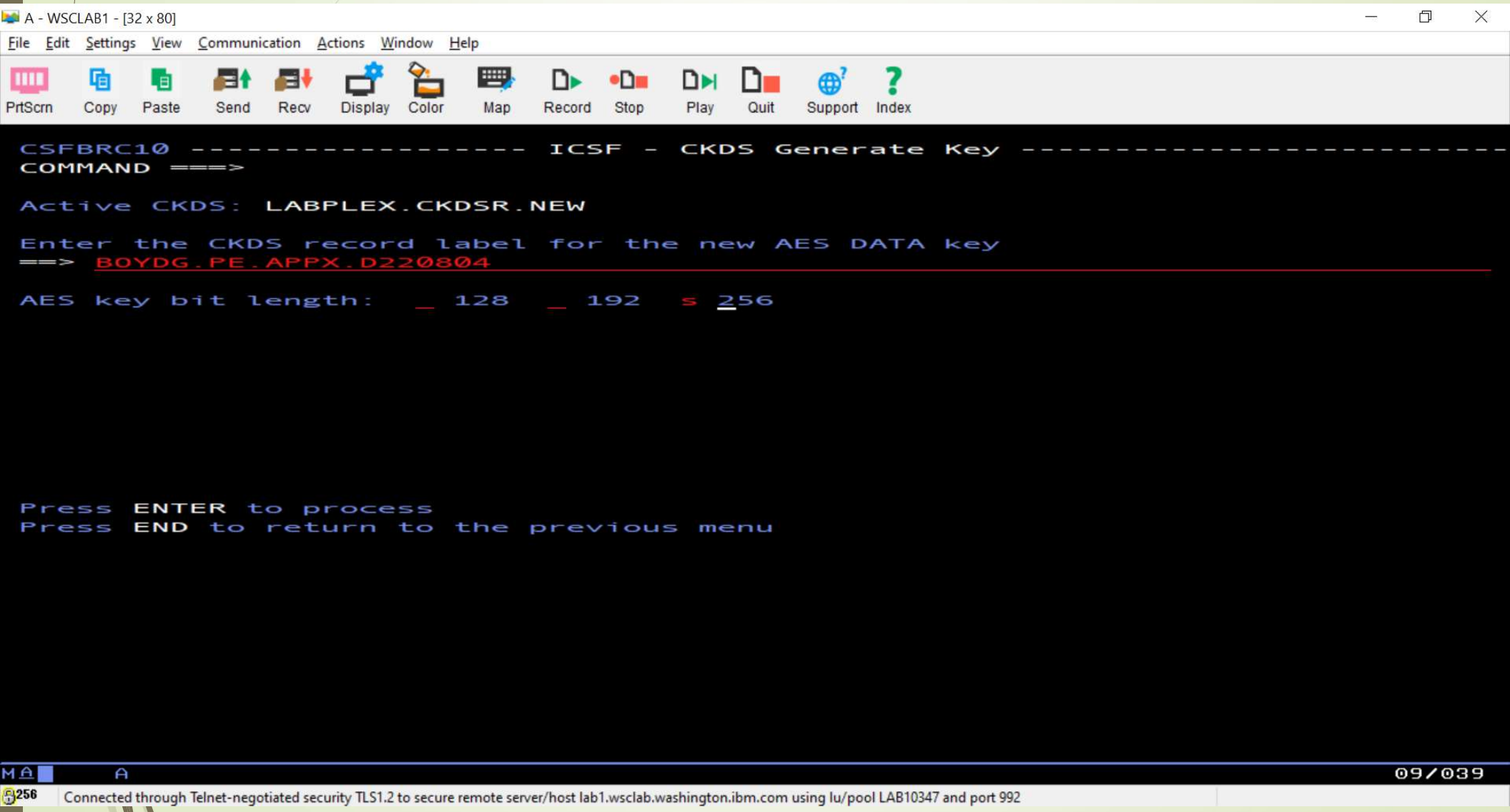
z/OS / LPAR 7

Control Domain 1-85

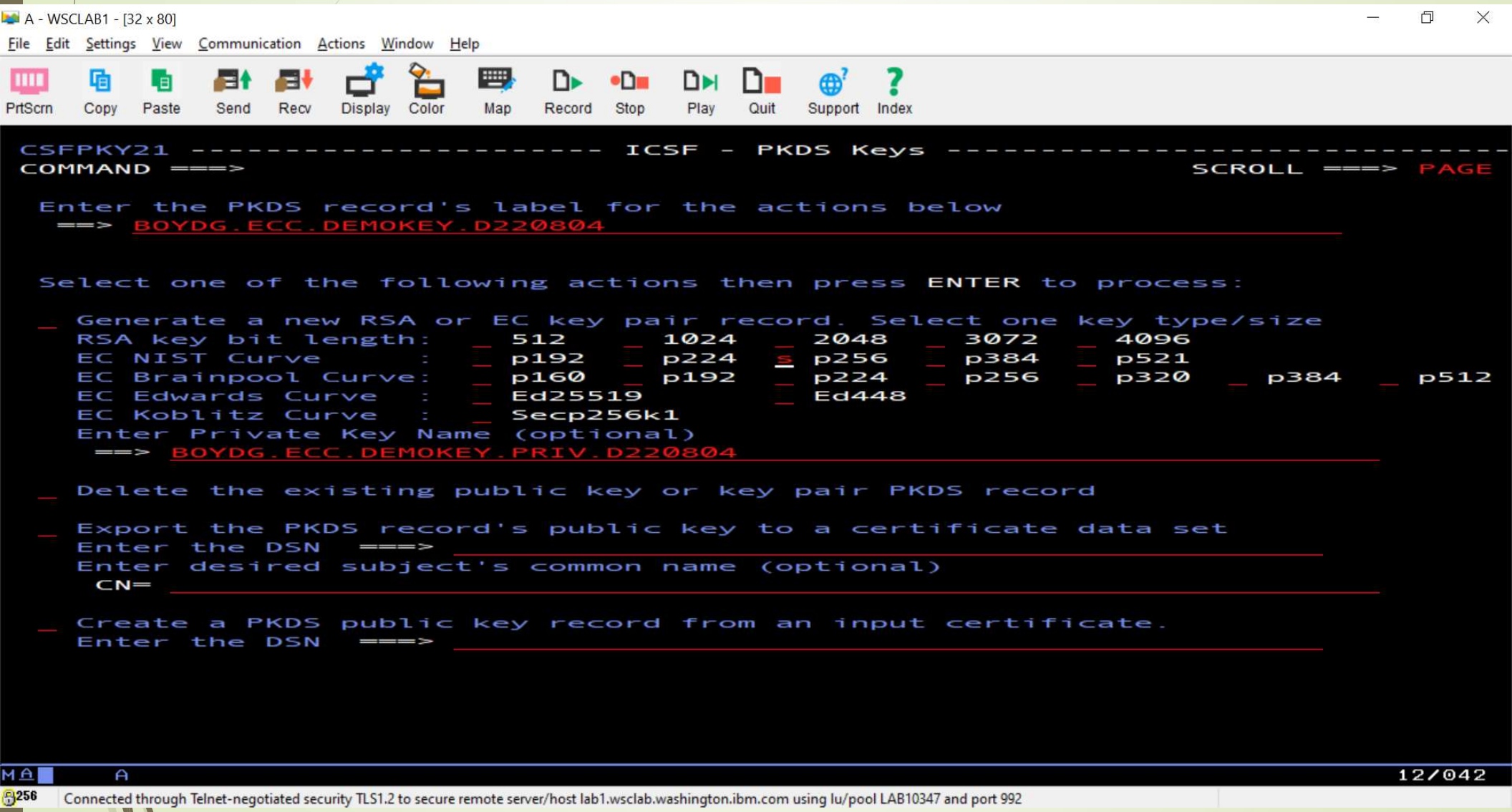
Operational Key Management Utilities

- CKDS Keys Utility / PKDS Keys Utility
- Key Generation Utility Program
- APIs (REXX/COBOL/etc.)
- Trusted Key Entry (TKE) Workstation

CKDS Keys Utility



PKDS Keys Utility



KGUP Add a Key

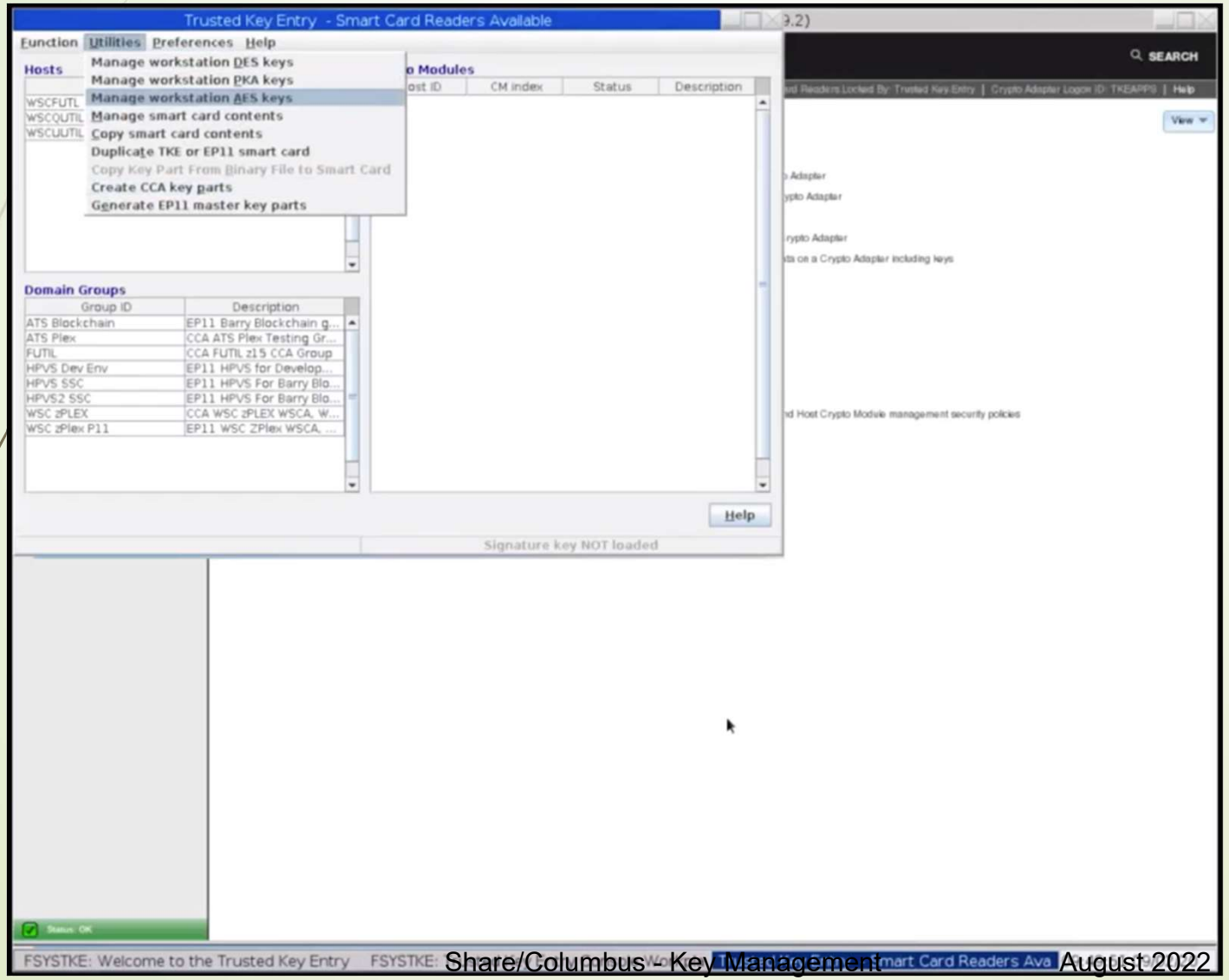
```
CSFCSE10 ----- ICSF - Create ADD, UPDATE, or DELETE Key Statement ------------
COMMAND ===>
Specify control statement information below

   Function  ===> ADD___     ADD, UPDATE, or DELETE
   Algorithm ===> AES        DES or AES
   Key Type  ===> CLRAES__    Outtype ===> ________    (Optional)
   Label ===> BOYDG.AES256.AA.D220103_____________________________________________
    Group Labels  ===> NO_   NO or YES
 or Range:
   Start ===> ____________________________________________________________________
   End   ===> ____________________________________________________________________

    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     ===>
     C9EB3A8B63F8B180 , F345801E9585061C , 26AEF2B3187DA3AE , 3DA06CF98AABD557
   Comment Line   ===> ____________________________________________________________

Press ENTER to create and store control statement
Press END   to exit to the previous panel without saving
```

Key Management: ICSF API

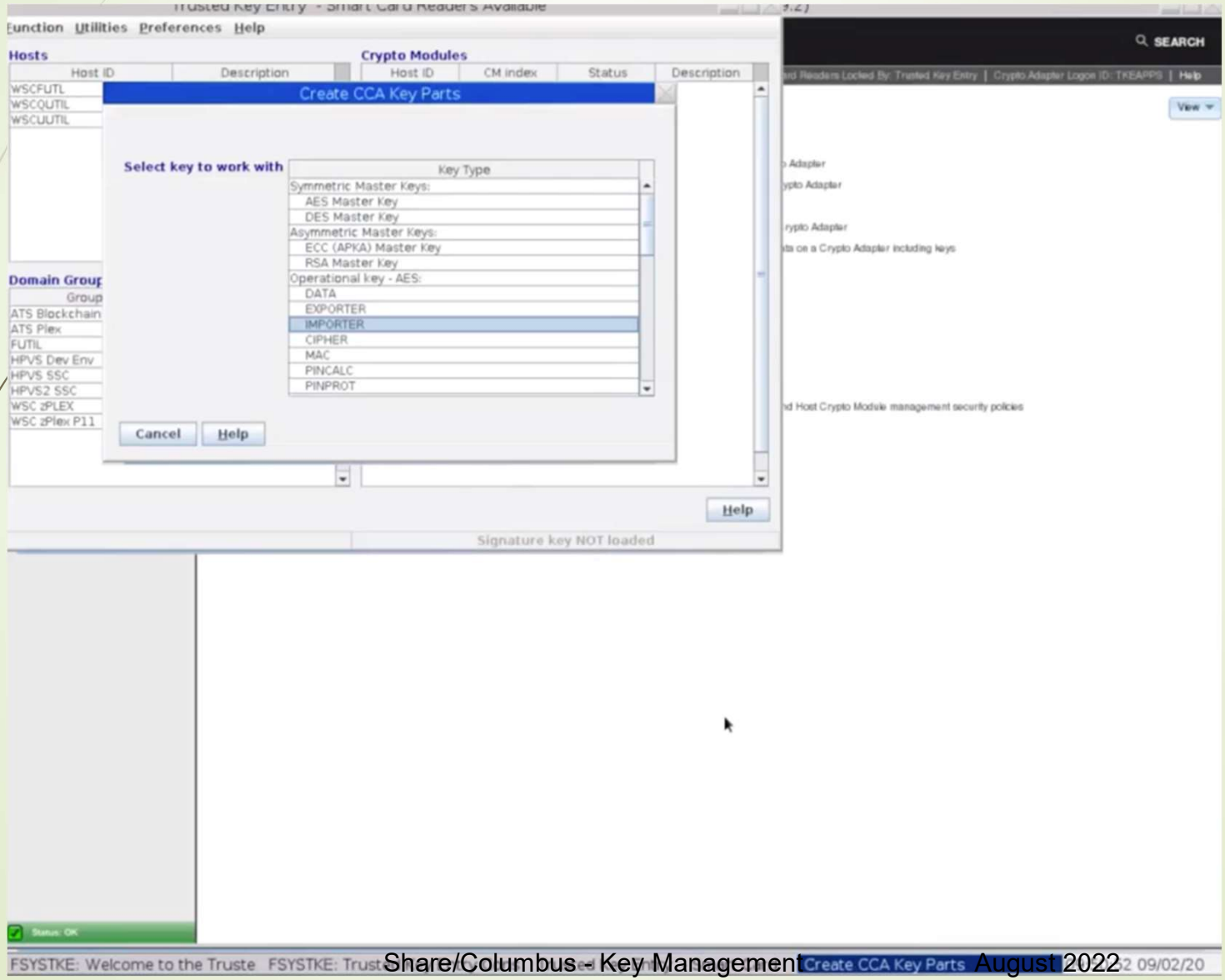
```
/*-------------------------------------------------------------------*/
/* Generate a secure AES DATA key, store the key in the CKDS and     */
/* display the key label and key. If the key label already exists,   */
/* return the existing key label and key.                            */
/*-------------------------------------------------------------------*/
/* Instructions:                                                     */
/* - Update aes_key_label with your desired key label name           */
/*                                                                   */
/*      Note: An example key label naming scheme is                  */
/*             DATASET.<dataset_resource>.ENCRKEY.<seqno>            */
/*                                                                   */
/* - EXECUTE THIS CLIST FROM TSO                                     */
/*   (E.G. EX 'HLQ.MLD.LLQ(GENKEY)')                                 */
/*-------------------------------------------------------------------*/
                          signal on novalue;
                          aes_key_label = ,
                     left('SYSPROG.DATASET.KEYS',64);
/*-------------------------------------------------------------------*/
/* Check if the key exists in the CKDS (to prevent overwriting)      */
/*-------------------------------------------------------------------*/
                       krr_label = aes_key_label;
                     krr_token = copies('00'x,64);
 Call CSNBKRR;                    /* If key is found, print and exit */
                           say 'new key...'
/*-------------------------------------------------------------------*/
/* Generate a 256-bit AES DATA key                                   */
/*-------------------------------------------------------------------*/
                    kgn_key_form           = 'OP  ';
                  kgn_key_length         = 'KEYLN16 ';
                  kgn_key_type_1         = 'CIPHER  ';
                  kgn_key_type_2         = 'CIPHER  ';
               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;
/*-------------------------------------------------------------------*/
/* Store the key in the CKDS                                         */
/*-------------------------------------------------------------------*/
                       krc2_label = aes_key_label;
```

- IBM Community
  - Pervasive (DS) Encryption sample: Generate a secure AES CIPHER key
  - Rexx Sample: Change the key validity start and end dates for a key record in the CKDS
- SG24-8410 Getting Started with z/OS Data Set Encryption Redbook
  - Example B-1 CIPHER key creation sample
  - Example B-2 DATA key creation sample

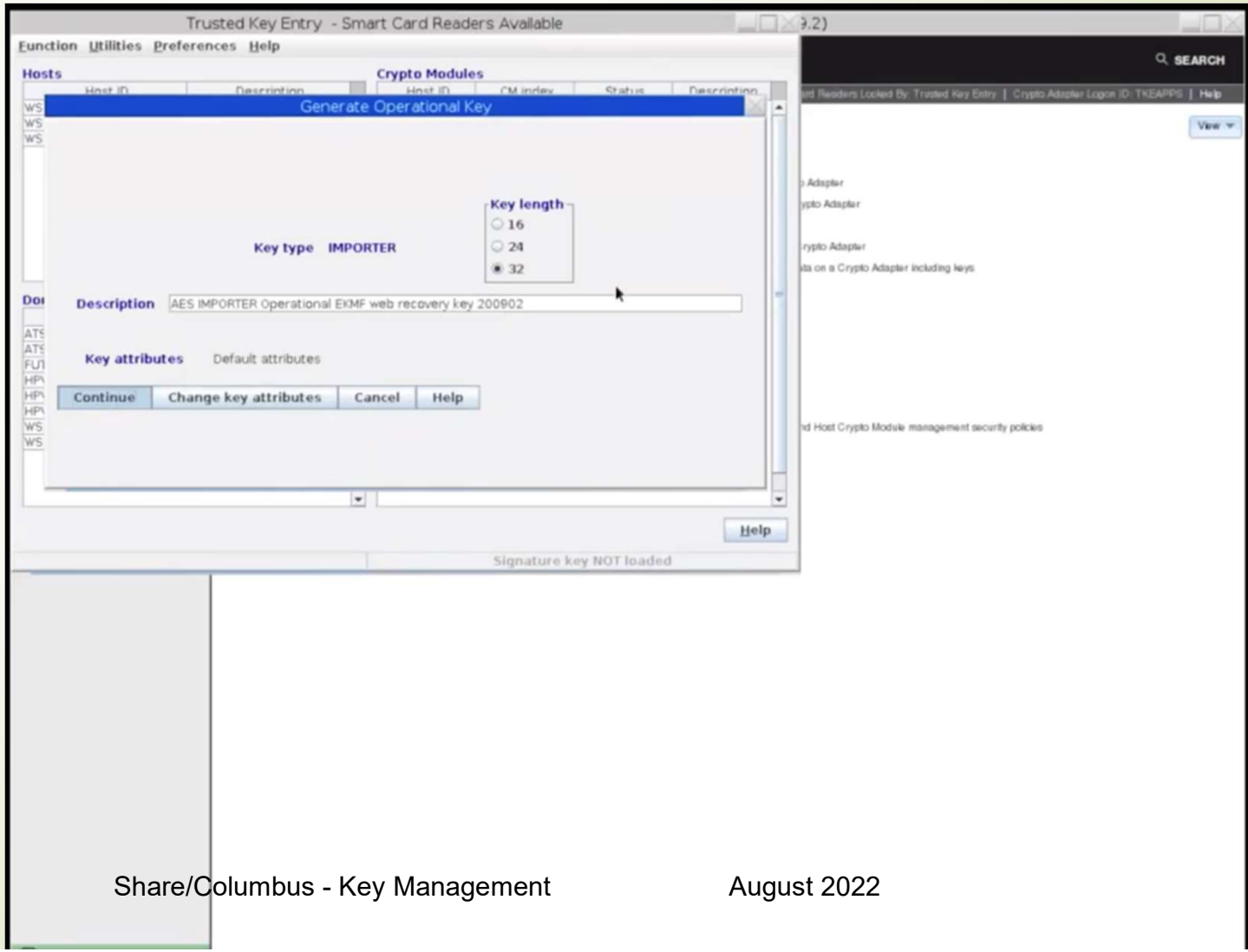
TKE Operational Keys



TKE Operational Key Type



Description and Length

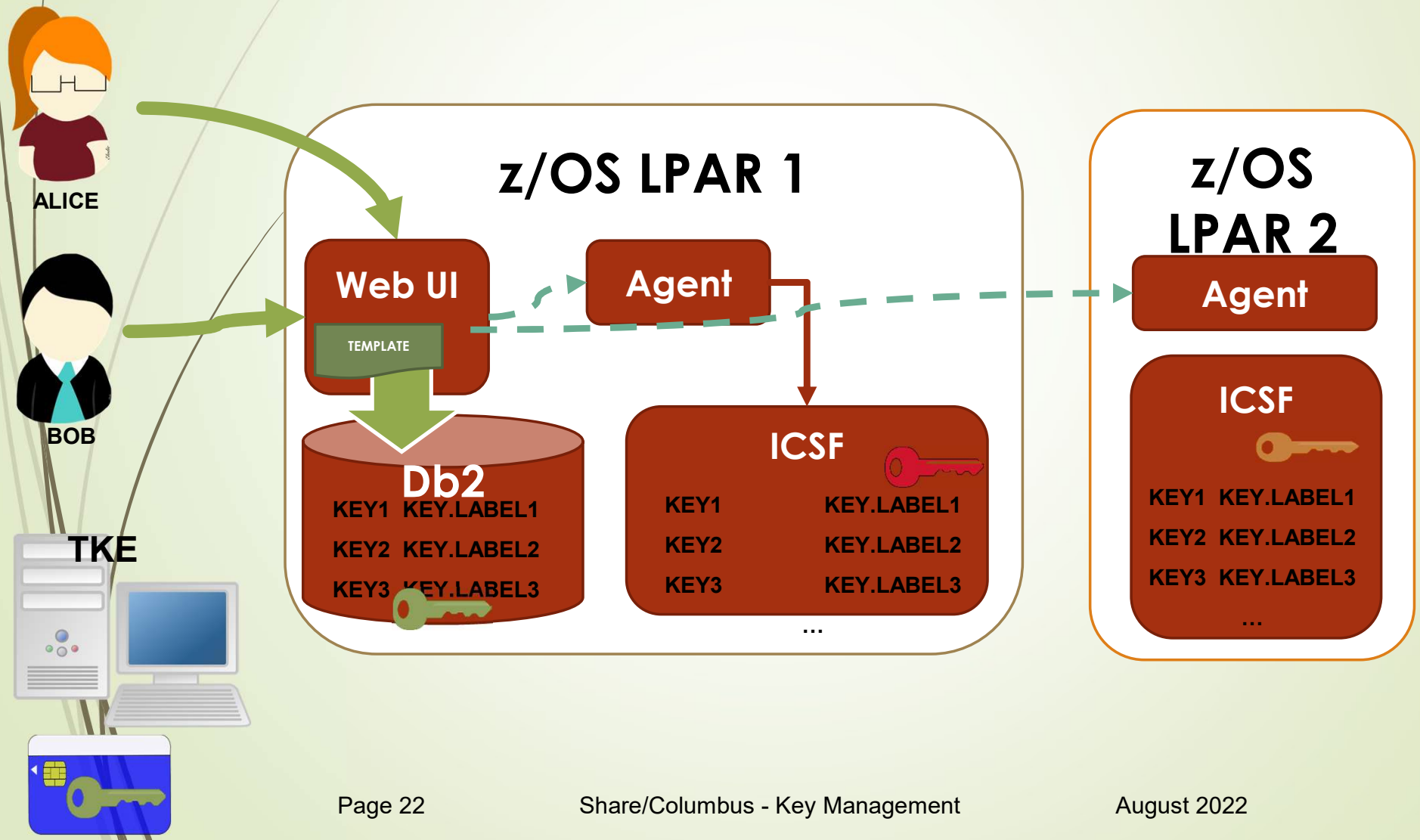


Key Management Products

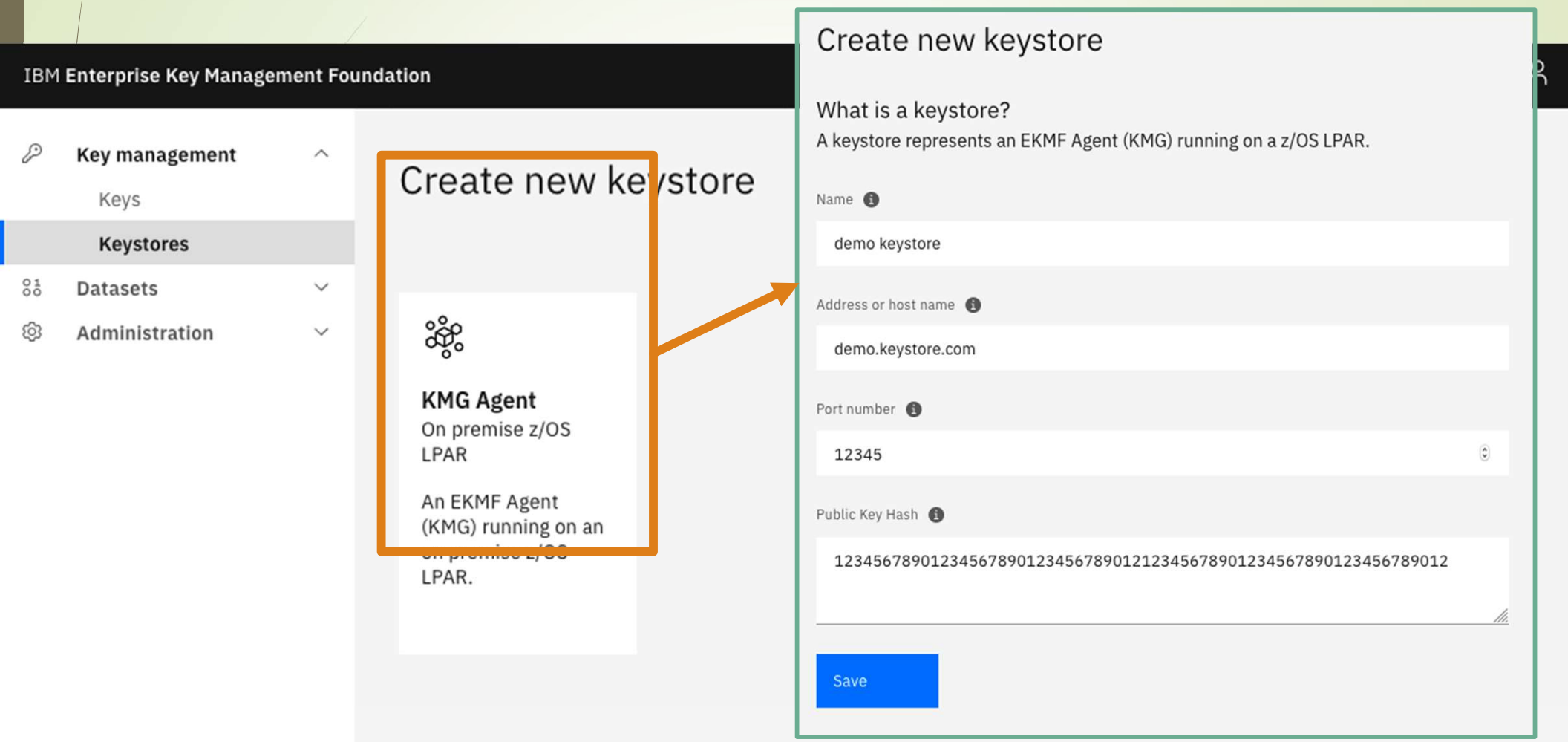
- EKMF Workstation
  - Service Offering
  - EKMF Appliance (similar, but not identical to the TKE)
- EKMF Web
  - Program Product
  - Uses the CEX cards on the host
  - Recommended to have a TKE
  - Only supports keys for Data Set Encryption
- ~~GKLM / ISKLM~~
- ~~Unified Key Orchestrator~~

Enterprise Key Management Foundation – EKMF Web Edition

- For z/OS Dataset Encryption only…
- No workstation (server) required. WAS Liberty profile-based UI.



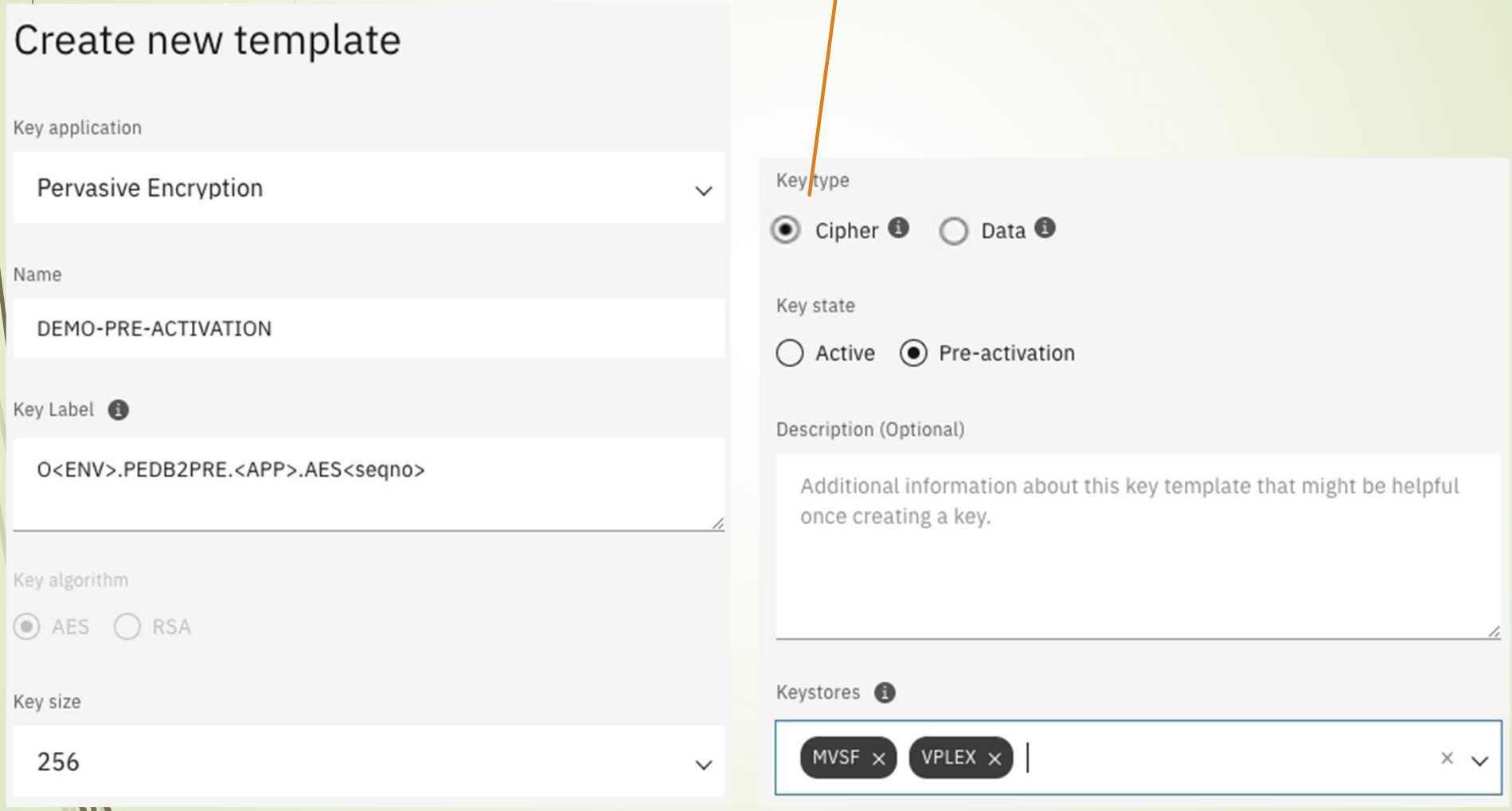
Create Keystore



New Template

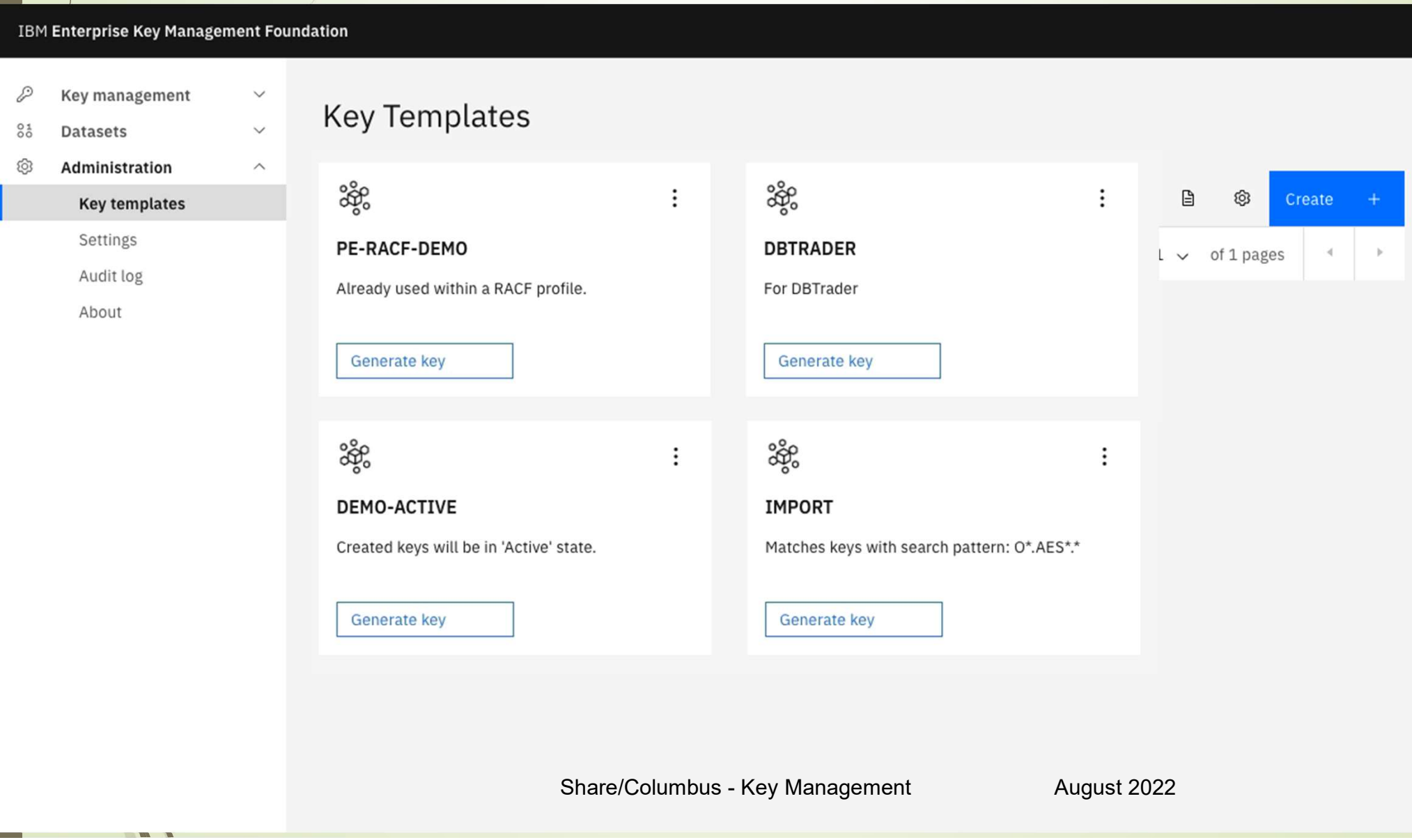
IBM z13 can only generate data keys.

We recommend to use AES cipher keys, available from z14 with CEX6 or later.

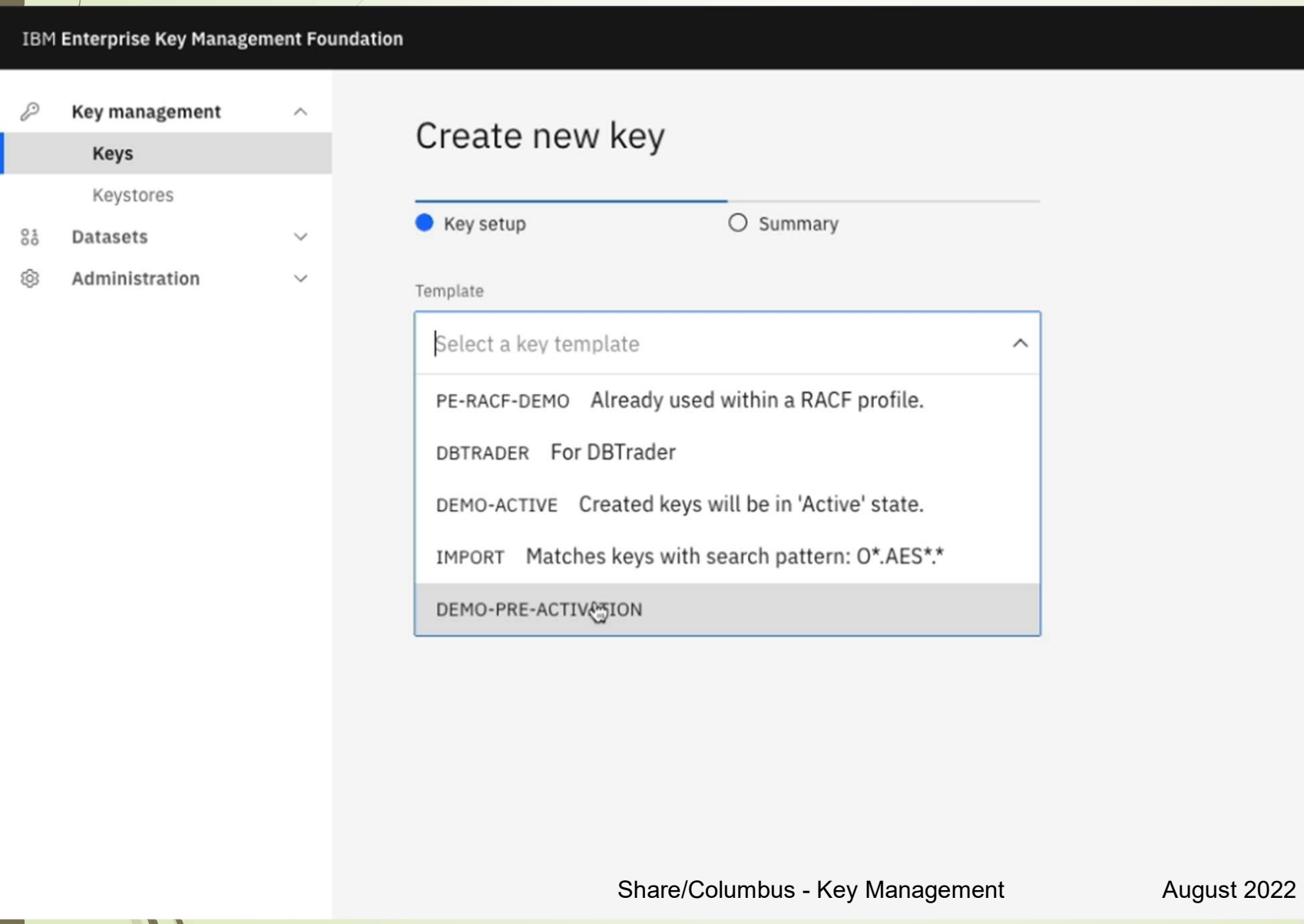


Key Templates

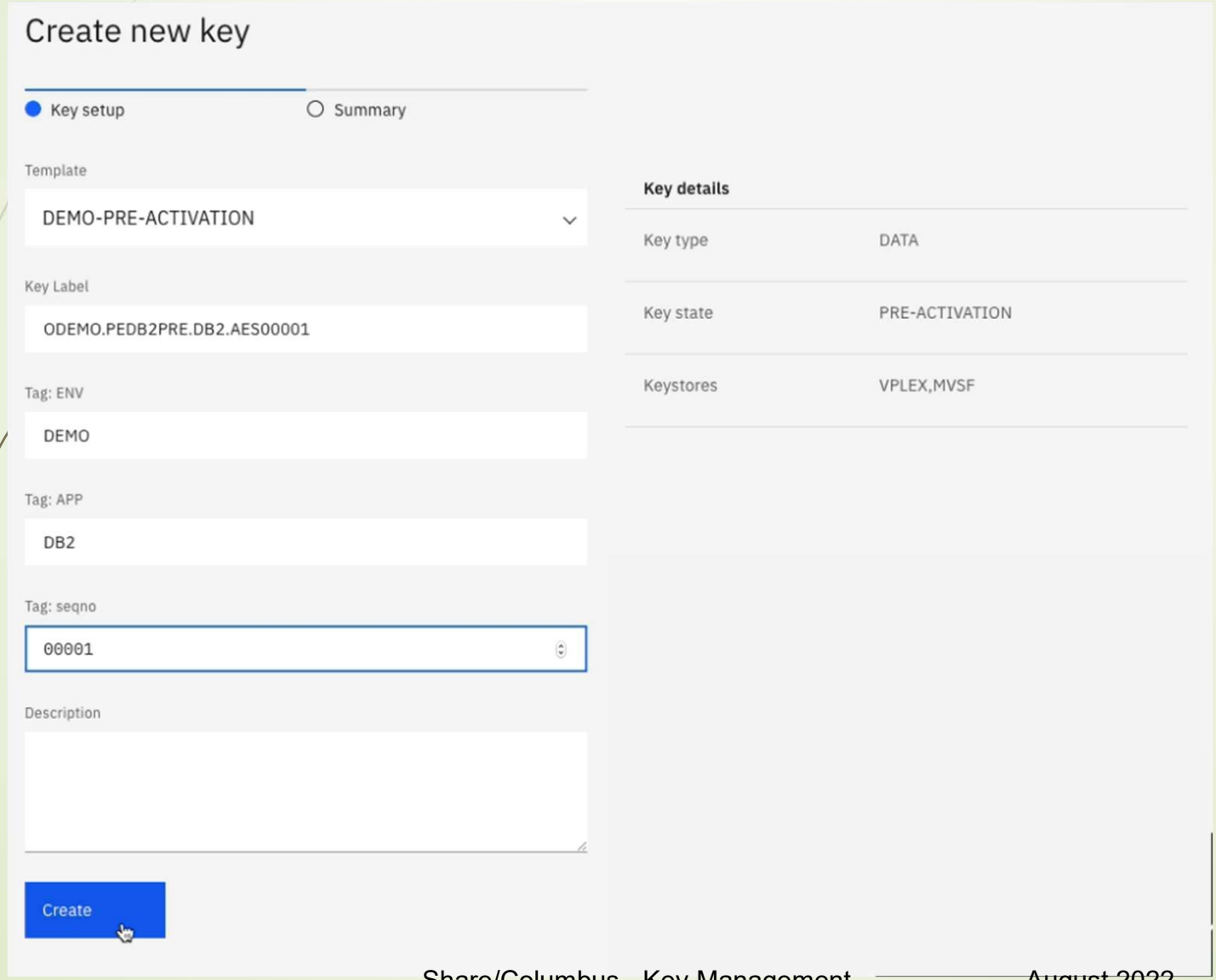
These are the policies that define how your keys are created



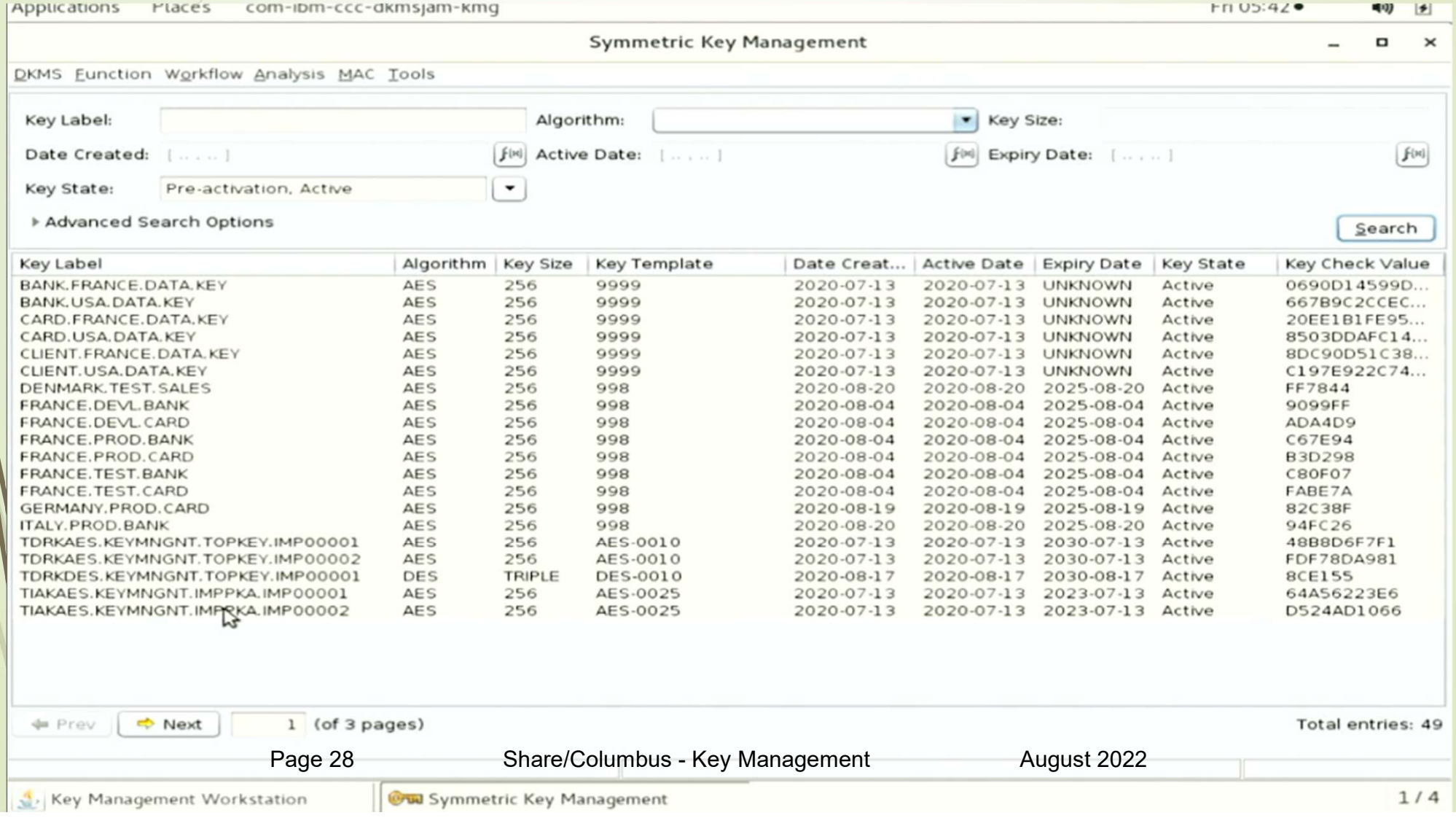
Create new key



Create the key



EKMF - Keys


Applications Places com-ibm-ccc-dkmsjam-kmg
Fri 05:42
Symmetric Key Management
DKMS Function Workflow Analysis MAC Tools
Key Label:
Algorithm:
Key Size:
Date Created:
Active Date:
Expiry Date:
Key State: Pre-activation, Active
Advanced Search Options
Search
Key Label | Algorithm | Key Size | Key Template | Date Creat... | Active Date | Expiry Date | Key State | Key Check Value
BANK.FRANCE.DATA.KEY | AES | 256 | 9999 | 2020-07-13 | 2020-07-13 | UNKNOWN | Active | 0690D14599D...
BANK.USA.DATA.KEY | AES | 256 | 9999 | 2020-07-13 | 2020-07-13 | UNKNOWN | Active | 667B9C2CCEC...
CARD.FRANCE.DATA.KEY | AES | 256 | 9999 | 2020-07-13 | 2020-07-13 | UNKNOWN | Active | 20EE1B1FE95...
CARD.USA.DATA.KEY | AES | 256 | 9999 | 2020-07-13 | 2020-07-13 | UNKNOWN | Active | 8503DDAFC14...
CLIENT.FRANCE.DATA.KEY | AES | 256 | 9999 | 2020-07-13 | 2020-07-13 | UNKNOWN | Active | 8DC90D51C38...
CLIENT.USA.DATA.KEY | AES | 256 | 9999 | 2020-07-13 | 2020-07-13 | UNKNOWN | Active | C197E922C74...
DENMARK.TEST.SALES | AES | 256 | 998 | 2020-08-20 | 2020-08-20 | 2025-08-20 | Active | FF7844
FRANCE.DEVL.BANK | AES | 256 | 998 | 2020-08-04 | 2020-08-04 | 2025-08-04 | Active | 9099FF
FRANCE.DEVL.CARD | AES | 256 | 998 | 2020-08-04 | 2020-08-04 | 2025-08-04 | Active | ADA4D9
FRANCE.PROD.BANK | AES | 256 | 998 | 2020-08-04 | 2020-08-04 | 2025-08-04 | Active | C67E94
FRANCE.PROD.CARD | AES | 256 | 998 | 2020-08-04 | 2020-08-04 | 2025-08-04 | Active | B3D298
FRANCE.TEST.BANK | AES | 256 | 998 | 2020-08-04 | 2020-08-04 | 2025-08-04 | Active | C80F07
FRANCE.TEST.CARD | AES | 256 | 998 | 2020-08-04 | 2020-08-04 | 2025-08-04 | Active | FABE7A
GERMANY.PROD.CARD | AES | 256 | 998 | 2020-08-19 | 2020-08-19 | 2025-08-19 | Active | 82C38F
ITALY.PROD.BANK | AES | 256 | 998 | 2020-08-20 | 2020-08-20 | 2025-08-20 | Active | 94FC26
TDRKAES.KEYMNGNT.TOPKEY.IMP00001 | AES | 256 | AES-0010 | 2020-07-13 | 2020-07-13 | 2030-07-13 | Active | 48B8D6F7F1
TDRKAES.KEYMNGNT.TOPKEY.IMP00002 | AES | 256 | AES-0010 | 2020-07-13 | 2020-07-13 | 2030-07-13 | Active | FDF78DA981
TDRKDES.KEYMNGNT.TOPKEY.IMP00001 | DES | TRIPLE | DES-0010 | 2020-08-17 | 2020-08-17 | 2030-08-17 | Active | 8CE155
TIAKAES.KEYMNGNT.IMPPKA.IMP00001 | AES | 256 | AES-0025 | 2020-07-13 | 2020-07-13 | 2023-07-13 | Active | 64A56223E6
TIAKAES.KEYMNGNT.IMPPKA.IMP00002 | AES | 256 | AES-0025 | 2020-07-13 | 2020-07-13 | 2023-07-13 | Active | D524AD1066
Prev
Next
1 (of 3 pages)
Total entries: 49
Key Management Workstation
Symmetric Key Management
1 / 4

Summary

- Key Management is Important
- Key Labeling Conventions and Policies are necessary
- Key Management Tooling is probably in your future

References

- ICSF Administration Guide
- ICSF Application Programmer's Guide
- SG24-8410 Getting Started with z/OS Data Set Encryption Redbook
  - Example B-1 CIPHER key creation sample
  - Example B-2 DATA key creation sample

References – Sample Code

- IBM Community
  - Pervasive (DS) Encryption sample: Generate a secure AES CIPHER key (https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/eysha-shirrine-powers2/2020/03/25/pervasive-ds-encryption-sample-generate-a-secure-aes-cipher-key)
  - Rexx Sample: Change the key validity start and end dates for a key record in the CKDS (https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/eysha-shirrine-powers2/2020/03/25/rexx-sample-change-the-key-validity-start-and-end-dates-for-a-key-record-in-the-ckds)