A flexible solution to your high-security cryptographic processing needs

IBM 4765 PCIe Cryptographic Coprocessor

Certificate No. 1505

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

Highlights

- ***A PCIe card with a multi-chip embedded module intended to be a high-end secure coprocessor***
- ***Suitable for high-security processing and high-speed cryptographic operations***
- ***Tamper-responding programmable secure hardware that meets FIPS 140-2 Level 4 certification, the highest level of security***
- ***Hardware to perform AES, DES, T-DES, random number generation, SHA-1, SHA-256, MD5, HMAC, and large number modular math functions for RSA (up to 4096-bit), ECC Prime Curve and other public-key cryptographic algorithms***
- ***IBM Common Cryptographic Architecture (CCA Support Program)***
- ***Custom software options***
- ***Secure code loading that enables updating of the functionality while installed in application systems***
- ***Foundation for secure applications, such as high-assurance digital signature generation or financial transaction processing***
- ***Maximum flexibility, maximum trust with minimum physical security***

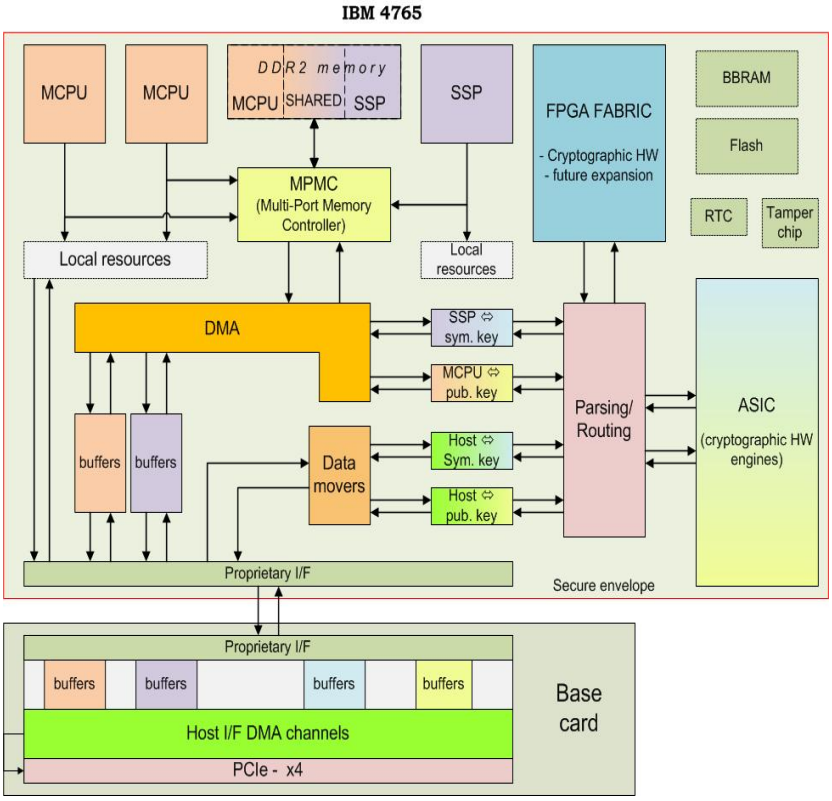
The use of cryptography is a crucial element of modern business applications. These applications use cryptography in a variety of ways to protect the privacy and confidentiality of data, to ensure the integrity of data, and to provide user accountability through digital signature techniques. The IBM® 4765 PCIe Cryptographic Coprocessor is a programmable PCIe 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 Internet business transactions, and is suited for a wide variety of secure cryptographic applications.

The IBM 4765 is the latest generation of the IBM cryptographic coprocessor family. It is certified by NIST (certificate no. 1505) under the U.S. Government FIPS 140-2, “Security Requirements for Cryptographic Modules” at the Level 4 standard.

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

IBM provides the Common Cryptographic Architecture (CCA) Support Program that you can load into the coprocessor to perform cryptographic functions common in the finance industry and in Internet business applications. You can also purchase consulting services or a programming toolkit to extend or replace the standard functions provided by IBM.

Typical applications
The IBM 4765 PCIe 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, Internet business and Web-serving applications, Public Key Infrastructure applications, smart card 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 that it is processing, you will find cryptography an essential tool.

IBM 4765 hardware

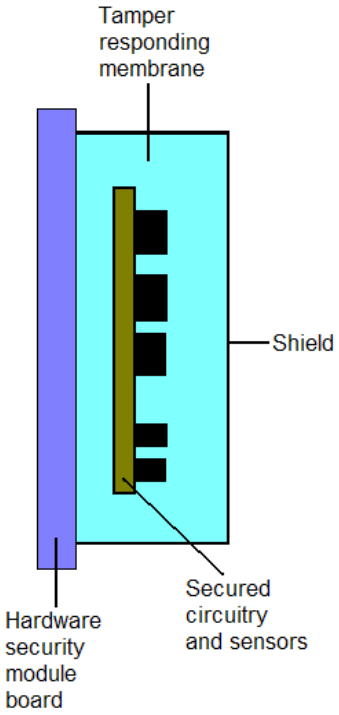
The secure processing environment (security module) of the coprocessor contains redundant embedded IBM PowerPC microprocessors (405Gr), custom hardware to perform AES, DES, T-DES, SHA-1, SHA-256, MD5, HMAC, and public key cryptographic algorithms, a secure clock/calendar, and a hardware random number 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/private 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, and temperature manipulation, consistent with the FIPS 140-2 Level 4 requirements. From the time of manufacture, if the tamper sensors are triggered, the coprocessor zeroizes its critical keys, destroys its certification, and is rendered permanently 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 permanently inoperable.

A battery replacement kit can be obtained from IBM (part number 45D5803). A multi-battery replacement pack (part number 74Y0465) containing 20 batteries is also available. This pack requires a battery tray to install the batteries. The tray comes with the battery replacement kit.

IBM 4765 software

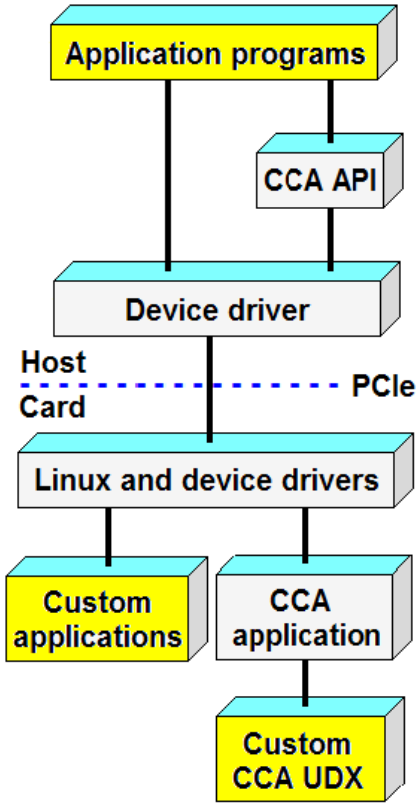
- *IBM-supplied no-charge support program feature: IBM Common Cryptographic Architecture (CCA)*
- *Or choose customization options:*
  - *IBM custom development to your specification*
  - *Toolkit under custom contracts and export control*

CCA Support Program

Available for use with SUSE™ Linux Enterprise Server 11 Service Pack 1 (SLES 11 SP1) from Novell (32-bit)

CCA highlights:

- *AES, DES, and T-DES based data confidentiality and message integrity – AES, DES and T-DES CBC encryption, DES and T-DES MACs, and HMAC*
- *RSA-based and ECC-based digital signature generation and verification and message hashing—PKCS #1, ISO 9796-1, ANSI X9.31, SHA up to 512 bits, and MD5 – RSA keys to 4096 bits*
- *PIN processing—several generation and verification processes, many PIN block formats*
- *Key distribution based on AES, DES, and RSA, generation of symmetric keys and ECC and RSA key pairs—RSA keys to 4096 bits*
- *Support for smart card applications using the EMV® specifications*
- *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 4765, with the same security as the other CCA functions.*
- *Support for applications that implement the SET™ Protocol*



4765 technology in IBM servers

The following IBM server families support 4765 technology, either directly or as orderable features.

- *IBM System x—IBM 4765 can be ordered and installed. CCA support program for SLES 11 SP1 can be downloaded from the **ibm.com/security/cryptocards** Web site*
- *IBM Power Systems—selected models offer an optional cryptographic coprocessor feature*
- *IBM System z—selected models offer an optional Crypto Express3 (CEX3) feature. Support is provided by ICSF cryptographic services in z/OS. Support for the Crypto Express3 feature is provided for Linux on IBM System z by the CCA for Linux on System z rpm, available from: **ibm.com/security/cryptocards/pciecc/ordersoftware.shtml***

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 embedded Linux operating system and special device drivers, which provide the platform for application support. Custom applications can be written to run within the coprocessor, using the internal APIs to perform cryptographic functions. Developing additional functions through User Defined Extensions (UDXs) using CCA as a starting point can be more economical and less time-consuming than creating an entirely new application.

Special key management functions and PIN processing routines are typical extensions.

When an application is substantially different from CCA, or is proprietary, a complete custom application can be built on the embedded Linux 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 a toolkit you can use to create and debug custom applications yourself. The toolkit is supported by documentation that you can obtain from **ibm.com/security/cryptocards**. Because this is a specialized programming environment and because there are special considerations related to the export and import of cryptographic implementations, the toolkit is available only under special contracts. Generally, in addition to the actual toolkit, 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

Courses are held periodically to provide education about the IBM 4765 and CCA. The courses can also be taught at your location, worldwide. These courses cover programming for the CCA API and the IBM 4765 installation and configuration.

In addition, custom courses can be arranged to cover other topics including programming and debugging applications that operate within the IBM 4765.

IBM 4765 PCIe Cryptographic Coprocessor technical specifications

Physical characteristics:	
Card type:	PCIe Short Type PCI Local Bus Specification 2.2, PCIe specification 1.1
Voltage:	+3.3 VDC ± 10% 23.44 W max
System requirements	The following sections describe requirements for the system in which the 4765 is installed.
Software (downloadable from PCIe Cryptographic Coprocessor link of ibm.com/security/cryptocards):	IBM CCA Support Program for use on SUSE Linux 11 Service Pack 1 (32-bit)
Hardware:	The coprocessor can be installed in an IBM System x ServerProven® server. For a list of approved System x servers for the 4765, go to the **PCIe Cryptographic Coprocessor** link of the **ibm.com/security/cryptocards** Web page. From there, click on the **Product summary** link, then click on the **IBM ServerProven** link.
Environmental requirements	From the time of manufacture, the IBM 4765 PCIe Cryptographic Coprocessor card must be shipped, stored, and used within the following environmental specifications. Outside of these specifications, the IBM 4765 tamper sensors can be activated and render the IBM 4765 permanently inoperable.

IBM 4765

Shipping: Card should be shipped in original IBM packaging (electrostatic discharge bag with desiccant and thermally insulated box with gel packs).

Temp shipping	-40°C to +60°C
Pressure shipping	min 550 mbar
Humidity shipping	5% to 100% RH

Storage: Card should be stored in electrostatic discharge bag with desiccant.

Temp storage	+1°C to +60°C
Pressure storage	min 700 mbar
Humidity storage	5% to 80% RH

Operation (ambient in system)

Temp operating	+10°C to +35°C
Humidity operating	8% to 80% RH
Operating altitude (max)	10 000 ft equivalent to 700 mbar min

For more information

Documentation and publications, ordering procedures, and news concerning the IBM 4765 PCIe Cryptographic Coprocessor can be found at: **ibm.com/security/cryptocards,** or call IBM DIRECT at 1-800-IBM-CALL, or contact your IBM representative.

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

Produced in the United States of America
May 2011