Trusted Key Entry Workstation (Part 1)

Greg Boyd

gregboyd@mainframecrypto.com

December 2015

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

-
-
- **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

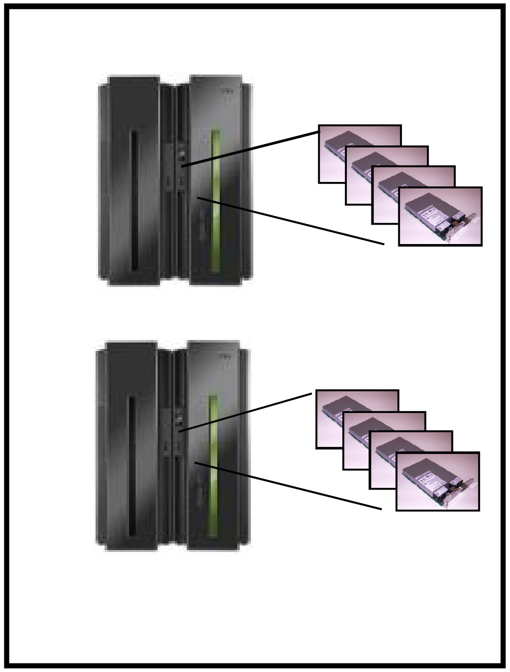
- Trusted Key Entry Workstation Description
- Smart Cards
- Host Setup
- Privileged Modes
- Profiles, Roles & Authorities
- TKE Setup
- TKE Utilities and Apps

Key Loading

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

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

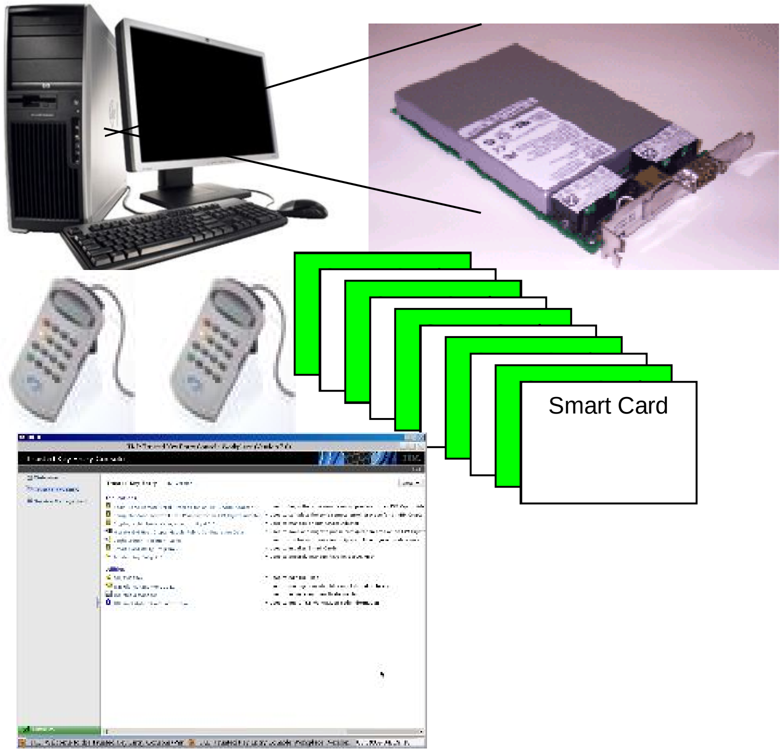


TKE – and what it doesn’t do

- Crypto for applications
- Key storage

TKE - Components

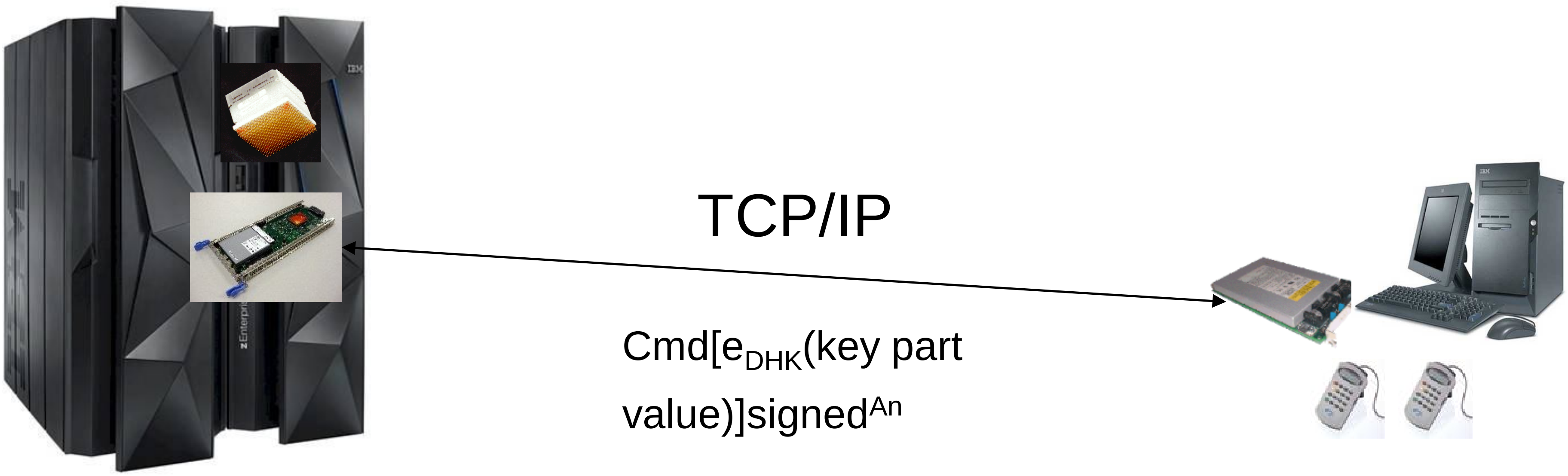
- Workstation with a crypto coprocessor
  - Intel Workstation with an embedded operating system
  - Cryptographic coprocessor
  - A TKE application (Java)
  - Optional TKE smart card support
    - Readers and 20 smart cards
    - 10 Additional smart cards



TKE Hardware/Software and Host Adapters managed

TKE Software (LIC) FC	TKE Hardware FC	Host system (order)	Host Crypto cards managed
TKE 8.0 (#0877)	#0847	z13, 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	z10 EC/BC, z9 109/EC/BC	CEX3C, CEX2C, PCIXCC

Secure Host Connection



TCP/IP

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

Host w/ Secure Crypto HW

Trusted Key Entry Workstation

Smart Cards

- Store credentials
- Store key material
- Perform encryption functions

http://www.gocomics.com/pearlsbeforeswine/2008/02/07

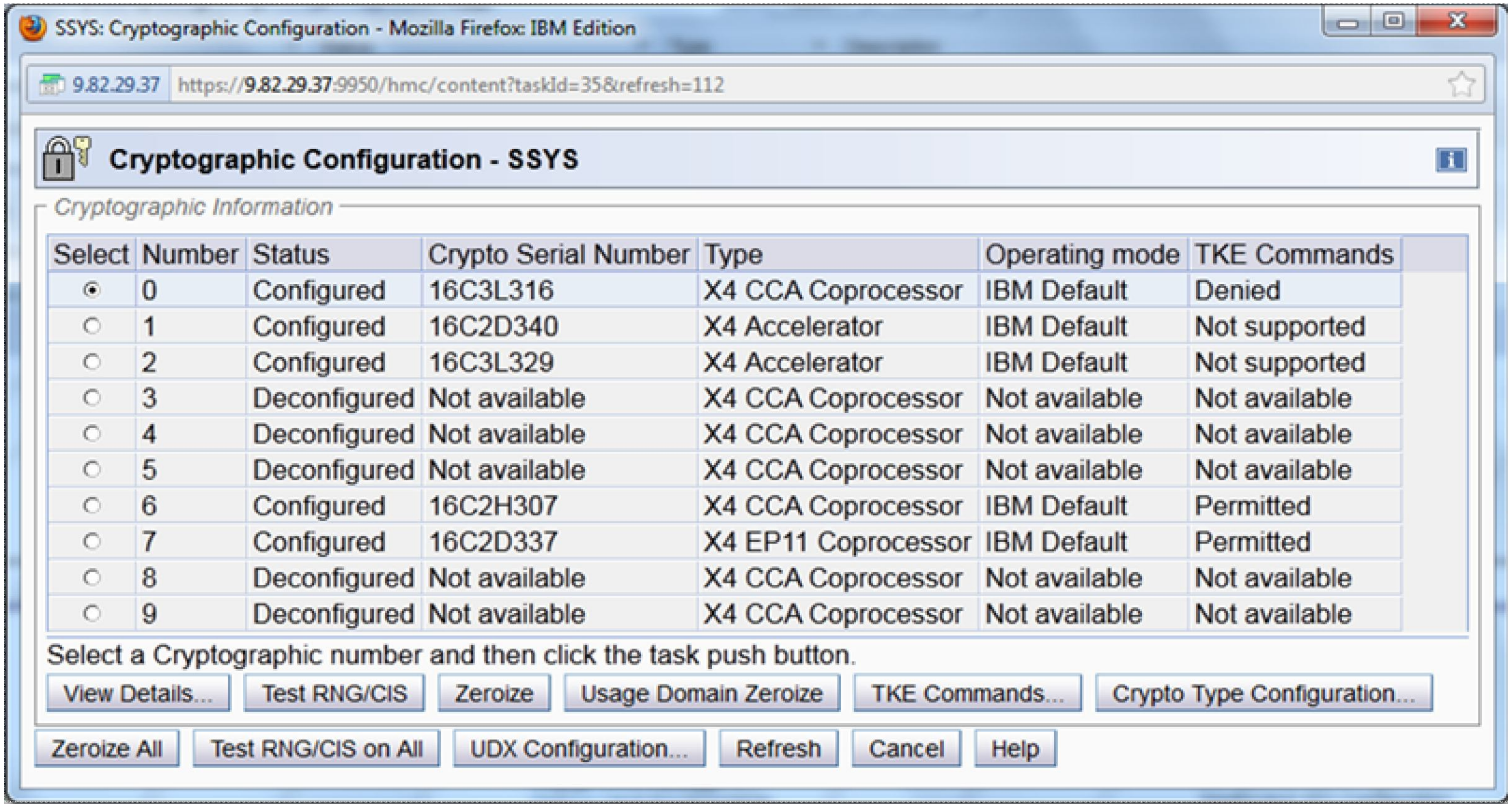
TKE Zones

- Members of (Entities in) a zone
  - CA (Certificate Authority) Smart Card
  - TKE Workstation Crypto Adapter
  - TKE Smart Cards
  - EP11 Smart Cards
- Enrollment Generates a Zone ID which is assigned to each entity
  - Zone ID is created when you create the CA Smart Card and the workstation crypto adapter is associated with that CA smart card
  - As TKE and EP11 smart cards are created they also are associated with the zone id

Smart Cards

- Certificate Authority (CA) Smart Card – Establishes the zone (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

HMC – Crypto Configuration



SSYS: Cryptographic Configuration - Mozilla Firefox: IBM Edition

9.82.29.37 https://9.82.29.37:9950/hmc/content?taskId=35&refresh=112

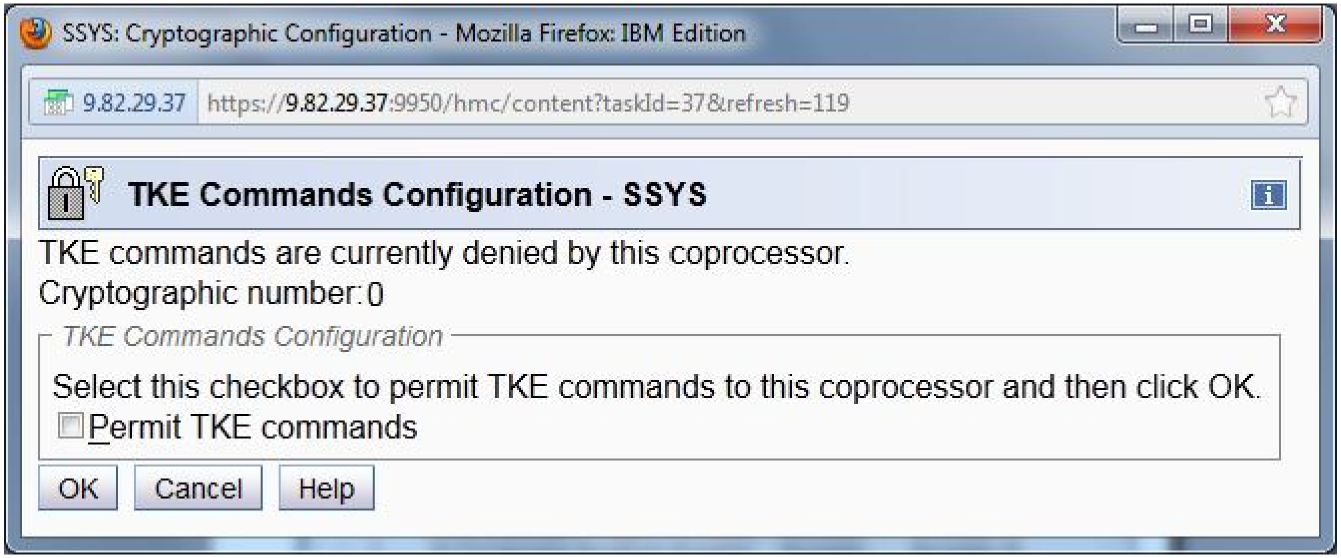
Cryptographic Configuration - SSYS

Cryptographic Information

Select	Number	Status	Crypto Serial Number	Type	Operating mode	TKE Commands
●	0	Configured	16C3L316	X4 CCA Coprocessor	IBM Default	Denied
○	1	Configured	16C2D340	X4 Accelerator	IBM Default	Not supported
○	2	Configured	16C3L329	X4 Accelerator	IBM Default	Not supported
○	3	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available
○	4	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available
○	5	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available
○	6	Configured	16C2H307	X4 CCA Coprocessor	IBM Default	Permitted
○	7	Configured	16C2D337	X4 EP11 Coprocessor	IBM Default	Permitted
○	8	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available
○	9	Deconfigured	Not available	X4 CCA Coprocessor	Not available	Not available

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

Config TKE Commands



SSYS: Cryptographic Configuration - Mozilla Firefox: IBM Edition
9.82.29.37
https://9.82.29.37:9950/hmc/content?taskId=37&refresh=119

TKE Commands Configuration - SSYS

TKE commands are currently denied by this coprocessor.

Cryptographic number: 0

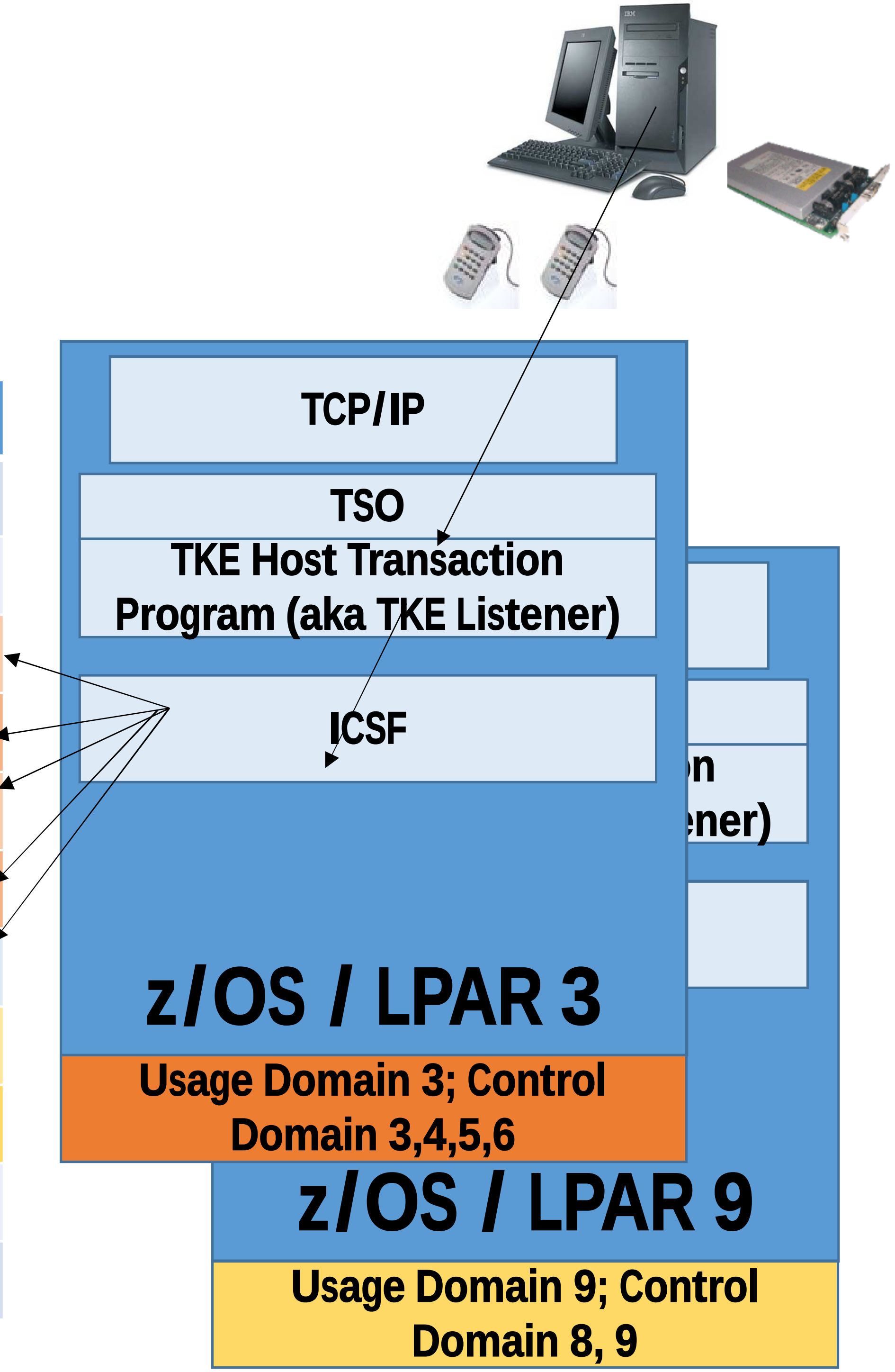
TKE Commands Configuration

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

□ Permit TKE commands

Control Domains

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



TCP/IP

TSO

TKE Host Transaction Program (aka TKE Listener)

ICSF

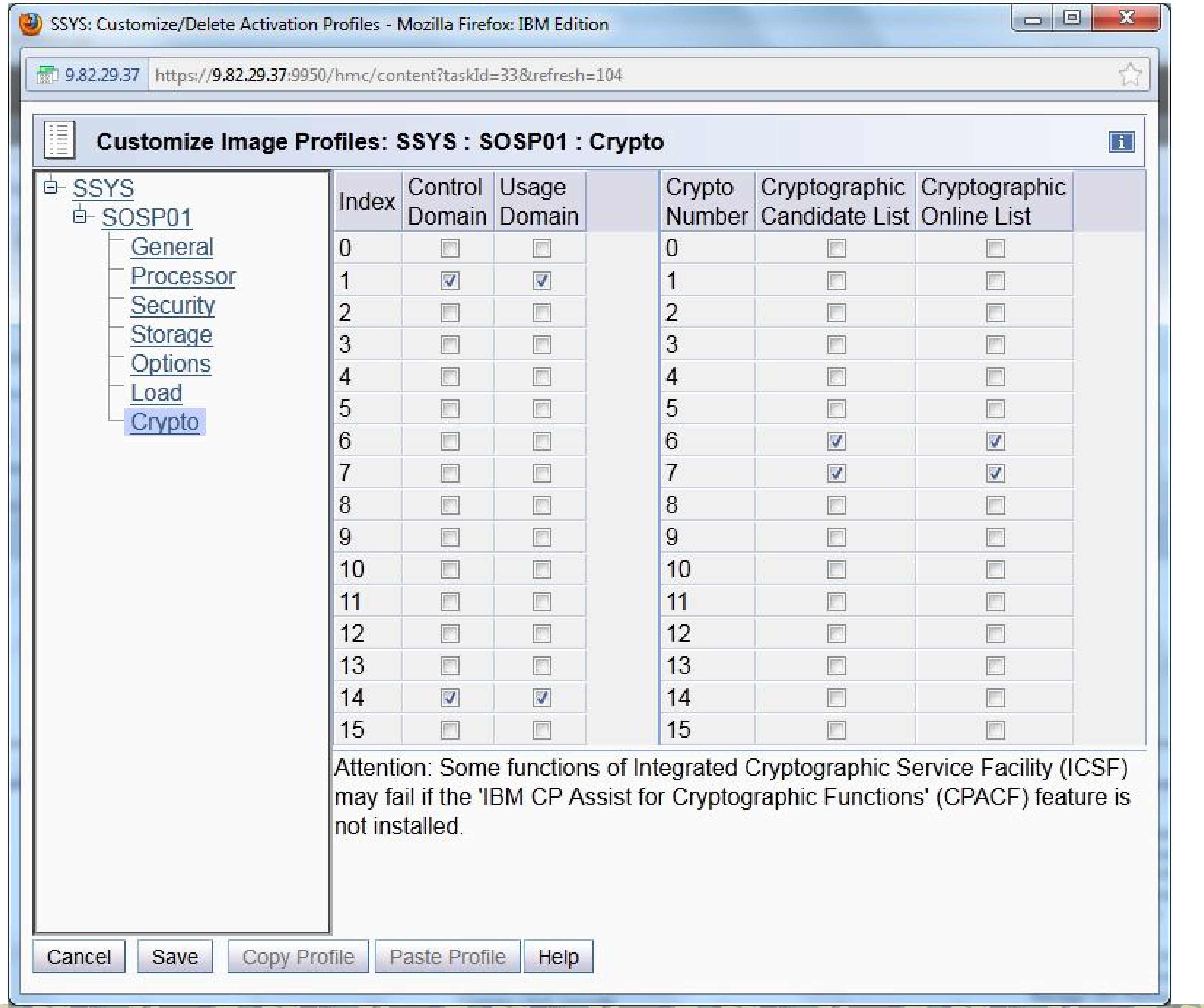
z/OS / LPAR 3

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

z/OS / LPAR 9

Usage Domain 9; Control Domain 8, 9

Setting Usage/Control Domain



SSYS: Customize/Delete Activation Profiles - Mozilla Firefox: IBM Edition

9.82.29.37 https://9.82.29.37:9950/hmc/content?taskId=33&refresh=104

Customize Image Profiles: SSYS : SOSP01 : Crypto

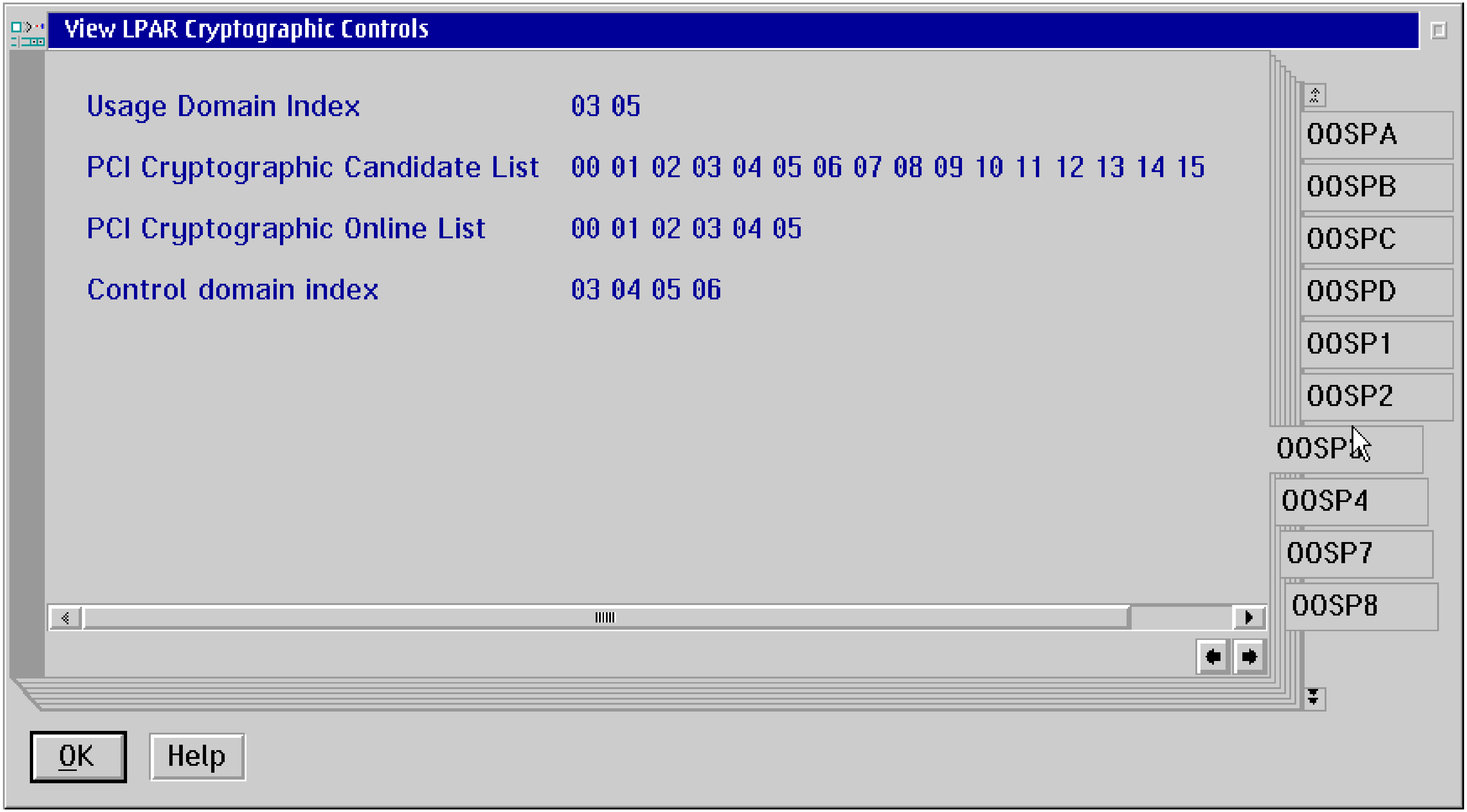
- SSYS
  - SOSP01
    - General
    - Processor
    - Security
    - Storage
    - Options
    - Load
    - Crypto

Index	Control Domain	Usage Domain
0	☐	☐
1	☑	☑
2	☐	☐
3	☐	☐
4	☐	☐
5	☐	☐
6	☐	☐
7	☐	☐
8	☐	☐
9	☐	☐
10	☐	☐
11	☐	☐
12	☐	☐
13	☐	☐
14	☑	☑
15	☐	☐

Crypto Number	Cryptographic Candidate List	Cryptographic Online List
0	☐	☐
1	☐	☐
2	☐	☐
3	☐	☐
4	☐	☐
5	☐	☐
6	☑	☑
7	☑	☑
8	☐	☐
9	☐	☐
10	☐	☐
11	☐	☐
12	☐	☐
13	☐	☐
14	☐	☐
15	☐	☐

Attention: Some functions of Integrated Cryptographic Service Facility (ICSF) may fail if the 'IBM CP Assist for Cryptographic Functions' (CPACF) feature is not installed.

View LPAR Cryptographic Controls



View LPAR Cryptographic Controls

Usage Domain Index 03 05

PCI Cryptographic Candidate List 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

PCI Cryptographic Online List 00 01 02 03 04 05

Control domain index 03 04 05 06

TKE Listener Started Task

```
//CSFTTCP PROC LEVEL=CSF,MEMBER=CSFTHTP3,
// CPARM=’PORT;1000;SET DISPLAY LEVEL;TRACE ALL’
//CLIST EXEC PGM= IKJEFT01,
// PARM=’EX ’’&LEVEL..SCSFCLI0(&MEMBER)’’ ’’&CPARM’’ EXEC’
//STEPLIB DD DSN=EZA.SEZALINK,DISP=SHR
//SYSABEND DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSEXEC DD DSN=&LEVEL..SCSFCLI0,DISP=SHR
//SYSPROC DD DSN=&LEVEL..SCSFCLI0,DISP=SHR
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD DUMMY
//TKEPARMS DD DSN=&LEVEL..SAMPLIB(CSFTPRM),DISP=SHR
//*
//* customize the DSN to be the TCP/IP data set on your system
//*
//*SYSTCPD DD DSN=TCPIP.SEZAINST(TCPDATA),DISP=SHR
// PEND CSFTTCP
//* ------------------------------------------------------------
```

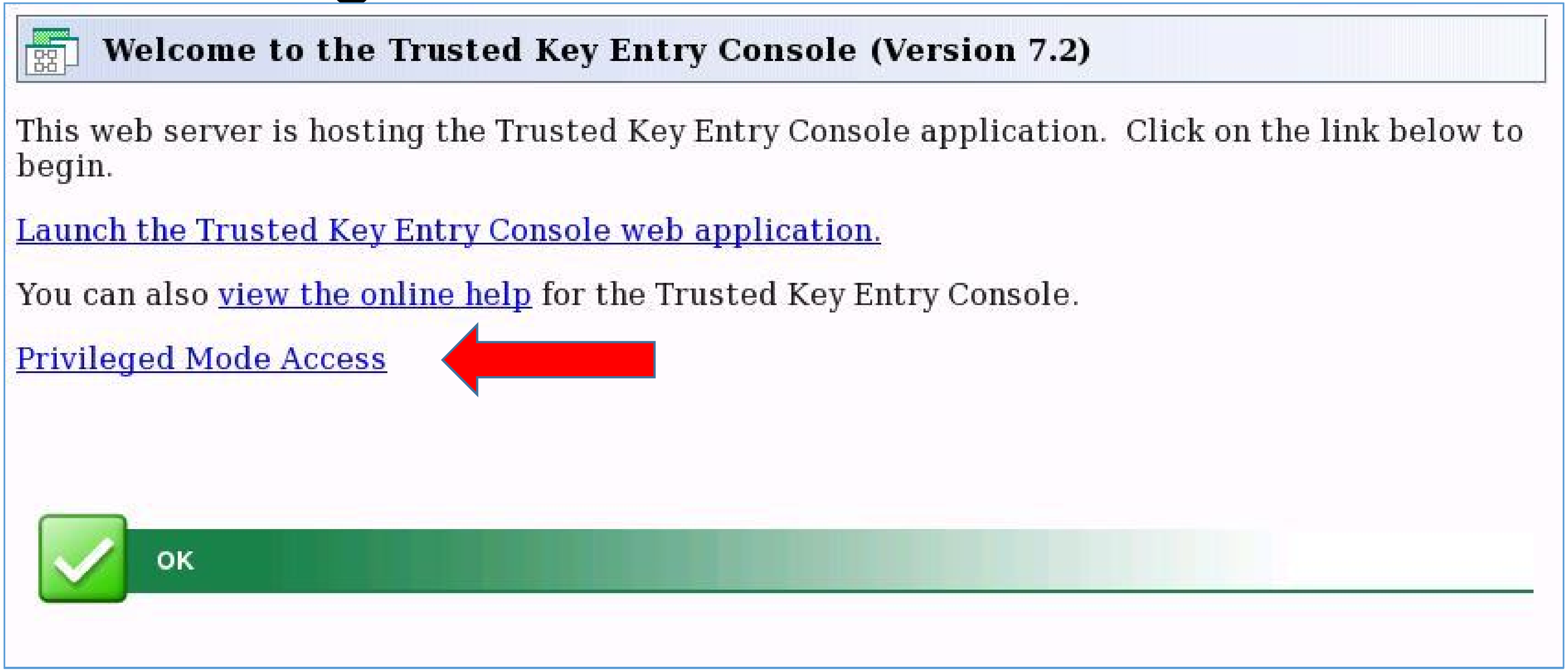
More Setup

- Assign a userid to the TKE Listener started task

  RDEFINE STARTED CSFTTCP.CSFTTCP STDATA(USER(userid))

- SAF Protect CSFTTKE
  - RDEFINE FACILITY CSFTTKE UACC(NONE)
  - PERMIT CSFTTKE CLASS(FACILITY) ID(userid or group) ACCESS(READ)
  - RDEFINE APPL CSFTTKE UACC(NONE)
  - PERMIT CSFTTKE CLASS(APPL) ID(userid or group) ACCESS(READ)
- Authorized Command List in IKJTSOxx
  - AUTHCMD NAMES (... CSFTTKE ....)

TKE Logon



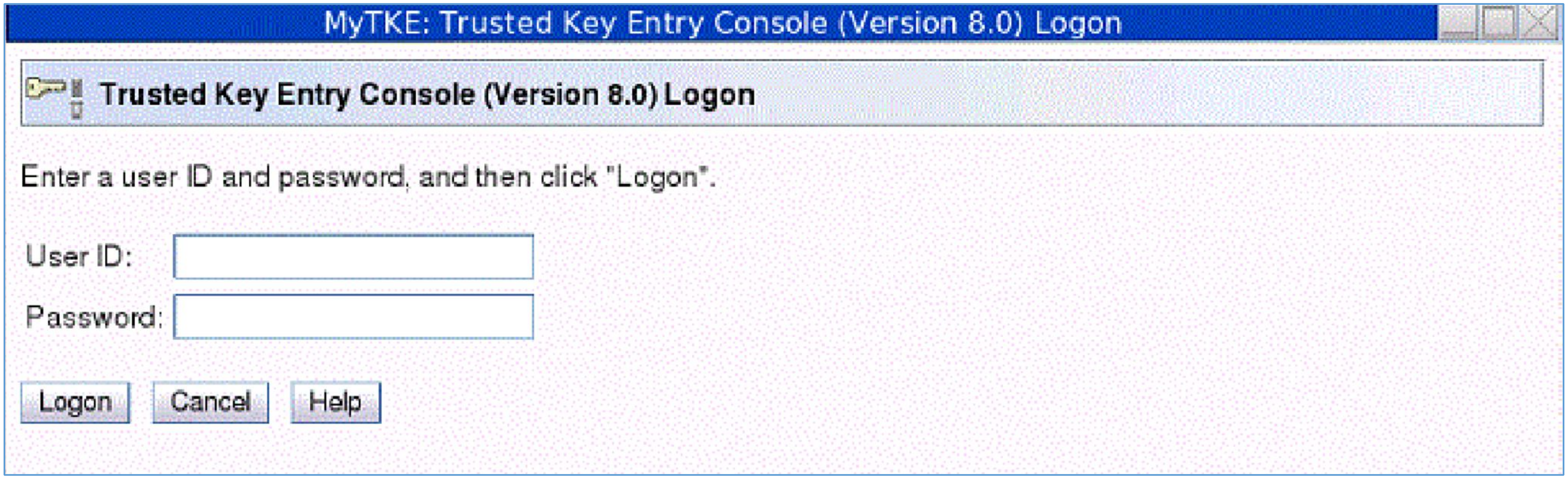
Welcome to the Trusted Key Entry Console (Version 7.2)

This web server is hosting the Trusted Key Entry Console application. Click on the link below to begin.

Launch the Trusted Key Entry Console web application.

You can also view the online help for the Trusted Key Entry Console.

Privileged Mode Access



MyTKE: Trusted Key Entry Console (Version 8.0) Logon

Trusted Key Entry Console (Version 8.0) Logon

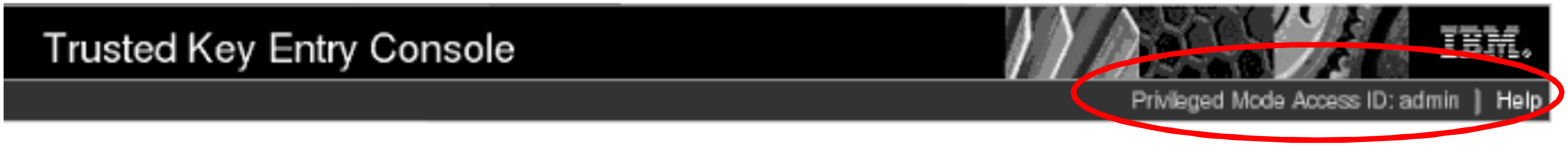
Enter a user ID and password, and then click "Logon".

User ID:

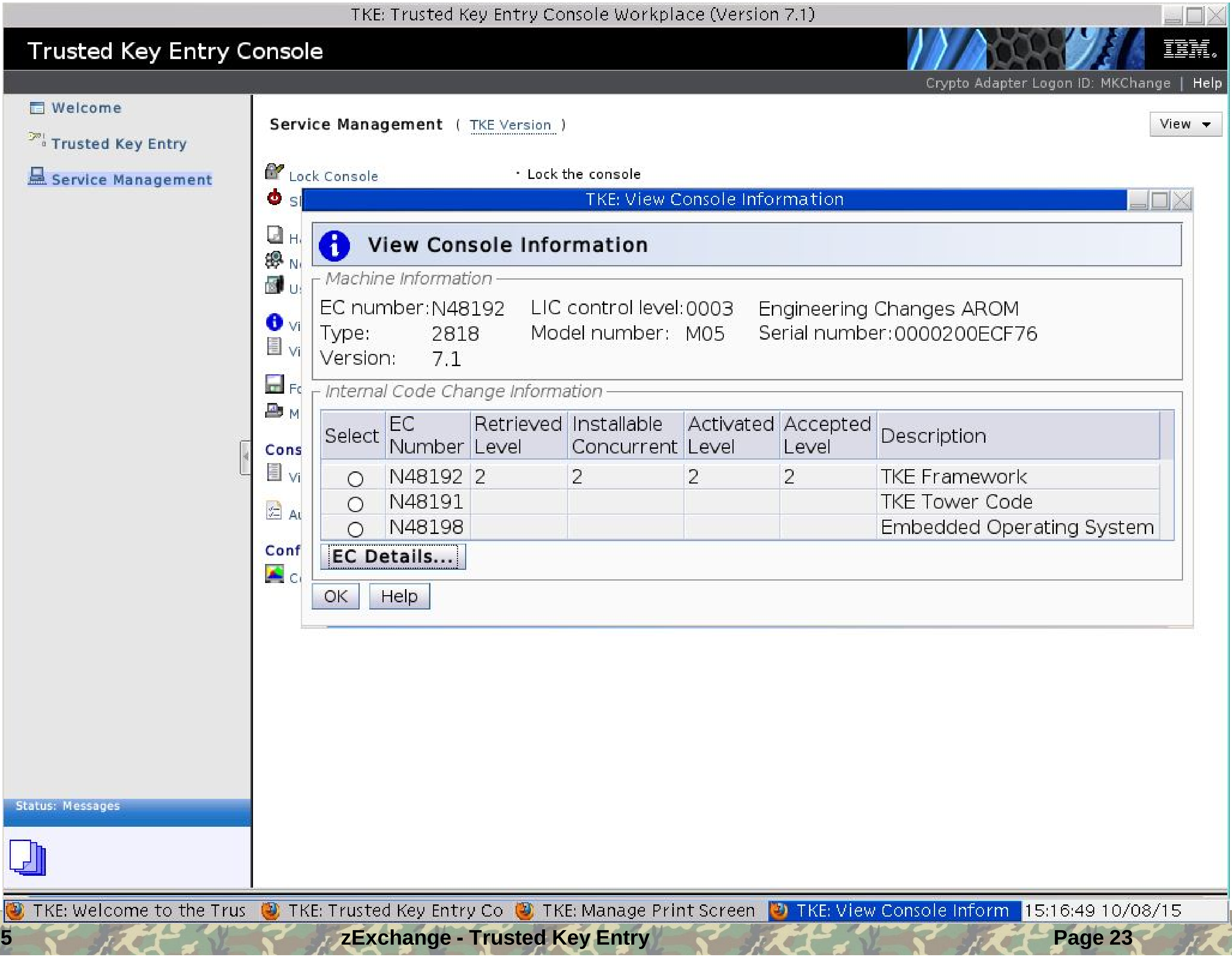
Password:

Privileged Mode Access

- ADMIN
- AUDITOR
- SERVICE


Trusted Key Entry Console
IBM.
Privileged Mode Access ID: admin | Help

View Console Information



View Console Information

Machine Information

EC number: N48192
Type: 2818
Version: 7.1
LIC control level: 0003
Model number: M05
Engineering Changes AROM
Serial number: 0000200ECF76

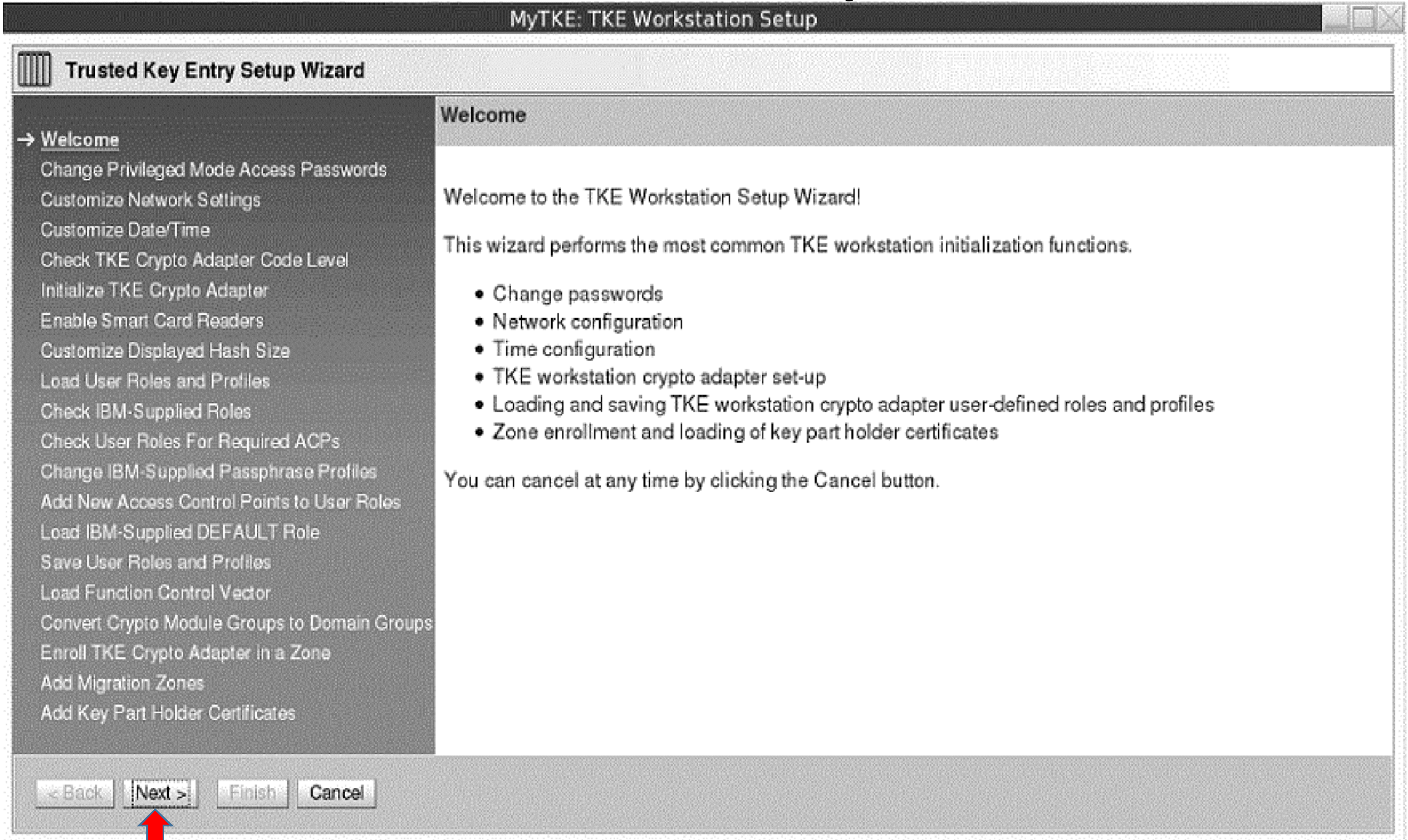
Internal Code Change Information

Select	EC Number	Retrieved Level	Installable Concurrent	Activated Level	Accepted Level	Description
○	N48192	2	2	2	2	TKE Framework
○	N48191					TKE Tower Code
○	N48198					Embedded Operating System

EC Details...

OK Help

TKE Workstation Setup Wizard



MyTKE: TKE Workstation Setup

Trusted Key Entry Setup Wizard

- → Welcome
- 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 IBM-Supplied Roles
- Check User Roles For Required ACPs
- Change IBM-Supplied Passphrase Profiles
- Add New Access Control Points to User Roles
- Load IBM-Supplied DEFAULT Role
- Save User Roles and Profiles
- Load Function Control Vector
- Convert Crypto Module Groups to Domain Groups
- Enroll TKE Crypto Adapter in a Zone
- Add Migration Zones
- Add Key Part Holder Certificates

Welcome

Welcome to the TKE Workstation Setup Wizard!

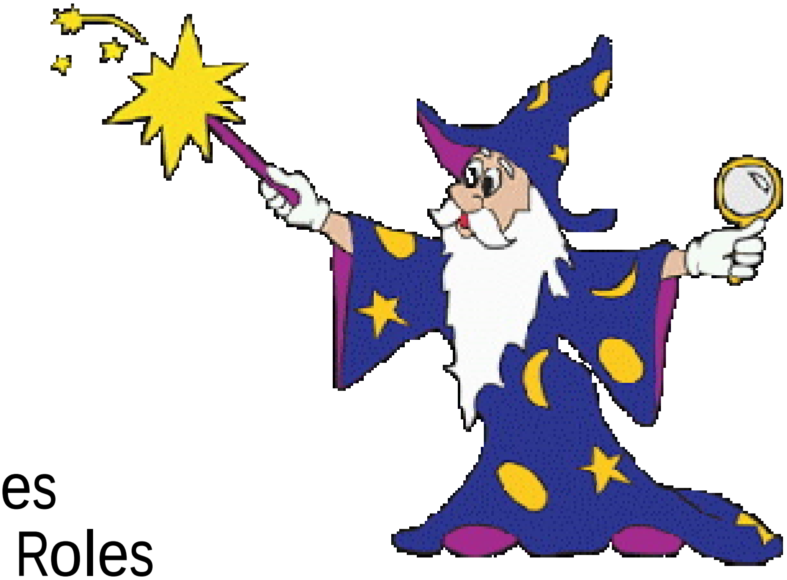
This wizard performs the most common TKE workstation initialization functions.

- Change passwords
- Network configuration
- Time configuration
- TKE workstation crypto adapter set-up
- Loading and saving TKE workstation crypto adapter user-defined roles and profiles
- Zone enrollment and loading of key part holder certificates

You can cancel at any time by clicking the Cancel button.

TKE Installation Wizard

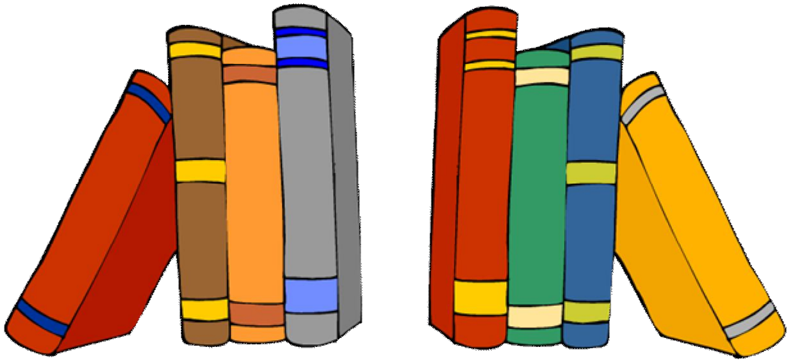
1. Change Privileged Mode Access Passwords
2. Customize Network Settings
3. Customize Date/Time
4. Check TKE Crypto Adapter Code Level
5. Initialize TKE Crypto adapter
6. Enable Smart Card Readers
7. Customize Displayed Hash Size
8. Load User Roles and Profiles
9. Check IBM Supplied Roles
10. Change IBM Supplied Passphrase Profiles
11. Add New Access Control Points to User Roles
12. Load IBM Supplied DEFAULT Role
13. Save User Roles and Profiles
14. Load Function Control Vector
15. Enroll TKE Crypto Adapter in a Zone
16. Add Migration Zones
17. Add Key Part Holder Certificates



TKE Exclusives

- Secure loading of master keys
- Migration Wizard
- Enabling/Disabling ACPs
    - 24-Byte DES-MK
- Loading MKs for inactive LPARs
- 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