

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. 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.

### 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 symmetric and hashing algorithms, including AES (CBC, ECB, GCM, XTS, CMAC, others), DES and T-DES (CBC, ECB, MAC, others), hashing (SHA-1, SHA-2, MD5) and HMAC
- Hardware to support asymmetric algorithms including large number modular math functions for RSA (up to 4096-bit) Elliptic Curve (Prime Curves to 521 and Brainpool Curves up to 512)
- Standards-compliant hardware random number generator
- Hardware-based prime number generator
- Secure code loading with hardware assisted image verification 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
- Tamper-responding programmable secure hardware meets FIPS 140-2 Level 4, the highest level of security

### Certifications

The IBM 4767 is validated by NIST ([certificate number 3164](#)) at FIPS 140-2 Level 4, the highest security level possible.

IBM Enterprise PKCS#11 firmware is [Common Criteria EAL4+ certified](#).

The IBM 4767 with CCA firmware is compliant with the [German Banking Industry Committee \(GBIC\)](#) security requirements.

Certification details are on page 5.

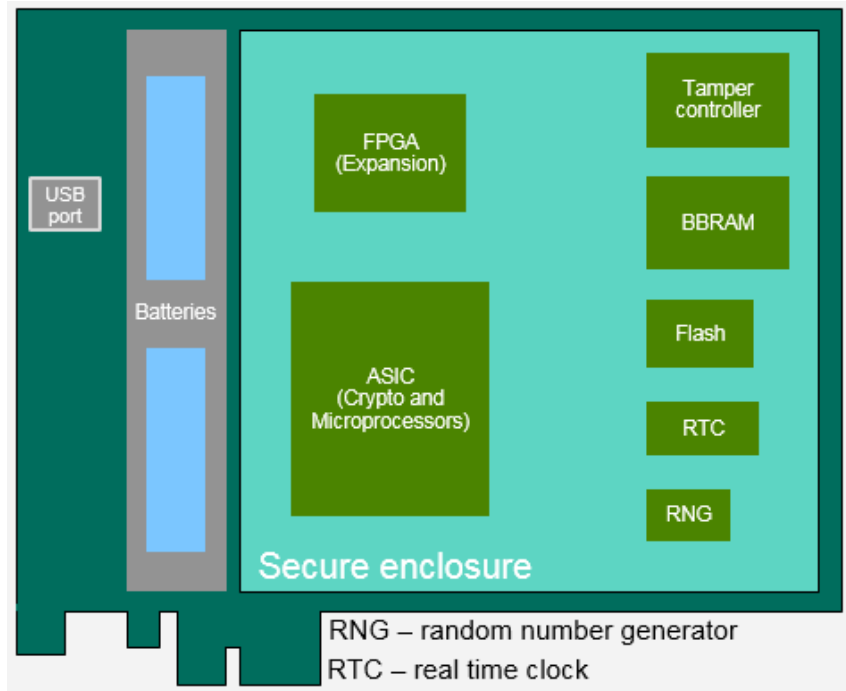
*The 4767 HSM includes sensors to protect against attacks involving power manipulation, temperature manipulation, and penetration of the secure module.*

### Software functionality

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, key management systems, 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 software that it is supposed to run, with confidence that the software has 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 improvements 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, and custom public key cryptographic algorithm engines to 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 and immediately destroys all keys and sensitive data if tampering is detected.

### 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 in the secure module verify the hardware and firmware loaded on the module is secure and reliable at every power on. Then, built-in RAS features check it continuously in real time.

### 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

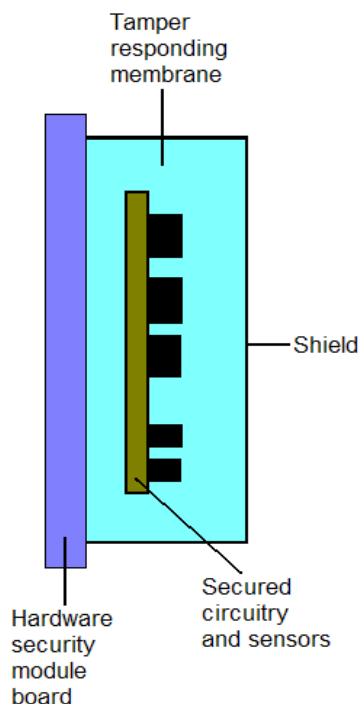
The 4767 HSM has been certified to meet the FIPS 140-2 Level 4 requirements by protecting against attacks that include penetration of

the secure module, side-channel attacks, and environmental failure protection (power or temperature manipulation). From the time of manufacture, the hardware is fully self-protecting. If tamper sensors detect a possible attack, all critical keys and other sensitive data are immediately destroyed and the HSM 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

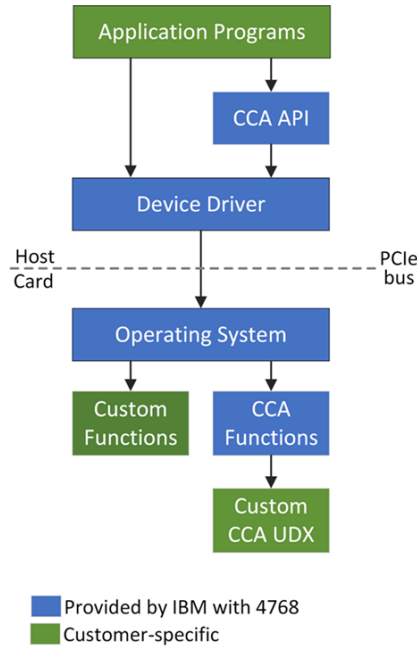
- IBM-supplied IBM Common Cryptographic Architecture (CCA) as a no-charge support program feature:
- Or choose customization options:
  - IBM custom development to your specification
  - Toolkit under custom contracts and export control



## 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. DUKPT key management is supported.
- 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 Power® Systems – selected models offer an optional cryptographic coprocessor feature, supported on IBM AIX®, IBM i®, and selected Linux® distributions.*
- *IBM 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 <https://www.ibm.com/security/cryptocards/pciacc2/tonzsoftware.shtml>.*

## Programming custom HSM functions

It is possible to implement custom functions in the 4767 to meet specialized needs. Two options are available. User Defined Extensions (UDX) use CCA as a starting point and add new functions to the standard CCA API set. This is the approach that is most commonly used. However, when your application is substantially different from CCA, a complete custom application can be built on top of the HSM's embedded Linux environment. With this method, you can implement very different approaches to cryptographic applications, or even non-cryptographic applications that benefit from running in a secure processing environment.

The internal environment of the 4767 consists of an embedded Linux operating system and associated device drivers for the HSM's specialized hardware. IBM provides documented API functions that custom software can use to perform cryptographic operations or to assist their applications in other ways. Your custom application is digitally signed using a key that you generate yourself, and the application is securely loaded to the HSM using the same FIPS 140-2 certified processes that are used to protect IBM-provided HSM code.

## Custom programming services

The 4767 HSM represents a specialized programming environment with its own tools, debug aids, and code release procedures. Customers may not want to learn how to create applications in this environment. In this case, they can obtain custom programming services through an experienced IBM services team or through selected contractors. IBM is pleased to jointly develop specifications and quote on custom solutions.

## Custom software Toolkit

Alternatively, IBM offers a toolkit that you can use to create and debug custom applications yourself. Toolkit documentation can be obtained from the [IBM CryptoCards 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 this 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.

## Certification Information

The IBM 4767 is certified at FIPS 140-2 Level 4, at Common Criteria EAL4+, and by the German Banking Industry Committee (GBIC).



The IBM 4767 is validated by NIST ([certificate number 3164](#)) at FIPS 140-2 Level 4, the highest security level possible.

Certificate No. 3164  
TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

The IBM 4767 with IBM Enterprise PKCS#11 firmware is [Common Criteria Part 3 conformant \(EAL4+\)](#).



The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.



The IBM 4767-002 with CCA version 5.3 firmware fulfills the security requirements of the [German Banking Industry Committee \(GBIC\)](#). The report is listed under number 3299.

The CCA release 5.3 provides sophisticated state-of-the-art protections for handling sensitive information like PIN data, cryptographic key data and account data.

The HSM IBM Model 4767-002 CCA Release 5.3 implementation is compliant with GBIC's security requirements.

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



© Copyright IBM Corporation 2016, 2018

**Physical characteristics**

<b>Card type:</b>	Half-length PCIe card PCI Local Bus Specification 2.2 PCIe specification 1.1
<b>Voltage:</b>	+3.3 VDC ± 10% 23.44 W max

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

Produced in the United States of America  
April 2018

**System requirements**

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

**Software (downloadable from HSM 4767 download software link of the [product website](#)):** IBM CCA Support Program for use on Linux, Windows, or AIX. See the [operating system reference chart](#) for a list of supported operating systems.

**Hardware:** The coprocessor can be installed in selected IBM Z models and selected IBM Power servers as a feature, as well as in x86 servers that meet the environmental requirements listed below. For details, see [IBM 4767 x86 servers](#).

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, ibm.com, IBM Z, System z, Power Systems, and z/OS are trademarks or registered trademarks of IBM Corporation in the United States, other countries or both.

Linux is a registered trademark of Linus Torvalds 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.

EMV is a trademark owned by EMVCo LLC.

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.

**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).

<b>Temp shipping</b>	-34°C to +60°C
<b>Pressure shipping</b>	min 550 mbar
<b>Humidity shipping</b>	5% to 100% RH

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

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

**Operation (ambient in system)**

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

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.

**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.