IBM CHIM (Crypto Hardware Initialization and Maintenance)

Workstation User's Guide
References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights or other legally protectable rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by IBM, are the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Commercial Relations, IBM Corporation, Purchase, NY 10577.
# Table of Contents

About this Publication ........................................................................................................... 1

1. Introduction .......................................................................................................................... 2
   Overview ................................................................................................................................. 2
   Concepts and mechanisms ...................................................................................................... 3
      Components ......................................................................................................................... 3
      Security ............................................................................................................................... 4

2. User interface ....................................................................................................................... 7
   CHIM main window ............................................................................................................... 7
      File menu ............................................................................................................................ 7
      Overview page ..................................................................................................................... 7
      Device Groups page .......................................................................................................... 9
      Devices page ..................................................................................................................... 10
      Change a Passphrase ....................................................................................................... 11
   Device Group window ........................................................................................................ 11
      Devices page ..................................................................................................................... 11
      Import Key Parts ............................................................................................................... 13
      General page .................................................................................................................... 15
      Status page ....................................................................................................................... 16
      Profiles page .................................................................................................................... 16
      Roles page ......................................................................................................................... 18
      PINs page ......................................................................................................................... 19
      Master Keys page ............................................................................................................. 19
      Smart Cards page ............................................................................................................ 21
      Key Stores ......................................................................................................................... 22

3. Pending Operations window ............................................................................................... 22
   Copy Smart Card window ................................................................................................... 23

4. Operation ............................................................................................................................ 24
   Managing Devices and Device Groups ............................................................................. 24
      Managing Individual Devices ......................................................................................... 24
      Managing Device Groups ............................................................................................... 25
   Logging on to a Device Group .......................................................................................... 25
   Configuring basic coprocessor functionality. ................................................................... 26
      Set coprocessor clock ....................................................................................................... 28
   Managing smart card zones ............................................................................................... 30
      Create CA smart card ...................................................................................................... 30
      Backup CA smart card ................................................................................................. 33
      Enroll device group ........................................................................................................ 40
   Managing access control .................................................................................................. 42
      Create or edit role .......................................................................................................... 43
      Delete roles ...................................................................................................................... 45
      Delete profiles ............................................................................................................... 53
   Managing master keys ....................................................................................................... 54
      Generate key parts ......................................................................................................... 55
      Load master key parts ................................................................................................. 57
      Set master keys ............................................................................................................. 59
      Reencipher key stores ................................................................................................. 60

4. CHIM audit log ..................................................................................................................... 63
About this Publication

This document describes the configuration and use of the IBM CHIM — Crypto Hardware Initialization and Maintenance.
1. Introduction

Overview

With IBM Cryptographic Hardware Initialization and Management (CHIM) you can from a central trusted location securely manage remote IBM PCIe Cryptographic Coprocessors located in x Systems and Power Systems in a hostile environment. Management tasks are done using a specialized workstation, the CHIM workstation. The figure below shows the context in which CHIM operates:

The CHIM workstation connects via secure sessions directly to the cryptographic coprocessors to let authorized personnel perform the following tasks:

- View coprocessor status
- View and manage coprocessor configuration
- Manage coprocessor access control (user roles and profiles)
- Generate and load coprocessor master keys
- Create and load operational key parts

Access to manage coprocessors is governed by the standard access control system built into the coprocessors. The access control system lets you enforce dual control and separation of duties. This is useful when loading master keys or configuring the coprocessors.

CHIM uses smart cards for user authentication and storage of coprocessor master key parts. Authorized personnel logs on to the coprocessors using personal smart cards protected with 6 digit PIN's. Likewise, master key parts are kept on smart cards protected with 6 digit PIN's, ensuring that the master key parts never appear in clear outside the tamper resistant environment provided by the smart cards and coprocessors.
Communication between the CHIM workstation and a coprocessor is over an encrypted secure session. The session is terminated inside the tamper resistant shell of the coprocessor. During session establishment, the CHIM workstation verifies the authenticity of the coprocessor and the two exchange a session key. When the secure session is in place, authorized personnel authenticate to the coprocessor by logging on using smart cards.

Concepts and mechanisms

The figure below shows the important elements in the CHIM solution:

Components

**CHIM workstation**

The CHIM workstation is the trusted workstation used by authorized personnel (CHIM users) to connect to and manage the IBM cryptographic coprocessors located in a remote, possibly hostile, environment. The security of the CHIM solution depends on the integrity of the CHIM workstation, and therefore it must be placed in a trusted secure environment.

**CHIM application**

The CHIM application is the application providing the CHIM functionality and user interface. It also provides the security mechanisms used by the workstation to securely connect to and manage the remote coprocessors.

**Smart card**

Smart cards are used for three purposes:

1. Two factor authentication of authorized CHIM users. Each authorized CHIM user has a personal PIN protected smart card containing a logon key - to be able to log on the user must possess a smart card with a valid logon key AND know the corresponding PIN.

2. Secure storage of coprocessor master keys parts. The key parts are kept on PIN
protected smart cards and can only be read from and written to the smart cards in encrypted form.

3. A facility for local HSM (hardware secure module) functions in instances where the workstation does not have a local crypto card.

If you would like to utilize smart cards or need more, you can purchase them from the IBM retail parts store by following the link below and searching for the IBM part numbers.


Part numbers: 74Y0551 and 00JA710

**Server**

Servers are system x (Linux) and/or system p (AIX) servers hosting IBM cryptographic coprocessors managed with CHIM. The servers may be located in a hostile environment.

**IBM Cryptographic Coprocessor**

The IBM cryptographic coprocessors are managed with CHIM. The coprocessors provide a tamper resistant environment, and accepts secure connections from the CHIM workstation when loaded with CHIM-enabled CCA firmware.

**Key stores**

Key stores holding CCA keys used by customer applications on the server. The key stores are encrypted with the cryptographic coprocessor master keys, and therefore need to be reenciphered when master keys are changed.

**CHIM agent**

The CHIM agent is a started task listening for network connections from the CHIM workstation. It provides a channel for the CHIM workstation to establish secure sessions to the IBM cryptographic coprocessors in the server. It also provides a channel for the CHIM workstation to query public coprocessor information and read and update key stores on the server.

**Security**

**Secure session between CHIM application and IBM cryptographic coprocessor**

When the CHIM workstation connects to a coprocessor, a secure session established. The secure session provides secrecy and integrity of the communication between the CHIM workstation and the coprocessor. It also authenticates the coprocessor to the CHIM workstation.

The session begins with a handshake, in which the coprocessor sends a certificate chain certifying its public key. The CHIM workstation verifies the certificate chain using the IBM factory root certificate which is encoded into the CHIM application. The certificate chain proves that the coprocessor is a genuine IBM cryptographic coprocessor loaded with authorized CCA and CHIM firmware. The session establishment is done using the Diffie-hellman key exchange. The CHIM workstation generates a public and private key pair and sends the public key to the coprocessor. The coprocessor does the same and sends the CHIM workstation it's public key.
Then they both combine their private keys with the public keys they received, and following NIST SP 800-56A standard: algorithm 7 come up with a key agreement. Both sides should have come up with the same key. From this point all communication is encrypted using the session key. Transaction sequence numbers and hash values within the encrypted messages provides integrity and replay protection.

Note, that even though the secure session is encrypted, an additional layer of protection is used when transmitting master key parts (see Secure session between smart card and IBM cryptographic coprocessor (p. 5)).

**IBM cryptographic coprocessor logon**

The secure session in itself provides one way authentication only. It authenticates the coprocessor, but it does not authenticate the CHIM user connecting to the coprocessor. CHIM user authentication is taken care of using the standard IBM access control system built into the coprocessor. The access control system requires users to authenticate by logging on using either smart cards or pass phrases.

The access control system is based on roles and profiles: A role defines a set of permissions. Each authorized user must be associated with a user profile in the coprocessor. The user profile defines the user id, logon method and role activated when the user logs on. A special kind of profiles, group profiles, allows you to enforce dual control by requiring two or more users to log on before activating the role associated with the group profile.

When no one is logged on, a role called the DEFAULT role defines the permissions in effect. It is mainly used to configure the roles and profiles initially. In a properly configured system, the DEFAULT role has a very restricted permission set.

Roles and profiles can be customized as you like, but the CHIM solution comes with a set of standard role definitions you should use, as they have been carefully designed for optimal security.

**Secure session between smart card and IBM cryptographic coprocessor**

Coprocessor master key parts are generated in the coprocessors and stored on smart cards. Later the master key parts are loaded from the smart cards into the coprocessors master key registers. To protect the master key parts while in transit between a coprocessor and a smart card, a secure session is established directly between the coprocessor and the smart card. The secure session provides authentication, secrecy and integrity, and ensures that master key parts are always encrypted when outside the tamper resistant coprocessor and smart card hardware. This type of secure session can only be established if the coprocessor and the smart card are enrolled in the same smart card zone (see Smart card zone (p. 5)).

Note, that this type of secure session is embedded inside the secure session established between the CHIM workstation and the coprocessor (see Secure session between CHIM application and IBM cryptographic coprocessor (p. 4)), giving an additional layer of security.

**Smart card zone**

- Smart cards provide the ability to store and transfer coprocessor master key parts and logon keys securely. The security is based on the concept of a smart card zone.
- IBM cryptographic coprocessors: Can generate coprocessor master key parts and have their master key registers loaded with these parts. IBM cryptographic coprocessors can establish secure sessions with TKE smart cards in the same zone in order to read and write coprocessor master key parts on the smart cards.
Members of a smart card zone can exchange information with other members in the same zone.

A smart card zone consists of the following members:

- CA smart card: Is the certificate authority card that defines the zone. The CA smart card can enroll members into the zone. Enrolling is a very sensitive operation, and each CA card is therefore protected with two six digit PIN's.

- TKE smart cards: Can hold coprocessor master key parts and logon keys. TKE smart cards can establish secure sessions with other TKE smart cards and IBM cryptographic coprocessors in the same zone in order to exchange coprocessor master key parts and logon keys. Each TKE card is protected with a six digit PIN.

- IBM cryptographic coprocessors: Can generate coprocessor master key parts and have their master key registers loaded with these parts. IBM cryptographic coprocessors can establish secure sessions with TKE smart cards in the same zone in order to read and write coprocessors master key parts on the smart cards.

In fact, the zone implements a small public key infrastructure (PKI), where each member has a certified key pair. The CA smart card acts as a Certificate Authority (CA) that issues a zone certificate to each of the zone members. The zone certificate proves the zone membership and contains the public key belonging to the member. The process of issuing a zone certificate is also known as enrolling a member into the zone.

When two members establish a secure session, they first authenticate by exchanging and verifying each others zone certificates. Then one of the members generates a session key and sends it to the other member encrypted under that members public key. The other member deciphers the session key using its private key, and from this point, all communication is encrypted with the session key. Transaction sequence numbers and hash values within the encrypted messages provides integrity and replay protection.

SCUP is used to create CA smart cards and to create and enroll TKE smart cards. The CHIM application is used to enroll the IBM cryptographic coprocessors managed with CHIM.
2. User interface

This chapter explains the main windows in the CHIM application.

CHIM main window

File menu

Settings

The settings menu allows you to change a few things related to the CHIM workstation itself.

You can switch between Production and Development mode, reflecting whether the devices is loaded with production or development firmware. You can have both types defined in CHIM at the same time, but only one type can be worked with at a time.

Analysis at startup can be enabled or disabled. Analysis is when CHIM requests each device for all relevant information and analyzes whether they can be accessed and if there are any differences between them. This takes some time and can be postponed by Disabling analysis at CHIM startup.

Access points. The access points known to CHIM can be seen here and new ones can be added and removed.

Smart Card Copy Wizard

The copy smart card wizard allows you to copy smart card parts from one smart card to another.

Manage Local Adapter

The manage local adapter allows you to manage an adapter locally if the CHIM application and IBM cryptographic coprocessor are on the same CHIM workstation.

Audit Log

The audit log menu item allows you to view the CHIM audit log. See section 5 for more details.

Overview page

The Overview page shows all the device groups you have defined in CHIM. For each device group CHIM will query all the devices and show the name, number of devices and a health status indicating whether CHIM has detected any problems that needs to be taken care of. Things that will be checked includes:

- If a device has been modified (for example if firmware has been reloaded).
- If a device has been removed (was not found in the server where it was supposed to be installed).
- If a device is not trusted (has an invalid certificate, or has a development certificate when CHIM is running production mode or vice versa).
- If a device has registered an intrusion attempt.
• If a device battery is running low.

• If there are configuration mismatches between devices in the group, such as mismatch on CCA level, roles, profiles and master keys.

The following operations are available:

• More... - opens a pane where you can see detailed status information for the group.

• Log In – lets you logon to the device group. You need to logon in order to manage a device group (see Logging on to a Device Group (p. 25))

More...

The window contains details of the device status and any errors or differences. This analysis is done at startup (unless it has been disabled) and can be requested by the 'Refresh' menu in this window.

The 'Details' menu will expand the information shown to include some key elements of the devices.

The 'Fetch' menu item is used to fetch the certificates used to setup the secure session with the devices. If there are no suitable certificates, they will have to be created, but since this may indicate an abnormal situation, you will be prompted for whether a new certificate should be created. This is to make it possible to investigate the situation if it is not expected. This can be due to planned segment 3 updates, but could also indicate otherwise.

The 'Edit' menu will allow you to edit the group.
Device Groups page

The Device Groups page lets you view, create, delete and update device groups definitions. A device group consists of a number of IBM devices located on one or more hosts.

Add - create a new device group definition. CHIM will prompt for a name of the device group and then let you add devices to the group. Note that you can only add devices that have already been defined using the Devices page (see below).

Edit – edit an existing device group definition. You can change the device group name and add and remove devices to the group. Note that you can only add devices that have already been defined using the Devices page (see below).

Remove – delete an existing device group.

Logon – lets you logon on to and manage the selected device group. Once logged on, CHIM will open a device group notebook with which you can manage the device group (see Device Group window (p. 11))

For more information on defining devices and device groups, see Managing Devices and Device Groups (p. 24).
Devices page

The Devices page lets you view, create, delete and update device definitions. It also lets you open a subset of devices to work on them separately from the other devices in that group. This feature must be used when adding or replacing devices to properly initialize them to be identical to the other devices; this is needed for loading FCV and setting master keys. It is done by selecting the device(s) and right-clicking on the mouse and selecting the menu that pops up.

The following operations are available:

- **Add** – add a new device definition manually. CHIM will prompt for the information necessary to locate and communicate with the device and then add the device definition to the list.

- **Edit (by double click)** – change a device definition.

- **Remove** – remove a device definition.

- **Discover Devices** – discover the devices present on a specific host. CHIM will prompt for the IP address of the host and then display a list of the devices present on the server. You can then select the devices you want to add to the list.

- **Create Device Group** - create a new device group definition. CHIM will prompt for a name of the device group and then let you add devices to the group. Note that you can only add devices that have already been defined.

For more information on defining devices and device groups, see Managing Devices and Device Groups (p. 24).
Change a Passphrase

When logging onto a device, a list of profiles will be presented to choose from. If the profile chosen is a passphrase type profile, you will have the option to logon and change your passphrase by selecting the checkbox before logging as shown:

![Passphrase Change Window]

You will be presented a window to enter in your current passphrase, and the passphrase you want to change it to with another field to confirm.

![Device Group Notebook]

If all the fields are valid, that profiles passphrase will be changed and next time you login, you will have to start using the new passphrase.

Device Group window

When you have successfully logged in to a device group, CHIM will open a notebook to let you work with the device group. The notebook has a number of pages, that are described below.

Devices page

The Devices page shows a list of the devices in the device group. You can see which device is the Main Device (primary), whether devices are online or not, and you can see the smart card zone the devices are enrolled into.
The following operations are available:

- **Enroll** – enroll devices into a smart card zone. You need to enroll the devices of the group into a smart card zone in order to work with master keys. The smart card zone provides the security necessary to protect the master keys during generation, storage and loading (see Smart card zone (p. 5)).

- **Load FCV** – loads a function control vector into the devices in the device group. The function control vector is a file used to enable cryptographic capabilities in the IBM coprocessor.

- **Import Key Parts** – help in loading and creating a DES or an AES operational key. See below for more.

- **Initialize** – zeroize the crypto module to factory settings
**Import Key Parts**

The Import Key Parts button found on the Device Page will present a panel that allows for creation and loading of DES and AES Operational Key parts.

**Steps:**

- Press “New Key”
- Select between Keyboard or Card Reader in the drop down menu for input source
- Select the Key Standard, Key Label, and number of key parts to create. You may use the TEST button next to the Key Label field to see if the key labeled entered fits the format...
• Choose what kind of a Key Type the key needs to be, and choose the correct attributes. If you know the Key Check Value, you may enter it in the field also to ensure you have entered the intended key correctly.

• Enter in the key part and it will load it to key storage.
General page

The General page shows general information about the device group.

Please note that the information presented on the General page is from the Primary Device only.

The following operations are available:

- Manage Wrapping Key Options – Change the type of wrapping key option for internal and external to ECB or ECH, as defined in the CCA User's Guide.
Status page

The Status page shows status information for the device group.

Please note that the information presented on the Status page is from the Primary Device only.

The following operations are available:

- Set Clock – synchronize the system clock of the devices in the group with the system clock in the servers hosting the devices. The request to synchronize the clock is not executed right away but instead added to the Pending Change list (see Pending Operations window (p. 22))

- Commit – commit all changes contained in the Pending Change list.

- Refresh – refresh the information shown on the page

- Set Environment ID – Set the environment ID of the crypto card

- Reset Intrusion Latch – Reset the intrusion latch of the crypto card

- Reset Battery Low Indicator – Reset the battery low indicator of the crypto card

Profiles page

The Profiles page lets you view, create, edit and delete user profiles in the device group.

Please note that the information presented on the Profiles page is from the Main Device only, but operations you carry out are applied to all devices in the group.
The following operations are available:

- **Create** – create a new user profile. You can create smart card profiles, pass phrase profiles and group profiles. New profiles are not installed right away but instead added to the pending change list (see Pending Operations window (p. 22)).

- **Edit** – edit an existing user profile. Changed profiles are not installed right away but instead added to the pending change list (see Pending Operations window (p. 22)).

- **Delete** – delete existing user profiles. Profile deletion requests are not executed right away but instead added to the pending change list (see Pending Operations window (p. 22)).

- **Export** – export one or more user profiles. The profiles are exported into a file, that can later be imported using the Import function.

- **Import** – import user profiles previously exported using the Export function. The imported profiles are not installed right away but instead added to the pending change list (see Pending Operations window (p. 22)).

- **Run Diagnostics** – compares all devices in the group with the Main Device and reports any mismatches with respect to profiles, roles, and master keys.

- **Fix** – correct profile mismatches identified by the Run Diagnostics function. Does so by aligning the devices in the group to the Main Device. The resulting corrections are not executed right away but instead added to the pending change list.

- **Commit** – commit all changes contained in the Pending Change list.

- **Refresh** – refresh the information shown on the page
Roles page

The Roles page lets you view, create, edit and delete user roles in the device group.

Please note that the information presented on the Roles page is from the Main Device only, but operations you carry out are applied to all devices in the group.

The following operations are available:

- **Create** – create a new user role. New roles are not installed right away but instead added to the pending change list (see Pending Operations window (p. 22)).

- **Edit** – edit an existing user role. Changed roles are not installed right away but instead added to the pending change list (see Pending Operations window (p. 22)).

- **Delete** – delete existing user roles. Role deletion requests are not executed right away but instead added to the pending change list (see Pending Operations window (p. 22)).

- **Export** – export one or more user roles. The roles are exported into a file, that can later be imported using the Import function.

- **Import** – import user roles previously exported using the Export function. The imported roles are not installed right away but instead added to the pending change list (see Pending Operations window (p. 22)).

- **Run Diagnostics** – compares all devices in the group with the Main Device and reports any mismatches with respect to profiles, roles, and master keys.

- **Fix** – correct role mismatches identified by the Run Diagnostics function. Does so by aligning the devices in the group to the Main Device. The resulting corrections are not executed right away but instead added to the pending change list. Commit – commit all changes contained in the Pending Change list.

- **Refresh** – refresh the information shown on the page
PINs page

The PINs page shows the ID, state, and value of the PINs loaded in the decimalization table and the weak PINs table. On this page you can create new PINs, activate, and delete PINs, as well as export them to a file or import them.

You can switch between the two tables using the radio buttons at the top of the panel.

The following operations are available:

• Activate – If a PIN entry was loaded with a profile that did not have the authority to activate the corresponding table entry, another profile with that authority can move it into the “Active” state. Otherwise, the entry will be left in the “Loaded” state.

• Import – Imports from a file PIN entries that were done using the export function and attempts to load them into the table.

• Export – Exports all the PINs in the selected table into a file for importing.

• New – Opens a window to help with creating a new PIN entry.

Tip: Hover over each input field to help explain the formatting. The panels have been designed to prevent a user from entering in values that are not accepted.

• Delete – Deletes the currently selected entries from the table, given the proper authority.

Master Keys page

The Master Keys page shows status and verification patterns for master key registers in the device group. On this page you can clear the NEW and OLD master key registers, activate (SET) master keys and initialize or reencipher the corresponding key stores.

For DES and RSA master key registers, you can choose between MDC-4 and SHA-1 key verification methods.
Please note that the information presented on the Master Keys page is from the Main Device only, but operations you carry out are applied to all devices in the group.

<table>
<thead>
<tr>
<th>Register</th>
<th>Status</th>
<th>Verification Method</th>
<th>Verification Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES OLD</td>
<td>CLEAR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKA NEW</td>
<td>CLEAR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKA CURRENT</td>
<td>COMPLETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKA OLD</td>
<td>CLEAR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES NEW</td>
<td>CLEAR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES CURRENT</td>
<td>COMPLETE</td>
<td>SHA-256</td>
<td>0F:0A:6F:78:9B:B1:B6</td>
</tr>
<tr>
<td>AES OLD</td>
<td>CLEAR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APKA NEW</td>
<td>CLEAR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APKA OLD</td>
<td>CLEAR</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following operations are available:

- **Clear Register** – clears the selected NEW and OLD master key registers (see also Clear new and old master key registers (p. 61))
- **Set Master Key** – Activates the selected NEW master key (see also Set master keys (p. 59))
- **Reencipher Key Store** – Reenciphers the key store corresponding to the selected CURRENT master key from encryption under the OLD master key to encryption under the CURRENT master key (see also Reencipher key stores (p. 60))
- **Run Diagnostics** – Compares all master key registers across the devices in the group and reports any mismatches between devices.
- **Refresh** – refresh the information shown on the page

For more information on master key management, see Managing master keys (p. 54).
Smart Cards page

The Smart Cards page lets you view and work with the contents of the smart card currently inserted into smart card reader 1: You can generate, load and delete master key parts, generate logon keys. You can also copy content from one smart card to another.

The following operations are available:

- **Load Key Parts** – loads the selected master key parts from the smart card into the corresponding NEW master key registers in all devices in the device group (see also Load master key parts (p. 57))

- **Generate** – generates master key parts for selected master key registers and stores them on the smart card (see also Generate key parts (p. 55)).

- **Delete** – deletes the selected master key parts from the smart card.

- **Generate Logon Key** – generates a logon key on the smart card. Together with a smart card profile, the logon key can be used to authenticate the smart card user when logging on to the device group.

- **Copy smart card** – opens a dialog that will let you copy contents from one smart card to another (see Copy Smart Card window (p. 23))

- **Refresh** – refresh the information shown on the page

For more information on smart cards and master key management, see Managing master keys (p. 54).
Key Stores

The CCA key store files on the device servers can be initialized from this pane. This is normally only done on fresh server installations. The key store files can be initialized when the proper master keys has been set. As a safety precaution only key store files in the following states will be initialized:

- Non existing key files
- Malformed key files
- Empty key files

3. Pending Operations window

The Pending Operations window shows operations awaiting execution. The window is normally hidden, but opens when pending operations are created.

Some changes are not carried out right away, but added to the Pending Operations list, giving you the opportunity to review the changes and possibly cancel (undo) them before they are executed. This is especially useful when working with the CHIM diagnostics function, which will add suggested corrective changes to the Pending Operations list, giving you the opportunity to see the changes before committing them.

Pending operations will be executed in the order they appear in the Pending Operations list.
The following operations are available:

- **Undo:** Remove the last operation from the Pending Operations list. You can remove operations one by one using this function.

- **Undo all:** Removes all pending operations from the Pending Operations list.

- **Commit:** Executes all pending operations in the Pending Operations list

### Copy Smart Card window

Pressing the Copy Smart Card button on the Smart Cards page in the Device Groups window opens the Copy Smart Card window. Copy Smart Card window lets you copy content from one smart card to another.

The following operations are available:

- **Copy:** Copy selected content from on smart card to the other. The arrow on the button determines the direction of the copy.

- **Delete:** Delete the selected content from the smart card.
4. Operation

Managing Devices and Device Groups

With CHIM you manage groups of IBM cryptographic coprocessors. Even if you only want to manage a single device, you still need to use a Device Group to manage the device. This section explains how to define devices and device groups.

Managing Individual Devices

In order to manage device groups, you need to define devices. To do so, use the 'Devices' tab in the main program window. Here you can add and remove devices, or create device groups from selected devices.

Discovering devices

To add devices, press the Discover Devices button. This will bring up a window to search for devices:

![Device Editor](image1)

Figure 4.1. Managing Individual Devices

Enter the IP address of the server holding the devices you want to add. The CHIM workstation will now query the server for the devices present, and show the devices
in a list. Press Process Devices to automatically define the devices to the CHIM workstation.

Managing Device Groups

Editing Device Groups

Each device group must contain a name. You can create device groups from either the 'Device Groups' tab, or the 'Devices' tab.

Device groups comprise one or more devices.

Main device — one device is queried for roles, profiles and master key registers' statuses. It is assumed that all other devices in a device group contain the same sets of roles and profiles, and that their master key registers are in the same states. The main device is set via the 'Set as Main' button, visible when editing a device group.

Logging on to a Device Group

When you have started the CHIM application with device groups defined, you can log on to a device group from the Overview page in the main window.

---

1 Device groups created using the 'Devices' tab are pre-populated with the selected devices.
Selecting the device group and clicking 'Log In' shows the logon screen. The application will log on using the supplied credentials to all adapters in the device group. The logon window will show only profiles common to all adapters in the device group.

There is one additional item in the list; '<<<DEFAULT ROLE>>>'. This will skip any logon attempts and work with the adapters using the DEFAULT role. This can be useful when setting up the adapters for the first time. After the initial setup, the DEFAULT role should be limited.

CHIM supports passphrase, smartcard and group logon profiles.

Once logged on, CHIM will maintain the session as long as the device group’s window is open. To log off, simply close the window.

Configuring basic coprocessor functionality.

The IBM cryptographic coprocessor is shipped with cryptographic functionality disabled. To enable the cryptographic functionality you need to load a so called
Function Control Vector (FCV). The coprocessor also contains an internal clock that needs to be set.

This section describes how to carry out these tasks.

**Load function control vector (FCV)**

**Overview**

IBM Cryptographic coprocessors are enabled using a function control vector (FCV). The FCV defines the cryptographic algorithms and key lengths provided by the coprocessor. The FCV is delivered by IBM in a signed file and must be loaded into the coprocessors as part of the initial coprocessor configuration.

**Prereqs**

- You must be logged on to the relevant device group with sufficient authority (e.g., a user having the DEFAULT role on an unconfigured coprocessor or a user having the CHIMADM role on a configured coprocessor).
- You have a signed FCV file from IBM

**Steps**

- Go to the ‘Devices’ page.

  ![Image of Device Management Interface]

- Press 'Load FCV'. This will bring up a dialog to select the file containing the FCV.
• Select the file holding the FCV (eg fcv_td4kECC521.crt) and press ‘Open’. This will add the operation to the pending operations list.

• Press ‘Commit’ to carry out the pending Load FCV operation

The selected FCV should now be loaded.

Set coprocessor clock

Overview

The IBM Cryptographic coprocessor maintains an internal clock which is used to control time limited access to the coprocessor. The clock should be set as part of the initial coprocessor configuration and whenever it is incorrect. When you request the clock to be set, it is simply synchronized with the clock in the server, so you won’t have to supply the clock value yourself.

Prereqs

• You must be logged on to the relevant device group with sufficient authority (eg a user having the DEFAULT role on an unconfigured coprocessor or a user having the CHIMADM role on a configured coprocessor)
### Steps

- Go to the 'Status' page.

- Press 'Set Clock'. This will add the operation to the pending operations list.

- Press 'Commit' to carry out the pending Set Clock operation.

The coprocessor clock should now be set (i.e. synchronized with the clock in the server hosting the coprocessor).
Managing smart card zones

To use smart cards with CHIM you must create one or more smart card zones. A smart card zone provides protection for IBM coprocessor master key parts and logon keys. A smart card zone consists of a CA smart card, a number of TKE smart cards and a number of IBM coprocessors. To set up a smart card zone, you will have to perform the following steps:

• Create a CA smart card (see Create CA smart card (p. 30)).

• Create one or more back ups of the CA smart card (see Backup CA smart card (p. 33)).

• Create and personalize TKE smart cards (see Create and personalize TKE smart card (p. 36)).

• Enroll IBM cryptographic coprocessors (see Enroll device group (p. 40)).

When the zone has been set up, you can use the TKE smart cards to store master key parts for the IBM coprocessors in the zone, and you can use the TKE smart cards for holding coprocessor logon keys. If you already have a smart card zone, you may want to create additional CA smart card back ups and/or TKE smart cards and you may want to enroll additional IBM coprocessors.

This chapter describes the operations you perform to manage master keys. For more information about smart card zones (see Smart card zone (p. 5)).

Create CA smart card

Overview

In essence, the CA smart card defines a smart card zone. When you create a new CA smart card, you create a new smart card zone. The CA smart card is used whenever you want to add members to the zone (TKE smart cards and IBM Cryptographic coprocessors).

The management of a smart card zone is a critical task. Therefore the CA smart card is protected by two 6 digit PIN's to let you enforce dual control on the use of the CA smart card.

Here we show how to create a new CA smart card, and thereby, a new smart card zone.

Prereqs

• You have an empty smart card to use as CA smart card.

• Two people, each to provide a 6 digit PIN to govern access to the CA card, are present.

Steps

• Start SCUP.
• Select CA Smart Card → Initialize and personalize CA smart card:

• Insert the smart card to be initialized.

After the smart card has been inserted you will be prompted for the zone key length:

The zone key length determines the length of the keys used when authenticating the members of the zone and when establishing secure sessions between the members. You want this to be as long as possible.

• Select '2048 bits' and press 'Ok'

You will be asked to confirm that you really want to initialize the card, and when you have confirmed, the CA card will be initialized.

When initialization has completed, you will be prompted to enter twice the first 6 digit PIN for the CA smart card:
• The first of the two people to use the CA smart card must now select a 6 digit PIN and enter it twice on the smart card reader PIN pad.

Next you will be prompted to enter twice the second 6 digit PIN for the CA smart card:

• The second of the two people to use the CA smart card must now select a 6 digit PIN and enter it twice on the smart card reader PIN pad.

You will now be prompted to name the smart card zone:

It is recommended to choose a unique name that identifies the cryptographic environment protected by the zone, e.g. ATM PROD. The name can be at most 12 characters long.

• Choose an appropriate name and press ‘OK’.

You will also be prompted for an optional description of the smart card zone:
It is recommended to choose a description that reflects the cryptographic environment protected by the zone, e.g. ATM Production Zone CA. The description can be at most 30 characters long.

- Choose an appropriate description and press 'OK'.

The CA smart card will now go through final configuration (building). After a while you should see the following message, indicating that the CA smart card was created successfully:

```
The CA smart card was created successfully.
```

When you have created a CA smart card, it is highly recommended to make one or more backups (see Backup CA smart card (p. 33)).

### Backup CA smart card

#### Overview

Here we show how to create a backup of a CA smart card.

#### Prereqs

- You have the CA smart card to be backed up.
- You have an empty smart card to use as CA smart card backup.
- The two people holding the two 6 digit PINs used to protect the CA smart card are present.

#### Steps

- Start the SCUP utility.
- Insert the CA smart card to be backed up in smart card reader 1.
- Select CA Smart Card → Backup CA smart card:
You will be prompted to enter the first 6 digit PIN for the CA smart card:

- The person holding the first 6 digit PIN for the CA smart card must enter that PIN on the smart card reader PIN pad.

Next you will be prompted to enter the second 6 digit PIN for the CA smart card:
• The person holding the second 6 digit PIN for the CA smart card must enter that PIN on the smart card reader PIN pad.

• When prompted, insert the backup smart card in smart card reader 2.

If the smart card already contains data you will be prompted whether to overwrite. Then the backup card will be initialized and configured with the two 6 digit PIN's from the original CA smart card.

After a while, you will be prompted to enter the first 6 digit PIN for the CA backup smart card:

• The person holding the first 6 digit PIN for the CA smart card must enter that PIN on the smart card reader PIN pad. Note this must be the same PIN as is used on the original CA smart card.

Then you will be prompted to enter the second 6 digit PIN for the CA backup smart card:

• The person holding the second 6 digit PIN for the CA smart card must enter that PIN on the smart card reader PIN pad. Note this must be the same PIN as is used on the original CA smart card.

The remaining data will now be copied from the original CA smart card to the backup CA smart card. After a while you should see the following message, indicating that the CA smart card was backed up successfully:
Create and personalize TKE smart card

Overview

TKE smart cards are used to keep logon keys and master key parts for IBM coprocessors.

When you initialize a TKE smart card, it is enrolled into a smart card zone as well. This means it can be used to store master key parts for IBM coprocessors enrolled into that zone, and it can exchange data with other smart cards enrolled in the same zone.

After initialization, the TKE smart card cannot be enrolled into another zone without being reinitialized. During reinitialization all data on the smart card is lost. This means that data cannot be moved between smart card zones.

Here we show how to create and initialize a TKE smart card.

Prereqs

- You have the CA smart card for the relevant smart card zone.
- You have an empty smart card to use as TKE smart card.
- The two people holding the two 6 digit PINs used to protect the CA smart card are present.
- The person to provide the 6 digit PIN to protect the TKE smart card is present.

Steps

- Start the SCUP utility.
- Select TKE Smart Card → Initialize and enroll TKE smart card:
• Insert the CA smart card in smart card reader 1.

You will be prompted to enter the first 6 digit PIN for the CA smart card:

• The person holding the first 6 digit PIN for the CA smart card must enter that PIN on the smart card reader PIN pad.

Next you will be prompted to enter the second 6 digit PIN for the CA smart card.
• The person holding the second 6 digit PIN for the CA smart card must enter that PIN on the smart card reader PIN pad.

• When prompted, insert the smart card to be initialized as a TKE smart card in card reader 2.

You will be asked to confirm that you really want to initialize the card, and when you have confirmed, the TKE smart card will be initialized. After a while you should receive a message indicating that the card was initialized successfully:

Now the TKE smart card must be personalized by setting the 6 digit PIN and adding a description:

• Select TKE Smart Card → Personalize TKE smart card
After you have confirmed that the card has been inserted, you will be prompted to enter twice a 6 digit PIN for the TKE smart card:

- The person to use the TKE smart card must now select and enter a 6 digit PIN twice on the smartcard reader PIN pad.

You will now be prompted for an optional description for the smart card:
It is recommended to choose a description that reflects the owner and the intended use of the smart card. The description can be at most 30 characters long.

- Choose an appropriate description and press 'OK'

After a while you should see the following message, indicating that the TKE smart card was personalized successfully:

The TKE smart card is now ready to hold coprocessor master key parts and/or a coprocessor log on key.

**Enroll device group**

**Overview**

IBM coprocessor master key parts can be stored on TKE smart cards, but only when the coprocessors and the smart cards are members of the same smart card zone. When you enroll a device group into a smart card zone, you make the coprocessors of the device group members of that zone.

Here we show how to enroll the IBM coprocessors of a device group into a smart card zone.

**Prereqs**

- You must be logged on to the device group with sufficient authority (eg a user having the CHIMADM role).
- You have the CA smart card for the relevant smart card zone.
- The two people holding the two 6 digit PINs used to protect the CA smart card are present.

**Steps**

- Go to the ‘Devices’ page.
- Press ‘Enroll’.
• When prompted, insert the CA smart card into smart card reader 1.

• You will be prompted to enter the first 6 digit PIN for the CA smart card:

• The person holding the first 6 digit PIN for the CA smart card must enter that PIN on the smart card reader PIN pad.

Next you will be prompted to enter the second 6 digit PIN for the CA smart card:

• The person holding the second 6 digit PIN for the CA smart card must enter that PIN on the smart card reader PIN pad.

The coprocessors in the device group will now be enrolled into the smart card zone.

After a while you should see a message in the bottom of the device group page, indicating that the IBM coprocessors in the device group have been enrolled in to the smart card zone successfully:

The coprocessors in the device group are now able to exchange master key parts with TKE smart cards enrolled in the same zone.
Managing access control

CHIM uses the IBM coprocessor access control system to control access to coprocessors managed by the CHIM workstation. The access control system is based on roles and profiles:

**Role:** A role defines a set of permissions that can be granted to a user or a group of users.

**Smart card profile:** A smart card profile defines a user who authenticates using a personal smart card. The profile contains the user ID, a public logon key (used to verify the signature generated by the smart card during log on) and a reference to the role assigned to the user.

**Pass phrase profile:** A pass phrase profile defines a user who authenticates using a pass phrase. The profile contains the user ID, a pass phrase and a reference to the role assigned to the user. Note: CHIM administrators should never use pass phrase profiles!

**Group profile:** A group profile defines a group of users who can log on collectively to obtain permissions different from the permissions they obtain when logging on individually. The group profile contains the user ID of the group, references to the profiles of the individual group members, the number of members required to authenticate, and a reference to the role assigned to the group.

The figure below shows an example of an access control configuration based on the role definitions delivered with CHIM:

![Access Control Diagram](image)

There are four users, Peter, Susan, Carol and John. In the example the following profiles are defined:

- Peter has a personal profile with user id PETER and role CHIMFST.
- Susan has a personal profile with user id SUSAN and role CHIMFST.
- Carol has a personal profile with user id CAROL and role CHIMLST.
- John has a personal profile with user id JOHN and role CHIMLST.
• All four are members of a group with user id ADMIN and role CHIMADM.

The set up works like this:

• When none of the users are logged on, the DEFAULT role is in effect.

• If Peter or Susan logs on using their personal profiles, they gain permission to load first master key parts via the CHIMFST role.

• If Carol or John logs on using their personal profiles, they gain permission to load last master key parts via the CHIMLST role.

• If any two of the four logs on using the ADMIN profile, they gain permission to manage access control via the CHIMADM role.

To configure the IBM access control system from the default state, you will normally go through the following steps:

• Create and personalize TKE smart cards to be used for log on by individual users (see Create and personalize TKE smart card (p. 36)).

• Define roles (see Create or edit role (p. 43)).

• Generate and back up log on keys for users (see Generate IBM coprocessor logon key (p. 46)).

• Create smart card profiles for users (see Create or edit smart card profile (p. 47)).

• Create group profiles (see Create or edit group profile (p. 46)).

• Limit the permissions of the DEFAULT role to an absolute minimum. (see Create or edit role (p. 43)).

Once the access control system has been properly configured, you can use the same functions to perform ordinary maintenance of the access control system (for example to introduce new users or revoke access for existing users).

This chapter describes the operations you perform to manage access control. For more information about the IBM access control system, refer to the document PCIe Cryptographic Coprocessor CCA Support Program Installation Manual.

**Create or edit role**

**Overview**

A role defines a set of permissions to use functionality in an IBM coprocessor. It can be associated with one or more user profiles in the coprocessor and provides an efficient way manage permissions for those users.

Here we show how to edit a new or existing role in a device group.

**Prereqs**

• You must be logged on to the relevant device group with sufficient authority (eg a user having the DEFAULT role on unconfigured coprocessors or a user having the CHIMADM role on configured coprocessors).

**Steps**

• Go to the 'Roles' page.
• Press 'Create' or select an existing role and press 'Edit' to open the role editing window:

In this window you must specify:

**Role**: The name of the role (up to 8 characters long). The name must be unique and is used to identify the role elsewhere, for example when you create user profiles.

**Comment**: An optional description of the role.

**Valid Times in GMT**: A time interval (in UTC time reference), when the role is active. You can use this to limit the use of the role to a specific time window every day. If you specify the same value in both fields (e.g. 00:00 and 00:00 or 23:00 and 23:00) it means that the role will be active all 24 hours.

**Valid Days**: What days of the week the role is active. You can use these to limit the use of the role to certain week days.

**Permitted Operations**: Functions that are permitted by this role. Some of the functions are related to the management of the IBM coprocessors, for example loading of master keys and access control management, while others are related to the cryptographic functions used by applications. For more information about the permitted operations, see IBM CCA Basic Services Reference and Guide for the IBM PCIe and IBM PCI-X Cryptographic Coprocessors. For your convenience, CHIM is delivered with standard role definitions for roles that can be used by CHIM managers. **Restricted Operations**: Functions that are not permitted by the role.

**Required Authentication Strength**: Leave at 0.

• Fill in the values as required and press 'Save'.

The new or changed role will be added to the pending operations list:
You need to commit the pending operation to install the role. You can do it now, or you can add further changes to the pending operations list and commit them all at once (see Pending Operations window (p. 22)).

• Press 'Commit' if you want to carry out the pending role operation now. This will install the role in the device group.

Delete roles

Overview

Here we show how to delete one or more roles from a device group.

Prereqs

• You must be logged on to the relevant device group with sufficient authority (eg a user having the DEFAULT role on unconfigured coprocessors or a user having the CHIMADM role on configured coprocessors)

• The roles to be deleted are not referenced by any existing user profiles. This restriction applies to the moment when the roles are actually deleted, that is, when the pending role deletion operations are committed. However CHIM will make the check as soon as you schedule the delete operation.

Steps

• Go to the ‘Roles’ page.

• Select the roles to be deleted.

• Press ‘Delete’.

The request to delete the roles will now be added to the pending operations list:
You need to commit the pending operations to delete the roles. You can do it now, or you can add further changes to the pending operations list and commit them all at once (see Pending Operations window (p. 22)).

- Press 'Commit' if you want to carry out the pending delete operations now. This will delete the roles from the device group.

**Generate IBM coprocessor logon key**

**Overview**

In order to log on to IBM coprocessors using a smart card, you need a smart card with a logon key.

Here we show how to generate a logon key on a smart card.

**Prereqs**

- You must be logged on to a device group.

- The person to logon using smart card must be present, must have a personalized TKE smart card (see Create and personalize TKE smart card (p. 36)), and must know the 6 digit PIN to access the smart card.

**Steps**

- Go to the 'Smart Cards' page.

- Insert the personalized TKE smart card into smart card reader 1.

- Press 'Generate Logon Key'.

- If prompted for a PIN enter 6 digit PIN.

You will now be prompted for a profile name:
The name you enter here will be used as profile name when logging on to IBM coprocessors using the smart card. Therefore make sure to select a unique name that is not used by any other user.

- Enter the name of the smart card user (up to 8 characters long).
- If prompted whether to overwrite an existing key, make sure you want to do so before confirming.

The logon key will now be generated. This may take a minute or more.

The smart card can now be used as a logon card. You need to create a smart card profile in order to use the smart card to log on to a device group (see Create or edit smart card profile (p. 47)).

Create or edit smart card profile

Overview

A smart card profile defines a smart card user to an IBM coprocessor. A smart card user is a user who logs on to the coprocessor using a smart card.

Here we show how to edit a new or existing smart card profile in a device group.

Prereqs

- You must be logged on to the relevant device group with sufficient authority (eg a user having the DEFAULT role on unconfigured coprocessors or a user having the CHIMADM role on configured coprocessors)
- If you are creating a new smart card profile, then the smart card user is present and has a smart card with an IBM coprocessor logon key (see Generate IBM coprocessor logon key (p. 46)).

Steps

- Go to the 'Profiles' page.
- Press 'Create' or select an existing smart card profile and press 'Edit'.
- If you are creating a new profile, you will be prompted for the profile type. In that case select 'SMARTCARD' and insert the smart card with the IBM coprocessor log on key.

You should now see the smart card profile editing window:
In this window you must specify:

**User ID:** The name of the smart card user (up to 8 characters long). This is read from the smart card and cannot be changed. The name is stored on the smart card along with the IBM coprocessor logon key when the key is generated (see Generate IBM coprocessor logon key (p. 46)).

**Comment:** An optional description of the profile.

**Activation Date:** The first date that the profile is active.

**Expiration Date:** The last date that the profile is active (it will be inactive after this date).

**Role:** The role associated with this profile. When the user logs on using this profile, he will be granted the permissions defined by the selected role.

**Public Key:** The public part of the users IBM coprocessor logon key. This is read from the smart card.

- Press 'Read Smart Card' to read the logon key from the smart card. You can use this to update the logon key for an existing user.

- Fill in the values as required and press 'Save'.

The new or changed profile will be added to the pending operations list:
You need to commit the pending operation to install the profile. You can do it now, or you can add further changes to the pending operations list and commit them all at once (see Pending Operations window (p. 22)).

- Press 'Commit' if you want to carry out the pending profile operation now. This will install the profile in the device group.

Create or edit pass phrase profile

Overview

A pass phrase profile defines a pass phrase user to an IBM coprocessor. A pass phrase user is a user who logs on to the coprocessor using a pass phrase.

Note: Don't create pass phrase profiles for CHIM administrators and operators – CHIM personnel should always use smart cards for authentication, and hence be associated with smart card profiles.

Here we show how to edit a new or existing pass phrase profile in a device group.

Prereqs

- You must be logged on to the relevant device group with sufficient authority (e.g., a user having the DEFAULT role on unconfigured coprocessors or a user having the CHIMADM role on configured coprocessors).
- The person knowing the pass phrase must be present. The pass phrase must be specified no matter whether the pass phrase profile is created or changed.

Steps

- Go to the ‘Profiles’ page.
- Press ‘Create’ or select an existing pass phrase profile and press ‘Edit’.
- If you are creating a new profile, you will be prompted for the profile type. In that case select ‘PASSPHRASE’.

You should now see the pass phrase profile editing window:
In this window you must specify:

**User ID:** The name of the pass phrase user (up to 8 characters long). Must be specified when creating a new user. If you are editing an existing user it cannot be changed.

**Comment:** An optional description of the profile.

**Activation Date:** The first date that the profile is active.

**Expiration Date:** The last date that the profile is active (it will be inactive after this date).

**Role:** The role associated with this profile. When the user logs on using this profile, he will be granted the permissions defined by the selected role.

**Passphrase & Confirm Passphrase:** The pass phrase used to log on to the profile.

**Passphrase Expiry Date:** Date the pass phrase can no longer be used (it will be inactive after this date).

- Fill in the values as required and press ‘Save’.

The new or changed profile will be added to the pending operations list:
You need to commit the pending operation to install the profile. You can do it now, or you can add further changes to the pending operations list and commit them all at once (see Pending Operations window (p. 22)).

• Press ‘Commit’ if you want to carry out the pending profile operation now. This will install the profile in the device group.

**Create or edit group profile**

**Overview**

A group profile defines a user group to an IBM coprocessor. A group profile allows a group of people to log on together to obtain permissions, that you would not want any single person to have.

Here we show how to edit a new or existing group profile in a device group

**Prereqs**

• You must be logged on to the relevant device group with sufficient authority (eg a user having the DEFAULT role on un-configured coprocessors or a user having the CHIMADM role on configured coprocessors).

• The coprocessors in the device group already contain profiles for the members that you want to include in the group.

**Steps**

• Go to the ‘Profiles’ page.

• Press ‘Create’ or select an existing group profile and press ‘Edit’.

• If you are creating a group profile, you will be prompted for the profile type. In that case select ‘GROUP’.

You should now see the group profile editing window:
In this window you must specify:

**User ID:** The name of the group (up to 8 characters long). Must be specified when creating a new group. If you are editing an existing group it cannot be changed.

**Comment:** An optional description of the group.

**Activation Date:** The first date that the profile is active.

**Expiration Date:** The last date that the profile is active (it will be inactive after this date).

**Role:** The role associated with this profile. When a group of users logs on using this profile, they will be granted the permissions defined by the selected role.

**Type:** The type of profiles to include in this group. The members of a group must all be the same type of profile. You can’t mix for example pass phrase profiles and smart card profiles in a single group.

**Required Group Members:** The number of group members required to log on in order to log on to this group. If the group members themselves are groups, then the logon requirements of the individual groups must also be satisfied.

**Available Profiles:** Profiles that can be included in the group.

**Group Members:** Profiles that are members of the group.

- Fill in the values as required and press ‘Save’.

The new or changed profile will be added to the pending operations list:
You need to commit the pending operation to install the profile. You can do it now, or you can add further changes to the pending operations list and commit them all at once (see Pending Operations window (p. 22)).

• Press ‘Commit’ if you want to carry out the pending profile operation now. This will install the profile in the device group.

Delete profiles

Overview

Here we show how to delete one or more profiles from a device group.

Prereqs

• You must be logged on to the relevant device group with sufficient authority (eg a user having the DEFAULT role on unconfigured coprocessors or a user having the CHIMADM role on configured coprocessors)

• The profiles to be deleted are not referenced by any existing group profiles. This restriction applies to the moment when the profiles are actually deleted, that is, when the pending profile deletion operations are committed. However CHIM will make the check as soon as you schedule the delete operation.

Steps

• Go to the ‘Profiles’ page.

• Select the profiles to be deleted.

• Press ‘Delete’.

The request to delete the profiles will now be added to the pending operations list:
You need to commit the pending operations to delete the profiles. You can do it now, or you can add further changes to the pending operations list and commit them all at once (see Pending Operations window (p. 22)).

- Press ‘Commit’ if you want to carry out the pending delete operations now. This will delete the profiles from the device group.

**Managing master keys**

The ‘Master Keys’ page shows the contents of the master key registers in the device group. Note that the values shown are taken from the default device in the group. Under normal conditions, the values are the same in the remaining devices in the group.
The IBM coprocessor uses four different master keys to protect application keys, the DES, RSA, AES and ECC master keys:

- The DES master key encrypts DES keys in the DES key store.
- The RSA master key encrypts RSA and DSA keys in the PKA key store.
- The AES master key encrypts AES keys in the AES key store.
- The ECC master key encrypts ECC keys in the PKA key store.

The IBM coprocessor keeps track of three generations of each master key: the NEW, CURRENT and OLD.

- The CURRENT master keys are the master keys currently in service.
- The NEW master keys are the master keys ready to be brought in service.
- The OLD master keys are the previous master keys no longer in service.

For each master key register you can see the status (whether it is empty, contains a partial master key or a complete master key) and the master key verification pattern. For DES and RSA master key registers, you can choose between MDC-4 and SHA-1 key verification methods.

The IBM coprocessor cannot operate without master keys being present. The steps required to get master keys in place are the following:

1. You must generate key parts for the master keys. Each master key requires at least two key parts (first and last) to be generated. Key parts are stored on smart cards. (see Generate key parts (p. 55)) You should create back ups of the master key parts on separate smart cards (see Copy Smart Card window (p. 23)).

2. You must load master key parts into the NEW master key registers to form complete master keys. (see Load master key parts (p. 57))

3. You must set the master keys. When you do that, the NEW master keys are moved to the current master key registers and the CURRENT master keys (if present) are moved to the OLD master key registers. (see Set master keys (p. 59))

4. You must reencipher (or initialize) key stores associated with the master keys that have been changed. (see Reencipher key stores (p. 60)).

Master key management may also involve getting rid of obsolete master keys and key parts. You can clear the NEW and OLD master key registers (see Clear new and old master key registers (p. 61)) and key parts stored on smart cards (see Smart Cards page (p. 21)).

This chapter describes all the operations you perform to manage master keys.

Generate key parts

Overview

Master keys are assembled from two or more master key parts. Here we show how to generate master key parts and store them securely on a smart card. The master key parts are generated using a secure random number generator within the tamper resistant IBM hardware of a device in the device group, and transferred to the smart card via a secure session. The secure session is established directly between the
IBM coprocessor and the smart card and requires the IBM coprocessor and the smart card to be enrolled in the same zone (see Smart card zone (p. 5)). Note: The master key parts can only be loaded to devices enrolled in the zone that was used when the key parts were originally created.

**Prereqs**

- You must be logged on to the relevant device group with sufficient authority (e.g., a user having the CHIMFST, CHIMINT, or CHIMLST role).

- The device group and the smart card to hold the key parts must be enrolled in the same smart card zone (see Smart card zone (p. 5) and Devices page (p. 11)).

**Steps**

- Go to the ‘Smart Cards’ page.

- Insert the key card to hold the key parts in smart card reader 1.

The window will update to show the smart card contents (if any):

- Press 'Generate'. If you are prompted for a smart card, then you possibly inserted the card in the wrong reader, so try to move it to the other reader.

- If prompted enter the 6 digit PIN to access the smart card.
You should now see the Master Key Parts dialog:

- Select the key part type you want to generate, either first, middle or last and one or more master keys that you want to generate key parts for. It is highly recommended that you also fill in the key part descriptions, for example: PROD EMV servers 2013901

- Press 'Generate'.

The dialog should now update to reflect the new key parts on the smart card. It is recommended that you back up the key parts to another smart card (see Copy Smart Card window (p. 23)) before loading them to the master key registers (see Load master key parts (p. 57)).

**Load master key parts**

**Overview**

Master keys are assembled from two or more master key parts. Here we show how to load master key parts from a smart card into the NEW master key registers in a device group. Key parts must be loaded in correct order (first key parts first, then any middle key parts, and finally last key parts). The master key parts are transferred using secure sessions established directly between the smart card and the IBM coprocessor devices in the device group. Note: The master key parts can only be loaded to devices enrolled in the same zone as the smart card (see Smart card zone (p. 5)).

**Prereqs**

- You must be logged on to the relevant device group with sufficient authority (eg a user having the CHIMFST, CHIMINT or CHIMLST role for loading first, intermediate or last key parts respectively)

- The devices in the device group and the smart card holding the key parts must be enrolled in the same smart card zone. (see Smart card zone (p. 5) and Devices page (p. 11))
The relevant NEW master key registers must be in the appropriate status (EMPTY when loading first key parts, PARTIAL when loading intermediate or last key parts). If any of the new master key register contains key material you don’t need, you can clear them. (see Clear new and old master keys (p. 61))

The status and value of all the target master key registers are the same in all modules in the group.

**Steps**

- Go to the ‘Smart Cards’ page.
- Insert the smart card holding the key parts in smart card reader 1.

The window will update to show the smart card contents:

- Select the key parts to load in the list (press and hold Ctrl while clicking to select multiple parts).
• Press 'Load Key Parts'. This will bring up a confirmation dialog.

• Press 'Load master key parts' to confirm.

• If prompted enter the 6 digit PIN to access the smart card.

The key parts should now be loaded.

• Go to the 'Master Keys' page and verify that the key parts have been loaded as expected. You should see some turn to PARTIAL.

To activate the master keys just loaded, they must be set. (see Set master keys (p. 56)).

**Set master keys**

**Overview**

When new master keys have been loaded they must be activated. Here we show how to activate (set) master keys that have been loaded to the NEW master key registers in a device group. When set, the new master keys are moved from the NEW master key registers to the CURRENT master key registers, and the previous master keys are moved to the OLD master key registers. When master keys have been set you should reencipher any key stores that are enciphered under the previous master keys. (see Reencipher key stores (p. 60))

**Prereqs**

• You must be logged on to the relevant device group with sufficient authority (eg a user having the CHIMLST role).

• The new master keys must be present in the relevant NEW master key registers (registers must be in COMPLETE status).

• The value of NEW master key registers must be the same in all devices in the group for each type of master key.

• There are no key stores encrypted under one of the old master keys currently present in the OLD master key registers (as the old master keys will be overwritten and the key stores rendered unusable). If you have such key stores, you should reencipher them to the current master keys before setting the new master keys. (see Reencipher key stores (p. 60))

**Steps**

• Go to the 'Master Keys' page.

• Select the NEW master key registers holding the master keys to be activated in the list (press and hold Ctrl while clicking to select multiple registers).
Press ‘Set’. This will bring up a confirmation dialog.

Press ‘Set current Master Key register’ to confirm.

The master keys should now be set. To reencipher key stores encrypted under the previous master keys, see Reencipher key stores (p. 60).

Reencipher key stores

Overview

When new master keys have been activated, key stores enciphered under the previous master keys must be reenciphered to encryption under the activated master keys. Here we show how to reencipher key stores.

Prereqs

- You must be logged on to the relevant device group with any authority (reenciphering is not considered a sensitive operation).

- The new master keys must have been activated and the previous master keys present in the OLD master key registers.

- The key stores to be reenciphered must be encrypted with the previous master keys present in the OLD master key registers.

Steps

- Go to the ‘Master Keys’ page.
• Select the CURRENT master key registers holding the activated master keys (press and hold Ctrl while clicking to select multiple registers).

• Press ‘Reencipher Key Store’. This will bring up a confirmation dialog.

• Press ‘Reencipher to current Master Key’ to confirm.

The key stores should now be reenciphered.

**Clear new and old master key registers**

**Overview**

You can clear the NEW and OLD master key registers. This is useful for example if you loaded wrong key parts to a NEW master key register or if you want to make sure an
OLD master key can no longer be used (CCA allows keys encrypted under the OLD master key to be used).

**Prereqs**

- You must be logged on to the relevant device group with sufficient authority (e.g., a user having the CHIMFST role)
- There is no key store encrypted under the master key(s) to be cleared.

**Steps**

- Go to the 'Master Keys' page.
- Select the master key register(s) to be cleared.

- Press 'Clear Register'. This will bring up a confirmation dialog.
- Press 'Clear Master Key registers' to confirm.

The selected master key registers should now be cleared.

---

²Please note that once logged on to the local adapter, the session will be maintained as long as the device group window is open.

4. CHIM audit log

The CHIM workstation application generates an audit trail containing log records for the actions performed when working with CHIM. The audit trail is stored in up to three generations in files named as follows:

/var/log/chim-audit.log
/var/log/chim-audit.log.1
/var/log/chim-audit.log.2
...

the /var/log/chim-audit.log **being the most recent file**, /var/log/chim-audit.log.1 **being the second most recent file** and so on.

Audit files are written using Linux root authority and are read-only for other users in order to prevent ordinary users from manipulating the log. The files are written in plain text and can be read using any Linux text viewer or editor, for example gedit.