Trusted Key Entry Workstation (Part 2)

Greg Boyd

gregboyd@mainframecrypto.com

January 2016

Copyrights . . .

- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 10 years

. . . And Trademarks

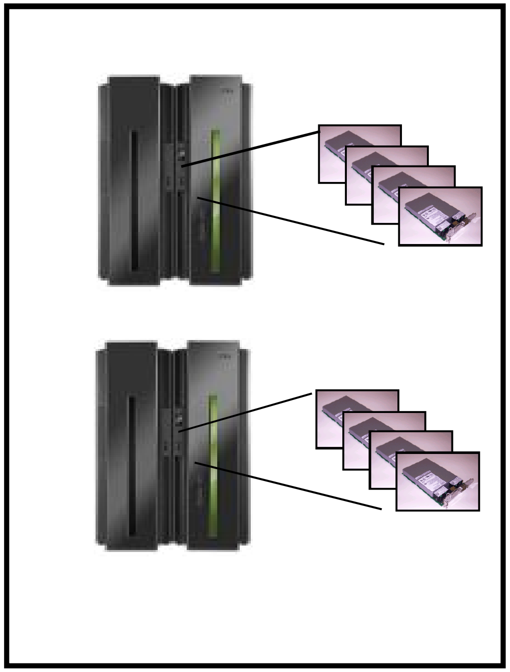
-
- All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. IBM, System z, zEnterprise and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks 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

- Trusted Key Entry Workstation Description
- Smart Cards
- Host Setup
- Privileged Modes
- Profiles, Roles & Authorities
- TKE Setup
- TKE Utilities and Apps

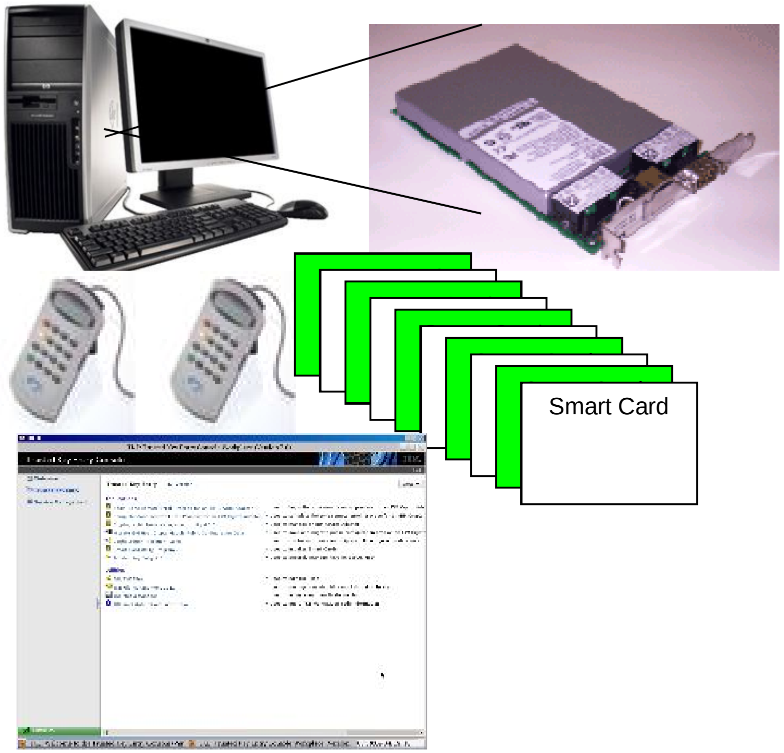
TKE – What does it do?

- Secure Key Entry
  - Master keys or operational keys
  - Key material generated in hardware and never exists in the clear, outside of the tamper hardware (security)
  - Can provide dual control
- Manage host crypto modules
  - As domain groups
  - Across CECs
  - Migration Wizard
  - Wizard like feature for loading master keys in one task

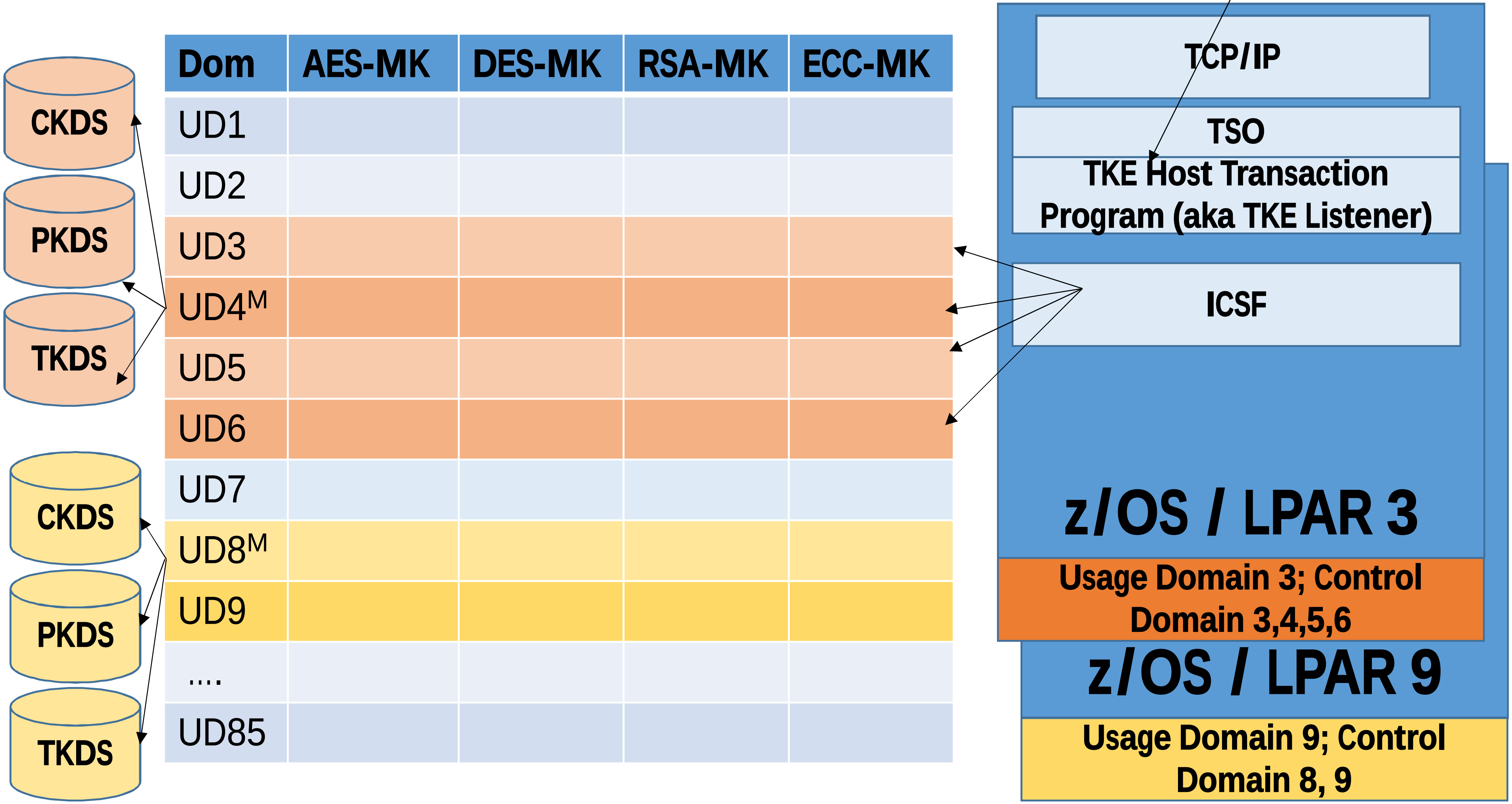


TKE - Components

- Workstation with a crypto coprocessor
  - Intel Workstation with an embedded operating system
  - Cryptographic coprocessor
  - A TKE application (Java)
  - Optional TKE smart card support
    - Readers and 20 smart cards
    - 10 Additional smart cards



Control Domains



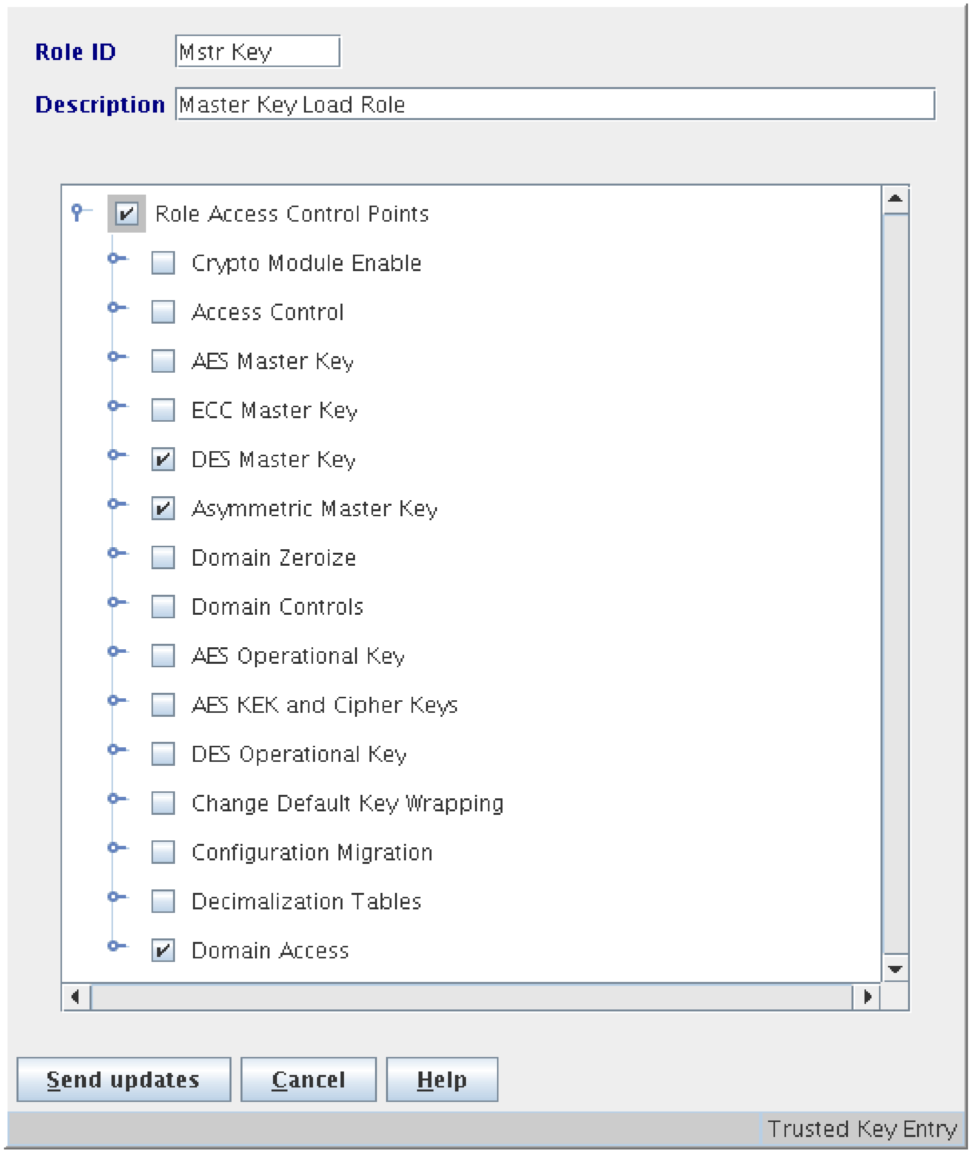
Dom	AES-MK	DES-MK	RSA-MK	ECC-MK
UD1				
UD2				
UD3				
UD4^M				
UD5				
UD6				
UD7				
UD8^M				
UD9				
....				
UD85				

CKDS
PKDS
TKDS
CKDS
PKDS
TKDS
TCP/IP
TSO
TKE Host Transaction Program (aka TKE Listener)
ICSF
z/OS / LPAR 3
Usage Domain 3; Control Domain 3,4,5,6
z/OS / LPAR 9
Usage Domain 9; Control Domain 8, 9

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

Role Definitions

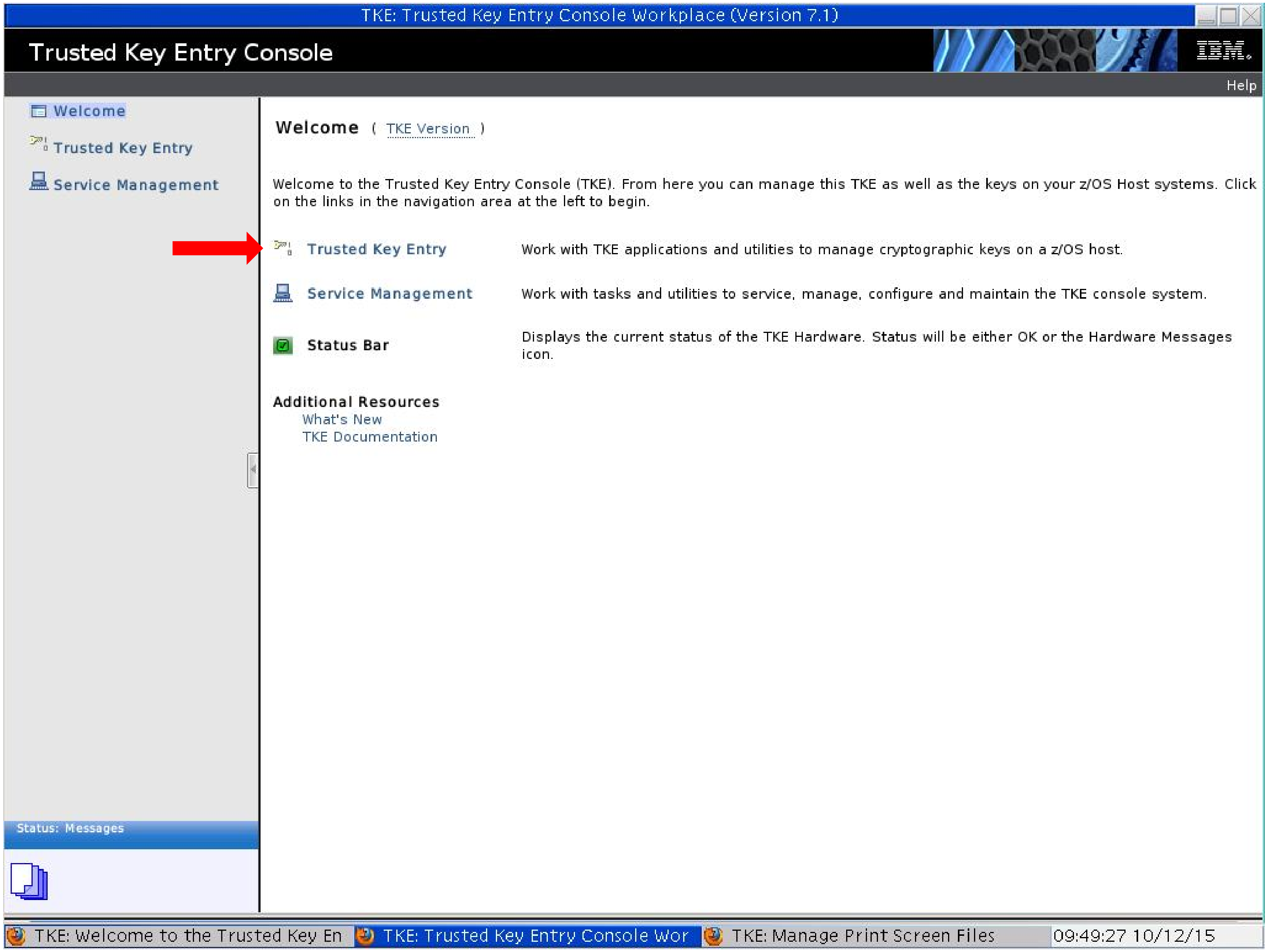


Role ID: Mstr Key

Description: Master Key Load Role

- ☑ Role Access Control Points
  - □ Crypto Module Enable
  - □ Access Control
  - □ AES Master Key
  - □ ECC Master Key
  - ☑ DES Master Key
  - ☑ Asymmetric Master Key
  - □ Domain Zeroize
  - □ Domain Controls
  - □ AES Operational Key
  - □ AES KEK and Cipher Keys
  - □ DES Operational Key
  - □ Change Default Key Wrapping
  - □ Configuration Migration
  - □ Decimalization Tables
  - ☑ Domain Access

TKE Welcome Screen



TKE: Trusted Key Entry Console Workplace (Version 7.1)

Trusted Key Entry Console

Welcome (TKE Version)

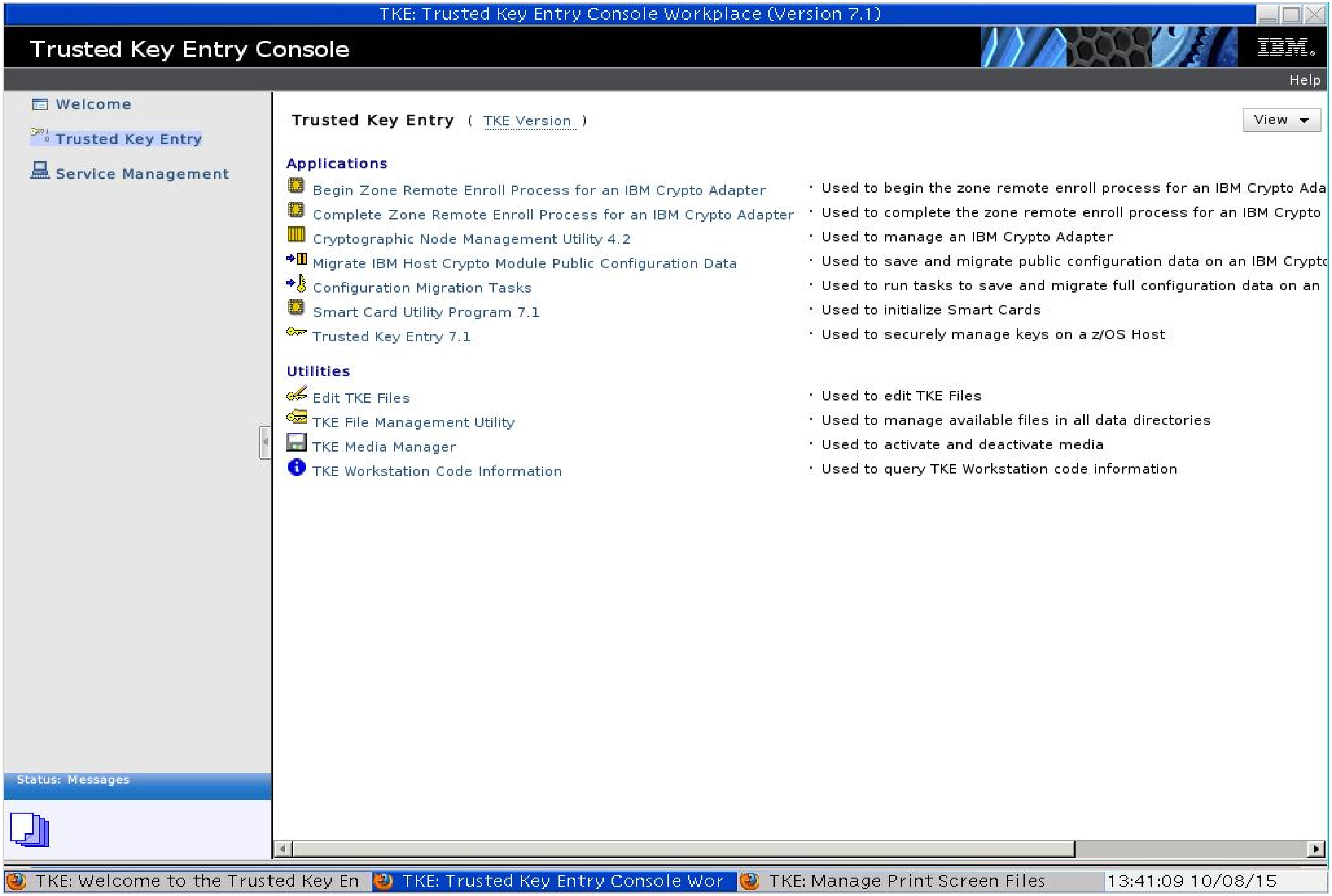
Welcome to the Trusted Key Entry Console (TKE). From here you can manage this TKE as well as the keys on your z/OS Host systems. Click on the links in the navigation area at the left to begin.

Trusted Key Entry	Work with TKE applications and utilities to manage cryptographic keys on a z/OS host.
Service Management	Work with tasks and utilities to service, manage, configure and maintain the TKE console system.
Status Bar	Displays the current status of the TKE Hardware. Status will be either OK or the Hardware Messages icon.

Additional Resources
What's New
TKE Documentation

TKE: Welcome to the Trusted Key En
TKE: Trusted Key Entry Console Wor
TKE: Manage Print Screen Files
09:49:27 10/12/15

TKE 7.1 Main Menu


TKE: Trusted Key Entry Console Workplace (Version 7.1)
Trusted Key Entry Console
IBM.
Help
Welcome
Trusted Key Entry
Service Management
View
Status: Messages
TKE: Welcome to the Trusted Key En
TKE: Trusted Key Entry Console Wor
TKE: Manage Print Screen Files
13:41:09 10/08/15

Trusted Key Entry (TKE Version)

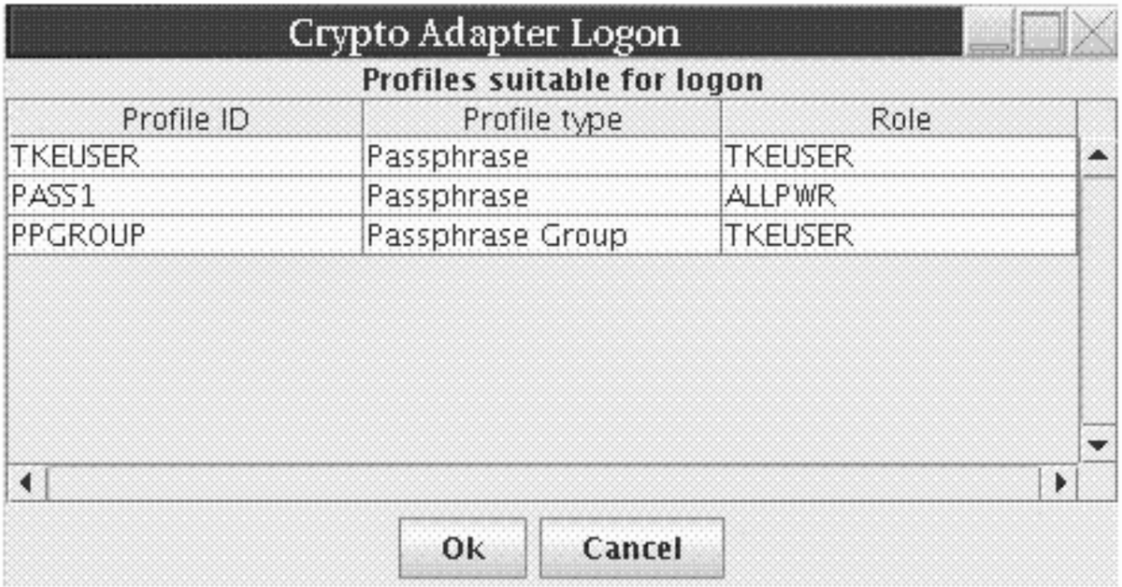
Applications

Begin Zone Remote Enroll Process for an IBM Crypto Adapter	· Used to begin the zone remote enroll process for an IBM Crypto Ada
Complete Zone Remote Enroll Process for an IBM Crypto Adapter	· Used to complete the zone remote enroll process for an IBM Crypto
Cryptographic Node Management Utility 4.2	· Used to manage an IBM Crypto Adapter
Migrate IBM Host Crypto Module Public Configuration Data	· Used to save and migrate public configuration data on an IBM Crypto
Configuration Migration Tasks	· Used to run tasks to save and migrate full configuration data on an
Smart Card Utility Program 7.1	· Used to initialize Smart Cards
Trusted Key Entry 7.1	· Used to securely manage keys on a z/OS Host

Utilities

Edit TKE Files	· Used to edit TKE Files
TKE File Management Utility	· Used to manage available files in all data directories
TKE Media Manager	· Used to activate and deactivate media
TKE Workstation Code Information	· Used to query TKE Workstation code information

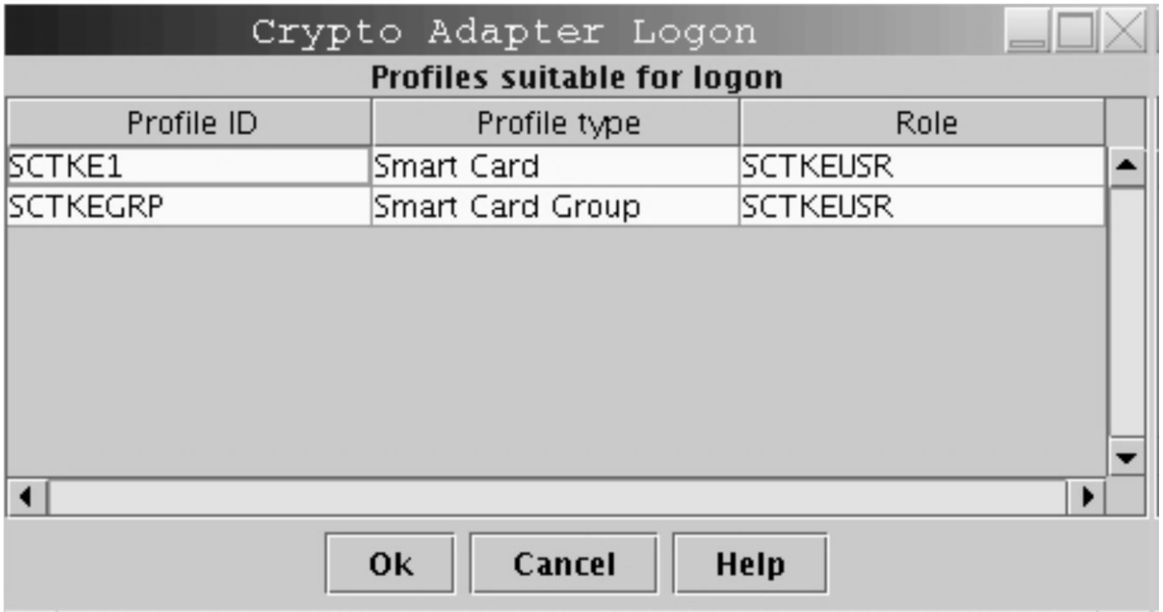
Crypto Adapter Logon



Profiles suitable for logon

Profile ID	Profile type	Role
TKEUSER	Passphrase	TKEUSER
PASS1	Passphrase	ALLPWR
PPGROUP	Passphrase Group	TKEUSER

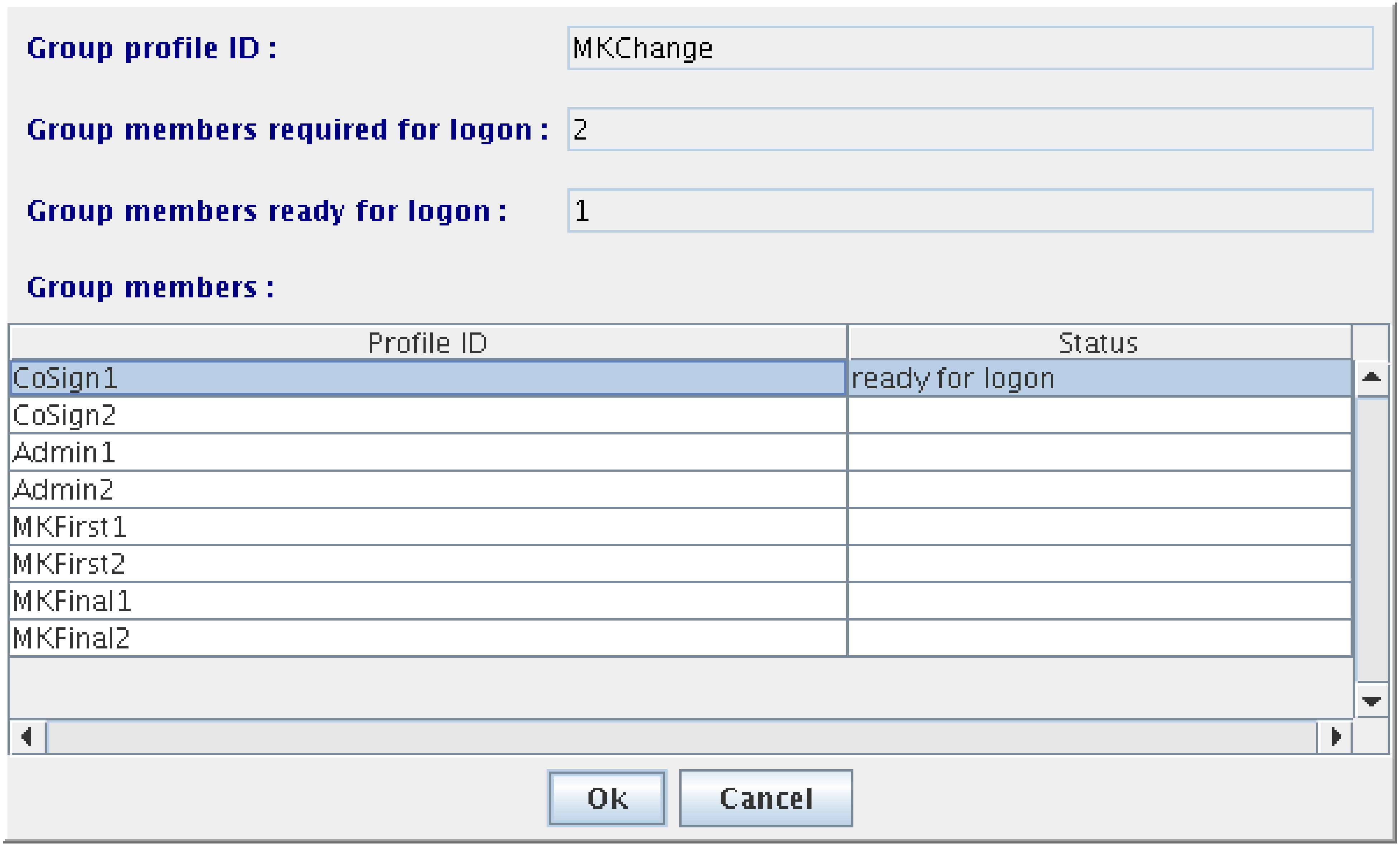
- Group Profile
    - 1 to 10 members
    - Passphrase or Smart Card Group
    - Minimum # of members that must authenticate



Profiles suitable for logon

Profile ID	Profile type	Role
SCTKE1	Smart Card	SCTKEUSR
SCTKEGRP	Smart Card Group	SCTKEUSR

Group Profiles



Group profile ID : MKChange

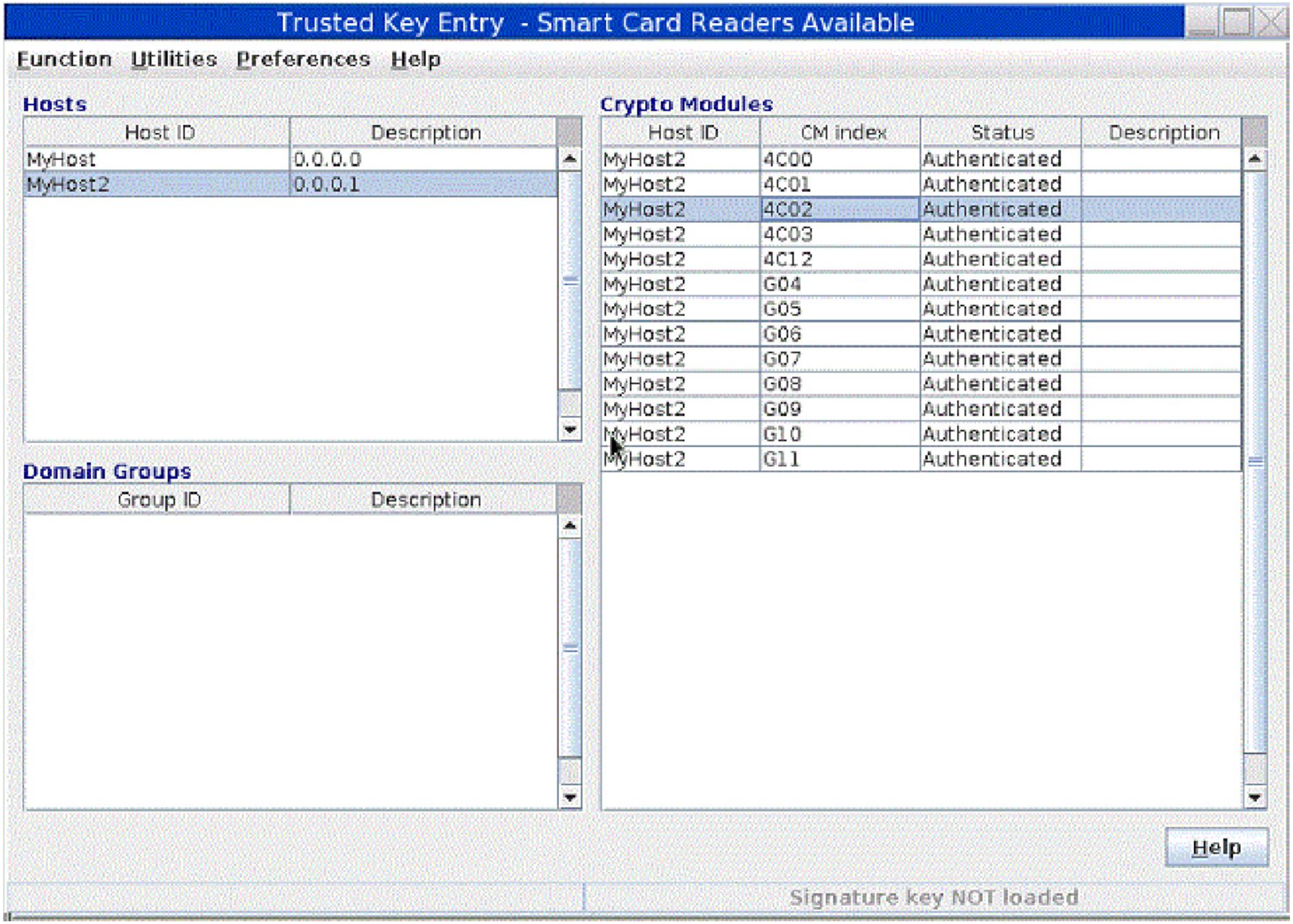
Group members required for logon : 2

Group members ready for logon : 1

Group members :

Profile ID	Status
CoSign1	ready for logon
CoSign2	
Admin1	
Admin2	
MKFirst1	
MKFirst2	
MKFinal1	
MKFinal2	

TKE 8.0 Main Window



Trusted Key Entry - Smart Card Readers Available
Function Utilities Preferences Help

Hosts

Host ID	Description
MyHost	0.0.0.0
MyHost2	0.0.0.1

Domain Groups

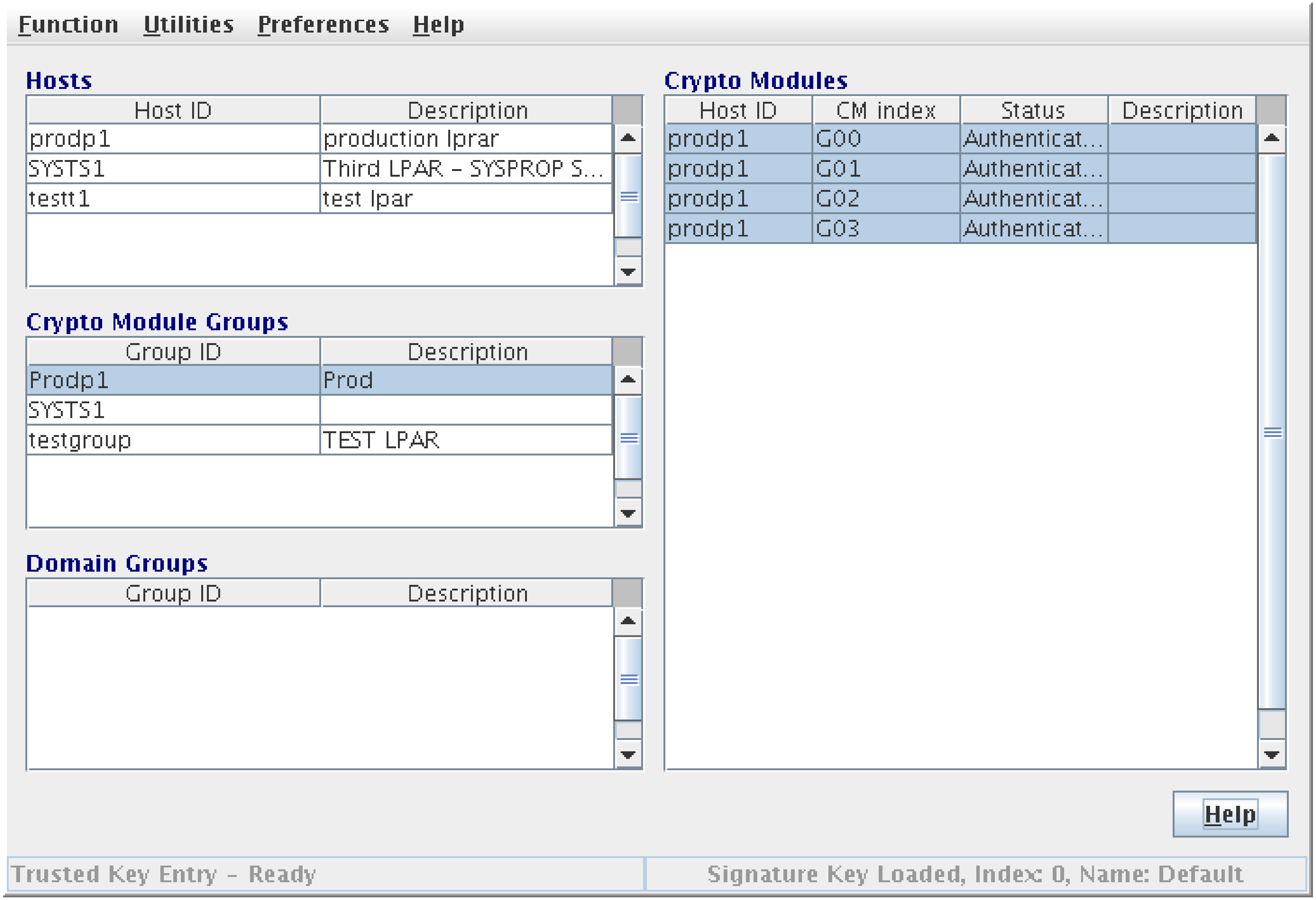
Group ID	Description

Crypto Modules

Host ID	CM index	Status	Description
MyHost2	4C00	Authenticated	
MyHost2	4C01	Authenticated	
MyHost2	4C02	Authenticated	
MyHost2	4C03	Authenticated	
MyHost2	4C12	Authenticated	
MyHost2	G04	Authenticated	
MyHost2	G05	Authenticated	
MyHost2	G06	Authenticated	
MyHost2	G07	Authenticated	
MyHost2	G08	Authenticated	
MyHost2	G09	Authenticated	
MyHost2	G10	Authenticated	
MyHost2	G11	Authenticated	

Signature key NOT loaded

TKE 7.1 Main Window



Hosts

Host ID	Description
prodp1	production lprar
SYSTS1	Third LPAR - SYSPROP S...
testt1	test lpar

Crypto Module Groups

Group ID	Description
Prodp1	Prod
SYSTS1	
testgroup	TEST LPAR

Domain Groups

Group ID	Description

Crypto Modules

Host ID	CM index	Status	Description
prodp1	G00	Authenticat...	
prodp1	G01	Authenticat...	
prodp1	G02	Authenticat...	
prodp1	G03	Authenticat...	

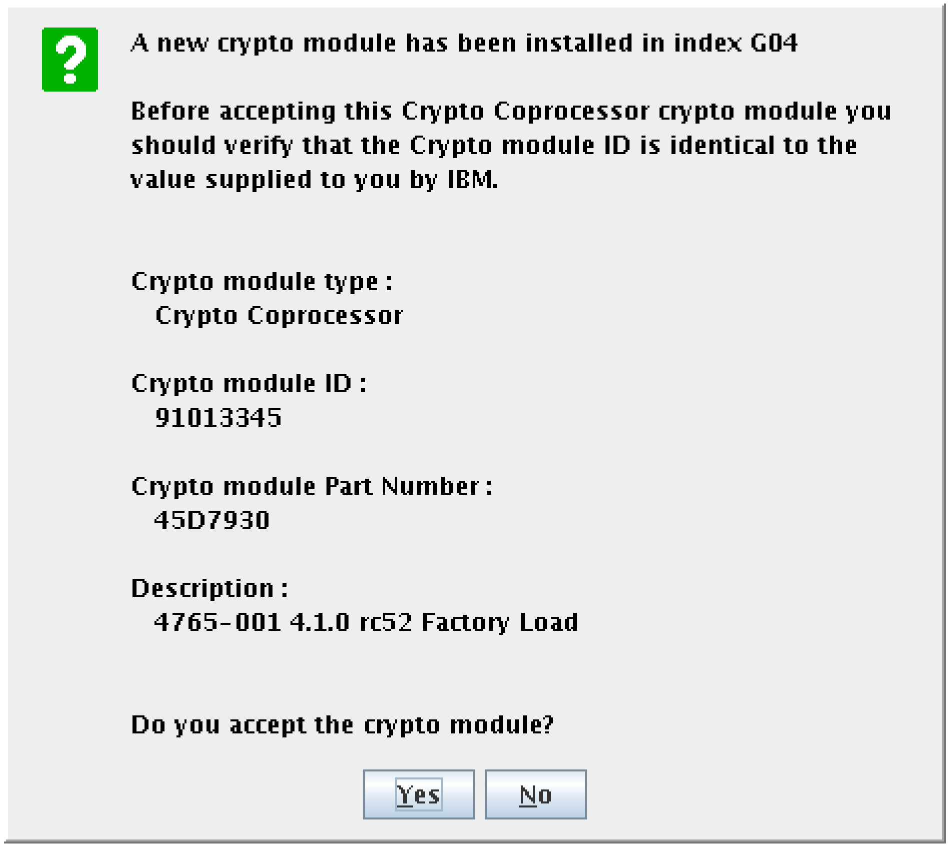
Trusted Key Entry - Ready

Signature Key Loaded, Index: 0, Name: Default

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)
- Crypto Module Group – perform operations on a set of crypto modules as you would a single crypto module*

Verify crypto modules



A new crypto module has been installed in index G04

Before accepting this Crypto Coprocessor crypto module you should verify that the Crypto module ID is identical to the value supplied to you by IBM.

Crypto module type :
Crypto Coprocessor

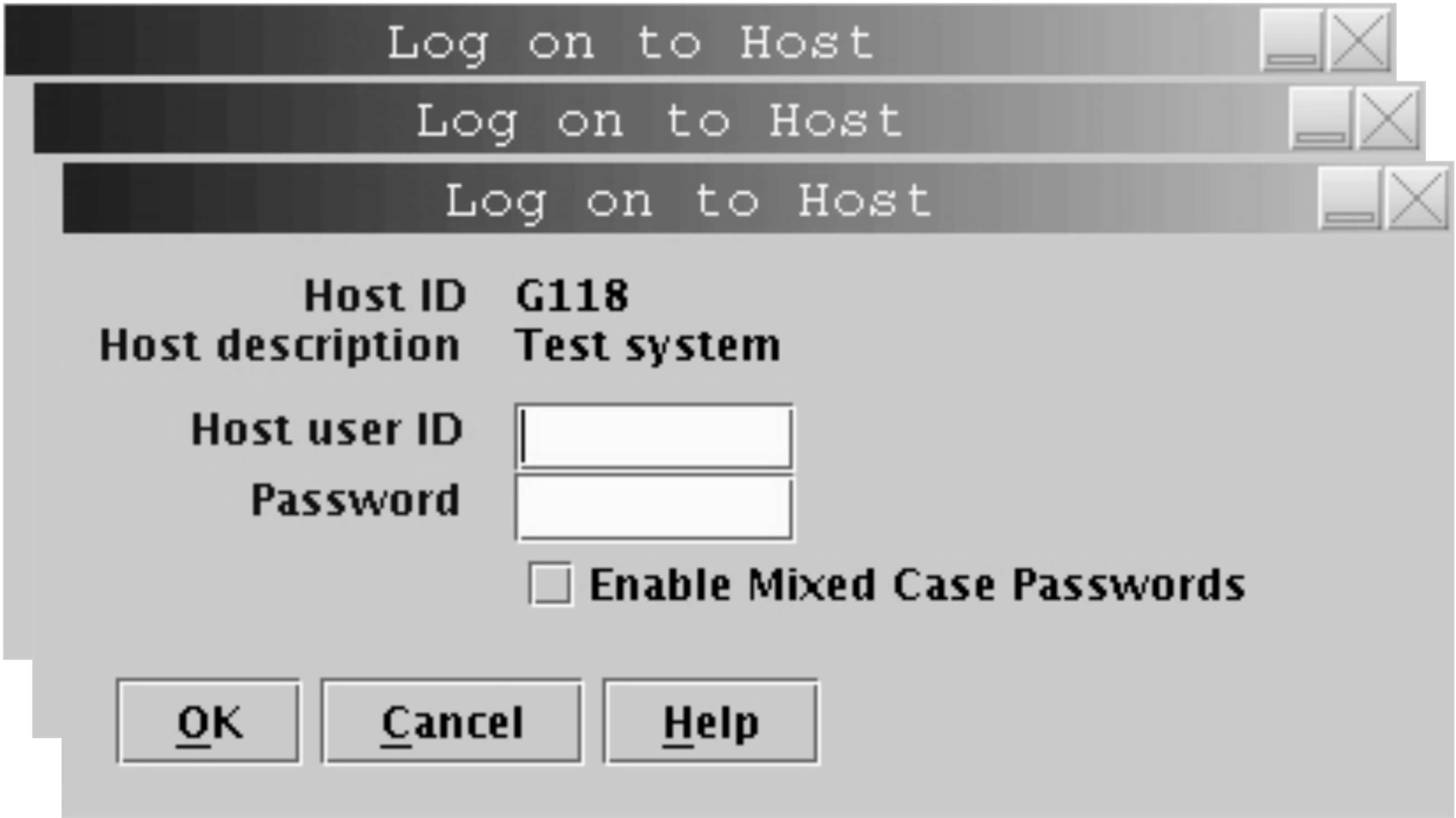
Crypto module ID :
91013345

Crypto module Part Number :
45D7930

Description :
4765-001 4.1.0 rc52 Factory Load

Do you accept the crypto module?

Logon to the Host(s)



Log on to Host

Log on to Host

Log on to Host

Host ID G118

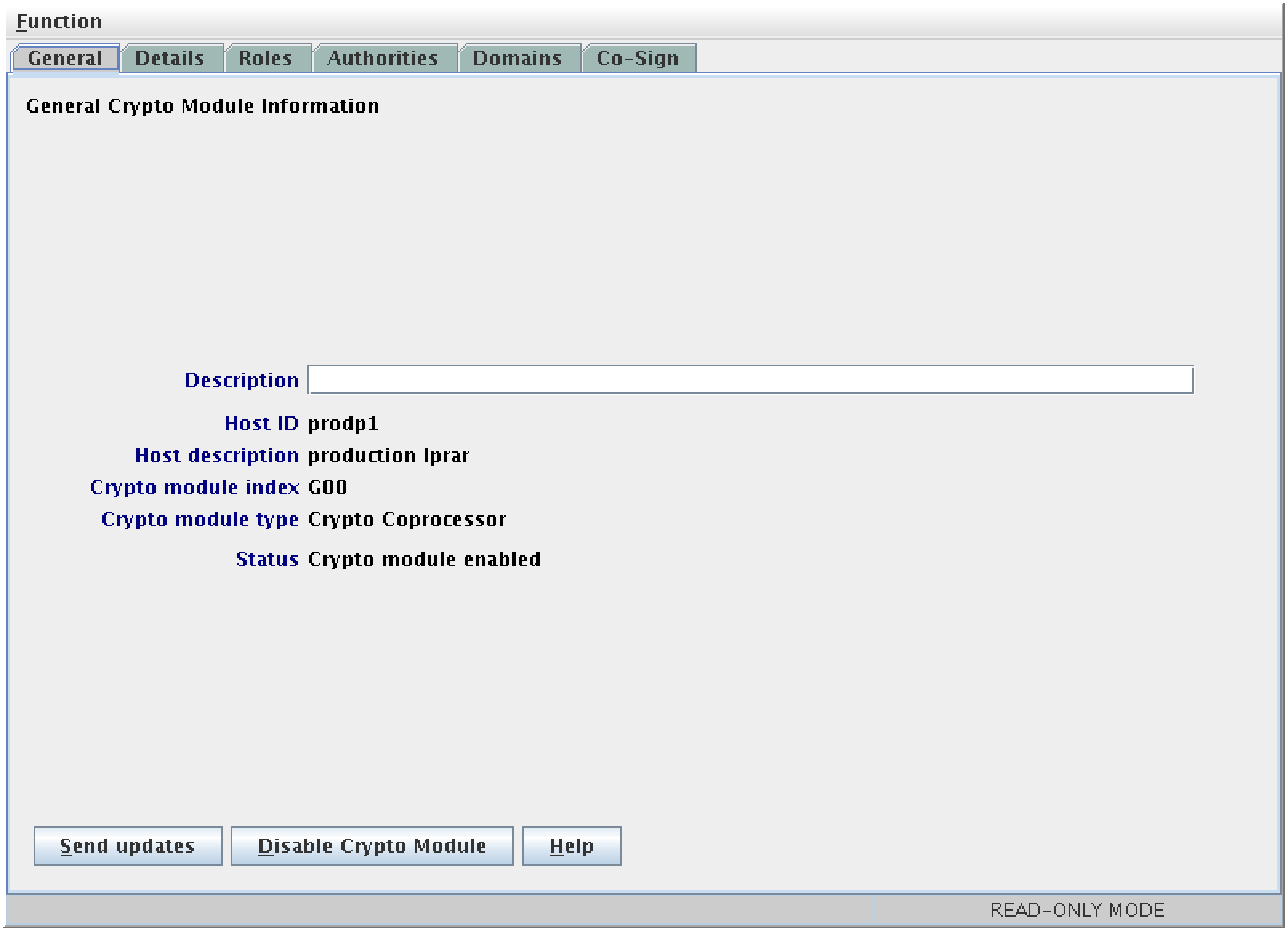
Host description Test system

Host user ID

Password

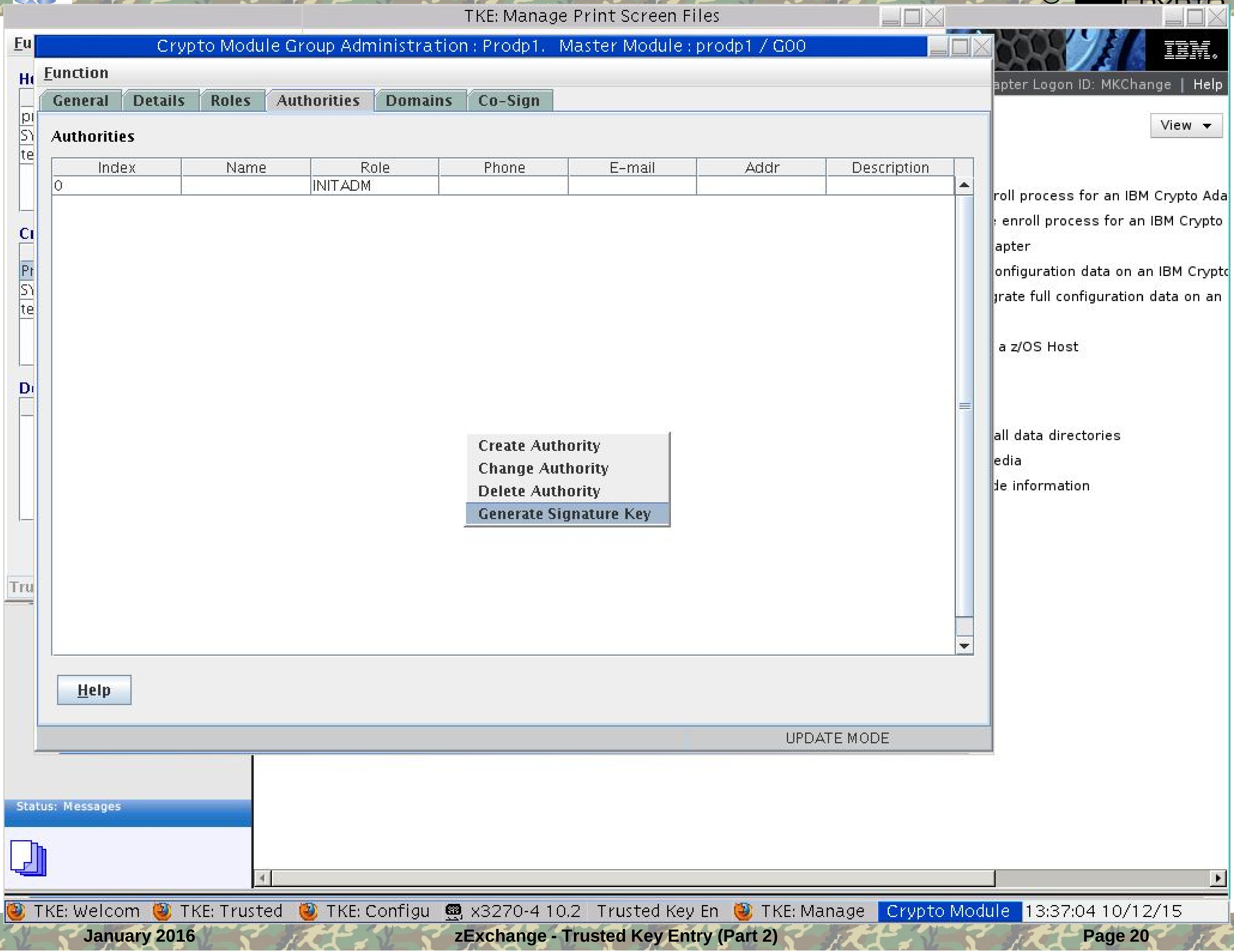
□ Enable Mixed Case Passwords

CCA Crypto Module Notebook



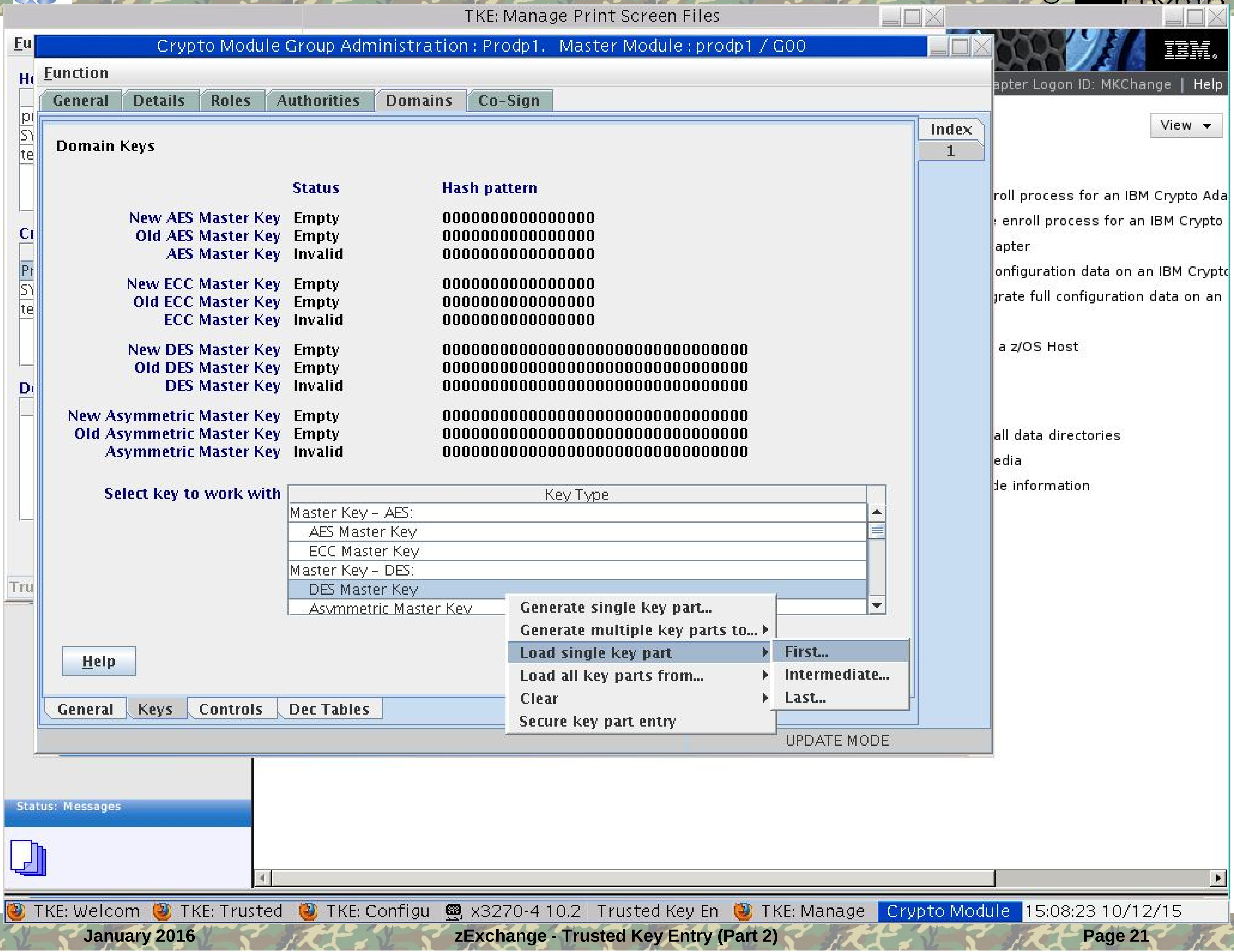
General Crypto Module Information

Description	
Host ID	prodp1
Host description	production lprar
Crypto module index	G00
Crypto module type	Crypto Coprocessor
Status	Crypto module enabled



Authorities

Index	Name	Role	Phone	E-mail	Addr	Description
0		INITADM				



Crypto Module Group Administration : Prodp1.   Master Module : prodp1 / G00

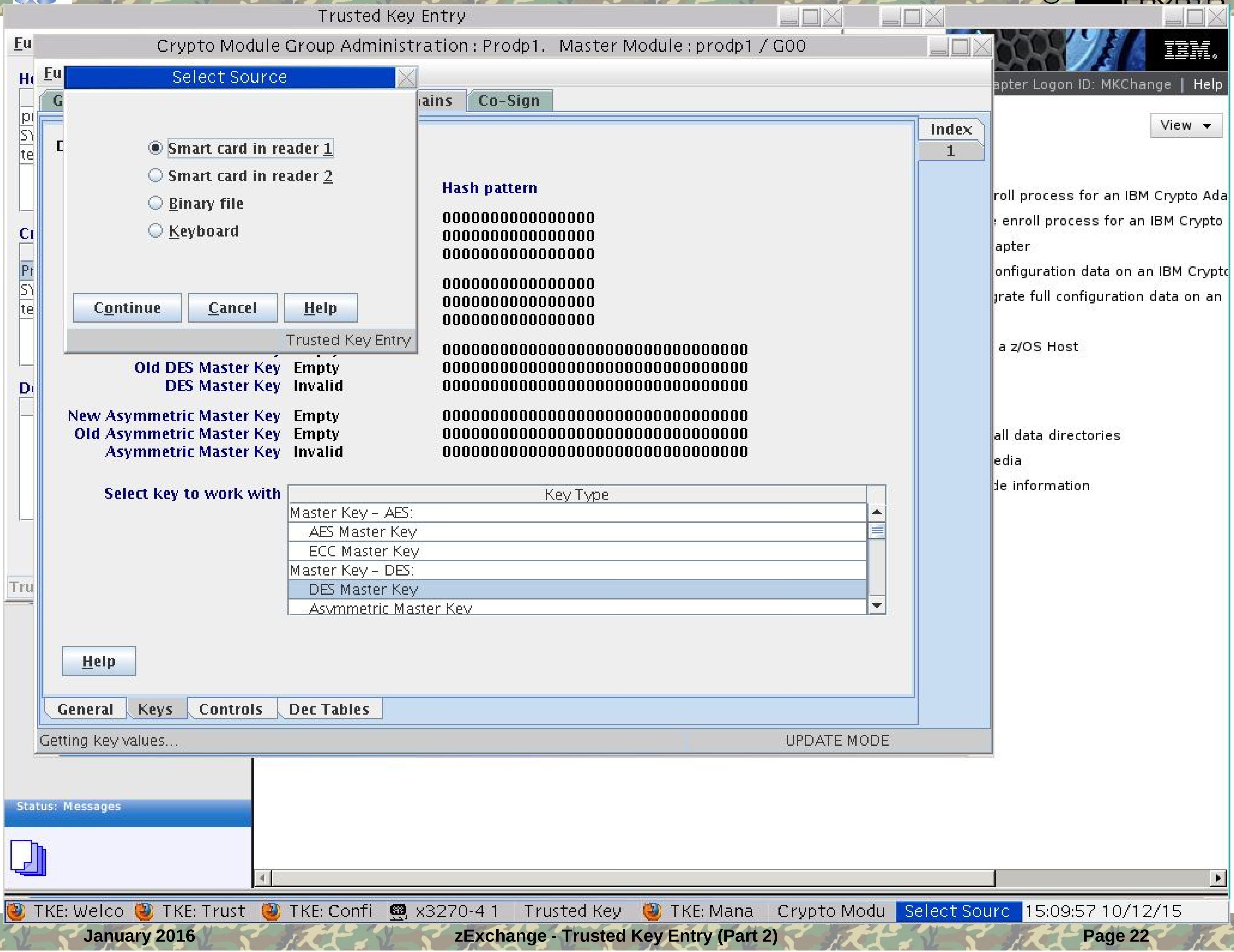
Domain Keys

	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

UPDATE MODE



Trusted Key Entry

Crypto Module Group Administration : Prodp1.   Master Module : prodp1 / G00

Select Source

● Smart card in reader 1
○ Smart card in reader 2
○ Binary file
○ Keyboard

Continue   Cancel   Help

Trusted Key Entry

Hash pattern

0000000000000000
0000000000000000
0000000000000000

0000000000000000
0000000000000000
0000000000000000

		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

Help

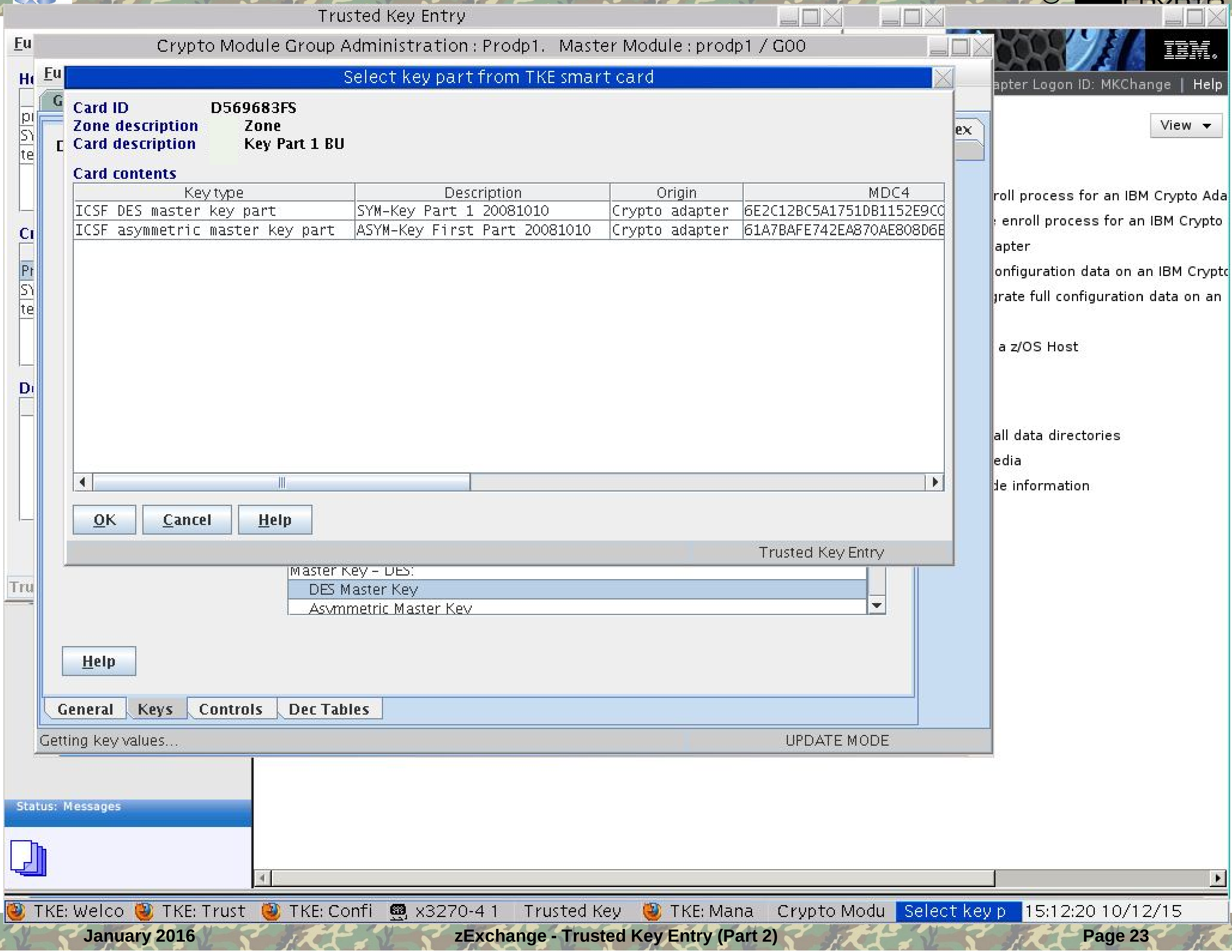
Getting key values...   UPDATE MODE

apter Logon ID: MKChange | Help

roll process for an IBM Crypto Ada
enroll process for an IBM Crypto
apter
onfiguration data on an IBM Crypto
grate full configuration data on an
a z/OS Host
all data directories
edia
de information

Status: Messages

15:09:57 10/12/15



Trusted Key Entry

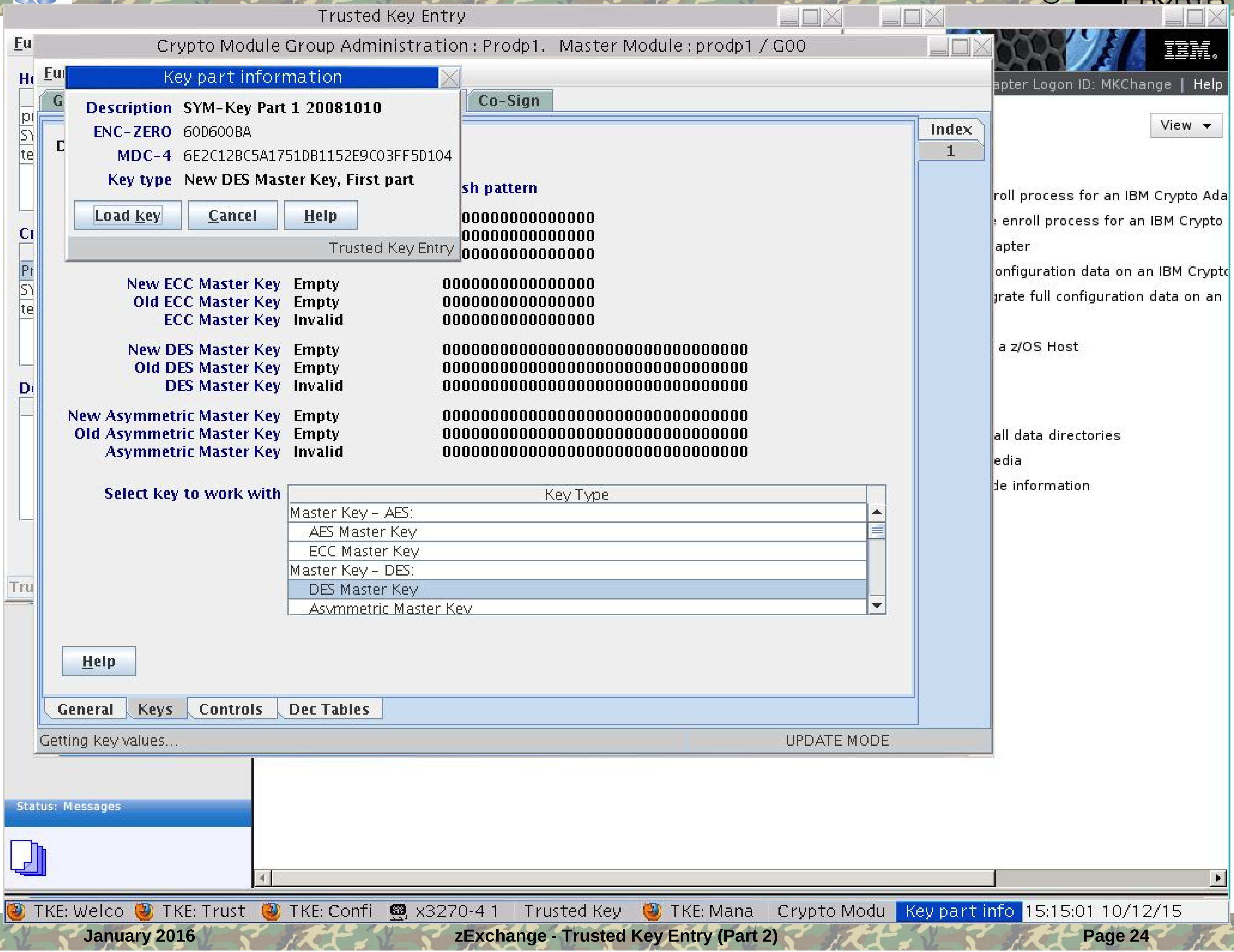
Crypto Module Group Administration : Prodp1.   Master Module : prodp1 / G00

Select key part from TKE smart card

Card ID D569683FS
Zone description Zone
Card description Key Part 1 BU

Card contents

Key type	Description	Origin	MDC4
ICSF DES master key part	SYM-Key Part 1 20081010	Crypto adapter	6E2C12BC5A1751DB1152E9CC
ICSF asymmetric master key part	ASYM-Key First Part 20081010	Crypto adapter	61A7BAFE742EA870AE808D6E



Description SYM-Key Part 1 20081010
ENC-ZERO 60D600BA
MDC-4 6E2C12BC5A1751DB1152E9C03FF5D104
Key type New DES Master Key, First part

		sh pattern
		0000000000000000
		0000000000000000
		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

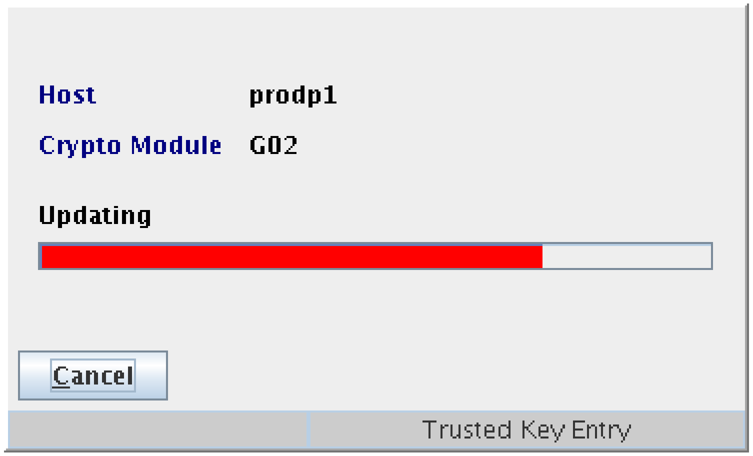
Select key to work with

Key Type
Master Key - AES:
AES Master Key
ECC Master Key
Master Key - DES:
DES Master Key
Asymmetric Master Key

Getting key values...   UPDATE MODE

roll process for an IBM Crypto Ada
enroll process for an IBM Crypto
apter
onfiguration data on an IBM Crypto
grate full configuration data on an
a z/OS Host
all data directories
edia
de information

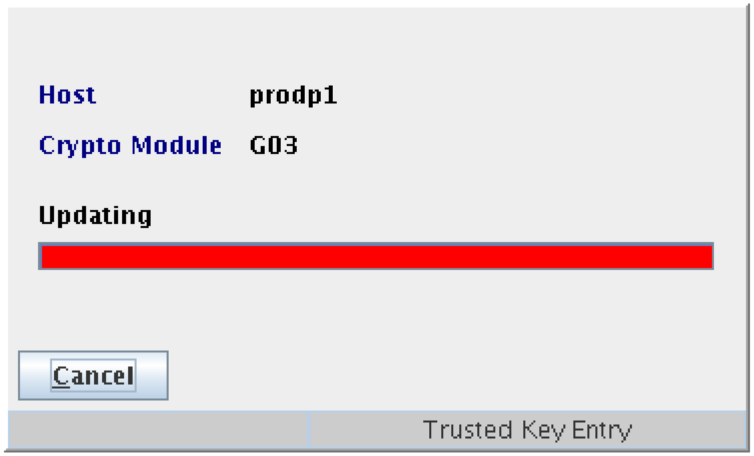
Each crypto module gets updated



Host prodp1

Crypto Module G02

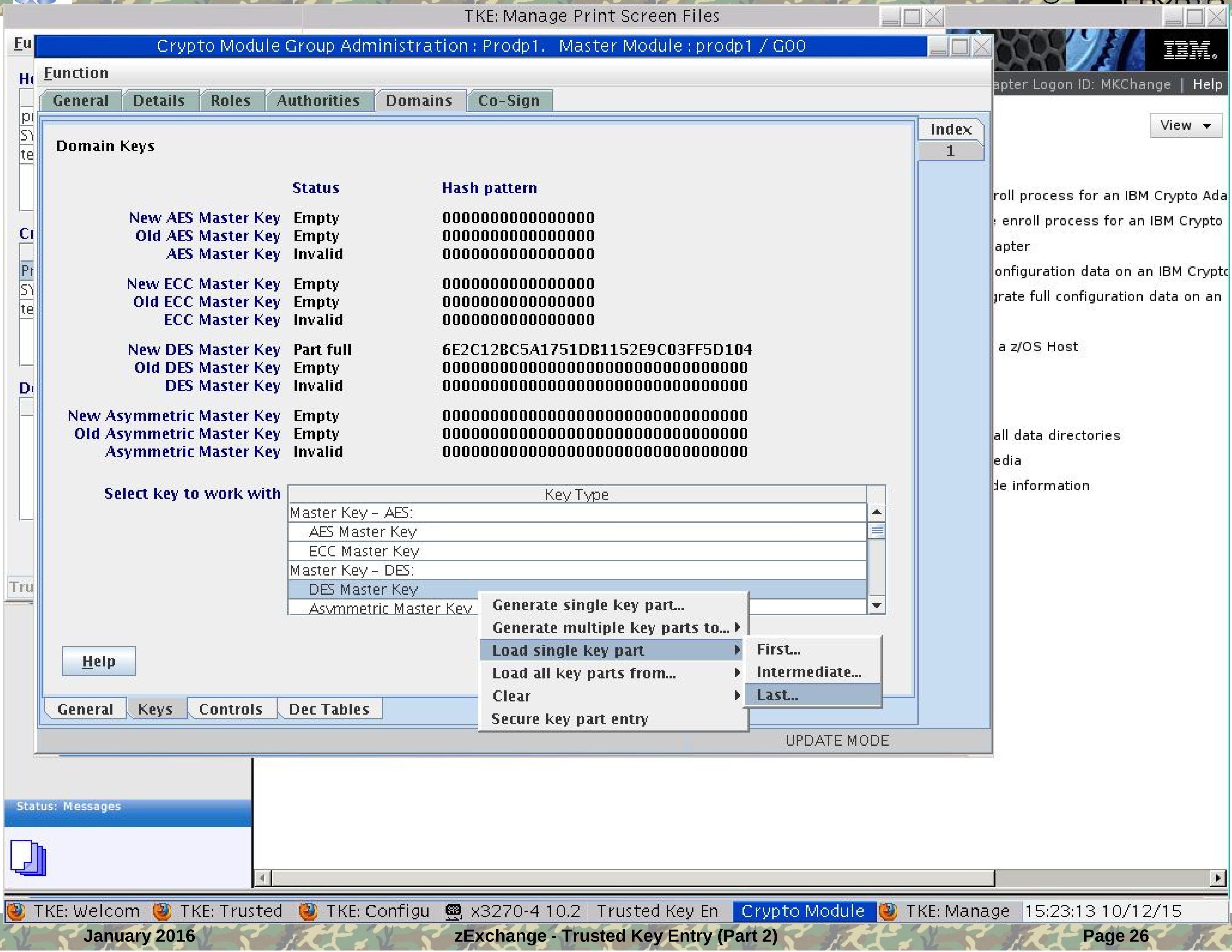
Updating



Host prodp1

Crypto Module G03

Updating



Crypto Module Group Administration : Prodp1. Master Module : prodp1 / G00

Domain Keys

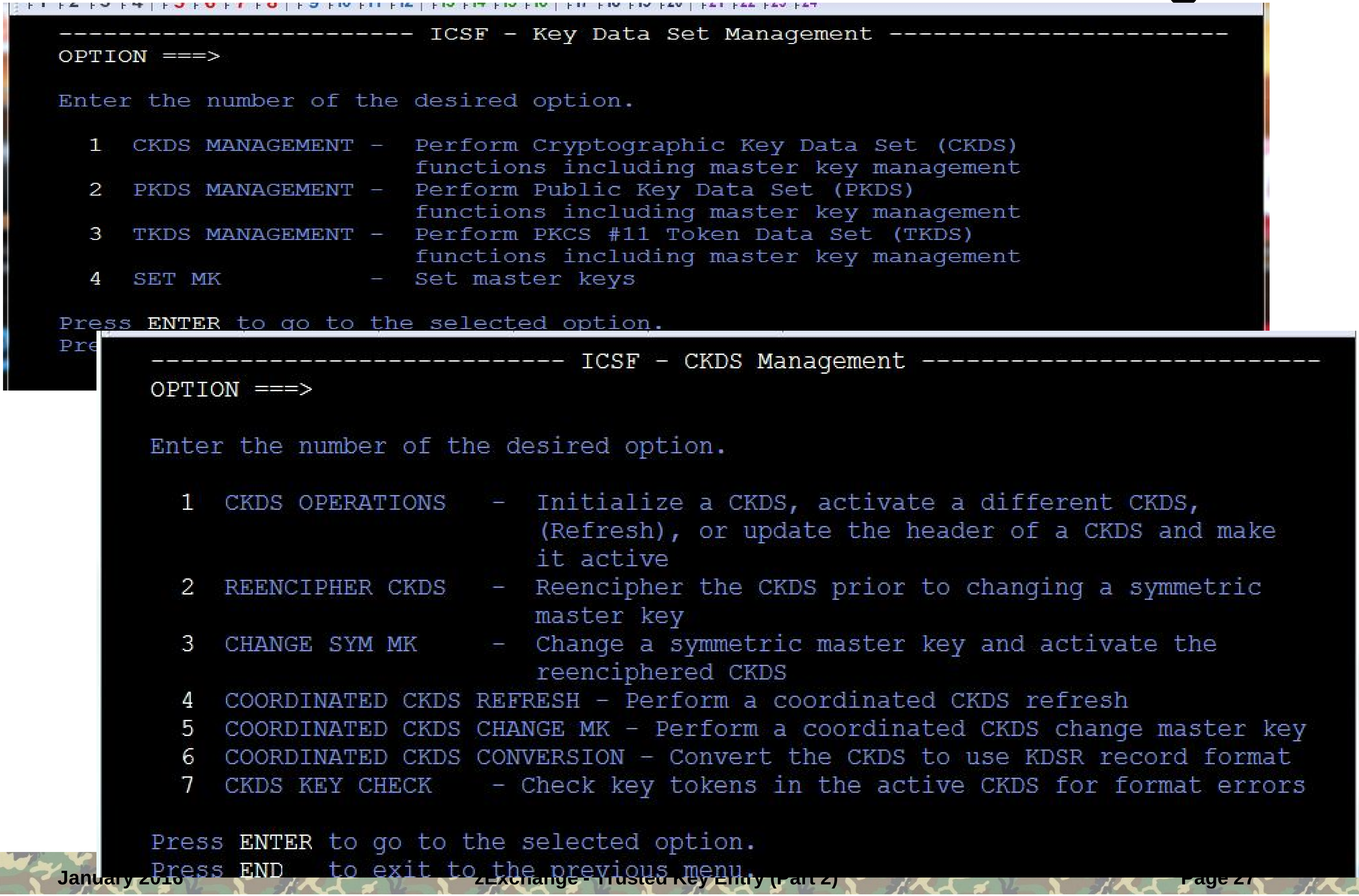
	Status	Hash pattern
New AES Master Key	Empty	0000000000000000
Old AES Master Key	Empty	0000000000000000
AES Master Key	Invalid	0000000000000000
New ECC Master Key	Empty	0000000000000000
Old ECC Master Key	Empty	0000000000000000
ECC Master Key	Invalid	0000000000000000
New DES Master Key	Part full	6E2C12BC5A1751DB1152E9C03FF5D104
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

UPDATE MODE

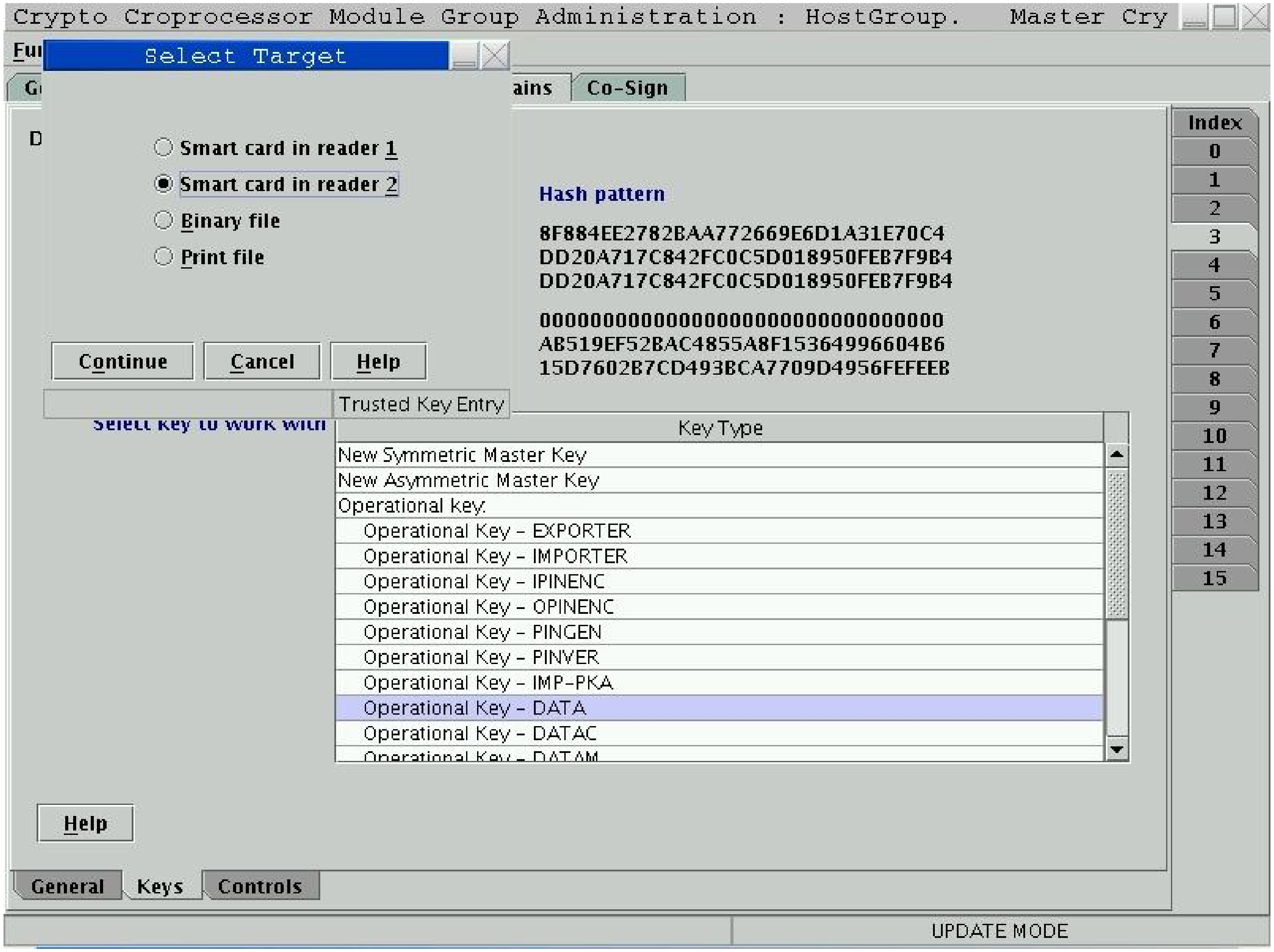
Pre-TKE V7.3 – Finish the MK Chg



```
------------------------ 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.
Pre
```

```
---------------------------- 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



Crypto Croprocessor Module Group Administration : HostGroup.   Master Cry

Select Target

○ Smart card in reader 1

● Smart card in reader 2

○ Binary file

○ Print file

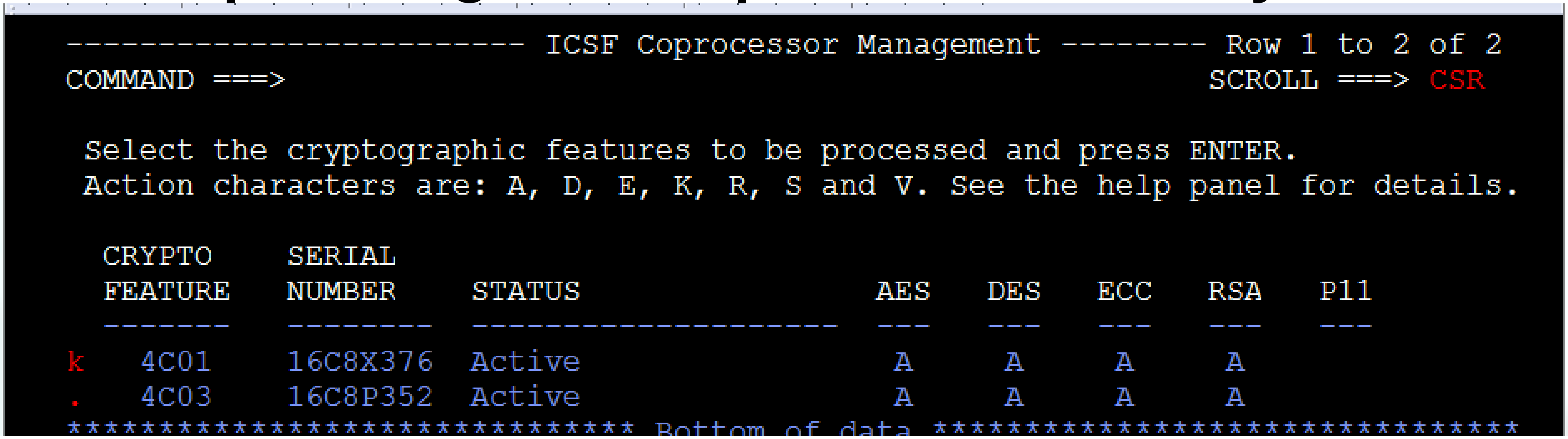
Hash pattern

```
8F884EE2782BAA772669E6D1A31E70C4
DD20A717C842FC0C5D018950FEB7F9B4
DD20A717C842FC0C5D018950FEB7F9B4

00000000000000000000000000000000
AB519EF52BAC4855A8F15364996604B6
15D7602B7CD493BCA7709D4956FEFEEB
```

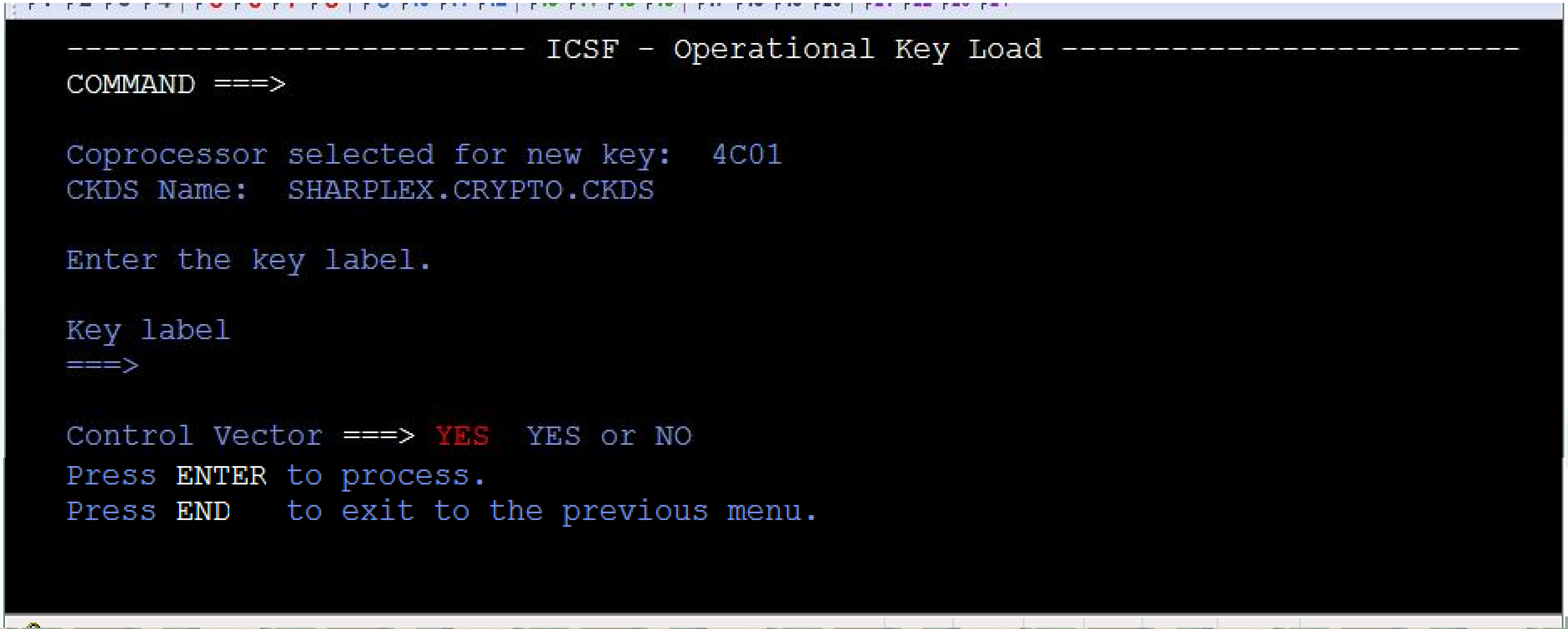
Key Type

- New Symmetric Master Key
- New Asymmetric Master Key
- Operational key
  - Operational Key – EXPORTER
  - Operational Key – IMPORTER
  - Operational Key – IPINENC
  - Operational Key – OPINENC
  - Operational Key – PINGEN
  - Operational Key – PINVER
  - Operational Key – IMP-PKA
  - Operational Key – DATA
  - Operational Key – DATAC
  - Operational Key – DATAM

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 ********************************
```



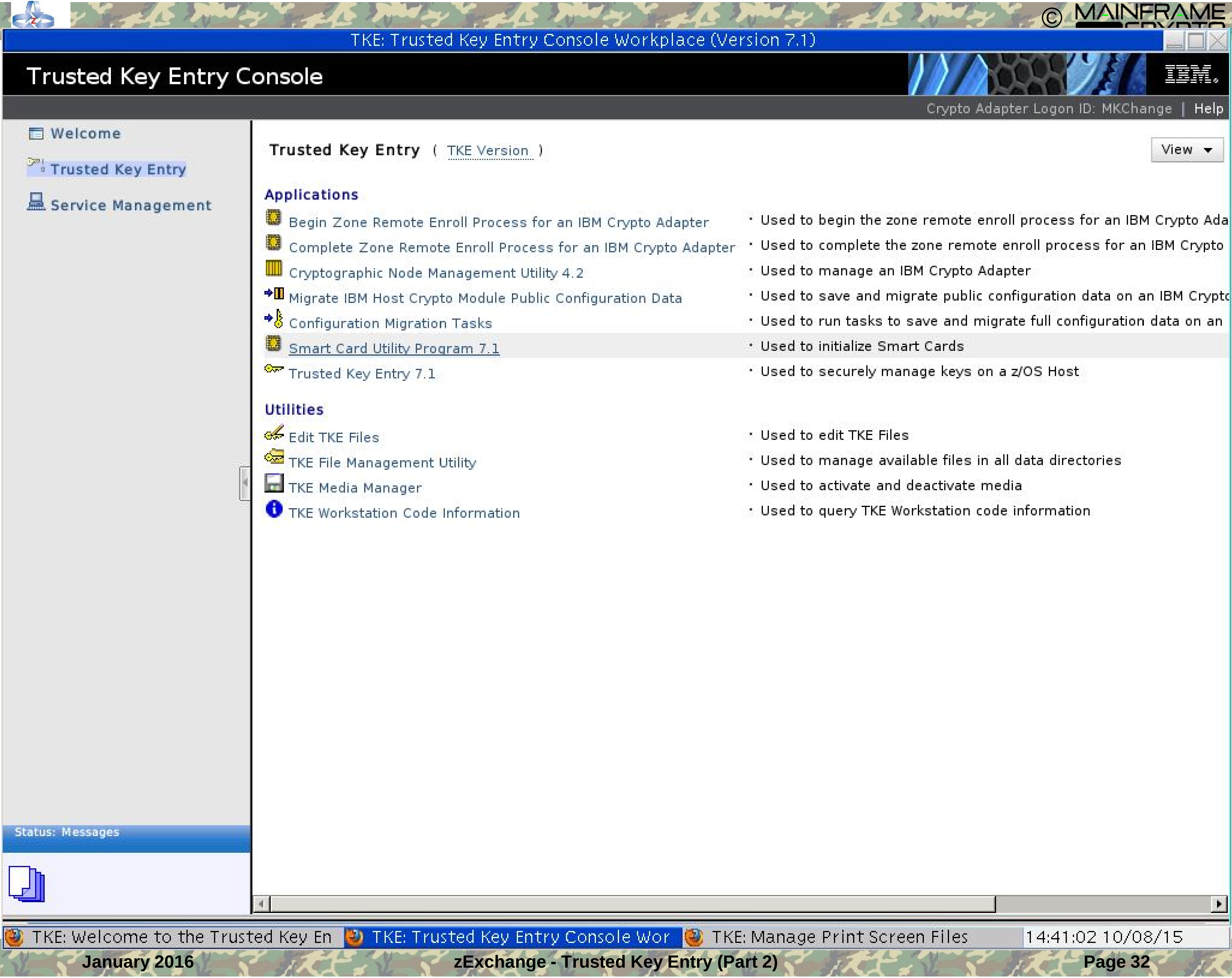
```
------------------------- ICSF - Operational Key Load --------------------------
COMMAND ===>

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.
```

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 8.0

TKE Console Workspace

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



TKE: Trusted Key Entry Console Workplace (Version 7.1)
Trusted Key Entry Console
IBM.
Crypto Adapter Logon ID: MKChange | Help
Welcome
Trusted Key Entry
Service Management
Status: Messages
View ▾

Trusted Key Entry (TKE Version)

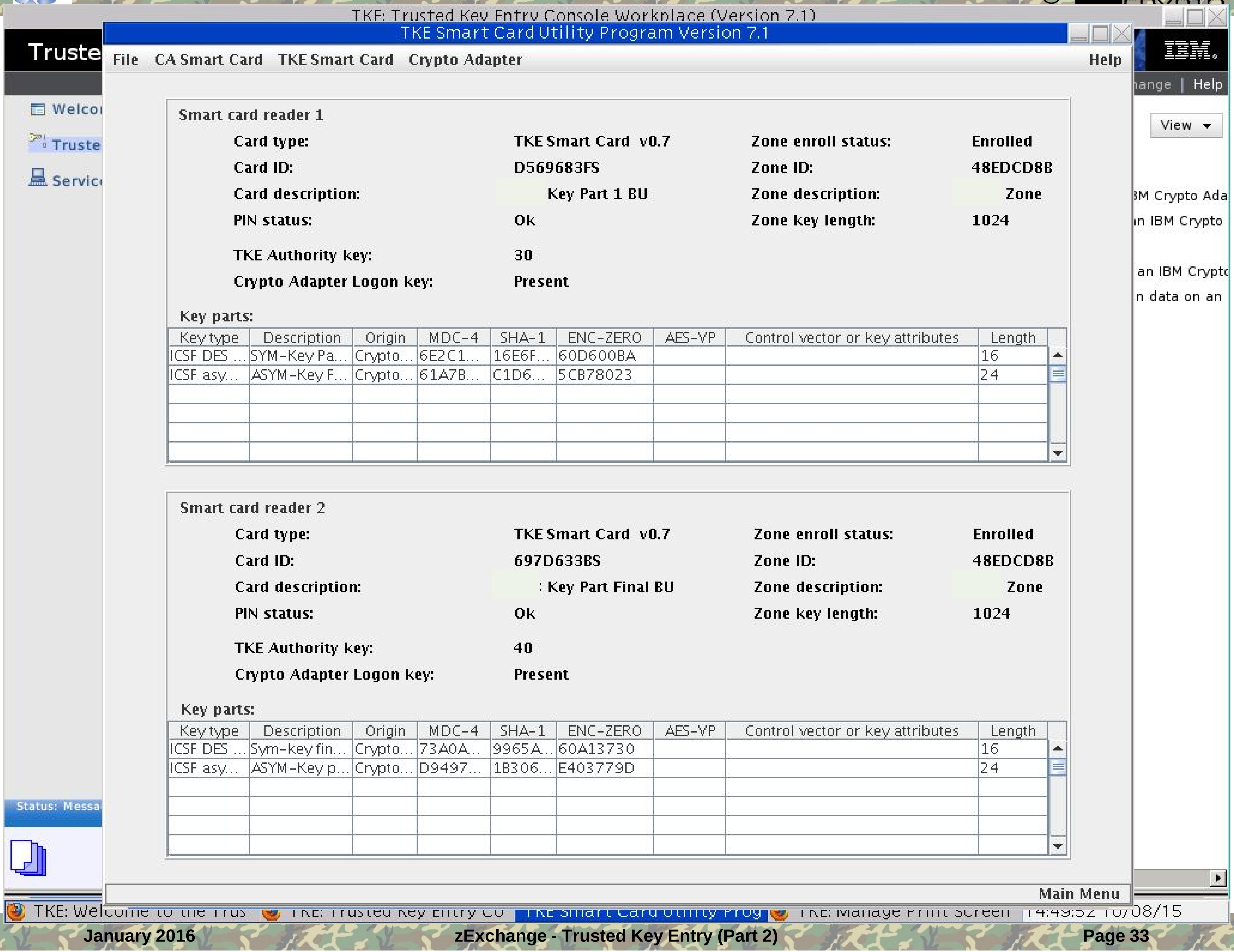
Applications

Begin Zone Remote Enroll Process for an IBM Crypto Adapter	Used to begin the zone remote enroll process for an IBM Crypto Ada
Complete Zone Remote Enroll Process for an IBM Crypto Adapter	Used to complete the zone remote enroll process for an IBM Crypto
Cryptographic Node Management Utility 4.2	Used to manage an IBM Crypto Adapter
Migrate IBM Host Crypto Module Public Configuration Data	Used to save and migrate public configuration data on an IBM Crypto
Configuration Migration Tasks	Used to run tasks to save and migrate full configuration data on an
Smart Card Utility Program 7.1	Used to initialize Smart Cards
Trusted Key Entry 7.1	Used to securely manage keys on a z/OS Host

Utilities

Edit TKE Files	Used to edit TKE Files
TKE File Management Utility	Used to manage available files in all data directories
TKE Media Manager	Used to activate and deactivate media
TKE Workstation Code Information	Used to query TKE Workstation code information

TKE: Welcome to the Trusted Key En
TKE: Trusted Key Entry Console Wor
TKE: Manage Print Screen Files
14:41:02 10/08/15


TKE: Trusted Key Entry Console Workplace (Version 7.1)
TKE Smart Card Utility Program Version 7.1
File
CA Smart Card
TKE Smart Card
Crypto Adapter
Help
Main Menu
TKE: Welcome to the Trus
TKE: Trusted Key Entry Co
TKE Smart Card Utility Prog
TKE: Manage Print Screen
14:49:52 10/08/15

Smart card reader 1

Card type: TKE Smart Card v0.7
Card ID: D569683FS
Card description: Key Part 1 BU
PIN status: Ok

TKE Authority key: 30
Crypto Adapter Logon key: Present

Zone enroll status: Enrolled
Zone ID: 48EDCD8B
Zone description: Zone
Zone key length: 1024

Key parts:

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	AES-VP	Control vector or key attributes	Length
ICSF DES ...	SYM-Key Pa...	Crypto...	6E2C1...	16E6F...	60D600BA			16
ICSF asy...	ASYM-Key F...	Crypto...	61A7B...	C1D6...	5CB78023			24

Smart card reader 2

Card type: TKE Smart Card v0.7
Card ID: 697D633BS
Card description: Key Part Final BU
PIN status: Ok

TKE Authority key: 40
Crypto Adapter Logon key: Present

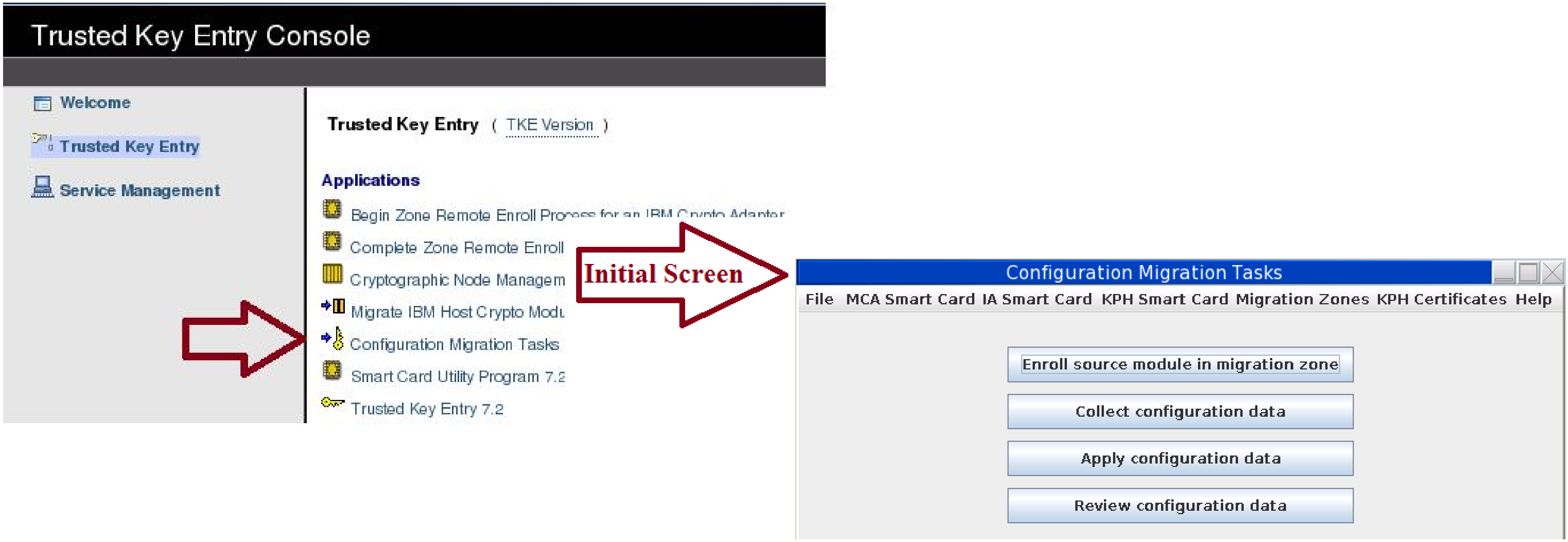
Zone enroll status: Enrolled
Zone ID: 48EDCD8B
Zone description: Zone
Zone key length: 1024

Key parts:

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	AES-VP	Control vector or key attributes	Length
ICSF DES ...	Sym-key fin...	Crypto...	73A0A...	9965A...	60A13730			16
ICSF asy...	ASYM-Key p...	Crypto...	D9497...	1B306...	E403779D			24

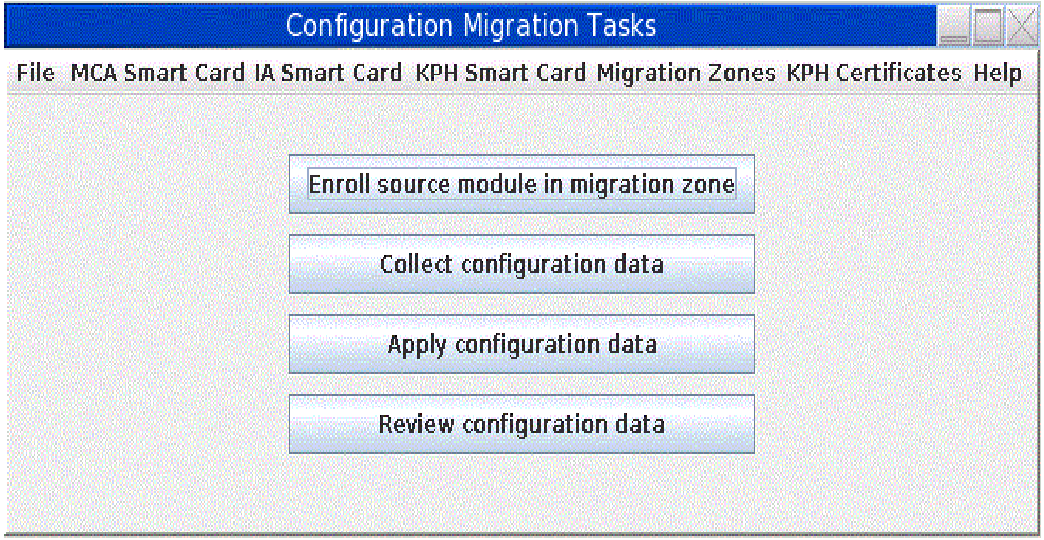
TKE 7.3 Full Function EP11 Migration Wizard

- Extension of CCA Migration Wizard
- Collect config data from one EP11 Host Crypto Module and apply to another EP11 Host Crypto Module

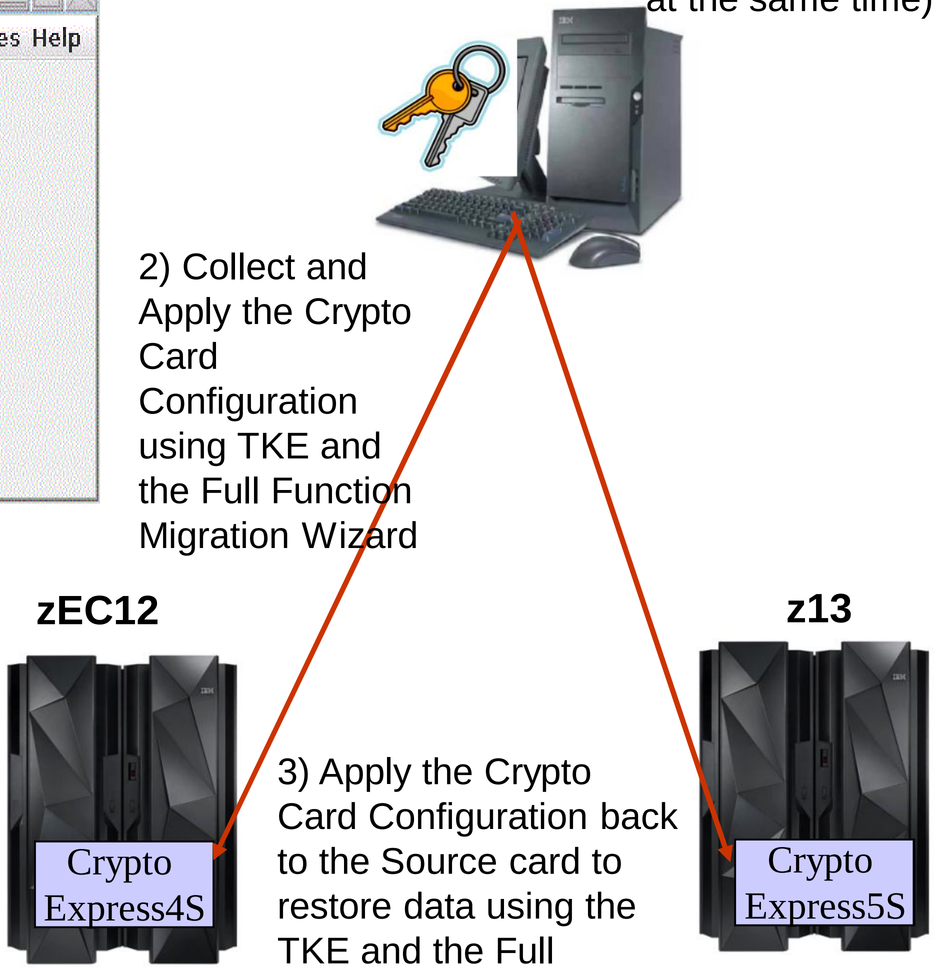

Trusted Key Entry Console
Welcome
Trusted Key Entry
Service Management
Trusted Key Entry (TKE Version)
Applications
Begin Zone Remote Enroll Process for an IBM Crypto Adapter
Complete Zone Remote Enroll
Cryptographic Node Managem
Migrate IBM Host Crypto Modu
Configuration Migration Tasks
Smart Card Utility Program 7.2
Trusted Key Entry 7.2
Configuration Migration Tasks
File
MCA Smart Card
IA Smart Card
KPH Smart Card
Migration Zones
KPH Certificates
Help
Enroll source module in migration zone
Collect configuration data
Apply configuration data
Review configuration data

Initial Screen

TKE Enhancement: Full Function Migration Wizard for EP11


Configuration Migration Tasks
File
MCA Smart Card
IA Smart Card
KPH Smart Card
Migration Zones
KPH Certificates
Help
Enroll source module in migration zone
Collect configuration data
Apply configuration data
Review configuration data

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



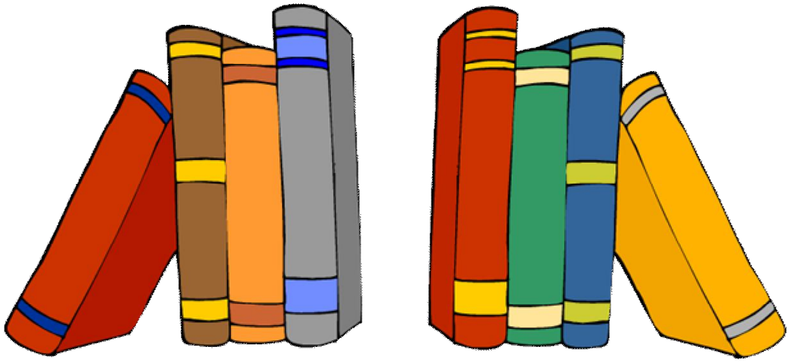
2) Collect and Apply the Crypto Card Configuration using TKE and the Full Function Migration Wizard

3) Apply the Crypto Card Configuration back to the Source card to restore data using the TKE and the Full Function Migration Wizard

TKE Exclusives

- Secure loading of master keys
- Migration Wizard
- Enabling/Disabling ACPs
    - 24-Byte DES-MK
- Loading MKs for inactive LPARs
- Loading MKs for Linux guests
- Loading P11-MK
- Loading PIN Decimalization Tables

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’

YouTube TKE Videos

- http://www.youtube.com/user/IBMTKE
  - Managing CCA Mode Host Crypto Modules From TKE
    - Manage-CCA-Modules-Overview-Presentation
    - Manage-CCA-Modules-Host-Definitions
    - Manage-CCA-Modules-Concept-Presentation-Authority-Signature-Keys-and-Authority-Indexes
    - Manage-CCA Modules-Concept-Presentation-Multiple-Domains
    - Concept-Presentation-TKE-Designing-Domain-Groups
  - How to use IBM TKE Zones with TKE Smart Card Members
    - Video Series Overview - How to use IBM TKE Zones with TKE Smart Card Members
    - 1 of 6 - Initializing a TKE Workstation Crypto Adapter for Use with SMART CARD Profiles
    - 2 of 6 - Create A TKE Zone with TKE Smart Card Members
    - 3 of 6 - Create TKE Workstation Smart Card Profiles
    - 4 of 6 - Create a TKE Workstation Smart Card Group Profile
    - 5 of 6 - Enroll a TKE Workstation in a TKE Zone
    - 6 of 6: Create Backup CA and TKE Smart Cards

Questions