Note: Before using this information and the products it supports, be sure to read the general information under “Notices” on page 57.

Sixth Edition (January, 2016)
This and other publications related to the IBM 4765 PCIe Cryptographic Coprocessor can be obtained in PDF format from the product Web site. Click on the PCIe Cryptographic Coprocessor link at http://www.ibm.com/security/cryptocards, and then click on the Library link.

Reader’s comments can be communicated to IBM by contacting the Crypto team at crypto@us.ibm.com.

© Copyright International Business Machines Corporation 2011, 2016.
Note to U. S. Government Users—Documentation related to restricted rights Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.
Contents

About this document.................................................................................................................................vii
Prerequisite knowledge...............................................................................................................................vii
Typographic conventions............................................................................................................................vii
Related publications.................................................................................................................................vii
Summary of changes.................................................................................................................................viii
Overview..................................................................................................................................................1
Supported hardware and software..............................................................................................................2
SCUP/CNM setup.....................................................................................................................................3
  Differences between RHEL and SLES.....................................................................................................3
  Installation steps....................................................................................................................................3
  Configure operating system (RHEL only).................................................................................................3
  Configure GCC (RHEL only)....................................................................................................................4
  Install prerequisite packages..................................................................................................................4
    Install RHEL packages.........................................................................................................................4
    Install SLES packages..........................................................................................................................5
  Build posc-lite......................................................................................................................................7
  Install libusb-1 (RHEL only)..................................................................................................................8
  Download OMNIKEY device driver and support files........................................................................8
    OMNIKEY device driver......................................................................................................................8
    OpenCard Framework..........................................................................................................................9
  Install OMNIKEY device driver and support files............................................................................9
  Start smart card service.........................................................................................................................10
  Set up 32-bit Java (RHEL only).............................................................................................................10
  Install and set up SCUP and CNM..........................................................................................................12
  Initialize CCA using CNM.....................................................................................................................12
    Enable required access control points..............................................................................................12
    Enable smart card support in CNM.....................................................................................................13
Smart card initialization with SCUP............................................................................................................14
  Handling multiple adapters in SCUP.....................................................................................................14
  Launch SCUP......................................................................................................................................14
  Initialize and personalize a CA smart card.........................................................................................17
  Initialize and enroll a TKE smart card..................................................................................................23
  Personalize a TKE smart card...............................................................................................................27
  Enroll the crypto adapter in a zone.......................................................................................................31
CNM smart card functions..........................................................................................................................34
  Handling multiple adapters in CNM.....................................................................................................34
  Generate a crypto logon key...................................................................................................................34
  CCA profiles using smart cards for authentication data.......................................................................36
  CCA logon with a smart card profile.....................................................................................................39
  Smart card master key parts..................................................................................................................40
  Change TKE smart card PIN..................................................................................................................43
  View smart card details.........................................................................................................................45
  Manage smart card contents.................................................................................................................46
  Copy smart card..................................................................................................................................47
    Group logon......................................................................................................................................49
Smart card security....................................................................................................................................52
  Error codes.........................................................................................................................................53
Troubleshooting.........................................................................................................................................54
Notices......................................................................................................................................................57
  Copying and distributing softcopy files.................................................................................................57
  Trademarks.........................................................................................................................................57
List of abbreviations and acronyms..........................................................................................................58
Index.........................................................................................................................................................59
Figures

Figure 1 Crypto adapter logon..............................................................15
Figure 2 Passphrase ........................................................................15
Figure 3 TKE SCUP main window.....................................................16
Figure 4 OMNIKEY Card Readers..................................................17
Figure 5 Initialize and personalize CA smart card window.............18
Figure 6 Initialize CA smart card dialog.......................................18
Figure 7 CA smart card zone key length dialog............................19
Figure 8 CA smart card initialization............................................19
Figure 9 CA smart card PIN entry message.................................19
Figure 10 CA PIN entry.................................................................20
Figure 11 CA smart card second PIN message..............................20
Figure 12 CA smart card zone dialog............................................20
Figure 13 CA smart card description dialog.................................21
Figure 14 CA smart card build message.......................................21
Figure 15 CA smart card success dialog.....................................22
Figure 16 TKE SCUP main window with CA smart card details...22
Figure 17 Initialize and enroll TKE smart card window..............23
Figure 18 CA smart card insertion dialog....................................24
Figure 19 CA smart card PIN 1 message.......................................24
Figure 20 CA PIN entry.................................................................24
Figure 21 CA smart card PIN 2 message.......................................25
Figure 22 TKE smart card insertion message...............................25
Figure 23 TKE smart card initialization message.........................26
Figure 24 TKE smart card success dialog.....................................26
Figure 25 TKE SCUP main window with TKE smart card details..27
Figure 26 Personalize TKE smart card window............................28
Figure 27 TKE smart card insertion message...............................28
Figure 28 TKE smart card PIN message.......................................29
Figure 29 TKE PIN entry...............................................................29
Figure 30 TKE smart card description dialog...............................29
Figure 31 TKE smart card success dialog.....................................30
Figure 32 TKE main window with smart card details....................30
Figure 33 Enroll adapter window................................................31
Figure 34 Enroll adapter dialog....................................................32
Figure 35 Enroll adapter insertion dialog.....................................32
Figure 36 Enroll adapter PIN 1 message........................................32
Figure 37 Enroll adapter PIN 1 entry message...............................33
Figure 38 Enroll adapter PIN 2 entry message...............................33
Figure 39 Enroll adapter success dialog........................................33
Figure 40 CNM Generate Logon Key window...............................35
Figure 41 Generate Logon Key insert dialog.................................35
Figure 42 Generate Logon Key PIN message.................................35
Figure 43 Generate Logon Key user ID dialog..............................36
Figure 44 Generate Logon Key success dialog..............................36
Figure 45 CNM Profiles window..................................................37
Figure 46 Profile Management window........................................37
Figure 47 New profile dialog........................................................38
Figure 48 New profile insert dialog...............................................38
Figure 49 New profile setup window.............................................38
Figure 50 New profile success dialog..........................................39
Figure 51 CNM Smart Card Logon window.................................39
Figure 52 TKE Smart Card insertion message.............................40
Figure 53 TKE PIN on card reader 2............................................40
Figure 54 CNM Smart Card Parts window

Figure 55 Insert TKE smart card reader 2 dialog

Figure 56 Master key parts window

Figure 57 Master key parts description dialog

Figure 58 Master key parts window with results

Figure 59 CNM Change PIN window

Figure 60 Change PIN dialog

Figure 61 Change PIN message

Figure 62 TKE PIN on card reader 2

Figure 63 New PIN entry message

Figure 64 Change PIN success dialog

Figure 65 CNM display details window

Figure 66 Smart card details window

Figure 67 CNM manage contents window

Figure 68 Manage contents window

Figure 69 CNM copy smart card window

Figure 70 Source TKE smart card dialogs

Figure 71 Copy smart card dialog

Figure 72 CNM create profile window

Figure 73 CNM select profile type dialog

Figure 74 Profile management window

Figure 75 CNM profile success dialog

Figure 76 CNM profile window
Tables

Table 1 Supported hardware and software.................................................................2
Table 2 List of Required ACPs...............................................................................13
Table 3 CNM return/reason codes.........................................................................53
About this document
This document contains information to help you use the Smart Card Utility Program (SCUP) and
Cryptographic Node Management utility (CNM) to manage smart cards with the IBM 4765 PCIe
Cryptographic Coprocessor.
This manual should be used in conjunction with the manuals listed under “Related publications” in this
section.

Prerequisite knowledge
The reader of this book should understand how to perform basic tasks (including editing, system
configuration, file system navigation, and package installation) on the host machine and in the Linux®
environment. Familiarity with IBM 4765 Cryptographic Common Architecture (CCA) and CNM is required.
Knowledge of Trusted Key Entry (TKE) is also useful.

Typographic conventions
This publication uses the following typographic conventions:

- Commands that you enter verbatim onto the command line are presented in monospace type.
- Variable information and parameters, such as file names, are presented in italic type. Variables in
  commands are enclosed in <> symbols. For example:
  COMMAND parameter1 <variablename>
- Constants are presented in bold type.
- The names of items that are displayed in graphical user interface (GUI) applications, such as pull-
  down menus, check boxes, radio buttons, and fields, are presented in bold type.
- Items displayed within pull-down menus are presented in bold italic type.
- Function names are presented in italic type.
- System responses in a shell-based environment are presented in monospace type.
- Web addresses and directory paths are presented in italic type.
- Syntax diagrams follow these typographic conventions. Optional items appear in brackets. Lists
  from which a selection must be made appear in braces with vertical bars separating the choices.
  For example:
  COMMAND  firstarg [secondarg] {a | b}
  A value for firstarg must be specified. secondarg may be omitted. Either a or b must be specified.

Related publications
Publications about IBM’s family of cryptographic coprocessors are available at:

Publications about the IBM 4765 PCIe Cryptographic Coprocessor and CCA are available at:

Various publications about cryptography are available at:

**Summary of changes**

This edition of *IBM 4765 PCIe Cryptographic Coprocessor Smart Card User Guide* contains product information that is current with the IBM 4765 PCIe Cryptographic Coprocessor announcements.
Overview
Starting with CCA release 4.2, support for smart card functionality is in the IBM System x® workstation release of CCA. Specifically, it is now possible to use smart cards to accomplish the following tasks:

- Initialize smart cards for use with CNM.
- Generate and store CCA DES and PKA master key parts on supported smart cards.
- Load CCA master key parts stored on supported smart cards.
- Log on to CCA using smart card CCA profiles tied to an RSA key pair associated with a particular smart card and user profile.

There are two GUI-based components for dealing with smart cards using the workstation release CCA and the IBM 4765 Cryptographic Coprocessor.

The first component is named SCUP (Smart Card Utility Program) which is used to initialize smart cards and perform other smart card related administrative tasks.

The second component is an updated version of CNM which contains new functionality targeted for use with smart cards initialized by SCUP.

Each of these components is described in the sections that follow.

To obtain smart cards from IBM, or for additional assistance in setting up and configuring SCUP and CNM, please contact either the EMEA Crypto Competence Center at ccc@dk.ibm.com or IBM Crypto support at crypto@us.ibm.com.
Supported hardware and software
This section describes the set of hardware and software that is supported by SCUP/CNM.

In this document, Linux operating systems are referred to by these short names:

<table>
<thead>
<tr>
<th>Operating System Name</th>
<th>Short Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Novell® SUSE® Linux Enterprise Server 11 Service Pack 3</td>
<td>SLES 11.3</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server</td>
<td>RHEL</td>
</tr>
</tbody>
</table>

Table 1 Supported hardware and software

<table>
<thead>
<tr>
<th>Hardware or software</th>
<th>Release</th>
</tr>
</thead>
</table>
| Operating system     | RHEL 6 64-bit and 32-bit  
                        | SLES 11.3 64-bit and 32-bit  
                        | SLES 11.2 64-bit |
| CCA                  | 4.4.55, 4.4.20, and 4.4.16  |
| Java                 | 6 (32-bit only) |
| Card readers (2)     | OMNIKEY CardMan® Model 3821  
| Smart card type      | NXP JCOP 41 v2.2.1 72k SmartCard I/F  
SCUP/CNM setup

The following steps describe how to set up the smart card readers and SCUP for use with CNM. This document assumes that the 4765 device driver and support program have been downloaded and installed from the IBM Crypto Web site:

Differences between RHEL and SLES

By default, SLES users should not have to configure the operating system or configure gcc. However, by default on RHEL, gcc is not configured to properly build/link 32-bit applications. Also, even with the compatibility options specified during the OS install, only a small subset of 32-bit packages are installed.

Furthermore, only a 64-bit JVM is installed. A 32-bit JVM is needed, and it requires the installation of several additional RPMs. Several of the steps in this list are specifically included to enable 32-bit application support that is needed for smart card functions.

Installation steps

Complete these steps to set up the smart card readers and SCUP for use with CNM. You must perform the steps in the order listed in order to manage the interdependencies among the packages.

1. **RHEL only** Configure the RHEL installation to include 32-bit support.
2. **RHEL only** Configure gcc to build 32-bit applications.
3. Install and build the prerequisite packages required to build the pcsc-lite package required by the OMNIKEY drivers.
4. Build the pcsc-lite package from source.
5. **RHEL only** Install libusb-1.
6. Download the OMNIKEY device driver and support files.
7. Install the OMNIKEY device driver and support files.
8. Start the smart card service.
9. **RHEL only** Set up 32-bit Java.
10. Install the CCA Support Program.
11. Initialize CCA with CNM.
12. Use SCUP and CNM to manage Certificate Authority (CA) and TKE smart cards.
13. Perform troubleshooting activities.

Details for each step are in the following sections.

Configure operating system (RHEL only)

During the 64-bit RHEL OS installation, when configuring as a “Software Development Workstation,” for Base System Additional Software, ensure that “Compatibility Libraries” and “Legacy UNIX compatibility” are selected. If these are not installed, the instructions below will fail because 64-bit RHEL does not include 32-bit support by default.

During both 64-bit and 32-bit RHEL OS installation, some versions of RHEL do not include smart card support by default. When configuring as a “Software Development Workstation,” for Base System
Additional Software, ensure that “Smart Card Support” is selected. If this is not installed, the instructions below will fail.

After RHEL is installed and the server is rebooted, and before attempting the rest of the instructions in this section, ensure that no process that uses smart cards is running. Also, remove any such process from the list of programs that are autostarted with RHEL.

**Configure GCC (RHEL only)**

By default, gcc is not configured to compile and link 32-bit applications on 64-bit RHEL.

The following package from the RHEL 6.x 64-bit ISO is required for proper GCC configuration:

<table>
<thead>
<tr>
<th>gcc for RHEL 6.5 / 6.4 / 6.3 64-bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>glibc-devel-2*.i686.rpm</td>
</tr>
</tbody>
</table>

To install this RPM, issue this command:

```
rpm –ivh glibc-devel-2*.i686.rpm
```

**Install prerequisite packages**

This section describes how to install the prerequisite RHEL or SLES packages as well as how to build and install libusb on RHEL. These packages are required by the OMNIKEY device driver.

**Install RHEL packages**

As mandated by the prerequisites for the current version of the smart card reader drivers provided by OMNIKEY, several RHEL packages need to be installed or updated in order to build pcsc-lite from source. The following additional packages are required:

**32-bit RHEL**

The default installation for 32-bit RHEL includes all of the necessary packages. No additional packages are needed.

**64-bit RHEL**

The following additional packages are required for 64-bit RHEL. Install these packages from the RHEL 6.x 32-bit (x86) ISO. If you install the packages separately, the packages must be installed in the order listed and any packages shown in the same row must be installed together.

<table>
<thead>
<tr>
<th>32-bit RHEL 6.5 / 6.4 / 6.3 Packages for 64-bit RHEL</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit-libs-2*.i686.rpm</td>
<td></td>
</tr>
<tr>
<td>expat-2*.i686.rpm</td>
<td></td>
</tr>
<tr>
<td>libuuid-2*.i686.rpm</td>
<td></td>
</tr>
<tr>
<td>libblkid-2*.i686.rpm</td>
<td></td>
</tr>
</tbody>
</table>
Place these files in a single directory and then issue individual rpm commands in the same order as the list of packages above. For example:

```
rpm --ivh --force audit-libs-2*.i686.rpm
rpm --ivh --force expat-2*.i686.rpm
...```

When instructed to install packages together, issue the rpm command with multiple packages together. For example:

```
rpm --ivh --force gamin-0*.i686.rpm zlib-1*.i686.rpm glib2-2*.i686.rpm```

Note: `--force` is needed to ensure that pcsc-lite installs properly.

### Install SLES packages

As mandated by the prerequisites for the current version of the smart card reader drivers provided by OMNIKEY, several SLES packages need to be installed or updated in order to build pcsc-lite from source.

### 32-bit SLES

The following additional packages are required for 32-bit SLES. Install these packages from the SLES 11.3 / 11.2 32-bit (x86) OS DVDs and SDK DVDs, which are both a part of a SLES 11.3 / 11.2 download.
when a license is purchased. At the time of publication of this document, only image 1 of the SLES OS and image 1 of the SLES SDK are required.

<table>
<thead>
<tr>
<th>32-bit SLES 11.3 / 11.2</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>libcom_err-devel-1*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>libuuid-devel-2*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>libext2fs-devel-1*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>libblkid-devel-2*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>libsmbios-devel-2*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>libusb-0*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>libusb-1_0-devel-1*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>libusb-1_0-0-1*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>libusbpp-0_1-4-0*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>libusb-devel-0*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>dbus-1-devel-1*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>glib2-devel-2*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>dbus-1-glib-devel-0*.i586.rpm</td>
<td></td>
</tr>
<tr>
<td>hal-devel-0*.i586.rpm</td>
<td></td>
</tr>
</tbody>
</table>

Place these files in a single directory and then issue individual rpm commands in the same order as the list of packages above (except for the libusb packages, which must be installed together). For example:

```
rpm –ivh libcom_err-devel-1*.i586.rpm
rpm –ivh libuuid-devel-2*.i586.rpm
...
```

**64-bit SLES**

The following additional 32-bit packages are required for 64-bit SLES. Install these packages from the SLES 11.3 / 11.2 32-bit (x86 / i586) OS DVDs and SDK DVDs, which are both a part of a SLES 11.3 / 11.2 download when a license is purchased. At the time of publication of this document, only image 1 of the SLES OS and image 1 of the SLES SDK are required.

<table>
<thead>
<tr>
<th>32-bit SLES 11.3 / 11.2 Packages</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>libcom_err-devel-1*.i586.rpm</td>
<td></td>
</tr>
</tbody>
</table>

6 IBM 4765 Smart Card User Guide
Place these files in a single directory and then issue individual rpm commands in the same order as the list of packages above (except for the libusb packages, which must be force-installed together). For example:

```
rpm –ivh libcom_err-devel-1*.i586.rpm
rpm –ivh libuuid-devel-2*.i586.rpm
...
```

**Build pcsc-lite**

The pcsc-lite package provides a smart card interface for communicating with smartcards and readers. After the prerequisite packages have been installed and built, you can build the pcsc-lite package from source. Follow these steps:

1. Download pcsc-lite. Navigate to:
   

   **Note:** You may encounter a browser warning about this Web site being untrusted. You can add an exception to allow the browser to continue to access the site.

2. Under “PCSC-Lite,” press Download. The project file list will be displayed. Scroll down to pcsc-lite and select pcsc-lite-1.6.7.tar.bz2. The file will be downloaded.

3. As a non-root user, unpackage and untar the pcsc-lite source bundle:
   
   `tar -xvjf pcsc-lite-1.6.7.tar.bz2`

4. As a non-root user, build pcsc-lite:
   
   - `cd pcsc-lite-1.6.7`
• export PKG_CONFIG_PATH=/opt/lib/pkgconfig:/usr/local/lib/pkgconfig:
  /usr/lib/pkgconfig
• CFLAGS="-m32" LDFLAGS="-m32" ./configure --prefix=/usr --build=i686-pc-
  linux-gnu
• make

5. As root or via sudo:
   make install

Note: If you get an error indicating that libhal is not installed, you have most likely not exported
PKG_CONFIG_PATH.

Note: To make sure that pcsc-lite built properly, run it to check its version number:
   /usr/sbin/pcscd -v

pcsc-lite should run and report its version number.

Once these steps are complete, you can proceed to install libusb-1 (RHEL only) and the OMNIKEY files.

**Install libusb-1 (RHEL only)**
The following package is needed on RHEL to provide a required 32-bit library. Install this package from
the RHEL 6.x 32-bit ISO.

<table>
<thead>
<tr>
<th>32-bit libusb-1 for RHEL 6.5 / 6.4 / 6.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>libusb1-1*.i686.rpm</td>
</tr>
</tbody>
</table>

Issue this command:
   rpm –ivh libusb1-1*.i686.rpm

**Download OMNIKEY device driver and support files**
SCUP and CNM were designed to use the OMNIKEY smart card readers. You need the device driver and
OpenCard Framework to use the OMNIKEY readers.

**OMNIKEY device driver**
The necessary device driver files for the OMNIKEY smart card readers can be downloaded from:
The web page will then display several download links. Ensure you are viewing the correct list of
packages for Linux, and then download the following packages:

• CardMan 3x21 PC/SC CCID for Linux 32 Bit
  Make sure you select version 3.7.0:
  ifdokccid_inx_i686-3.7.0.tar.gz - 135.24 KB – 12/18/2012
• CardMan SPE-API for Linux
  speapi_inx-1.0.1.tar.gz - 2.55 MB – 12/18/2012

If necessary, you can search for the package from the HID Global drivers and downloads page:
From the drop down lists on the right side, select the following:

- Brand: OMNIKEY
- Product: 3821 USB Pinpad
- OS: Linux

Make sure you select version 3.7.0 of the Cardman 3x21 PC/SC CCID for Linux 32 Bit and version 1.0.1 of the Cardman SPE-API for Linux.

**OpenCard Framework**

The necessary library for the OpenCard Framework can be downloaded from:

http://www.openscdp.org/ocf/download.html

Select OpenCard Framework (under Latest release) and download.

**Install OMNIKEY device driver and support files**

Follow these steps to install the OMNIKEY device driver and the additional files needed by SCUP.

1. Install the PC/SC Chip/Smart Card Interface Devices (CCID) files for Linux 32 bit:

   ```
   tar -xvzf ifdokccid_lnx-<version>.tar.gz
   cd ifdokccid_lnx-<version>
   As root (or via sudo if applicable):
   ./install
   ```

   Note: Needed version is 3.7.0.

   After the installation completes, search for the ifdokccid.so file within that directory and copy the file into the /usr/lib directory.

2. Install the CardMan Secure Pin Entry Application Programming Interface (SPE-API) for Linux:

   ```
   tar -xvzf speapi_lnx-<version>.tar.gz
   cd speapi_lnx-<version>
   ```

   Note: Needed version is 1.0.1.

   **Note:** If you want to install the CardMan documentation, you must create the documentation directory before running the install script:

   ```
   mkdir /usr/doc
   ```

   As root (or via sudo if applicable):

   ```
   ./install
   ```

3. Unzip the OpenCard Framework ocf-<timestamp>.zip file:

   ```
   unzip ocf-<version>.zip
   ```

   Note: Needed version is 1.3.1747.

4. Copy the libOCFPCSC1.so shared library from the lib directory of the unzipped OpenCard Framework file into the /usr/lib directory:

   As root (or via sudo if applicable):

   ```
   cd < the directory where you ran unzip ocf-<version>.zip >
   cd ocf/lib
   cp libOCFPCSC1.so /usr/lib/
   ```
Start smart card service
After plugging both smart card readers into USB ports on the server, the smart card readers should display an icon indicating that they are plugged in. This verifies that the USB ports are active.

Note: The smart card readers do not connect directly to the IBM 4765. Instead, they connect to the host computer in which the 4765 resides. The readers use session keys to establish encrypted communication channels with the IBM 4765.

Once both smart card readers indicate that they are connected, start the smart card service by entering the following command (as root or via sudo):

```
/etc/init.d/pcscd restart
```

Once the service has been started, the display on the smart card reader should read:

```
HID OMNIKEY 3821
```

If pcscd fails to start, you may get an error message in `/var/log/messages` stating that `/var/run/pcscd/pcscd.comm` already exists. If this happens, you need to remove `/var/run/pcscd/pcscd.comm` and restart the daemon (as root or via sudo):

```
rm /var/run/pcscd/pcscd.comm
/etc/init.d/pcscd restart
```

Set `pcscd` to restart upon system reboot by entering the following command (as root or via sudo):

```
chkconfig pcscd on
```

You can make sure this change took effect by entering a `chkconfig` command.

Set up 32-bit Java (RHEL only)
IBM does not ship a 32-bit JVM with the installation package. It is up to the customer to ensure that they have a properly installed and configured 32-bit JVM. Install these packages from the RHEL 6.x 32-bit ISO.

Note: the RHEL operating system installation ISO contains a suitable 32-bit JVM. Specifically, these packages provide a suitable JRE:

<table>
<thead>
<tr>
<th>32-bit Java on RHEL 6.5 / 6.4 / 6.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>alsa-lib-1*.i686.rpm</td>
</tr>
<tr>
<td>flac-1*.i686.rpm</td>
</tr>
<tr>
<td>freetype-2*.i686.rpm</td>
</tr>
<tr>
<td>giflib-4*.i686.rpm</td>
</tr>
<tr>
<td>java-1.6.0-openjdk-1.6.0.0*.i686.rpm</td>
</tr>
<tr>
<td>java-1.6.0-openjdk-devel-1.6.0.0*.i686.rpm</td>
</tr>
<tr>
<td>keyutils-libs-1*.i686.rpm</td>
</tr>
</tbody>
</table>
Place these files in a single directory and then issue a single rpm command:

```
rpm -ivh --force *.i686.rpm
```

RPM will figure out the dependencies among the packages.

Note: Other JVMs are available and can be installed. The installation of a suitable JVM is up to the user. For convenience, this procedure is included to depict one example of installing a 32-bit Java. Contact your system administrator for assistance.
Install and set up SCUP and CNM

To install SCUP-enabled CCA and SCUP, run the CCA installer. SCUP and SCUP-enabled CNM are installed if you choose Custom Installation → Smart Card Support during CCA installation. If CCA has already been installed without smart card support, you can run the installer again. Modify the existing instance and specify smart card support. Refer to the IBM 4765 PCIe Cryptographic Coprocessor CCA Support Program Installation Manual for additional information about installing CCA.

Once SCUP and SCUP-enabled CNM are installed, you need to initialize CCA to use SCUP.

Initialize CCA using CNM

This section contains a summary of a sample set of steps to initialize CCA to use SCUP.

1. Run the CCA initialization program that is shipped with the CCA installation package (. /opt/IBM/4765/cnm/cca_test_init.e). This program initializes a CCA profile named tester with a DEFAULT role that has all permissions turned on, and has a logon passphrase of tester. You need this to bootstrap CCA to get ready to enter the master keys. See “Enable required access control points” on page 12 for details about the ACPs.

   **Note:** Your organization’s security policy may cause you to create and manage this initial setup role and profile yourself. For example, you may want the role to have its own name or you may want the profile to be active for only a short period of time. To create the role and profile yourself, use CNM as described in Chapter 5 of the CCA Support Program Installation Manual.

2. Use the tester profile to create the smart cards using SCUP. See “Smart card initialization with SCUP” on page 14 for details.

3. Launch CNM:

   ./opt/IBM/4765/cnm/csulcnm [/SC]

   **Note:** /SC is needed only if you want to use CNM smart card functions before enabling smart card support permanently in cnm.ini (ENABLE_SC=true). See Enable smart card support in CNM on page 13 for instructions.

4. Logon to CNM and perform these tasks:

   a. Update the access control system to narrow the permissions back down to where you want them to be. Make sure the required access control points are enabled (see “Enable required access control points” on page 12 for a list.

   b. Generate the crypto logon keys.

   c. Generate a smart card profile, which associates the logon key with that profile.

   See CNM smart card functions on page 34 for more information.

5. Set a new master key in parts using the smart cards.

   **Note:** Depending on the roles you set up in Step 1 above, this might require several users to logon, one or more at a time.

6. Initialize key storage.

Enable required access control points

To use SCUP and SCUP-enabled CNM, you must enable certain access control points (ACPs) in CNM. For more information about enabling ACPs in roles in CNM, see Chapter 5 of the CCA Support Program Installation Manual.

Ensure that the ACPs in Table 2 on page 13 are listed in Permitted Operations for the role(s) that need to
run SCUP and SCUP-enabled CNM.

Table 2 List of Required ACPs

<table>
<thead>
<tr>
<th>Offset</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>X’0103’</td>
<td>PKA96 PKA Key Generate</td>
</tr>
<tr>
<td>X’0203’</td>
<td>Delete Retained Key</td>
</tr>
<tr>
<td>X’02A5’</td>
<td>CCA Device Cert Imp Auth</td>
</tr>
<tr>
<td>X’02A6’</td>
<td>TKE CA Cert Imp Auth</td>
</tr>
<tr>
<td>X’02A8’</td>
<td>Delete Retained Device Key</td>
</tr>
<tr>
<td>X’02A9’</td>
<td>CCA Device Cert Exp Auth</td>
</tr>
<tr>
<td>X’8002’</td>
<td>TKE User Login</td>
</tr>
</tbody>
</table>

Enable smart card support in CNM

Once you have run CNM once, you can enable smart card support in CNM. To do this, edit the cnm.ini file to specify smart card enablement. By default, cnm.ini is located in /opt/IBM/4765/cnm. Change the line that reads ENABLE_SC=false to ENABLE_SC=true.

After enabling smart card support, you can launch CNM without specifying /SC:

```
./opt/IBM/4765/cnm/csulcnm
```
Smart card initialization with SCUP

SCUP is used to initialize CA and TKE smart cards.

This section contains an illustration of how to use SCUP to initialize and personalize smart cards for use with CNM.

The steps involved in initializing and personalizing smart cards are:

1. Initialize CCA using CNM with a temporary master key and temporary profile.
2. If needed, set the default adapter.
3. Launch SCUP.
4. Initialize and personalize a Certificate Authority (CA) smart card.
5. Initialize and enroll a TKE smart card.
6. Personalize a TKE smart card.
7. Enroll the crypto adapter in a zone.

Handling multiple adapters in SCUP

If your system has more than one IBM 4765 adapter installed, you must ensure that you are referring to the correct adapter when using both SCUP and CNM. On one hand, CLU refers to the first adapter in the system as adapter 0. On the other hand, the CCA environment variable specifying the default adapter for which to target commands refers to the first adapter as CRP01. The “first adapter” can change on system reboot; it merely indicates the first adapter that the host device driver finds upon reboot.

Before launching SCUP, use the export command to set the CSU_DEFAULT_ADAPTER environment variable to indicate a certain adapter. For example:

```bash
export CSU_DEFAULT_ADAPTER=CRP02
```

instructs SCUP to point to the second discovered adapter in the system, which is adapter 1 in CLU.

If this environment variable is not set when you launch SCUP, coprocessor CRP01 is assumed to be the default adapter. If this environment variable is set to an invalid value, you will get an error until the environment variable is set to a valid value.

Launch SCUP

To launch SCUP, run the scup shell script (/opt/IBM/4765/cnm/scup). When SCUP is launched, it displays a login prompt that allows you to log in to a CCA profile to be used by SCUP. See Figure 1 on page 15.

**Note:** Both CNM and SCUP require Java6. In addition, SCUP requires at least one CCA profile with the ACPs listed above enabled. Once SCUP is launched, do not disconnect the smart card reader(s). If a smart card reader is disconnected while SCUP is running, you must exit SCUP and launch it again.

If no CCA profiles are displayed, you must create one to use for SCUP.
Select an appropriate profile, and press Ok.

**Note:** If the list of CCA profiles is empty, then you may not have any profiles that have a role that has the required ACPs enabled. Follow the instructions in Chapter 5 of the *CCA Support Program Installation Manual* to use CNM to enable ACPs in a role and define a user profile associated with that role.

A dialog will appear allowing you to enter the passphrase for the selected profile. See Figure 2. Enter the passphrase for the selected profile and press Ok. **Note:** If the profile is a smart card profile, you will be prompted to enter the PIN through one of the attached smart card readers.

After login, the *TKE SCUP* main window is displayed. See Figure 3 on page 16.
Warning: Only one instance of SCUP or CNM can be running at any given time. Each of these programs must have exclusive use of the smart cards. Running two instances of SCUP, two instances of CNM, or one instance of SCUP and one instance of CNM at the same time will lead to errors.

Two OMNIKEY CardMan 3821 USB smart card readers have been attached to the test machine for this example walkthrough. Initially both smart cards are empty. SCUP will be used to initialize one of the cards as a CA smart card and the other card as a TKE smart card. The card readers have small LCD screens that display prompts at appropriate times. An example setup would look like Figure 4 on page 17. In this setup, card reader 1 is the reader on the left, and card reader 2 is the reader on the right. This document will use these names to refer to the two card readers.
Initialize and personalize a CA smart card

See Figure 5 on page 18. To initialize and personalize a CA smart card, select Initialize and personalize CA smart card from the CA Smart Card menu item of the TKE SCUP main window.
You (in the role of Security Officer) will be prompted to insert the smart card to be used as the CA smart card into smart card reader 1. See Figure 6.

Insert an empty smart card into card reader 1. The gold symbol must be face up and must be inside the
card reader. Once you have inserted the smart card, press Ok and SCUP prompts you to select a 1024-bit or 2048-bit zone key. See Figure 7.

![Zone key length dialog](image.png)

**Figure 7 CA smart card zone key length dialog**

Select the radio button corresponding to the desired zone key length and press Ok.

SCUP will then validate smart card communication and will warn you if you are trying to initialize a smart card that is not empty. SCUP proceeds to initialize the card. See Figure 8.

Once the smart card is initialized, SCUP prompts you to enter a 6-digit PIN twice which will be used as the first CA PIN as shown in Figure 9. To enter the PIN twice, simply type it in and then type it in again. Do not press any other keys in between. For example, if the PIN is 123456, type 123456123456.

**Note:** There is a timeout of around 30 seconds for entering information on the card reader. If the reader times out before you complete the PIN entry, you must start over on the TKE SCUP main window.

![Smart card initialization](image.png)

**Figure 8 CA smart card initialization**

![CA smart card PIN entry message](image.png)

**Figure 9 CA smart card PIN entry message**

Smart card initialization with SCUP 19
The card reader's display will then change to indicate that input is required. See Figure 10.

![Figure 10 CA PIN entry](image)

**Figure 10 CA PIN entry**

Enter the first CA PIN on card reader 1, then re-enter it for confirmation. Do not press any other keys in between entering the PIN the first time and entering it the second time. For example, if the PIN is 123456, enter 123456123456.

At this point, SCUP will have card reader 1 issue a prompt for you to enter the second 6-digit CA PIN twice. See Figure 11.

![Figure 11 CA smart card second PIN message](image)

**Figure 11 CA smart card second PIN message**

Enter the second CA PIN on card reader 1, then re-enter it for confirmation.

Once the second CA PIN has been entered, the CA smart card can then be personalized by entering an optional zone description (Figure 12 on page 21) and an optional smart card description (Figure 13 on page 21).
After you input the optional zone description and the optional smart card description and press Ok on each dialog, a message will appear stating that the CA smart card is building. If you want to skip either description, simply press Ok. See Figure 14.

Once the smart card build successfully completes, the message shown in Figure 15 on page 22 will be displayed.
When you press Ok, the TKE SCUP main window will be displayed, and the details for the CA smart card will be visible. See Figure 16.
**Note:** If you cancel the smart card initialization process before the card is completely initialized, the smart card you are initializing is left in an unusable state and must be re-initialized to be made usable again. You may have to re-initialize the smart card as a different type of smart card to force the partially-initialized state to be erased. For example, if you cancel the initialization of a CA smart card in the middle, you may need to initialize that card as a TKE smart card before you can initialize it as a CA smart card again.

**Initialize and enroll a TKE smart card**

After the CA smart card has been initialized, the TKE smart card (which can contain the master key parts and crypto adapter logon keys) can be initialized and enrolled.

To initialize and enroll a TKE smart card, select *Initialize and enroll TKE smart card* from the *TKE Smart Card* menu item of the *TKE SCUP* main window. See Figure 17.

![Initialize and enroll TKE smart card window](image)

Figure 17 Initialize and enroll TKE smart card window

You will be prompted to insert the CA smart card into card reader 1. See Figure 18 on page 24.
Note: If a CA smart card is already in card reader 1, and if you previously entered the CA smart card PIN, you will not be prompted to go through the CA smart card verification process. Skip to Figure 22.

Figure 18 CA smart card insertion dialog

Press Ok to continue. You will be prompted to enter the first CA PIN (as created above) on the smart card reader PIN pad. See Figure 19.

Figure 19 CA smart card PIN 1 message

The PIN pad will then prompt for the PIN. See Figure 20.

Figure 20 CA PIN entry

Enter the first CA PIN. After the first PIN is entered, the second CA PIN is also required for dual authentication. The smart card reader PIN pad will prompt for the second PIN. See Figure 21 on page 25.
Enter the second PIN.

Figure 21 CA smart card PIN 2 message

At this point, the CA smart card has authenticated you so that the TKE smart card can now be initialized. SCUP will prompt you to insert the smart card to be initialized as the TKE smart card into card reader 2. See Figure 22. If the card is not empty, you will be warned and given the option to continue or stop.

Note: If you remove the CA smart card before you initialize the TKE smart card, you will be prompted for the CA smart card PIN before you are allowed to continue. If you leave the CA smart card in the reader, you will not be prompted for the CA smart card PIN.

Figure 22 TKE smart card insertion message

Once you insert the TKE smart card into reader 2 and press Ok, the smart card will be initialized, and a message will be displayed. See Figure 23 on page 26.
Once initialization successfully completes, the message shown in Figure 24 will be displayed.

At this point, the card is initialized and enrolled as a TKE smart card, and needs to be personalized with its own 6-digit PIN. When you press Ok, the TKE SCUP main window will be displayed, and the details for the TKE smart card will be visible. See Figure 25 on page 27.
Figure 25 TKE SCUP main window with TKE smart card details

**Note:** If you do not complete the smart card initialization process, the smart card you are initializing is left in an unusable state and must be re-initialized to be made usable again. You may have to re-initialize the smart card as a different type of smart card to force the partially-initialized state to be erased. For example, if you cancel the initialization of a TKE smart card in the middle, you may need to initialize that card as a CA smart card before you can initialize it as a TKE smart card again.

**Personalize a TKE smart card**

After the TKE smart card has been initialized and enrolled, it needs to be personalized. To personalize the TKE smart card, select *Personalize TKE smart card* from the *TKE SCUP* menu item of the *TKE SCUP* main window. See Figure 26 on page 28.
Figure 26 Personalize TKE smart card window

You will be prompted to ensure that the TKE smart card to be personalized is inserted in card reader 2. See Figure 27.

Figure 27 TKE smart card insertion message

Press Ok, and you will be prompted to enter the 6-digit PIN twice that is to be used with the TKE smart card. This is not the CA smart card PIN, but is a new PIN for the TKE smart card. See Figure 28 on page 29.

28 IBM 4765 Smart Card User Guide
Card reader 2 will then prompt twice for the PIN to be entered. See Figure 29.

Once you have entered the 6-digit PIN twice, you can then personalize the smart card with a description. See Figure 30.
After entering an optional description, press Ok. SCUP will personalize the TKE smart card and display a confirmation. See Figure 31.

Figure 31 TKE smart card success dialog

When you press Ok, the TKE SCUP main window will be displayed, and the details for the TKE smart card will be visible. See Figure 32.

Figure 32 TKE main window with smart card details
Enroll the crypto adapter in a zone

The crypto adapter must be enrolled in a zone. To do so, select Enroll Crypto Adapter from the Crypto Adapter menu item of the TKE SCUP main window. See Figure 33.

SCUP will prompt you to enroll the adapter as shown in Figure 34 on page 32.
Press *Ok*. You will be prompted to insert the CA smart card into smart card reader 1. See Figure 35.

After inserting the CA smart card into card reader 1, you will be prompted to enter the first CA PIN. See Figure 36.

Enter the first CA PIN on smart card reader 1. See Figure 37 on page 33.
You will then be prompted to enter the second CA PIN. See Figure 38.

The reader will display the PIN input as shown above. Enter the second CA PIN.

After the second CA PIN has been entered, SCUP will enroll the adapter. After the second CA PIN has been successfully entered, SCUP will enroll the adapter. See Figure 39.
CNM smart card functions

To start CNM with smart card support enabled, you must specify the /SC input parameter:

```bash
./csulcnm /SC
```

Alternatively, you can edit the cnm.ini file to enable smart card support. See Initialize CCA using CNM on page 12 for details.

**Note:** Java6 is required.

The following sections contain examples of smart card CNM functionality.

**Handling multiple adapters in CNM**

If your system has more than one IBM 4765 adapter installed, you must ensure that you are referring to the correct adapter when using both SCUP and CNM. On one hand, CLU refers to the first adapter in the system as adapter 0. On the other hand, the CCA environment variable specifying the default adapter for which to target commands refers to the first adapter as CRP01. The “first adapter” can change on system reboot; it merely indicates the first adapter that the host device driver finds upon reboot.

From the Crypto Node menu, select Select Adapter. Then choose adapter 1, 2, or 3, depending on which installed CCA adapter you want to be the default. Press Select using the buttons at the bottom of the window, and then press OK. These actions in CNM point to the desired adapter for the duration of the CNM session. Once you exit CNM, the default adapter designation is lost.

**Generate a crypto logon key**

In order to log on to the adapter using a CCA profile and a TKE smart card, a logon key of type RSA must be generated. The following steps outline the procedure to generate a logon key.

**Note:** To generate a crypto logon key and generate master key parts on smart cards, you must first enroll the adapter. See “Enroll the crypto adapter in a zone” on page 31 for details.

From the Smart Card menu item, select Generate Crypto Adapter Logon Key. See Figure 40 on page 35.
You will be prompted to insert a TKE smart card into card reader 2. See Figure 41.

Once the card has been inserted and you have pressed OK, you will be prompted to enter the PIN for the TKE card. See Figure 42.

Enter the PIN for the TKE card, at which time you will be prompted to enter a new user ID to associate with the key pair. This user ID is a new ID that you will use in the future as the associated profile for this smart card. See Figure 43 on page 36 for an example using user ID testkey.
Figure 43 Generate Logon Key user ID dialog

Note: User IDs must be unique and cannot be the same as other types of crypto profiles.

In this example, user ID testkey was entered. After entering the user ID, press OK and a logon key will be generated. CNM will then display a pop-up dialog indicating the logon key was successfully generated. See Figure 44.

Figure 44 Generate Logon Key success dialog

CCA profiles using smart cards for authentication data

Smart card enabled CNM has the ability to store CCA profile authentication data on a smart card in the form of a public/private RSA key pair generated as described in “Generate a crypto logon key” on page 34.

Note: Prior to setting up a CCA profile to use a smart card for authentication, make sure you set up a role that has full permissions and has the required ACPs enabled. For the following example, a role named SMRTCRD is used. The required ACPs are listed in Table 2 on page 13. See Chapter 5 of the CCA Support Program Installation Manual for instructions about setting up roles.

To set up a CCA profile that uses a smart card for its authentication data, perform the following steps. First, select Profiles from the Access Control menu. See Figure 45 on page 37.
CNM will then display the Profile Management window. See Figure 46.

Press New, using the buttons on the bottom of the window, and a pop-up dialog will be displayed. See Figure 47 on page 38.
Select the *Smart Card* radio button and press *Continue*. You will then be prompted to insert a TKE smart card into card reader 2. See Figure 48.

After you insert a TKE smart card and press *OK*, a panel will appear allowing you to set up a profile. See Figure 49.

You can then set up the standard fields associated with a profile. See Chapter 5 of the *CCA Support*.
Program Installation Manual for instructions about setting up roles and profiles using CNM.

**Note:** The User ID on this window is not editable because it is populated from the Crypto Logon Key Identifier you specified when you generated a crypto logon key.

Once the profile has been set up, press Load at the bottom of the window to load the profile, at which time a pop-up message will appear stating that the profile has been created successfully. See Figure 50.

![Profile Management](image)

**Figure 50** New profile success dialog

**CCA logon with a smart card profile**

The smart card profile created above can be used later to log a user into CCA with that profile. To log into CCA using a profile whose authentication data is stored on a smart card, select Smart Card Logon... from the File menu of CNM. See Figure 51.

![CCA Node Management Utility](image)

**Figure 51** CNM Smart Card Logon window

You will then be prompted to insert a TKE smart card into card reader 2 and press OK. See Figure 52 on page 40.
You will then be prompted for the TKE PIN. See Figure 53. Enter it on the PIN pad.

**Note:** There is a timeout of about 30 seconds for entering information on the card reader. If the reader times out before you complete the PIN entry, you must start over on the CCA main window.

Once you enter the TKE PIN, you will be logged on using the logon key and authentication data stored on the smart card.

**Smart card master key parts**

Smart card enabled CNM provides functionality to store master key parts securely on smart cards. The following discussion illustrates how to generate and store a master key part on a smart card.

**Note:** To generate a crypto logon key and generate master key parts on smart cards, you must first enroll the adapter. See “Enroll the crypto adapter in a zone” on page 31 for details.

From the DES/PKA Master Keys sub-menu of the Master Key menu, select Smart Card Parts. See Figure 54 on page 41.
You will then be prompted to insert a TKE smart card into card reader 2 and press **OK**. See Figure 55.

Once you insert the TKE smart card and press OK, the window shown in Figure 56 on page 42 will be displayed.
Figure 56 Master key parts window

For each master key part, select the appropriate radio button for the key part and then press Generate & Save at the bottom of the window to create and store the part of the DES/PKA master key. A dialog will ask for an optional description for each master key part. See Figure 57.

![Master Key Parts Window](image)

Figure 57 Master key parts description dialog

Enter a description for each key part and press OK. The dialog for entering a PIN on the second card reader will be displayed. Enter the TKE smart card PIN. CNM will generate and save the master key part on the smart card. If you want to load the key part, press the Load button.

**Note:** As is standard with CNM, the master key (MK) must be set separately after all of the MK parts have been generated and saved. Generate & save does not load the MK part into the MK registers. It just generates the MK part and saves it on the smart card. If you also want to load the MK part, do so by pressing Load at the bottom of the window. Select it via the description that was entered when it was generated and saved. This can be done at the time the MK part is generated and saved or when needed later.

**Note:** Any key parts that you generate and save can be deleted later if desired.

Once CNM completes generating the master key parts on the smart card, the master key parts will appear in the list of Master Key Parts On Smart Card as shown in Figure 58 on page 43.
Change TKE smart card PIN

To change the PIN of a TKE smart card using CNM, select Change PIN on the Smart Card menu. See Figure 59.

You will be prompted to enter a TKE smart card into card reader 2 and press OK as shown in Figure 60 on page 44.
After you press OK, you will be prompted to enter the current PIN on the smart card reader. See Figure 61.

The smart card reader then prompts you to enter the old PIN as shown in Figure 62.

Once you have entered the old PIN, CNM prompts for the new PIN to be entered twice. See Figure 63.

Enter the new PIN twice. Once you have entered the new PIN twice and CNM has verified that the PINs match, the PIN will be changed, and the dialog shown in Figure 64 on page 45 will be displayed.
View smart card details

Smart card enabled CNM allows you to display the basic details of what is present (and publicly available) on the card. To view this information, select Display Smart Card Details from the Smart Card menu. See Figure 65.

Enter a TKE smart card in card reader 2 and press OK. The window shown in Figure 66 on page 46 will be displayed.
Manage smart card contents

Smart card enabled CNM allows you to manage the contents of your TKE smart cards. Select Manage Smart Card Contents on the Smart Card menu. See Figure 67.

You can delete items from the card after providing the appropriate PIN(s). See Figure 68 on page 47.
Note: This example shows a test card. For security reasons, you would normally have only one master key part on each TKE smart card.

**Copy smart card**

Smart card enabled CNM allows you to copy a TKE smart card for backup or recovery purposes. Select *Copy Smart Card* on the *Smart Card* menu as shown in Figure 69.
You will be prompted to insert a source TKE smart card in card reader 1 and a target smart card in card reader 2. See Figure 70.

![Figure 70 Source TKE smart card dialogs](image)

A dialog similar to the one shown in Figure 71 will be displayed. The contents of the smart card may differ depending on the smart card you select to be copied. For example, if your smart card contains any master key parts, those will be displayed.

![Figure 71 Copy smart card dialog](image)

Once you press OK, CNM copies the contents of the TKE smart card in reader 1 to the TKE smart card in reader 2.
**Group logon**

Group profiles are useful for n of m authentication. For example, you may want to require that three of your five security officers be present for certain authentication activities.

You can create a group that contains smart card profiles. You can also create a group that contains smart card group profiles. To use group profiles, create one or more profiles. Then put them in a group.

To add a profile to a group, select *Profiles* from the *Access Control* menu of CNM. See Figure 72.

![Figure 72 CNM create profile window](image)

Press *New*. The window in Figure 73 will be displayed.

![Figure 73 CNM select profile type dialog](image)
Select Group and then press Continue. The window shown in Figure 74 will be displayed.

![Figure 74 Profile management window](image)

Fill in the entry fields for the group, including the group's user ID, and optional comment, the activation and expiration dates, and an appropriate role. Choose the available profiles and add them to the group. Once your changes are complete, press Load. The dialog shown in Figure 75 will be displayed.

![Figure 75 CNM profile success dialog](image)

Once you press OK, the window shown in Figure 76 on page 51 will be displayed.
Figure 76 CNM profile window

<table>
<thead>
<tr>
<th>Test</th>
<th>Testkey</th>
<th>Testgrp</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Smart card security

The addition of smart cards to a cryptographic environment brings additional security considerations into play. Special considerations should be taken to ensure the security of the smart cards. Consult your organization’s security policy for guidelines. Some examples of smart card security considerations include, but are not limited to:

- physical security of the smart cards, such as storing them in various locked cabinets,
- storing only one master key part on each smart card,
- assigning each smart card to a different individual,
- ensuring that an accurate inventory of smart cards is kept current, and
- other security practices that implement your organization’s security policy.

Consult with your security architect to ensure that you have the appropriate security guidelines in place. Please contact IBM if you have questions.
Error codes
This section contains a set of return/reason codes you may encounter when using SCUP-enabled CNM.

Table 3 CNM return/reason codes

<table>
<thead>
<tr>
<th>Return code in decimal</th>
<th>Reason code in decimal</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>2080</td>
<td>The group profile was not found.</td>
</tr>
<tr>
<td>8</td>
<td>2081</td>
<td>The group has duplicate elements.</td>
</tr>
<tr>
<td>8</td>
<td>2082</td>
<td>The group profile is not in the group.</td>
</tr>
<tr>
<td>8</td>
<td>2083</td>
<td>The group has the wrong user ID count.</td>
</tr>
<tr>
<td>8</td>
<td>2084</td>
<td>The group user ID failed.</td>
</tr>
<tr>
<td>8</td>
<td>2085</td>
<td>The profile is not in the specified group.</td>
</tr>
<tr>
<td>8</td>
<td>2086</td>
<td>The group role was not found.</td>
</tr>
<tr>
<td>8</td>
<td>2087</td>
<td>The group profile has not been activated.</td>
</tr>
<tr>
<td>8</td>
<td>2088</td>
<td>The expiration date of the group profile has been reached or exceeded.</td>
</tr>
<tr>
<td>8</td>
<td>2090</td>
<td>A required SRDI was not found.</td>
</tr>
<tr>
<td>8</td>
<td>2091</td>
<td>A required CA SRDI was not found.</td>
</tr>
</tbody>
</table>

For a complete list of CCA/CNM return and reason codes, see Appendix A of the *CCA Basic Services Reference and Guide for the IBM 4765*. 
Troubleshooting
This section contains various troubleshooting tips and techniques that may be useful when working with SCUP and CNM.

- When running SCUP or CNM, if Java reports that the class file has the wrong version, this is caused by using Java5 instead of Java6. Java6 is the required version of Java for SCUP. CNM and SCUP support only the 32-bit version of Java.

- When launching SCUP or CNM, if an error stating that smart card communications could not be initialized is encountered, this is sometimes caused by the smart card lock file. This file is used by SCUP/CNM to claim exclusive access to the smart card reader(s). After exiting SCUP/CNM, delete the /console/tke/common/smartCardLockFile file and try again.

- If you have previously installed a 64-bit version of PCSCD or any of the OMNIKEY files, ensure that CNM and SCUP are using the 32-bit versions of these files. Running CNM or SCUP in pure 64-bit mode is not supported.

- When launching SCUP, if an error appears stating that smart card functions will not be available or that the number of terminals available is less than the expected count, this could be caused by another smart card management service already running. If this is the case, ensure that the other service is stopped. You must kill the process and remove it from the autostart list to prevent it from starting on a later login.

  For example, to kill esc and remove it from autostart (as root):
  
  /usr/bin/esc stop
  /etc/init.d/escd stop
  rm /etc/xdg/autostart/esc.desktop

- When launching SCUP, if an error appears stating an unknown smart card exception has occurred, this could be caused by another smart card management service already running or by an incorrect installation of the various smart card packages and components. See the instructions above for killing and removing the smart card service for a possible solution.

- When launching CNM, if a smart card reader error appears (similar to: ScardConnect PC/SC Error, the smart card cannot be accessed because of other connections outstanding), this could be caused by another smart card management service already running. See the instructions above for killing and removing the smart card service for a possible solution.

- If the smart card readers do not indicate HID OMNIKEY 3821 on the reader screen after starting Linux, the PCSCD may need to be started. Start this via the pcscd command (usually requires sudo) or via /etc/init.d/pcscd restart. Another possible cause of this error is incorrect installation of the various smart card packages and components.

- If the pcscd command indicates that the restart option is not valid, ensure that you are invoking the pcscd in the /etc/init.d directory, not the one that is in the /sbin or /usr/sbin directories.

- If CNM or SCUP encounters an error stating that no smart card readers can be found, verify that the smart card readers are attached to the USB ports on the server, and verify that the displays of both readers indicate HID OMNIKEY 3821. If the readers just indicate that they are plugged in (there will be a graphic of a USB connector in this case) PCSCD needs to be started as described above.

- If you disconnect a smart card reader while SCUP is running, you must exit and restart SCUP.

- If you do not complete the smart card initialization process, the smart card you are initializing is
left in an unusable state and must be re-initialized to be made usable again. You may have to re-
initialize the smart card as a different type of smart card to force the partially-initialized state to be
erased. For example, if you cancel the initialization of a CA smart card in the middle, you may
need to initialize that card as a TKE smart card before you can initialize it as a CA smart card
again.

- If SCUP or CNM does not present dialogs to enter PINs for various functions, the SPEAPI JNI
layer is not in the LD_LIBRARY_PATH. Please verify all required libraries are present.
Specifically in this case the required libraries are libspeapejni.so and libspeapi.so.1.

- If no CCA profiles suitable for login are displayed when launching SCUP, verify that ACP X’8002’
is enabled in the active role, as well as the other TKE-specific ACPs. See Table 2 on page 13.

- If CNM encounters an error stating that the SUN COMM API for serial communication is not
installed or not in the classpath, this is caused by running CNM from /opt/IBM/4765/cnm but not
having the correct SCUP-enabled CNM files in that directory, so you are running an older version
of CNM that does not work with smart cards. Verify that the correct SCUP-enabled CNM files
have been copied to /opt/IBM/4765/cnm before running CNM.

- When entering PINs or any input through the smart card readers, a general timeout of around 30
seconds is imposed by SCUP and CNM.

- If you insert an invalid smart card or the wrong type of smart card for what you are trying to do, an
error dialog will be displayed. Insert the correct type of smart card and press Ok to continue.

- If SCUP’s list of available CCA profiles is empty, then you do not have any profiles that have a
role that has the required ACPs enabled. Follow the instructions in Chapter 5 of the CCA Support
Program Installation Manual to use CNM to enable ACPs in a role and define a user profile with
that role.

- If SCUP’s list of available CCA profiles does not contain a profile that you are sure is attached to
a role that has the correct ACPs enabled, make sure that the profile name contains only printable
characters. It is possible to create a profile or role in CCA that contains unprintable characters in
its name, but CNM and SCUP do not support profiles or roles with these characters in them.

- If you are having trouble communicating with the smart cards, the smart card daemon can be
started in debug mode that prints diagnostic messages. To do this, stop the daemon and then
start it again with the pcsd –d –f command. Note: This is the actual daemon binary file, not the
script that runs in the /etc/init.d directory. To ensure that you are using the 32-bit version of
PCSCD, you can run the file command against the PCSCD executable file and it will display
whether the binary is a 32-bit or 64-bit executable.

- If you cannot generate crypto logon keys or generate master key parts on smart cards, ensure
that you have enrolled the adapter in a zone. See “Enroll the crypto adapter in a zone” on page
31 for instructions.

- If users encounter a permissions or access denied error when launching SCUP or CNM, it is
likely that SCUP or CNM was run as root the first time it was launched. Running SCUP or CNM
as root the first time prevents other users from running them. To fix this condition, you must
manually change the permissions for all of the files in /opt/IBM/4765/console directory back to the
permissions they had when the installer originally installed them.

- If you have more than one IBM 4765 installed, set the CSU_DEFAULT_ADAPTER environment
variable to point to the correct adapter before using SCUP. See “Handling multiple adapters in
SCUP” on page 14 for details. Also, set the CNM default adapter each time you use CNM. See
“Handling multiple adapters in CNM” on page 34 for details.

- If SCUP or CNM encounters an error that is not explained by the other errors listed in this
document, ensure that you have only one instance of SCUP or CNM running. Only one instance
of SCUP or CNM can be running at any given time. Each of these programs must have exclusive use of the smart cards. Running more than one instance of SCUP, more than one instance of CNM, or one instance of SCUP and one instance of CNM at the same time will lead to errors.
Notices

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 Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY, 10594, USA.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Copying and distributing softcopy files

For online versions of this document, we authorize you to:

- Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.
- Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program’s license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine readable documentation.

Trademarks

The following terms are registered trademarks of the IBM Corporation in the United States and/or other countries or both:

IBM
System x

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

OMNIKEY and CardMan are registered trademarks of OMNIKEY AG.

Other company, product, and service names may be trademarks or service marks of others.
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACP</td>
<td>Access Control Point</td>
<td>PCSCD</td>
<td>PC/SC Smart Card Daemon</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>CCA</td>
<td>Common Cryptographic Architecture</td>
<td>PKA</td>
<td>Public Key Algorithm</td>
</tr>
<tr>
<td>CNM</td>
<td>Cryptographic Node Management utility</td>
<td>RNX</td>
<td>Random Number Extended</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
<td>RPM</td>
<td>RPM Package Manager</td>
</tr>
<tr>
<td>IBM</td>
<td>International Business Machines Corporation</td>
<td>SLES</td>
<td>SUSE Linux Enterprise Server</td>
</tr>
<tr>
<td>MK</td>
<td>Master Key</td>
<td>SCUP</td>
<td>Smart Card Utility Program</td>
</tr>
<tr>
<td>MK</td>
<td>Master Key</td>
<td>SRDI</td>
<td>Security Relevant Data Item</td>
</tr>
<tr>
<td>PCIe</td>
<td>Peripheral Component Interconnect Express</td>
<td>TKE</td>
<td>Trusted Key Entry</td>
</tr>
</tbody>
</table>
## Index

abbreviations .......................................................... 58  
access control points, enabling required ............................ 12  
building pcsc-lite .................................................... 7  
CCA profiles ........................................................... 36  
changing a TKE smart card PIN ..................................... 43  
CNM setup ............................................................... 1  
CNM smart card functions ............................................ 34  
CNM smart card support, enabling .................................. 13  
copying smart card contents ........................................... 47  
crypto adapter, enrolling in a zone .................................. 31  
enrolling a TKE smart card ............................................ 23  
enrolling the crypto adapter in a zone ............................... 31  
error codes ................................................................. 53  
functions, CNM smart card ............................................ 34  
generating a crypto logon key ......................................... 34  
group logon ............................................................... 49  
hardware and software, supported .................................... 2  
initializing a CA smart card .......................................... 17  
initializing a TKE smart card ........................................... 23  
installing CNM .......................................................... 12  
installing prerequisite packages ...................................... 4  
installing SLES packages ............................................. 4, 5  
launching SCUP ......................................................... 14  
managing smart card contents ....................................... 46  
master key parts ........................................................ 40  
multiple adapters, handling in CNM ................................. 34  
multiple adapters, handling in SCUP .................................. 14  
OMNIKEY device driver, downloading ............................. 8  
OMNIKEY device driver, installing ................................ 9  
overview ................................................................. 1  
personalizing a TKE smart card ...................................... 27  
prerequisite knowledge ............................................... vii  
related publications ................................................... vii  
SCUP setup .............................................................. 1  
smart card profile ..................................................... 39  
smart card security ..................................................... 52  
smart card, initializing with SCUP ................................... 14  
starting smart card service .......................................... 10  
TKE smart card, personalizing ...................................... 27  
viewing smart card details ............................................ 45  
notices ...................................................................... 57  
XE .......................................................................... 9