# Contents

About this document ..................................................................................................................... vi
Prerequisite knowledge .................................................................................................................. vi
Typographic conventions .............................................................................................................. vi
Related publications .................................................................................................................... vii
Summary of changes ...................................................................................................................... vii
Overview .................................................................................................................................... 1
Supported software ....................................................................................................................... 2
Using CCA Backup/Restore (BR) .................................................................................................. 3
- Install CCA BR ............................................................................................................................. 3
- Before using CCA BR .................................................................................................................... 3
- Launch CCA BR ............................................................................................................................ 3
- Adapter functions .......................................................................................................................... 4
  - Select an adapter ......................................................................................................................... 5
  - Obtain adapter status .................................................................................................................... 5
- Backup functions ........................................................................................................................... 6
  - Backup selected information ....................................................................................................... 7
  - Backup all information ............................................................................................................... 9
- Restore functions .......................................................................................................................... 10
Using the CCA test initialization utility ......................................................................................... 15
- Install CCA Init ............................................................................................................................. 15
- Launch CCA Init ........................................................................................................................... 15
- CCA Init results ............................................................................................................................ 16
Using the CCA HSM utility ............................................................................................................. 18
- Install CCA HSM .......................................................................................................................... 18
- Launch CCA HSM ........................................................................................................................ 18
- CCA HSM output .......................................................................................................................... 18
- CCA-related status and master key information ........................................................................... 18
- Coprocessor related information ................................................................................................. 19
- Diagnostic information ............................................................................................................... 19
- Date/time information ................................................................................................................... 20
- Function control vector information ............................................................................................ 20
- User profiles information ........................................................................................................... 21
- User role information.................................................................................................................... 21
Using the CSU Check Version utility ............................................................................................ 23
- Install CSU Check Version ............................................................................................................. 23
- Launch CSU Check Version .......................................................................................................... 23
- CSU Check Version output ......................................................................................................... 23
Using the CSU Snapshot script ...................................................................................................... 24
- Install CSU Snapshot ..................................................................................................................... 24
- Launch CSU Snapshot ................................................................................................................... 24
  - Description ................................................................................................................................. 24
  - Usage details ............................................................................................................................... 24
- CSU Snapshot output .................................................................................................................... 25
Troubleshooting ............................................................................................................................. 26
- CCA BR ....................................................................................................................................... 26
- CCA HSM .................................................................................................................................. 26
Notices .......................................................................................................................................... 28
- Copying and distributing softcopy files ....................................................................................... 28
- Trademarks ................................................................................................................................. 28
- List of abbreviations .................................................................................................................... 29
Index ............................................................................................................................................ 30
Tables
Table 1 Supported software......................................................................................................................... 2
Table 2 List of required ACPs..................................................................................................................... 11
About this document
This document contains information to help you use the IBM Common Cryptographic Architecture (CCA) and Coprocessor Services Utility (CSU) programs for the IBM 4767 PCIe Cryptographic Coprocessor. These utility programs include:
- CCA Backup/Restore
- CCA Test Initialization
- CCA HSM
- CSU Check Version
- CSU Snapshot

This manual should be used in conjunction with the manuals listed under “Related publications” in this section.

Prerequisite knowledge
The reader of this manual should understand how to use IBM 4767 CCA.

Typographic conventions
This manual uses the following typographic conventions:
- Commands entered 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 a vertical bar separating each choice. For example:
  command firstarg [secondarg] {a | b}
  A value for firstarg must be specified. A value for 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 4767 PCIe Cryptographic Coprocessor and CCA are available at:
The IBM 4767 PCI-e Cryptographic Coprocessor Installation Manual contains useful information about the 4767 adapter itself. The IBM CCA Basic Services Reference and Guide for the IBM 4767 and IBM 4765 PCIe Cryptographic Coprocessors and the IBM 4767 PCIe Cryptographic Coprocessor CCA Support Program Installation Manual contain useful information about using the CCA Node Management (CNM) utility and CCA.


**Summary of changes**

This edition of IBM 4767 PCIe Cryptographic Coprocessor CCA Utilities User Guide contains product information that is current with the IBM 4767 PCIe Cryptographic Coprocessor announcements.
Overview

CCA for the IBM 4767 for select x86 workstations includes support for smart card functionality. A set of CCA utilities, including backup and restore, initialization, HSM (crypto adapter) information, version check, and diagnostic snapshot, is available on the workstation release of CCA.

CCA Backup/Restore can be used to accomplish these tasks:

- Obtain diagnostic and status information about adapters that have CCA installed.
- Back up CCA user roles, user profiles, and key storage keys to a file on the server. Master keys are not backed up.
- Restore CCA user roles, user profiles, and key storage keys from a CCA backup file on the server.

Use the CCA Initialization utility to initialize CCA on the adapter for development and test.

The CCA HSM utility displays status and diagnostic information about CCA and the IBM 4767.

Use the CSU Check Version utility to obtain the version information for the host and card CCA binaries.

CSU Snapshot is a script that gathers information for service requests and field reports.

Each utility is described in the sections that follow.
## Supported software

Table 1 shows the software that is supported by the CCA utilities.

<table>
<thead>
<tr>
<th>Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit operating systems</td>
<td>Novell® SUSE® Linux® Enterprise Server 12, Service Pack 1 (SLES 12 SP 1)</td>
</tr>
<tr>
<td></td>
<td>Red Hat® Enterprise Linux 6.7 (RHEL 6.7)</td>
</tr>
<tr>
<td></td>
<td>Microsoft® Windows® Server 2012 R2</td>
</tr>
<tr>
<td>CCA</td>
<td>Release 5.3 (Windows), 5.2 (Linux)</td>
</tr>
<tr>
<td>Java</td>
<td>Java version 7</td>
</tr>
</tbody>
</table>
Using CCA Backup/Restore (BR)
This section contains an illustration of how to use CCA Backup/Restore (BR) to obtain CCA diagnostic information and to back up and restore CCA information.

Install CCA BR
CCA BR is installed as a part of CCA.

Before using CCA BR
Before launching CCA BR to back up or restore CCA information, the adapter must have a function control vector (FCV) loaded. The CCA Node Management (CNM) utility can be used to ensure that the FCV is loaded.

To launch CNM, navigate to the directory containing CNM and then run the program:

On Linux:
```
cd /opt/ibm/4767/cnm
./csulcnm
```

On Windows:
```
cd "C:\Program Files\IBM\4767\cnm"
csuncnm.bat
```

Select Authorization on the Crypto Node menu. Then select Load. Choose the correct FCV file as described in the CCA Support Program Installation Manual, and click OK. On the verification dialog, click Yes.

An FCV must be loaded before launching CCA BR to back up CCA information on the originating system, and an FCV must be loaded before launching CCA BR to restore CCA information on the receiving system.

Launch CCA BR
To launch CCA BR, run the following shell script:

On Linux:
```
/opt/ibm/4767/cnm/cca_backup_restore
```

On Windows:
```
"C:\Program Files\IBM\4767\cnm\cca_backup_restore.bat"
```

When launched, CCA BR displays its main window and prompts to select an adapter. Refer to Figure 1 on page 4 for an example of the window you will see. Your version information may be different.

Note: On Linux, CCA BR must be run as root. If you run CCA BR via sudo, be sure to use the -E option to preserve the current environment variables. On Windows, CCA BR must be run with administrator privileges. CCA BR requires Java 7.
Select the adapter and then click Select. The main window is displayed as in Figure 2.

On the CCA BR main window, you can perform adapter functions, backup functions, and restore functions.

**Adapter functions**

The Adapter menu allows you to select and work with IBM 4767 adapters that have CCA loaded. Refer to Figure 3 on page 5.
Select an adapter
To select an adapter to work with, click Select on the Adapter menu. The Select Adapter window is displayed (refer to on page 4). Select the desired adapter and click OK. The CCA BR main window is displayed again. You can obtain status, back up CCA information, and restore CCA information for the selected adapter.

Obtain adapter status
Click Status on the Adapter menu. The CCA BR Adapter Status window is displayed. This window displays diagnostic, CCA, and adapter information. The first set of information is the diagnostic information. You can use this information to monitor important adapter status, including low battery warnings. Refer to Figure 4.

![Figure 3 Adapter menu](image)

![Figure 4 Adapter Status window with diagnostics](image)

To see the CCA status window, select CCA Status Info. CCA information similar to that in Figure 5 on page 6 is displayed.
To see the adapter information window, select **Adapter Info**. Adapter information is displayed. Refer to Figure 6 for an example.

**Backup functions**

Before using CCA BR to back up CCA data, ensure that the FCV is loaded. To ensure whether the FCV is loaded, perform these steps:

1. Launch CNM. Select **Authorization** on the Crypto Node menu. Then select **Load**. Choose the correct FCV file and click **OK**. On the verification dialog, click **Yes**.

2. Exit CCA BR (if it is running) and restart it. It must be started after the FCV is loaded.
Refer to “Before using CCA BR” for information about loading the FCV before launching CCA BR in order to perform backup activities.

To back up CCA data, click either Selected or All on the Backup pull-down menu of the CCA BR main window. Clicking Selected backs up only the CCA data you selected, while All backs up all of the CCA data for the selected adapter. This includes all user roles, all user profiles, and all key storage files. Refer to Figure 7.

![Backup menu](image)

**Figure 7 Backup menu**

**Backup selected information**

If you chose Selected, the user role selection window is displayed. Refer to Figure 8.

![Select Role(s) to Backup window](image)

**Figure 8 Select Role(s) to Backup window**

Choose the user role(s) to back up, and then click Next. The profile selection window is displayed as shown in Figure 9 on page 8.
Choose the user profile(s) you want to back up, and then click **Next**. The key storage files selection window is displayed. Refer to Figure 10. On Windows, the default key storage location is in directory “C:\Program Files\IBM\4767\keys”.

Choose the Advanced Encryption Standard (AES), Private Key Access (PKA), and Data Encryption Standard (DES) key storage files you want to back up. You can use the **Browse…** function to find your key storage files. Once you have selected the key storage files, click **Next**.

**Note:** If you specify a non-existent key storage directory or file, the error shown in Figure 11 on page 9 will be displayed.

---

Figure 9 Select Profile(s) to Backup window

Choose the user profile(s) you want to back up, and then click **Next**. The key storage files selection window is displayed. Refer to Figure 10. On Windows, the default key storage location is in directory “C:\Program Files\IBM\4767\keys”.

Figure 10 Select Key Storage File(s) to Backup window

Choose the Advanced Encryption Standard (AES), Private Key Access (PKA), and Data Encryption Standard (DES) key storage files you want to back up. You can use the **Browse…** function to find your key storage files. Once you have selected the key storage files, click **Next**.

**Note:** If you specify a non-existent key storage directory or file, the error shown in Figure 11 on page 9 will be displayed.
Figure 11 Key storage file error

If there are no errors, Figure 12 will be displayed.

Figure 12 Backup Selected Entries (Primary System) window

Choose an appropriate location and file name for the CCA archive file and then click Save. The CCA archive will be created.

Note: You must enter a backup archive file name. The archive file will be stored in zip format. If the file name entered does not end with the .zip file extension, CCA BR will append .zip to the file name. The backup also creates a .md5sum file, which contains a hash of the .zip file. This file is provided so that the authenticity of a backup can be verified at restore time. To later guarantee the backup's authenticity, the two files must be kept separately and not be allowed to be handled by the same person. CCA BR assumes that the .zip and .md5sum files are in the same directory. If you browse for one file, it will try to fill in the other file name for you.

Backup all information

To backup all CCA information, click All on the Backup pull-down menu. The Backup All (Primary System) window is displayed. Refer to Figure 13 on page 10.
Choose an appropriate location and file name for the CCA backup archive file and then click Save. The CCA archive will be created and a success message similar to the one in Figure 14 will be displayed. On Windows, the file will be saved to a different directory.

**Figure 13 Backup All (Primary System) window**

![Backup All (Primary System) window](image)

**Figure 14 Backup success dialog**

![Backup success dialog](image)

**Restore functions**

Use the Restore menu to restore CCA data that was previously saved with CCA BR. This function is useful for loading a previously saved set of user roles, user profiles, and keys to a new adapter.

To restore a set of CCA data, the IBM 4767 adapter must be in an initialized state with the DEFAULT user role that has the required access control points (ACPs) enabled, and the FCV must be loaded. To get the adapter into this state, use CNM to initialize the adapter, check the DEFAULT role, and check the FCV. For additional information about using CNM, refer to Chapter 5 of the *CCA Support Program Installation Manual*.

In CNM, follow these steps:

1. Select Initialize… on the Crypto Node menu and then click Yes.

   **Warning:** Initializing the crypto node will completely wipe out the CCA data on the adapter, including the master keys, user roles, user profiles, and other security relevant data items (SRDIs). Make sure you really want to do this before using the Restore function.

2. Ensure that the DEFAULT user role has each required ACP enabled. Select Roles on the Access Control menu and then click the Edit button at the bottom of the screen. Ensure that the ACPs listed in Table 2 are listed under Permitted Operations.
Table 2 List of required ACPs

<table>
<thead>
<tr>
<th>Offset</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>X'0107'</td>
<td>One-Way Hash, SHA-1</td>
</tr>
<tr>
<td>X'0110'</td>
<td>Set Clock</td>
</tr>
<tr>
<td>X'0111'</td>
<td>Reinitialize Device</td>
</tr>
<tr>
<td>X'0112'</td>
<td>Initialize Access-Control System</td>
</tr>
<tr>
<td>X'0113'</td>
<td>Change User Profile Expiration Date</td>
</tr>
<tr>
<td>X'0114'</td>
<td>Change User Profile Authentication Data</td>
</tr>
<tr>
<td>X'0115'</td>
<td>Reset User Profile Logon-Attempt-Failure Count</td>
</tr>
<tr>
<td>X'0116'</td>
<td>Read Public Access-Control Information</td>
</tr>
<tr>
<td>X'0117'</td>
<td>Delete User Profile</td>
</tr>
<tr>
<td>X'0118'</td>
<td>Delete Role</td>
</tr>
<tr>
<td>X'0119'</td>
<td>Load Function-Control Vector</td>
</tr>
<tr>
<td>X'011A'</td>
<td>Clear Function-Control Vector</td>
</tr>
</tbody>
</table>

3. If any of these ACPs are not permitted, select it in the Restricted Operations list and click Permit to add it to the list of permitted operations.

4. Ensure that the FCV is loaded. Select Authorization on the Crypto Node menu. Then select Load. Choose the correct FCV file and click OK. On the verification dialog, click Yes.

5. Exit CCA BR (if it is running) and restart it. It must be started after the FCV is loaded in order to perform restore activities.

**Note:** Although your adapter must have an FCV loaded before you start the restore process, CCA BR will replace that FCV with the one that was saved in the archive file during the CCA BR backup procedure.

The restore operation checks for the presence of the following items on the target adapter and will not continue if any of the following are found:

- non-DEFAULT roles,
- User-created profiles, or
- RETAINed keys.

The presence of any of these items indicates the adapter has been previously configured and it is not safe to perform a full restore until these items are addressed. This is done primarily as a safeguard against accidentally overwriting important user configuration data.

Once the adapter is in the correct state, you can start the restore process in CCA BR. Select All on the CCA BR Restore menu, as shown in Figure 15.

**Figure 15 Restore menu**

The Restore window, shown in Figure 16 on page 12, is displayed.
Use the Browse… function to navigate to a valid CCA backup file, which should be named <backupfilename>.zip. Refer to Figure 17 for an example.

Once you locate and select the correct .zip file, click Open. The Restore window is filled in as shown in Figure 18 on page 13. Locate and select the matching .md5sum file and click Open.

Note: The .md5sum file contains the hash of the backup file and is used to authenticate the validity of the backup.
backup file. It should be stored and controlled separately from the .zip file. On Windows, the paths will be different.

![Backup system window with files selected](image1)

**Figure 18 Restore (Backup System) window with files selected**

Click *Restore* to finalize the data loading process. You will be prompted for the password for the user profile that was saved in the archive file. For example, if the saved profile was named *tester*, you will see a prompt like the one shown in **Figure 19**.

![Password prompt dialog](image2)

**Figure 19 Restore profile password prompt dialog**

You will then be prompted to confirm this password. Refer to **Figure 20**.

![Password confirmation dialog](image3)

**Figure 20 Restore profile password confirmation dialog**

**Note:** If you restore an archive that contains more than one user profile, CCA BR will prompt you to enter and confirm the password for each profile in the archive.
A success dialog will be displayed as shown in Figure 21 on page 14.

Figure 21 Restore success dialog
Using the CCA test initialization utility

The CCA Test Initialization utility returns CCA on an IBM 4767 to an initial state.

In this document, this utility is referred to as CCA Init. It is intended to be used for development and test purposes only, not for production.

Install CCA Init

CCA Init is installed as a part of CCA. Refer to the CCA Support Program Installation Manual for instructions about installing CCA.

Launch CCA Init

To launch CCA Init, navigate to the directory containing the utilities and then run the program:

On Linux:

```
cd /opt/ibm/4767/utils
./cca_test_init.e [-adapter <adapternum>] 
[-quiet]
[-overwrite_existing_data] 
[-help]
```

On Windows:

```
“cd C:\Program Files\IBM\4767\utils”
cca_test_init.exe [-adapter <adapternum>] 
[-quiet]
[-overwrite_existing_data] 
[-help]
```

Note: On Linux, CCA Init must be run as root. If you run CCA Init via sudo, use the -E option to preserve the current environment variables. Refer to Figure 22 for an example of a CCA Init invocation without any parameters.

```
/opt/IBM/4767/cnm> ./cca_test_init.e
Warning! Proceeding with initialization will erase all existing CCA data.
This includes all roles, profiles, retained keys, Master Keys, and key storage files.
Do you want to continue with initialization (y/n)?  
```

Figure 22 CCA Init warning

To proceed, type y at the prompt and then press Enter.

If more than one IBM 4767 is installed, use adapternum to specify which adapter you want to initialize, starting with 0 for the first adapter in the system. To determine which adapter is which, use the CLU status command:
On Linux:

```
/opt.ibm/4767/cla/csulclu -l <logfilename> -c ST -a <adapternum>
```

On Windows:

```
"C:\Program Files\IBM\4767\cla\csunclu.exe -l <logfilename> -c ST -a <adapternum>"
```

Specifying the –overwrite_existing_data option allows CCA Init to proceed without prompting you to confirm that you want all CCA data, including master keys and key storage files, to be deleted.

To see a list of the possible options, use the –help option.

**CCA Init results**

Use the CCA Init tool to automate the set of steps you would normally have to perform manually to set up CCA for development and test activities. CCA Init removes all existing CCA setup information and initializes CCA for development and test by performing the following tasks:

- Initialize the adapter in the standard CCA manner.
- Expand the DEFAULT user role to enable operations suitable for development.
- Create a user profile named `tester`, with a passphrase of `tester`, and attach the DEFAULT user role to that profile.
- Automatically set master keys for data encryption standard (DES) / public key algorithm (PKA) and for advanced encryption standard (AES).
- Load the function control vector (FCV).
- Initialize all three types of key storage: AES, DES, and PKA.

CCA Init writes its results to `stdout`. To retain this information to be viewed later, pipe the output to a file of your choice:

On Linux:

```
./cca_test_init.e > <somedirectory>/<outputfilename>
```

On Windows:

```
cca_test_init.exe > <somedirectory>/<outputfilename>
```

A sample set of results is shown in Figure 23 on page 17.
Figure 23 CCA Init results

------------ CCA Initialization Started -------------
Allocating Adapter: CRP01...
Adapter 1 allocated!
Working on adapter with serial number: DV48T308
Adapter initialization TOKEN step complete...
Adapter Initialized using TOKEN from step 1...
Adapter Initialization Complete!
DEFAULT Role set to MAXROLE!
tester profile created with password "taster"
DES/PKA First Master Key Part Processed...
DES/PKA Last Master Key Part Processed...
DES/PKA Master Key Set!
AES First Master Key Part Processed...
AES Last Master Key Part Processed...
AES Master Key Set!
APKA First Master Key Part Processed...
APKA Last Master Key Part Processed...
APKA Master Key Set!
Loading FCV...
FCV Loaded!
Initializing AES, DES, & PKA Storage...
AES, DES, & PKA Storage Initialized!
Deallocating Adapter: CRP01
Adapter 1 deallocated.
------------ CCA Initialization Complete -------------
Using the CCA HSM utility
The CCA HSM utility program lists various diagnostic and status information for the IBM 4767.

Install CCA HSM
CCA HSM is installed as a part of CCA. Refer to the CCA Support Program Installation Manual for instructions about installing CCA.

Launch CCA HSM
To launch CCA HSM, navigate to the directory containing the utilities and then run the program:

On Linux:

```
cd /opt/ibm/4767/utils
./cca_hsm_util.e –F <somedirectory>/<outputfilename>
```

On Windows:

```
cd “C:\Program Files\IBM\4767\utils”
cca_hsm_util.exe –F <somedirectory>\<outputfilename>
```

When it is launched, CCA HSM writes various status and diagnostic information about the IBM 4767 and CCA to the output file you specify.

CCA HSM output
CCA HSM contains these sets of information:

1. CCA-related status
2. AES master key information
3. coprocessor related
4. diagnostic
5. coprocessor date/time
6. function control vector
7. user profiles
8. user roles, including ACP data

Note: When viewing the output from CCA HSM, make sure the file viewer does not wrap lines. If your 4767 has a large number of user roles, user profiles, or both, the CCA HSM output can stretch across many columns.

The following sections describe the contents of the output produced by CCA HSM.

CCA-related status and master key information
CCA status information includes the MK register status as well as CCA version, date, and current user role. A sample set of CCA status is shown in Figure 24 on page 19. Your version information may differ.
**CCA HSM Utility. Version 0100. List Coprocessor Information.**

***CCA-Related Status Information***
- New Symmetric MK Register: Clear
- Current Symmetric MK Register: Complete
- Old Symmetric MK Register: Clear
- New Asymmetric MK Register: Clear
- Current Asymmetric MK Register: Complete
- Old Asymmetric MK Register: Clear
- CCA Application Version: 5.2.20
- CCA Application Build Date: 20160210
- User Role: DEFAULT

***AES Master Key Information***
- AES New MK Register: Clear
- AES Current MK Register: Complete
- AES Old MK Register: Clear
- AES Key Length Enablement: 256

---

**Figure 24 CCA-related status and master information**

**Coprocessor related information**
This information describes various hardware and version information for the IBM 4767. Refer to Figure 25 for an example. Your version information may differ.

***Coprocessor related Information***
- No of Installed Adapters: 1
- DES Hardware Level: 0
- RSA Hardware Level: 0
- POST Version: 010c0110
- Operating System Name: Linux
- Operating System Version: 2.6
- Part Number: 03LU051
- EC Level: N36880A
- MiniBoot Version: 01020102
- CPU Speed: 830
- Adapter ID: 8504344B18060888
- Flash Memory Size: 128
- DRAM Memory Size: 10066329
- Battery-Backed Memory Size: 4598
- Serial Number: DV487308

---

**Figure 25 Coprocessor information**

**Diagnostic information**
This information describes the current state of the possible warning and tamper conditions in the IBM
4767.

Note: Be sure to check the low-battery warning indicator on a regular basis. Check preferably weekly, but at least monthly. If this indicator is not Normal, use the battery replacement procedure to change the batteries as soon as feasible to prevent complete and unrecoverable loss of the IBM 4767 due to batteries that are too weak to maintain the adapter. Refer to the IBM 4767 PCI-e Cryptographic Coprocessor Installation Manual for instructions on replacing the batteries in the IBM 4767.

A sample of the diagnostic output is in Figure 26.

```
*** Diagnostic Information ***
Battery State          : Normal
Intrusion Latch State  : Not Set
Error Log Status       : Empty
Mesh Intrusion detected: No
Low Voltage Detected   : No
High Voltage Detected  : No
Temperature Range Exceeded: No
Radiation Detected    : No

*** Environment Identifier ***
EID                    : TestEID
```

Figure 26 Diagnostic information

Note: It is common to encounter a return/reason code of 8/1029 error in place of the EID name. Refer to the IBM CCA Basic Services Reference and Guide for more information about when an EID is required.

Date/time information

The current date and time of the IBM 4767 is displayed as shown in Figure 27.

```
*** Co-Processor Date/Time(GMT)***
Year/Month/Day hour:min:sec : 2016/02/25 16:39:13
Day in week{=sunday}       : 5
```

Figure 27 Date/time information

Function control vector information

CCA’s function control vector (FCV) data and master key share information are displayed as shown in Figure 28 on page 21.
Note: It is common to encounter a return/reason code of 8/1030 error instead of the master key share information. This indicates that CCA is not being set up to share or clone DES or PKA master keys. Refer to the IBM CCA Basic Services Reference and Guide for more information about cloning master keys.

**User profiles information**

Information about the current CCA user profiles for the IBM 4767 is displayed as shown in Figure 29.

```
*** List IBM 4767 Profiles ***

tester

>>>Profile name : tester
Major/Minor Version: 1/0
Comment :
Role : DEFAULT
Logon Failure Count: 0
Pad : 0
Valid from : 2015:01:01 until 2020:01:01
Mech. Strength/ID : 0000 - 0001 - Type: Passphrase.
Expire date : 2020:01:01
```

Figure 29 Profiles information

**User role information**

Details about each user role defined in the IBM 4767, including the enabled ACPs and a listing of each ACP, is displayed. Refer to Figure 30 on page 22 for a sample listing of the first part of the results. Some details of the access control list and individual ACPs are not shown here due to the length of the output.
### Figure 30 User role information

<table>
<thead>
<tr>
<th>Bit</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0107</td>
<td>ON</td>
<td>0107 One-Way Hash, SHA-1</td>
</tr>
<tr>
<td>0110</td>
<td>ON</td>
<td>0110 Set Clock</td>
</tr>
<tr>
<td>0111</td>
<td>ON</td>
<td>0111 Reinitialize Device</td>
</tr>
<tr>
<td>0112</td>
<td>ON</td>
<td>0112 Initialize Access-Control System</td>
</tr>
<tr>
<td>0113</td>
<td>ON</td>
<td>0113 Change User Profile Expiration Date</td>
</tr>
<tr>
<td>0114</td>
<td>ON</td>
<td>0114 Change User Profile Authentication Data</td>
</tr>
<tr>
<td>0115</td>
<td>ON</td>
<td>0115 Reset User Profile Logon-Attempt-Failure Count</td>
</tr>
<tr>
<td>0116</td>
<td>ON</td>
<td>0116 Read Public Access-Control Information</td>
</tr>
<tr>
<td>0117</td>
<td>ON</td>
<td>0117 Delete User Profile</td>
</tr>
<tr>
<td>0118</td>
<td>ON</td>
<td>0118 Delete Role</td>
</tr>
<tr>
<td>0119</td>
<td>ON</td>
<td>0119 Load Function-Control Vector</td>
</tr>
<tr>
<td>011A</td>
<td>ON</td>
<td>011A Clear Function-Control Vector</td>
</tr>
</tbody>
</table>
Using the CSU Check Version utility

The CSU Check Version utility program lists the currently installed version of both the host-side and card-side CCA binary files. This list can either be displayed in the windows in which it is run or can be piped to an output file for your convenience.

Install CSU Check Version

CSU Check Version is installed as a part of CCA. Refer to the CCA Support Program Installation Manual for instructions about installing CCA.

Launch CSU Check Version

To launch CSU Check Version, navigate to the directory containing the utilities and then run the program:

On Linux:

```bash
    cd /opt/ibm/4767/utils
    ./csuchkversion
```  

On Windows:

```bash
    cd "C:\Program Files\IBM\4767\utils"
    csuchkversion.exe
```

When it is launched, CSU Check Version writes the CCA version information to stdout.

CSU Check Version output

Figure 31 depicts a sample set of output produced by CSU Check Version. Your version information may differ depending on which CCA release you have chosen to load.

```
csuchkversion: CCA Code Level Verification
CCA Lib Version, Date:
  5.2.22  20160303
CCA Card Version, Date, Serial Number:
  5.2.22  20160303  DV5CX338
```

Figure 31: CSU Check Version output
Using the CSU Snapshot script
The CSU Snapshot script gathers various diagnostic and status information for the IBM 4767.

Install CSU Snapshot
CSU Snapshot is installed as a part of CCA. Refer to the CCA Support Program Installation Manual for instructions about installing CCA.

Launch CSU Snapshot
To launch CSU Snapshot, navigate to the directory containing the utilities and then run the script as root:

```
CSU Snapshot is available only on Linux:
cd /opt/ibm/4767/utils
./csu_snap (see the argument list below)
```

Description

csu_snap is a command line shell script that retrieves the necessary information on the customer's machine to diagnose CCA installation issues. When instructed to do so by Crypto Support, the customer should follow the steps below to aid Crypto Support in diagnosing CCA installation issues:

1. Log in as root.
2. Invoke the script.

   Note: For customers with multiple adapters in the machine where the script is invoked, invoke the script as many times as the number of adapters in the system, changing the -a parameter each time. For customers with only one adapter, invoke the script with parameter "-a 0". For n adapters, invoke the script n times with "-a X" such that 0 <= X <= n-1.

3. Retrieve the .tar.gz file(s) to send to Crypto Support. They will have the form:

   `/tmp/csu_snap_out/snaps/[machine].[X].[date].csu_snap.snap.tar.gz`

   where:
   
   X is the adapter number (0-based)
   date is the date and time of the invocation, in yymmddHHMMSS format

   There will be a unique .tar.gz file for each invocation of the script. For a system with multiple cards, and therefore multiple csu_snap invocations, there will be multiple .tar.gz files that need to be sent to Crypto Support.

4. [Optional] Save the .tar.gz file(s) elsewhere and delete /tmp/csu_snap_out.
5. Review all of the .tar.gz files(s) to ensure they do not contain any information you do not want to send to IBM. Then, send the .tar.gz files(s) to Crypto Support at crypto@us.ibm.com.

Usage details
The csu_snap script options are described below.

csu_snap [-a adapter_number] [-r] [-n] [-v] [-h]

-r will call clu ST
The recommended invocation is:

```
   csu_snap -a 0 -r -n
```

When it is launched, CSU Snapshot writes various status and diagnostic information to the file listed after the script is invoked.

**CSU Snapshot output**

Figure 32 depicts a sample set of output produced by CSU Snapshot:

```
cd /opt/ibm/4767/utils
./csu_snap

csu_snap SUCCESSFUL. Diagnostic data is located at:
/tmp/csu_snap_out/snaps/server.0.160406143825.csu_snap.tar.gz
```

**Figure 32: CSU Snapshot output**
Troubleshooting

CCA BR

This section contains various troubleshooting tips and techniques that may be useful when working with CCA BR.

- When backing up CCA information to an archive, if you encounter an error that indicates all key storage files must be specified, it means either you specified a directory or a key storage file that does not exist. You can use the Browse… button to locate key storage files. The default installation directory is /opt.ibm/4767/keys on Linux, and “C:\Program Files\IBM\4767\keys” on Windows.

- When restoring CCA from an archive, if you encounter an error that indicates the selected adapter contains non-default user roles, user profiles, or keys, it means that your adapter is not in a “clean” initial state that can receive a restored set of CCA information. To wipe out your existing user roles, user profiles, and keys, use CNM to initialize the adapter and to enable the required ACPs to the DEFAULT CCA role. Refer to “Restore functions” on page 10 for detailed instructions. Once these steps are complete, use CCA BR to restore the archived CCA information to the initialized adapter.

- When restoring CCA from an archive, if you encounter an error that indicates the ACPs are not found, it means that your DEFAULT user role does not have the required ACPs enabled to perform the restore action. To enable the required ACPs, use CNM to edit the DEFAULT role. Refer to “Restore functions” on page 10 for details about editing the DEFAULT role to enable the required ACPs.

- When restoring CCA from an archive, if you encounter an error that indicates a key storage file is not writable, it means that the host system user ID being used does not have the necessary authority to update the key storage files. Either switch user IDs or obtain write authority to the key storage directories, and retry the restore operation.

- When restoring CCA from an archive, you must be able to enter every password for all user profiles that were backed up to that archive.

- If the list of available CCA user profiles does not contain a user profile known to be attached to a user role that has the correct ACPs enabled, make sure that the profile name contains only printable characters. Even though CCA allows the creation of user profiles and user role names that contain unprintable characters, the CCA utilities do not support profiles or roles with any unprintable characters in their names.

- Before launching CCA BR to back up or restore CCA information, you must have an FCV loaded. Refer to “Before using CCA BR” on page 3 for instructions or refer to Chapter 5 of the CCA Support Program Installation Manual for additional information.

- If permissions issues are encountered, use CNM to ensure that ACP X’001D’ and X’0230’ are enabled in the DEFAULT user role. Exit and re-launch CCA BR.

CCA HSM

Errors and warnings in the output displayed by CCA HSM can provide information about the health of the IBM 4767 and CCA. Some possible warnings are:

- It is common to encounter a return/reason code of 8/1029 error, which refers to the Environment ID. It is typical for the EID to not be set. Refer to the IBM CCA Basic Services Reference and Guide for more information.
It is common to encounter a return/reason code of 8/1030 error, which refers to CCA not being set up to share or clone the DES and PKA master keys. This is typical. Refer to the *IBM CCA Basic Services Reference and Guide* for more information.
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

IBM is a registered trademark of the IBM Corporation in the United States, other countries, or both.

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

Windows is a registered trademark of Microsoft Corporation in the United States, other countries, or both.

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

28 IBM 4767 CCA Utilities User Guide
### List of abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACP</td>
<td>Access Control Point</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>CCA</td>
<td>Common Cryptographic Architecture</td>
</tr>
<tr>
<td>CCA BR</td>
<td>CCA Backup/Restore</td>
</tr>
<tr>
<td>CCA HSM</td>
<td>CCA Hardware Security Module</td>
</tr>
<tr>
<td>CCA Init</td>
<td>CCA initialization utility</td>
</tr>
<tr>
<td>CNM</td>
<td>Cryptographic Node Management</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>FCV</td>
<td>Function Control Vector</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>IBM</td>
<td>International Business Machines</td>
</tr>
<tr>
<td>MK</td>
<td>Master Key</td>
</tr>
<tr>
<td>PCIe</td>
<td>Peripheral Component Interconnect Express</td>
</tr>
<tr>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>PKA</td>
<td>Public Key Architecture</td>
</tr>
<tr>
<td>RHEL</td>
<td>Red Hat Enterprise Linux</td>
</tr>
<tr>
<td>SLES</td>
<td>SUSE Linux Enterprise Server</td>
</tr>
</tbody>
</table>
# Index

adapter functions ........................................... 4  
adapter, electing ........................................... 5  
backing up CCA data ........................................ 6  
backup ...................................................... 3  
before using .................................................. 3  
  CCA BR .................................................. 3  
CCA backup ................................................ 3  
CCA BR troubleshooting .................................. 26  
CCA HSM ................................................... 18  
CCA HSM coprocessor status ......................... 19  
CCA HSM date/time ..................................... 20  
CCA HSM diagnostics ................................... 19  
CCA HSM diagnostics ................................... 19  
CCA HSM FCV data ...................................... 20  
CCA HSM profiles ....................................... 21  
CCA HSM roles ........................................... 21  
CCA HSM troubleshooting .............................. 26  
CCA restore ............................................... 3  
CCA status ............................................... 18  
CSU Check Version ..................................... 23  
CSU Snapshot ........................................... 24  
hardware and software, supported .................. 2  
installing ................................................... 3  
  CCA BR .................................................. 3  
CCA HSM ................................................... 18  
CCA Init .................................................. 15  
CSU Check Version ..................................... 23  
CSU Snapshot ........................................... 24  
launching .................................................... 3  
  CCA BR .................................................. 3  
CCA HSM ................................................... 18  
CCA Init .................................................. 15  
CSU Check Version ..................................... 23  
CSU Snapshot ........................................... 24  
master key data ........................................... 18  
obtaining status .......................................... 5  
output ..................................................... 1  
  CCA HSM ................................................... 18  
CCA Init .................................................. 16  
 prerequisites knowledge ................................. vi  
related publications ..................................... vi  
results ..................................................... 25  
  CCA Init .................................................. 16  
notices ..................................................... 28