GC31-8644-00

IBM SecureWay Cryptographic Products

IBM 4758 PCI Cryptographic Coprocessor Technical Overview for Original Equipment Manufacturers

IBM SecureWay Cryptographic Products

GC31-8644-00

IBM 4758 PCI Cryptographic Coprocessor Technical Overview for Original Equipment Manufacturers

Note!

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

First Edition (August, 1997)

This edition, GC31-8644-00, applies to the PCI Cryptographic Coprocessor product as announced in June, 1997.

Changes are made periodically to the information herein; before using this publication in connection with the operation of IBM* systems, consult your IBM representative to be sure that you have the latest edition and any Technical Newsletters.

IBM does not stock publications at the address given below; requests for IBM publications should be made to your IBM representative or to the IBM branch office serving your locality.

A form for reader’s comments is provided at the back of this publication. If the form has been removed, comments may be addressed to IBM Corporation, Department VM9A, MG81, 8501 IBM Drive, Charlotte, NC 28262-8563, U.S.A. IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Table of Contents

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
IBM World Registry
OS/2
Operating System/2
SecureWay

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

Acrobat Reader	Adobe Systems, Inc.
Pentium Pro	Intel Corporation
Pentium	Intel Corporation
Microsoft	Microsoft Corporation
Windows NT	Microsoft Corporation

About This Book

The *IBM 4758 PCI Cryptographic Coprocessor Technical Overview for Original Equipment Manufacturers* describes the hardware and software included with the cryptographic coprocessor. The audience for this manual includes customer executives, system analysts, application programmers, and others who:

- Evaluate the benefits and the advantages of the product.
- Select and order a suitable configuration of the product.
- Create applications that employ the product.

Chapter 1, “Introduction” summarizes the PCI Cryptographic Coprocessor.

Chapter 2, “Hardware Overview ” introduces the hardware components that make up the PCI Cryptographic Coprocessor.

Chapter 3, “Software Overview” describes the software features of the PCI Cryptographic Coprocessor.

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

Related Publications

The list below reflects source information regarding the IBM 4758 PCI Cryptographic Coprocessor, commercial cryptography, and products that use the IBM Common Cryptographic Architecture (CCA) application program interface (API).

IBM 4758 PCI Cryptographic Coprocessor Publications

Check the product web site at *http://www.ibm.com/security/cryptocards* for the availability of these publications. From the web site, you can download, view, and print publications available in the Acrobat** Reader portable document format (PDF):

- *IBM 4758 PCI Cryptographic Coprocessor Installation Manual*, SC31-8623
- *IBM 4758 CCA Basic Services Reference and Guide*, SC31-8609
- *IBM 4758 CCA Services Installation and I/O Guide*, SC31-8610

Cryptography Publications

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

- *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
- *IBM Systems Journal* Volume 30 Number 2, 1991, G321-0103
- *IBM Systems Journal* Volume 32 Number 3, 1993, G321-5521
- *IBM Journal of Research and Development Volume 38 Number 2, 1994*, G322-0191
- *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
- *ISO 9796 Digital Signal Standard*
- *Internet Engineering Taskforce RFC 1321*, April 1992, MD5
- *Secure Electronic Transaction Protocol Version 1.0*, May 31, 1997

Other IBM Cryptographic Product Publications

The following publications describe products that utilize the IBM Common Cryptographic Architecture (CCA) application program interface (API):

- *IBM Transaction Security System General Information Manual*, GA34-2137
- *IBM Transaction Security System Basic CCA Cryptographic Services*, SA34-2362
- *IBM Transaction Security System I/O Programming Guide*, SA34-2363
- *IBM Transaction Security System Finance Industry CCA Cryptographic Programming*, SA34-2364
- *IBM Transaction Security System Workstation Cryptographic Support Installation and I/O Guide*, GC31-4509
- *IBM 4755 Cryptographic Adapter Installation Instructions*, GC31-4503
- *IBM Transaction Security System Physical Planning Manual*, GC31-4505
- *IBM Common Cryptographic Architecture Services/400 Installation and Operators Guide, Version 2*, SC41-0102
- *IBM Common Cryptographic Architecture Services/400 Installation and Operators Guide, Version 3*, SC41-0102
- *IBM ICSF/MVS General Information*, GC23-0093
- *IBM ICSF/MVS Application Programmer's Guide*, SC23-0098

Summary of Changes

This first version of the *IBM 4758 PCI Cryptographic Coprocessor Technical Overview for Original Equipment Manufacturers* contains product information that is current with the IBM 4758 PCI Cryptographic Coprocessor announcements made in June 1997.

Chapter 1. Introduction

This chapter summarizes the following characteristics of the IBM 4758 PCI Cryptographic Coprocessor:

- Security functions
- Hardware components
- Software components
- Applications

The IBM 4758 PCI Cryptographic Coprocessor—a member of the SecureWay* family of products—combines hardware and software to provide a wide variety of security services, including customized applications that run inside a tamper-protected enclosure.

This document describes the cryptographic coprocessor and gives detailed technical information about its components.

Summary of Security Functions

The cryptographic coprocessor can reliably effect the following security functions:

- Data encryption standard (DES) (56- and 40-bit keys) encryption and decryption, with pre- and post-padding; the coprocessor uses both electronic codebook (ECB) and cipher block chain (CBC) modes of encryption.
- MAC generation and MAC verification services
- Triple DES (three key) encryption and decryption of eight-byte units
- Secure RSA key-pair generation
- RSA signature generation and signature verification
- Hardware random number generation
- Secure data storage and retrieval
- Other non-cryptographic security utilities

Summary of Hardware Components

The cryptographic coprocessor contains the following hardware components:

- A general-purpose Intel-compatible 80486-DX2 microprocessor
- High-speed, bulk-data DES-encryption hardware
- A large-integer modular math coprocessor used to support public-key cryptographic operations
- Four megabytes of random access memory (RAM)
- Two megabytes of flash memory
- A hardware-based random number generator
- Battery-backed memory to preserve sensitive data when primary power is lost
- A time of day (TOD) clock

- A serial port

Tamper-responding elements (membranes and circuitry) inside the coprocessor protect data and software from attack by voltage, temperature, radiation, probe, or other agents.

Summary of Software Components

Software for the cryptographic coprocessor includes the following components:

- Cryptographic libraries
- An embedded operating system and auxiliary control routines
- Software to control and allow updates to the software itself
- Power on self test (POST) diagnostic routines
- Device drivers
- Source-level debuggers
- Utilities

Summary of Applications

The IBM 4758 PCI Cryptographic Coprocessor combines a completely enclosed, tamper-protected processor with high-speed encryption engines. It is particularly well-suited to applications that must run in uncontrolled surroundings:

- dispensers in public kiosks
- postage meters
- electronic mints
- electronic cash registers
- gaming servers
- usage meters

The cryptographic coprocessor is ideal for applications supporting a heavy cryptographic workload, such as electronic commerce gateways used to process electronic signatures. Its bulk-data encryption and decryption speeds are outstanding; it can easily sustain loads as heavy as those experienced when encrypting audio and video digital data.

The cryptographic coprocessor is also well-suited for use in government and defense applications requiring strong security features and high-speed cryptographic processing.

Chapter 2. Hardware Overview

This chapter describes the IBM 4758 PCI Cryptographic Coprocessor card, its components, and the physical security features that protect it.

The PCI Cryptographic Coprocessor Card

The PCI Cryptographic Coprocessor card is a state-of-the-art cryptography tool: a completely enclosed, tamper-protected processor mounted on a PCI-bus card. It offers high-performance cryptographic processing, using DES and RSA algorithms.

All software executed on the card runs inside a secure enclosure; this enclosure was designed to meet the stringent requirements of Level 4 of the Federal Information Processing Standard (FIPS) Publication 140-1 for Cryptographic Modules. All software operating within this secure environment has been authenticated using digital-signature techniques.

The coprocessor card is composed of:

- A central processing unit (CPU)
- RAM, ROM and flash EPROM
- A PCI-bus interface and a serial port interface
- Access-control elements
- Security provisions

Central Processing Unit (CPU)

The CPU is mounted on the PCI card and includes:

- An Intel-compatible 80486-DX2 microprocessor
- A hardware-based random number generator
- A backup battery
- A time of day (TOD) clock
- Chips to enable high-speed cryptographic processing

Microprocessor

The microprocessor is an Intel-compatible 486-DX2 66MHz general purpose computer housed in a single chip. A floating-point coprocessor is not included; floating-point operations are emulated in the software.

Random Number Generator

A noise-source-based random number generator delivers a serial bit stream designed to meet statistical random number generator tests described in FIPS Publication 140-1, section 4.11. A 16-bit collector register gathers random bits, then interrupts the coprocessor when the register is full.

Battery

The card contains a battery power-source to preserve cryptographic keys and other sensitive data that must persist in storage even when system power is turned off. With two battery receptacles, the customer can replace the batteries while maintaining battery-backed data.

See “Physical Security” on page 2-4 for an important notice regarding battery replacement.

TOD Clock

This clock is used to generate secure timestamps and is maintained by the battery when system power is lost.

Encryption Hardware

The cryptographic coprocessor can support both Data Encryption Standard (DES) and Public-Key Algorithm (PKA) processing.

The DES processor is designed to meet the requirements set forth in the Federal Information Processing Standard (FIPS) Publication 46-2. Features of this chip include:

- An internal 64-bit key register
- A 16-bit control/status register, used for chip configuration
- Support for electronic codebook (ECB) and cipher block chain (CBC) modes of operation
- First in, first out (FIFO) buffers with a complete set of full/empty interrupts; these interrupts allow for asynchronous software control of the buffers.

The PKA processor uses 1024-bit hardware to accelerate public-key operations. The hardware supports RSA algorithm key lengths to 1024-bits; the software supports sign, verify, and key-generate functions to 2048-bits in length, using the 1024-bit hardware to assist.

The public-key algorithm processor lends hardware assistance to the following modular arithmetic operations:

- modular exponentiation (A^x mod N)
- modular multiplication ($A \times B$) mod N)
- modular reduction (A mod N)

RAM, ROM, and Flash EPROM

The coprocessor uses four megabytes of RAM to execute applications. It uses two megabytes of flash EPROM memory and battery-backed RAM to house code, nonvolatile product proprietary data (PPD), and other data that must be maintained during periods of power loss; the data so maintained includes cryptographic keys.

Some of the ROM and flash EPROM is reserved for code and associated data, such as certificates; this memory is divided into four segments, zero through three. The content of each segment is detailed below:

- Segment_0 is read-only memory; it contains a portion of the POST and miniboot software.
- Segment_1 is flash EPROM; it contains the remainder of the POST and miniboot software.
- Segment_2 is flash EPROM; it contains the operating system and its auxiliary routines.

- Segment_3 is flash EPROM; it contains original equipment manufacturer (OEM) application software.

Each segment is associated with a region of battery-backed RAM that holds sensitive data relating to that memory segment. For example, the battery-backed memory corresponding to Segment_3 could contain keys associated with the code in Segment_3.

Interfaces

The cryptographic coprocessor card has two interfaces: a PCI-bus attachment and a serial port.

PCI-Bus

The cryptographic coprocessor attaches to the host computer through a PCI bus and operates in computers running under AIX, Windows NT**, and OS/2.* The card requires a two-thirds length PCI slot.

A simple host-based application program interface (API) to the coprocessor device driver facilitates communication between it and the host applications. To achieve maximum throughput, the device driver uses PCI busmaster hardware to send large amounts of data to and from the card.

Serial Port

The serial port is included to facilitate development debugs.

Access Control Elements

The control gate array and the router work together to control cryptographic functions and transfer data among the system components.

Control Gate Array

This array is used to access and control cryptographic functions, the flash memory write function, and coprocessor I/O. It also operates to automate high-speed bulk DES using FIFO input/output buffering.

The control gate array configures the router to set up data paths as required by the coprocessor. All data paths inside the secure boundary are controlled in this way; there is no externally-controlled access path across the secure boundary of the coprocessor.

Router

The router takes configuration data from the control gate array and uses it to set up data transfer paths as required by the coprocessor. Examples of data transfer paths include, but are not limited to, the following:

- External PCI bus, through the DES chip, and back to the external PCI bus
- External PCI bus, through the DES chip, to coprocessor memory
- Coprocessor memory, through the DES chip, back to coprocessor memory
- Coprocessor memory, through the DES chip, to the external PCI bus
- External PCI bus, bypassing all cryptographic functions, to coprocessor memory

Physical Security

The coprocessor is designed to meet US Federal Information Processing Standard (FIPS) 140-1. FIPS 140-1 is the most demanding standard currently governing cryptographic hardware.

The tamper-responding hardware is sensitive to attack by voltage, temperature, radiation, probe, or other agents. Detection of invasive processes causes the card to zero all values stored in RAM and in battery-backed RAM. This process cannot be reversed; the card must be replaced after an attack has been detected.

IMPORTANT NOTICES:

1. During transport or when powered down, the card must be maintained within a specific temperature range. Failure to do so will negate the factory certification and void the warranty.
2. During battery replacement, at least one of two batteries must be charged and in place at all times. Failure to keep at least one charged battery in place will negate the factory certification and void the warranty.

Chapter 3. Software Overview

The software documented in this chapter:

- Boots and tests the cryptographic coprocessor.
- Operates the cryptographic coprocessor.
- Interfaces between cryptographic coprocessor hardware and the host computer.
- Provides tools for applications development.

Boot Software

The software below is responsible for the boot and self-testing of the cryptographic coprocessor:

- Power on self test (POST)
- Miniboot

When the cryptographic coprocessor is first powered on or reset, the POST software gains control of the coprocessor and performs a power on self test. Once the test is successfully completed, the POST software transfers coprocessor control to the miniboot software. If the miniboot software finishes successfully, it transfers control to the CP/Q system software. Whichever software—POST or miniboot—detects an error in its routine, that software shuts down the cryptographic coprocessor.

Once coprocessor control is passed to CP/Q, the operating system retains control of the coprocessor until it is powered down or reset. Any POST failure in the coprocessor is reported to the host system. If the host system device driver detects a pre-existing coprocessor POST or miniboot error, it precludes every application from accessing the device.

Power On Self Test

The power on self test (POST) software verifies that the hardware components of the coprocessor are operating properly. POST tests include, but are not limited to, the following:

- Memory tests
- DES-algorithm tests
- RSA-algorithm tests
- Random number generator tests
- Host communication tests

Miniboot

Miniboot software performs two functions: it initializes the coprocessor operating system, and it controls updates to software in flash memory.

Details of the miniboot software are proprietary, but can be obtained through a non-disclosure agreement with IBM.

CP/Q Operating System

CP/Q is the operating system within the 4758 PCI Cryptographic Coprocessor; it is designed to run on Intel processors, from series 80386 to Pentium Pro**. The version of CP/Q used by the cryptographic coprocessor is informally referred to as CP/Q^{++}; it contains extensions to support cryptographic processing and other security-related functions.

CP/Q is uniquely adapted to cryptographic processing:

- It provides full multitasking, so the user can do other work during cryptographic operations.
- It isolates supervisor memory space from application memory space, so that applications cannot disrupt the operating system.
- It isolates applications from each other. Once an application has memory space allotted to it, no other application can use that space until the controlling application task has ended; the memory is reset to zero before it is made available for reuse.

The base CP/Q operating system follows conventions for message formats, error codes, and warning codes. All auxiliary routines follow these conventions as well. The standardization of commands and messages helps to streamline the development of applications to be used inside the cryptographic coprocessor.

CP/Q supports the configuration of system components; the standard version of the operating system includes:

- A supervisor call (SVC) handler.
- A resource manager.
- A memory manager.

Extensions

Functional extensions of CP/Q^{++} include:

- A data encryption standard (DES) manager to control access to the DES hardware and to the FIFO registers
- A public-key algorithm (PKA) manager to control access to the modular mathematic hardware
- A random number generator (RNG) Manager to control access to the random number generator hardware
- A communications (Comm) manager to control the flow of data between the host and internal applications
- A product proprietary data (PPD) manager to control access to flash memory and battery-backed memory
- A secure cryptographic coprocessor (SCC) manager to control access to other managers and to handle service requests from applications.

Internal Application Program Interface

Applications running inside the coprocessor need a way to access the cryptographic hardware and other hardware resources inside the coprocessor. The SCC internal API supports, among others, the following functions:

- Cryptographic functions
- The manipulation of PPD
- Clock setting

Development Tools and Utilities

Development tools and utilities are features available to original equipment manufacturers (OEM) developing applications to run inside the cryptographic coprocessor. These tools and utilities include the following:

- An interactive remote debugger
- A file translator to convert executables so that they can be run inside the card
- A hardware initialization utility to load both code and data into flash memory

These tools and utilities are available only to computers operating under OS/2 and Windows NT.

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
C	celsius
CA	certification authority
CBC	cipher block chain
CCA	common cryptographic architecture
CDMF	commercial data masking facility
CL	coprocessor load
cm	centimeter
CP/Q	control program/q
CPU	central processing unit
CV	control vector
DEA	data encryption algorithm
DES	data encryption standard
DMA	direct memory access
ECB	electronic codebook
EPROM	erasable programmable read only memory
F	fahrenheit
FCC	federal communications commission
FIFO	first in first out
FIPS	federal information processing standard
IBM	international business machines
in	inch
I/O	input/output
IPL	initial program load
ISO	international organization for standardization
KEK	key encrypting key
LU	logical unit
MB	megabyte
MAC	message authentication code
MBps	megabytes per second
MD5	message digest 5 (hashing algorithm)
MDC	modification detection code
MHz	megahertz
mm	millimeter
NI	node initialization
NM	node management
NT	new technology
OEM	original equipment manufacturer
OS/2	operating system/2
PC	personal computer
PCI	peripheral component interconnect
PDD	physical device driver
PDF	portable document format
PIN	personal identification number
PKA	public key algorithm
PKCS	public key cryptography standard
POST	power on self test
PPD	product proprietary data
RAM	random access memory
RNG	random number generator
ROM	read only memory
RSA	rivest, shamir, and adleman
SAA	systems application architecture
SCC	secure cryptographic coprocessor
SHA	secure hashing algorithm
SKA	secret key authentication
SNA	systems network architecture
SVC	supervisor call
TOD	time of day (clock)
V	volt
VDC	volts direct current

Glossary

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

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

American national Standard Code for Information Interchange (ASCII). The standard code, using a coded character set consisting of 7-bit characters (8 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 in the United States. (A)

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.

Authorized Program Facility (APF). A facility that permits identification of programs authorized to use restricted functions.

B

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

C

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

CDMF algorithm. An algorithm for data confidentiality applications; it is based on the DES algorithm and possesses 40-bit key strength.

ciphertext. (1) Text that results from the encipherment of plaintext. (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) Text that has not been altered by a cryptographic process. (2) Synonym for *plaintext*. (3) See also *ciphertext*.

Common Cryptographic Architecture (CCA) API. The application programming interface described in the *IBM 4758 CCA Basic Services Reference and Guide*, SC31-8609.

control_vector. (1) In the CCA, a 16-byte string that is exclusive-ORd with a master key or a key-encrypting key to create another key that is used to encipher and decipher data or data keys. A control_vector determines the type of key and the restrictions on its use. (2) See also *key_token*.

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.

cryptographic coprocessor (IBM 4758). An expansion board that provides to a workstation a comprehensive set of cryptographic functions.

cryptographic key data set (CKDS). A data set that contains the encryption keys used by an installation.

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 implementations of the data-encryption algorithm.

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

driver. A program that contains the code needed to attach and use a device.

E

electronic codebook (ECB). A mode of operation used with block-cipher cryptographic algorithms in which plaintext or ciphertext is placed in the input to the algorithm and the result is contained in the output of the algorithm.

electrostatic discharge (ESD). An undesirable discharge of static electricity that can damage equipment and degrade electrical circuitry.

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

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

expansion board. Synonym for *expansion card*.

expansion card. (1) A circuit board that a user can install in an expansion slot to add memory or special features to a computer. (2) Synonym for *card*.

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

exporter key. (1) In the CCA, a type of DES key-encrypting key that can encipher a key at a sending node. (2) Contrast with *importer key*.

F

feature. A part of an IBM product that can be ordered separately.

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

Flash EPROM. A specialized version of EPROM commonly used to store code in small computers.

function-control vector. A signed value provided by IBM to enable the CCA application in the IBM 4758 PCI Cryptographic Coprocessor to provide a level of cryptographic service consistent with applicable export-and-import regulations.

H

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

host computer. In regard to the CCA Cryptographic Coprocessor Support Program, the workstation into which the IBM 4758 PCI Cryptographic Coprocessor is installed.

I

importer key. (1) In CCA products, a type of DES key-encrypting key that can decipher a key at a receiving node. (2) Contrast with *exporter key*.

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.

interface. (1) A boundary shared by two functional units, as defined by functional characteristics, signal characteristics, or other characteristics as appropriate. The concept includes the specification of the connection of 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 to facilitate the international exchange of goods and services, and to foster cooperation in intellectual, scientific, technological, and economic activity.

J

jumper. A wire that joins two unconnected circuits on a printed circuit board.

K

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

key-encrypting key (KEK). (1) A key used for the encryption and decryption of other keys. (2) Contrast with *data-encrypting key*.

key_label. In CCA products, an indirect identifier for a key_token record in key storage.

key storage. In CCA products, a data file that contains cryptographic keys.

key_token. In CCA products, a data structure that can contain a cryptographic key, its control_vector, and other information related to the key.

L

LAN/DP. An IBM-licensed program product, LAN Distributed Processing.

M

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

megabyte (MB). 1 048 576 bytes.

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 a cipher block chain (CBC) mode of operation.

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.

node. (1) In a network, a point at which one or more functional units connects channels or data circuits. (I) (2) An endpoint of a link or a 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.

O

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

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 the data stored therein.

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

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

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. The 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.

profile. Data that describes the significant characteristics of a user, a group of users, or one-or-more computer resources.

Programmed Cryptographic Facility (PCF). An IBM-licensed program that provides facilities for enciphering and deciphering data and for creating, maintaining, and managing cryptographic keys.

public key. (1) In computer security, a key that is widely known and used with a public-key algorithm to encrypt 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) Contrast with *Data Encryption Algorithm* and *Data Encryption Standard algorithm*. (3) See also *RSA algorithm*.

R

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

read only memory (ROM). Memory in 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.

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

S

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.

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

session level encryption (SLE). A Systems Network Architecture (SNA) protocol that provides a method for establishing a session with a unique key for that session. This protocol establishes a cryptographic key, and rules for deciphering and enciphering information in a session.

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

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. **Note:** The layered structure of SNA allows the ultimate origins and destinations of information, that is, the end users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

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's data-transfer-rate is usually measured in bits-per-second.

token. (1) A string of characters that is treated as a single entity. (2) A particular message or bit pattern that signifies permission to transmit. (3) See also *key_token*.

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.

W

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

Numerics

4758. IBM 4758 PCI Cryptographic Coprocessor.

Index

Communicating Your Comments to IBM

IBM SecureWay Cryptographic Products
IBM 4758 PCI Cryptographic Coprocessor
Technical Overview for
Original Equipment Manufacturers

Publication No. GC31-8644-00

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

If you are mailing a readers' comment form (RCF) from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number:

  United States and Canada: **1-800-227-5088**
- If you prefer to send comments electronically, use this network ID:
  - IBM Mail Exchange: **USIB2HPD at IBMMAIL**
  - IBMLink: **CIBMORCF at RALVM13**
  - Internet: **USIB2HPD@VNET.IBM.COM**

Make sure to include the following in your note:

- Title and publication number of this book
- Page number or topic to which your comment applies.

Help us help you!

IBM SecureWay Cryptographic Products
IBM 4758 PCI Cryptographic Coprocessor
Technical Overview for
Original Equipment Manufacturers

Publication No. GC31-8644-00

We hope you find this publication useful, readable and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	□	□

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	□	□
Complete	□	□
Easy to find	□	□
Easy to understand	□	□
Well organized	□	□
Applicable to your task	□	□

Specific Comments or Problems:

____

____

____

Please tell us how we can improve this book:

____

____

____

Thank you for your response. When you send information to IBM, you grant IBM the right to use or distribute the information without incurring any obligation to you. You of course retain the right to use the information in any way you choose.

____________________ Name	____________________ Address
____________________ Company or Organization	____________________
____________________ Phone No.	____________________

Help us help you!
GC31-8644-00

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Information Development
Department CGMD
International Business Machines Corporation
PO BOX 12195
RESEARCH TRIANGLE PARK NC 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

File Number: GC31-8644

Printed in U.S.A.

GC31-8644-00