*Use the IBM® hardware security module (HSM) to provide a flexible solution to your high-security cryptographic processing needs.*

# IBM 4767-002 PCIe Cryptographic Coprocessor (HSM)

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, ensure its integrity, and provide user accountability through digital signature techniques.

The IBM 4767 PCIe Cryptographic Coprocessor is an HSM. This HSM 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.

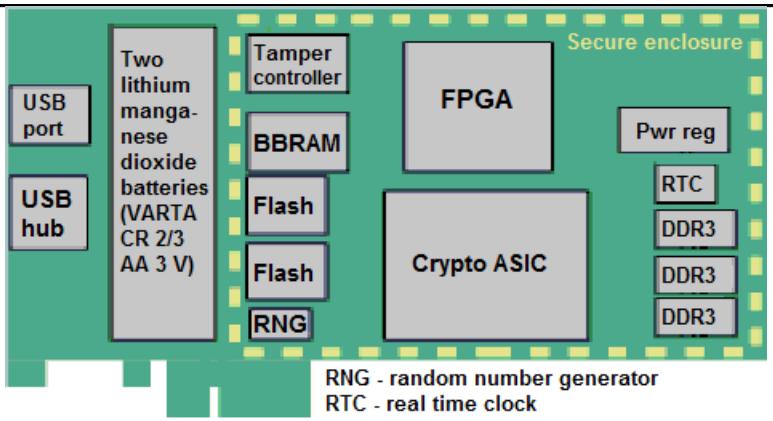
In April 2016, the IBM 4767 became the latest generation of the IBM cryptographic coprocessor family. The 4767 is currently undergoing certification to the U.S. Government NIST standard FIPS 140-2, “Security Requirements for Cryptographic Modules” at security level 4, the highest security level possible.

## Highlights

- *A high-end secure coprocessor implemented on a PCIe card with a multi-chip embedded module*
- *Foundation for secure applications, such as high-assurance digital signature generation or financial transaction processing*
- *Custom software options*
- *Hardware to perform AES, DES, T-DES, HMAC, random number generation, SHA-1, SHA-256, SHA-384, SHA-512, MD5, HMAC, and large number modular math functions for RSA (up to 4096-bit), ECC Prime Curve and other public-key cryptographic algorithms*
- *Secure code loading that enables updating of the functionality while installed in application systems*
- *IBM Common Cryptographic Architecture (CCA) API and security architecture*
- *Maximum flexibility and maximum trust while operating in physical environments that have minimum physical security*
- *Suitable for high-security processing and high-speed cryptographic operations*
- *Visa Data Secure Platform (DSP) Point-to-Point Encryption (P2PE) including Visa FPE encryption, decryption, and translation.*
- *AES encryption, decryption, and translation using CBC, ECB, or GCM mode.*
- *Tamper-responding programmable secure hardware designed to meet FIPS 140-2 Level 4 certification, the highest level of security*

*The 4767 HSM includes sensors to protect against attacks involving power manipulation, temperature manipulation, and penetration of the secure module.*

IBM provides the Common Cryptographic Architecture (CCA) Support Program that you can load into the coprocessor (HSM) to perform cryptographic functions common in the finance industry and in Internet business applications. You can also add custom functions to the HSM using an available programming toolkit or through IBM consulting services.




**Typical applications**

The IBM 4767 PCIe Cryptographic Coprocessor (HSM) 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 HSM and the opportunity to offload computationally intensive cryptographic processing.

**What is a secure HSM?**

A secure HSM is a general-purpose computing environment that withstands both physical 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 HSM 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 4767 hardware**

The IBM 4767 hardware provides significant performance and architectural extensions over its predecessor while enabling future growth. The secure module contains redundant IBM PowerPC 476 processors, custom symmetric key and hashing engines to perform AES, DES, T-DES, SHA-1, SHA-384, SHA-512, and SHA-2, MD5 and HMAC as well as public key cryptographic algorithm support for RSA and Elliptic Curve Cryptography. Other hardware support includes a secure real-time clock, hardware random number generator and a prime number generator. The secure module is protected by a tamper responding design that protects against a wide variety of attacks against the system.

*Reliability, Availability, and Serviceability (RAS)*

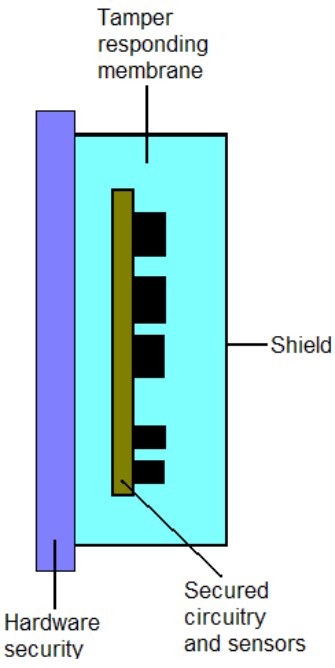
Hardware has also been designed to support the highest level of RAS requirements that enables the secure module to self-check at all times. This is achieved by running a pair of PowerPC processors in lock step and comparing the result from each cycle by cycle. Also all interfaces, registers, memory, cryptographic engines, and buses are protected at all times using parity, ECC, or CRC. Power on self-tests that are securely stored inside the secure module verify the hardware and firmware loaded on the module is secure and reliable at every power on.

*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 other keys and sensitive data. The public key of the coprocessor is certified at the factory by an IBM private key and the certificate is retained in the coprocessor. Subsequently, the private key of the coprocessor is used to sign the 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 4767 HSM has been designed to meet the FIPS 140-2 Level 4 requirements by protecting against attacks that include probe penetration or other intrusion into the secure module, side-channel attacks, power manipulation, and temperature manipulation. From the time of manufacture, the hardware is self-protecting by using tamper sensors to detect probing or drilling attempts. If the tamper sensors are triggered, the 4767 HSM destroys critical keys and certificates, and is rendered permanently inoperable. Note therefore that the 4767 HSM must be maintained at all times within the temperature, humidity, and barometric pressure ranges specified. Refer to the environmental requirements section of the technical references table on the last page.




A pair of batteries mounted on the coprocessor board provides backup power when the 4767 HSM 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).

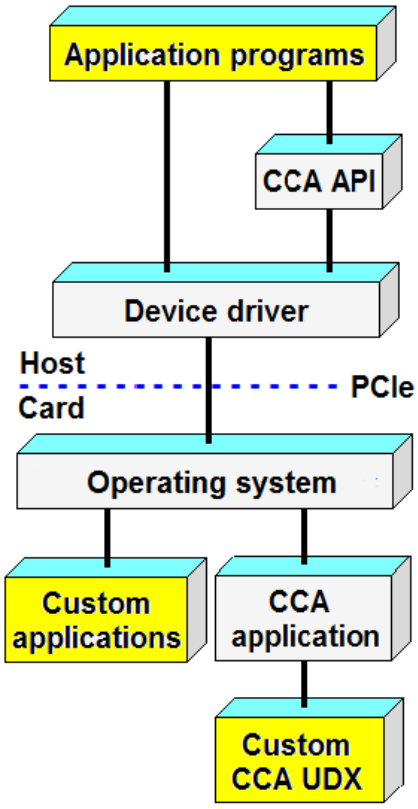
**IBM 4767 software**

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

**CCA Support Program highlights**

CCA includes these capabilities:

- AES, DES, and T-DES based data confidentiality and message integrity – AES, DES and T-DES CBC encryption and decryption, DES and T-DES MACs, CMAC, and HMAC
- Digital signature generation and verification using RSA or ECC with formatting according to PKCS#1, ISO 9796-1, and ANSI X9.31. RSA keys up to 4096 bits. ECC keys using NIST prime curves up to 521 bits and Brainpool curves up to 512 bits.
- Hashing using SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, MD5, and RIPEMD-160.
- PIN processing—several generation and verification processes, many PIN block formats, PIN translation to change keys or formats
- Support for German Banking Industry Committee, Die Deutsch Kreditwirtschaft (DK), financial services
- Variable-length symmetric key-token that meets key bundling requirements, enforces key usage, and tracks a key's lifecycle events and pedigree.
- Key distribution based on AES, DES, and RSA. Key agreement using Elliptic Curve Diffie-Hellman (ECDH).
- Secure generation of symmetric and asymmetric keys, including AES, DES, and T-DES, RSA (up to 4096 bits), and ECC (Prime curves up to 521 bits and Brainpool curves up to 512 bits).
- Support for smart card applications using the EMV® specifications




- Initialization and backup options
- 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 4767, with the same security as the other CCA functions.
- Generation of high-quality random numbers
- Refined key typing, to block attacks through misuse of the key-management system

**4767 technology in IBM servers**

The following IBM server families support 4767 technology, either directly or as orderable features.

- *x86—IBM 4767 can be ordered and installed. CCA support program for each supported operating system can be downloaded from the product website*
- *IBM System z—selected models offer an optional Crypto Express5S (CEX5S) feature. Support is provided by ICSF cryptographic services in z/OS. Support for the Crypto Express5S feature is provided for Linux on IBM System z by the CCA for Linux on System z rpm, available from ibm.com/security/cryptocards/pciecc2/ordersoftware.shtml*

**Custom software support**

The 4767 HSM 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 HSM, 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 HSM.

**Programming custom applications**

The 4767 HSM 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 that you can use to create and debug custom applications yourself. Toolkit documentation can be obtained from the product website. Because this is a specialized programming environment and 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 4767 and CCA. The courses can also be taught at your location, worldwide. These courses cover programming for the CCA API and the IBM 4767 installation and configuration.

In addition, custom courses can be arranged to cover other topics including programming and debugging applications that operate within the IBM 4767.

## HSM technical specifications:
## IBM 4767 PCIe Cryptographic Coprocessor

| **Physical characteristics** | |
|---|---|
| Card type: | Half-length PCIe card<br>PCI Local Bus Specification 2.2<br>PCIe specification 1.1 |
| Voltage: | +3.3 VDC ± 10% 23.44 W max |

**System requirements**

This section describes requirements for the system in which the 4767 is installed.

| | |
|---|---|
| **Software (downloadable from HSM 4767 link of product website):** | IBM CCA Support Program for use on:<br>• Red Hat Enterprise Linux 6.7 (64-bit)<br>• SUSE Linux 12 Service Pack 1 (64-bit) |
| **Hardware** | The coprocessor can be installed in a select x86 server. For a list of IBM-approved x86 servers for the 4767, go to the HSM 4767 link of the product website. From there, click on the Approved x86 servers link. |
| **Environmental requirements** | From the time of manufacture, the IBM 4767 PCIe Cryptographic Coprocessor card must be shipped, stored, and used within the following environmental specifications. Outside of these specifications, the IBM 4767 tamper sensors can be activated and render the IBM 4767 permanently inoperable. |

**IBM 4767**

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

| | |
|---|---|
| Temp shipping | -34°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 4767 PCIe Cryptographic Coprocessor can be found at the product website**,** 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
April 2016