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

IBM 4758 Models 2 and 23 PCI Cryptographic Coprocessor

Highlights

- *Suitable for high-security processing and high-speed cryptographic operations.*
- *Tamper-responding design submitted for evaluation under FIPS 140-1.*
- *Hardware to perform DES, T-DES, random number generation, and modular math functions for RSA and similar public-key cryptographic algorithms.*
- *IBM® Common Cryptographic Architecture (CCA) and PKCS #11 Support Programs.*
- *Custom software options.*
- *OEM and end-user purchase options.*
- *Secure code loading that enables updating of the functionality while installed in application systems.*

The use of cryptography 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 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 secure cryptographic applications.

The IBM 4758 Models 2 and 23 PCI Cryptographic Coprocessors are the latest generation of the IBM 4758 family. They are built upon the tamper responding design of the IBM 4758 Models 1 and 13 which have been certified under the US Government FIPS 140-1 standard, "Security Requirements for Cryptographic Modules" at Level 4 and Level 3, respectively. Evaluation of Models 2 and 23 for FIPS 140-1 compliance by an independent evaluation laboratory is in progress.

IBM provides the Common Cryptographic Architecture (CCA) Support Program feature and the PKCS #11 Support Program feature that you can load into the Coprocessor to perform cryptographic functions common in the finance industry and in Internet e-business applications. You can also purchase consulting services or programming toolkits to extend or replace the standard IBM software offering.

Typical applications...

The IBM 4758 PCI Cryptographic Coprocessor is suited to applications requiring high-speed cryptographic functions for data encryption and digital signing, secure storage of signing keys, or custom cryptographic applications. These can include financial applications such as PIN generation and verification in automated teller and point-of-sale transaction servers, e-business and Web-serving applications, Public Key Infrastructure applications, and custom proprietary solutions. Applications can benefit from the strong security characteristics of the Coprocessor and the opportunity to off load computationally intensive cryptographic processing.

The Coprocessor includes sensors to protect against attacks involving probe penetration, power sequencing, radiation, and temperature manipulation . . .

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, unmolested. 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 an essential tool.

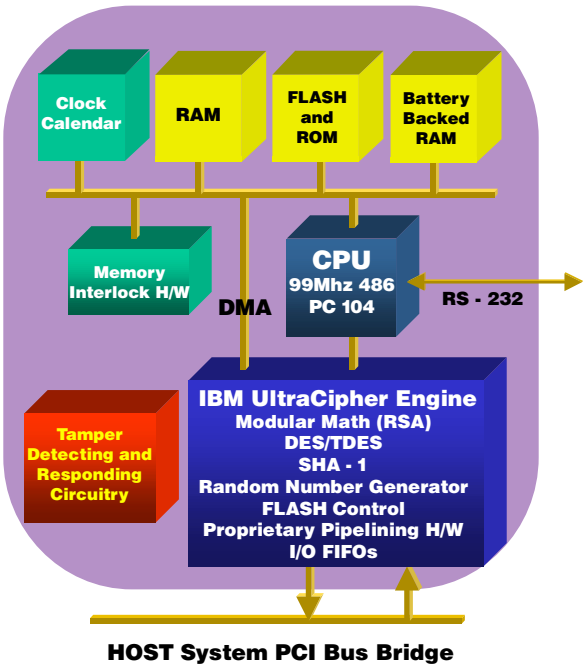
IBM 4758 Model 2 and 23 Hardware...

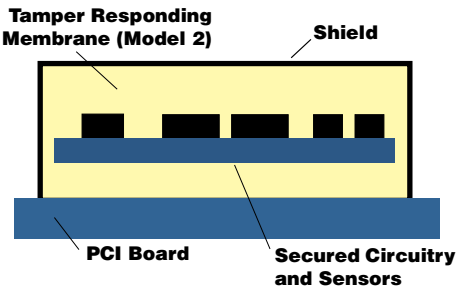
The Coprocessor secure processing environment contains a 99 MHz 486-compatible microprocessor, custom hardware to perform DES, T-DES, hashing, and public key cryptographic algorithms, a secure clock/calendar, and a hardware random number generator. It also has protective shields, sensors, and control circuitry to protect against a wide variety of attacks against the system.

Embedded Certificate

During the final manufacturing step, the Coprocessor generates a unique public key pair, which is stored in the device. The tamper detection circuitry is activated at this time and remains active throughout the useful life of the Coprocessor, protecting this private key, as well as all other keys and sensitive data. The Coprocessor public key is certified at the factory by an IBM private key and the certificate is retained in the Coprocessor. Subsequently, the Coprocessor private key is used to sign Coprocessor status responses which, in conjunction with a series of public key certificates, demonstrates that the Coprocessor remains intact and is genuine.

IBM 4758 PCI Cryptographic Coprocessor





Tamper Responding Design

The Coprocessor includes sensors to protect against attacks involving probe penetration, power sequencing, radiation, and temperature manipulation, consistent with the FIPS 140-1 Level 4 requirements (Model 2) and FIPS 140-1 Level 3 requirements (Model 23). From the time of manufacture, if the tamper sensors are triggered, the Coprocessor zeroizes its critical keys, destroys its certification, and is rendered inoperable. Note therefore that the Coprocessor must be maintained at all times within the temperature, humidity, and barometric pressure ranges specified in the *Environmental Requirements* section of this specification sheet.

A pair of batteries mounted on the Coprocessor board provide backup power when the Coprocessor is not in a powered-on machine. These batteries must only be removed according to the documented battery replacement procedure to avoid zeroizing the Coprocessor and rendering it inoperable. The batteries (standard commercial items) and a temporary holder can be obtained from IBM.

IBM 4758 Model 2 and 23 Software...

- Choose from IBM-supplied no-charge support program features:
  - IBM Common Cryptographic Architecture (CCA)
  - PKCS #11
- Or choose customization options:
  - IBM custom development to your specification
  - Toolkits under custom contracts and export control

CCA Support Program Feature...

- Available for Windows NT® and IBM OS/2®.

Highlights:

- DES-based data confidentiality and message integrity—DES CBC and T-DES encryption and single-key and double-key MACs
- RSA-based digital signature generation and verification (keys to 2048 bits) and message hashing—PKCS #1, ISO 9796, SHA-1, MD5
- PIN processing—Several generation and verification processes, many PIN block formats
- DES and RSA-based key distribution, generation of symmetric keys and RSA key pairs—PKCS and CCA, RSA keys to 2048 bits
- Support for applications that implement the SET™ Protocol
- Initialization and backup options
- Generation of high-quality random numbers
- Refined key-typing to block attacks through misuse of the key management system
- User Defined Extension (UDX) facility can be used to add custom functions to the standard CCA command set. Custom functions execute inside the secure module of the IBM 4758, with the same security as the other CCA functions.

PKCS #11 Support Program Feature...

- Available for Windows NT
- Subset of PKCS #11
- Cryptographic Token Interface Standard (version 2.01)
- Satisfies requirements of Netscape Security Library

Mechanism classes provided:

DES

DES3

RSA (up to 2048-bit modulus)

DSA

SHA-1

MD5

MD2

SSL3

- Multiple Coprocessors running PKCS #11 on a single host system are supported
- Multiple PKCS #11 applications may safely access the IBM 4758 simultaneously

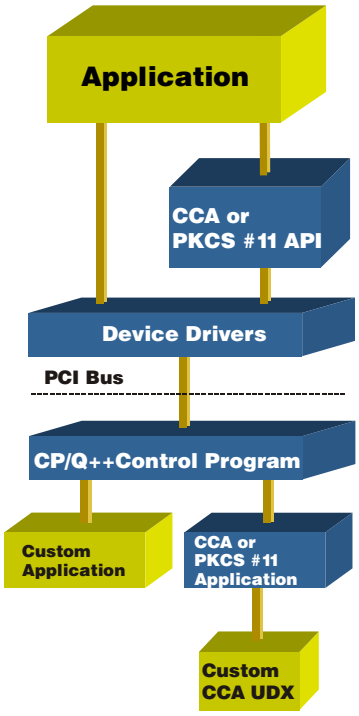
The following are not supported:

C_WaitForSlotEvent

Dual-purpose cryptographic functions

User callback functions

(Refer to "Implementing PKCS #11 for the Netscape Security Library" at the Netscape Web site *http://developer.netscape.com/docs/manuals/security/pkcs/pkcs.htm* for more information.)



Custom Software Support...

The Coprocessor contains firmware to manage its specialized hardware and to control loading of additional software based on Coprocessor-validated digital signatures. Software support includes the IBM CP/Q++ control program, which provides the platform for application support. Custom applications can be written to the CP/Q++ API to run within the Coprocessor, and to the 4758 host API library.

Developing additional functions through User Defined Extensions (UDX) using CCA as a starting point can be more economical than creating an entirely new application. Special key management functions and PIN processing routines are typical extensions. Other cryptographic algorithms such as Elliptic Curve cryptography can also be incorporated in this manner.

When an application is substantially different from CCA, or is proprietary, a complete custom application can be built on the CP/Q++ environment. Very different approaches to cryptographic processing or even non-cryptographic applications that require a secure processing environment can be developed for the Coprocessor.

Programming Custom Applications...

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. IBM is pleased to jointly develop specifications and quote on custom solutions.

Alternatively, IBM offers toolkits that work with IBM VisualAge® C++ and Microsoft® Visual C++® compilers and tools. The toolkits are supported by documentation that you can obtain from the IBM 4758 Web site. Because this is a specialized programming environment, and because there are special considerations related to the export and import of cryptographic implementations, the toolkits are only available under special contracts. Generally, in addition to the actual toolkits, customers will need to purchase consulting time for education and ongoing support. Any export or import considerations will be part of the toolkit custom contract.

Education...

Scheduled education courses about the IBM 4758 and CCA are held periodically in Charlotte, NC in the USA, and in Germany. These courses cover programming for the CCA API, and IBM 4758 installation and configuration. See the IBM 4758 Web page for further details.

In addition, custom courses can be arranged to cover other topics including programming and debugging applications that operate within the IBM 4758.

Additional information...

Documentation and publications, ordering procedures, and news concerning the IBM 4758 Coprocessor can be found on the Web at *http://www.ibm.com/security/cryptocards.*

To learn more...

Visit the IBM 4758 World Wide Web site at *http://www.ibm.com/security/cryptocards* or call IBM DIRECT at 1 800 IBM-CALL in the U.S. and Canada.

OEM customers can send an e-mail to *hanya@us.ibm.com*. OEM customers in the U.S. should call 1 800 IBMS-OEM.

Australia	132 426
Austria	0660.5109
Belgium	02-225.33.33
Brazil	0800-111426
China	(20) 8755 3828
France	0800-03-03-03
Germany	01803-313233
Hong Kong	(20) 2825 6222
Hungary	165-4422
India	(80) 526 9050
Indonesia	(21) 252 1222
Ireland	1-850-205-205
Israel	03-6978111
Italy	167-017001
Japan	0120 300 426
Korea	(02) 781 7800
Malaysia	(03) 717 7890
Mexico	91-800-00316
Netherlands	020-513.5151
New Zealand	0800-801-800
Philippines	(02) 819 2426
Poland	(022) 878-6777
Singapore	1800 320 1975
South Africa	0800-130130
Spain	900-100400
Sweden	020-220222
Switzerland	0800 55 12 25
Taiwan	(06) 2725 9300
Thailand	(02) 273 4444
Vietnam Hanoi	(04) 843 6675
Vietnam HCM	(08) 829 8342
United Kingdom	0990-390390

The IBM 4758 is a product offering of IBM S/390® Division.

Technical Specifications

Physical characteristics:

- Card Type: two-thirds length PCI Version 2.1
- Voltage: +5.0VDC ±5% and +12VDC ±5%

System Requirements

Software:

- *IBM CCA Support Program:* Windows NT and OS/2
- *PKCS #11 Subset Support Program:* Windows NT

Hardware:

- PC workstations or servers with available PCI 2.1 bus slot

IBM Corporation
Marketing Communications,
Enterprise Systems Group
Route 100
Somers, NY 10589

Printed in the United States of America, 02-00

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the products or services available in your area.

You can find additional information via IBM's World Wide Web server at *http://www.ibm.com.*

IBM hardware products are manufactured from new parts or new and serviceable used parts. Regardless, our warranty terms apply.

The products and services described in this offering are also available separately.

By 'Year 2000 ready', IBM means the capability of a product, when used in accordance with its associated documentation, to correctly process, provide and/or receive date data within and between the 20th and 21st centuries, provided that all products (for example, hardware, software and firmware) used with the product properly exchange date data with it. IBM's statements concerning the Year 2000 readiness of its products are Year 2000 readiness disclosures under the Year 2000 Readiness Information and Disclosure Act of 1998.

Environmental Requirements

From the time of manufacture, the IBM 4758 PCI Cryptographic Coprocessor card must be shipped, stored, and used within the following environmental specifications. Outside of these specifications, the IBM 4758 tamper sensors will be activated and render the IBM 4758 permanently inoperable.

	IBM 4758-002	**IBM 4758-023**
Temp Shipping	-15°C to 60°C	-15°C to 60°C
Temp Storage	1°C to 60°C	1°C to 60°C
Temp Operating	10°C to 40°C	10°C to 40°C
Humidity Shipping	5% to 100% RH with original IBM package	5% to 100% RH with original IBM package
Humidity Storage	5% to 80% RH	5% to 80% RH
Humidity Operating	8% to 80% RH	8% to 80% RH
Pressure Shipping	min 550 mbar / max 1039 mbar	not specified
Pressure Storage	min 700 mbar / max 1039 mbar	not specified
Pressure Operating	min 768 mbar / max 1039 mbar	min 768 mbar / max 1039 mbar

G221-9091-01