Note!

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

---

**Sixth Edition (May 2002)**

This edition applies to:

- IBM 4758 Models 001, 013, 002, and 023
- IBM RPQs 8V1183 and 8V1185
- IBM eServer pSeries features 4958 and 4963
- IBM eServer iSeries features 4801 and 4802
- IBM eServer zSeries features 0865, 0866, and 0869

with information as of May, 2002.

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 Comments and Questions form on 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.

© Copyright International Business Machines Corporation 1997, 2002. All rights reserved.

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.
# Contents

**About This Publication** .................................................. v
Summary of Changes ....................................................... v
Related Publications ....................................................... vi
  IBM 4758 PCI Cryptographic Coprocessor Publications .......... vi
  Other IBM CCA-Product Publications ............................... vii
  Cryptography Publications ........................................... vii

**Chapter 1. Introduction to the IBM 4758 PCI Cryptographic Coprocessor** 1-1
  Highlights ................................................................... 1-2
  Typical Applications ..................................................... 1-2
  What is a Secure Coprocessor... ....................................... 1-3
  FIPS PUB 140-1 Standard and the IBM 4758 ..................... 1-3
  Security Functions Overview ............................................ 1-4
  Obtaining Information and Ordering the Coprocessor ............ 1-5

**Chapter 2. IBM 4758 Hardware** ......................................... 2-1
  Coprocessor Board ....................................................... 2-1
  Low-level Bootstrap and Diagnostic Software ..................... 2-6

**Chapter 3. IBM 4758 CCA Support Program** ............................ 3-1
  Overview ................................................................... 3-1
  Description .................................................................. 3-2
  Requirements and Specifications ...................................... 3-3

**Chapter 4. IBM 4758 PKCS #11 Support Program** ....................... 4-1
  Overview ................................................................... 4-1
  Description .................................................................. 4-2
  Requirements ................................................................ 4-2

**Chapter 5. IBM 4758 Custom Software Development** ..................... 5-1

**Chapter 6. Ordering the IBM PCI Cryptographic Coprocessor** 6-1
  Obtaining the Software .................................................. 6-2

**Appendix A. Notices** ....................................................... A-1
  Copying and Distributing Softcopy Files ............................. A-1
  Trademarks .................................................................. A-2

**List of Abbreviations and Acronyms** .................................... X-1

**Glossary** ........................................................................ X-3

**Index** ............................................................................. X-7
Figures

1-1. FIPS PUB 140-1 Security Levels and the IBM 4758 Models .................. 1-4
2-1. IBM 4758 Physical and Environmental Specifications ..................... 2-2
2-2. IBM 4758 Cryptographic Coprocessor Schematic ............................... 2-3
4-1. Interface Between PKCS #11 and IBM 4758 ..................................... 4-2
6-1. IBM 4758 PCI Cryptographic Coprocessor Ordering Information ........... 6-1
About This Publication

This edition applies to the IBM 4758 Models 002 and 023, IBM RPQs 8V1183 and 8V1185, and to IBM eServer pSeries with feature code 4963, IBM eServer iSeries features 4801 and 4802, IBM eServer zSeries features 0865, 0866, and 0869, all as available in May, 2002. Information is also provided for the IBM 4758 Models 001 and 013, and pSeries feature 4958 which are no longer available. 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 manual contains these chapters:

- Chapter 1, “Introduction to the IBM 4758 PCI Cryptographic Coprocessor,” introduces the IBM 4758 and supporting software available from IBM.
- Chapter 2, “IBM 4758 Hardware,” describes the IBM 4758 hardware and low-level software. The product ordering process and models are described.
- Chapter 4, “IBM 4758 PKCS #11 Support Program,” describes the IBM 4758 PKCS #11 Support Program optional software.
- Chapter 5, “IBM 4758 Custom Software Development,” describes custom programming possibilities and toolkits for the IBM 4758.
- Chapter 6, “Ordering the IBM PCI Cryptographic Coprocessor,” describes the product ordering process.

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

Summary of Changes

The sixth revision of the IBM 4758 PCI Cryptographic Coprocessor General Information Manual contains product information that is current with the IBM PCI Cryptographic Coprocessor products that are shipping in May, 2002, including the 2.41 release of the CCA and the PKCS #11 Support Programs. The change bar at the left indicates changes to the previous version of the manual.

The IBM PCI Cryptographic Coprocessor technology can be purchased from IBM as:

- The IBM 4758, Models 002 and 023, and as RPQs #8V1183 and #8V1185, for use in personal computers and servers including the IBM eServer xSeries products
- Feature number 4963 on IBM eServer pSeries
- Feature numbers 4801 and 4802 on IBM eServer iSeries

© Copyright IBM Corp. 1997, 2002
Feature numbers 0865, 0866, and 0869 on IBM eServer zSeries

Note that IBM 4758 Models 001 and 013 and pSeries feature 4958 are no longer available.

Related Publications

The list below reflects source information regarding the PCI Cryptographic Coprocessor, IBM Common Cryptographic Architecture (CCA) application program interface (API), PKCS #11 Support Program, other IBM CCA products, and cryptography reference information.

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 Adobe Acrobat portable document format (PDF).

General Interest


IBM 4758 Common Cryptographic Architecture (CCA) Support Program

- IBM 4758 CCA Basic Services Reference and Guide.

IBM 4758 PKCS #11 Support Program


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 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
Research Reports Related to the IBM 4758


Other IBM CCA-Product Publications

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

- IBM ICSF/MVS General Information, GC23-0093

Cryptography Publications

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


• 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.


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 1-914-945-3836.
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 IBM PCI Cryptographic Coprocessor is a programmable PCI board 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 Coprocessor technology is offered by IBM as an end-product for use in personal computer machines and as features in IBM eServer pSeries (RS/6000), iSeries (AS/400), and zSeries (S/390) servers.

Using the optional IBM Common Cryptographic Architecture (CCA) Support Program software, the Coprocessor can perform DES and RSA cryptographic functions common in the finance industry and in Internet e-business applications. For use with AIX, Windows NT and Windows 2000, IBM also provides the PKCS #11 Support Program that implements a subset of the Cryptoki 2.01 API. Under custom contracts, you can also purchase consulting, services, and programming toolkits to extend or replace the support program features to perform processing and cryptographic functions to your specification.

The US Government FIPS PUB 140-1 standard, Security Requirements for Cryptographic Modules, is the benchmark standard by which commercial cryptographic implementations are measured. The IBM 4758 Models 001 and 002 are certified under the FIPS PUB 140-1 level four standard, the highest security classification for a commercial cryptographic device. The Models 013 and 023 are certified at level three under the standard. Models 002 and 023 are similar in all respects to each other except in their detection of physical penetration attacks. Devices certified at level three are suitable for many applications while devices certified at level four provide the highest assurance of tamper detection.

The Coprocessors plug into industry-standard PCI slots in personal computers and IBM eServer iSeries, pSeries, xSeries, and zSeries, and other systems that support the PCI bus. Variations of the Coprocessors support 5 volt and 3.3 volt buses.

The Coprocessor secure processing environment contains a 486-compatible microprocessor, custom hardware to perform SHA-1, 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.
Highlights

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, triple-DES, SHA-1, random number generation, and modular math functions for RSA and similar public-key cryptographic algorithms.
- Secure code loading that enables updating of the software with the Coprocessor installed in application systems.
- IBM Common Cryptographic Architecture (CCA) and PKCS #11 (Cryptoki) implementations as well as custom software options.
- OEM and end-user purchase options.

Typical Applications

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.

Smart card initialization and personalization systems can exploit the programmable nature of the secure processor for the wide variety of cryptographic techniques used in those systems. The toolkits that can be obtained from IBM for programming in the secure Coprocessor environment enable application developers to stay abreast of the evolving needs in this area.

PKI applications such as Certification Authority systems can exploit the high-security protection of private keys afforded by the Coprocessor. Based on your application design, certificate-signing keys can be generated and held within the Coprocessor hardware, or you can arrange for secure backup of these very sensitive and hard-to-replace keys.

Other business applications can access the Coprocessor via the the IBM Common Cryptographic Architecture API, or the PKCS #11 API. 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 Derived 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 (for example, Common Criteria) 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. Certification requires an evaluation conducted by a qualified and independent third party that is supervised and approved by the USA Government National Institute of Standards. 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 evaluated under the FIPS standard as indicated in the table.

The IBM 4758 Models 001 and 002 are each one of a very few devices to be certified at the rigorous FIPS PUB 140-1, level four. High-level PKI certification authorities and/or applications where the cryptographic equipment is subject to attack by skilled adversaries should consider level 4 devices.
Figure 1-1. FIPS PUB 140-1 Security Levels and the IBM 4758 Models

<table>
<thead>
<tr>
<th>FIPS 140-1 Level</th>
<th>IBM 4758 Model</th>
<th>Simplified Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>A certified implementation correctly performs recognized algorithms. Software-only implementations can meet this level.</td>
</tr>
<tr>
<td>2</td>
<td>013</td>
<td>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.</td>
</tr>
<tr>
<td>3</td>
<td>013 023</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>001 002</td>
<td>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.</td>
</tr>
</tbody>
</table>

A numerically higher level must meet the requirements of all lower levels.

As compared to IBM 4758 Models 001 and 002, the Models 013 and 023 devices employ a more economical approach to protecting internal sensitive information. Both Models 023 and 013 are certified at level three. These devices are suitable in a broad range of applications where the Coprocessors are less subject to tampering attacks and/or the impact of any loss is less far reaching.

Models 002 and 023 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 (all models)
- 56-bit DES general data encryption through a pipelined DES engine
- Triple-DES general data encryption through a pipelined, three-key DES engine (Models 002 and 023)
- SHA-1 hashing through a pipelined hashing engine (Models 002 and 023)
- RSA key generation and private-and public-key operations for keys up to 2048 bits in length
- 1024-bit (Models 001 and 013) and 2048-bit (Models 002 and 023) 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
• Several approaches to cryptographic processing including PKCS #11 and IBM CCA
• 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

The product website http://www.ibm.com/security/cryptocards provides current information about the IBM 4758 PCI Cryptographic Coprocessor. On this site you will find information 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 in Adobe Acrobat 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. IBM eServer iSeries users should visit the iSeries website http://www.ibm.com/servers/eserver/iseries.

The product website provides a complete step-by-step process for ordering the hardware and downloading the software. Customers complete an on-line registration process to gain access to the software downloads for the CCA and PKCS #11 Support Programs. The registration 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
• PKCS #11 Support Program feature
• Custom software development and the embedded operating system
• Ordering the Coprocessor.
Chapter 2. IBM 4758 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 Coprocessor family consists of several models and variations. Each Coprocessor 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 electronics include:

- Noise-source random-number generation
- DES and TDES (Models 002 and 023) encryption engine
- SHA-1 hashing engine
- 1024-bit or 2048-bit (models 002/023) modular arithmetic processing
- Several memory technologies which enable secure data-storage
- An Intel® 80486-compatible computer
- Tamper sensors, 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 USA FIPS PUB 140-1 standard.

Optional IBM Common Cryptographic Architecture (CCA) and PKCS #11 software and toolkits are described in subsequent chapters.

Coprocessor Board

The Coprocessor consists of a two-thirds length PCI Version 2.1 bus board on which are mounted a self-contained cryptographic coprocessor, battery holders with 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 on page 2-2 lists many of the capacities and environmental specifications of the IBM 4758 Coprocessors. IBM 4758 Coprocessors should be shipped in their original IBM packaging. The Coprocessors should not be shipped in system units.

The IBM 4758 Models 002 and 023, and the no longer available older Models 001 and 013, are equipped with two batteries and operate on a 5-volt PCI bus. The RPQ versions of the Model 002 and 023 are equipped with four batteries and operate on either a 3.3 or a 5-volt PCI bus. The four-battery versions are used for the PCI Cryptographic Coprocessor (PCICC) features on the IBM eServer iSeries, pSeries, and zSeries.
Except for the PCI bus interface processor module, the Coprocessor electronics are contained within a sealed steel enclosure. Other than the tamper sensors, the enclosed electronics and software environment are identical between Models 002 and 023, and between Models 001 and 013.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Model 002 RPQ 8V1183</th>
<th>Model 023 RPQ 8V1185</th>
<th>Model 001 No longer available</th>
<th>Model 013 No longer available</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS 140-1 certification level</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>CPU speed</td>
<td>99MHz</td>
<td>99MHz</td>
<td>66MHz</td>
<td>66MHz</td>
</tr>
<tr>
<td>RAM size</td>
<td>4MB</td>
<td>4MB</td>
<td>4MB</td>
<td>4MB</td>
</tr>
<tr>
<td>Flash-memory size</td>
<td>2x2MB</td>
<td>2x2MB</td>
<td>2x1MB</td>
<td>2x1MB</td>
</tr>
<tr>
<td>Battery-backed RAM size</td>
<td>32KB</td>
<td>32KB</td>
<td>8KB</td>
<td>8KB</td>
</tr>
<tr>
<td>DES engine</td>
<td>Three-key</td>
<td>Three-key</td>
<td>Single-key</td>
<td>Single-key</td>
</tr>
<tr>
<td>SHA-1 engine</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Large integer, modular</td>
<td>2048 bits</td>
<td>2048 bits</td>
<td>1024 bits</td>
<td>1024 bits</td>
</tr>
<tr>
<td>arithmetic processor, width</td>
<td>2.1, 2/3 length, 5v</td>
<td>2.1, 2/3 length, 5v</td>
<td>2.1, 2/3 length, 5v</td>
<td>2.1, 2/3 length, 5v</td>
</tr>
<tr>
<td>(also available: 3.3v OEM option)</td>
<td>+5.0VDC ±5%</td>
<td>+5.0VDC ±5%</td>
<td>+5.0VDC ±5%</td>
<td>+5.0VDC ±5%</td>
</tr>
<tr>
<td>Temperature, shipping¹,²</td>
<td>-15°C to 60°C</td>
<td>-15°C to 60°C</td>
<td>-15°C to 60°C</td>
<td>-15°C to 60°C</td>
</tr>
<tr>
<td>Temperature, storage¹</td>
<td>10°C to 60°C</td>
<td>1°C (one) to 60°C</td>
<td>10°C to 60°C</td>
<td>1°C (one) to 60°C</td>
</tr>
<tr>
<td>Temperature, operating¹</td>
<td>10°C to 40°C</td>
<td>10°C to 40°C</td>
<td>10°C to 40°C</td>
<td>10°C to 40°C</td>
</tr>
<tr>
<td>Relative humidity, shipping²</td>
<td>5% to 100%</td>
<td>5% to 100%</td>
<td>5% to 100%</td>
<td>5% to 100%</td>
</tr>
<tr>
<td>Relative humidity, storage</td>
<td>5% to 80%</td>
<td>5% to 80%</td>
<td>5% to 80%</td>
<td>5% to 80%</td>
</tr>
<tr>
<td>Relative humidity, operating</td>
<td>8% to 80%</td>
<td>8% to 80%</td>
<td>8% to 80%</td>
<td>8% to 80%</td>
</tr>
<tr>
<td>Pressure, shipping²</td>
<td>550mbar, minimum 1039mbar, maximum</td>
<td>not specified</td>
<td>550mbar, minimum 1039mbar, maximum</td>
<td>not specified</td>
</tr>
<tr>
<td>Pressure, storage</td>
<td>700mbar, minimum 1039mbar, maximum</td>
<td>not specified</td>
<td>700mbar, minimum 1039mbar, maximum</td>
<td>not specified</td>
</tr>
<tr>
<td>Pressure, operating</td>
<td>768mbar, minimum 1039mbar, maximum</td>
<td>768mbar, minimum 1039mbar, maximum</td>
<td>768mbar, minimum 1039mbar, maximum</td>
<td>768mbar, minimum 1039mbar, maximum</td>
</tr>
<tr>
<td>Tamper-detection techniques</td>
<td>Mesh, high and low temperature, radiation, power-sequencing</td>
<td>Steel shell, high temperature, power-sequencing</td>
<td>Mesh, high and low temperature, radiation, power-sequencing</td>
<td>Steel shell, high and low temperature, power-sequencing</td>
</tr>
</tbody>
</table>

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.
2. Shipping-condition specifications apply when the product is transported in its original IBM packaging.
3. MHz: Megahertz; MB: Megabytes; KB: Kilobytes; mbar: millibar.
The cryptographic Coprocessor subsystem, shown schematically in Figure 2-2 on page 2-4, consists of these principle elements:

**Tamper Detection Sensors** Models 001 and 002 and Models 013 and 023 differ in the approach to tamper detection. The FIPS 140-1 level 4 rated Models 001 and 002 surround the internal electronics with a polyurethane mixture and a film with an imprinted circuit pattern to detect minute penetration and erosion attacks. The FIPS 140-1 level-3-rated Models 013 and 023 employ an electrical circuit connected to the steel case to detect attempts at opening the case.

Additional environmental sensors as listed in Figure 2-1 on page 2-2, implement additional tamper-detection techniques. The Models 001 and 002 implement a full complement of techniques to monitor environmental conditions: high and low temperature, power sequencing, and radiation.

All of 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 486-class CPU provides an industry-standard computing environment for flexible control of secure processing and cryptographic algorithms and processes.

The 486-class processor virtual-memory architecture enables a control program to isolate control program memory from application memory. Use of protection rings zero and three can enable a control program to exercise exclusive access to I/O.

**PCI Bus Interface Processor Module** This module couples the secured electronics to the PCI bus and provides for busmaster operation with inbound and outbound DMA operations between the FIFO buffers and the host-system memory. The module 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 and SHA-1 engines. 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 provides DES processing at high sustained rates. All models support 56-bit CBC and ECB DES encryption. Models 002 and 023 also support three-key triple-DES in outer CBC and ECB modes. Because of the need to inject keys under control of the subsystem software, to setup the FIFO buffer connection controls, and to initialize the DMA controllers, throughput is sensitive to the data block-size and to the host-system bus design and load. See the performance information available on the product website.
SHA-1 Engine Models 002 and 023 also contain a SHA-1 hashing engine connected between the FIFO buffers.

Random-Number Generator An electronic noise source provides unpredictable input to a random bit-value accumulator. (The CP/Q++ control program periodically uses the hardware output to seed a FIPS 140-1 approved pseudo random-number generator. The control program provides both the raw accumulated hardware output and the pseudo random-number generator output to internal application programs.)

Large-Integer Modular Arithmetic Processor A 1024-bit or 2048-bit 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 both hardware processors for keys up to 2048 bits in length.

Clock Calendar A time and date source accurate to within one minute per month provides a internal time value that is under the exclusive control of software running within 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 information in a separate 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.

This separate battery-backed memory is not accessible to the main 486-class processor; changes to data in this memory can only be made by the state controller based on requests to the state controller and hardware reset and tamper signals. 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 website.

**RAM Memory** DRAM memory is available for the use of subsystem software and data storage.

**Flash Memory** Two or four 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. Use of the 486-class processor page-control tables enable a control program to reserve access to this memory for itself.

Two 256K-byte 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 ensures that reloading of the low-level control software can be interrupted at any point without affecting the continued availability of the device.

The remainder of flash memory is allocated to program segments two (control program) and three (application program), to Miniboot (64KB), and to retain persistent data used application programs. The design grants segment two 768KB (512KB for Models 001 and 013), and segment three 768KB (256KB for Models 001 and 013). An application program can exceed the reserved size for segment three at the expense of less space for persistent-data storage. Loading and access to segments two and three is controlled by the Miniboot bootstrap software operating in conjunction with the state controller. These operations are part of the FIPS-certified security-policy enforcement mechanism.

Note that writing to flash memory is slow and can only be performed reliably thousands of times. The IBM-supplied CP/Q++ control-program flash-memory-manager manages the memory similar to a disk file with error checking and bad-sector logic. Application programs are not given direct access to flash memory and are forced to access memory under the imposed security policies. The manager also attempts to distribute usage across all of flash memory to avoid write-cycle limits.

---

1 See “CP/Q” on page 5-1
Battery-Backed Random Access Memory (BBRAM) As with flash memory, a control program can restrict access to the battery-backed RAM. Read and write times are comparable to that of DRAM. The contents of this memory are quickly zeroized in the event of a detected tamper. (Note that this memory is distinct from the BBRAM addressed by the state controller.)

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 (that is, to a segment-two control program), the port can be enabled by a segment three application program.

Batteries In the absence of power delivered over the PCI interface, batteries power the tamper sensor electronics and battery-backed RAM. In projected usage in server systems, power will rarely be drained from the batteries, therefore 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. Multiple 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.

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. See Figure 6-1 on page 6-1 for battery ordering information. The battery replacement process is described in the IBM 4758 PCI Cryptographic Coprocessor Installation Manual.

Note: If you remove all battery power and system power, the Coprocessor will zeroize and become permanently non-functional.

The 3.3 volt versions of the Model 002 and 023 have two additional batteries that extend the battery-life reliability such that in many cases the battery life can be assumed to exceed the installed life of a Coprocessor.

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 zero and one. (Flash-memory segment zero 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 contents of segments zero and one are 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 one, for assigning “ownership” of segment two, and for validating a digital signature on a “segment two public key.” With a successful conclusion of the one-time factory
After software-content changes or unrecoverable exception conditions, 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 two and three. Status information, which includes the device serial number, state information, and ownership and software content of segments one, two, and three, 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 zero and segment one 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 two and normally also into segment three. The standard IBM 4758 Coprocessor is sold by IBM without software resident in segments two or three. (No-charge software is available as described later in this manual.)

Code intended for segments one, two, and three 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 two. 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 export regulations.

Loading code into segment two requires an IBM-signed establish segment two ownership command incorporating an ownership code assigned by IBM. The developer of the segment two 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 one control information
- His code-load digitally signed and verifiable by his public key contained within the certificate.

The Coprocessor bootstrap routines process a segment two code-loading request by first validating the ownership assignment request and recording the new ownership of segment two. (A state change occurs which initiates a reset sequence.) The bootstrap validates the load-code request by (1) matching the

---

2 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 PUB 140-1 standard.
segment-ownership code, (2) checking the certificate digital signature, and (3) using that now-trusted public key to validate 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 two. Thus, another vendor can provide code for segment two.

Loading of code into segment three follows the same pattern, replacing two by three and one by two. The owner of segment two must administer the segment three ownership identifiers and sign the segment three ownership command and certify the segment three code-validating public key. Again, the segment-two party needs never have access to the actual segment three 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 Coprocessor 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 website.

IBM provides an embedded operating system, CP/Q++, for loading into segment two, 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 three applications. See Chapter 5, "IBM 4758 Custom Software Development" on page 5-1.

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, DSA, and SHA-1 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 PUB 140-1 certified product with confidence in its security features.
Chapter 3. IBM 4758 CCA Support Program

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

The optional, no-charge IBM 4758 CCA Support Program is offered for use with AIX, Windows NT, Windows 2000, or OS/2 systems. Chapter 5, “IBM 4758 Custom Software Development” describes tools that you can use to extend the CCA Support Program and/or to create an alternative application.

The CCA software described in this chapter has been independently reviewed and certified by the German ZKA industry organization for use in specific finance systems. Also, IBM believes the software described in this chapter can be operated compliant with the FIPS 140-1 cryptographic module standard.

Overview

The IBM 4758 CCA Support Program provides host-system software and Coprocessor software that together 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, Windows 2000, and IBM OS/2 Warp, Warp Server, and Warp Server SMP.

- **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, AIX, OS/400®, and OS/390® platforms.

- **Flexibility to meet unique requirements** by employing toolkits to extend the function provided with the IBM implementation (see Chapter 5, “IBM 4758 Custom Software Development”).

- **A growth path** for users of the IBM Transaction Security System products.
The IBM 4758 CCA Support Program is offered in several releases. Release 1.32 supports IBM 4758 Models 001 and 013, while Release 2.x supports Models 002 and 023. The support program exploits the full capabilities of the Coprocessor hardware to furnish services, including:

- DES encryption and decryption with support for CBC and ANSI X9.23 last-block processing. Release 1.32 supports 56-bit DES encryption while Release 2.x supports both 56-bit DES and triple-DES using double-length DES keys.
- 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, and also beginning with Release 2.30, RIPEMD-160, and MDC-2 and MDC-4
- RSA signature generation and verification, with signatures formatted according to ISO 9796, PKCS #1 block type 0 and 1 rules, and also beginning with Release 2.30, ANSI X9.31
- 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
  - Export and import of DES data keys using RSA with PKCS #1.2 and IBM CCA PKA92 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. Release 2.x also supports processing of an encrypted PIN block.
- 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 selected Visa, MasterCard, and American Express card-verification codes
- Diversified key generation for use with smart-card initialization processes.


The API is supported for use by applications written in C. Calls from multiple processes and from multiple threads within a process are supported. The API is implemented in a thread-safe manner. Beginning with Release 2.30, multiple IBM CCA products can use the same copy of the CCA Library simultaneously.

\(^1\) PKCS standards and the MD5 hashing algorithm (see RFC 1321) are developments of RSA Data Security, Incorporated.
4758 Model 002 and Model 023 Coprocessors can be supported in a single system.

**Export-Controlled Cryptographic Function** regulations of the USA Government have changed and now permit IBM to export the full-function product to all customers including triple-DES and RSA keys up to 2048 bits for the encryption of symmetric keys.

---

**Requirements and Specifications**

**Software Requirements:** Different support program versions support the models:

- For Models 001 and 013: Release 1.32
- For Models 002 and 023: Releases 2.x.
- See Chapter 3 in the *IBM 4758 PCI Cryptographic Coprocessor CCA Support Program Installation Manual* for the Support Program release you will use for the operating system and Java software levels required by the release you intend to employ.

See “Software updates” at Web site http://www.ibm.com/security/cryptocards for the currently supported software levels.

**Version 1 and Version 2 Differences and Migration:** The Release 2.x Support Program API is designed with greater consistency with the IBM zSeries S/390 CCA API. Minor differences exist between the DES and RSA key tokens used in Release 1.x and Release 2.x. Some application program changes may be needed to migrate to use of Release 2.x. Application program authors should review the “Revision History” section of the *IBM 4758 CCA Basic Services Reference and Guide* for insight into changes in the CCA API that could affect their programs.

Because of the CCA API changes and the different performance characteristics of the Model 002 and Model 023 hardware and software, all applications should be carefully retested with the new hardware and Support Program.
Chapter 4. IBM 4758 PKCS #11 Support Program

The IBM 4758 PKCS #11 Support Program provides a subset of RSA Laboratories’ standard PKCS #11 application programming interface (API) for use with the IBM 4758 Models 002 and 023 Coprocessors running under AIX, Windows NT, and Windows 2000.

The IBM 4758 Coprocessor can be used with Netscape since the Netscape Security Library also uses the PKCS #11 APIs.

This chapter describes the PKCS #11 Support Program which is optional, no-charge software for the Coprocessor. IBM believes the software described in this chapter can be operated compliant with the FIPS 140-1 cryptographic module standard.

Information in this chapter includes:

- PKCS #11 support program overview
- Requirements.

Overview

The PKCS #11 Support Program includes the following features:

- Support for version 2.01 of the PKCS #11 Cryptoki API with the following exceptions:
  - C_WaitForSlotEvent
  - Dual-purpose cryptographic functions.

  **Note:** User callback functions are not currently supported.

- The following mechanism classes are provided:
  - DES
  - DES3
  - RSA
  - DSA
  - SHA-1
  - MD5
  - MD2
  - SSL3.

- Support for triple-length DES keys (CKK_DES3). Double-length DES keys (CKK_DES2) are not supported.

- Support for multiple Coprocessors.

- Multiple PKCS #11 applications may safely access the IBM 4758 simultaneously.
Description

For the Windows NT and Windows 2000 platforms, the PKCS #11 Support Program provides a PKCS #11 access dynamic load library (DLL) and an API import library as well as code for the Coprocessor. For the AIX platform, the AIX system provides the host code while the Coprocessor software and the Coprocessor Load Utility are downloaded from the IBM 4758 website. (The website also has the current device driver for AIX.)

Figure 4-1 illustrates the flow between your application, the PKCS #11 access DLL, device drivers, CP/Q++ control program, and PKCS #11.

The API import library is supported for use by applications written in C language. Calls from multiple processes and from multiple threads within a process are supported. Your applications can access multiple Coprocessors.

Requirements

For IBM 4758 Model 002 and Model 023 PCI Cryptographic Coprocessors:

- Installed in a PC:
  - Windows NT Version 4.0 and Windows 2000
- Installed in IBM eServer pSeries (RS/6000):
  - AIX Version 4.3.3 (32-bit mode) (and possibly later versions, see the product website: http://www.ibm.com/security/cryptocards).
Chapter 5. IBM 4758 Custom Software Development

IBM offers two toolkits you can use to develop applications that run within the Coprocessor. The first toolkit enables you to create, sign, load, debug, and release application programs that perform within segment three of the IBM 4758 PCI Cryptographic Coprocessor. The second toolkit enables you to extend the functionality of the CCA Support Program.

The toolkits are obtainable from IBM under custom contracts. With the toolkits you can potentially implement new and very strong cryptographic processes. Therefore, the toolkits are subject to USA export regulations. IBM can distribute the toolkits to all customers (except those in a few select countries) after obtaining a brief, non-confidential statement-of-intended-use. These statements and the customer's name and address are reported to the USA Bureau of Export Administration on a semi-annual basis after delivery of the toolkits.

The toolkit 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 work-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.

You develop your Coprocessor application in C using Microsoft** tools. Development and debug is supported on a Windows NT or Windows 2000 platform. You can also debug the application running within the Coprocessor by connecting the Coprocessor’s serial port to the debug tool running in a Windows platform. This latter approach permits you to operate the Coprocessor under test in a non-Windows platform.

** CP/Q++ Control Program:** IBM provides an embedded control program, CP/Q++, for loading into segment two. (Segments are described in “Low-level Bootstrap and Diagnostic Software” on page 2-6.) 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 microkernel concepts and provides memory management, multi-tasking and task synchronization, a C-language library, and so on.
Two toolkits are available. The first toolkit supports the development of any segment-three 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 three 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-three Coprocessor application. The toolkit also provides the means for you to create a host-system application programming interface 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 contact IBM concerning availability of the toolkits, submit a request for information via the “Contact the Crypto Team” navigation item on the [http://www.ibm.com/security/cryptocards](http://www.ibm.com/security/cryptocards) Web site.

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.
Chapter 6. Ordering the IBM PCI Cryptographic Coprocessor

This chapter lists the IBM PCI Cryptographic Coprocessor models, features, and RPQs, and directs you to further product ordering and software downloading sources. Current information is available on the product Web site Order page, http://www.ibm.com/security/cryptocards where you should check for updated information.

For complete information about software downloading and installation, refer to the following publications available from the Library page on the product website:


Notes:

1. The support programs require an IBM PCI Cryptographic Coprocessor and the Coprocessor cannot function without software such as the CCA Support Program or the PKCS #11 Support Program, or software from another vendor.

These models of the IBM 4758, and the optional battery replacement kit, can be ordered as products from IBM.

Figure 6-1. IBM 4758 PCI Cryptographic Coprocessor Ordering Information

<table>
<thead>
<tr>
<th>Description</th>
<th>Order Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM 4758 PCI Cryptographic Coprocessor FIPS 140-1, level 4 5-volt PCI bus</td>
<td>4758, Model 002</td>
</tr>
<tr>
<td>IBM 4758 PCI Cryptographic Coprocessor FIPS 140-1, level 3 5-volt PCI bus</td>
<td>4758, Model 023</td>
</tr>
<tr>
<td>PCI Cryptographic Coprocessor FIPS 140-1, level 4 3.3-volt and 5-volt PCI bus</td>
<td>RPQ 8V1183</td>
</tr>
<tr>
<td>PCI Cryptographic Coprocessor FIPS 140-1, level 3 3.3-volt and 5-volt PCI bus</td>
<td>RPQ 8V1185</td>
</tr>
<tr>
<td>PCI Cryptographic Coprocessor for IBM eServer pSeries servers (RS/6000) FIPS 140-1, level 4 See IBM pSeries at <a href="http://www.ibm.com/security/cryptocards">http://www.ibm.com/security/cryptocards</a> for currently supported systems.</td>
<td>Feature code 4963</td>
</tr>
<tr>
<td>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.</td>
<td>Feature code 1008 on machine type 4758 or Part number 09J8199</td>
</tr>
</tbody>
</table>
Obtaining the Software

IBM provides no-charge Coprocessor software for personal computers including IBM eServer xSeries using Windows NT or Windows 2000, and for IBM eServer pSeries systems using AIX. The product Web site at http://www.ibm.com/security/cryptocards and the manuals listed at the start of this chapter explain in greater detail how you can obtain and install the CCA or PKCS #11 Support Program software. The software for a specific platform type and release is downloaded over the Internet. To reach the download pages you will be asked to complete a registration. A portion of the registration information is required by the USA Government to ensure that the software that implements cryptographic processes is going to permissible parties.

Software supporting the Coprocessor features in IBM eServer iSeries and zSeries is provided with the hardware and the respective operating systems, OS/400, and z/OS or MVS.
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.

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

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 are trademarks of the IBM Corporation in the United States or other countries or both:

AIX
IBM
IBM Registry
OS/2
OS/400

PowerPC
RS/6000
S/390
SecureWay
VisualAge

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

Java and all Java-related trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows NT, and Windows 2000 are trademarks of Microsoft Corporation in the United States, other countries, or both.

SET is a trademark owned by SET Secure Electronic Transaction LLC.

UNIX is a registered trademark in the United States, other countries, or both and is licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.
# List of Abbreviations and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>AIX</td>
<td>Advanced Interactive Executive (Operating System)</td>
</tr>
<tr>
<td>API</td>
<td>Application Program Interface</td>
</tr>
<tr>
<td>ASCII</td>
<td>American National Standard Code for Information Interchange</td>
</tr>
<tr>
<td>BBRAM</td>
<td>Battery-Backed Random Access Memory</td>
</tr>
<tr>
<td>C</td>
<td>Celsius</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CBC</td>
<td>Cipher Block Chaining</td>
</tr>
<tr>
<td>CCA</td>
<td>Common Cryptographic Architecture</td>
</tr>
<tr>
<td>CDMF</td>
<td>Commercial Data Masking Facility</td>
</tr>
<tr>
<td>cm</td>
<td>Centimeter</td>
</tr>
<tr>
<td>CP/Q++</td>
<td>Control Program/q (See “CP/Q” on page 5-1.)</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CV</td>
<td>Control Vector</td>
</tr>
<tr>
<td>CVC</td>
<td>Card Verification Code</td>
</tr>
<tr>
<td>CVV</td>
<td>Card Verification Value</td>
</tr>
<tr>
<td>DEA</td>
<td>Data Encryption Algorithm</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DMA</td>
<td>Direct Memory Access</td>
</tr>
<tr>
<td>DRAM</td>
<td>Dynamic Random Access Memory</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
</tr>
<tr>
<td>ECB</td>
<td>Electronic Code Book</td>
</tr>
<tr>
<td>EPROM</td>
<td>Erasable Programmable Read Only Memory</td>
</tr>
<tr>
<td>F</td>
<td>Fahrenheit</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FCV</td>
<td>Function Control Vector</td>
</tr>
<tr>
<td>FIFO</td>
<td>First In First Out</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>IBM</td>
<td>International Business Machines</td>
</tr>
<tr>
<td>in</td>
<td>Inch</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>IPL</td>
<td>Initial Program Load</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITSEC</td>
<td>Information Technology Security Evaluation Criteria</td>
</tr>
<tr>
<td>KB</td>
<td>Kilobyte</td>
</tr>
<tr>
<td>MB</td>
<td>Megabyte</td>
</tr>
<tr>
<td>mbar</td>
<td>Millibar</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>MBps</td>
<td>Megabytes per Second</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5 (Hashing Algorithm)</td>
</tr>
<tr>
<td>MDC</td>
<td>Modification Detection Code</td>
</tr>
<tr>
<td>MHz</td>
<td>Megahertz</td>
</tr>
<tr>
<td>mm</td>
<td>Millimeter</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>OS/2</td>
<td>Operating System/2</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PCI</td>
<td>Peripheral Component Interconnect</td>
</tr>
<tr>
<td>PDD</td>
<td>Physical Device Driver</td>
</tr>
<tr>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PKA</td>
<td>Public Key Algorithm</td>
</tr>
<tr>
<td>PKCS</td>
<td>Public Key Cryptography Standard</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>POS</td>
<td>Point-of-Sale</td>
</tr>
<tr>
<td>POST</td>
<td>Power-on Self-Test</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>RNG</td>
<td>Random Number Generator</td>
</tr>
<tr>
<td>ROM</td>
<td>Read-only Memory</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, and Adleman</td>
</tr>
<tr>
<td>SAA</td>
<td>Systems Application Architecture</td>
</tr>
<tr>
<td>SCC</td>
<td>Secure Cryptographic Coprocessor</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hashing Algorithm</td>
</tr>
<tr>
<td>SET</td>
<td>Secure Electronic Transaction</td>
</tr>
<tr>
<td>SNA</td>
<td>Systems Network Architecture</td>
</tr>
<tr>
<td>SVC</td>
<td>Supervisor Call</td>
</tr>
<tr>
<td>TOD</td>
<td>Time of Day (Clock)</td>
</tr>
<tr>
<td>V</td>
<td>Volt</td>
</tr>
<tr>
<td>VDC</td>
<td>Volts Direct Current</td>
</tr>
<tr>
<td>ZKA</td>
<td>Zentraler Kreditausschuss (German Central Credit Control Committee of Banks)</td>
</tr>
</tbody>
</table>
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 42nd 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 Code Book (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.

**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**

**FCV.** A digitally-signed data structure. The Function Control Vector is read by support programs to determine permissible function, especially associated with governmental export and import controls.

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.
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.

**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.

**Point-of-Sale (POS).** A class of equipment used to enter sales transactions.

**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. (1) 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.


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.

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.

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

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.

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

### Numerics

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4758</td>
<td>See IBM 4758 PCI Cryptographic Coprocessor</td>
</tr>
</tbody>
</table>

### A

- American National Standards Institute (ANSI)
  - X9.19 standard 3-2
  - X9.9 standard 3-2

### B

- battery kit 6-1
- board 2-1
- bootstrap software 2-6

### C

- CBC
  - See Cipher-Block Chaining
- CCA
  - See Common Cryptographic Architecture
- CDMF
  - See Commercial Data Masking Facility
- changes, summary of v
- Cipher-Block Chaining 3-2
- Common Cryptographic Architecture (CCA)
  - support program 3-1
  - user defined extensions 5-1
- contacting IBM 1-5
- CP/Q++ control program 5-1
- custom software 5-1

### D

- Data Encryption Standard (DES)
  - ANSI X9.23 standard 3-2
- DEA
  - See Data Encryption Standard
- DES
  - See Data Encryption Standard
- description, PKCS #11 support program 4-2
- diagnostic software 2-6
- digital signature 3-2
- download 6-1

### E

- edition notice v
- environmental specifications 2-2

### F

- features, PKCS #11 support program 4-1
- FIPS 140-1 2-1, 3-1
  - defined 1-3
  - model certification levels 1-1, 1-4

### H

- hardware description 2-1
- hashing algorithms
  - MD5 3-2
  - SHA-1 3-2
- highlights 1-2

### I

- IBM 4758 PCI Cryptographic Coprocessor
  - battery kit 6-1
  - board 2-1
  - bootstrap 2-6
  - CCA support program 3-1
  - certification levels 1-1
  - code loading 2-7
  - diagnostics 2-6
  - hardware description 2-1
  - low-level software 2-6
  - memory segments 2-6
  - ordering 6-1
  - physical, environmental specifications 2-2
  - secure coprocessor 1-3
  - security enclosure 2-3
  - software, custom 5-1
  - user defined extensions 5-1
- information, about the coprocessor 1-5
- introduction 1-1

### K

- key management 3-2

### L

- legal notices A-1
- low-level software 2-6

### M

- MAC
  - See Message Authentication Code
- MD5
  - See hashing algorithms
Message Authentication Code (MAC) 3-2
migration, version 1 to 2 3-3

N
notices, legal A-1

O
obtaining information 1-5
ordering 6-1
ordering the product 1-5
overview, PKCS #11 support program 4-1

P
physical characteristics 2-2
PIN processing 3-2
PKCS #11 Support Program 4-1
  APIs not supported 4-1
description 4-2
  mechanism classes provided 4-1
  overview 4-1
requirements 4-2
POST, power-on self-test 2-6
Public-Key Cryptography Standard (PKCS)
  #1.0 3-2
  #1.1 3-2
  #1.2 3-2
  #11 4-1
publications, related vi

R
related publications vi
requirements, PKCS #11 support program 4-2

S
sales, coprocessor 1-5
secure coprocessor 1-3
Secure Electronic Transaction, SET 3-1, 3-2
security enclosure 2-3
security functions, overview 1-4
SET
  See Secure Electronic Transaction
SHA
  See hashing algorithms
software download 6-1
software, custom 5-1
software, requirements 3-3
state controller 2-6
support program, CCA 3-1
support program, PKCS #11 4-1

T
toolkits 5-1
typical applications 1-2

V
Version 1 migration 3-3

X
X9.19 ANSI standard 3-2
X9.23 ANSI standard 3-2
X9.9 ANSI standard 3-2
IBM