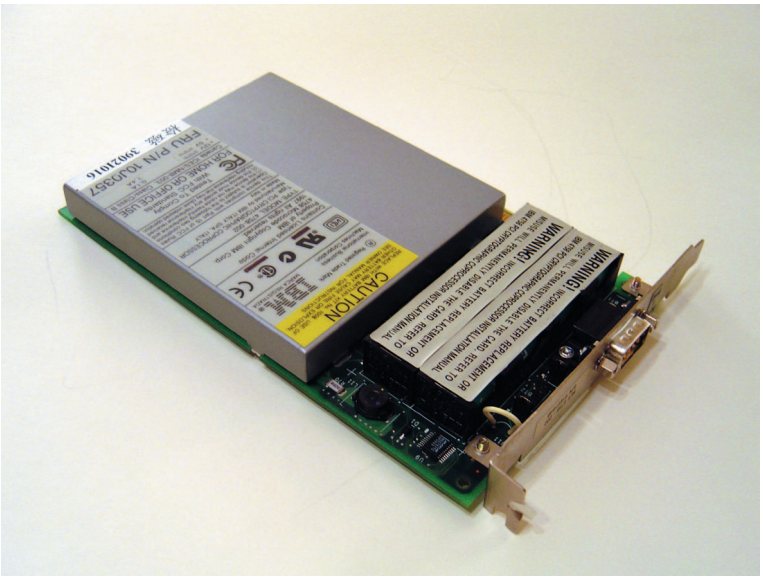
A flexible solution to your high-security cryptographic and secure processing needs

IBM 4758 Models 2 and 23 PCI Cryptographic Coprocessor



Highlights

- ***Suitable for high-security processing and high-speed cryptographic operations***
- ***Tamper-responding hardware design certified 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 crucial 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 offloads 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.

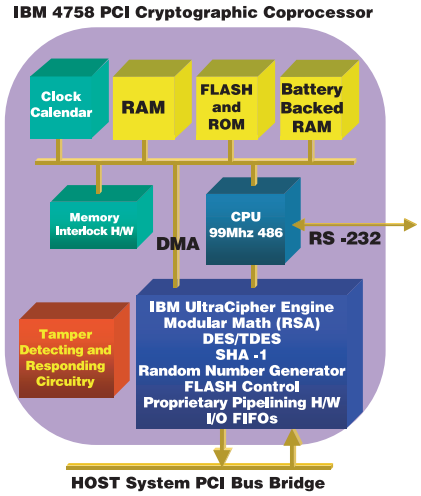
The IBM 4758 Models 2 and 23 PCI Cryptographic Coprocessors are the latest generation of the IBM 4758 family. They have been certified under the U.S. Government FIPS 140-1 standard, “Security Requirements for Cryptographic Modules” at Level 4 and Level 3, respectively.

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

IBM provides the Common Cryptographic Architecture (CCA) Support Program feature and the PKCS #11 Support Program feature that you can load into the FIPS 140-1 certified 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 functions provided by IBM.

Typical applications

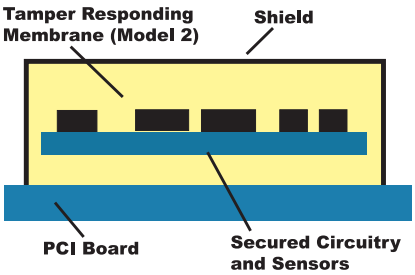
The IBM 4758 PCI Cryptographic Coprocessor is suited to applications requiring high-speed cryptographic functions for data encryption and digital signing, secure storage of signing keys, or custom cryptographic applications. These can include financial applications such as PIN generation and verification 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 offload computationally intensive cryptographic processing.

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 run,



with confidence that those programs have not been modified. 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. 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 Models 2 and 23

Hardware

The coprocessor secure processing environment contains an Intel® 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, demonstrate that the coprocessor remains intact and is genuine.

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 data sheet.

A pair of batteries mounted on the coprocessor board provides 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 Models 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

- *Available for Microsoft® Windows® 2000 and IBM AIX®.*

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, ANSI X 9.31, SHA-1, MD5*
- *PIN processing–Several generation and verification processes, many PIN block formats*
- *DES-based and RSA-based key distribution, generation of symmetric keys and RSA key pairs–PKCS and CCA, RSA keys to 2048 bits*

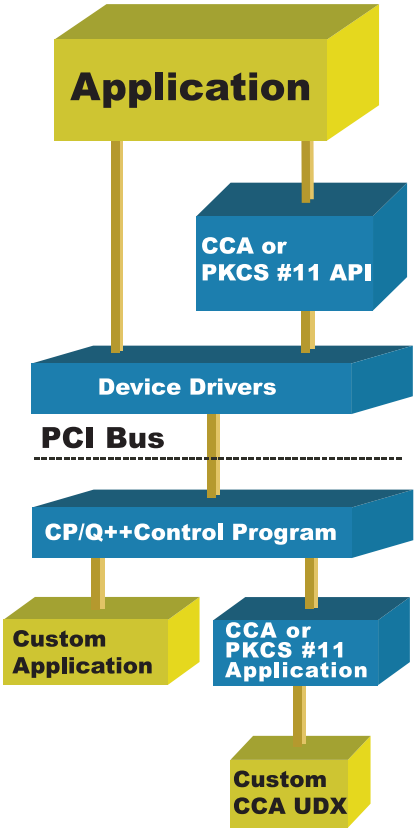
- *Support for applications that implement the SET™ Protocol*
- *Initialization and backup options*
- *Generation of high-quality random numbers*
- *Refined key-typing to block attacks through misuse of the key management system*
- *User Defined Extension (UDX) facility can be used to add custom functions 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

- *Available for Windows 2000 and IBM AIX*
- *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 developer.netscape.com/docs/manuals/security/pkcs/pkcs.htm for more information.)

4758 technology in IBM servers

All IBM server families support 4758 technology, either directly or as orderable features:

- *IBM @server® xSeries® and IBM Netfinity® servers–IBM 4758 Models 2 and 23 can be ordered and installed. CCA and PKCS #11 support programs for Windows 2000 can be downloaded from the 4758 Web site.*
- *IBM @server pSeries®, IBM RS/6000®, IBM RS/6000 SP™–Selected models offer an optional cryptographic coprocessor feature. CCA and PKCS #11 support programs available for AIX can be downloaded from the 4758 Web site.*
- *IBM @server iSeries™, IBM AS/400®–Selected models offer an optional cryptographic coprocessor feature. Support is provided by cryptographic services in OS/400®.*
- *IBM @server zSeries® 900 and IBM S/390® G5/G6 offer an optional PCICC feature which works in conjunction with the CMOS Cryptographic Coprocessor on those servers. Support is provided by cryptographic services in z/OS® and in OS/390® V2.*

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++ operating system, 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, N.C. in the United States, and in Germany. The courses can also be taught at your location, worldwide. These courses cover programming for the CCA API and the IBM 4758 installation and configuration. Visit **ibm.com**/security/cryptocards 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.

IBM 4758 Models 2 and 23 PCI Cryptographic Coprocessor Technical Specifications

Physical characteristics:

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

System Requirements

The following sections describe requirements for the system in which the 4758 is installed.

Software: (Downloadable from the IBM 4758 Web site)

IBM CCA Support Program: Windows 2000, IBM AIX

PKCS #11 Support Program: Windows 2000, IBM AIX

Hardware:

PC workstations or servers with available PCI 2.1 bus slot

For AIX selected IBM @server pSeries, IBM RS/6000 and IBM RS/6000 SP models installed with optional cryptographic feature.

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 operating	min 768 mbar max 1039 mbar	min 768 mbar max 1039 mbar
Pressure shipping	min 550 mbar max 1039 mbar	not specified
Pressure storage	min 700 mbar max 1039 mbar	not specified

For more information

Documentation and publications, ordering procedures, and news concerning the IBM 4758 Coprocessor can be found at **ibm.com**/security/cryptocards or call IBM DIRECT at 1 800 IBM-CALL or contact your IBM representative.

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

© Copyright IBM Corporation 2004

IBM Corporation
Integrated Marketing Communications,
Server Group
Route 100
Somers, NY 10589

Produced in the United States of America
May 2004

All Rights Reserved

References in this publication to IBM products or services do not imply that IBM intends to make them available in every country in which IBM operates. Consult your local IBM business contact for information on the products, features, and services available in your area.

IBM, the IBM logo, the e-business logo, AIX, AS/400, iSeries, OS/390, OS/400, pSeries, RS/6000, S/390, SP, Tivoli, VisualAge, xSeries, z/OS and zSeries are trademarks or registered trademarks of IBM Corporation in the United States, other countries or both.

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

SET Secure Electronic Transaction, Secure Electronic Transaction, SET and the SET Secure Electronic Transaction design mark are trademarks and service marks owned by SET Secure Electronic Transaction LLC.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows, and Windows 2000 are registered trademarks of Microsoft Corporation.

Other trademarks and registered trademarks are the properties of their respective companies. IBM hardware products are manufactured from new parts, or new and used parts. Regardless, our warranty terms apply.

Photographs shown are of engineering prototypes. Changes may be incorporated in production models.

This equipment is subject to all applicable FCC rules and will comply with them upon delivery.

Information concerning non-IBM products was obtained from the suppliers of those products. Questions concerning those products should be directed to those suppliers.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

G221-9091-04