MAINFRAME CRYPTO

z/OS Key Management for non-z/OS Folks

Greg Boyd (gregboyd@mainframecrypto.com)

November 2022

Copyrights and Trademarks

- Copyright © 2022 Greg Boyd, Mainframe Crypto, LLC. All rights reserved.
- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 30+ years

- All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. IBM, System z, zEnterprise and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.
- **THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY**. Greg Boyd and Mainframe Crypto, LLC assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Greg Boyd or Mainframe Crypto, LLC be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if expressly advised in advance of the possibility of such damages.

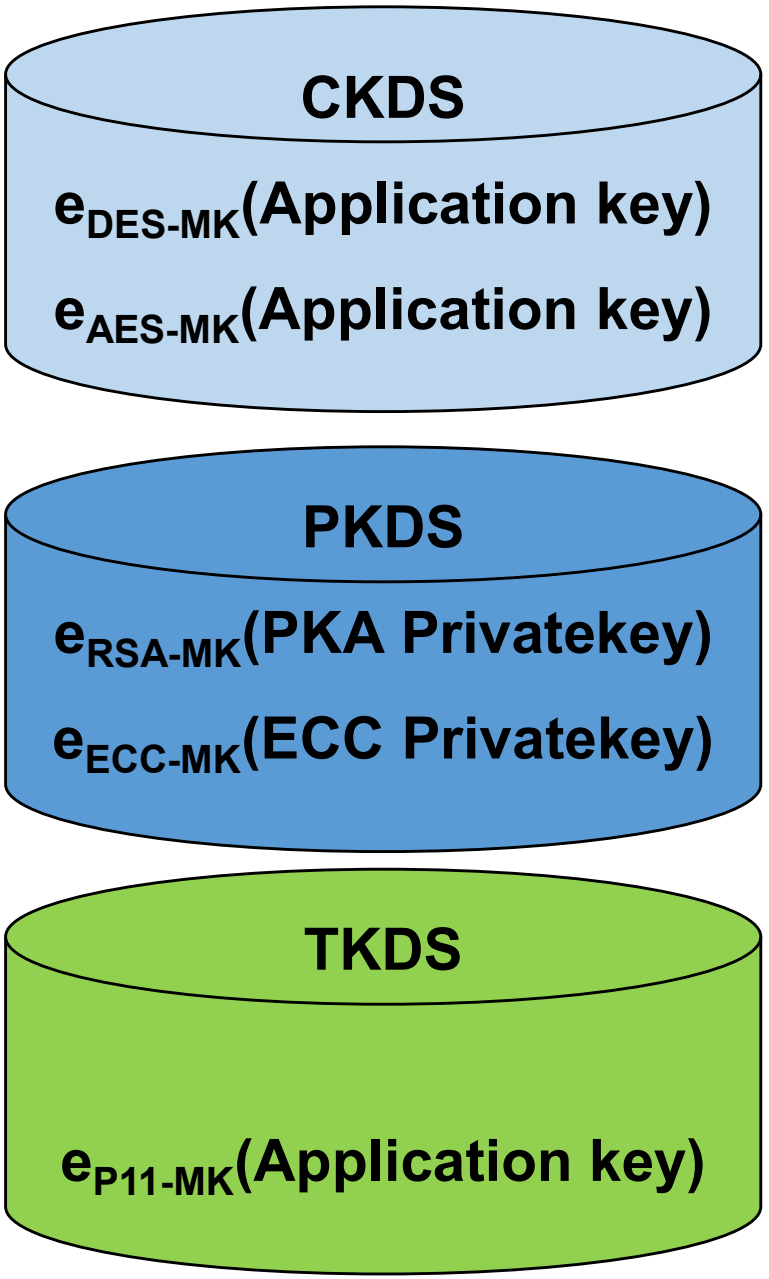
Agenda – z/OS Key Management for non-z/OS Folks

- Key Stores
- Master Keys
- Operational Keys
- Tooling

z/OS Key Repositories

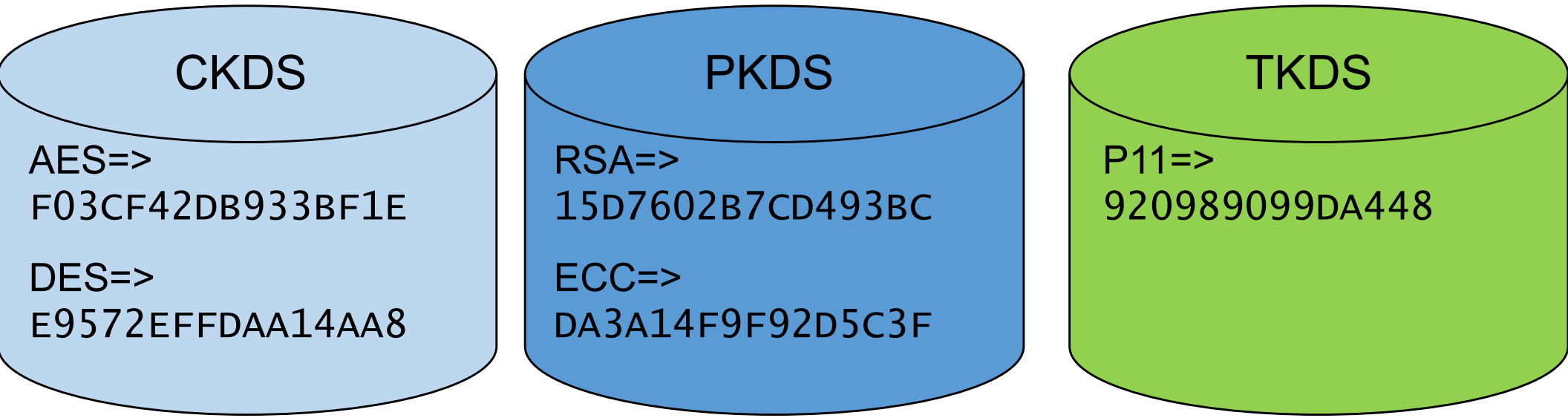
- Cryptographic Key Data Set (CKDS)
  - AES keys
  - DES/TDES keys
- PKA Key Data Set (PKDS)
  - ECC keys
  - RSA keys
  - Public and/or public/private key pairs
- Token Key Data Set (TKDS)
  - PKCS #11 objects

- Key stores are ‘System data sets’
  - Part of the operating system; backed up and managed by your Systems team as part of normal operations

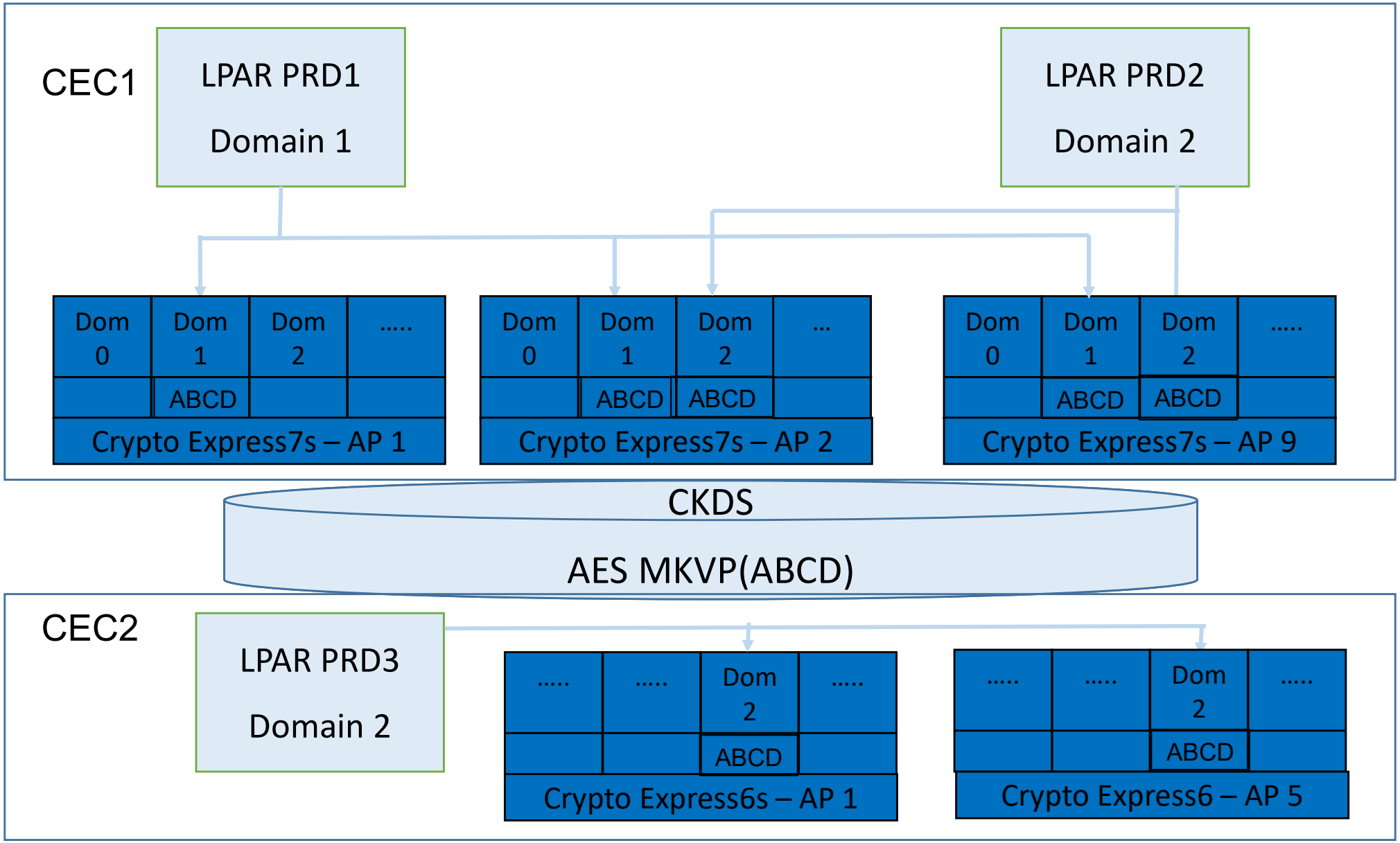


MKVP Master Key Verification Patterns

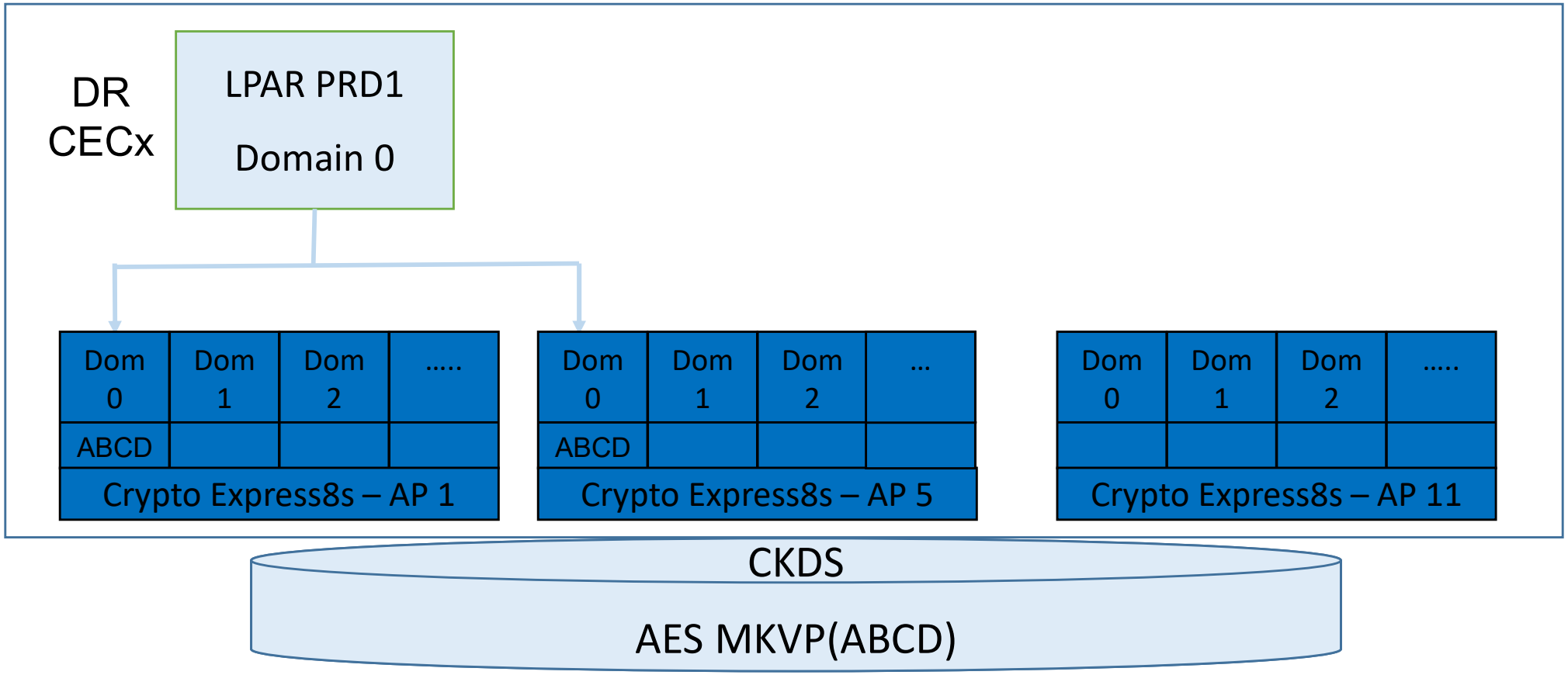
Crypto Express (CEX) Card				
UD/LPAR	**LPAR1**	**LPAR2**	**LPARx**	**LPARx**
AES	F03CF42DB933BF1E			
DES	E9572EFFDAA14AA8			
ECC	DA3A14F9F92D5C3F			
RSA	15D7602B7CD493BC			
P11		920989099DA448		



Master Keys reside in the HSM (CEX card)



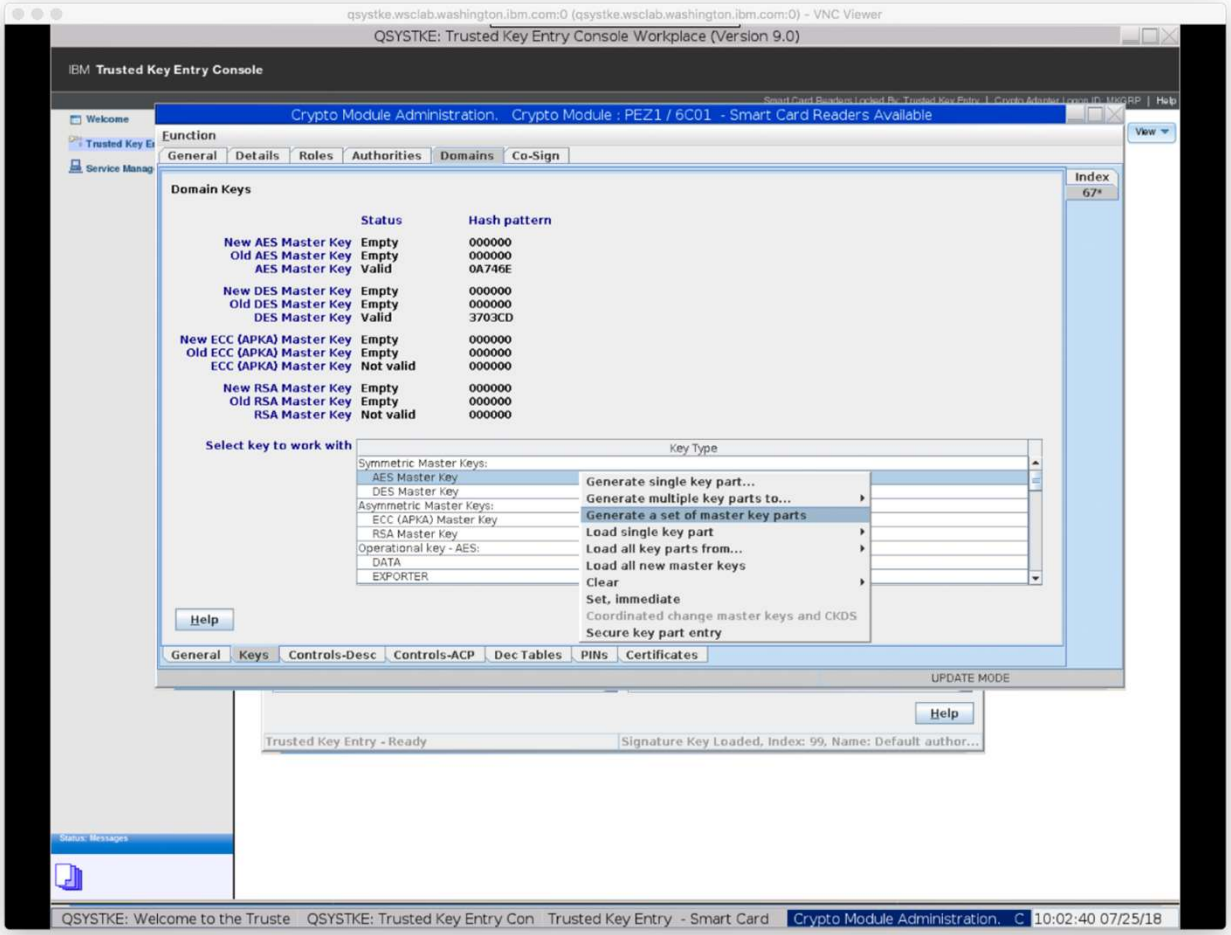
Master Keys reside in the DR HSM



Loading Master Keys

- Passphrase Initialization (aka PPINIT)
- ISPF Panels for ICSF
- From the Trusted Key Entry Workstation

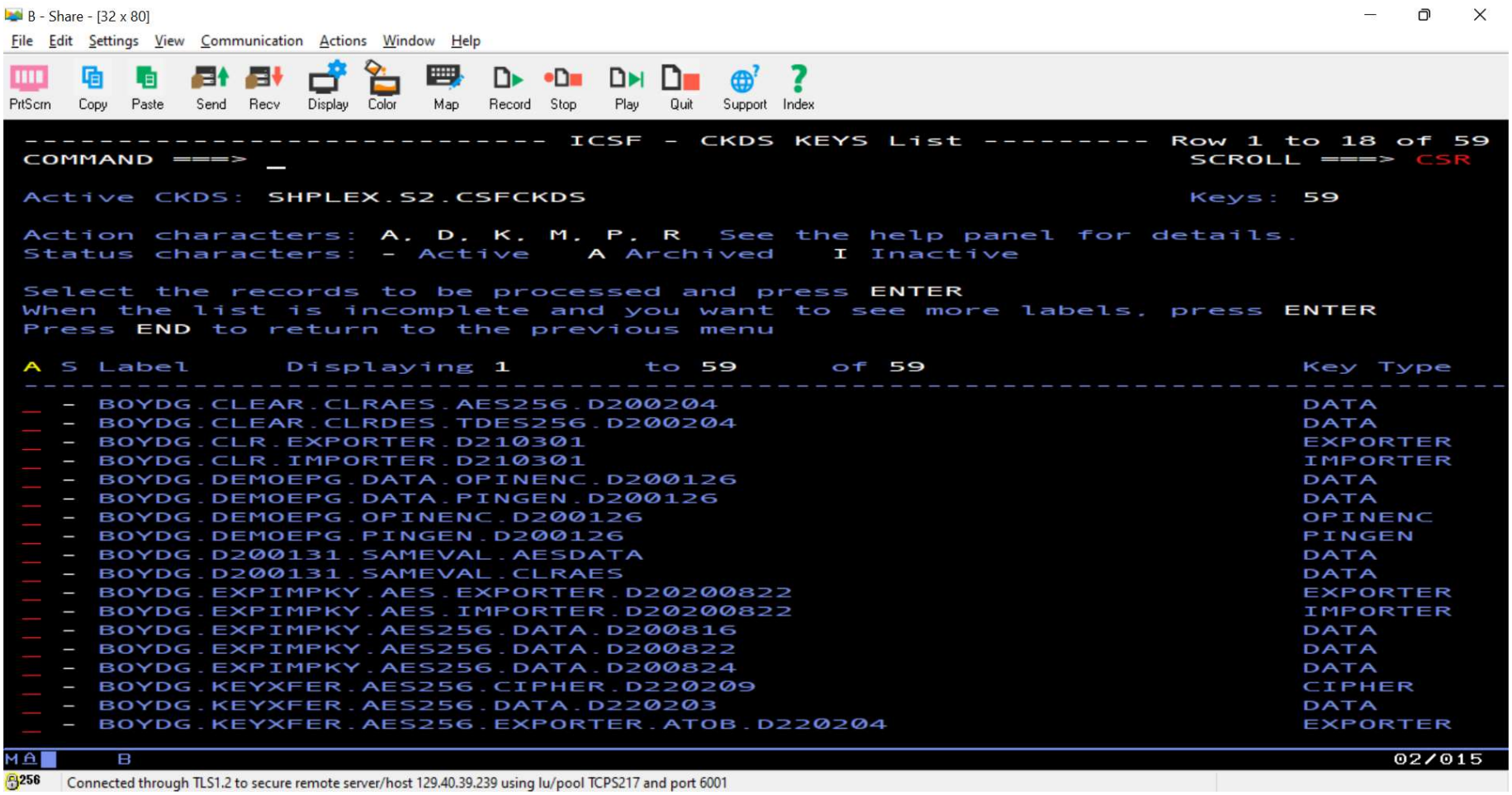
TKE Wizards


QSYSTKE: Trusted Key Entry Console Workplace (Version 9.0)
IBM Trusted Key Entry Console
Crypto Module Administration. Crypto Module : PEZ1 / 6C01 - Smart Card Readers Available
Function
General
Details
Roles
Authorities
Domains
Co-Sign
Domain Keys
Status
Hash pattern
New AES Master Key Empty 000000
Old AES Master Key Empty 000000
AES Master Key Valid 0A746E
New DES Master Key Empty 000000
Old DES Master Key Empty 000000
DES Master Key Valid 3703CD
New ECC (APKA) Master Key Empty 000000
Old ECC (APKA) Master Key Empty 000000
ECC (APKA) Master Key Not valid 000000
New RSA Master Key Empty 000000
Old RSA Master Key Empty 000000
RSA Master Key Not valid 000000
Select key to work with
Key Type
Symmetric Master Keys:
AES Master Key
DES Master Key
Asymmetric Master Keys:
ECC (APKA) Master Key
RSA Master Key
Operational key - AES:
DATA
EXPORTER
Generate single key part...
Generate multiple key parts to...
Generate a set of master key parts
Load single key part
Load all key parts from...
Load all new master keys
Clear
Set, immediate
Coordinated change master keys and CKDS
Secure key part entry
Help
General
Keys
Controls-Desc
Controls-ACP
Dec Tables
PINs
Certificates
UPDATE MODE
Trusted Key Entry - Ready
Signature Key Loaded, Index: 99, Name: Default author...
QSYSTKE: Welcome to the Truste
QSYSTKE: Trusted Key Entry Con
Trusted Key Entry - Smart Card
Crypto Module Administration. C
10:02:40 07/25/18

Operational Keys

- DATA
- CLRAES, CLRDES
- CIPHER
- DECIPHER, ENCIPHER
- CIPHERXI, CIPHERXL, CIPHERXC
- DATAM, DATAMV
- MAC, MACVER
- HMAC
- PINGEN, PINVER
- IPINENC, OPINENC
- PINCALC
- PINPROT
- PINPRW
- EXPORTER/IMPORTER
- IMPPKA
- IKEYXLAT, OKEYXLAT
- KEYGENKY, DKYGENKY
- CVARENC, CVARXCVL, CVARXCVR
- SECMSG

Key Label and Key Type

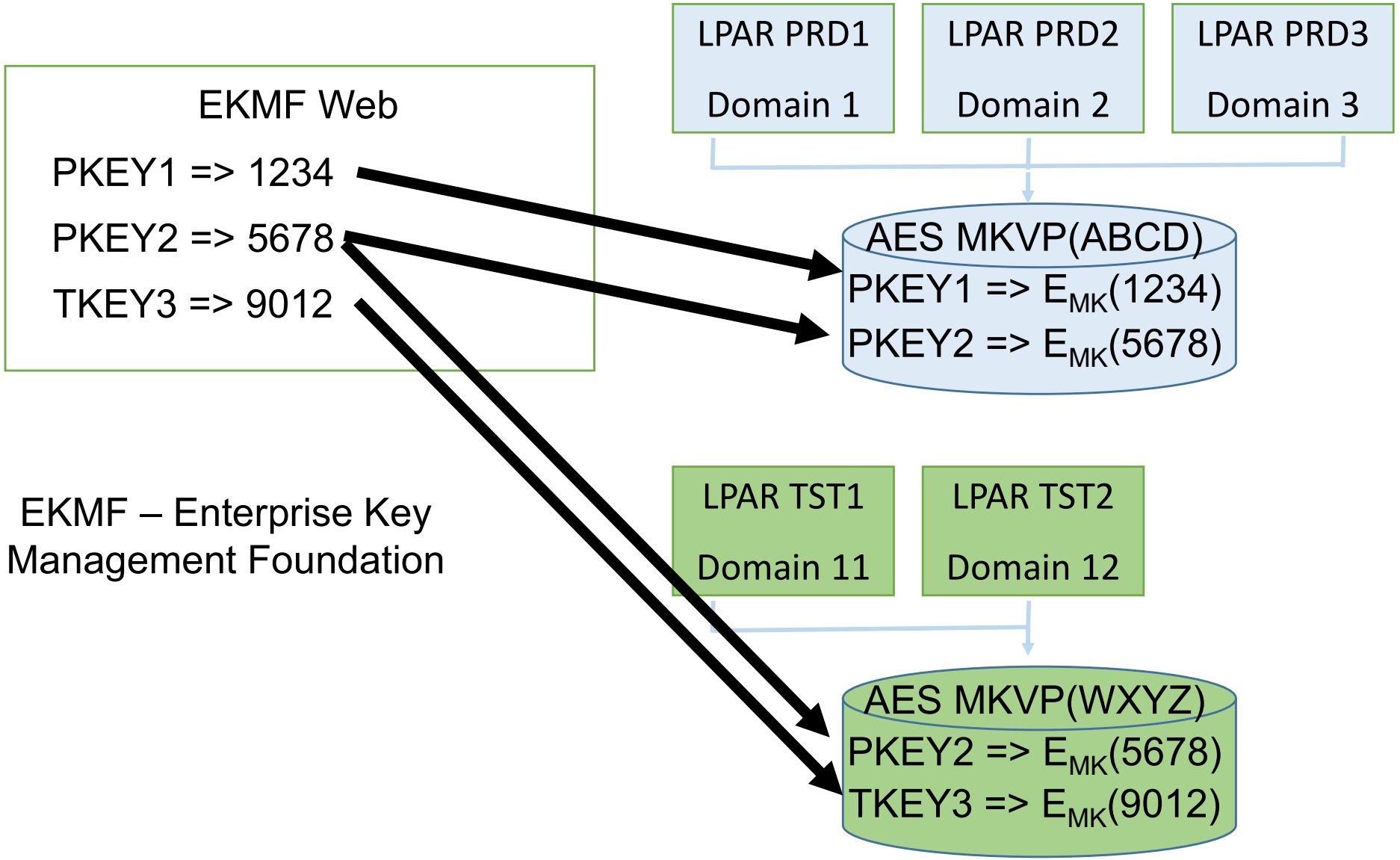


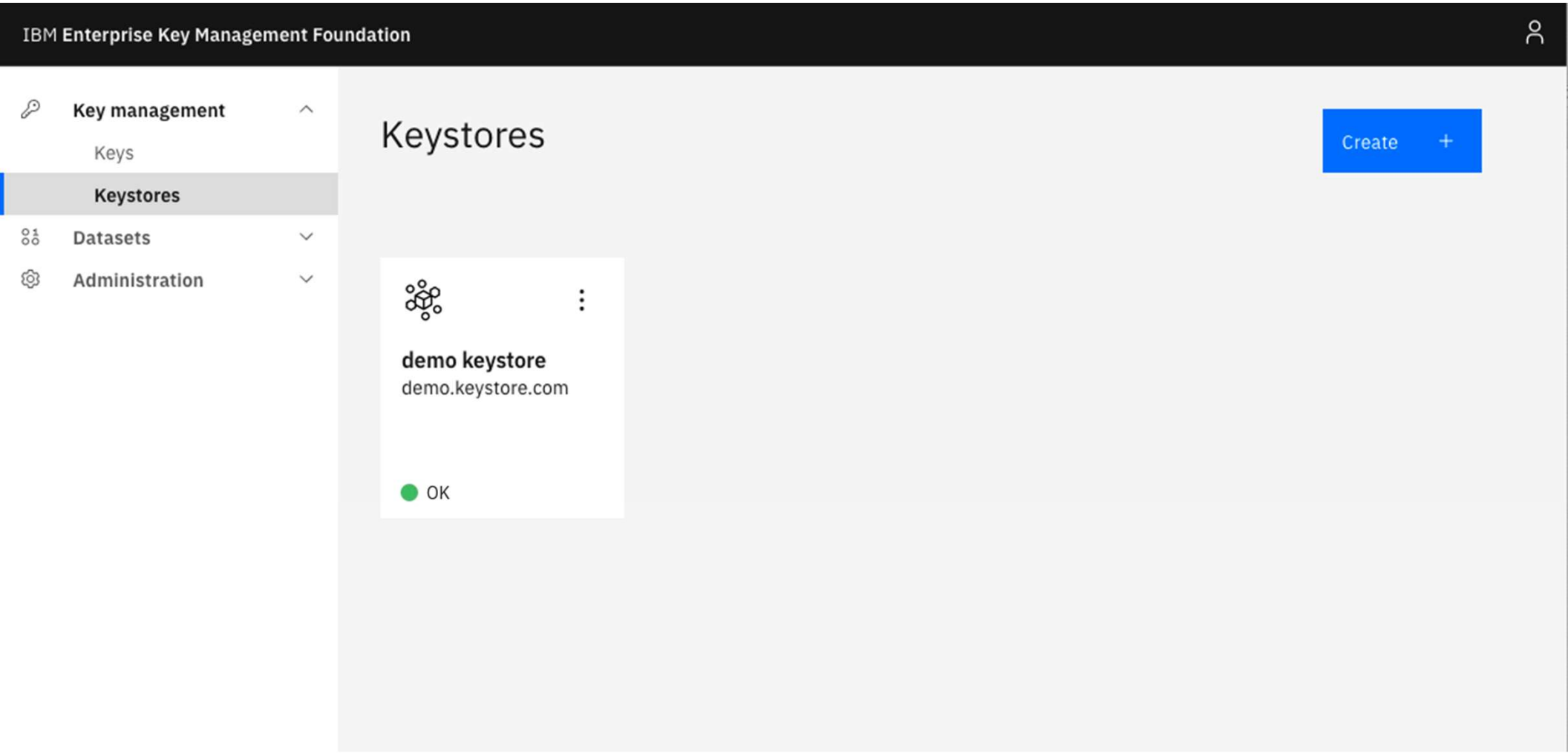
Key Labels

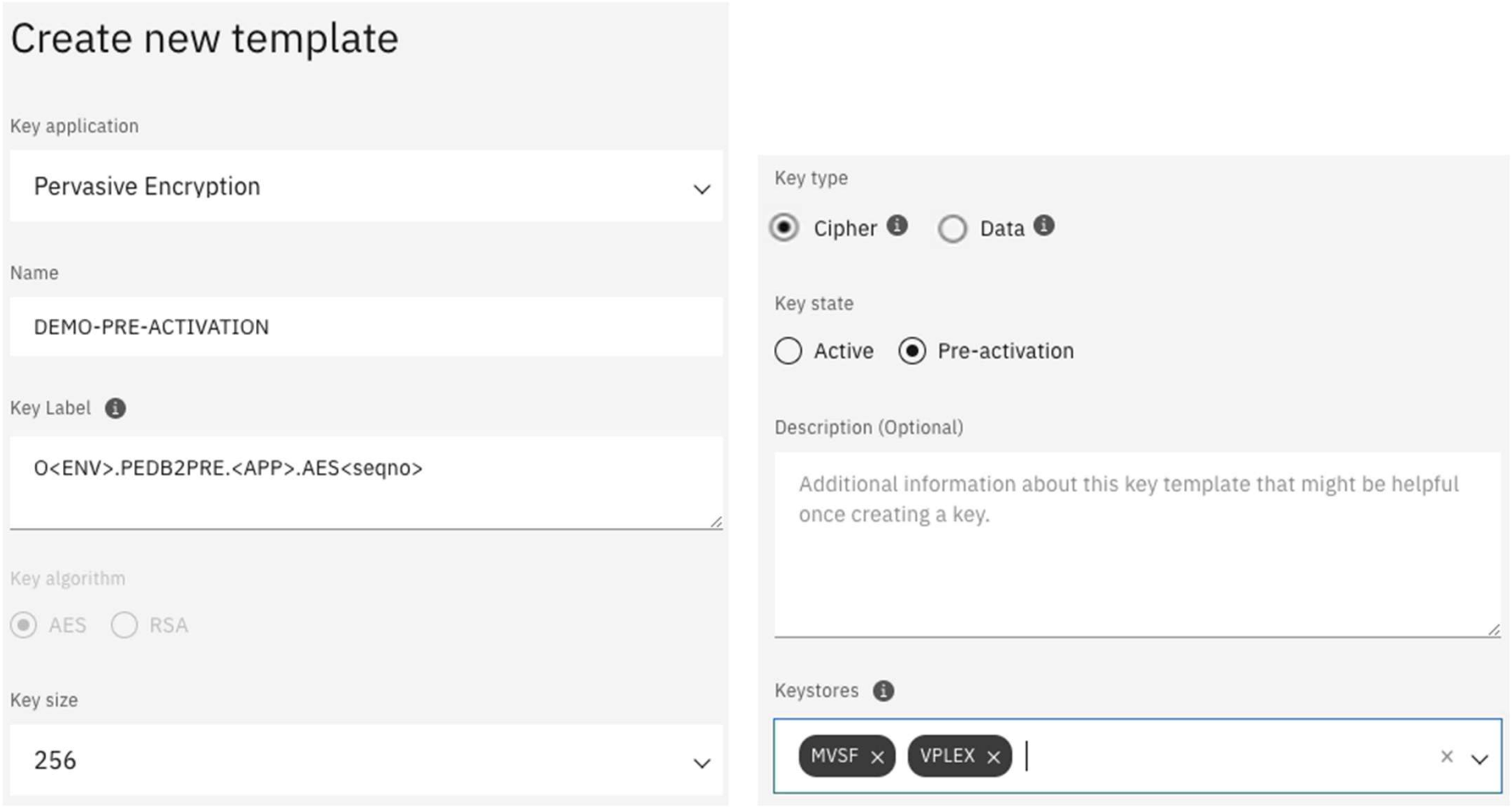
- 64 byte character string, left justified, right padded with blanks
- 1st character alphabetic or national (#, $, @)
- The rest can be alphabetic, national or period (.)
- All alphabetic are upper case

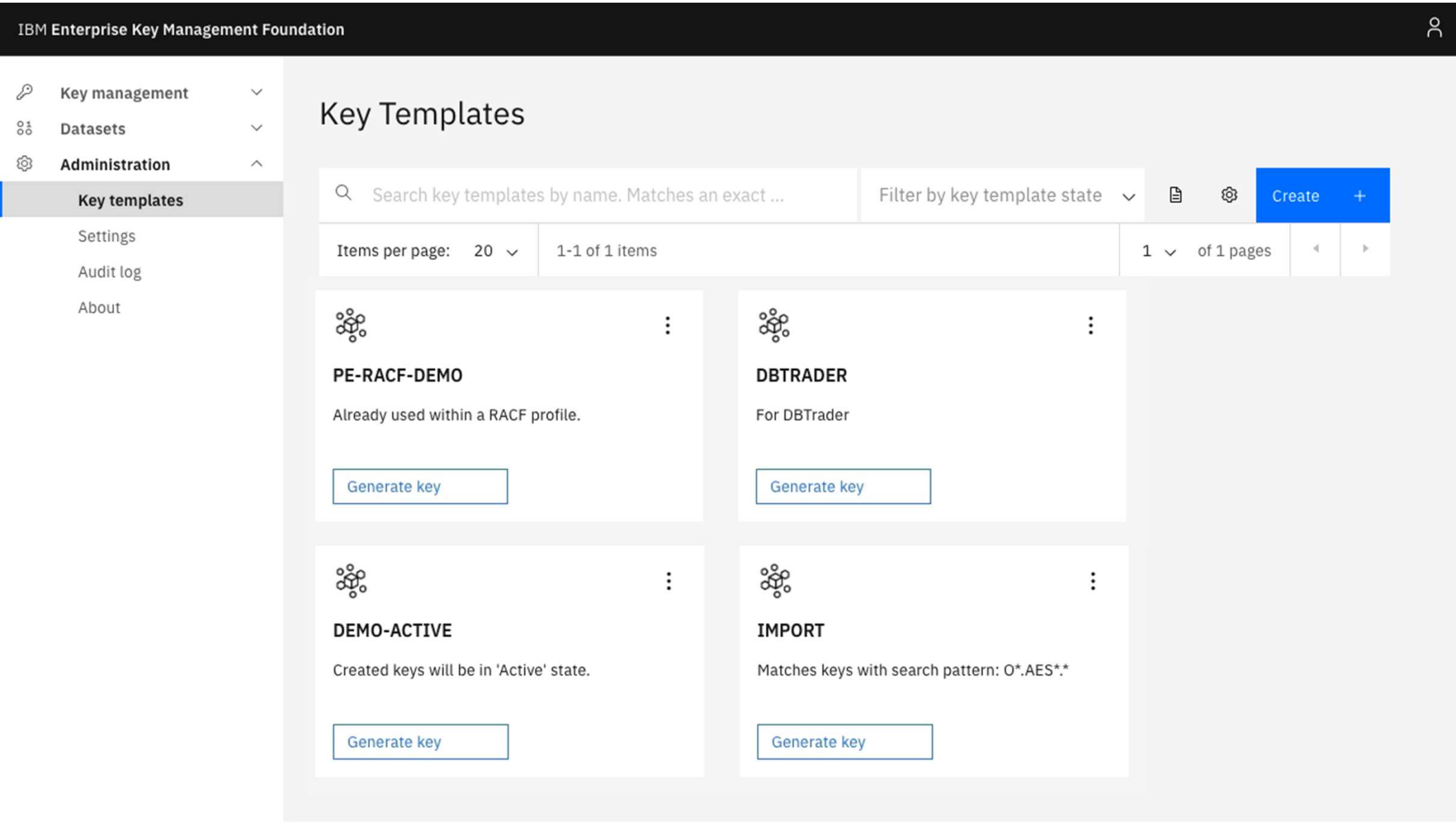
- Used, along with the key type, to find the specific key in the key store
- Used to identify the security profile that controls who and what access authority an individual has to the key

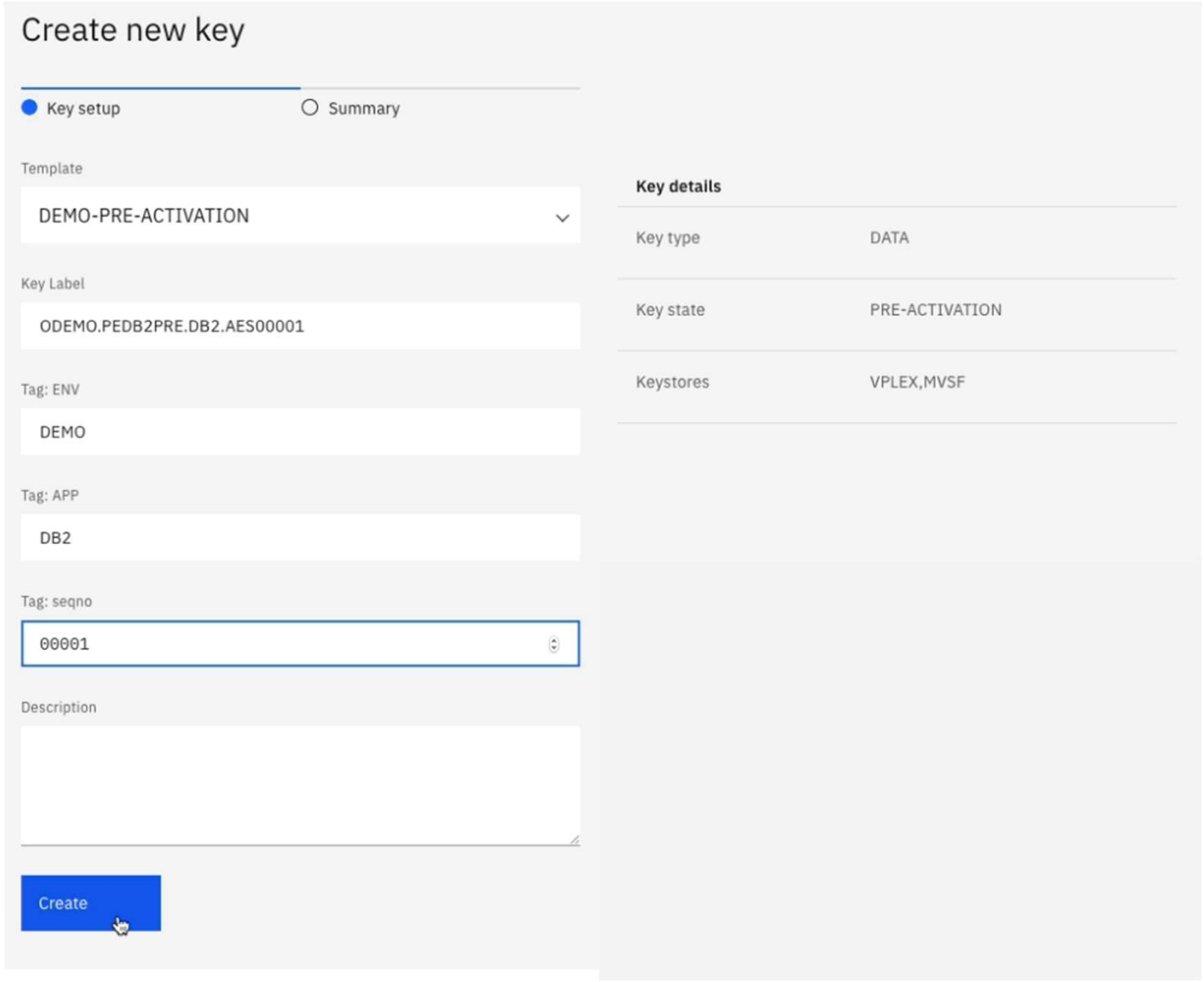
Key Management and Distribution




IBM Enterprise Key Management Foundation
Key management
Keys
Keystores
Datasets
Administration
Keystores
Create +
demo keystore
demo.keystore.com
OK


Create new template
Key application
Pervasive Encryption
Name
DEMO-PRE-ACTIVATION
Key Label
O<ENV>.PEDB2PRE.<APP>.AES<seqno>
Key algorithm
AES
RSA
Key size
256
Key type
Cipher
Data
Key state
Active
Pre-activation
Description (Optional)
Additional information about this key template that might be helpful once creating a key.
Keystores
MVSF
VPLEX


IBM Enterprise Key Management Foundation
Key management
Datasets
Administration
Key templates
Settings
Audit log
About
Key Templates
Search key templates by name. Matches an exact ...
Filter by key template state
Create
Items per page: 20
1-1 of 1 items
1 of 1 pages
PE-RACF-DEMO
Already used within a RACF profile.
Generate key
DBTRADER
For DBTrader
Generate key
DEMO-ACTIVE
Created keys will be in 'Active' state.
Generate key
IMPORT
Matches keys with search pattern: O*.AES*.*
Generate key


Create new key
Key setup
Summary
Template
DEMO-PRE-ACTIVATION
Key Label
ODEMO.PEDB2PRE.DB2.AES00001
Tag: ENV
DEMO
Tag: APP
DB2
Tag: seqno
00001
Description
Create
Key details
Key type
DATA
Key state
PRE-ACTIVATION
Keystores
VPLEX,MVSF

Summary

- Master keys protect your operational keys
- Operational keys are stored in your key stores
- Master keys are managed differently and independently from operational keys

Questions?

Definitions

- Master keys – only exist in the Crypto cards and protect your operational keys
- Operational keys – encrypt your data
- CEX – Crypto Express card, IBM's Hardware Security Module (HSM) available on the IBM mainframes and inside the Trusted Key Entry Workstation
- Data Set Encryption (DSE) – the operating system function that will encrypt individual data sets on the mainframe
- EKMF – Enterprise Key Management Foundation – a tool for managing operational keys
- Hardware Security Module (HSM) – tamper recognizing, tamper-responding technology to protect crypto key material
- TKE – Trusted Key Entry Workstation, an appliance for managing the crypto hardware and loading master keys on the mainframe