GC31-8608-02

IBM 4758 PCI Cryptographic Coprocessor Models 001 and 013

General Information Manual

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.

Second Edition (October 1999)

This edition applies to the IBM 4758 Model 001, and to the Model 013 as announced in October 1999. This edition replaces prior editions of this manual as well as all editions of *IBM 4758 PCI Cryptographic Coprocessor Technical Overview for Original Equipment Manufacturers*, GC31-8644.

Changes are made periodically to the information herein. A current edition of this publication can be obtained from the Library page of the IBM 4758 product Web site at http://www.ibm.com/security/cryptocards.

Comments and questions about this publication may be addressed to IBM through the Support page of the IBM 4758 product web site at http://www.ibm.com/security/cryptocards, or you can send a letter to:

MG81/204-3
Department VM9A
IBM Corporation
8501 IBM Drive
Charlotte, NC 28262-8563
USA

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

About This Publication

This edition, GC31-8608-02, applies to the IBM 4758 Model 001, and to the Model 013 as announced in October, 1999. This edition replaces all prior editions of this manual as well as all editions of *IBM 4758 PCI Cryptographic Coprocessor Technical Overview for Original Equipment Manufacturers*, GC31-8644. This manual's audience 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.

The IBM 4758, Model 001, is also available as a feature within selected IBM AS/400 systems. See *http://www.as400.ibm.com/*.

Chapter 1, "Introduction to the IBM 4758 PCI Cryptographic Coprocessor" introduces the IBM 4758 and supporting software available from IBM.

Chapter 2, "IBM 4758 PCI Cryptographic Coprocessor Hardware" describes the IBM 4758 hardware and low-level software. The product ordering process and models are described.

Chapter 3, "IBM 4758 CCA Support Program" describes the IBM 4758 CCA Support Program optional software.

Chapter 4, "IBM 4758 Custom Software Development" describes custom programming possibilities and toolkits for the IBM 4758.

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

Summary of Changes

This second revision of the *IBM 4758 PCI Cryptographic Coprocessor General Information Manual* contains product information that is current with the announcement of the IBM 4758 Model 013 in October, 1999.

The manual has been substantially revised from the previous revision.

The Cryptographic Service Provider for the IBM 4758 CCA Support Program used with the IBM Keyworks implementation of the Common Data Security Architecture is no longer distributed with the IBM 4758 CCA Support Program. The Service Provider is now distributed with the IBM Keyworks offering.

Related Publications

The list below reflects source information regarding the 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 Library page of the IBM 4758 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 Adobe Acrobat** portable document format (PDF).

General Interest

- *IBM 4758 PCI Cryptographic Coprocessor Installation Manual*

IBM 4758 Common Cryptographic Architecture (CCA) Support Program Publications

- *IBM 4758 PCI Cryptographic Coprocessor CCA Support Program Installation Manual*
- *IBM 4758 CCA Basic Services Reference and Guide*

IBM 4758 Custom Programming Publications

- *IBM 4758 PCI Cryptographic Coprocessor Custom Software Developer's Toolkit Guide*
- *IBM 4758 PCI Cryptographic Coprocessor Custom Software Installation Manual*
- *IBM 4758 PCI Cryptographic Coprocessor Custom Software Interface Reference*
- *IBM 4758 PCI Cryptographic Coprocessor ICAT User's Guide*
- *IBM 4758 PCI Cryptographic Coprocessor CP/Q Operating System Overview*
- *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 Interface Reference*
- *IBM 4758 PCI Cryptographic Coprocessor CCA User Defined Extensions Programming Reference*
- *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/pciprod.pdf*.

Cryptography Publications

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

- “Application Support Architecture for a High-Performance, Programmable Secure Coprocessor,” J. Dyer, R. Perez, S.W. Smith, and M. Lindemann, 22nd National Information Systems Security Conference, October 1999.
- “Validating a High-Performance, Programmable Secure Coprocessor,” S.W. Smith, R. Perez, S.H. Weingart, and V. Austel, 22nd National Information Systems Security Conference, October 1999.
- “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. Springer-Verlag LNCS. 1998. ISBN 3-540-64951-4
- “Smart Cards in Hostile Environments,” H. Gobioff, S.W. Smith, J.D. Tygar, and B.S. Yee, *Proceedings of the Second USENIX Workshop on Electronic Commerce*, 1996
- “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.
- “Cryptography: It’s Not Just for Electronic Mail Anymore,” J.D. Tygar and B.S. Yee, Computer Science Technical Report, CMU-CS-93-107, Carnegie Mellon University, 1993.
- “Dyad: A System for Using Physically Secure Coprocessors,” J.D. Tygar and B.S. Yee, Harvard-MIT Workshop on Protection of Intellectual Property, April 1993.
- “An Introduction to Citadel—A Secure Crypto Coprocessor for Workstations,” E.R. Palmer, Research Report RC18373, IBM T.J. Watson Research Center, 1992.
- “Introduction to the Citadel Architecture: Security in Physically Exposed Environments,” S.R. White, S.H. Weingart, W.C. Arnold, and E.R. Palmer, Research Report RC16672, IBM T.J. Watson Research Center, 1991.

- “An Evaluation System for the Physical Security of Computing Systems,” S.H. Weingart, S.R. White, W.C. Arnold, and G.P. Double, Sixth Computer Security Applications Conference, 1990.
- “ABYSS: A Trusted Architecture for Software Protection,” S.R. White and L. Comerford, IEEE Security and Privacy, Oakland 1987.
- “Physical Security for the microABYSS System,” S.H. Weingart, IEEE Security and Privacy, Oakland 1987.
- *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*
- *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
- *Derived Test Requirements for FIPS PUB 140-1*, W. Havener, R. Medlock, L. Mitchell, and R. Walcott. MITRE Corporation, March 1995.
- *ISO 9796 Digital Signal Standard*
- *Internet Engineering Taskforce RFC 1321*, April 1992, MD5
- *Secure Electronic Transaction Protocol*, Version 1.0, May 31, 1997

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.

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

Chapter 1. Introduction to the IBM 4758 PCI Cryptographic Coprocessor

The IBM 4758 PCI Cryptographic Coprocessor...

> A flexible solution to your high-security cryptographic and secure processing needs.

The use of cryptographic techniques is a key element of modern e-business applications. These applications use cryptography in a variety of ways to protect the privacy and confidentiality of data, to ensure the integrity of data, and to provide user accountability through digital signature techniques. The 4758 PCI Cryptographic Coprocessor is a programmable PCI card that off-loads computationally intensive cryptographic processes from the hosting server and performs sensitive tasks unsuitable for less secure general purpose computers. It is a key product for enabling secure e-business transactions and is suited for a wide variety of cryptographic applications.

The IBM 4758 PCI Cryptographic Coprocessor is available in two models, identical in functional capability but differing in physical security characteristics. Both models have been certified under the US Government FIPS PUB 140-1 standard, *Security Requirements for Cryptographic Modules*. The IBM 4758 Model 001 has been certified at FIPS PUB 140-1 Level 4, the highest security classification for a commercial cryptographic device. The Model 013 has been certified at Level 3.

The Coprocessor plugs into industry-standard PCI slots in personal computers, IBM RS/6000 systems, and other systems that support the PCI bus. Software to support the Coprocessor is available for IBM AIX and OS/2, and for Windows NT** operating systems. The IBM 4758, Model 001, is also available as a feature within selected IBM AS/400 systems. (See *http://www.as400.ibm.com/*.)

The Coprocessor secure processing environment contains a 486-compatible microprocessor, custom hardware to perform DES and public key cryptographic algorithms, and a hardware random number generator. It also has protective shields, sensors, and control circuitry to protect against a wide variety of attacks against the secure environment.

IBM provides the Common Cryptographic Architecture (CCA) Support Program feature that you can load into the Coprocessor to perform cryptographic functions common in the finance industry, in Internet e-business applications, for DES data confidentiality and message authentication, and RSA-based digital signatures and key exchange services.

Under custom contracts, you can also purchase consulting, services, and programming toolkits to extend or replace the IBM CCA Support Program feature.

Highlights

Some of the highlights of the IBM 4758 PCI Cryptographic Coprocessor include the following:

- Tamper-responding design certified under FIPS PUB 140-1. Suitable for high-security processing and cryptographic operations. The 4758 provides a secure platform on which developers can build secure applications.
- Hardware to perform DES, random number generation, and modular math functions for RSA and similar public-key cryptographic algorithms.
- Secure code loading that enables updating of the functionality while installed in application systems.
- IBM Common Cryptographic Architecture (CCA), as well as custom software options.
- OEM and end-user purchase options.

Typical Applications

The IBM Payment Suite e-business applications are designed to exploit the Coprocessor for hardware-based cryptography. This class of application benefits from the strong security characteristics of the Coprocessor in the protection of private keys and the opportunity to off-load computationally intensive RSA cryptographic processing to the Coprocessor.

IBM Vault Registry provides functions for issuing and managing digital certificates. Vault Registry can use the 4758 for secure generation and storage of certification authority encryption keys and for signing certificates with those keys.

Finance industry applications such as PIN generation and verification in automated teller and point-of-sale transaction servers can benefit from the improved performance and the security afforded the long-life PIN generation keys. The CCA Support Program feature includes many services supporting PIN generation, verification, PIN-block format and encryption translation, generation of card verification values, and message authentication services.

Other business applications can access the Coprocessor via the Common Data Security Architecture (CDSA) API or the IBM Common Cryptographic Architecture API. The IBM KeyWorks toolkit provides the CDSA API and a service provider interface to access the Coprocessor. The IBM Communications Manager middleware for Windows NT and OS/2* can use the Coprocessor to protect sensitive traffic in SNA sessions.

Applications that must operate in a high-security environment that provides data confidentiality and/or certainty that the application remains unaltered can take advantage of the secure, programmable computing environment provided by the Coprocessor. For example, postage metering applications run in an environment where the user could benefit from tampering with the data or operation of the process. The IBM 4758 is uniquely qualified to provide a secure and flexible tool to address such challenging applications.

What is a Secure Coprocessor...

A secure coprocessor is a general-purpose computing environment that withstands physical attacks and logical attacks. The device must run the programs that it is supposed to, unaltered. You must be able to (remotely) distinguish between the real device and application, and a clever impersonator. The coprocessor must remain secure even if adversaries carry out destructive analysis of one or more devices.

Many servers operate in distributed environments where it is difficult or impossible to provide complete physical security for sensitive processing. And, in some applications, the motivated adversary is the end user. You need a device that you can trust even though you cannot control its environment.

Cryptography is an essential tool in secure processing. When your application must communicate with other distributed elements, or assert or ascertain the validity of data it is processing, you will find cryptography is an essential tool.

The FIPS PUB 140-1 certification declares that the IBM 4758 is uniquely qualified to detect attempted attacks, and to perform processing securely, including correct implementations of several commercially significant cryptographic algorithms.

FIPS PUB 140-1 Standard and the IBM 4758

Federal Information Processing Standard (FIPS) PUB 140-1, *Security Requirements for Cryptographic Modules*, is available from the US Government at http://csrc.nist.gov/cryptval/140-1.htm. This standard, its test requirements, and the independent validation program which is overseen by the US National Institute of Technology, is widely recognized as *the* benchmark for evaluating the security characteristics of commercial cryptographic devices. Generally, other standardized evaluations (e.g., ITSEC) focus less on the hardware characteristics of a device as compared to the FIPS PUB 140-1 standard. The standard is the basis for evaluating cryptographic implementations used to protect unclassified US government information and systems. The standard is used directly, or paraphrased, by many other organizations in many parts of the world.

FIPS PUB 140-1 defines four levels of security for cryptographic devices. Figure 1-1 is a simplified definition of these levels. A higher level must meet the requirements of the lower levels. You may wish to review the standard for a more complete understanding. The IBM 4758 hardware and the low-level software shipped in the product from the factory are certified under the FIPS standard as indicated in the table.

Figure 1-1. FIPS PUB 140-1 Security Levels and the IBM 4758 Models

FIPS 140-1 Level	IBM 4758 Model	Simplified Definition
1		A certified implementation correctly performs recognized algorithms. Software-only implementations can meet this level.
2		Both software and hardware implementations can meet this level. Hardware must incorporate a limited degree of tamper-evident design or employ locks to secure sensitive information. Role-based authentication is required to authorize a defined set of services.
3	013	This level requires a hardware implementation, and the hardware must be designed to prevent an intruder from obtaining secrets from the device. Detected tampering must result in zeroization of critical information.
4	001	Hardware certified at this level must resist the most sophisticated attacks. Cryptographic functions are performed within an “envelope” protected by advanced mechanisms which, if breached, will result in zeroization of the security parameters. Such devices are suitable for operation in physically unprotected environments.
A numerically higher level must meet the requirements of all lower levels.		

The IBM 4758 Model 001 is one of a very few devices to be certified at the rigorous FIPS PUB 140-1, level 4. Certification requires an evaluation conducted by a qualified and approved independent third party. High-level PKI certification authorities and/or applications where the cryptographic equipment is subject to attack by skilled adversaries should consider level 4 devices.

The IBM 4758 Model 013 device can be transported in a wider temperature range and employs a more economical approach to protecting internal sensitive information than the Model 001. This model is certified at level 3 and is suitable in a broad range of applications where the equipment is less subject to tampering attacks and/or the impact of loss is less far reaching.

Both models provide the same cryptographic functionality and secure processing capabilities.

Security Functions Overview

The Coprocessor hardware and software, further described in subsequent chapters, cooperate to provide capabilities listed next. With custom software, you or other vendors can extend these capabilities.

- Accept only certified software to assure processing integrity
- Secure storage of data up to two megabytes
- Triple-DES encryption of keys and financial PIN blocks
- 56-bit DES general data encryption through a pipelined DES engine at speeds up to 22.5 megabytes per second
- RSA key generation and private and public key operations for keys up to 2048 bits in length
- 1024-bit modular math hardware to support RSA and DSA algorithms
- Hardware noise source to seed random number generation
- Random number generation certified under FIPS PUB 140-1

- Sophisticated DES-based key management system supporting distributed systems
- RSA-based key management
- Finance industry cryptographic processing
  - Data encryption
  - Message authentication code (MAC) generation and verification
  - PIN generation using several algorithms
  - PIN block verification and translation for several PIN-block formats
  - Card verification value / code (CVV, CVC) generation and verification
  - Secure Electronic Transaction** (SET) support
  - Diversified key generation for support of smart card initialization, personalization, and transaction processing.
- Secure clock-calendar
- Embedded software replacement without the need to remove the Coprocessor from its operating environment
- Signed responses to enable remote assurance of the integrity and status of the Coprocessor and its software.

Obtaining Information and Ordering the Coprocessor

Information about the IBM 4758 PCI Cryptographic Coprocessor can be found on a Web site at *http://www.ibm.com/security/cryptocards*. On this site you will find current news about the product, periodic education announcements, a product description, and the product-ordering process. In the library pages you will find papers and all of the generally available product publications. The publications are available for download in Adobe PDF format. You may wish to periodically revisit this site for late-breaking news.

The IBM 4758 PCI Cryptographic Coprocessor can generally be ordered through IBM's sales representatives. In the United States and in Canada the product can also be ordered through IBM Direct, 1-800-IBM-CALL. When calling IBM Direct, please reference the IBM 4758 so that you will be connected to an IBM 4758 product specialist. Customers in the USA who are interested in establishing an OEM relationship should call 1-800-IBM-OEMS. AS/400 users should visit the AS/400 Web site, see *http://www.as400.ibm.com/*.

The product web site provides a complete step-by-step process for ordering the hardware and downloading the software. There are unusual steps that a customer must take to obtain a License Key to decrypt the software delivered over the Internet. This extra process relates to cryptographic-shipment reports required by the regulations of several countries, including the USA.

Subsequent chapters in this book provide additional detail about:

- Coprocessor hardware
- CCA support program feature
- Custom software development and the embedded operating system.

Chapter 2. IBM 4758 PCI Cryptographic Coprocessor Hardware

This chapter describes:

- The Coprocessor board and its components
- Physical and environmental specifications
- The low-level software shipped with the product.

The IBM 4758 is a secure, programmable subsystem mounted on a board that you can plug into systems that support the PCI Version 2.1 bus. The subsystem provides electronics for random number generation, 56-bit DES and 1024-bit modular arithmetic processing, several memory technologies enabling secure data storage, an Intel** 80486 compatible computer, and tamper sensors to detect attacks which, if activated, quickly zeroize data and render stored data indecipherable.

The IBM 4758 hardware and software described in this chapter have been evaluated and certified under the FIPS 140-1 standard.

Optional IBM Common Cryptographic Architecture (CCA) software and toolkits are described in subsequent chapters.

Coprocessor Board

The Coprocessor, depicted in Figure 2-1, consists of a two-thirds length PCI Version 2.1 *bus board* on which are mounted a self-contained *cryptographic coprocessor*, two battery holders and batteries for standby power, and a mounting bracket with a 9-pin RS-232 port connector. The cryptographic coprocessor is a separate electronic subassembly mounted within a steel enclosure on the bus board.

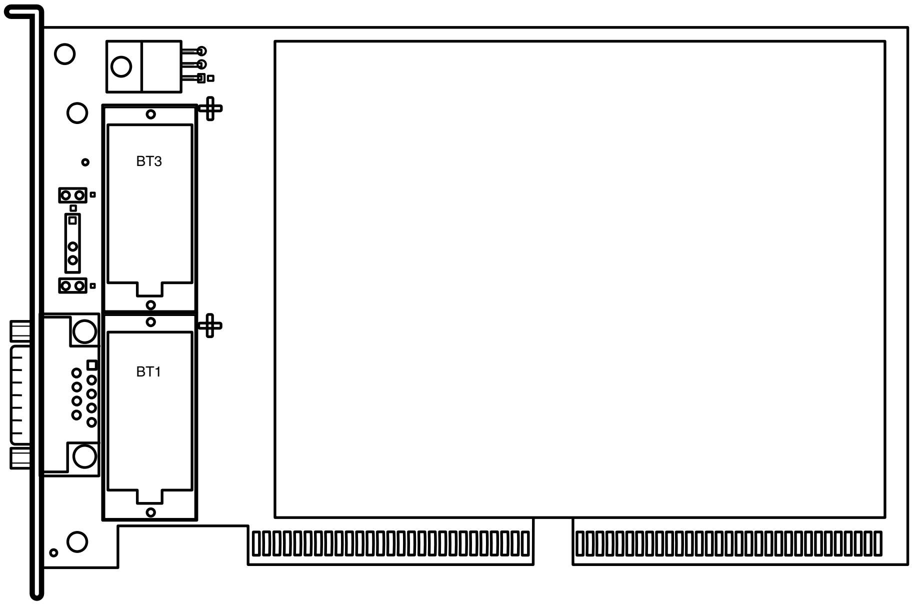

Figure 2-1. The IBM 4758 PCI Cryptographic Coprocessor

The cryptographic coprocessor subsystem, shown schematically in Figure 2-2 on page 2-3, consists of these principle elements:

Security Enclosure Except for the PCI bus interface processor chip, the Coprocessor electronics are contained within a sealed steel enclosure. The Model 001 and Model 013 differ in the approach to physical penetration detection. The FIPS level 4 rated Model 001 surrounds the internal electronics with a polyurethane mixture and a film with an imprinted circuit pattern to detect minute penetration and erosion attacks. The FIPS level 3 rated Model 013 employs an electrical circuit connected to the steel case fasteners to detect attempts at opening the case.

Tamper Detection Sensors Other sensors on both models detect high and low temperatures, radiation (Model 001 only), and abnormal power sequencing.

The sensors are continuously powered from the time of factory initialization and certification to the end of productive life of the Coprocessor. Any sensor-detected tamper event causes immediate power loss to the battery-backed RAM resulting in zeroization of this memory, and a subsystem reset resulting in a processor shutdown and the end of RAM-memory refresh cycles. The result is the immediate destruction of any sensitive data stored in these memories and the CPU.

Central Processing Unit, CPU A 66MHz 486-class processor provides an industry-standard computing environment for flexible control of secure processing and cryptographic algorithms and processes.

PCI Bus Interface Processor Chip This chip couples the secured electronics to the PCI bus and provides for busmaster operation and inbound and outbound DMA operations between the FIFO buffers and the host system memory. The chip also provides mailboxes and interrupts to permit the exchange of control information between the Coprocessor and the host-system Coprocessor device driver.

Internal Bus The internal 32-bit bus connects the CPU to the components listed below and supports bi-directional DMA operations to both of the FIFO buffers.

FIFO Buffers The first-in, first-out buffers connect to the internal and external DMA channels and to the DES engine. An internal device driver directs the flow of data in conjunction with the host system device driver. High bulk transfer rates are supported. The buffers smooth the flow rate of data and support asynchronism between the connected components.

DES Engine The DES engine employs a single 56-bit key and supports DES processing at sustained rates up to 22.5 megabytes per second. Because of the need to inject a key under control of the subsystem software, to setup the FIFO buffer connection controls, and to initialize the DMA controllers, throughput is sensitive to the block size to be processed and to the host system design and load. See the performance information available on the product Web site.

Random Number Generator An electronic noise source provides unpredictable input to a random bit-value accumulator.

Large-Integer Modular Arithmetic Processor A 1024-bit wide modular-arithmetic processor supports the processing that is the basis of cryptographic algorithms such as RSA, Diffie-Hellman, and DSA. IBM provides software that exploits this hardware for keys up to 2048 bits in length.

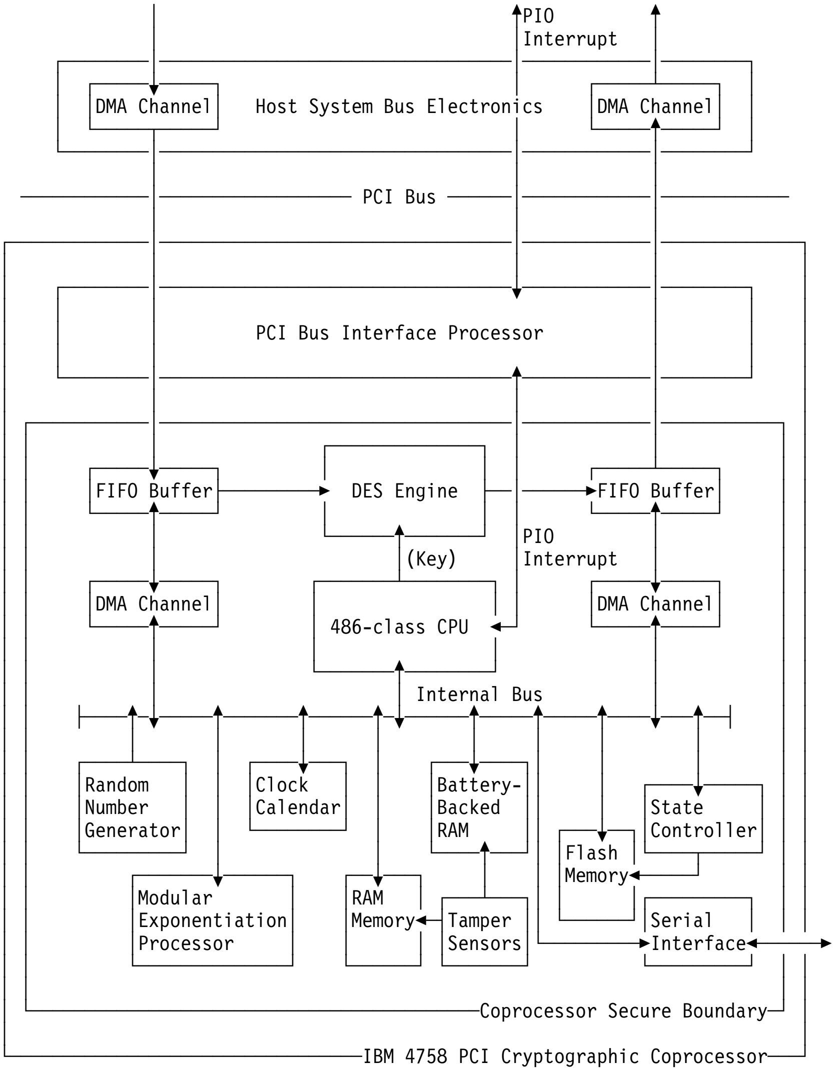

Figure 2-2. IBM 4758 Cryptographic Coprocessor Schematic

Clock Calendar A time and date source accurate to one minute per month provides an internal time value that is under the exclusive control of software running on the subsystem.

State Controller The state controller's software and function is fixed at the time of manufacture. Outputs from this controller are combined with battery-backed RAM and flash memory addressing requests to control when portions of those memories are available to programs running in the Coprocessor CPU. The state controller moves through a carefully architected, FIPS-certified arrangement of states to enforce a strong security policy. The low-level bootstrap software in the CPU can request state changes while the actual changes affecting memory access are administered by the state controller. For additional information about the security design that incorporates the controller, see Research Report RC 21102, *Building a High-Performance, Programmable Secure Coprocessor* that is available on the Library page of the product Web site.

RAM Memory Four megabytes of memory is available for the use of subsystem software and data storage.

Flash Memory Two megabytes of electrically erasable, persistent-data memory are incorporated in the design. IBM provides software to selectively encrypt sensitive data stored in flash memory. The encryption keys used for this are stored in battery-backed RAM and are zeroized in the event of a detected tamper event.

Two 256K segments in the flash memory are alternately used to store diagnostic and bootstrap software and control data. The state controller and the unique memory addressing electronics ensure the availability of a valid bootstrap copy. Any bootstrap replacement is written to the “inactive” segment. Once the new content is validated, a latch is flipped and the just-validated segment contents become the active segment. This instantaneous change insures that reloading of the low-level control software can be interrupted at any point without affecting the continued availability of the device.

The next two 256K byte segments in the flash memory are reserved for an embedded operating system and an application program. Loading and access to these two segments is controlled by the bootstrap software operating in conjunction with the state controller and is part of the FIPS-certified security policy enforcement mechanism.

Battery-backed Random Access Memory (BBRAM) Eight kilobytes (8K) of battery-backed RAM is incorporated in the Coprocessor. Access to portions of this memory is also controlled by the state controller and unique memory addressing electronics. This enforces parts of the security policy rendering portions of this memory unaddressable by the CPU software in selected system states. The actions of a malicious embedded operating system or application program cannot affect reserved portions of the BBRAM.

RS-232 Serial Interface An RS-232 serial interface communications port is provided as an alternative interface to the PCI bus. During routine bootstrap processing, codes are emitted indicating the progress of the start-up process. Once control is transferred from the low-level bootstrap software (i.e., to the embedded operating system), the port could be enabled for application purposes.

Batteries In the absence of power delivered over the PCI interface, two batteries power the tamper sensor electronics and battery-backed RAM memory. In projected usage in server systems, power will rarely be drained from the batteries. In this case, battery shelf-life becomes important. If the Coprocessor is stored for long periods without external power, a fresh battery should maintain the battery-backed RAM contents and tamper sensors for more than three years. Two batteries are provided for redundancy. In most applications, the batteries should be changed every few years as part of a customer-managed, planned maintenance cycle.

The batteries are a commercially available item. IBM offers an optional kit that includes replacement batteries and an auxiliary battery holder that can be connected and used during the battery replacement process. (If you remove all battery power and system power, the Coprocessor will zeroize and become non-functional.) The battery replacement process is described in the *IBM 4758 PCI Cryptographic Coprocessor Installation Manual*.

Physical Characteristics and Environmental Specifications

Figure 2-3 provides many of the physical characteristics and environmental specifications of the IBM 4758 Coprocessor.

Figure 2-3. IBM 4758 Physical and Environmental Specifications

Characteristic	IBM 4758 Model 1	IBM 4758 Model 13
FIPS 140-1 certification level	4	3
CPU speed	66MHz	66MHz
RAM size	4MB	4MB
Flash memory size	2x1MB	2x1MB
Battery-backed RAM size	8KB	8KB
PCI Bus	2.1, 2/3 length, 5v Minimum of 100 insertions	2.1, 2/3 length, 5v Minimum of 100 insertions
Power	+5.0VDC ±5% +12VDC ±5%	+5.0VDC ±5% +12VDC ±5%
Temperature, shipping	-15°C to 65°C	-15°C to 60°C
Temperature, storage	10°C to 65°C	1°C (one) to 60°C
Temperature, operating	10°C to 40°C	10°C to 40°C
Relative humidity, shipping	5% to 100%	5% to 100%
Relative humidity, storage	5% to 80%	5% to 80%
Relative humidity, operating	8% to 80%	8% to 80%
Pressure, shipping	500mbar, minimum 1039mbar, maximum	not specified
Pressure, storage	700mbar, minimum 1039mbar, maximum	not specified
Pressure, operating	768mbar, minimum 1039mbar, maximum	768mbar, minimum 1039mbar, maximum

Notes:

1. -15°C=5°F, 1°C=34°F, 10°C=50°F, 40°C=104°F, 60°C=140°F. 65°C=149°F. MHz: Megahertz; MB: Megabytes; KB: Kilobytes.
2. Shipping condition specifications apply when the product is transported in its original IBM packaging.

Low-level Bootstrap and Diagnostic Software

When purchased from IBM, the Coprocessor contains diagnostic and bootstrap software already loaded in flash memory. With a reset signal, from the PCI bus or from a software-initiated reset, the CPU performs diagnostic Power-On Self-Test (POST) routines in flash memory segments 0 and 1. (Flash memory segment 0 is a small portion of the flash written at the factory and rendered unalterable.) With successful completion of POST, control passes to the bootstrap routines (“miniboot”).

The content of segments 0 and 1 is written during Coprocessor manufacture with the state controller signaling factory initialization. Several one-time processes occur including generation of a (RSA) *device-key* pair, assignment of a guaranteed-unique serial number, and recording of part numbers and identifying description. The factory process uses a factory key to certify the public device key, device serial number, and description. The resulting certificate is returned to the Coprocessor. A public key is also installed and used later to validate a digital signature on any replacement software for segment 1, for assigning “ownership” of segment 2, and for validating a digital signature on a “segment 2 public key.” With a successful conclusion of the one-time factory processes, the bootstrap software signals the state controller to move beyond the factory initialization state, a state which is not re-enterable[1].

After state changes, the Coprocessor initiates a reset sequence causing the POST routines to test the hardware and the bootstrap to confirm state information that it manages. The bootstrap routines then will honor requests for status information, segment ownership assignment, and the loading of code into segments 2 and 3. Status information, which includes the device serial number, state information, and ownership and software content of segments 1, 2, and 3, and a nonce provided by the status requestor, is signed by the device private key. The validity of the status response can be confirmed using the device certificate and a factory-key certificate-chain that IBM provides. Such confirmation can be performed locally or remotely, and at the time of the status request or later as your security needs dictate.

As initialized by IBM, the segment 0 and segment 1 software, and therefore the Coprocessor, perform no “application-useful” cryptographic function. To use the Coprocessor's secure computing environment and/or latent cryptographic capabilities, software must be introduced into segment 2 and normally also into segment 3. The standard IBM 4758 is sold by IBM without software resident in segments 2 or 3. (No-charge software is available as described later in this manual.)

Code intended for segments 1, 2, and 3 must be digitally signed. The bootstrap routines use public keys retained within the Coprocessor to validate commands and software-loading requests. The bootstrap software accepts *ownership codes* assigned by IBM for segment 2. Associated with assigning an ownership code, IBM can certify code-load validating public keys and digitally sign the command to assign a specific ownership code. Besides performing this service for IBM developers, IBM will assign ownership codes and sign keys for other vendors subject to custom contracts and subject to US Government cryptographic-implementation export regulations.

Loading code into segment 2 requires an IBM-signed *establish segment 2 ownership* command incorporating an ownership code assigned by IBM. The developer of the segment 2 code prepares a command that incorporates:

- His ownership identifier
- A certificate for his code-signing public key that can be validated by the public key saved within the Coprocessor segment 1 control information

[1] If the device is “tampered,” several primitive states, including the factory initialization state, can be entered. However, because IBM cannot determine what changes might have been made to such a device, as a business policy IBM will not employ the special keys needed to re-enter the primitive states and reclaim the device. In any case, these primitive states cause the complete destruction of any information remaining within the Coprocessor. These states and processes are also certified under the FIPS 140-1 standard.

- His code-load digitally signed and verifiable by his public key contained within the certificate.

The Coprocessor bootstrap routines process a segment 2 code-loading request by first validating the ownership assignment request and recording the new ownership of segment 2. (A state change occurs which initiates a reset sequence.) The bootstrap validates the load-code request by checking the certificate digital signature and matching the ownership code, and then using that now-trusted public key, validating the digital signature over the code. Note that this strategy does not require IBM to ever have access to the code actually loaded into segment 2. Thus another vendor can provide code for segment 2.

Loading of code into segment 3 follows the same pattern, replace 2 by 3 and 1 by 2. The owner of segment 2 must administer the segment 3 ownership identifiers and sign the segment 3 ownership command and certify the segment 3 code-validating public key. Again, the segment 2 party needs never have access to the actual segment 3 code.

There are additional controls that can be invoked during the code loading processes to enforce additional security policy considerations. Among these are the possibility of signing a request specific to one serial number. Only the device with that serial number will honor the request.

To further explore the code loading possibilities and the software environment, review the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Developer's Toolkit Guide* that you can download from the Custom Software page reached from the Library page on the product Web site.

IBM provides an embedded operating system, CP/Q^{++}, for loading into segment 2, that provides access to all of the cryptographic capabilities of the Coprocessor. IBM also provides, under custom contract, a toolkit for exploiting the operating system, and developing and debugging segment 3 applications. See Chapter 4, "IBM 4758 Custom Software Development."

In summary, the IBM 4758 PCI Cryptographic Coprocessor provides a high-security platform on which to deploy security-sensitive processing. With the specialized electronics that enhance the performance of DES, RSA, and DSA cryptography, and in conjunction with IBM's software offerings and related products, end-users and other-vendor application developers can exploit this independently validated and FIPS 140-1 certified product with confidence in its security features.

Chapter 3. IBM 4758 CCA Support Program

The IBM Common Cryptographic Architecture (CCA) defines an application program interface (API) and an architected set of DES- and RSA-based cryptographic services. The IBM 4758 CCA Support Program provides an implementation of the CCA architecture for use with the IBM 4758 Coprocessor. The CCA services are available to application programs that you create or purchase through an API that is substantially the same for several IBM systems which implement the CCA architecture.

This chapter describes the IBM 4758 CCA Support Program which is an optional, no-charge software feature for the Coprocessor. A subsequent chapter describes tools that you can use to extend the CCA Support Program and/or to create an alternative application.

IBM believes the implementation of the software described in this chapter complies with the intent of cryptographic module standards such as FIPS PUB 140-1 and finance industry cryptographic system requirements as promulgated by the German ZKA.

Information in this chapter includes:

- CCA Support Program overview, description, and requirements
- Ordering information.

Overview

The IBM 4758 CCA Support Program optional feature for the Coprocessor provides host-system software and Coprocessor software that implement the IBM Common Cryptographic Architecture (CCA). Features of the software include:

- **Standards-Based Cryptographic Services** such as encryption and message authentication, digital signatures and hashing, random-number generation, PIN generation and verification techniques, and support for Secure Electronic Transaction (SET) cryptographic functions.
- **Host System Support** on selected IBM RS/6000 systems with AIX, and on personal computers running Windows NT and IBM OS/2 Warp, Warp Server, and Warp Server SMP. Support on specific RS/6000 models requires an enabling RPQ.
- **Role-Based Access Control System** that permits differing levels of function based on logons of individuals or applications.
- **Application Interface Supports Common Development** since essentially the same API is available on OS/2, Windows NT, AIX, OS/400, and S/390 platforms.
- **Flexibility to Meet Unique Requirements** by employing toolkits to extend the function provided with the IBM implementation (see Chapter 4, "IBM 4758 Custom Software Development").
- **A growth path** for users of the IBM Transaction Security System products.

Description

The IBM 4758 CCA Support Program exploits the full capabilities of the PCI Cryptographic Coprocessor hardware to furnish services, including:

- 56-bit DES encryption and decryption with support for CBC and ANSI X9.23 last-block processing
- ANSI X9.9-1 and X9.19 single-DES and triple-DES MAC generation and verification
- Hashing using the SHA-1 and MD5[1] algorithms
- RSA signature generation and verification, with signatures formatted according to ISO 9796, PKCS #1.0, and PKCS #1.1 rules.
- Extensive key management options...
  - Triple-length master key encrypts working keys permitting an unlimited number of DES and RSA working keys
  - DES key management functions that permit secure generation of keys under the Coprocessor's master key
  - Import and export of DES keys using double-length DES key-encrypting keys with control-vector-based key typing to securely control the use of a key in distributed systems
  - Import and export of DES data keys using RSA with PKCS #1.2 formatting
  - Generation and importation of double-length key-encrypting transport keys using advanced RSA key encryption techniques
  - Generation of RSA key pairs with modulus lengths as long as 2048 bits
- Secure Electronic Transaction (SET) support for Internet commerce processing at banks and merchants
- PIN generation and verification with support for many PIN-block formats and PIN algorithms
- PIN-block re-encryption with optional PIN-block-format changes
- Generation and verification of Card Verification Codes/Values
- Diversified key generation for use with smart card initialization processes.

The supported CCA services generally conform to services offered with other IBM CCA products. For a complete description of the services offered by the IBM 4758 CCA Support Program, refer to the *IBM 4758 CCA Basic Services Reference and Guide*, which is available in PDF format from the Library page of the product web site, *http://www.ibm.com/security/cryptocards*. Ordering, installation, and operation is described in the *IBM 4758 PCI Cryptographic Coprocessor CCA Support Program Installation Manual* on the web site.

The API is supported for use by applications written in C. Both IBM VisualAge C++ and Microsoft C++ tools can be used to interface your C-language application to the API. Calls from multiple processes and from multiple threads within a process are supported. The API is thread safe.

You can order the support program for use with IBM's AIX operating system for RS/6000 machines, or for Windows NT or IBM OS/2 personal computers. The support program functions in the same manner in each environment.

Note: Use of the IBM 4758 on RS/6000 models requires an enabling RPQ.

[1] PKCS standards and the MD5 hashing algorithm (see RFC 1321) are developments of RSA Data Security, Incorporated.

Several IBM applications specifically support use of the IBM 4758 and the IBM 4758 CCA Support Program, including:

- IBM Payment Gateway for coupling SET e-Commerce transactions into traditional POS systems
- IBM Payment Registry for issuing certificates for the SET environment
- IBM Vault Registry serving as the basis of certification authority implementations
- IBM Communications Server on Windows NT and IBM OS/2 for support of SNA session-level encryption.

Export-Controlled Cryptographic Function satisfies governmental export and import control requirements; the CCA Support Program uses a *function-control vector* to specify the cryptographic capabilities of the CCA application within the Coprocessor. Certain functions are not exportable to a few geographic locations due to government regulations. The applicable regulations of the United States are changing soon after publication of this manual. Be sure to check the product web site and also check with IBM's export/import regulation coordination personnel in your country.

Requirements and Specifications

Software Requirements: At the time of publication, IBM supplies the support program at Version 1, Release 31 (1.31) with additional, optional fixes (see the web site). For IBM 4758 Model 001 and Model 013 PCI Cryptographic Coprocessors:

- Installed in an RS/6000 machine:
  - AIX Version 4.1.5, or later and
    Java runtime environment 1.1.2 through 1.1.6; the product is tested with the JDK available from http://www.ibm.com/java/jdk/download.
- Installed in a PC:
  - IBM OS/2 Warp, Version 4.0, or OS/2 Warp 4.0 Server, or OS/2 Warp 4.0 Server SMP, and
    Java runtime environment 1.1.1 through 1.1.7; the product is tested with the JDK available from http://www.ibm.com/java/jdk/download
  - Windows NT, Version 4.0 or later, and
    Java runtime environment 1.1.2 through 1.2; the product is tested with the JDK available from http://java.sun.com/products/OV_jdkProduct.html.

Ordering Information

This section explains how to order the PCI Cryptographic Coprocessor, and how to select the appropriate IBM 4758 CCA Support Program feature codes. This information is also available on the product web site where you should check for updated information.

Note: The IBM 4758 CCA Support Program requires an IBM 4758 Coprocessor,, and the Coprocessor cannot function without software such as the CCA Support Program (or software from another vendor). Before ordering the Coprocessor, review the following list to choose the features you need:

1. From the table below, choose the Coprocessor and the (optional) Battery Kit:

Description	Machine	Model	Feature
PCI Cryptographic Coprocessor FIPS 140-1, level 4	4758	001	
PCI Cryptographic Coprocessor FIPS 140-1, level 3	4758	013	
Replacement Battery Kit The battery kit contains two batteries and a temporary-battery tray. (Batteries require replacement after three or more years. When replacing batteries, be sure they are fresh and of recent manufacture.)			1008

2. From the table below, choose the IBM 4758 CCA Support Program feature codes that support your operating systems:

Support Program	Feature
for AIX; support on specific models requires an RPQ	4374
for OS/2	4372
for Windows NT	4376

3. As permitted by import and export regulations, choose **one** function-control vector from the table below. The function-control vector specifies the level of cryptographic support offered by the software; the permissible support varies according to government regulations.

Function-Control Vector (FCV)	Feature
56-bit DES and 40-bit IBM Commercial Data Masking Facility (CDMF), 1024-bit RSA symmetric-key management, and SET. This FCV is normally available to all customers in the United States and Canada, and to financial institutions outside of the USA and Canada. The applicable regulations are undergoing revision with this level of functionality likely to be available to most customers worldwide. Ask for advice when ordering.	5200
DES and CDMF, 512-bit RSA symmetric-key management, and SET. This FCV is generally available to customers outside of the United States and Canada.	5201
CDMF, 512-bit RSA symmetric-key management, and SET CDMF is a DES-based, 40-bit algorithm.	5202

An IBM export-regulation coordinator can help you determine the limitations that apply to you, and help you apply for an exception to the standard practice if you need one.

For the latest listing of function-control vectors available, refer to the product Web site at *http://www.ibm.com/security/cryptocards*.

Chapter 4. IBM 4758 Custom Software Development

Two toolkits have been created to enable you to create, sign, load, debug, and release application programs that perform within segment 3 of the IBM 4758 PCI Cryptographic Coprocessor. The toolkits are obtainable from IBM under custom contracts. The contracts normally provide education, post-education telephone support, licenses for the toolkits, and certification of your code-signing public keys enabling loading of your software into a Coprocessor. Often the contracts provide for consulting and application prototyping IBM can also perform works-for-hire, may enter into joint development activities with you, or undertake joint research studies.

The toolkits enable you to implement a variety of cryptographic capabilities within the IBM 4758. You can implement new algorithms and processes in the Coprocessor with the certainty that your object code can neither be observed while running, nor changed, by adversaries. Several megabytes of persistent storage are available for the secure storage of your information. And you can adopt or extend CCA-like techniques to encrypt working data under a master key for external storage. You can also use the secure operating environment for performing highly sensitive operations such as “minting” electronic money or postage.

With the toolkits you can potentially implement new and very strong cryptographic processes. Therefore, the toolkits are subject to USA export regulations. Obtaining export licenses minimally requires 60 to 90 days and the granting of licenses is never a certainty.

You develop your Coprocessor application in C using either IBM VisualAge or Microsoft** tools. Development and debug is supported on a Windows NT platform. Under contract, IBM will extend the basic toolkit to support debugging your application when the Coprocessor is operating in an RS/6000 machine running AIX or on a personal computer running OS/2.

IBM provides an embedded control program, CP/Q++, for loading into segment 2. (Segments are described in “Low-level Bootstrap and Diagnostic Software” on page 2-5.) CP/Q is a proprietary control program developed by IBM for use in Intel architecture and PowerPC* systems. It has been deployed as an embedded operating system in various IBM products since the mid 1980's. CP/Q++ is the designation applied when CP/Q is configured for use in an IBM 4758 and incorporates device drivers to access the hardware of the IBM 4758. The control program is based on modern micro kernel concepts and provides memory management, multi-tasking and task synchronization, a C-language library, etc.

Information about CP/Q, CP/Q++, and the toolkits can be found in the custom software publications available as PDF files on the IBM 4758 product web site, *http://www.ibm.com/security/cryptocards*. Go to the Library page and then to the Custom Software page. Begin your exploration of the toolkits and CP/Q by first reviewing the *IBM 4758 PCI Cryptographic Coprocessor Custom Software Developer’s Toolkit Guide* publication.

IBM is currently engaged in a review of CP/Q++ operating in segment 2. IBM has implemented the CP/Q++ services and environment in a manner that it believes, at a minimum, complies with FIPS 140-1 level 3.

Two toolkits are available. The first toolkit supports the development of any segment 3 application. The second toolkit supports extending the IBM CCA implementation incorporated in the IBM 4758 CCA Support Program.

- **Custom Software Development Toolkit for the IBM 4758**
  You use this toolkit in the preparation of applications that run in segment 3 of the IBM 4758. The toolkit provides the host-system device driver, code signing, packaging and loading utility programs, and a modern source level debug aid. Libraries to access the host device driver and CP/Q^{++} within the Coprocessor are included.
- **CCA User Extensions Software Development Toolkit for the IBM 4758**
  You use this toolkit to extend the functionality of the IBM CCA segment 3 Coprocessor application. The toolkit also provides the means for you to create a host-system application programming API consistent with CCA and to use the CCA Support Program infrastructure to convey service requests to your functions within the Coprocessor. You have access to both CCA subroutines within the Coprocessor and to the full CP/Q^{++} API. You use this toolkit with the previous toolkit.

To inquire further into the toolkits, you should review some of the custom software manuals on the product web site. To contact IBM concerning availability of the toolkits, submit a request for information with the Question form that you can locate from the Support page of the IBM 4758 product web site, *http://www.ibm.com/security/cryptocards*.

The Coprocessor represents a specialized programming environment with its own tools, debug aids, and code release procedures. Rather than learn to create applications for this specialized environment, customers can obtain custom programming services through an experienced IBM Global Services department or selected contractors. For developers who anticipate creating a single, fixed solution, it can be beneficial to contract for IBM services or those of an experienced Coprocessor software developer in the preparation of your application. IBM is pleased to jointly develop specifications and quote on custom solutions.

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:

- 3090
- ACF/VTAM
- AIX
- AIX/6000
- Application System/400
- AS/400
- CICS
- Enterprise System/3090
- Enterprise System/9000
- Enterprise System/9370
- ES/3090
- ES/9000
- ES/9370
- IBM
- IBM net.commerce
- IBM World Registry
- Micro Channel
- Operating System/2
- OS/2
- Operating System/400
- OS/400
- Personal Security
- Personal System/2
- PS/2
- PS/ValuePoint
- POWERserver
- POWERstation
- RACF
- RS/6000
- SecureWay
- System/360
- System/370
- System/390
- S/390 G3 Enterprise Server
- S/390 Multiprise
- Systems Application Architecture

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

Acrobat Reader	Adobe Systems, Inc.
Java	Sun Microsystems
MASTERCARD	MasterCard International, Incorporated
Microsoft	Microsoft Corporation
SET	SET Secure Electronic Transaction, LLC
Secure Electronic Transaction	
RSA	RSA Data Security, Inc.
UNIX	UNIX Systems Laboratories, Incorporated
VISA	VISA International Service Association
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
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
CVC	card verification code
CVV	card verification value
DEA	data encryption algorithm
DES	data encryption standard
DMA	direct memory access
DSA	digital signature algorithm
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
ITSEC	information technology security evaluation criteria
MB	megabyte
mbar	millibar
MAC	message authentication code
MBps	megabytes per second
MD5	message digest 5 (hashing algorithm)
MDC	modification detection code
MHz	megahertz
mm	millimeter
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
PKI	public key infrastructure
POST	power-on self-test
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
SET	secure electronic transaction
SNA	systems network architecture
SVC	supervisor call
TOD	time of day (clock)
V	volt
VDC	volts direct current
ZKA	*Zentraler Kreditausschuss* German central credit control committee of banks

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) after 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) after 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) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.

A

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

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)

Application System/400 (AS/400) system. One of a family of general purpose midrange systems with a single operating system, Operating System/400, that provides application portability across all models.

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) 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

BBRAM. A type of RAM storage powered by a system and by a battery for persistent data storage

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

C

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

CDMF algorithm. An alternate algorithm for data confidentiality applications, based on the DES algorithm and possessing 40-bit key strength.

ciphertext. (1) Text that results from the encipherment of plaintext. (2) See also *plaintext*.

Cipher Block Chaining (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 programming interface that is described in the *IBM 4758 CCA Basic Services Reference and Guide*.

control vector. 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.

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 networking coprocessor.

cryptographic coprocessor (4758). An expansion card that provides a comprehensive set of cryptographic functions for a workstation.

cryptography. The transformation of data to conceal its meaning.

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 8 bits are used for parity checking.

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) Synonym for *decrypt*. (3) Contrast with *encipher*.

decrypt. (1) Synonym for *decipher*. Contrast with *encrypt*.

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

E

Electronic CodeBook (ECB) Operation. 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.

encipher. (1) To scramble data or to convert data to a secret code that masks the meaning of the data. (2) Synonym for *encrypt*. (3) Contrast with *decipher*.

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

encrypt. (1) To convert cleartext into ciphertext. (2) Synonym for *encipher*. (T) (3) Contrast with *decrypt*.

Erasable Programmable Read-Only Memory (EPROM). A PROM that can be erased by a special process and then reused. (T)

F

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

Federal Communications Commission (FCC). A board of commissioners, appointed by the President under the Communications Act of 1934, having the power to regulate all interstate and foreign communications by wire and radio originating in the United States.

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

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.

I

Integrated Cryptographic Service Facility (ICSF). An IBM-licensed program that supports the cryptographic hardware feature for the high-end System/390 processor in an MVS environment.

interface. (1) A shared boundary between two functional units, 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 develop 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 encrypt or decrypt data.

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

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

key token. In CCA products, data structure that can contain a cryptographic key, a control vector, and other information related to the key.

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 Chaining (CBC) mode of operation, (3) a digital signature code.

N

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

O

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

Operating System/400 (OS/400). An operating system for the IBM Application System/400 computers.

P

password. In computer security, a string of characters known to the computer system and a user; the user must specify it to gain full or limited access to a system and to 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 are run automatically by a device when the 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 decrypt data. The data is encrypted 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 possible parameters.

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

PRPQ. Programming Request for Price Quotation.

public key. (1) In computer security, a key that is widely known and used with a public-key algorithm to encrypt data. The encrypted data can be decrypted 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 encrypt data and a related private key to decrypt data. (2) Contrast with *Data Encryption Algorithm* and *Data Encryption Standard algorithm*. (3) See also *Rivest-Shamir-Adleman algorithm*.

R

Random Access Memory (RAM). (1) A storage device into which data are entered and from which data are retrieved in a non-sequential manner. (2) See also *direct access storage*.

Read-Only Memory (ROM). Memory in which stored data cannot be modified by the user except under special conditions.

Reduced Instruction-Set Computer (RISC). A computer that uses a small, simplified set of frequently-used instructions for rapid processing.

Rivest-Shamir-Adleman (RSA) algorithm. A process for public-key cryptography that was developed by R. Rivest, A. Shamir, and L. Adleman.

RS-232. A specification that defines the interface between data terminal equipment and data circuit-terminating equipment, using serial binary data interchange.

RS-232C. A standard that defines the specific physical, electronic, and functional characteristics of an interface line that uses a 25-pin connector to connect a workstation to a communication device.

RSA algorithm. Rivest-Shamir-Adleman encryption algorithm.

S

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. A string of characters that is treated as a single entity.

U

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

V

verb. A function that has an entry-point name and a fixed-length parameter list. The procedure call for a verb uses the standard syntax of a programming language.

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

4755. IBM 4755 Cryptographic Adapter.

4758. IBM 4758 PCI Cryptographic Coprocessor.

Index

Printed in U.S.A.

GC31-8608-02