IBM SecureWay Cryptographic Products
IBM 4758 PCI Cryptographic Coprocessor
Custom Software Installation Manual
Draft Level

June 15, 1998

Security Solutions and Technology Department

IBM Corporation
8501 IBM Drive
Charlotte, North Carolina 28262-8563

Draft Level - 15-JUN-98, 11:30

Note!

Before using this information and the products it supports, be sure to read the general information under Appendix A, “Notices” on page A-1.

Draft Level

Development Information

This printout includes Development information that is not included in customer documentation.

End of Development Information

This manual is maintained by George Dolan and Jonathan Edwards.

NOTICE

This DRAFT version of the manual is provided for your product evaluation and planning purposes in advance of general availability of the IBM 4758 product that implements the functions described in this manual. The implementation described herein may change between availability of this preliminary manual and the final product. Only final product information should be used when programming for the device.

Note: This preliminary publication cannot be ordered through the usual channels; contact George Dolan (gmdolan@us.ibm.com) for additional information.

Table of Contents

About This Book

The *IBM 4758 PCI Cryptographic Coprocessor Custom Software Installation Manual* describes how to load software into the cryptographic coprocessor. It also explains how to load software on the host in which the coprocessor has been installed that allows applications running on the host to interact with the coprocessor.

The audience for this manual includes anyone who needs to configure a host in which a cryptographic coprocessor has been installed to allow applications on the host to use the cryptographic coprocessor and anyone who needs to load software into the cryptographic coprocessor itself.

Prerequisite Knowledge

The reader of this book should understand how to perform basic tasks (including editing, system configuration, and file system navigation) on the host machine in which the coprocessor has been installed. Familiarity with the coprocessor hardware and pre-installed software (as described in the *IBM 4758 PCI Cryptographic Coprocessor Technical Overview for Original Equipment Manufacturers*) may also be helpful.

Organization of This Book

This book is organized as follows:

Chapter 1, “Introduction” describes the various pieces of software that are needed to make use of a cryptographic coprocessor.

Chapter 2, “Host Software Installation” describes how to install the host-side device drivers for the PCI Cryptographic Coprocessor.

Chapter 3, “How to Load Software into the Cryptographic Coprocessor” describes how to load application software or operating system software (either supplied by IBM, supplied by a third party, or written by the reader) into the IBM 4758 PCI Cryptographic Coprocessor.

Appendix A, “Notices” includes product and publication notices.

A list of abbreviations, a glossary, and an index complete the manual.

Typographic Conventions

This publication uses the following typographic conventions:

- Commands that you enter verbatim onto the command line are presented in **bold** type.
- Variable information and parameters, such as file names, are presented in *italic* 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.
- System responses in a non-GUI environment are presented in `monospace` type.
- Web addresses and directory paths are presented in *italic* type.

Related Publications

Many of the publications listed below under “General Interest,” “CCA Support Program Publications,” and “Custom Software Publications” are available in Adobe Acrobat** portable document format (PDF) at *http://www.ibm.com/security/cryptocards*.

General Interest

The following publications may be of interest to anyone who needs to install, use, or write applications for a PCI Cryptographic Coprocessor:

- *IBM 4758 PCI Cryptographic Coprocessor General Information Manual*, GC31-8608 (version -01 or later)
- *IBM 4758 PCI Cryptographic Coprocessor Technical Overview for Original Equipment Manufacturers*
- *IBM 4758 PCI Cryptographic Coprocessor Installation Manual*, SC31-8623

CCA Support Program Publications

The following publications may be of interest to readers who intend to use a PCI Cryptographic Coprocessor to run IBM’s Common Cryptographic Architecture (CCA) Support Program:

- *IBM 4758 PCI Cryptographic Coprocessor CCA Support Program*, SC31-8610
- *IBM 4758 CCA Basic Services Reference and Guide*, SC31-8609

Custom Software Publications

The following publications may be of interest to persons who intend to write applications or operating systems that will run on a PCI Cryptographic Coprocessor:

- *IBM 4758 PCI Cryptographic Coprocessor CP/Q Operating System Overview*
- *IBM 4758 PCI Cryptographic Coprocessor Custom Software Interface Reference*
- *IBM 4758 PCI Cryptographic Coprocessor CP/Q Operating System Application Programming Reference*
- *IBM 4758 PCI Cryptographic Coprocessor CP/Q Operating System C Runtime Library Reference*
- *IBM 4758 PCI Cryptographic Coprocessor Custom Software Developer’s Toolkit Guide*
- *IBM 4758 PCI Cryptographic Coprocessor CCA User Defined Extensions Programming Reference*

- *IBM 4758 PCI Cryptographic Coprocessor Interactive Code Analysis Tool (ICAT) User's Guide*
- *AMCC S5933 PCI Controller Data Book*, available from Applied Micro Circuits Corporation, 6290 Sequence Drive, San Diego, CA 92121-4358. Phone 1-800-755-2622 or 1-619-450-9333. The manual is available online as an Adobe Acrobat** PDF file at *http://www.amcc.com/pdfs/5933db.pdf*.

Cryptography Publications

The following publications describe cryptographic standards, research, and practices applicable to the PCI Cryptographic Coprocessor:

- "Building a High-Performance, Programmable Secure Coprocessor," S.W. Smith and S.H. Weingart, Research Report RC21102, IBM T.J. Watson Research Center, February 1998.
- "Using a High-Performance, Programmable Secure Coprocessor, S.W. Smith, E.R. Palmer, and S.H. Weingart, in *FC98: Proceedings of the Second International Conference on Financial Cryptography*, Anguilla, February 1998. To appear, Springer-Verlag LNCS. 1998.
- "Secure Coprocessing Research and Application Issues," S.W. Smith, Los Alamos Unclassified Release LA-UR-96-2805, Los Alamos National Laboratory, August 1996.
- "Secure Coprocessing in Electronic Commerce Applications," B.S. Yee and J.D. Tygar, in *Proceedings of the First USENIX Workshop on Electronic Commerce*, New York, July 1995.
- "Transaction Security Systems," D.G. Abraham, G.M. Dolan, G.P. Double, and J.V. Stevens, in *IBM Systems Journal* Vol. 30 No. 2, 1991, G321-0103.
- "Trusting Trusted Hardware: Towards a Formal Model for Programmable Secure Coprocessors," S.W. Smith and V. Austel, in *Proceedings of the Third USENIX Workshop on Electronic Commerce*," Boston, August 1998.
- "Using Secure Coprocessors," B.S. Yee (Ph.D. thesis), Computer Science Technical Report CMU-CS-94-149, Carnegie-Mellon University, May 1994.
- *IBM Systems Journal* Vol. 32 No. 3, 1993, G321-5521
- *IBM Journal of Research and Development* Vol. 38 No. 2, 1994, G322-0191
- *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition*, Bruce Schneier, John Wiley & Sons, Inc. ISBN 0-471-12845-7 or ISBN 0-471-11709-9
- *ANSI X9.31 Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry*
- *Internet Engineering Taskforce RFC 1321*, April 1992, MD5
- *ISO 9796 Digital Signal Standard*
- *Secure Electronic Transaction Protocol Version 1.0*, May 31, 1997
- *USA Federal Information Processing Standard (FIPS):*
  - *Data Encryption Standard,* 46-1-1988
  - *Secure Hash Algorithm,* 180-1, May 31, 1994
  - *Cryptographic Module Security,* 140-1

- *Derived Test Requirements for FIPS PUB 140-1*, W. Havener, R. Medlock, L. Mitchell, and R. Walcott. MITRE Corporation, March 1995.

IBM Research Reports can be obtained from:

IBM T.J. Watson Research Center
Publications Office, 16-220
P.O. Box 218
Yorktown Heights, NY 10598

Back issues of the *IBM Systems Journal* and the *IBM Journal of Research and Development* may be ordered by calling (914) 945-3836.

Summary of Changes

This first edition of the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Developer's Toolkit Guide* contains product information that is current with the IBM 4758 PCI Cryptographic Coprocessor announcements made in May, 1998.

Chapter 1. Introduction

The IBM 4758 PCI Cryptographic Coprocessor runs customized applications in a tamper-resistant environment to provide services to applications on the host in which the coprocessor is installed. Applications on the host communicate with applications on the cryptographic coprocessor by way of a device driver, which must be installed on the host before any communication can take place.

Memory on the cryptographic coprocessor is divided into four segments, numbered zero through three. Segment zero is ROM and the remaining segments are flash EPROM. Segments zero and one contain power-on self-test routines and system microcode. Segment two contains the coprocessor operating system. Segment three contains any application code. A coprocessor may be shipped with the necessary software already installed, or software may be shipped separately for installation by the end user.

The remainder of this book describes how to install the host device driver that permits applications on the host to communicate with the coprocessor and how to load images containing the coprocessor operating system and coprocessor applications into the coprocessor. The instructions on loading software into the coprocessor are of necessity rather generic. If the reader has an application with its own instructions those instructions should be followed.

Chapter 2. Host Software Installation

Follow the procedures in this chapter to install the host-side device drivers for the coprocessor.

This chapter:

- List the software components installed by the procedures in this chapter.
- Lists the system requirements for installation.
- Describes how to install the software.
- Lists the default directories created by the Advanced Interactive Executive (AIX*) install process.
- Describes how to uninstall the coprocessor device drivers.

Software Components

The procedures in this chapter install and remove the following software components:

- The IBM 4758 PCI Cryptographic Coprocessor device driver
- On AIX systems, the coprocessor configuration methods
- The coprocessor shared library (AIX) or dynamic link library—Operating System/2* (OS/2*) and Windows** New Technology (NT**)

AIX

This section includes a description of the system requirements and procedures necessary to install and uninstall the software on an AIX operating system.

Important: The installation process requires root-level authority; it must be performed by a system administrator with that authority.

Requirements

Before you install the software, determine its directory location and make sure your system meets the following requirements:

Hardware

An RS/6000* computer with an IBM 4758 PCI Cryptographic Coprocessor installed. During system restart, the device driver interacts with the coprocessor to arbitrate interrupt settings, direct memory access (DMA) channels, and other system resources. For installation instructions regarding the coprocessor hardware, refer to the *IBM 4758 PCI Cryptographic Coprocessor Installation Manual*, SC31-8623.

Software

AIX version 4.1.0, or later.

Disk Space

One megabyte (MB) in the */usr* file system.

How to Install the Software

To install the software:

1. Insert the software medium into the appropriate drive.
2. Enter **smit** on the command line to start the System Management Interface Tool (SMIT); the System Management menu is displayed.
3. Select **Software Installation and Maintenance**; the Software Installation and Maintenance menu is displayed.
4. Select **Install and Update Software**; the Install and Update Software menu is displayed.
5. Select **Install/Update Selectable Software (Custom Install)**; the Install/Update Selectable Software (Custom Install) menu is displayed.
6. Select **Install Additional Device**; a popup dialog box is displayed.
7. Enter the name of the installation input device (tape, floppy, CD-ROM), or the network directory location of the software into the **INPUT device / directory for software** field.
8. Select **OK**; an installation panel is displayed.
9. Select the **List** button next to the **SOFTWARE to install** field; a software list panel is displayed.
10. Select **1.0.0.3 devices.pci.141009f00**.
11. Select **OK**.
12. Select **OK** again to accept the default settings and install the software; when the installation is complete, a confirmation panel is displayed.

    Note: For a listing of the directories created by the installation, see “Default Directories” on page 2-3.
13. Select **Done** to close the SMIT utility.
14. Enter the **cfgmgr** command to bring the coprocessor into the “Available” state.

    Note: It may take as long as 10 minutes to run **cfgmgr**. During that time, no status is reported to the user; this is not a system error.
15. Enter the following command to verify that the coprocessor has been properly installed:

    lsdev –Cc adapter¦ grep crypt

    The system returns a message similar to the following:

    ```
    crypt0 Available 04-01 4758 PCI cryptographic coprocessor
    ```

The software installation process is now complete.

Default Directories

The installation process creates the following directories:

Driver	*/usr/lib/drives/cryptdd*
Include files	*/usr/include/scc*
Support files	*/usr/lpp/devices.pci.14109f00*

How to Remove the Software

To remove the software:

1. Log in as the root user.
2. Enter the command **rmdev –dl crypt0**; the coprocessor device driver and related information are removed.
3. Enter the command **installp –u devices.pci.14109f00.rte**; the remaining software is removed.

OS/2

This section includes a description of the system requirements and procedures necessary to install and uninstall the software on OS/2.

Requirements

Before you install the software, determine its directory location and make sure your system meets the following requirements:

Hardware

An IBM-compatible PC with an IBM 4758 PCI Cryptographic Coprocessor installed. During system restart, the device driver interacts with the coprocessor to arbitrate interrupt settings, DMA channels, and other system resources. For installation instructions regarding the coprocessor hardware, refer to the *IBM 4758 PCI Cryptographic Coprocessor Installation Manual*, SC31-8623.

Software

OS/2 version 3.0, or later.

Disk Space

75 kilobytes (KBs)

How to Install the Software

To install the software:

1. Create a new directory on the host computer. For example, **c:\scc**.
2. Copy the following files into the directory.

   crypto.sys (coprocessor device driver)
   crypto.dll (dynamic link library)

3. Open the *config.sys* file.
4. At the end of the line that begins with “LIBPATH=”, add the full path of the directory you created in step 1. For example:

LIBPATH= *other commands* **;c:\scc**

5. At the end of the file, add a command to load the device driver at boot time. For example:
   DEVICE=c:\scc\crypto.sys

   Note: You can add the **/q** "quiet" parameter to the end of the command to suppress the signon message that is generated when the driver loads.
6. Save *config.sys* and restart the host computer; the installation process is complete.

How to Remove the Software

To remove the software:

1. Delete the following host computer files:

   crypto.sys (coprocessor device driver)
   crypto.dll (dynamic link library)
2. Open the *config.sys* file.
3. Remove the full path of the directory that you added on the LIBPATH in step 4 of "How to Install the Software" on page 2-3.
4. Remove the command to load the device driver at boot time. For example:
   DEVICE=c:\scc\crypto.sys
5. Save *config.sys*; the software removal process is complete.

Windows NT

This section includes a description of the system requirements and procedures necessary to install and uninstall the software on a Windows NT operating system.

Important: The installation process modifies the system registry; it must be performed by a user with administrator privilege.

Requirements

Before you install the software, determine its directory location and make sure your system meets the following requirements:

Hardware

An IBM-compatible PC with an IBM 4758 PCI Cryptographic Coprocessor installed. During system restart, the device driver interacts with the coprocessor to arbitrate interrupt settings, DMA channels, and other system resources. For installation instructions regarding the coprocessor hardware, refer to the *IBM 4758 PCI Cryptographic Coprocessor Installation Manual*, SC31-8623.

Software

Windows NT version 4.0, or later.

Disk Space

75 KBs

How to Install the Software

To install the software:

1. Copy *cryptont.dll* (the dynamic link library) into the *c:\WINNT\SYSTEM32* directory.
2. Copy *cryptont.sys* (the device driver) into the *c:\WINNT\SYSTEM32\DRIVERS* directory.
3. From the system prompt, enter **REGEDT32**; the Registry Editor starts.
4. Select the HKEY_LOCAL_MACHINE window.
5. Open the **System** folder.
6. Open the **CurrentControlSet** folder.
7. Highlight **Services**.
8. From the **Edit** menu, select ***Add Key...***; you are prompted to enter a name and class.
9. In the **name** field, enter **cryptont**. (Leave the **class** field blank.)
10. Select **OK**; the system creates the entry **cryptont** inside **Services**.
11. Find and highlight the newly created **cryptont** entry.
12. From the **Edit** menu, select ***Add Value...***; you are prompted to enter a name and datatype.
13. Enter **Start** in the **Value Name** field.
14. Select **REG_DWORD** in the **Data Type** field.
15. Select **OK**; you are prompted to enter a value.
16. Enter **2** as the value.
17. Select **OK**.
18. Highlight the newly created **cryptont** entry again.
19. From the **Edit** menu, select ***Add Value...***; you are prompted to enter a name and datatype.
20. Enter **Type** in the **Value Name** field.
21. Select **REG_DWORD** in the **Data Type** field.
22. Select **OK**; you are prompted to enter a value.
23. Enter **1** as the value.
24. Select **OK**.
25. Highlight the newly created **cryptont** entry once again.
26. From the **Edit** menu, select ***Add Value...***; you are prompted to enter a name and datatype.
27. Enter **ErrorControl** in the **Value Name** field.
28. Select **REG_DWORD** in the **Data Type** field.
29. Select **OK**; you are prompted to enter a value.

30. Enter **1** as the value.
31. Select **OK**
32. Find and open the **EventLog** folder located within the **Services** folder.
33. Open the **System** folder.
34. From the **Edit** menu, select ***Add Key...***; you are prompted to enter a name and class.
35. In the **name** field, enter **cryptont**. (Leave the **class** field blank.)
36. Select **OK**; the system creates the entry **cryptont** inside **EventLog**.
37. Find and highlight the newly created **cryptont** entry.
38. From the **Edit** menu, select ***Add Value...***; you are prompted to enter a name and datatype.
39. Enter **EventMessageFile** in the **Value Name** field.
40. Select **REG_EXPAND_SZ** in the **Data Type** field.
41. Select **OK**.
42. Enter **%SystemRoot%\System32\Drivers\cryptont.sys**.
43. Select **OK**.
44. Find and highlight the newly created **cryptont** entry.
45. From the **Edit** menu, select ***Add Value...***; you are prompted to enter a name and datatype.
46. Enter **TypesSupported** in the **Value Name** field.
47. Select **REG_DWORD** in the **Data Type** field.
48. Select **OK**; you are prompted to enter a value.
49. Enter **7** as the value.
50. Close the Registry Editor.
51. Restart the host computer; the installation process is complete.

How to Remove the Software

To remove the software:

1. Delete *cryptont.dll* from directory *c:\WINNT\SYSTEM32*.
2. Delete *cryptont.sys* from directory *c:\WINNT\SYSTEM32\DRIVERS*.
3. From the system prompt, enter **REGEDT32**; the Registry Editor starts.
4. Select the HKEY_LOCAL_MACHINE window.
5. Open the **System** folder.
6. Open the **CurrentControlSet** folder.
7. Open the **Services** folder.
8. Highlight the **cryptont** entry.
9. From the **Edit** menu, select ***Delete***; the **cryptont** entry is removed.
10. Open the **EventLog** folder.
11. Highlight the **cryptont** entry.

12. From the **Edit** menu, select ***Delete***; the **cryptont** entry is removed.
13. Close the Registry Editor; the removal process is complete.

Chapter 3. How to Load Software into the Cryptographic Coprocessor

This chapter describes how to load software into the IBM 4758 PCI Cryptographic Coprocessor.

The Coprocessor Load Utility (CLU) runs on the host and downloads software to the coprocessor. The command used to run CLU depends on the host operating system:

AIX	**csufclu**
OS/2	**csueclu**
Windows NT	**csunclu**

Files containing software to be loaded into the coprocessor incorporate a digital signature that allows the coprocessor to reject attempts to load unauthorized programs. These files typically have names of the form name.CLU.

CLU prompts for its arguments; alternatively, they can be supplied on the command line. The arguments are as follows:

- The name of a file to which CLU writes a log of the operations it performs and the result of each operation.
- The operation CLU is to perform, which may be ST (obtain the coprocessor status), PL (load software into the coprocessor), or RS (reboot the coprocessor).
- The name of the file containing software to load into the coprocessor. This argument is supplied only for the PL operation.
- An optional flag (-q) that directs CLU to perform the operation without displaying any output.

CLU's ST command lists the status of the coprocessor and information about the software currently loaded in the coprocessor. The RS command reboots the processor. The processor must be rebooted after new software is loaded to cause the software to run.

For example, to load the file APP.CLU and start the application it contains, issue the following commands on Windows NT:

```
csunclu clu.log pl app.clu
csunclu clu.log rs
```

Appendix A. 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.

Copying and Distributing Softcopy Files

For online versions of this book, 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, denoted by an asterisk (*) in this publication, are trademarks of the IBM Corporation in the United States or other countries or both:

IBM
OS/2
Operating System/2

The following terms, denoted by a double asterisk (**) in this publication, are the trademarks of other companies:

Acrobat Reader	Adobe Systems, Inc.
Microsoft	Microsoft Corporation
Windows	Microsoft Corporation
Windows NT	Microsoft Corporation

List of Abbreviations and Acronyms

ANSI	American National Standards Institute
AIX	Advanced Interactive Executive (operating system)
API	application program interface
ASCII	American National Standard Code for Information Interchange
BBRAM	battery-backed random access memory
C	Celsius
CBC	cipher block chain
CCA	Common Cryptographic Architecture
CDMF	Commercial Data Masking Facility
CLU	Coprocessor Load Utility
cm	centimeter
CP/Q	Control Program/Q
CPU	central processing unit
DEA	data encryption algorithm
DES	Data Encryption Standard
DLL	dynamic link library
DMA	direct memory access
EPROM	erasable programmable read-only memory
F	Fahrenheit
FIFO	first-in-first-out
FIPS	Federal Information Processing Standard
IBM	International Business Machines
ICAT	Interactive Code Analysis Tool
in	inch
I/O	input/output
IPL	initial program load
ISO	International Organization for Standardization
KEK	key-encrypting key
MB	megabyte
MAC	message authentication code
MBps	one million bytes per second
MD5	message digest 5 (hashing algorithm)
MDC	modification detection code
MHz	megahertz
mm	millimeter
ODM	object data manager
OEM	original equipment manufacturer
OS/2	Operating System/2
PC	personal computer
PCI	peripheral component interconnect
PDF	portable document format
PKA	public key algorithm
POST	power-on self-test
PPD	program proprietary data
RAM	random access memory
RNG	random number generator
ROM	read-only memory
RSA	Rivest-Shamir-Adleman (algorithm)
SCC	secure cryptographic coprocessor
SHA	secure hashing algorithm
SKA	secret key authentication
SVC	supervisor call
TOD	time-of-day (clock)
UART	universal asynchronous receiver/transmitters
V	volt
VDC	volts direct current
VPD	vital product data

Glossary

This glossary includes terms and definitions from the *IBM Dictionary of Computing*, New York: McGraw Hill, 1994. This glossary also includes terms and definitions taken from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42 Street, New York, New York 10036. Definitions are identified by the symbol (A) following the definition.
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) following the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) following the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.

A

access. In computer security, a specific type of interaction between a subject and an object that results in the flow of information from one to the other.

access control. Ensuring that the resources of a computer system can be accessed only by authorized users and in authorized ways.

access method. A technique for moving data between main storage and input/output devices.

adapter. Synonym for *expansion card*.

Advanced Interactive Executive (AIX) operating system. The IBM implementation of the UNIX** operating system.

agent. (1) An application that runs within the IBM 4758 PCI Cryptographic Coprocessor. (2) Synonym for *secure cryptographic coprocessor application*.

AIX operating system. Advanced Interactive Executive operating system.

American National Standard Code for Information Interchange (ASCII). The standard code, using a coded character set consisting of seven-bit characters (eight bits including parity check), that is used for information interchange among data processing systems, data communication systems, and associated equipment. The ASCII set consists of control characters and graphic characters. (A)

American National Standards Institute (ANSI). An organization consisting of producers, consumers, and general interest groups that establishes the procedures by which accredited organizations create and maintain voluntary industry standards for the United States. (A)

ANSI. American National Standards Institute.

API. Application program interface.

application program interface (API). A functional interface supplied by the operating system, or by a separate program, that allows an application program written in a high-level language to use specific data or functions of the operating system or that separate program.

ASCII. American National Standard Code for Information Interchange.

authentication. (1) A process used to verify the integrity of transmitted data, especially a message. (T) (2) In computer security, a process used to verify the user of an information system or protected resource.

authorization. (1) In computer security, the right granted to a user to communicate with or make use of a computer system. (T) (2) The process of granting a user either complete or restricted access to an object, resource, or function.

authorize. To permit or give authority to a user to communicate with or make use of an object, resource, or function.

B

battery-backed random access memory (BBRAM). Random access memory that uses battery power to retain data while the system is powered off. The IBM 4758 PCI Cryptographic Coprocessor uses BBRAM to store persistent data for SCC applications, as well as the coprocessor device key.

BBRAM. Battery-backed random access memory.

bus. In a processor, a physical facility along which data is transferred.

C

call. The action of bringing a computer program, a routine, or a subroutine into effect, usually by specifying the entry conditions and jumping to an entry point. (I) (A)

card. (1) An electronic circuit board that is plugged into an expansion slot of a system unit. (2) A plug-in circuit assembly. (3) See also *expansion card*.

CBC. Cipher block chain.

CCA. Common Cryptographic Architecture.

CDMF algorithm. Commercial Data Masking Facility algorithm.

central processing unit (CPU). (1) Synonym for processing unit. (T) (2) The part of a computer that includes the circuits that control the interpretation and execution of instructions.

ciphertext. (1) Data that has been altered by any cryptographic process. (2) See also *plaintext*.

cipher block chain (CBC). A mode of operation that cryptographically connects one block of ciphertext to the next plaintext block.

cleartext. (1) Data that has not been altered by any cryptographic process. (2) Synonym for *plaintext*. (3) See also *ciphertext*.

CLU. Coprocessor Load Utility.

Commercial Data Masking Facility (CDMF) algorithm. An algorithm for data confidentiality applications; it is based on the DES algorithm and has an effective key strength of 40 bits.

Comm_Mgr. Communications Manager.

Common Cryptographic Architecture (CCA). A comprehensive set of cryptographic services that furnishes a consistent approach to cryptography on major IBM computing platforms. Application programs can access these services through the CCA application program interface.

Common Cryptographic Architecture (CCA) API. The application program interface used to call Common Cryptographic Architecture functions; it is described in the *IBM 4758 CCA Basic Services Reference and Guide*, SC31-8609.

Communications Manager (Comm_Mgr). A CP/Q^{++} extension for the IBM 4758 PCI Cryptographic Coprocessor that manages communication among the host device driver, SCC applications, and CP/Q^{++}. It handles the receipt and delivery of request headers, and the inbound and outbound data buffers.

Control Program/Q (CP/Q). The operating system embedded within the IBM 4758 PCI Cryptographic Coprocessor. The version of CP/Q used by the coprocessor—including extensions to support cryptographic and security-related functions—is known as CP/Q^{++}.

coprocessor. (1) A supplementary processor that performs operations in conjunction with another processor. (2) A microprocessor on an expansion card that extends the address range of the processor in the host system, or adds specialized instructions to handle a particular category of operations; for example, an I/O coprocessor, math coprocessor, or a network coprocessor.

Coprocessor Load Utility (CLU). A program used to load validated code into the IBM 4758 PCI Cryptographic Coprocessor.

CP/Q. Control Program/Q.

CPU. Central processing unit.

Cryptographic Coprocessor (IBM 4758). An expansion card that provides a comprehensive set of cryptographic functions to a workstation.

cryptographic node. A node that provides cryptographic services such as key generation and digital signature support.

cryptography. (1) The transformation of data to conceal its meaning. (2) In computer security, the principles, means, and methods used to so transform data.

D

data encrypting key. (1) A key used to encipher, decipher, or authenticate data. (2) Contrast with *key-encrypting key*.

data encryption algorithm (DEA). A 64-bit block cipher that uses a 64-bit key, of which 56 bits are used to control the cryptographic process and eight bits are used to check parity.

Data Encryption Standard (DES). The National Institute of Standards and Technology (NIST) Data Encryption Standard, adopted by the U.S. government as Federal Information Processing Standard (FIPS) Publication 46, which allows only hardware implementation of the data encryption algorithm.

Data Encryption Standard Manager (DES_Mgr). A CP/Q++ extension that manages the IBM 4758 PCI Cryptographic Coprocessor DES processing hardware.

DEA. Data encryption algorithm.

decipher. (1) To convert enciphered data into clear data. (2) Contrast with *encipher*.

DES. Data Encryption Standard.

DES_Mgr. Data Encryption Standard Manager.

device driver. (1) A file that contains the code needed to use an attached device. (2) A program that enables a computer to communicate with a specific peripheral device; for example, a printer, videodisc player, or a CD drive.

direct memory access (DMA). The transfer of data between memory and input/output units without processor intervention.

DLL. Dynamic link library.

DMA. Direct memory access.

dynamic link library (DLL). A file containing executable code and data bound to a program at load time or run time, rather than during linking. The code and data in a dynamic link library can be shared by several applications simultaneously.

E

encipher. (1) To scramble data or convert it to a secret code that masks its meaning. (2) Contrast with *decipher*.

enciphered data. (1) Data whose meaning is concealed from unauthorized users or observers. (2) See also *ciphertext.*

EPROM. Erasable programmable read-only memory.

erasable programmable read-only memory (EPROM). Programmable read-only memory that can be erased by a special process and reused.

expansion board. Synonym for *expansion card*.

expansion card. A circuit board that a user can plug into an expansion slot to add memory or special features to a computer.

expansion slot. One of several receptacles in a PC or RS/6000 machine into which a user can install an expansion card.

F

feature. A part of an IBM product that can be ordered separately from the essential components of the product.

Federal Information Processing Standard (FIPS). A standard that is published by the US National Institute of Science and Technology.

FIFO. First-in-first-out.

FIPS. Federal Information Processing Standard

first-in-first-out (FIFO). A queuing technique in which the next item to be retrieved is the item that has been in the queue for the longest time. (A)

flash memory. A specialized version of erasable programmable read-only memory (EPROM) commonly used to store code in small computers.

H

hertz (Hz). A unit of frequency equal to one cycle per second. **Note:** In the United States, line frequency is 60 Hz, a change in voltage polarity 120 times per second; in Europe, line frequency is 50 Hz, a change in voltage polarity 100 times per second.

host. As regards to the IBM 4758 PCI Cryptographic Coprocessor, the workstation into which the coprocessor is installed.

I

ICAT. Interactive Code Analysis Tool.

initial program load (IPL). (1) The initialization procedure that causes an operating system to commence operation. (2) The process by which a configuration image is loaded into storage. (3) The process of loading system programs and preparing a system to run jobs.

inline code. In a program, instructions that are executed sequentially without branching to routines, subroutines, or other programs.

input/output (I/O). (1) Pertaining to input, output, or both. (A) (2) Pertaining to a device, process, or channel involved in data input, data output, or both.

Interactive Code Analysis Tool (ICAT). A remote debugger used to debug applications running within the IBM 4758 PCI Cryptographic Coprocessor.

interface. (1) A boundary shared by two functional units, as defined by functional characteristics, signal

characteristics, or other characteristics as appropriate. The concept includes specification of the connection between two devices having different functions. (T) (2) Hardware, software, or both that links systems, programs, and devices.

International Organization for Standardization (ISO). An organization of national standards bodies established to promote the development of standards that facilitate the international exchange of goods and services; also, to foster cooperation in intellectual, scientific, technological, and economic activity.

intrusion latch. A software-monitored bit that can be triggered by an external switch connected to a jumper on the IBM 4758 PCI Cryptographic Coprocessor. This latch can be used, for example, to detect when the cover of the coprocessor host workstation has been opened. The intrusion latch does not trigger the destruction of data stored within the coprocessor.

I/O. Input/output.

IPL. Initial program load.

ISO. International Organization for Standardization.

J

jumper. A wire that joins two unconnected circuits.

K

key. In computer security, a sequence of symbols used with an algorithm to encipher or decipher data.

M

MAC. Message authentication code.

master key. In computer security, the top-level key in a hierarchy of KEKs.

message authentication code (MAC). In computer security, (1) a number or value derived by processing data with an authentication algorithm, (2) the cryptographic result of block cipher operations, on text or data, using the cipher block chain (CBC) mode of operation.

miniboot. Software within the IBM 4758 PCI Cryptographic Coprocessor designed to initialize the CP/Q^{++} operating system and to control updates to flash memory.

multi-user environment. A computer system that supports terminals and keyboards for more than one user at the same time.

N

National Institute of Science and Technology (NIST). Current name for the US National Bureau of Standards.

NIST. National Institute of Science and Technology.

node. (1) In a network, a point at which one or more functional units connects channels or data circuits. (I) (2) The endpoint of a link or junction common to two or more links in a network. Nodes can be processors, communication controllers, cluster controllers, or terminals. Nodes can vary in routing and other functional capabilities.

NT. See *Windows NT*.

O

object data manager (ODM). In the AIX operating system, a data manager intended for the storage of system data.

ODM. Object data manager.

Operating System/2 (OS/2). An IBM operating system for personal computers.

OS/2. Operating System/2.

P

passphrase. In computer security, a string of characters known to the computer system and to a user; the user must specify it to gain full or limited access to the system and to the data stored therein.

PKA. Public key algorithm.

PKA_Mgr. Public Key Algorithm Manager.

POST. Power-on self-test.

power-on self-test (POST). A series of diagnostic tests that runs automatically when device power is turned on.

PPD. Program proprietary data.

PPD_Mgr. Program Proprietary Data Manager.

private key. (1) In computer security, a key that is known only to the owner and used with a public key algorithm to decipher data. Data is enciphered using the related public key. (2) Contrast with *public key*. (3) See also *public key algorithm*.

procedure call. In programming languages, a language construct for invoking execution of a procedure. (I) A procedure call usually includes an entry name and the applicable parameters.

program proprietary data (PPD). Persistent data stored within the IBM 4758 PCI Cryptographic Coprocessor flash memory or battery-backed RAM that is associated with a particular agent.

Program Proprietary Data Manager (PPD_Mgr). A CP/Q^{++} extension for the IBM 4758 PCI Cryptographic Coprocessor that manages the persistent data associated with a particular SCC application. Persistent data is stored in flash memory or battery-backed RAM, and is protected from other SCC applications.

public key. (1) In computer security, a key that is widely known and used with a public key algorithm to encipher data. The enciphered data can be deciphered only with the related private key. (2) Contrast with *private key*. (3) See also *public key algorithm*.

public key algorithm (PKA). (1) In computer security, an asymmetric cryptographic process that uses a public key to encipher data and a related private key to decipher data. (2) See also *RSA algorithm*.

Public Key Algorithm Manager (PKA_Mgr). A CP/Q^{++} extension that manages the IBM 4758 PCI Cryptographic Coprocessor PKA processing hardware.

R

RAM. Random access memory.

random access memory (RAM). A storage device into which data is entered and from which data is retrieved in a non-sequential manner.

random number generator (RNG). A system designed to output values that cannot be predicted. Since software-based systems generate predictable, pseudo-random values, the IBM 4758 PCI Cryptographic Coprocessor uses a hardware-based system to generate true random values for cryptographic use.

Random Number Generator Manager (RNG_Mgr). A CP/Q^{++} extension that manages the IBM 4758 PCI Cryptographic Coprocessor hardware-based random number generator.

read-only memory (ROM). Memory within which stored data cannot be modified routinely.

reduced instruction set computer (RISC). A computer that processes data quickly by using only a small, simplified instruction set.

return code. (1) A code used to influence the execution of succeeding instructions. (A) (2) A value returned to a program to indicate the results of an operation requested by that program.

RNG. Random number generator.

RNG_Mgr. Random Number Generator Manager.

ROM. Read-only memory.

RSA algorithm. A public key encryption algorithm developed by R. Rivest, A. Shamir, and L. Adleman.

S

SCC. Secure cryptographic coprocessor.

SCC_Mgr. Secure Cryptographic Coprocessor Manager.

secret key authentication (SKA) certificate. The SKA certificate contains enciphered values that could allow IBM to re-initialize a coprocessor after its tamper-sensors have been triggered. Without a copy of the certificate, there is no way to recover the coprocessor.

secure cryptographic coprocessor (SCC). An alternate name for the IBM 4758 PCI Cryptographic Coprocessor. The abbreviation “SCC” is used within the product software code.

secure cryptographic coprocessor (SCC) application. (1) An application that runs within the IBM 4758 PCI Cryptographic Coprocessor. (2) Synonym for *agent*.

Secure Cryptographic Coprocessor Manager (SCC_Mgr). A CP/Q^{++} extension that provides high-level management of all agents running within a IBM 4758 PCI Cryptographic Coprocessor. As the “traffic cop”, the SCC_Mgr identifies agents and controls the delivery of their messages and data.

security. The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

SKA certificate. Secret key authentication certificate.

SMIT. System Management Interface Tool.

supervisor call (SVC). In CP/Q, the mechanism whereby a task requests services from the system or from other system elements in the system in the system, or whereby it performs services for other elements in the system.

SVC. Supervisor call.

system administrator. The person at a computer installation who designs, controls, and manages the use of the computer system.

System Management Interface Tool (SMIT). An AIX utility program used to maintain the system in good working order and to modify the system to meet changing requirements.

T

time-of-day (TOD) clock. A hardware feature that is incremented once every microsecond, and provides a consistent measure of elapsed time suitable for indicating date and time. The TOD clock runs regardless of whether the processing unit is in a running, wait, or stopped state.

throughput. (1) A measure of the amount of work performed by a computer system over a given period of time; for example, number of jobs-per-day. (A) (I) (2) A measure of the amount of information transmitted over a network in a given period of time; for example, a network data-transfer-rate is usually measured in bits-per-second.

TOD clock. Time-of-day clock.

U

utility program. A computer program in general support of computer processes. (T)

V

verb. A function possessing an entry_point_name and a fixed-length parameter list. The procedure call for a verb uses the syntax standard to programming languages.

vital product data (VPD). A structured description of a device or program that is recorded at the manufacturing site.

VPD. Vital product data.

W

Windows NT. A Microsoft operating system for personal computers.

workstation. A terminal or microcomputer, usually one that is connected to a mainframe or a network, and from which a user can perform applications.

Numerics

IBM 4758. IBM 4758 PCI Cryptographic Coprocessor.

Index