MAINFRAME CRYPTO

Unscrambling the Complexity of Crypto!

Trusted Key Entry – Managing Your Keys AND Crypto Configuration

Greg Boyd

gregboyd@mainframecrypto.com

THE Z EXCHANGE

August 2018

Copyrights . . .

- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 15 years

. . . And Trademarks

- Copyright © 2018 Greg Boyd, Mainframe Crypto, LLC. All rights reserved.
- 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.

TKE Agenda

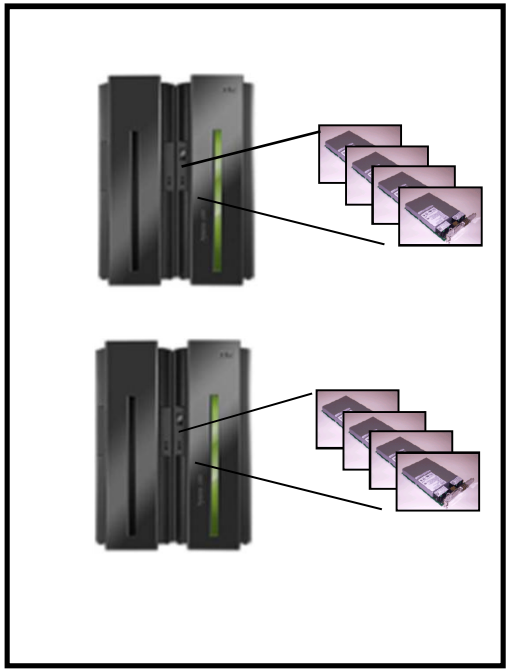
- Description
- Setup
- Smart Cards
- Roles
- TKE Application
- Loading Keys

Key Loading

- Master Keys
  - Trusted Key Entry Workstation
  - Passphrase Initialization (aka PPINIT)
  - Via the ISPF Panels for ICSF
- Operational Keys
  - Trusted Key Entry Workstation
  - Key Generation Utility Program (KGUP)
  - Enterprise Key Management Foundation
  - ICSF APIs

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 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

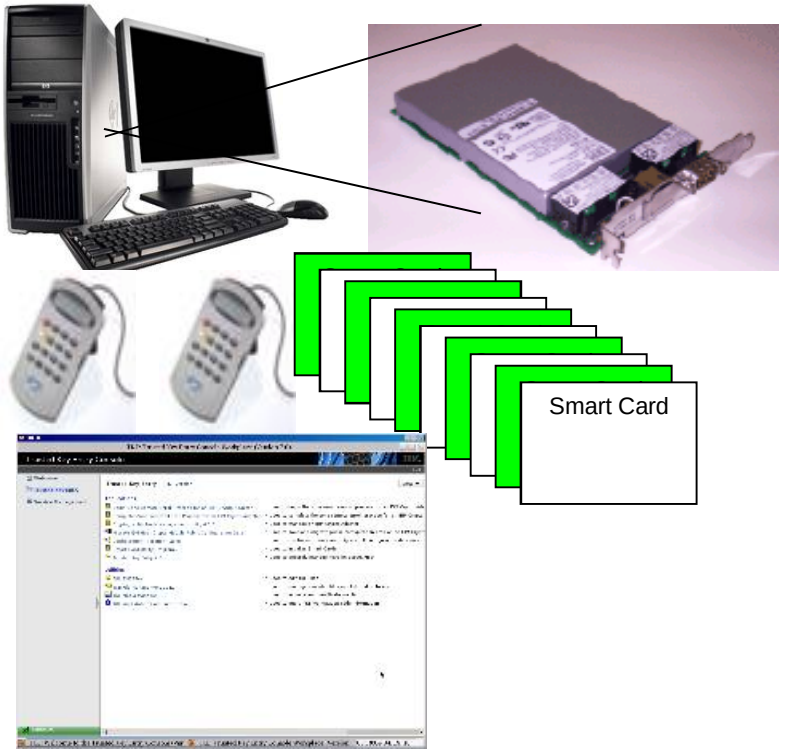


© MAINFRAME CRYPTO

TKE – Feature Codes

Intel Workstation with a cryptographic coprocessor and embedded operating system

- Hardware
  - Intel Workstation or Rack Mounted
  - Crypto ExpressN card
- Software
  - Looks a lot like Linux OS
  - TKE application (Java)
- Optional smart card support
  - 2 Readers and 20 smart cards
  - Can install up to 4 readers
- Optional 10 Additional smart cards

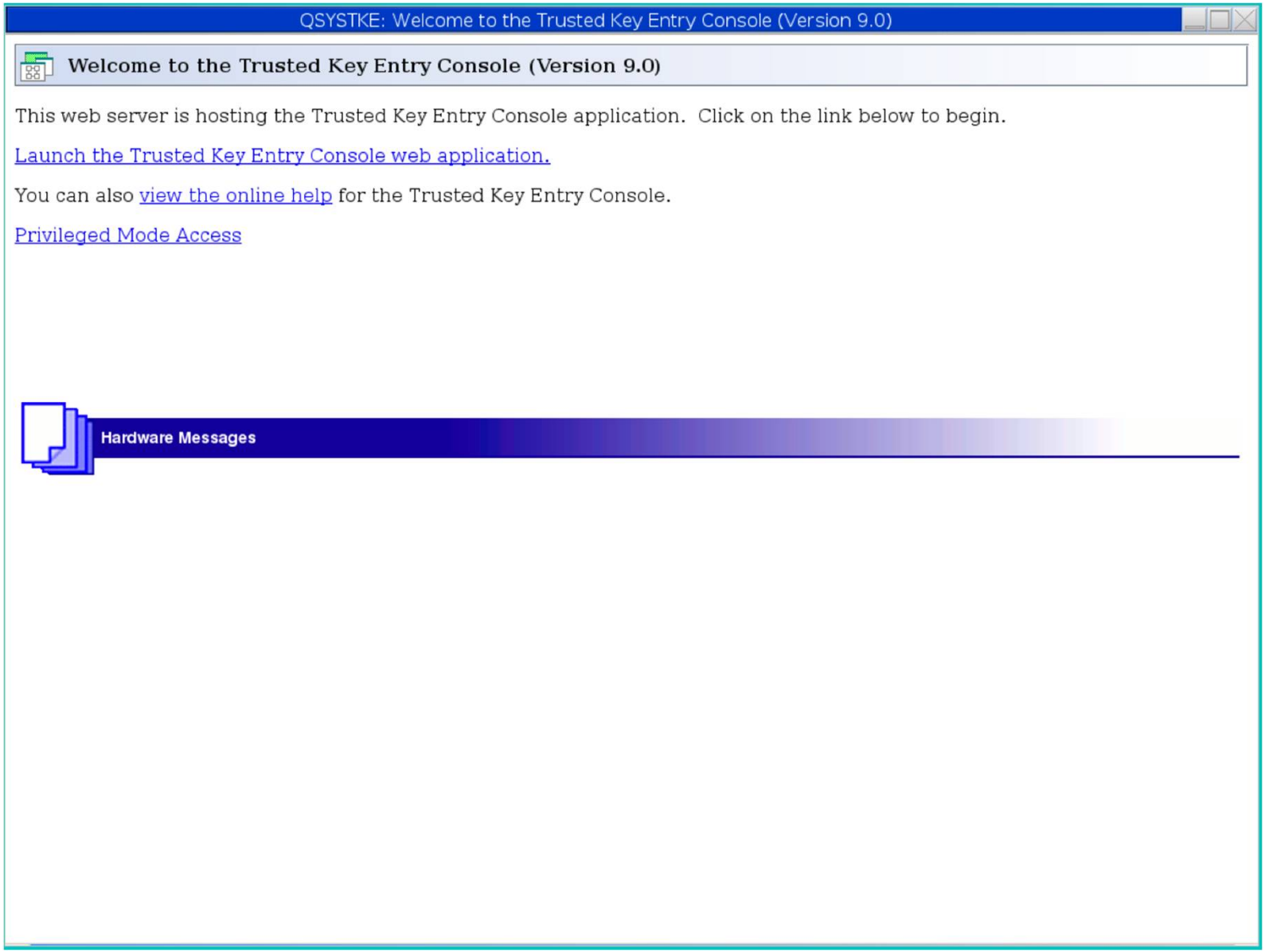


TKE Hardware/Software

TKE Software (LIC) FC	TKE Hardware FC	Host system	Host Crypto cards managed
TKE 9.0 (#0879)	#0842, #0847, #0097, #0098, #0849, #0080, #0081, #0085, #0086	z14/z14Model ZR1, z13/z13s, zEC12/zBC12	CEX6C, CEX6P, CEX5P, CEX5C, CEX4P, CEX4C, CEX3C, CEX2C
TKE 8.1 (#0878)	#0847 or #0097	z13/z13s, zEC12/zBC12	CEX5P, CEX5C, CEX4P, CEX4C, CEX3C, CEX2C
TKE 8.0 (#0877)	#0847	Z13/z13s, zEC12/zBC12	CEX5P, CEX5C, CEX4P, CEX4C, CEX3C, CEX2C
TKE 7.3 (#0872)	#0841 or #0842	zEC12/zBC12, z196/z114	CEX4P, CEX4C, CEX3C, CEX2C
TKE 7.2 (#0850)	#0841	zEC12, z196/z114	CEX4P, CEX4C, CEX3C, CEX2C
TKE 7.1 (#0867)	#0841	z196/z114, z10 EC/BC	CEX3C, CEX2C
TKE 7.0 (#0860)	#0841	z196/z114, z10 EC/BC	CEX3C, CEX2C
TKE 6.0 (#0858)	#0859, #0839, #0840	z196/z114, z10 EC/BC	CEX4C (sometimes), CEX3C, CEX2C

© MAINFRAME CRYPTO

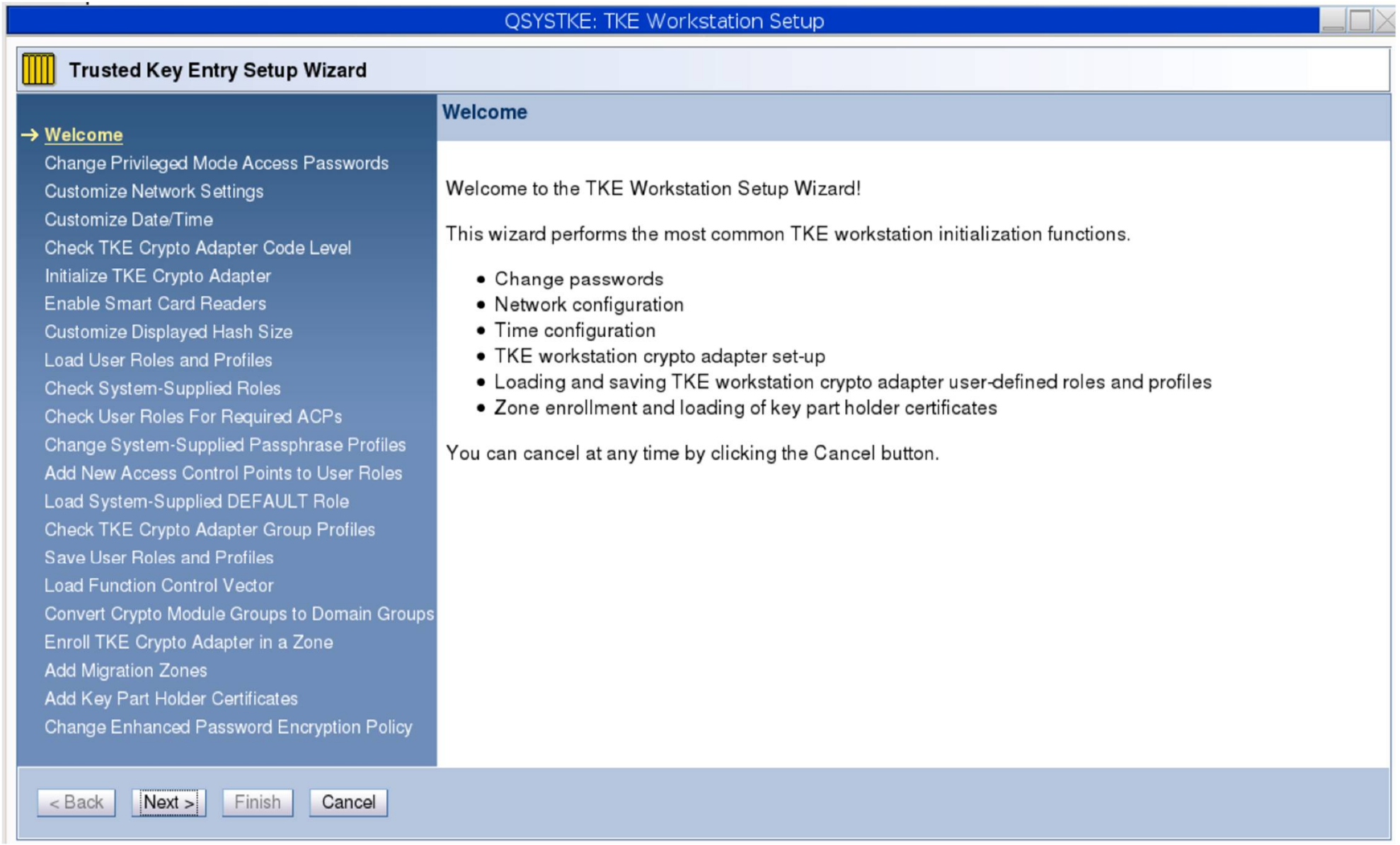
TKE Welcome Screen



Privileged Mode Access

- ADMIN
- AUDITOR
- SERVICE

TKE Setup Wizard



© MAINFRAME CRYPTO

Setup Wizard Steps (1 of 2)

- Change Privileged Mode Access Passwords
- Customize Network Settings
- Customize Date/Time
- Check TKE Crypto Adapter Code Level
- Initialize TKE Crypto Adapter
- Enable Smart Card Readers
- Customize Displayed Hash Size
- Load User Roles and Profiles
- Check System-Supplied Roles
- Check User Roles For Required ACPs
- Change System-Supplied Passphrase Profiles

© MAINFRAME CRYPTO

Setup Wizard Steps (2 of 2)

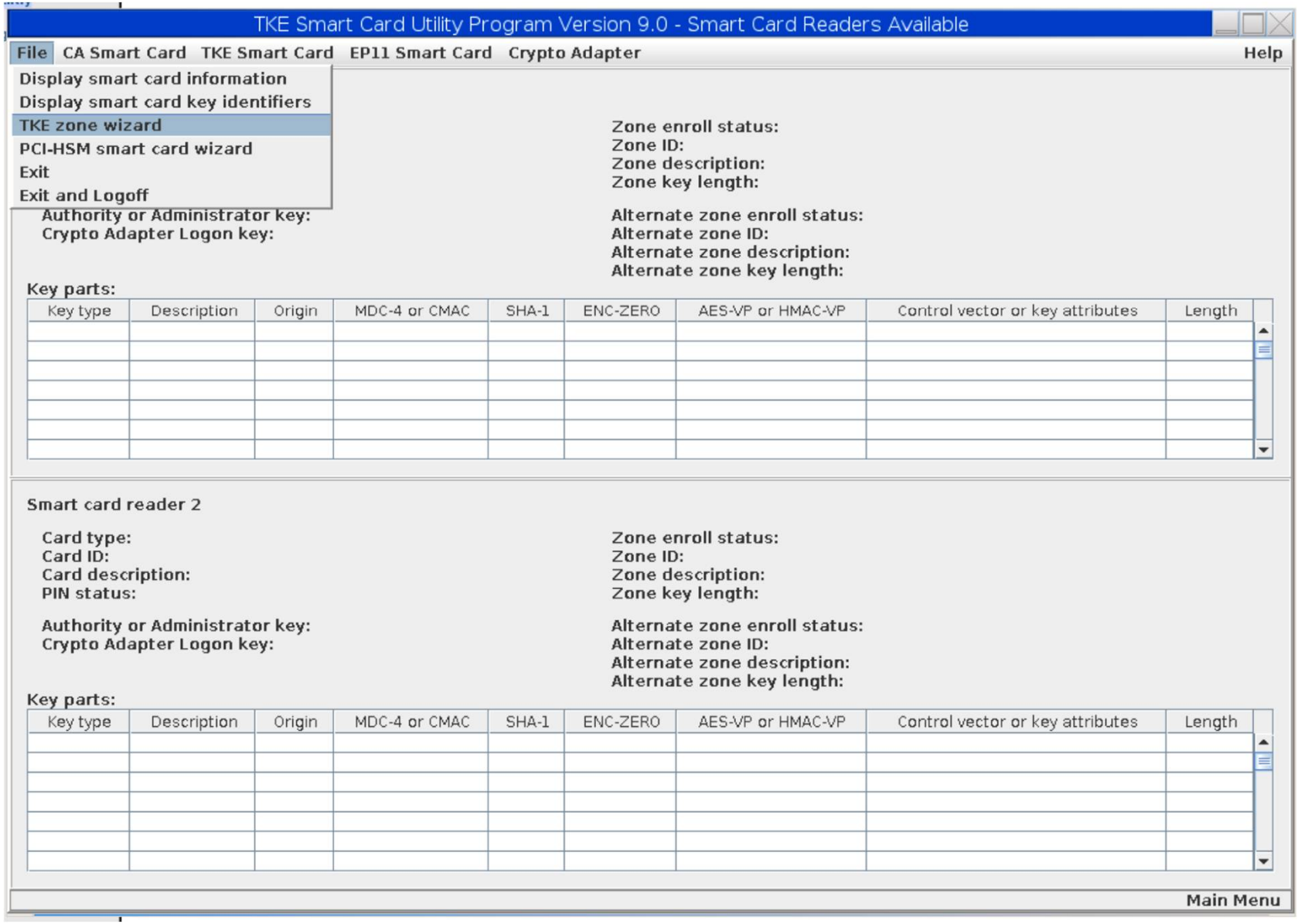
- Add New Access Control Points to User Roles
- Load System-Supplied DEFAULT Role
- Check TKE Crypto Adapter Group Profiles
- Save User Roles and Profiles
- Load Function Control Vector
- Convert Crypto Module Grups to Domain Groups
- Enroll TKE Crypto Adapter in a Zone
- Add Migration Zones
- Add Key Part Holder Certificates
- Change Enhanced Password Encryption Policy

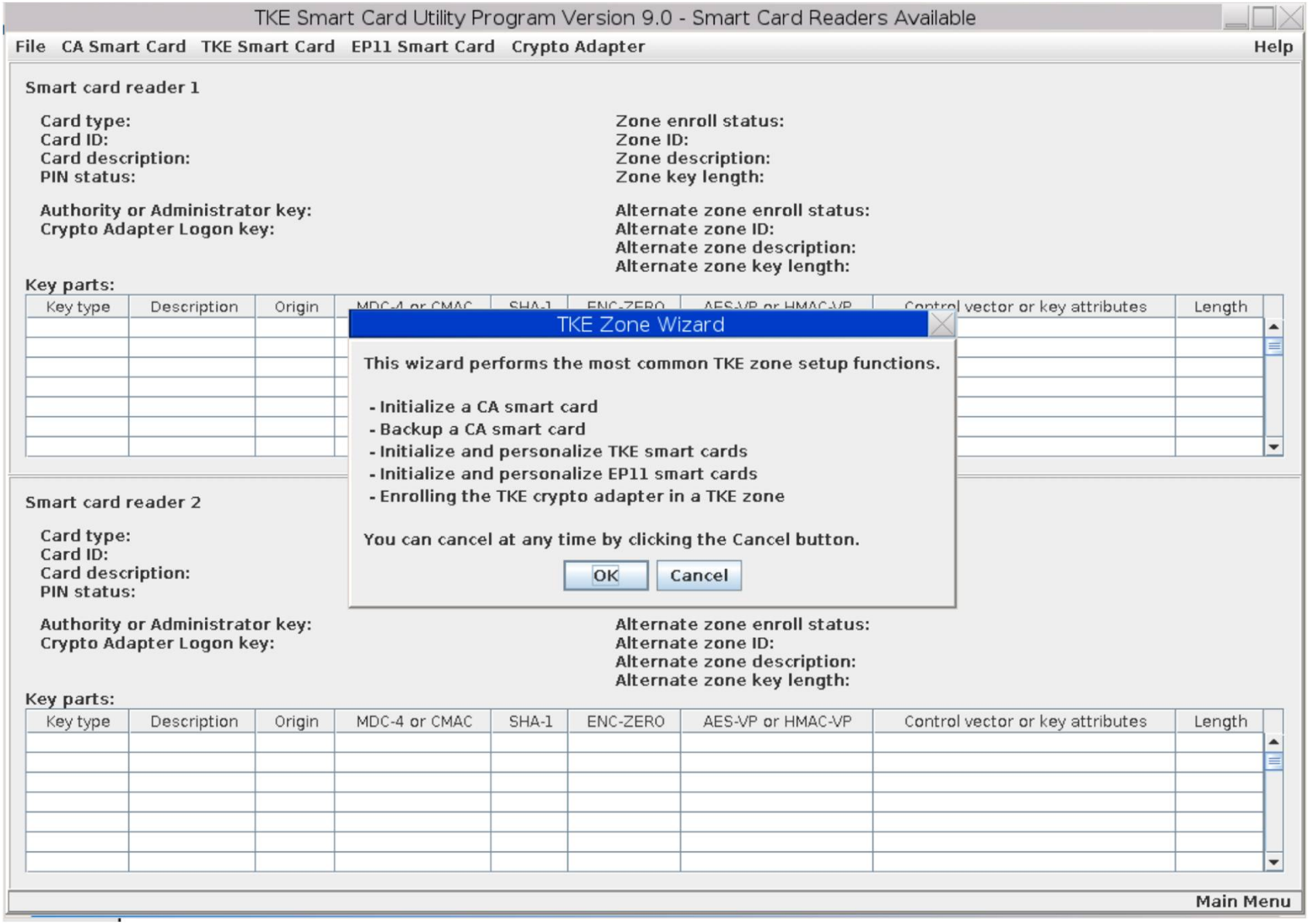
© MAINFRAME CRYPTO

TKE Zones

- Key parts on a smart card can be moved securely but only between members of a zone
- Members of (Entities in) a zone
  - CA (Certificate Authority) Smart Card
  - TKE Workstation Crypto Adapter
  - TKE Smart Cards
  - EP11 Smart Cards
- Zone is created when you create the CA Smart Card

© MAINFRAME CRYPTO




TKE Smart Card Utility Program Version 9.0 - Smart Card Readers Available
File
CA Smart Card
TKE Smart Card
EP11 Smart Card
Crypto Adapter
Help
Smart card reader 1
Card type:
Card ID:
Card description:
PIN status:
Authority or Administrator key:
Crypto Adapter Logon key:
Zone enroll status:
Zone ID:
Zone description:
Zone key length:
Alternate zone enroll status:
Alternate zone ID:
Alternate zone description:
Alternate zone key length:
Key parts:
Key type
Description
Origin
MDC-4 or CMAC
SHA-1
ENC-ZERO
AES-VP or HMAC-VP
Control vector or key attributes
Length
TKE Zone Wizard
This wizard performs the most common TKE zone setup functions.
- Initialize a CA smart card
- Backup a CA smart card
- Initialize and personalize TKE smart cards
- Initialize and personalize EP11 smart cards
- Enrolling the TKE crypto adapter in a TKE zone
You can cancel at any time by clicking the Cancel button.
OK
Cancel
Smart card reader 2
Card type:
Card ID:
Card description:
PIN status:
Authority or Administrator key:
Crypto Adapter Logon key:
Alternate zone enroll status:
Alternate zone ID:
Alternate zone description:
Alternate zone key length:
Key parts:
Key type
Description
Origin
MDC-4 or CMAC
SHA-1
ENC-ZERO
AES-VP or HMAC-VP
Control vector or key attributes
Length
Main Menu

© MAINFRAME CRYPTO

Smart Cards

- Store credentials
- Store key material
- Perform encryption functions

http://dilbert.com/strip/1997-03-21

Smart Cards

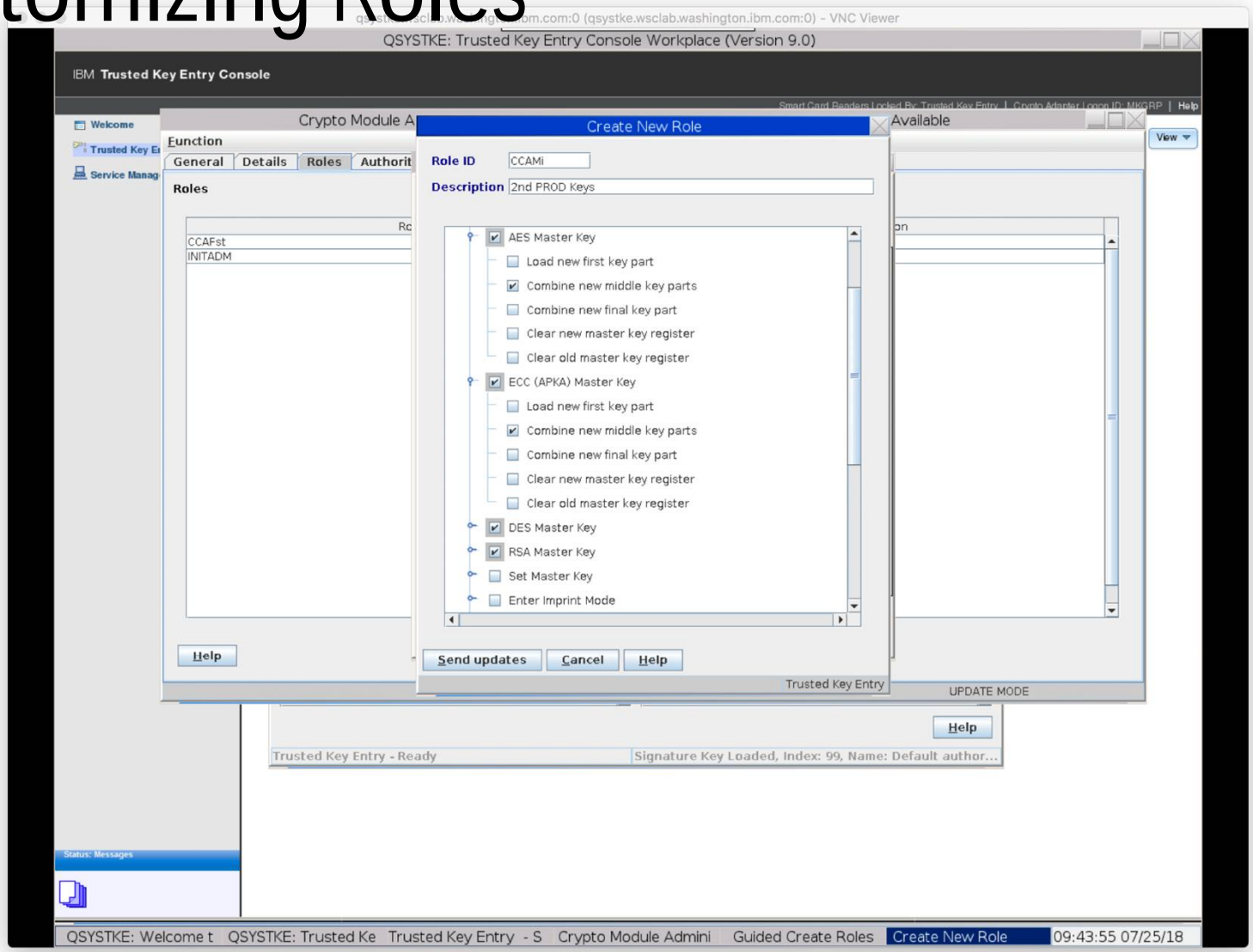
- Certificate Authority (CA) Smart Card
  - Two 6-digit PINs
- TKE Smart Card – Supports CCA Coprocessors
- EP11 Smart Card – Supports EP11 Coprocessors

- MCA (Migration Certificate Authority)
- Key Part Holder (KPH) Smart Card
- Injection Authority (IA) Smart Card

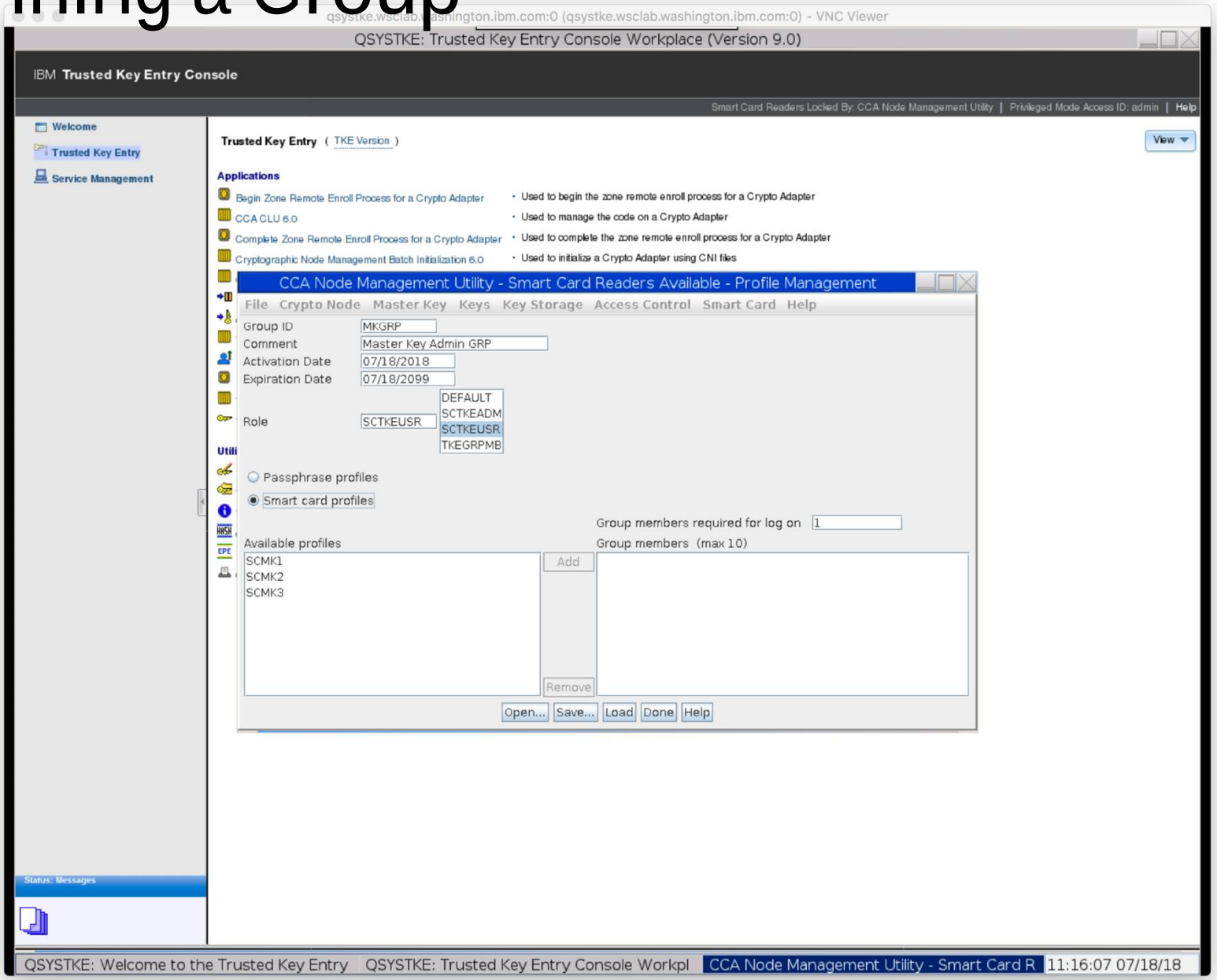
IBM Supplied Roles

- Passphrase Roles
  - TKEADM – for managing the TKE Workstation
  - TKEUSER – for managing host crypto modules
  - KEYMAN1 – clear new master key registers, load first part new master key
  - KEYMAN2 – load middle and final master key parts, set master keys, reencipher keystores
- Smart Card Roles
  - SCTKEUSR – for managing host crypto modules
  - SCTKEADM – for managing the TKE Workstation

Customizing Roles

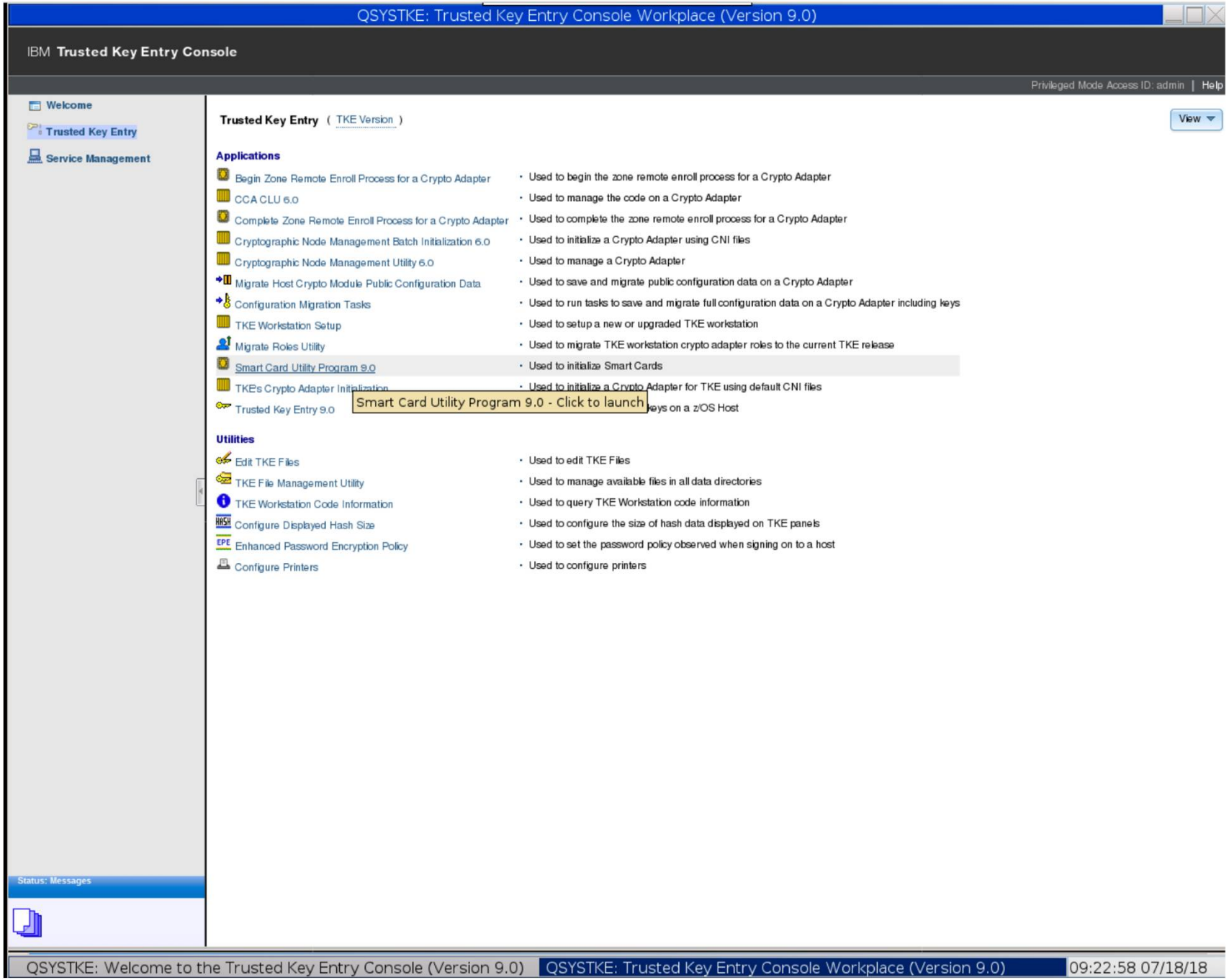


Defining a Group



© MAINFRAME CRYPTO

TKE 9.0 Main Menu

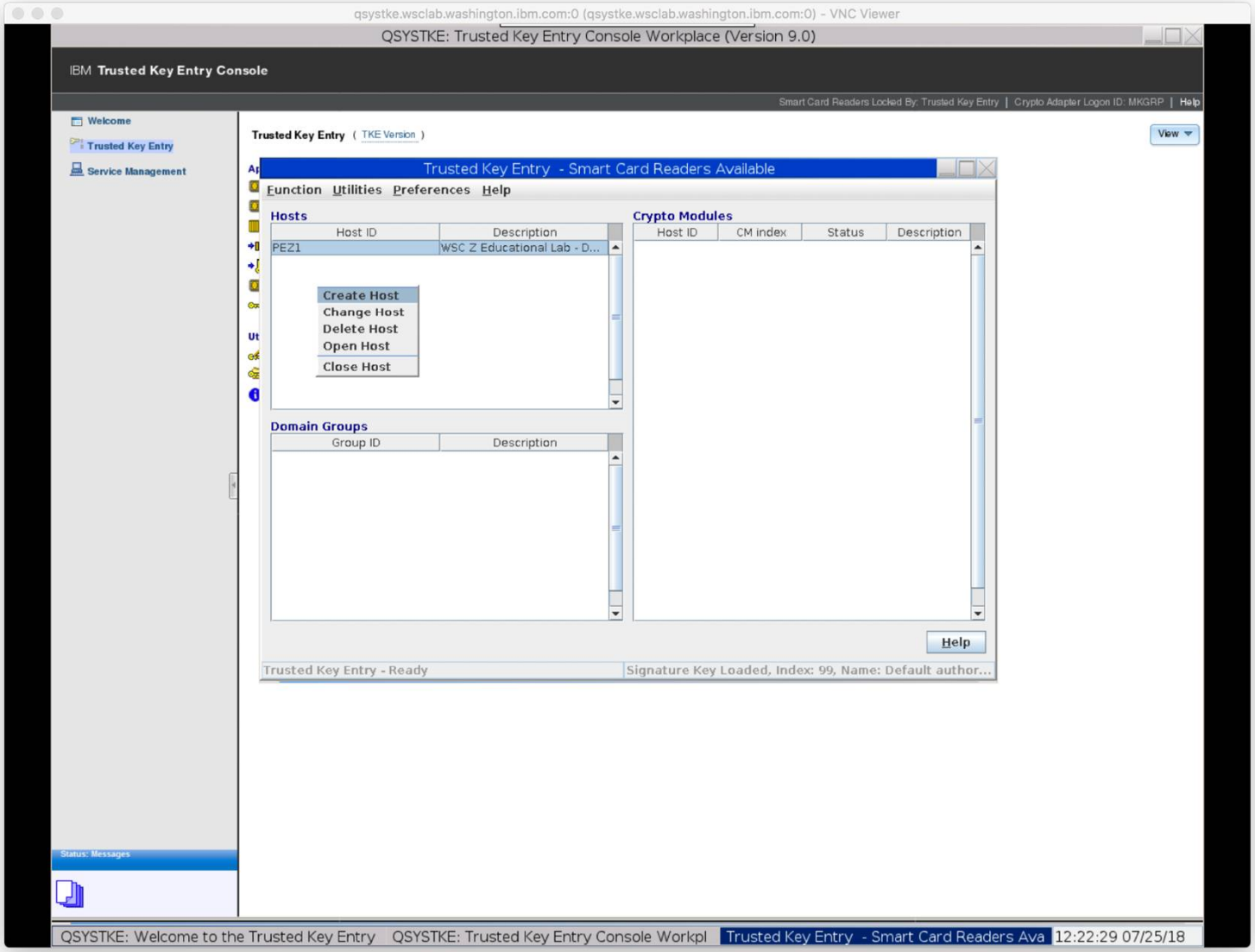


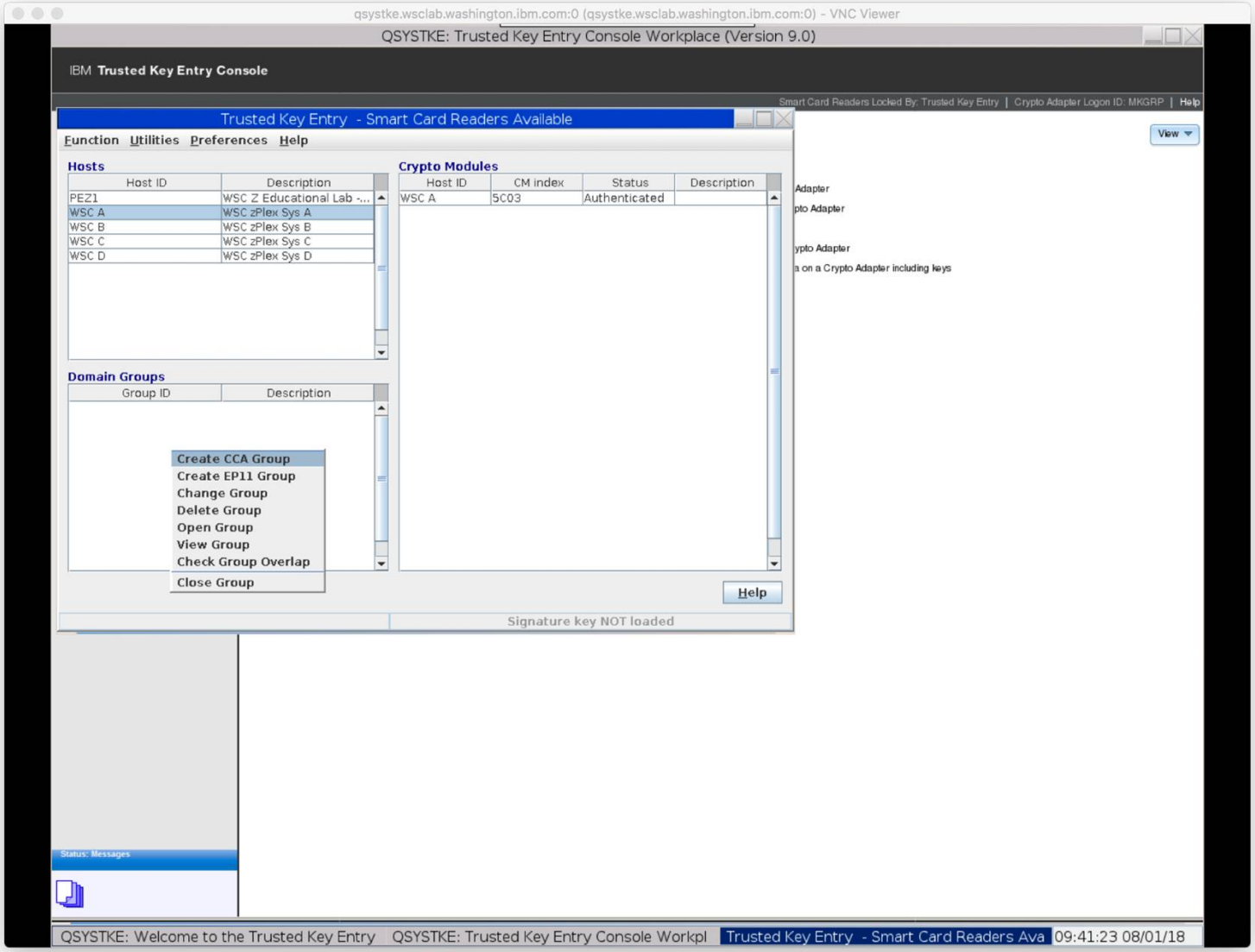
TKE Console Workspace

- Applications
  - Begin Zone Remote Enroll Process for an IBM Crypto Adapter
  - CCA CLU
  - Complete Zone Remote Enroll Process for an IBM Crypto Adapter
  - Crypto Node Management Batch Initialization
  - Crypto Node Management Utility
  - Migrate IBM Host Crypto Module Public Configuration Data (CCA Only)
  - Configuration Migration Tasks (CCA or EP11)
  - TKE Workstation Setup
  - Migrate Roles Utility
  - Smart Card Utility Program
  - TKE's IBM Crypto Adapter Initialization
  - Trusted Key Entry

TKE Console Workspace

- Utilities
  - Edit TKE Files
  - TKE File Management Utility
  - TKE Workstation Code Information
  - Configure Displayed Hash Size
  - Enhanced Password Encryption Policy
  - Configure Printers


qsystke.wsclab.washington.ibm.com:0 (qsystke.wsclab.washington.ibm.com:0) - VNC Viewer
QSYSTKE: Trusted Key Entry Console Workplace (Version 9.0)
IBM Trusted Key Entry Console
Smart Card Readers Locked By: Trusted Key Entry | Crypto Adapter Logon ID: MKGRP | Help
Welcome
Trusted Key Entry
Service Management
Trusted Key Entry (TKE Version)
View
Trusted Key Entry - Smart Card Readers Available
Function Utilities Preferences Help
Hosts
Host ID
Description
PEZ1
WSC Z Educational Lab - D...
Create Host
Change Host
Delete Host
Open Host
Close Host
Crypto Modules
Host ID
CM index
Status
Description
Domain Groups
Group ID
Description
Help
Trusted Key Entry - Ready
Signature Key Loaded, Index: 99, Name: Default author...
Status: Messages
QSYSTKE: Welcome to the Trusted Key Entry
QSYSTKE: Trusted Key Entry Console Workpl
Trusted Key Entry - Smart Card Readers Ava
12:22:29 07/25/18


qsystke.wsclab.washington.ibm.com:0 (qsystke.wsclab.washington.ibm.com:0) - VNC Viewer
QSYSTKE: Trusted Key Entry Console Workplace (Version 9.0)
IBM Trusted Key Entry Console
Smart Card Readers Locked By: Trusted Key Entry | Crypto Adapter Logon ID: MKGRP | Help
View
Trusted Key Entry - Smart Card Readers Available
Function Utilities Preferences Help
Hosts
Host ID
Description
PEZ1
WSC Z Educational Lab -...
WSC A
WSC zPlex Sys A
WSC B
WSC zPlex Sys B
WSC C
WSC zPlex Sys C
WSC D
WSC zPlex Sys D
Crypto Modules
Host ID
CM index
Status
Description
WSC A
5C03
Authenticated
Domain Groups
Group ID
Description
Create CCA Group
Create EP11 Group
Change Group
Delete Group
Open Group
View Group
Check Group Overlap
Close Group
Help
Signature key NOT loaded
Status: Messages
QSYSTKE: Welcome to the Trusted Key Entry
QSYSTKE: Trusted Key Entry Console Workpl
Trusted Key Entry - Smart Card Readers Ava
09:41:23 08/01/18

Scoped commands

- Module Scoped – refers to information or commands that apply to an entire crypto module (ex. enable/disable a crypto module; one set of Roles & Authorities loaded on a crypto module)
- Domain Scoped - refers to information or commands that apply to a domain on a crypto module (ex. set a common master key in multiple domains)

Loading Domains (1 Card)

CKDS
PKDS
TKDS

CKDS
PKDS
TKDS

Dom	AES-MK	DES-MK	RSA-MK	ECC-MK
UD1				
UD2				
UD3				
UD4[M]				
UD5				
UD6				
UD7				
UD8				
UD9				
....				
UD85				

TCP/IP

TSO

TKE Host Transaction Program (aka TKE Listener)

ICSF

z/OS / LPAR 3

Usage Domain 3; Control Domain 3,4,5,6

Loading Domains (2 or more Cards)

CKDS
PKDS
TKDS

CKDS
PKDS
TKDS

Dom	AES-MK	DES-MK	RSA-MK	ECC-MK
UD1				
UD2				
UD3				
UD4[M]				
UD5				
UD6				
UD7				
UD8				
UD9				
....				
UD85				

TCP/IP

TSO

TKE Host Transaction Program (aka TKE Listener)

ICSF

z/OS / LPAR 3

Usage Domain 3; Control Domain 3,4,5,6

Loading Domains (multiple CECs)

CKDS
PKDS
TKDS

CKDS
PKDS
TKDS

Dom	AES-MK	DES-MK	RSA-MK	ECC-MK
UD1				
UD2				
UD3				
UD4[M]				
UD5				
UD6				
UD7				
UD8				
UD9				
....				
UD85				

TCP/IP

TSO

TKE Host Transaction Program (aka TKE Listener)

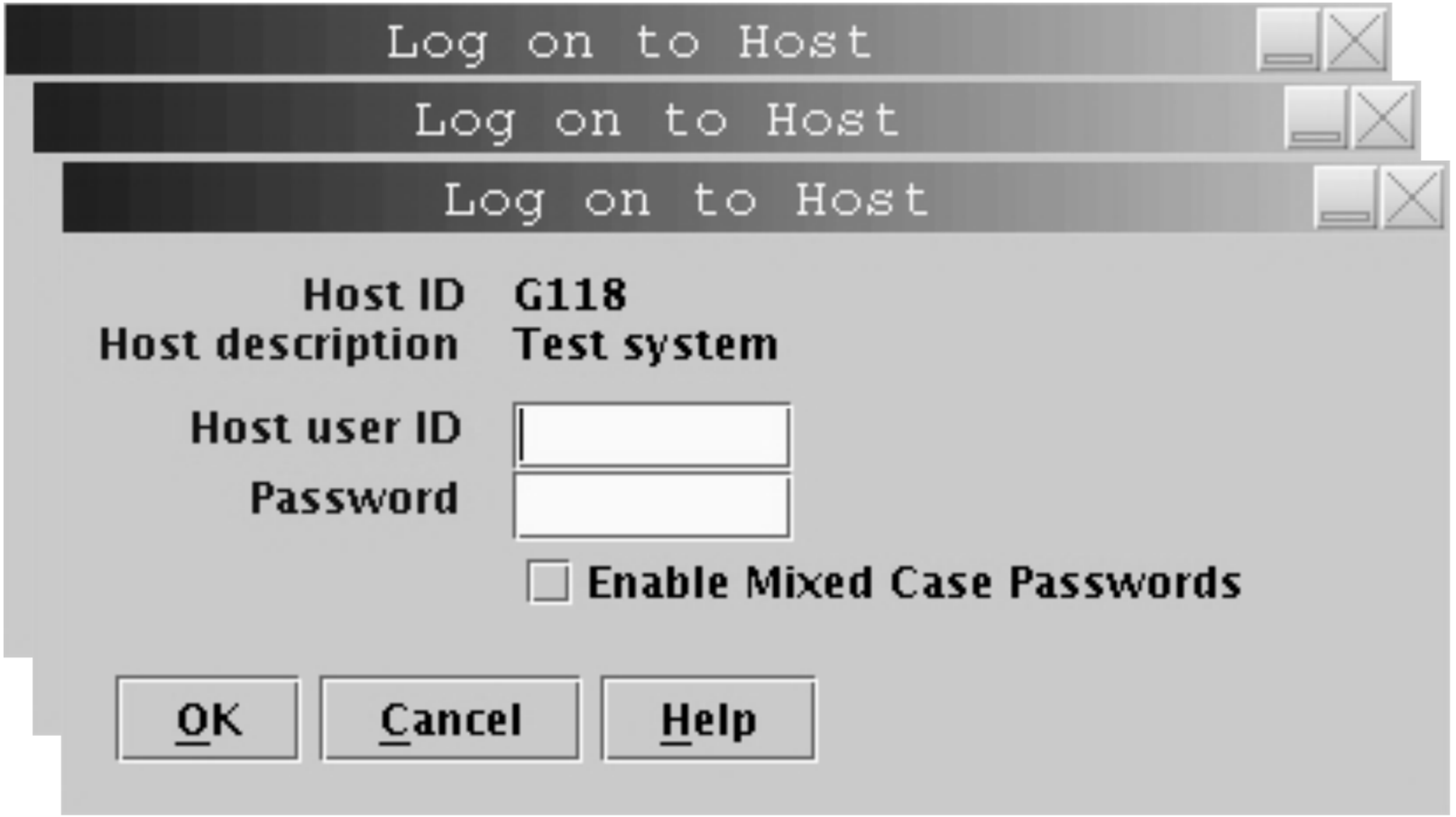
ICSF

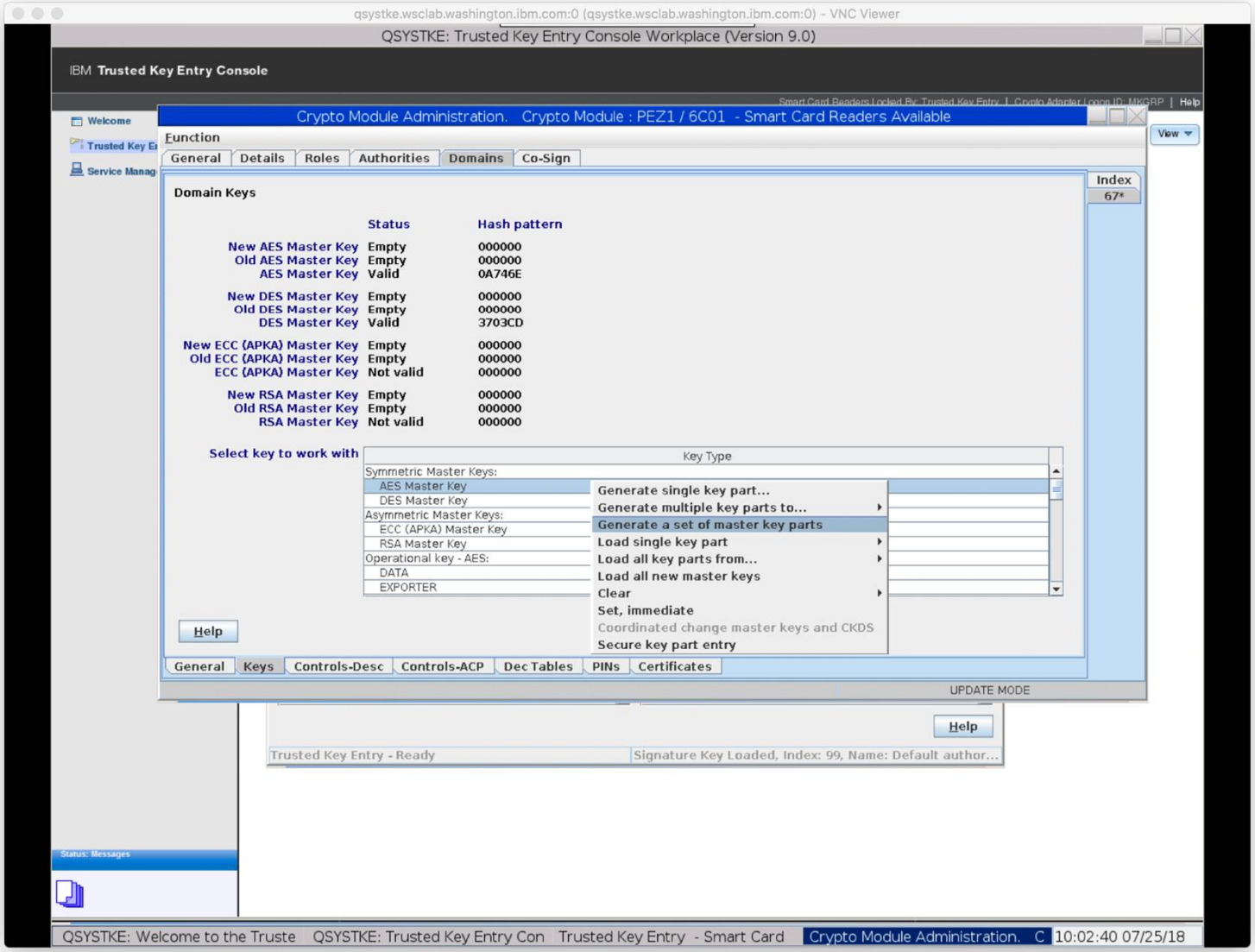
z/OS / LPAR 3

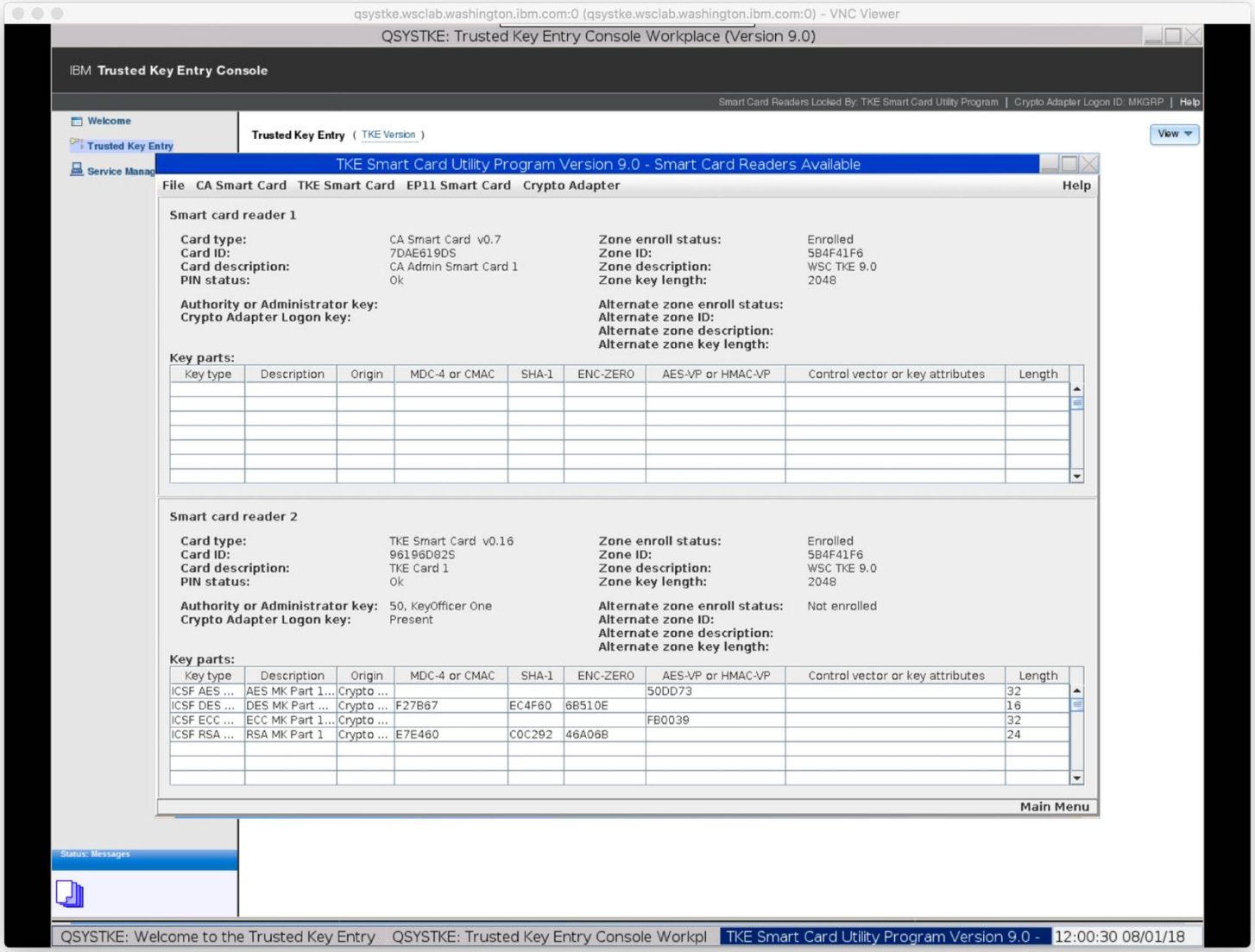
Usage Domain 3; Control Domain 3,4,5,6

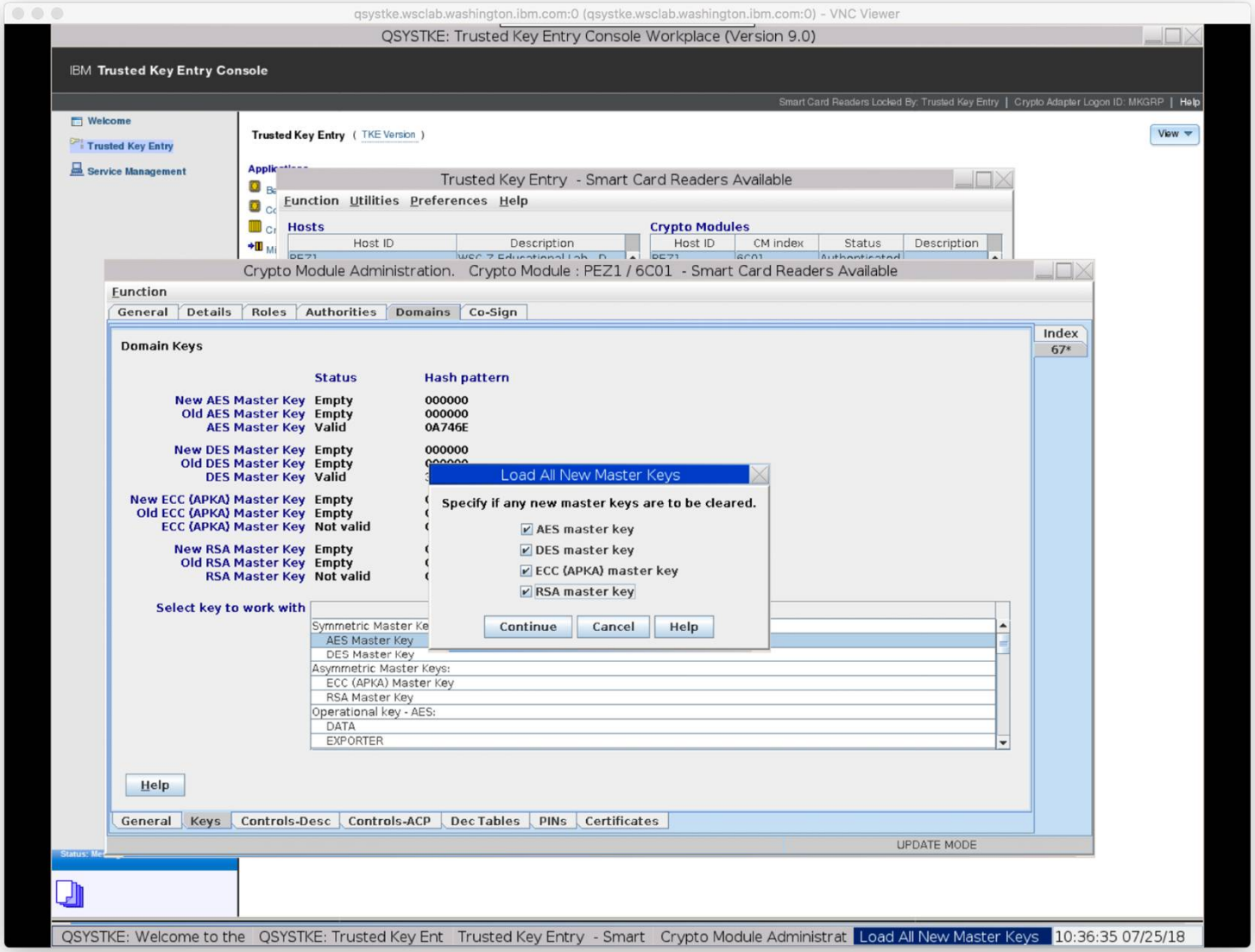
© MAINFRAME CRYPTO

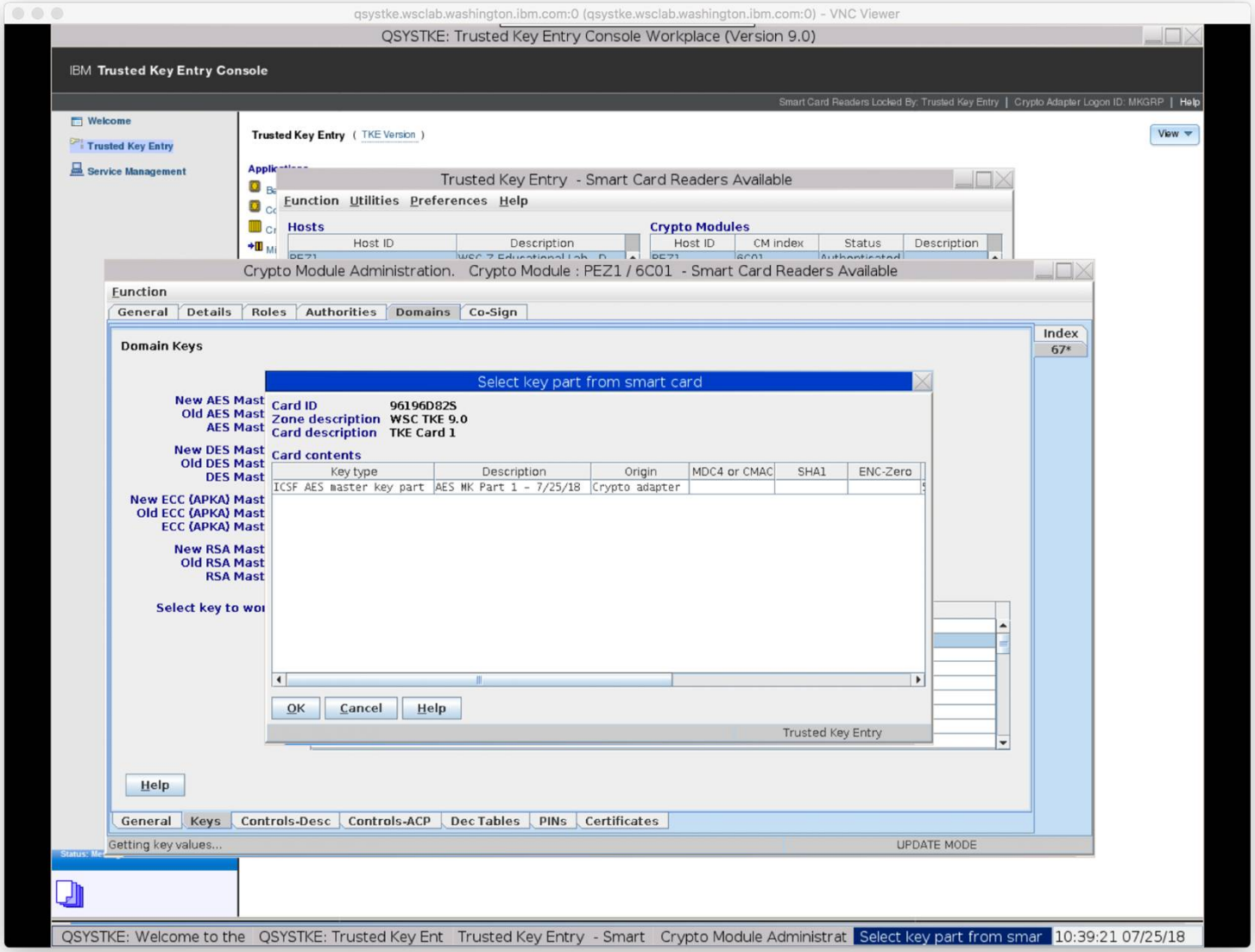
Logon to the Host(s)

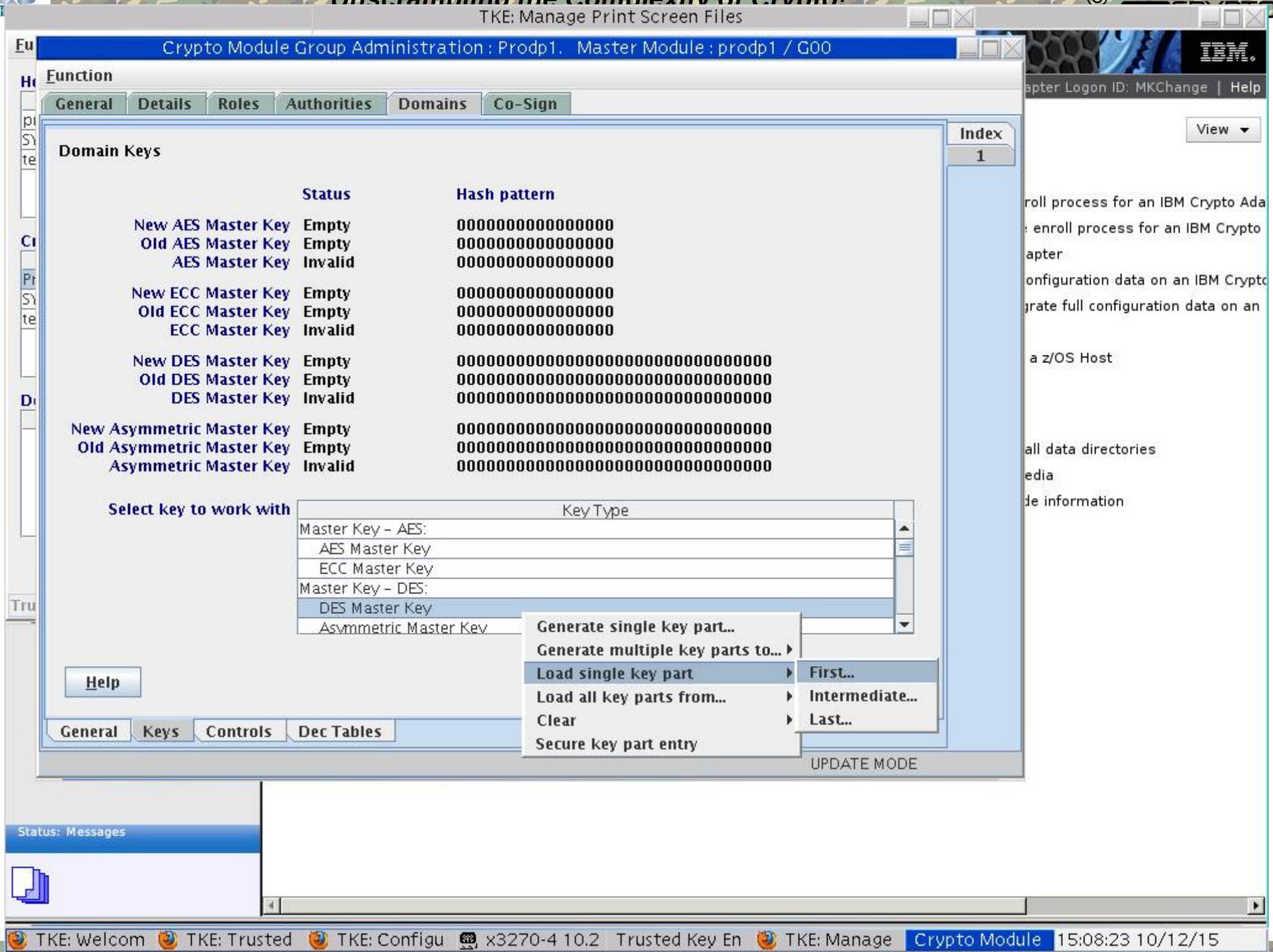



qsystke.wsclab.washington.ibm.com:0 (qsystke.wsclab.washington.ibm.com:0) - VNC Viewer
QSYSTKE: Trusted Key Entry Console Workplace (Version 9.0)
IBM Trusted Key Entry Console
Welcome
Trusted Key Entry
Service Management
Crypto Module Administration. Crypto Module : PEZ1 / 6C01 - Smart Card Readers Available
Function
General
Details
Roles
Authorities
Domains
Co-Sign
View
Index
67*
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
Help
Trusted Key Entry - Ready
Signature Key Loaded, Index: 99, Name: Default author...
Status: Messages
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


qsystke.wsclab.washington.ibm.com:0 (qsystke.wsclab.washington.ibm.com:0) - VNC Viewer
QSYSTKE: Trusted Key Entry Console Workplace (Version 9.0)
IBM Trusted Key Entry Console
Smart Card Readers Locked By: TKE Smart Card Utility Program | Crypto Adapter Logon ID: MKGRP | Help
Welcome
Trusted Key Entry
Service Manag
Trusted Key Entry (TKE Version)
View
TKE Smart Card Utility Program Version 9.0 - Smart Card Readers Available
File CA Smart Card TKE Smart Card EP11 Smart Card Crypto Adapter Help
Smart card reader 1
Card type: CA Smart Card v0.7
Card ID: 7DAE619DS
Card description: CA Admin Smart Card 1
PIN status: Ok
Authority or Administrator key:
Crypto Adapter Logon key:
Zone enroll status: Enrolled
Zone ID: 5B4F41F6
Zone description: WSC TKE 9.0
Zone key length: 2048
Alternate zone enroll status:
Alternate zone ID:
Alternate zone description:
Alternate zone key length:
Key parts:
Key type | Description | Origin | MDC-4 or CMAC | SHA-1 | ENC-ZERO | AES-VP or HMAC-VP | Control vector or key attributes | Length
Smart card reader 2
Card type: TKE Smart Card v0.16
Card ID: 96196D82S
Card description: TKE Card 1
PIN status: Ok
Authority or Administrator key: 50, KeyOfficer One
Crypto Adapter Logon key: Present
Zone enroll status: Enrolled
Zone ID: 5B4F41F6
Zone description: WSC TKE 9.0
Zone key length: 2048
Alternate zone enroll status: Not enrolled
Alternate zone ID:
Alternate zone description:
Alternate zone key length:
Key parts:
Key type | Description | Origin | MDC-4 or CMAC | SHA-1 | ENC-ZERO | AES-VP or HMAC-VP | Control vector or key attributes | Length
ICSF AES ... | AES MK Part 1... | Crypto ... | | | | 50DD73 | | 32
ICSF DES ... | DES MK Part ... | Crypto ... | F27B67 | EC4F60 | 6B510E | | | 16
ICSF ECC ... | ECC MK Part 1... | Crypto ... | | | | FB0039 | | 32
ICSF RSA ... | RSA MK Part 1 | Crypto ... | E7E460 | C0C292 | 46A06B | | | 24
Main Menu
Status: Messages
QSYSTKE: Welcome to the Trusted Key Entry
QSYSTKE: Trusted Key Entry Console Workpl
TKE Smart Card Utility Program Version 9.0 -
12:00:30 08/01/18

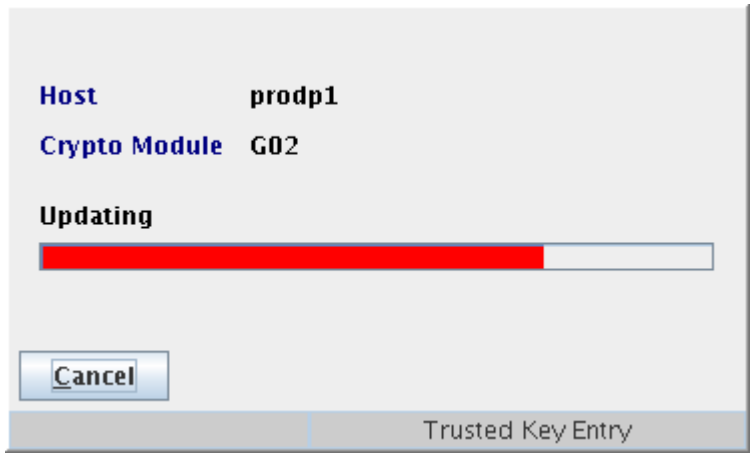

qsystke.wsclab.washington.ibm.com:0 (qsystke.wsclab.washington.ibm.com:0) - VNC Viewer
QSYSTKE: Trusted Key Entry Console Workplace (Version 9.0)
IBM Trusted Key Entry Console
Smart Card Readers Locked By: Trusted Key Entry | Crypto Adapter Logon ID: MKGRP | Help
Welcome
Trusted Key Entry
Service Management
Trusted Key Entry (TKE Version)
View
Trusted Key Entry - Smart Card Readers Available
Function Utilities Preferences Help
Hosts
Host ID
Description
Crypto Modules
Host ID
CM index
Status
Description
Crypto Module Administration. Crypto Module : PEZ1 / 6C01 - Smart Card Readers Available
Function
General Details Roles Authorities Domains Co-Sign
Domain Keys
Index
67*
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
DES Master Key Valid
New ECC (APKA) Master Key Empty
Old ECC (APKA) Master Key Empty
ECC (APKA) Master Key Not valid
New RSA Master Key Empty
Old RSA Master Key Empty
RSA Master Key Not valid
Load All New Master Keys
Specify if any new master keys are to be cleared.
AES master key
DES master key
ECC (APKA) master key
RSA master key
Continue
Cancel
Help
Select key to work with
Symmetric Master Ke
AES Master Key
DES Master Key
Asymmetric Master Keys:
ECC (APKA) Master Key
RSA Master Key
Operational key - AES:
DATA
EXPORTER
Help
General Keys Controls-Desc Controls-ACP Dec Tables PINs Certificates
UPDATE MODE
QSYSTKE: Welcome to the
QSYSTKE: Trusted Key Ent
Trusted Key Entry - Smart
Crypto Module Administrat
Load All New Master Keys
10:36:35 07/25/18

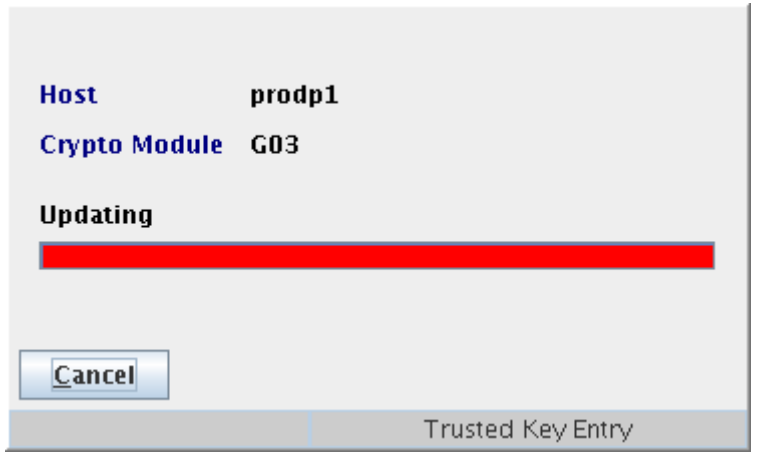

qsystke.wsclab.washington.ibm.com:0 (qsystke.wsclab.washington.ibm.com:0) - VNC Viewer
QSYSTKE: Trusted Key Entry Console Workplace (Version 9.0)
IBM Trusted Key Entry Console
Smart Card Readers Locked By: Trusted Key Entry | Crypto Adapter Logon ID: MKGRP | Help
Welcome
Trusted Key Entry
Service Management
Trusted Key Entry (TKE Version)
View
Trusted Key Entry - Smart Card Readers Available
Function Utilities Preferences Help
Hosts
Host ID
Description
Crypto Modules
Host ID
CM index
Status
Description
Crypto Module Administration. Crypto Module : PEZ1 / 6C01 - Smart Card Readers Available
Function
General Details Roles Authorities Domains Co-Sign
Domain Keys
Index
67*
New AES Mast
Old AES Mast
AES Mast
New DES Mast
Old DES Mast
DES Mast
New ECC (APKA) Mast
Old ECC (APKA) Mast
ECC (APKA) Mast
New RSA Mast
Old RSA Mast
RSA Mast
Select key to wo
Select key part from smart card
Card ID 96196D82S
Zone description WSC TKE 9.0
Card description TKE Card 1
Card contents
Key type
Description
Origin
MDC4 or CMAC
SHA1
ENC-Zero
ICSF AES master key part
AES MK Part 1 - 7/25/18
Crypto adapter
OK
Cancel
Help
Trusted Key Entry
Help
General Keys Controls-Desc Controls-ACP Dec Tables PINs Certificates
Getting key values...
UPDATE MODE
QSYSTKE: Welcome to the
QSYSTKE: Trusted Key Ent
Trusted Key Entry - Smart
Crypto Module Administrat
Select key part from smar
10:39:21 07/25/18


TKE: Manage Print Screen Files
Crypto Module Group Administration : Prodp1. Master Module : prodp1 / G00
Function
General
Details
Roles
Authorities
Domains
Co-Sign
Index
1
Domain Keys
Status
Hash pattern
New AES Master Key Empty 0000000000000000
Old AES Master Key Empty 0000000000000000
AES Master Key Invalid 0000000000000000
New ECC Master Key Empty 0000000000000000
Old ECC Master Key Empty 0000000000000000
ECC Master Key Invalid 0000000000000000
New DES Master Key Empty 00000000000000000000000000000000
Old DES Master Key Empty 00000000000000000000000000000000
DES Master Key Invalid 00000000000000000000000000000000
New Asymmetric Master Key Empty 00000000000000000000000000000000
Old Asymmetric Master Key Empty 00000000000000000000000000000000
Asymmetric Master Key Invalid 00000000000000000000000000000000
Select key to work with
Key Type
Master Key - AES:
AES Master Key
ECC Master Key
Master Key - DES:
DES Master Key
Asymmetric Master Key
Generate single key part...
Generate multiple key parts to...
Load single key part
Load all key parts from...
Clear
Secure key part entry
First...
Intermediate...
Last...
Help
General
Keys
Controls
Dec Tables
UPDATE MODE
Status: Messages
TKE: Welcom
TKE: Trusted
TKE: Configu
x3270-4 10.2
Trusted Key En
TKE: Manage
Crypto Module
15:08:23 10/12/15

© MAINFRAME CRYPTO

Each crypto module gets updated



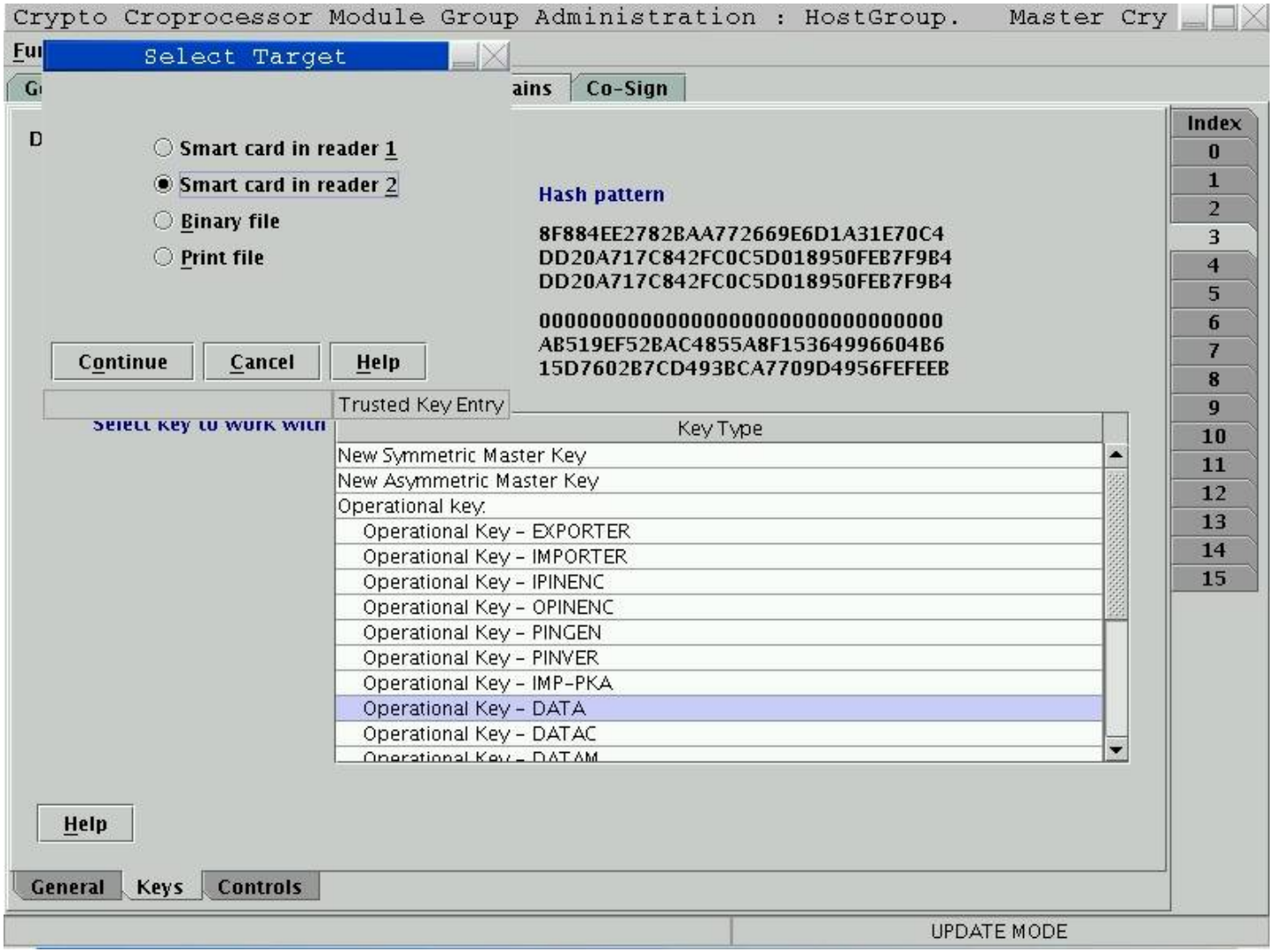


Finish the MK Change (without the TKE)

```
------------------------- ICSF - Key Data Set Management -----------------------
OPTION ===>

Enter the number of the desired option.

  1  CKDS MANAGEMENT -  Perform Cryptographic Key Data Set (CKDS)
                        functions including master key management
  2  PKDS MANAGEMENT -  Perform Public Key Data Set (PKDS)
                        functions including master key management
  3  TKDS MANAGEMENT -  Perform PKCS #11 Token Data Set (TKDS)
                        functions including master key management
  4  SET MK          -  Set master keys

Press ENTER to go to the selected option.
```

```
---------------------------- ICSF - CKDS Management ----------------------------
OPTION ===>

Enter the number of the desired option.

  1  CKDS OPERATIONS    -  Initialize a CKDS, activate a different CKDS,
                           (Refresh), or update the header of a CKDS and make
                           it active
  2  REENCIPHER CKDS    -  Reencipher the CKDS prior to changing a symmetric
                           master key
  3  CHANGE SYM MK      -  Change a symmetric master key and activate the
                           reenciphered CKDS
  4  COORDINATED CKDS REFRESH - Perform a coordinated CKDS refresh
  5  COORDINATED CKDS CHANGE MK - Perform a coordinated CKDS change master key
  6  COORDINATED CKDS CONVERSION - Convert the CKDS to use KDSR record format
  7  CKDS KEY CHECK     - Check key tokens in the active CKDS for format errors

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

Loading Operational Keys



Completing the Operational Key Load

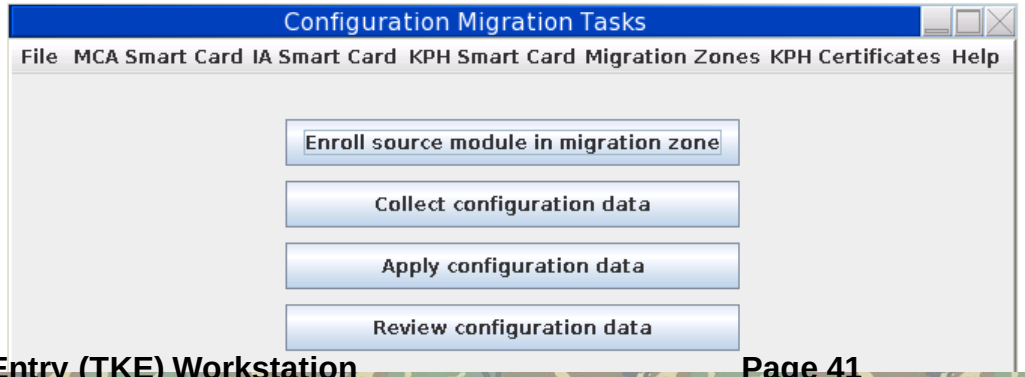
```
------------------------- ICSF Coprocessor Management -------- Row 1 to 2 of 2
COMMAND ===>                                                  SCROLL ===> CSR

 Select the cryptographic features to be processed and press ENTER.
 Action characters are: A, D, E, K, R, S and V. See the help panel for details.

  CRYPTO    SERIAL
  FEATURE   NUMBER    STATUS                AES   DES   ECC   RSA   P11
  -------   -------   -------------------   ---   ---   ---   ---   ---
k   4C01    16C8X376  Active                 A     A     A     A
.   4C03    16C8P352  Active                 A     A     A     A
******************************** Bottom of data ********************************
```

```
------------------------- ICSF - Operational Key Load -------------------------
COMMAND ===>

Coprocessor selected for new key:  4C01
CKDS Name:  SHARPLEX.CRYPTO.CKDS

Enter the key label.

Key label
===>

Control Vector ===> YES  YES or NO
Press ENTER to process.
Press END   to exit to the previous menu.
```

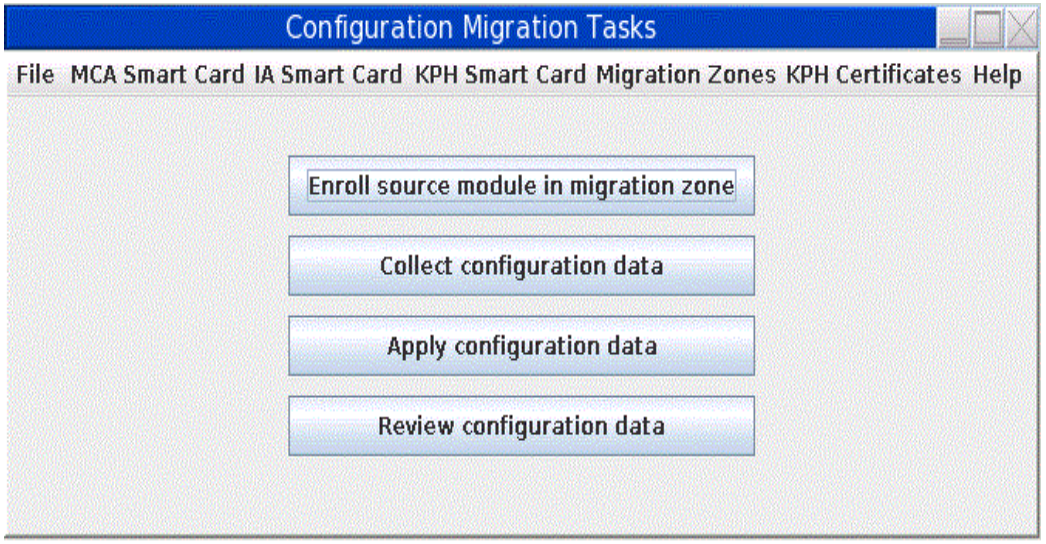
Migration Wizard

- Collect configuration data from one Host Crypto Module and apply to another Host Crypto Module

Initial Screen



Full Function Migration Wizard



1) Connect the TKE to the source and destination systems (does not have to be at the same time)

2) Collect and Apply the Crypto Card Configuration using TKE Migration Wizard

z14

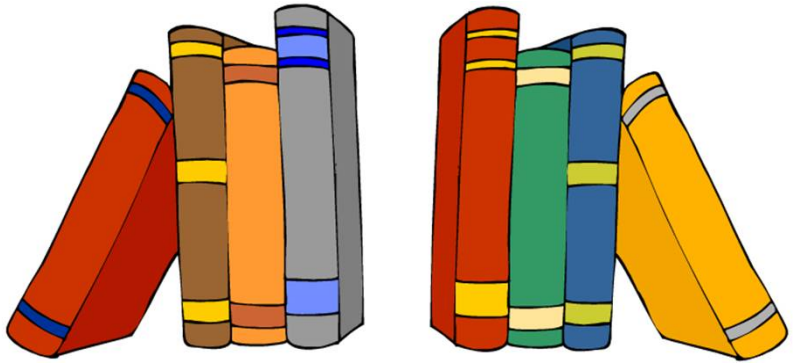
3) Apply the Crypto Card Configuration back to the Source card to restore data

z13

TKE Exclusives

- Secure loading of master keys
  - Key material is always protected
  - Two man rule (Four-eyes principal)
- Migration Wizard
- Enabling/Disabling ACPs
  - 24-Byte DES-MK
- Loading MKs for inactive LPARs
- PCI-HSM Enablement
- Loading PIN Decimalization Tables
- Loading MKs for Linux guests
- Loading P11-MK

References



- IBM Pubs
  - SC14-7511 TKE Workstation User's Guide z/OS V2.1 (TKE 7.3/8.0)
  - SA23-2211 TKE Workstation User's Guide z/OS V1.13 (TKE 7.2)
- IBM Redbooks
  - SG24-7848 System z Crypto and TKE Update (2011)
  - SG24-7123 z9-109 Crypto and TKE V5 Update (2005)
  - SG24-6499 zSeries Trusted Key Entry (TKE) V4.2 Update (2004)
  - SG24-5455 Exploiting S/390 Hardware Cryptography with Trusted Key Entry (1999)
  - REDP-5305 Streamline Management of the IBM z Systems Host Cryptographic Module Using IBM Trusted Key Entry

On the Web

- Techdocs – www.ibm.com/support/techdocs
  - TD106231 – TKE Hardware Support and Migration Information
  - Or search on ‘crypto’

TKE Videos

- www.youtube.com – search on

  'IBM Trusted Key Entry Workstation'

- For a list of videos see https://www.ibm.com/partnerworld/wps/servlet/mem/ContentHandler/ZSV03661USEN/lc=en_ALL_ZZ

Questions