Trusted Key Entry Workstation (Part 2)

Greg Boyd

gregboyd@mainframecrypto.com
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

- Copyright © 2016 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.
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

<table>
<thead>
<tr>
<th>Dom</th>
<th>AES-MK</th>
<th>DES-MK</th>
<th>RSA-MK</th>
<th>ECC-MK</th>
</tr>
</thead>
<tbody>
<tr>
<td>UD1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD4&lt;sup&gt;M&lt;/sup&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD8&lt;sup&gt;M&lt;/sup&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>....</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UD85</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Diagram
- **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**

---

January 2016

zExchange - Trusted Key Entry (Part 2)
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: Master 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

Send updates  Cancel  Help
TKE Welcome Screen

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.
Crypto Adapter Logon

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

Group profile ID: MKChange

Group members required for logon: 2

Group members ready for logon: 1

Group members:

<table>
<thead>
<tr>
<th>Profile ID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoSign1</td>
<td></td>
</tr>
<tr>
<td>CoSign2</td>
<td></td>
</tr>
<tr>
<td>Admin1</td>
<td></td>
</tr>
<tr>
<td>Admin2</td>
<td></td>
</tr>
<tr>
<td>MKFirst1</td>
<td>ready for logon</td>
</tr>
<tr>
<td>MKFirst2</td>
<td></td>
</tr>
<tr>
<td>MKFinal1</td>
<td></td>
</tr>
<tr>
<td>MKFinal2</td>
<td></td>
</tr>
</tbody>
</table>

Ok  Cancel
TKE 8.0 Main Window
TKE 7.1 Main Window

### Hosts

<table>
<thead>
<tr>
<th>Host ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prodp1</td>
<td>production lpar</td>
</tr>
<tr>
<td>SYSTS1</td>
<td>Third LPAR - SYSPROP S...</td>
</tr>
<tr>
<td>test1</td>
<td>test lpar</td>
</tr>
</tbody>
</table>

### Crypto Modules

<table>
<thead>
<tr>
<th>Host ID</th>
<th>CM index</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prodp1</td>
<td>G00</td>
<td></td>
<td>Authentication...</td>
</tr>
<tr>
<td>prodp1</td>
<td>G01</td>
<td></td>
<td>Authentication...</td>
</tr>
<tr>
<td>prodp1</td>
<td>G02</td>
<td></td>
<td>Authentication...</td>
</tr>
<tr>
<td>prodp1</td>
<td>G03</td>
<td></td>
<td>Authentication...</td>
</tr>
</tbody>
</table>

### Crypto Module Groups

<table>
<thead>
<tr>
<th>Group ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prodp1</td>
<td>Prod</td>
</tr>
<tr>
<td>SYSTS1</td>
<td></td>
</tr>
<tr>
<td>testgroup</td>
<td>TEST LPAR</td>
</tr>
</tbody>
</table>

### Domain Groups

<table>
<thead>
<tr>
<th>Group ID</th>
<th>Description</th>
</tr>
</thead>
</table>

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?
   Yes  No
Logon to the Host(s)
# CCA Crypto Module Notebook

**General Crypto Module Information**

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host ID</strong></td>
<td>prodpl</td>
</tr>
<tr>
<td><strong>Host description</strong></td>
<td>production lprar</td>
</tr>
<tr>
<td><strong>Crypto module index</strong></td>
<td>G00</td>
</tr>
<tr>
<td><strong>Crypto module type</strong></td>
<td>Crypto Coprocessor</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Crypto module enabled</td>
</tr>
</tbody>
</table>
## Authorities

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Role</th>
<th>Phone</th>
<th>E-mail</th>
<th>Addr</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>INITADM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Create Authority**
- **Change Authority**
- **Delete Authority**
- **Generate Signature Key**
### Domain Keys

<table>
<thead>
<tr>
<th>Status</th>
<th>Hash pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>New AES Master Key</td>
<td>Empty</td>
</tr>
<tr>
<td>Old AES Master Key</td>
<td>Empty</td>
</tr>
<tr>
<td>AES Master Key</td>
<td>Empty</td>
</tr>
<tr>
<td>Old AES Master Key</td>
<td>Valid</td>
</tr>
<tr>
<td>AES Master Key</td>
<td>Invalid</td>
</tr>
<tr>
<td>New ECC Master Key</td>
<td>Empty</td>
</tr>
<tr>
<td>Old ECC Master Key</td>
<td>Empty</td>
</tr>
<tr>
<td>ECC Master Key</td>
<td>Empty</td>
</tr>
<tr>
<td>Old ECC Master Key</td>
<td>Invalid</td>
</tr>
<tr>
<td>New DES Master Key</td>
<td>Empty</td>
</tr>
<tr>
<td>Old DES Master Key</td>
<td>Empty</td>
</tr>
<tr>
<td>DES Master Key</td>
<td>Empty</td>
</tr>
<tr>
<td>Old DES Master Key</td>
<td>Invalid</td>
</tr>
<tr>
<td>New Asymmetric Master Key</td>
<td>Empty</td>
</tr>
<tr>
<td>Old Asymmetric Master Key</td>
<td>Empty</td>
</tr>
<tr>
<td>Asymmetric Master Key</td>
<td>Invalid</td>
</tr>
</tbody>
</table>

### 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
- First...
- Last...

### Load single key part
- Intermediate...

### Clear

### Secure key part entry
Each crypto module gets updated

```
<table>
<thead>
<tr>
<th>Host</th>
<th>prodp1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto Module</td>
<td>GO2</td>
</tr>
<tr>
<td>Updating</td>
<td></td>
</tr>
</tbody>
</table>
```

```
<table>
<thead>
<tr>
<th>Host</th>
<th>prodp1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto Module</td>
<td>GO3</td>
</tr>
<tr>
<td>Updating</td>
<td></td>
</tr>
</tbody>
</table>
```

- Cancel

Trusted Key Entry
### Domain Keys

<table>
<thead>
<tr>
<th>New AES Master Key</th>
<th>Status</th>
<th>Hash pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Old AES Master Key</th>
<th>Status</th>
<th>Hash pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New AES Master Key</th>
<th>Status</th>
<th>Hash pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AES Master Key</th>
<th>Status</th>
<th>Hash pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Old AES Master Key</th>
<th>Status</th>
<th>Hash pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Trusted Key Entry (Part 2) - New DES-MK

- **DES Key:**
  - Status: Part full
  - Hash pattern: `6E2C12BC5A1751DB1152E90C03FF5D104`

- **Old DES Master Key:**
  - Status: Empty
  - Hash pattern: `0000000000000000000000000000000000000000000000000000000000000000`

- **New Asymmetric Master Key:**
  - Status: Empty
  - Hash pattern: `0000000000000000000000000000000000000000000000000000000000000000`

- **Old Asymmetric Master Key:**
  - Status: Empty
  - Hash pattern: `0000000000000000000000000000000000000000000000000000000000000000`

- **New Asymmetric Master Key:**
  - Status: Empty
  - Hash pattern: `0000000000000000000000000000000000000000000000000000000000000000`

- **Old Asymmetric Master Key:**
  - Status: Empty
  - Hash pattern: `0000000000000000000000000000000000000000000000000000000000000000`
Pre-TKE V7.3 – Finish the MK Chg

---

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.

---

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

![Image of Crypto Processor Module Group Administration interface]

- Select Target
- Smart card in reader 1
- Smart card in reader 2
- Binary file
- Print file

Hash pattern
8F8B4EE2782BAAB772669E6D1A31E70C4
DD20A717C842FC0C5D0189580FEB7F8B4
DD20A717C842FC0C5D0189580FEB7F8B4
00000000000000000000000000000000000000
AE519E5F52BAC4855A8F15364996604B6
15D7602B7CD493BCA7709D4955FEFEEB

Trusted Key Entry
- New Symmetric Master Key
- New Asymmetric Master Key
- Operational Key
  - Operational Key - EXPORTER
  - Operational Key - IMPORTER
  - Operational Key - IPINENC
  - Operational Key - OPINENC
  - Operational Key - PINENC
  - Operational Key - PINVER
  - Operational Key - IMP-PKA
  - Operational Key - DATA
  - Operational Key - DATAC
  - Operational Key - DATAM

General | Keys | Controls
Completing the Operational Key Load

```
COMMAND ===>  ICSF Coprocessor Management ======== Row 1 to 2 of 2
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.

<table>
<thead>
<tr>
<th>CRYPTO FEATURE</th>
<th>SERIAL NUMBER</th>
<th>STATUS</th>
<th>AES</th>
<th>DES</th>
<th>ECC</th>
<th>RSA</th>
<th>P11</th>
</tr>
</thead>
<tbody>
<tr>
<td>k 4C01</td>
<td>16C8X376</td>
<td>Active</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>. 4C03</td>
<td>16C8P352</td>
<td>Active</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>

*****************************************************************************************

COMMAND ===>  ICSF - Operational Key Load

Coproessor 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
### 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:

<table>
<thead>
<tr>
<th>Key type</th>
<th>Description</th>
<th>Origin</th>
<th>MDC-4</th>
<th>SHA-1</th>
<th>ENC-ZERO</th>
<th>AES-VP</th>
<th>Control vector or key attributes</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICSF DES...</td>
<td>Sym-Key Pa...</td>
<td>Crypto...</td>
<td>6E2C1...</td>
<td>16E6F...</td>
<td>60D600BA</td>
<td></td>
<td></td>
<td>16</td>
</tr>
<tr>
<td>ICSF asy...</td>
<td>ASYM-Key F...</td>
<td>Crypto...</td>
<td>61A7B...</td>
<td>C1D6...</td>
<td>5CB78023</td>
<td></td>
<td></td>
<td>24</td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th>Key type</th>
<th>Description</th>
<th>Origin</th>
<th>MDC-4</th>
<th>SHA-1</th>
<th>ENC-ZERO</th>
<th>AES-VP</th>
<th>Control vector or key attributes</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICSF DES...</td>
<td>Sym-Key fin...</td>
<td>Crypto...</td>
<td>73A0A...</td>
<td>9965A...</td>
<td>60A13730</td>
<td></td>
<td></td>
<td>16</td>
</tr>
<tr>
<td>ICSF asy...</td>
<td>ASYM-Key p...</td>
<td>Crypto...</td>
<td>D9497...</td>
<td>1B306...</td>
<td>E403779D</td>
<td></td>
<td></td>
<td>24</td>
</tr>
</tbody>
</table>
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
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 Enhancement: Full Function Migration Wizard for EP11
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](http://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](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