

# Trusted Key Entry (TKE): Key Ceremony Demo

Jessica Bonner  
IBM

February 28, 2007  
Session Number 5503



# Trademarks



The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

- IBM\*
- Linux
- System z\*
- S/390\*
- zSeries\*
- OS/2\*
- z9\*

\* Registered trademarks of IBM Corporation

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

## Objective

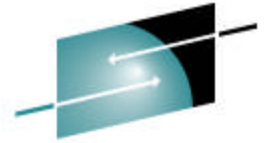
---

- Demonstrate the steps needed to customize a TKE workstation
- Show steps needed to load master keys to the host
- Walk through the steps to initialization the host CKDS and PKDS

## Steps to TKE Workstation Setup

---

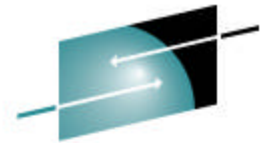
- Crypto Adapter Initialization
- SCUP Application Setup
- CNM Application Setup
- TKE Application Setup



**S H A R E**

Technology • Connections • Results

# Crypto Adapter Initialization

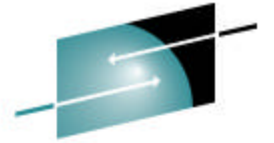


# TKE's IBM Crypto Adapter Initialization

```
csulcni.sh
All modifications to the cryptographic coprocessor will be lost.
Would you like to continue? (Y/N) [default=N]
y
Would you like to prepare your cryptographic coprocessor for Smart Card or Pass
Phrase use? (S/P) [default=P]
P ← Specify P for Passphrase or S for Smart Card
The cryptographic coprocessor will be prepared for Pass Phrase use.

Initialization Output
-----
Cryptographic facility initialized.
Time synchronized with host
Created user role DEFAULT
Created user role TKEADM
Created user role KEYMAN1
Created user role KEYMAN2
Created user role TKEUSER
Created user profile TKEADM
Created user profile KEYMAN1
Created user profile KEYMAN2
Created user profile TKEUSER
Master key set.
DES Key Storage initialized using desstore.dat
PKA Key Storage initialized using pkastore.dat
Created user role DEFAULT
Press <Enter> to exit.
```

The default roles and profiles are loaded into the 4764 in the workstation for logon.

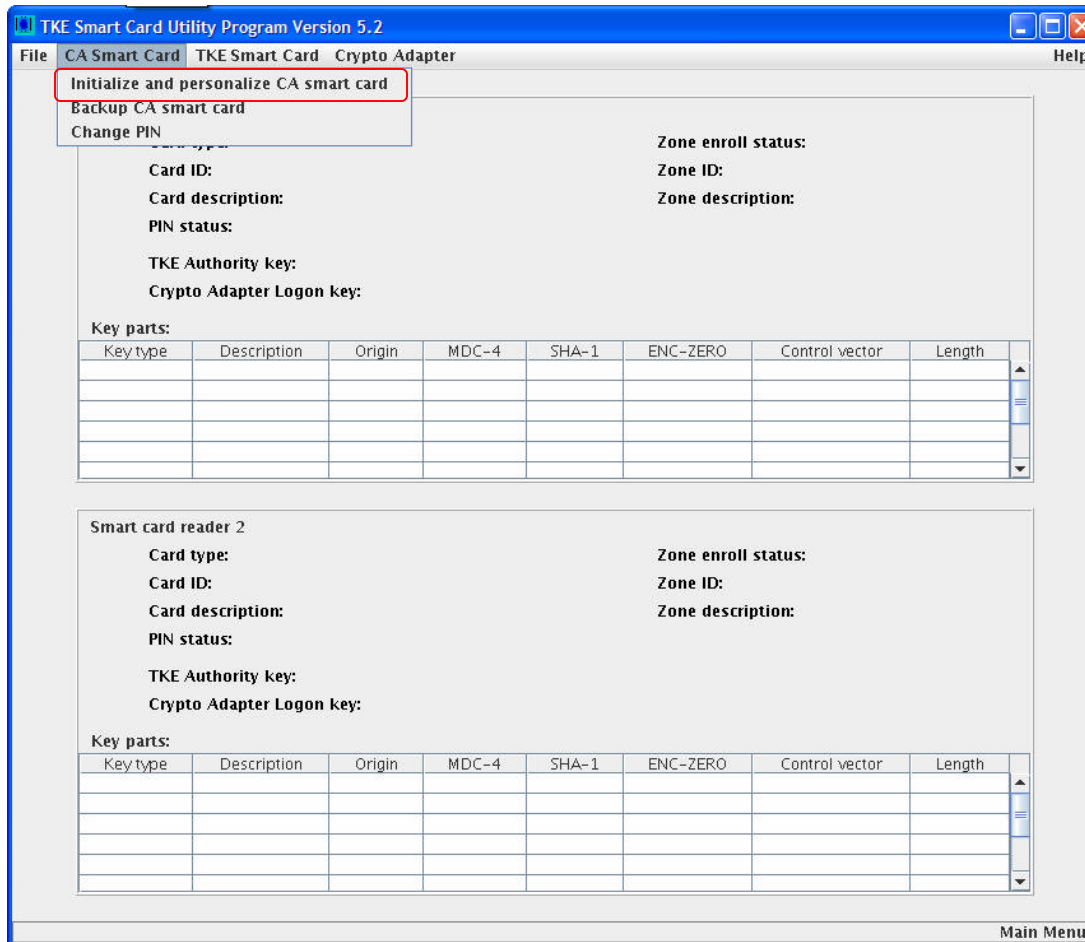


**SHARE**

Technology • Connections • Results

# SCUP Application Setup

# Initialize and personalize CA smart card



TKE Smart Card Utility Program Version 5.2

File CA Smart Card TKE Smart Card Crypto Adapter Help

Initialize and personalize CA smart card  
Backup CA smart card  
Change PIN

Zone enroll status:  
Zone ID:  
Zone description:

Card ID:  
Card description:  
PIN status:  
TKE Authority key:  
Crypto Adapter Logon key:

Key parts:

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	Control vector	Length

Smart card reader 2

Zone enroll status:  
Zone ID:  
Zone description:

Card type:  
Card ID:  
Card description:  
PIN status:  
TKE Authority key:  
Crypto Adapter Logon key:

Key parts:

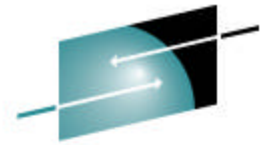
Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	Control vector	Length

Main Menu

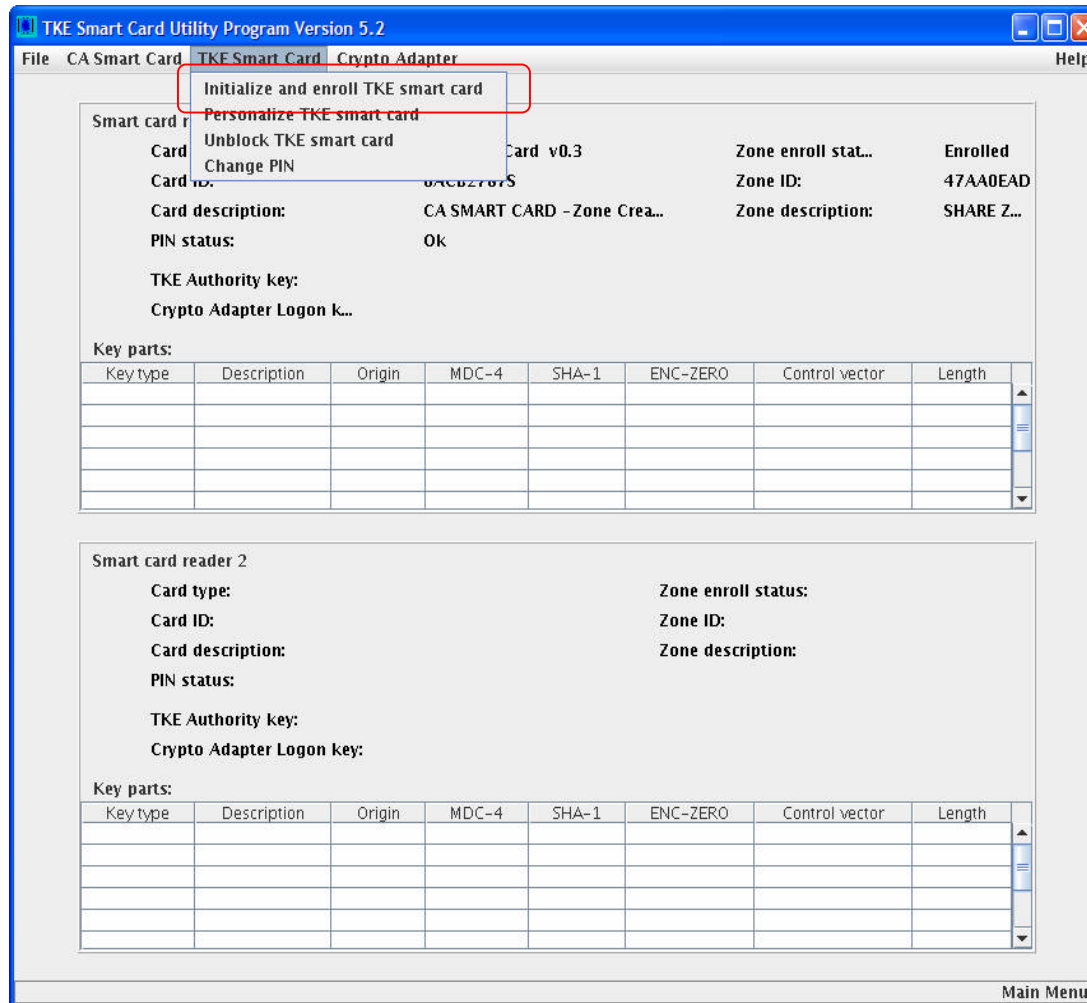
## Steps performed by TKE Administrators:

1. Insert Smart Card into reader
2. At prompt have Admin1 enter first 6-digit pin twice
3. Then have Admin2 enter second 6-digit pin twice
4. Enter Zone Description
5. Enter Optional Card Description



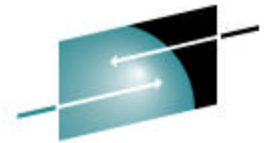


# Initialize TKE smart card

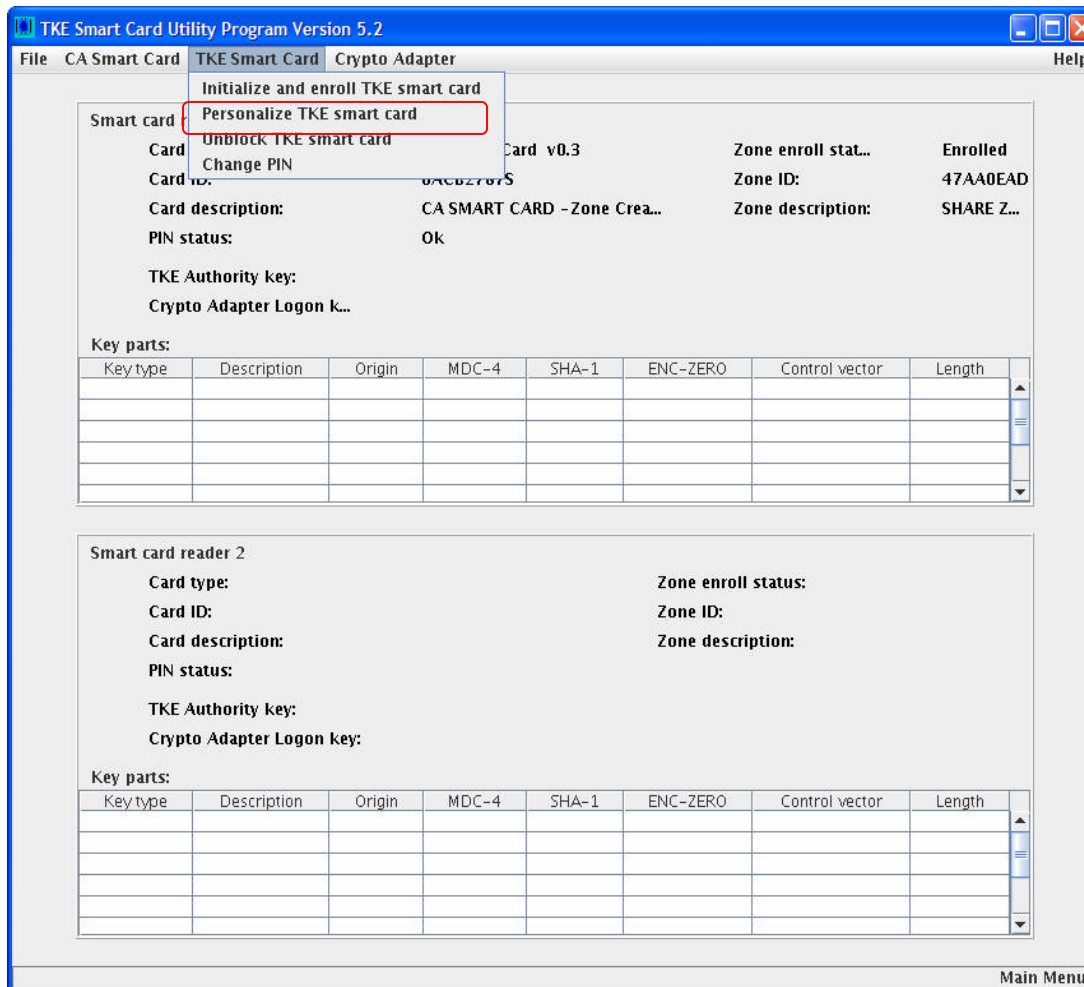


## Steps performed by TKE Administrators:

1. Insert CA Smart Card into reader 1
2. At prompt have Admin1 enter first 6-digit pin
3. Then have Admin2 enter second 6-digit pin
4. Insert TKE card into reader 2 at prompt

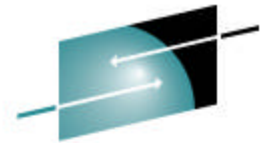


# Personalize TKE smart card



## Steps performed by TKE Card User:

1. Insert TKE card into reader 2 at prompt
2. Enter the 4-digit PIN twice for this TKE smart card
3. Optionally enter a description



# Enroll Crypto Adapter

TKE Smart Card Utility Program Version 5.2

File CA Smart Card TKE Smart Card **Crypto Adapter** Help

**Enroll Crypto Adapter**  
**View current zone**

Smart card reader 1

Card type: CA Smart Card v0.3      Zone enroll stat... Enrolled  
Card ID: 0ACB2787S      Zone ID: 47AA0EAD  
Card description: CA SMART CARD - Zone Crea...      Zone description: SHARE Z...  
PIN status: OK

TKE Authority key:  
Crypto Adapter Logon k...

Key parts:

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	Control vector	Length

Smart card reader 2

Card type: TKE Smart Card v0.3      Zone enroll status: Enrolled  
Card ID: BD058BB0S      Zone ID: 47AA0EAD  
Card description: SHARE TKE CARD      Zone description: SHARE ZONE  
PIN status: OK

TKE Authority key: Not present  
Crypto Adapter Logon key: Not present

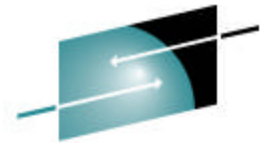
Key parts:

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	Control vector	Length

Main Menu

## Steps performed by TKE Administrators:

1. Insert CA Smart Card into reader 1
2. At prompt have Admin1 enter first 6-digit pin
3. Then have Admin2 enter second 6-digit pin



# View Crypto Adapter Zone

The screenshot shows the TKE Smart Card Utility Program Version 5.2 interface. It displays details for a smart card reader and a smart card. A dialog box titled "Crypto Adapter - View current zone" is open, showing the current zone information for the selected card. Red circles highlight the zone ID "47AA0EAD" in both the main interface and the dialog box.

Smart card reader 1

Card type: CA Smart Card v0.3      Zone enroll stat...: **Enrolled**

Card ID: 0ACB2787S      Zone ID: **47AA0EAD**

Card description: CA SMART CARD -Zone Crea...      Zone description: SHARE Z...

PIN status: OK

TKE Authority key:

Key parts:

Key type	Description	Origin	MDC-4	SHA-1	ENC-ZERO	Control vector	Length

Smart card 1

Card ID: BD058BB0S      Zone ID: **47AA0EAD**

Card description: SHARE TKE CARD      Zone description: SHARE ZONE

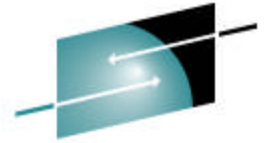
PIN status: OK

TKE Authority key: Not present

Crypto Adapter Logon key: Not present

Main Menu

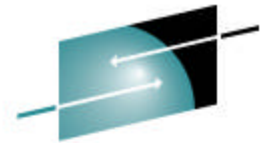
By viewing the Crypto Adapter Zone, you can see that all three entities have the same zone.



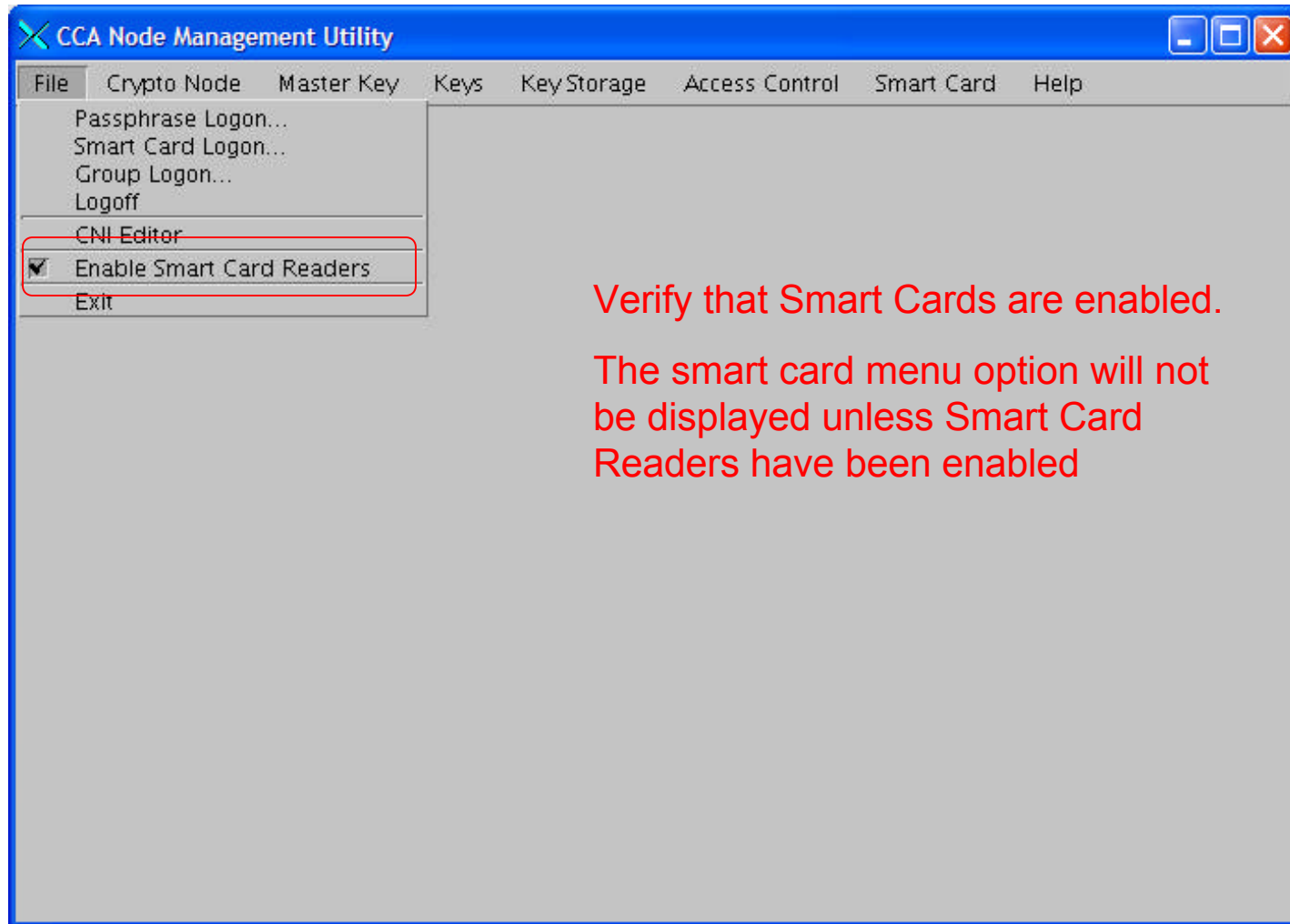
**S H A R E**

Technology • Connections • Results

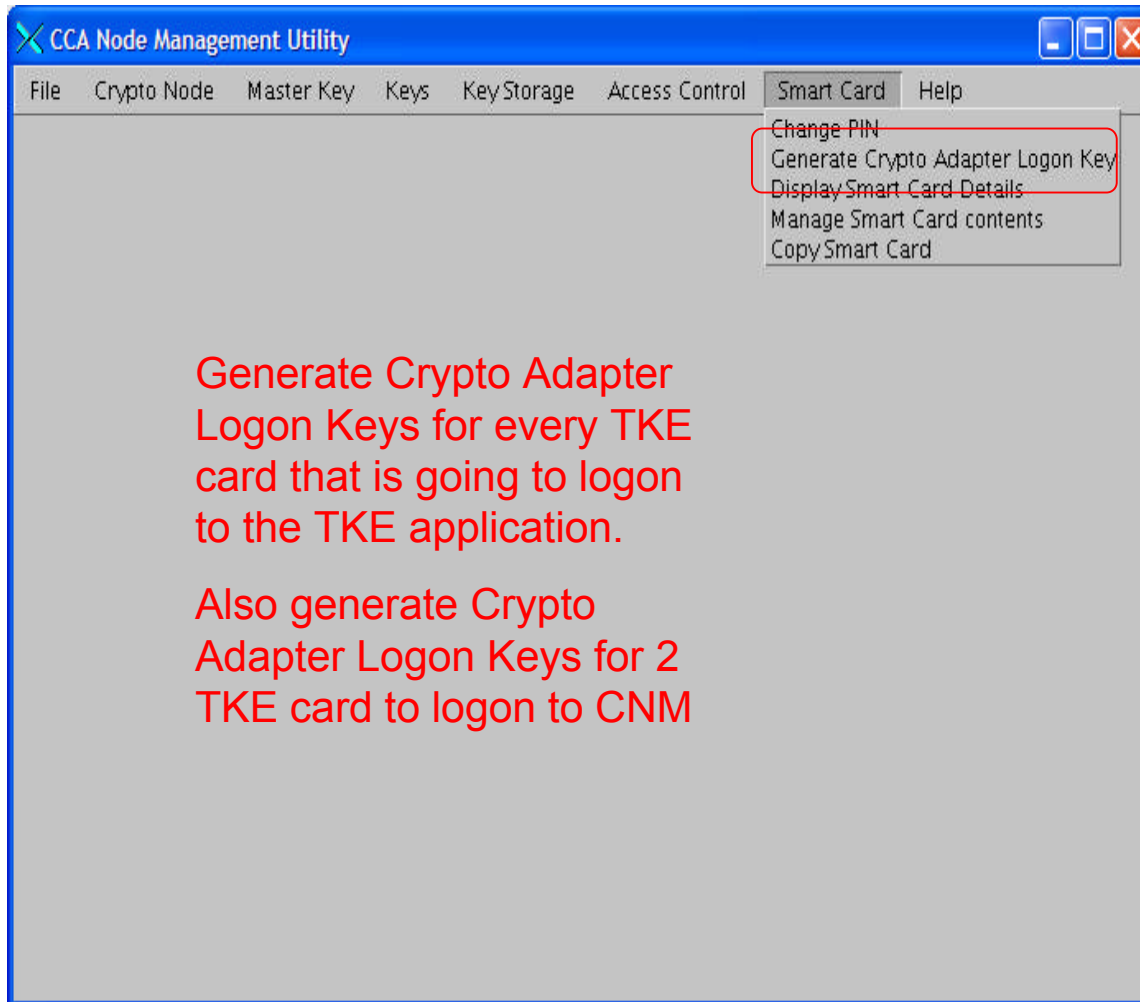
# CNM Application Setup



**SHARE**  
Technology • Connections • Results



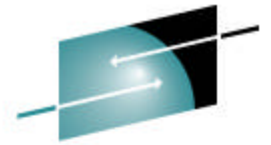
# Generate Crypto Adapter Logon Keys



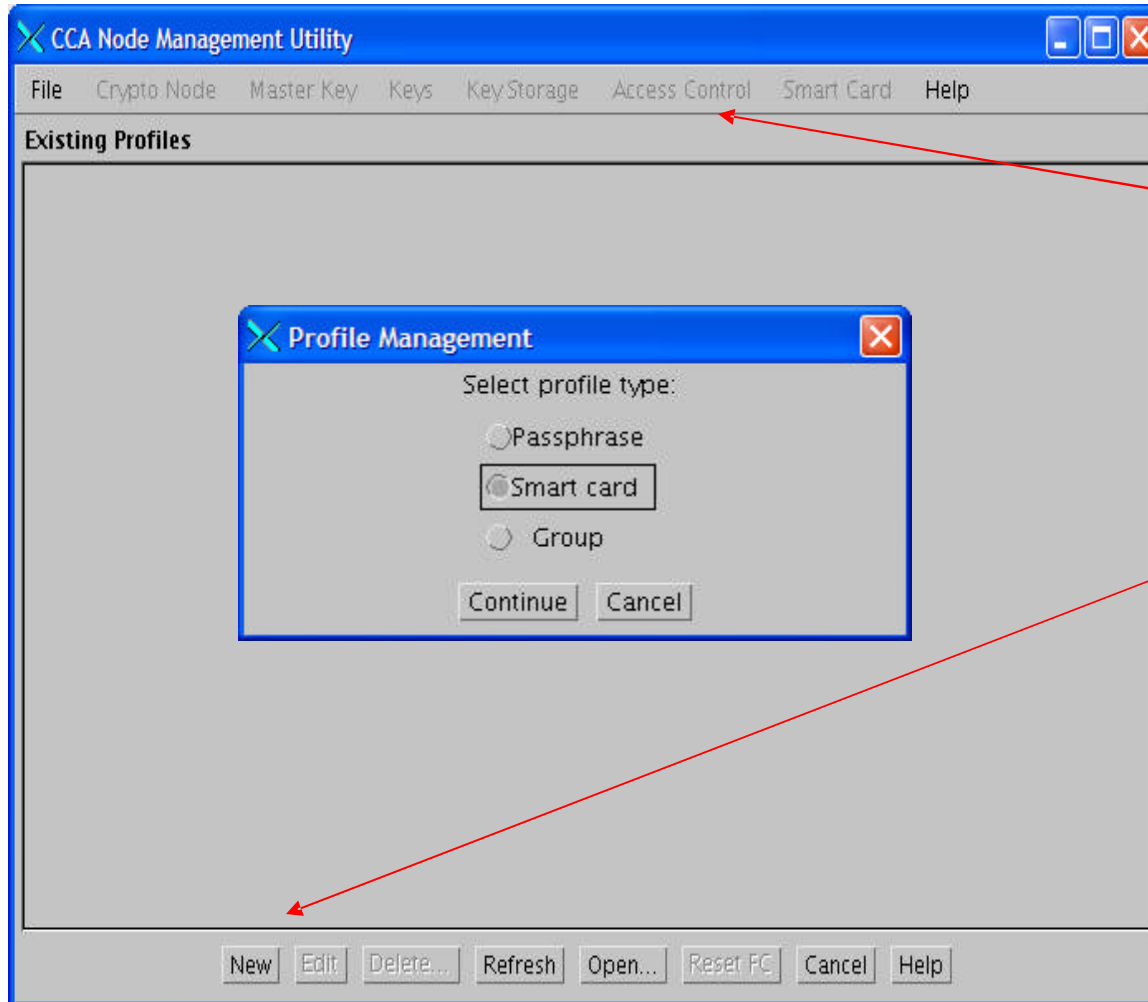
## Steps performed by TKE Card User:

1. Insert TKE smart card into Smart Card Reader 2.
2. Enter 4-digit PIN
3. Enter User ID for the smart card

Repeat these steps for each TKE card that needs a Crypto Adapter Logon key.



## Create a new Smart Card Profile



### Steps performed by TKE Card User:

1. Select Access Control menu option
2. Select Profiles
3. Select New
4. Select Smart Card, press Continue

Repeat these steps for each TKE smart card that will logon to the 4764.



# Create a new Smart Card Profile cont...



CCA Node Management Utility

File Crypto Node Master Key Keys KeyStorage Access Control Smart Card Help

User ID: SHARE

Comment: [Empty]

Activation Date: 02/06/2008

Expiration Date: 02/06/2009

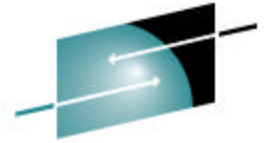
Role: SCKEUSR (Dropdown menu open showing: DEFAULT, SCKEADM, SCKEUSR)

Public modulus:  
AF72DDA5C03EE01C6FF76495E322F0932E32F66C81EC3C28AB94F83C9CAB9D87  
0B01D54297788FF2BD47FBA7C9AEC21D308A273F27BAF0D3F6A3C6C021F02519  
DDFD0A6AB56D463FD20D935B2334E6A19F8C44BADAF59D59FE535B38F7F0A3AE  
A70DD6BAF0DB5EBFE0B07F9E9C8EF1A649529AE9C6B72A0508D6EA11EE26177B

Open... Save... Load Read Smart Card List Cancel Help

## Steps performed by TKE Card User:

5. Insert TKE smart card into Smart Card Reader 2.
6. Enter 4-digit PIN
7. Change expiration date
8. Select Role from the list
9. Select Load

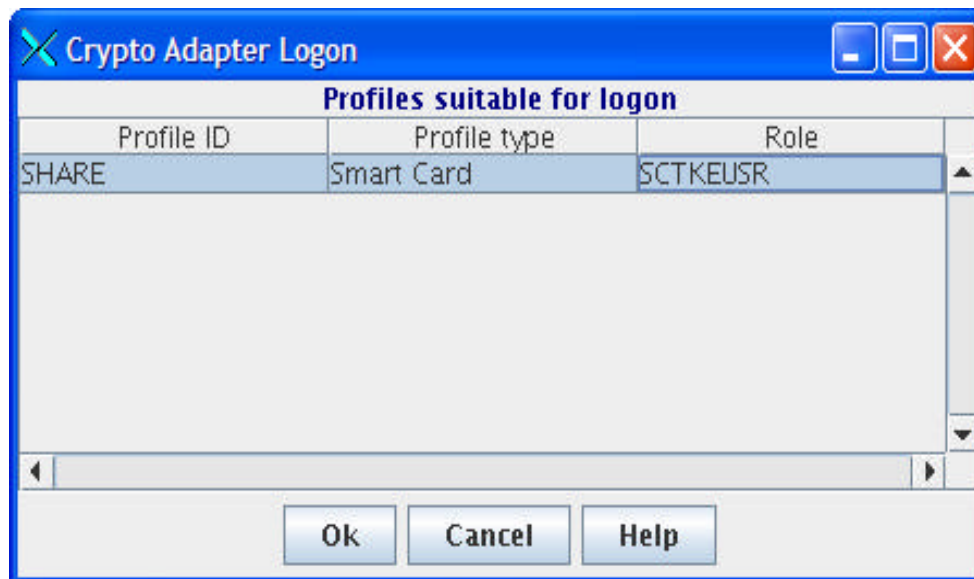


**S H A R E**

Technology • Connections • Results

# TKE Application Setup

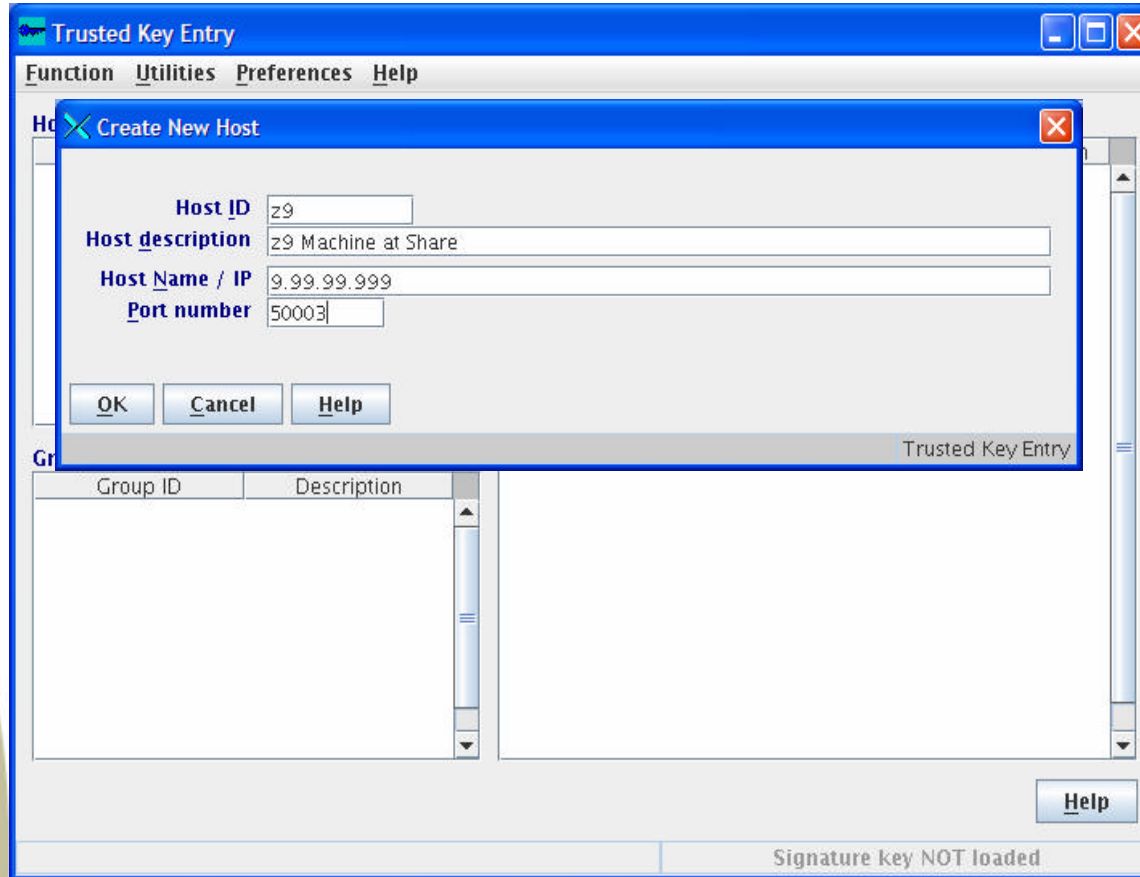
# Logon to TKE



## Steps performed by the TKE Card User:

1. Highlight a Profile ID, select OK
2. Insert TKE Smart Card into smart card reader 2
3. Enter 4-digit PIN for TKE Smart Card

# Create a Host



Trusted Key Entry

Function Utilities Preferences Help

Host ID: z9

Host description: z9 Machine at Share

Host Name / IP: 9.99.99.999

Port number: 50003

OK Cancel Help

Group ID	Description
----------	-------------

Trusted Key Entry

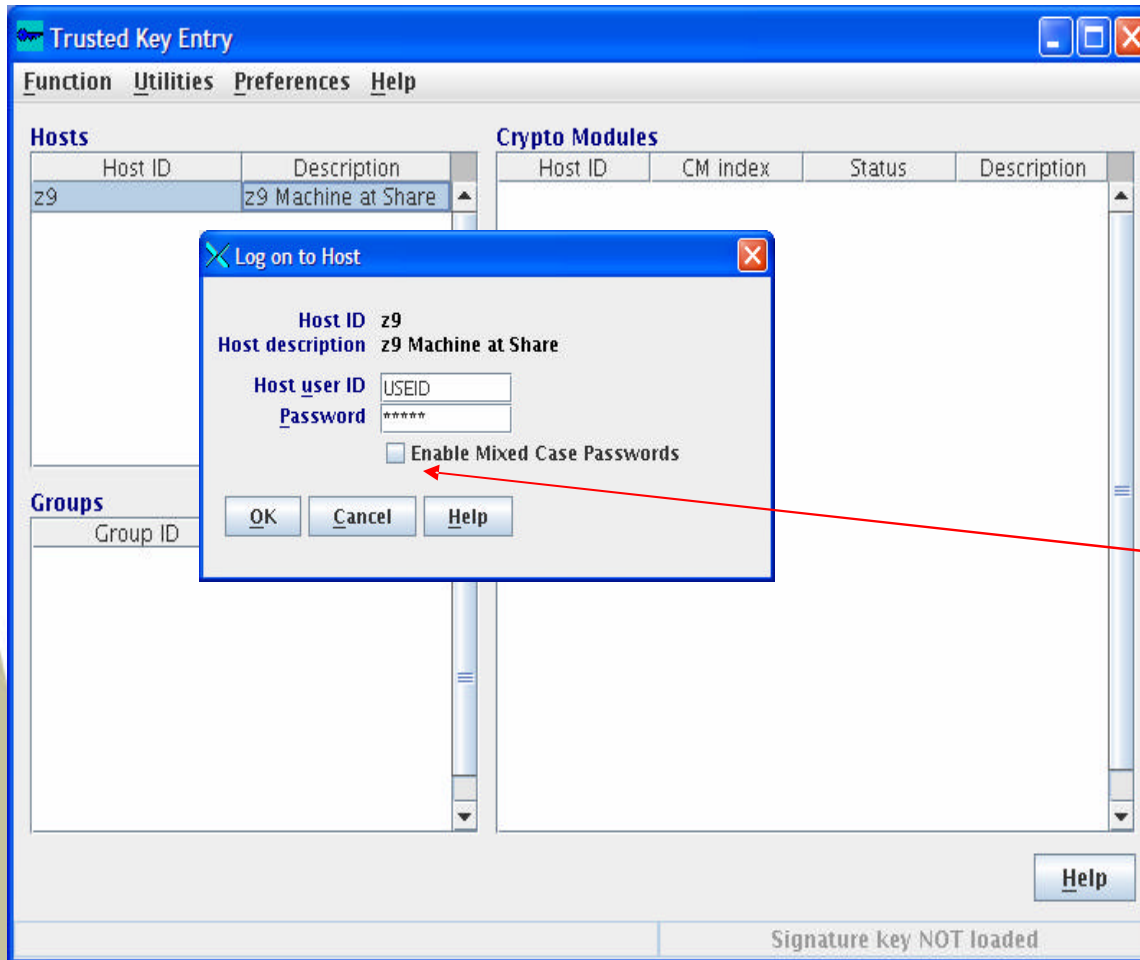
Help

Signature key NOT loaded

**Steps performed owner of the Host ID:**

1. Enter Host ID
2. Enter Host description, this field is optional.
3. Enter Host Name/IP
4. Enter Port number

# Logon to the Host

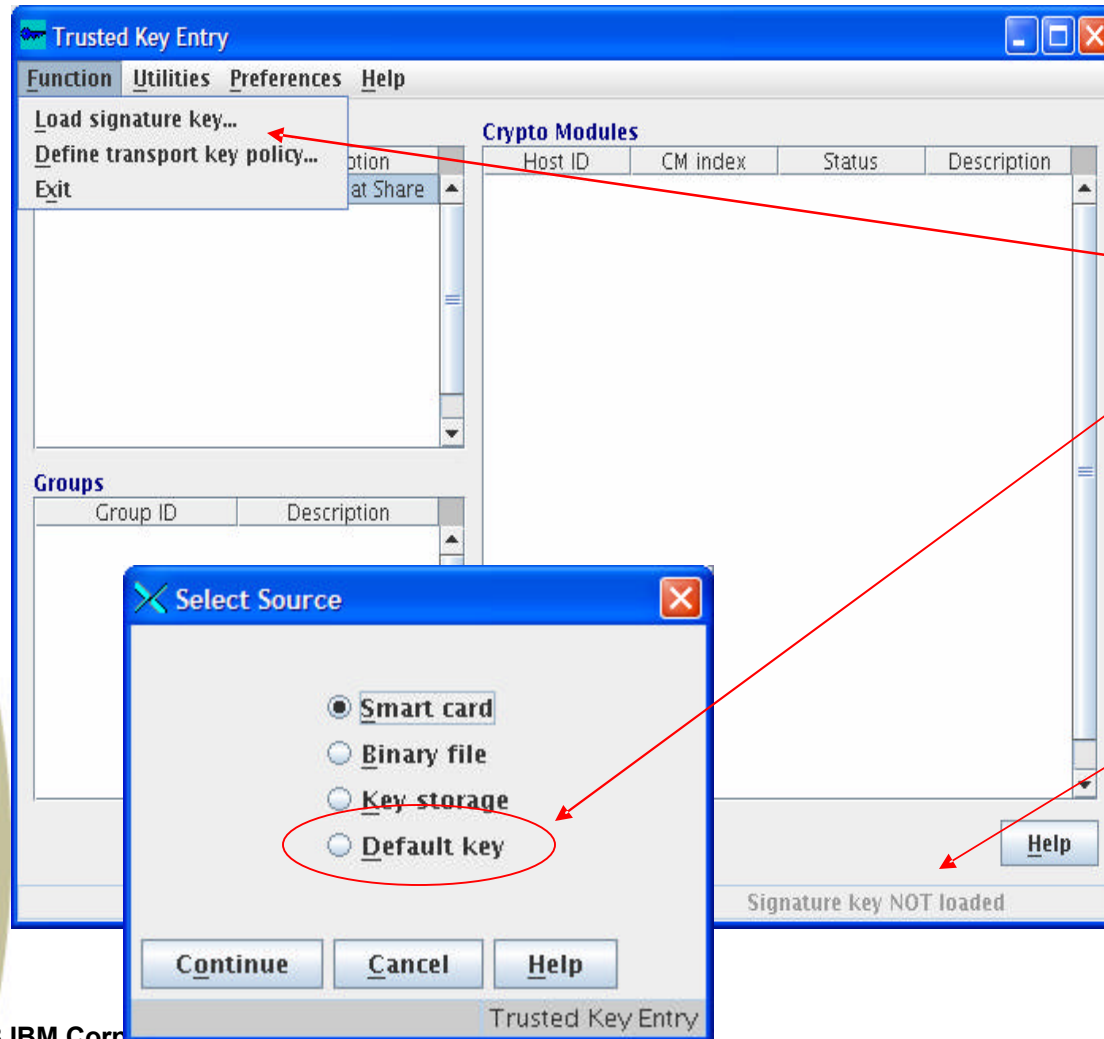


## Steps performed by the owner of the Host ID:

1. Right click on Host ID, select Open Host
2. Enter RACF Host user ID and Password

If your system uses mixed case passwords, select the Enable Mixed Case Passwords box

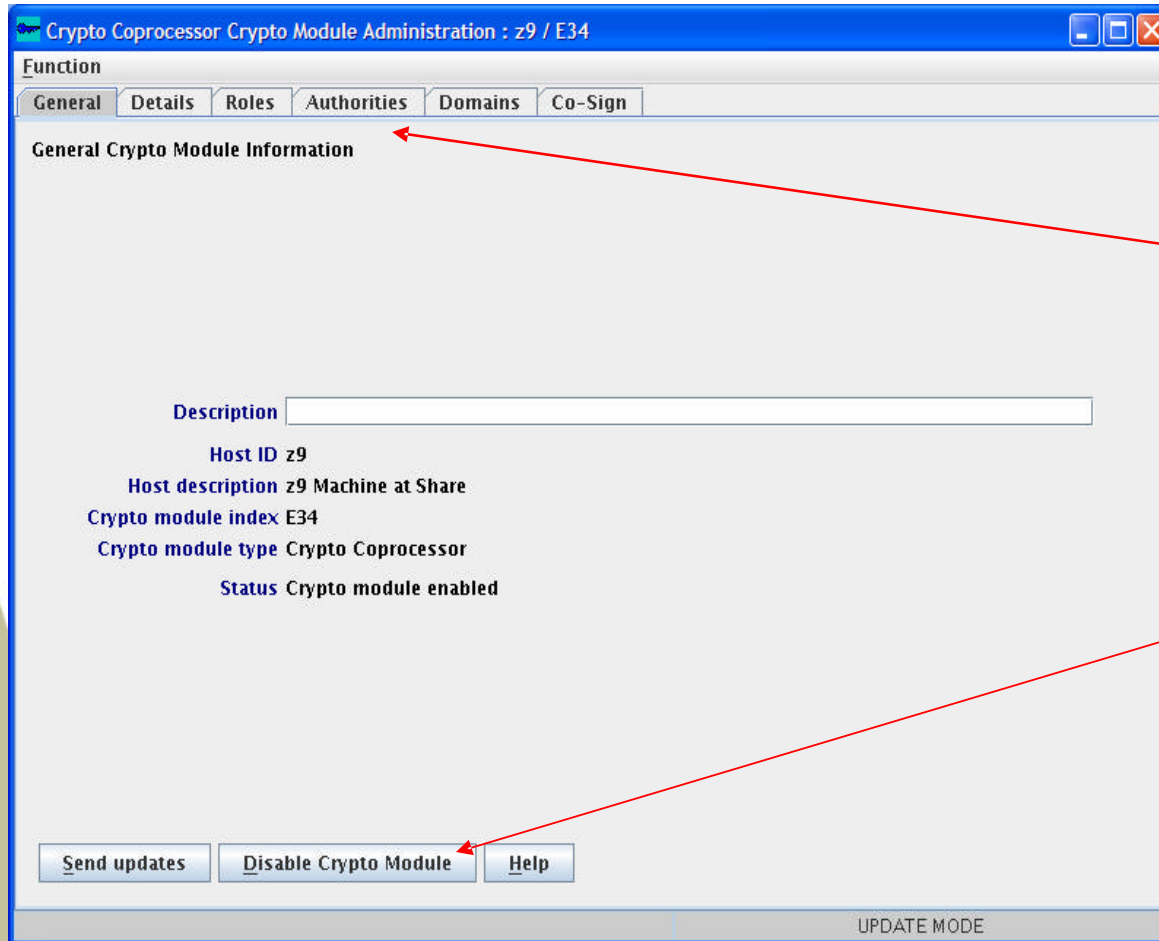
# Load authority signature key



## Steps performed by the TKE Administrator:

1. Select the Functions Menu Options
2. Select Load signature keys...
3. Select Default Key
4. Verify the authority index is 0
5. At the bottom of the window Signature key loaded will be displayed

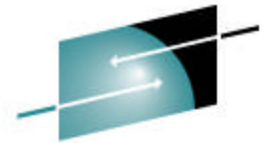
# Crypto Coprocessor Notebook



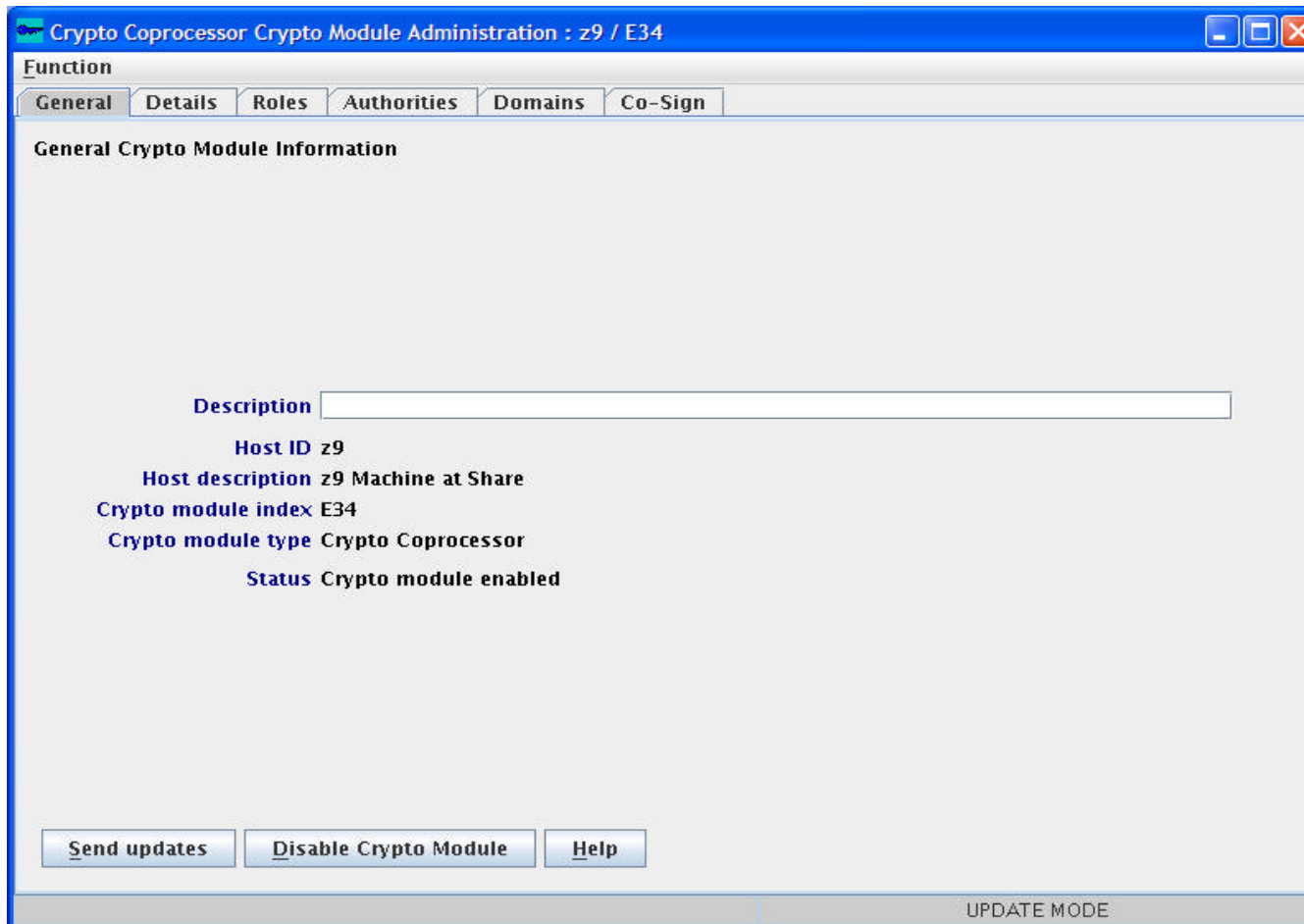
This is a view of the Crypto Coprocessor Notebook. The user can use the tabs across navigate to different panels.

From this panel a user can also disable a Crypto Module. A disable from this panel will make the card disabled for all LPARS/Domains.

# Crypto Coprocessor Notebook



**SHARE**  
Technology • Connections • Results



The screenshot shows a window titled "Crypto Coprocessor Crypto Module Administration : z9 / E34". The window has a blue title bar and standard Windows window controls (minimize, maximize, close). Below the title bar is a "Function" menu with tabs for "General", "Details", "Roles", "Authorities", "Domains", and "Co-Sign". The "General" tab is selected, and the main content area is titled "General Crypto Module Information".

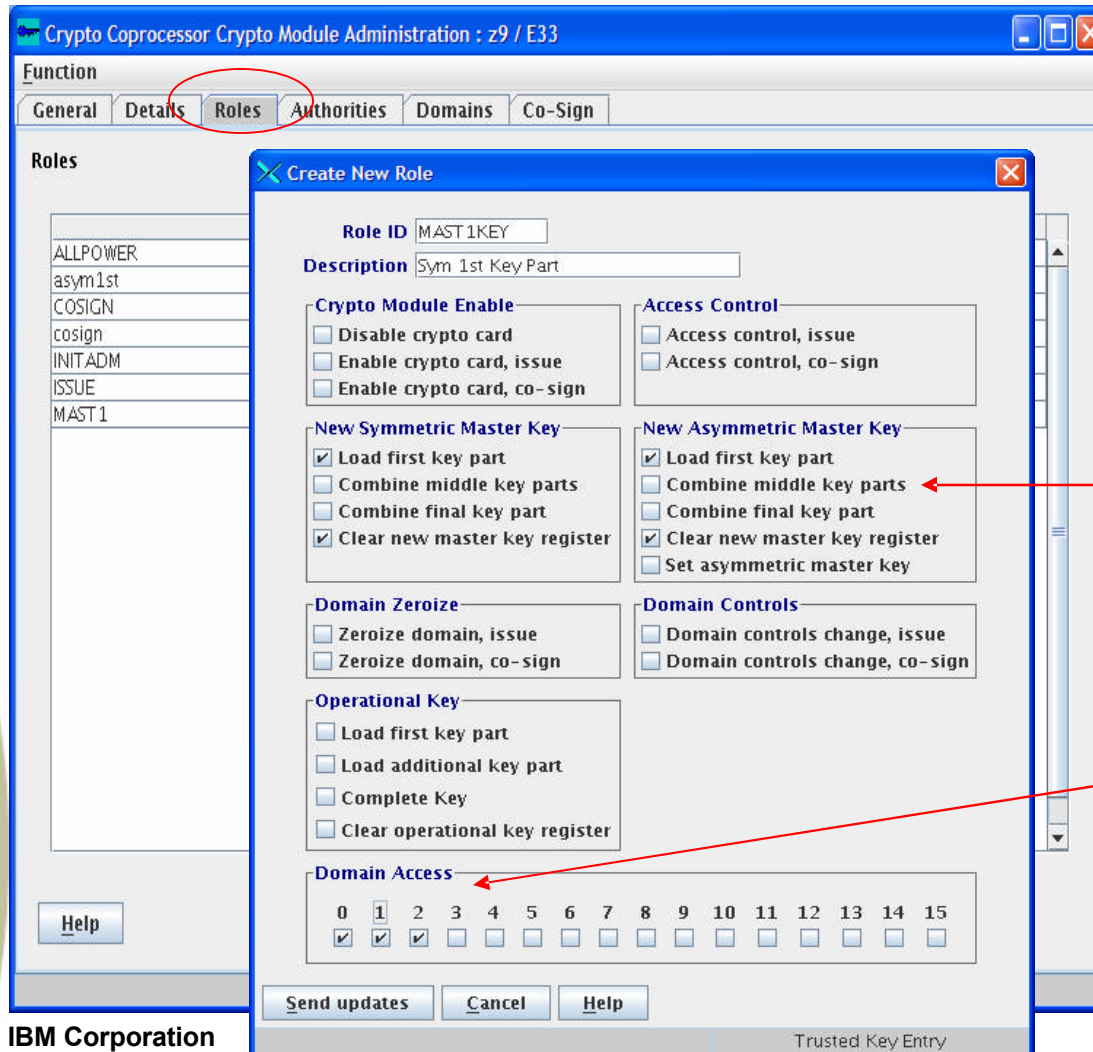
**Description**

**Host ID** z9  
**Host description** z9 Machine at Share  
**Crypto module index** E34  
**Crypto module type** Crypto Coprocessor  
**Status** Crypto module enabled

At the bottom of the window, there are three buttons: "Send updates", "Disable Crypto Module", and "Help". The status bar at the bottom right of the window displays "UPDATE MODE".



# Create a Role

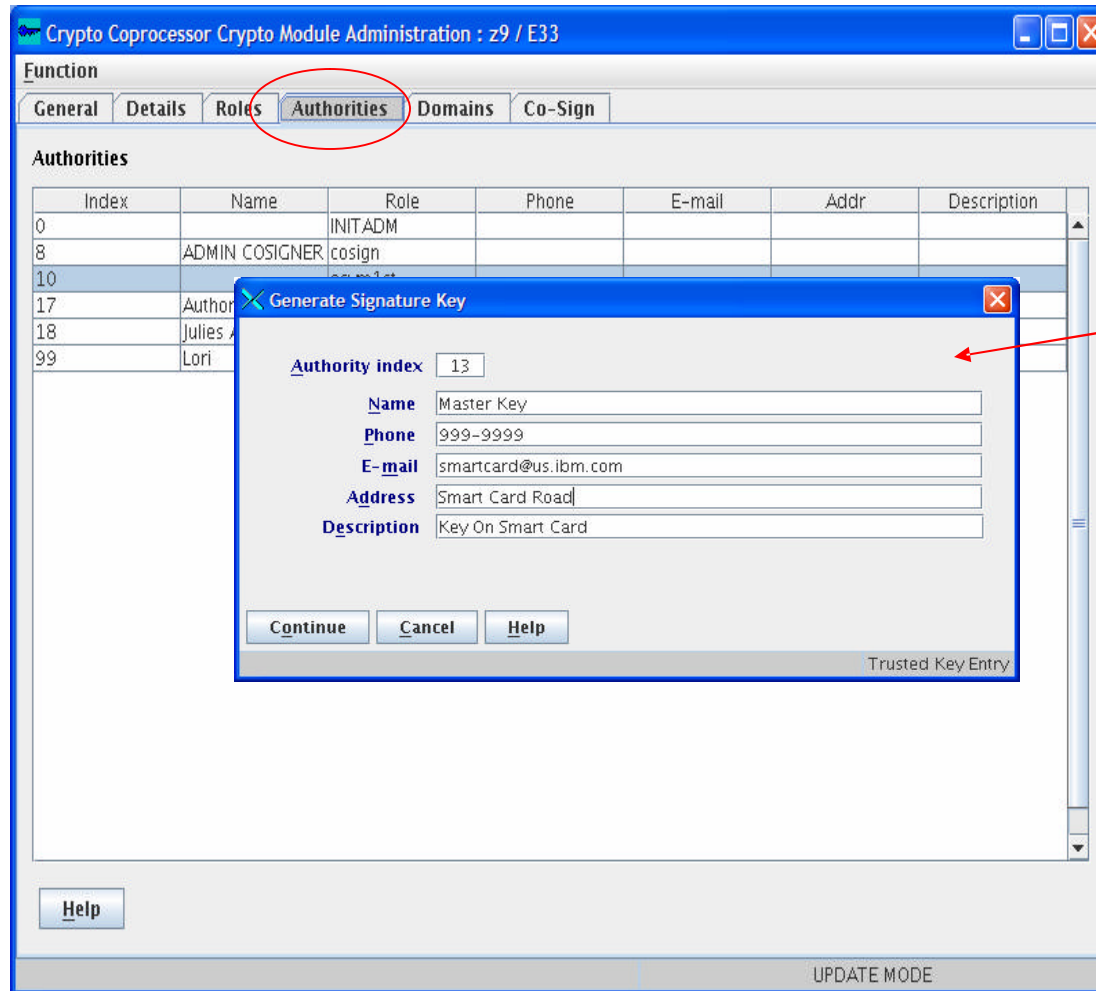


## Steps performed by the TKE Administrator:

1. Select the roles tab
2. Right click and select Create Role
3. Enter Role ID
4. Enter Description, this field is optional.
5. Select functions to enable
6. Select Domain Access

This role will be able to load Symmetric and Asymmetric First key part to Domains 0, 1, and 2

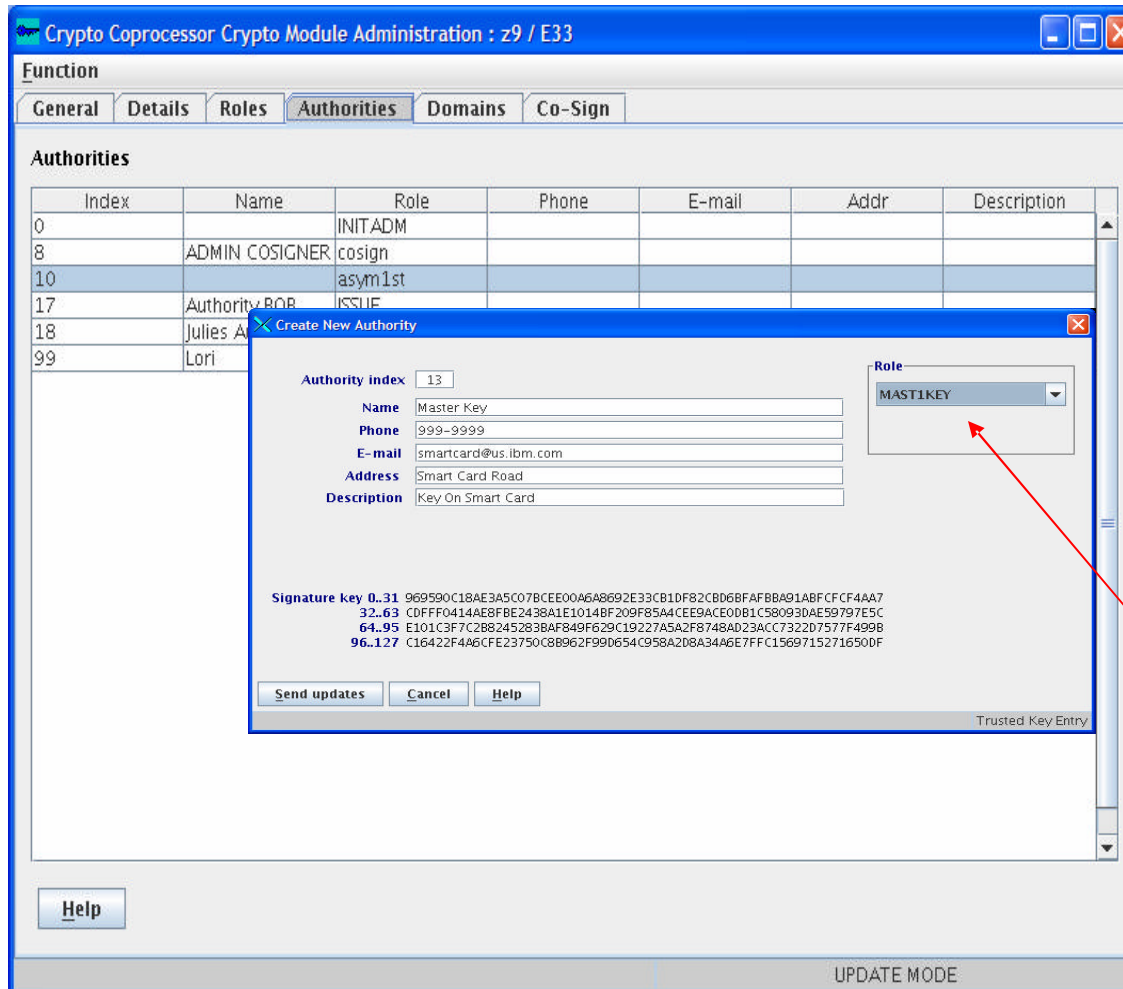
# Generate an Authority Signature Key



## Steps performed by the TKE Card User :

1. Select the Authorities tab
2. Right click in the authorities window and select Generate Signature Key
3. Select an Authority Index not used
4. Enter Authority Contact information
5. Select Location to save the signature key to.
6. Insert Smart Card
7. Enter 4-digit pin

# Create an Authority



**Function**  
General Details Roles **Authorities** Domains Co-Sign

**Authorities**

Index	Name	Role	Phone	E-mail	Addr	Description
0		INITADM				
8	ADMIN COSIGNER	cosign				
10		asym1st				
17	Authority BOB	ISSUE				
18	Julies A					
99	Lori					

**Create New Authority**

Authority index: 13

Name: Master Key

Phone: 999-9999

E-mail: smartcard@us.ibm.com

Address: Smart Card Road

Description: Key On Smart Card

Role: MAST1KEY

Signature key 0..31: 969590C18AE3A5C078CEE00A6A8692E33CB1DF82CD06BFAFBB891ABFCFCF4AA732.63 C0FF0414A8FBFE2438A1E1014BF209F8544CE9ACE0DB1C58093DAE59797E5C64.95 E101C3F7C2B82452838AF849F629C19227A5A2F8748AD23ACC7322D7577F499896.127 C16422F4A6CFE23750C8B962F990654C958A2D8A34A6E7FFC15697152716500F

Send updates Cancel Help

Trusted Key Entry

UPDATE MODE

## Steps performed by the TKE Card User :

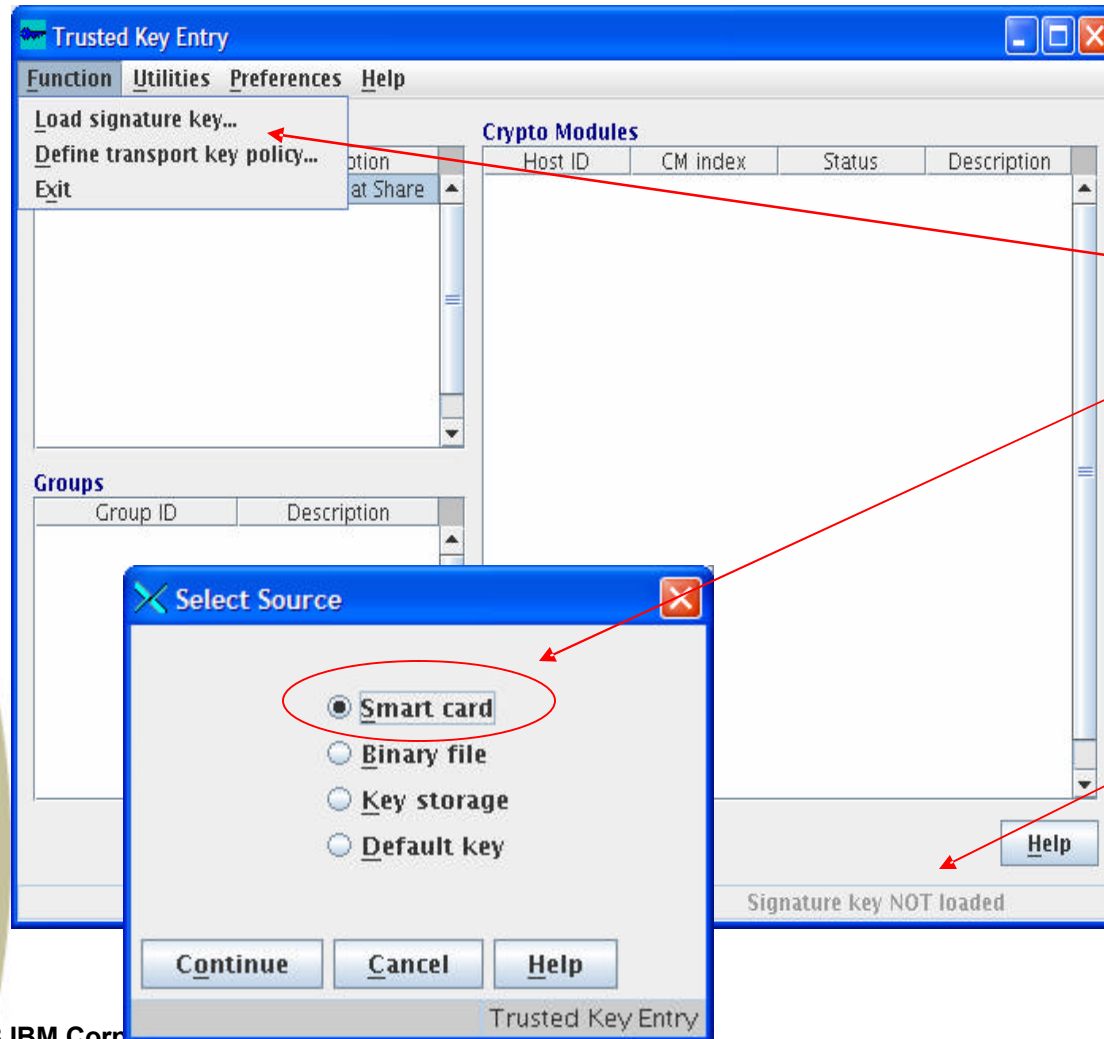
1. Right click in the authorities window and select Create Authority
2. Select Location to load the signature key from Smart Card
3. Insert Smart Card into Smart Card Reader 2
4. Enter 4-digit pin
5. Select the Role from the list and select Send updates

## Steps to Load the Master Keys

---

- Load authority signature key
- Generate Key Parts
- Load key Parts
- Disable PKA Callable Services
- Set Asymmetric Master Key

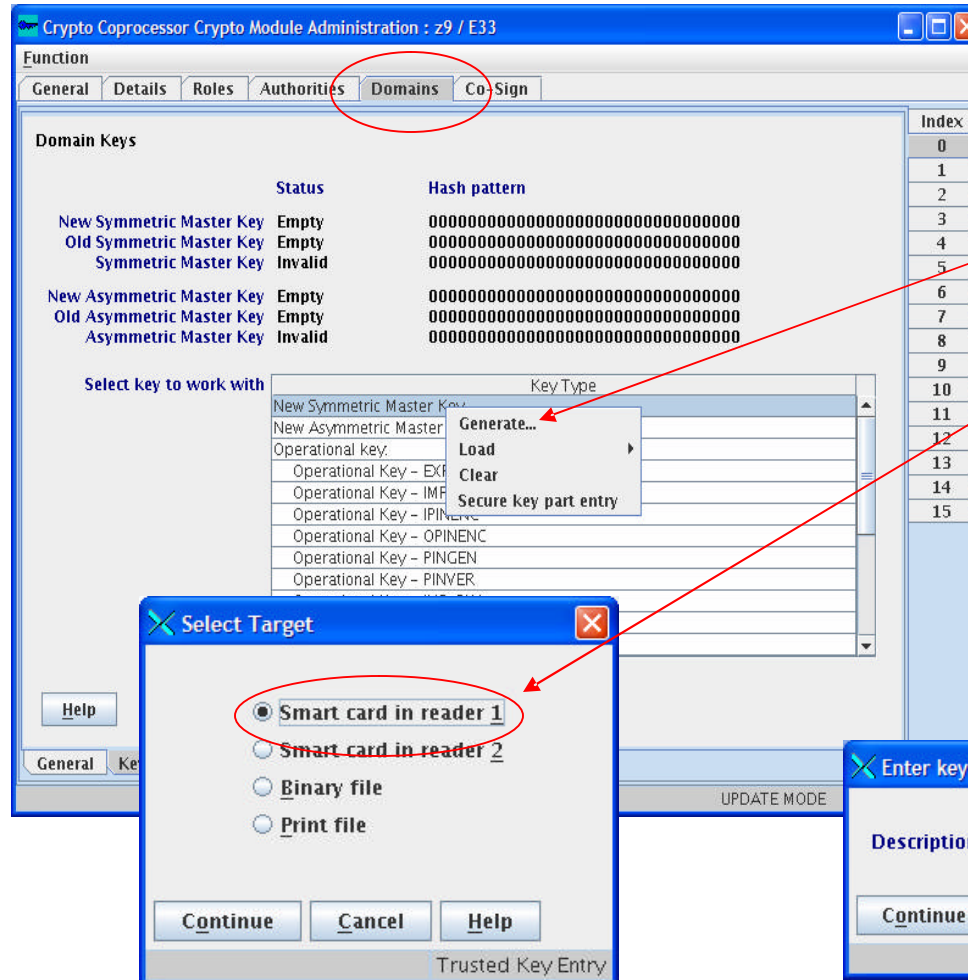
# Load authority signature key



## Steps performed by the TKE Card User :

1. Select the Functions Menu Options
2. Select Load signature keys...
3. Select Smart Card Reader as source
4. Insert Smart Card into Smart Card Reader
5. Enter 4-digit pin
6. Verify the authority index for this smart card
7. At the bottom of the window Signature key loaded will be displayed

# Generate Key Parts



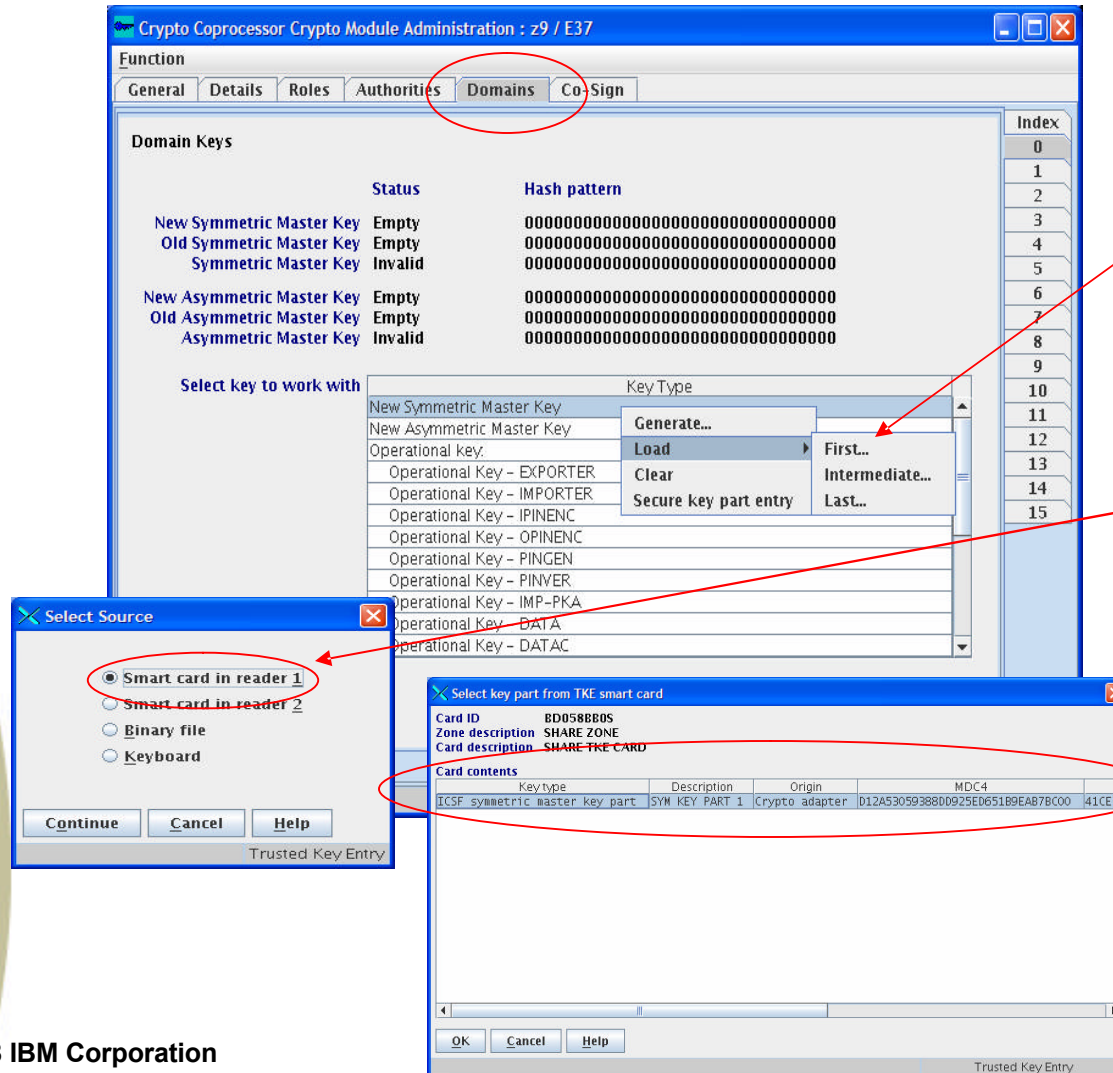
The screenshot shows the 'Crypto Coprocessor Crypto Module Administration' window with the 'Domains' tab selected. A table of 'Domain Keys' is visible, with columns for 'Status' and 'Hash pattern'. A context menu is open over the 'New Symmetric Master Key' entry, showing options like 'Generate...', 'Load', 'Clear', and 'Secure key part entry'. Two dialog boxes are overlaid: 'Select Target' with 'Smart card in reader 1' selected, and 'Enter key part description' with 'SYM KEY PART 1' entered in the description field.

Index	Status	Hash pattern
0		
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		

## Steps performed by the TKE Card User :

1. Select the Domains tab
2. Right click on a master key type
3. Select Smart Card Reader as the target
4. Insert Smart Card into Smart Card Reader
5. Enter 4-digit pin
6. Enter description for the master key part.

# Load Master Key Parts



The screenshot shows the 'Crypto Coprocessor Crypto Module Administration' window with the 'Domains' tab selected. A context menu is open over a 'New Symmetric Master Key' entry, with 'Load' selected. Two dialog boxes are overlaid: 'Select Source' with 'Smart card in reader 1' selected, and 'Select key part from TKE smart card' showing a table of key parts.

Card contents	Key type	Description	Origin	MDC4
TCSF symmetric master key part	SYN KEY PART 1	Crypto adapter	D12A53059388D0925ED651B9EAB7BC00	41CEB1

## Steps performed by the TKE Card User :

1. Select the Domains tab
2. Right click on a master key type
3. Select load, then select which part is going to be loaded
4. Select Smart Card Reader as the source
5. Insert Smart Card into Smart Card Reader
6. Enter 4-digit pin
7. Select key part

# Set Asymmetric Master Key

Crypto Coprocessor Crypto Module Administration : z9 / E37

Function

General Details Roles Authorities Domains Co-Sign

Domain Keys

	Status	Hash pattern	Index
New Symmetric Master Key	Full	EA2162E2400A5915296A2A0AEA5B9F22	0
Old Symmetric Master Key	Empty	00000000000000000000000000000000	1
Symmetric Master Key	Invalid	00000000000000000000000000000000	2
New Asymmetric Master Key	Full	9F38CD7CFE2F9AE3D3AE82BB429B335C	3
Old Asymmetric Master Key	Empty	00000000000000000000000000000000	4
Asymmetric Master Key	Invalid	00000000000000000000000000000000	5

Select key to work with

Key Type

- New Symmetric Master Key
- New Asymmetric Master Key
- Operational key:
- Operational Key - E
- Operational Key - IM
- Operational Key - IP
- Operational Key - O
- Operational Key - PL
- Operational Key - PINVER
- Operational Key - IMP-PKA
- Operational Key - DATA
- Operational Key - DATAC

Generate...  
Load  
Clear  
Set  
Secure key part entry

Help

General Keys Controls

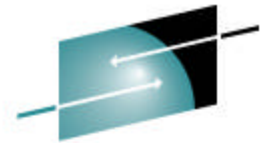
UPDATE MODE

The New Symmetric Master Key and the Asymmetric Master Key register are full. We need to set the Asymmetric Master Key Register

Steps performed by the TKE Card User :

1. Right click on New Asymmetric Master Key
2. Select Set





# Keys Completely Loaded

The screenshot shows the 'Crypto Coprocessor Crypto Module Administration : z9 / E37' window. The 'Function' tab is active, and the 'Domains' sub-tab is selected. The 'Domain Keys' table is displayed with the following data:

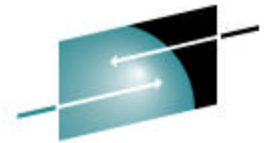
	Status	Hash pattern
New Symmetric Master Key	Full	EA2162E2400A5915296A2A0AEA5B9F22
Old Symmetric Master Key	Empty	00000000000000000000000000000000
Symmetric Master Key	Invalid	00000000000000000000000000000000
New Asymmetric Master Key	Empty	00000000000000000000000000000000
Old Asymmetric Master Key	Empty	00000000000000000000000000000000
Asymmetric Master Key	Valid	9F38CD7CFE2F9AE3D3AE82BB429B335C

Below the table, the 'Select key to work with' section shows a list of key types, with 'New Asymmetric Master Key' selected:

- 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

The key value has been moved from the New Asymmetric Master Key register to the Asymmetric Master Key register.

It is now time to go to the ICSF panels and complete the process



**S H A R E**  
Technology • Connections • Results

## Steps to Complete the Key Load Process

---

- Initialize the CKDS
- Initialize the PKDS
- Enable PKA Callable Services
- Verify Coprocessor Hardware Status

# Initialize the CKDS



Select option 2 MASTER KEY from ICSF Main Panel

```
CSFMKM00 ----- ICSF - Master Key Management -----  
OPTION ==> 1  
  
Enter the number of the desired option.  
  
 1 INIT/REFRESH CKDS - Initialize a Cryptographic Key Data Set or  
                        activate an updated Cryptographic Key Data Set  
 2 SET MK             - Set a DES/symmetric-keys master key  
 3 REENCIPHER CKDS   - Reencipher the CKDS prior to changing the DES  
                        /symmetric-keys master key  
 4 CHANGE MK         - Change the DES/symmetric-keys master key and  
                        activate the reenciphered CKDS  
  
 5 INITIALIZE PKDS   - Initialize or update a PKDS Cryptographic  
                        Key Data Set header record  
 6 REENCIPHER PKDS   - Reencipher the PKA Cryptographic Key Data Set  
 7 ACTIVATE PKDS     - Activate the PKDS after it has been reenciphered  
 8 REFRESH CACHE     - Refresh the PKDS Cache if enabled
```

```
CSFCKD10 ----- ICSF - Initialize a CKDS ----- Initialization Complete  
COMMAND ==> 1  
  
Enter the name of the desired option.  
  
 1 Initialize an empty CKDS (creates the header and system keys)  
 2 REFRESH - Activate an updated CKDS  
  
Enter the name of the CKDS below.  
  
CKDS ==> 'CSF.NEWCKDS'
```

This is CKDS is brand new empty CKDS.

# Initialize the PKDS

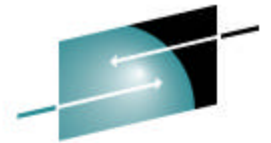


Select option 2 MASTER KEY from ICSF Main Panel

```
CSFMKM00 ----- ICSF - Master Key Management -----  
OPTION ==> 5  
  
Enter the number of the desired option.  
  
1 INIT/REFRESH CKDS - Initialize a Cryptographic Key Data Set or  
activate an updated Cryptographic Key Data Set  
2 SET MK - Set a DES/symmetric-keys master key  
3 REENCIPHER CKDS - Reencipher the CKDS prior to changing the DES  
/symmetric-keys master key  
4 CHANGE MK - Change the DES/symmetric-keys master key and  
activate the reenciphered CKDS  
  
5 INITIALIZE PKDS - Initialize or update a PKDS Cryptographic  
Key Data Set header record  
6 REENCIPHER PKDS - Reencipher the PKA Cryptographic Key Data Set  
7 ACTIVATE PKDS - Activate the PKDS after it has been reenciphered  
8 REFRESH CACHE - Refresh the PKDS Cache if enabled
```

```
CSFCMK30 ---- ICSF - Initialize PKA Cypographic Key Data Set ----  
COMMAND ==>  
  
Enter the name of the PKDS below.  
  
PKDS ==> 'CSF.NEWPKDS'
```

This is CKDS is brand new empty CKDS.



# Enable PKA Callable Services

Select option 4 ADMINCNTL from the ICSF Main Panel.

```

CSFACF00 ----- ICSF - Administrative Control Functions -- Row 1 to 4 of 4
COMMAND ==> SCROLL ==> PAGE

Active CKDS: CSF.CSFCKDS
Active PKDS: CSF.CSFPKDS
Active TKDS:

To change the status of a control, enter the appropriate character
(E - ENABLE, D - DISABLE) and press ENTER.

FUNCTION STATUS
-----
. Dynamic CKDS Access          ENABLED
e PKA Callable Services        DISABLED
e PKDS Read Access             DISABLED
e PKDS Write, Create, and Delete Access  DISABLED
***** Bottom of data *****

```

- Enable PKA Callable Services
- Enable PKDS Read Access
- Enable PKDS Write, Create, and Delete Access

```

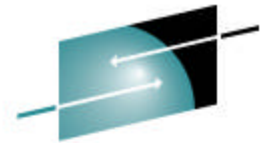
CSFACF00 ----- ICSF - Administrative Control Fun          FUNCTION CHANGED
COMMAND ==> SCROLL ==> PAGE

Active CKDS: CSF.CSFCKDS
Active PKDS: CSF.CSFPKDS
Active TKDS:

To change the status of a control, enter the appropriate character
(E - ENABLE, D - DISABLE) and press ENTER.

FUNCTION STATUS
-----
. Dynamic CKDS Access          ENABLED
. PKA Callable Services        ENABLED
. PKDS Read Access             ENABLED
. PKDS Write, Create, and Delete Access  ENABLED
***** Bottom of data *****

```



# Disable PKA Callable Services

```
CSFACF00 ----- ICSF - Administrative Control Functions -- Row 1 to 4 of 4
COMMAND ==>                                     SCROLL ==> PAGE
```

```
Active CKDS: CSF.CSFCKDS
Active PKDS: CSF.CSFPKDS
Active TKDS:
```

To change the status of a control, enter the appropriate character (E - ENABLE, D - DISABLE) and press ENTER.

FUNCTION	STATUS
. Dynamic CKDS Access	ENABLED
d PKA Callable Services	ENABLED
. PKDS Read Access	ENABLED
. PKDS Write, Create, and Delete Access	ENABLED

\*\*\*\*\* Bottom of data \*\*\*\*\*

PKA callable services must be disabled before entering the ASYM-MK.

Select option 4 ADMINCNTL from the ICSF Main Panel.

```
CSFACF00 ----- ICSF - Administrative Control Fun   PKA SERVICES DISABLED
COMMAND ==>                                     SCROLL ==> PAGE
```

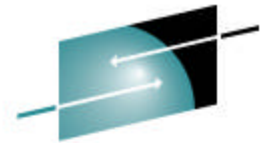
```
Active CKDS: CSF.CSFCKDS
Active PKDS: CSF.CSFPKDS
```

To change the status of a control, enter the appropriate character (E - ENABLE, D - DISABLE) and press ENTER.

FUNCTION	STATUS
. Dynamic CKDS Access	ENABLED
. PKA Callable Services	DISABLED
. PKDS Read Access	DISABLED
. PKDS Write, Create, and Delete Access	DISABLED

\*\*\*\*\* Bottom of data \*\*\*\*\*

Note: Disabling PKA Callable Services also disables PKDS Read Access and PKDS Write, Create, and Delete Access.



# Coprocessor Hardware Status

The status of the secure coprocessors is now ACTIVE and the current master key registers are VALID.

Select option 1 COPROCESSOR MGMT from the ICSF Main Panel.



```
CSFGCMP0 ----- ICSF Coprocessor Management ----- Row 1 to 5 of 5
COMMAND ==>                                     SCROLL ==> PAGE
```

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

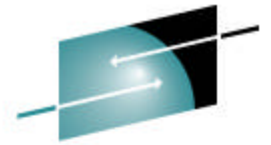
COPROCESSOR	SERIAL NUMBER	STATUS
A00		ACTIVE
S E02	94006004	ACTIVE
S E03	94006026	ACTIVE
S X01	93006015	ACTIVE

\*\*\*\*\* Bottom of data \*\*\*\*\*

```
CSFCMP40 ----- ICSF - Coprocessor Hardware Status -----
COMMAND ==>                                     SCROLL ==> HALF
                                                CRYPTO DOMAIN: 1
                                                More: >
REGISTER STATUS                                COPROCESSOR X01    COPROCESSOR E02

Crypto Serial Number      : 93006015                94006004
Status                    : ACTIVE                  ACTIVE
Symmetric-Keys Master Key
  New Master Key register : EMPTY                EMPTY
  Verification pattern     :                       :
  Hash pattern             :                       :
                          :                       :
Old Master Key register   : EMPTY                EMPTY
  Verification pattern     :                       :
  Hash pattern             :                       :
                          :                       :
Current Master Key register : VALID                VALID
  Verification pattern     : A996F8A939403A03        A996F8A939403A03
  Hash pattern             : AC40DD5EDFE94AB6        AC40DD5EDFE94AB6
                          : BA52CECE6B2941C9        BA52CECE6B2941C9

Asymmetric-Keys Master Key
  New Master Key register : EMPTY                EMPTY
  Hash pattern             :                       :
                          :                       :
Old Master Key register   : EMPTY                EMPTY
  Hash pattern             :                       :
                          :                       :
Current Master Key register : VALID                VALID
  Hash pattern             : F500D695FAE0ADA7        F500D695FAE0ADA7
                          : A60DB2BDA6F51537        A60DB2BDA6F51537
```



**S H A R E**  
Technology • Connections • Results

## Final Steps

- Record the verification and hash patterns of the keys loaded
  - Verification pattern : A996F8A939403A03
  - Hash pattern : AC40DD5EDFE94AB6  
: BA52CECE6B2941C9
- Take note of who loaded the different key parts, and which Smart Cards they were loaded from
- Make backups of all Smart Cards and store the Smart Cards in a secure location
- Verify that your Disaster Recovery Site has a TKE and Smart Cards will be there when they need to be



# Publications



- TKE Manuals –  
www-03.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/
  - Trusted Key Entry PCIX Workstation User's Guide, SA23-2211-02
- Redbooks – [www.redbooks.ibm.com](http://www.redbooks.ibm.com)
  - zSeries Trusted Key Entry (TKE) V4.2 Update, SG24-6499-00
  - z9-109 Crypto and TKE V5 Update, SG24-7123-00