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

IBM CEX6S (4768) 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 CEX6S 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 HSM 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 TDES (CBC, ECB, MAC, EMVMAC, X9.19, X9.9, others), hashing (SHA-1, SHA-2* (224-512)*, MD5, RIPEMD-160, MDC-2, MDC-4, PADMDC-2, PADMDC-4) and HMAC*
- *Hardware to support asymmetric algorithms including large number modular math functions for RSA (up to 4096-bit) Elliptic Curve (Prime curves up to 521 and Brainpool curves up to 512)*
- *Standards-compliant hardware random number generator*
- *Hardware-based prime number generator*
- *Scaling is supported through bundling of multiple adapters to meet the highest throughput requirements*
- *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*
- *IBM Enterprise PKCS #11 (EP11)*
- *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 designed to meet the highest level of security for FIPS 140-2 Level 4, Common Criteria, and PCI HSM certifications*

Certifications

The IBM CEX6S is validated by NIST (certificate number 3410) at FIPS 140-2 Level 4, the highest security level possible.

The IBM CEX6S with CCA 6.0 has PCI HSM certification.

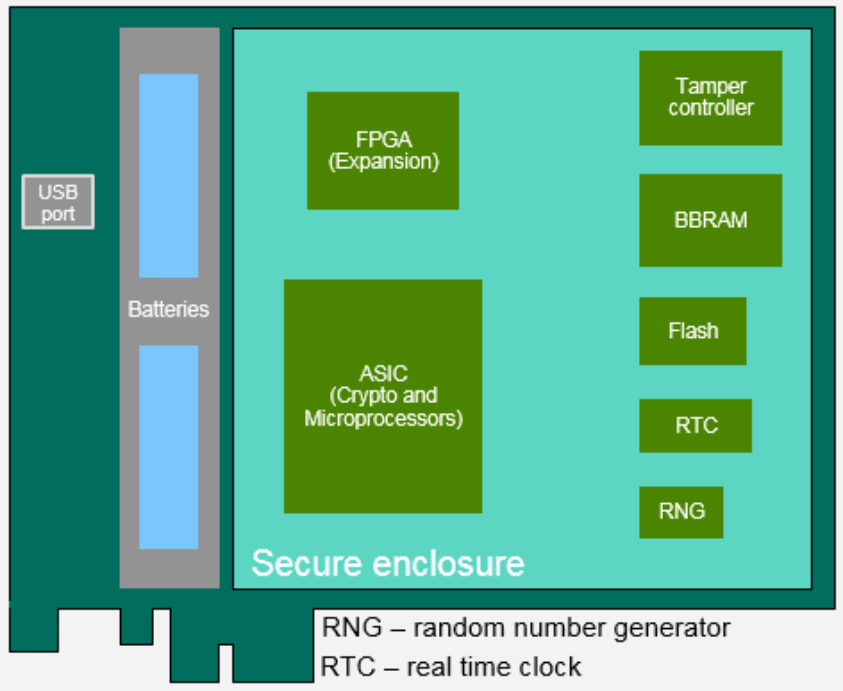
EP11 running on the CEX6S meets the requirements for conformance with Common Criteria Part 3.1 (rev. 4) with Evaluation Assurance Level (EAL) 4.

The CEX6S HSM includes sensors to protect against attacks involving power manipulation, temperature manipulation, and penetration of the secure module.

Software functionality
The IBM CEX6S adapter provides three modes of operation:
- Common Cryptographic Architecture (CCA) (financial transaction focus),
- IBM Enterprise PKCS #11 (EP11) (internet business application focus), and
- Accelerator mode for offload of computer intensive operations in clear key mode.

These modes are exclusive, so only one mode can be present at any time. With CCA, you can also add custom functions to the HSM through IBM consulting services.

Typical applications
The IBM CEX6S 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, PKCS #11 applications in general, 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.

Relevant Cryptographic Standards Supported by the IBM CEX6S HSM

FIPS 140	X9.8 / ISO 9564	GBIC (DK), MEPS
PCI-HSM	TR-31	NIST SP 800-90A
Common Criteria	X9.97 / ISO 13491	PKCS #1
X9.24 Parts 1, 2, and 3	X9.102	PKCS #11

IBM CEX6S hardware

The IBM CEX6S hardware provides significant performance 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, TDES, SHA-1 and SHA-2, MD5 and HMAC, and custom public key cryptographic algorithm engines to support RSA and Elliptic Curve Cryptography (ECC). 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)

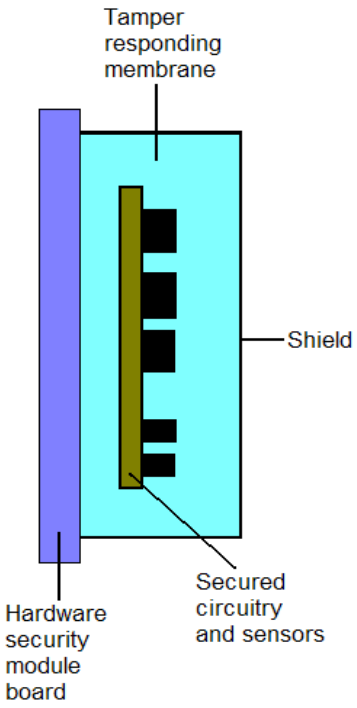
Hardware has also been designed to support the highest level of RAS requirements that enable the secure module to self-check at all times. This is achieved by running a pair of PowerPC processors in lock step and comparing the result from each cycle by cycle. Also, all interfaces, registers, memory, 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, the built-in RAS features check it continuously in real time.

Embedded certificate

During the final manufacturing step, the HSM 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 HSM, protecting this private key as well as other keys and sensitive data. The public key of the HSM is certified at the factory by an IBM private key and the certificate is retained in the HSM. Subsequently, the private key of the HSM is used to sign the HSM status responses which, in conjunction with a series of public key certificates, demonstrate that the HSM remains intact and is genuine.

Tamper responding design

The CEX6S HSM has been verified 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 CEX6S 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.



CEX6S technology in IBM servers

The IBM CEX6S is available on select IBM Z servers, which offer an optional CEX6S feature. On z/OS, support is provided by ICSF cryptographic services. On Linux on IBM Z, support for the CEX6S feature is provided by the CCA for Linux on Z package or the EP11 host package, here: www.ibm.com/security/cryptocards/pciecc3/lonzsoftware.

IBM CEX6S software

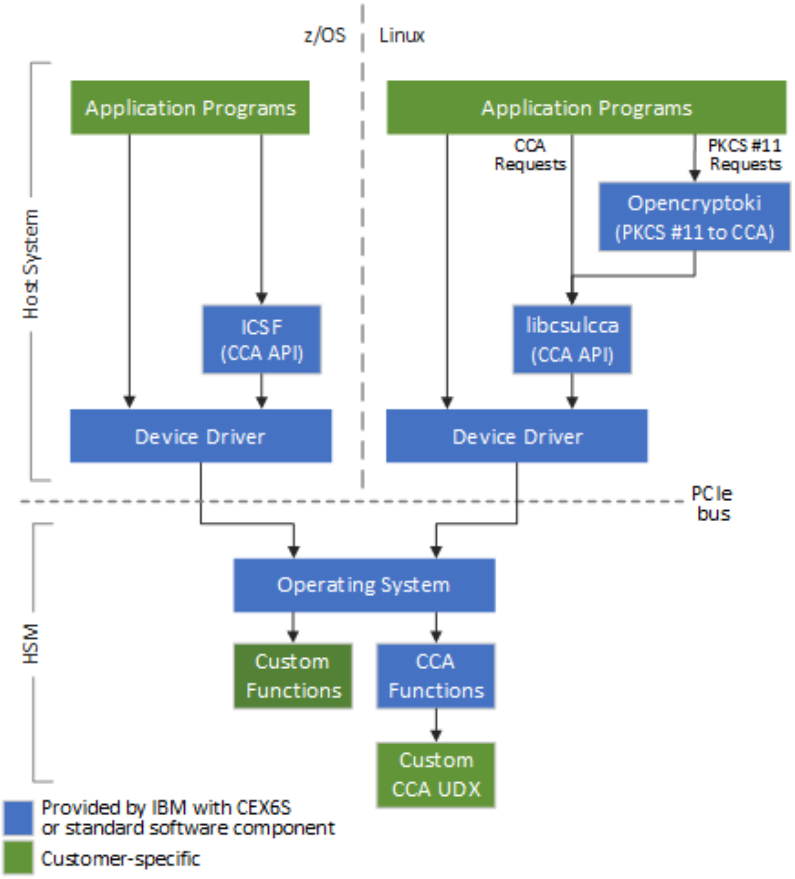
- IBM-supplied IBM Common Cryptographic Architecture (CCA), which includes the option for IBM custom development to your specification.
- IBM-supplied IBM Enterprise PKCS #11 (EP11).

Both come as a no-charge support program feature.

CCA highlights

CCA includes these capabilities:

- Data confidentiality using AES, DES, and TDES.
- Message integrity using AES, DES and TDES MAC, CMAC, and HMAC.
- Digital signature generation and verification using RSA or ECC with formatting according to PKCS #1, RSA-PSS, 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-2, 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 TDES, 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.
- HSM initialization options, a wide variety of backup capabilities for the HSM, and the ability to clone to another HSM.
- Administrative commands digitally signed by administrators and verified in the HSM.
- 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 CEX6S, 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 functions.
- Secrets stored externally are cryptographically protected against disclosure or modification.
- PCI PTS HSM compliance-tagged DES, AES, and RSA key tokens are usable alongside existing keys and services in a non-disruptive fashion.
- X9 TR-34 key exchange services for secure remote key load of ATMs.
- Non-disruptive transition to PCI PTS HSM mode.
- Secure Audit Log hosted from the HSM as required by the PCI PTS HSM standard.
- Secure public key infrastructure: native X.509 certificate support including PKCS #10 certificate request generation through a new PKI hosted from the HSM.
- Assistance for planning the migration to PCI-HSM compliance mode using run-time analysis and reporting by the HSM.
- Certain classes of HSM-protected AES and TDES keys can be securely exported to CPACF.



If you have additional questions about the IBM CEX6S or about CCA, please contact crypto@us.ibm.com.

Custom software support

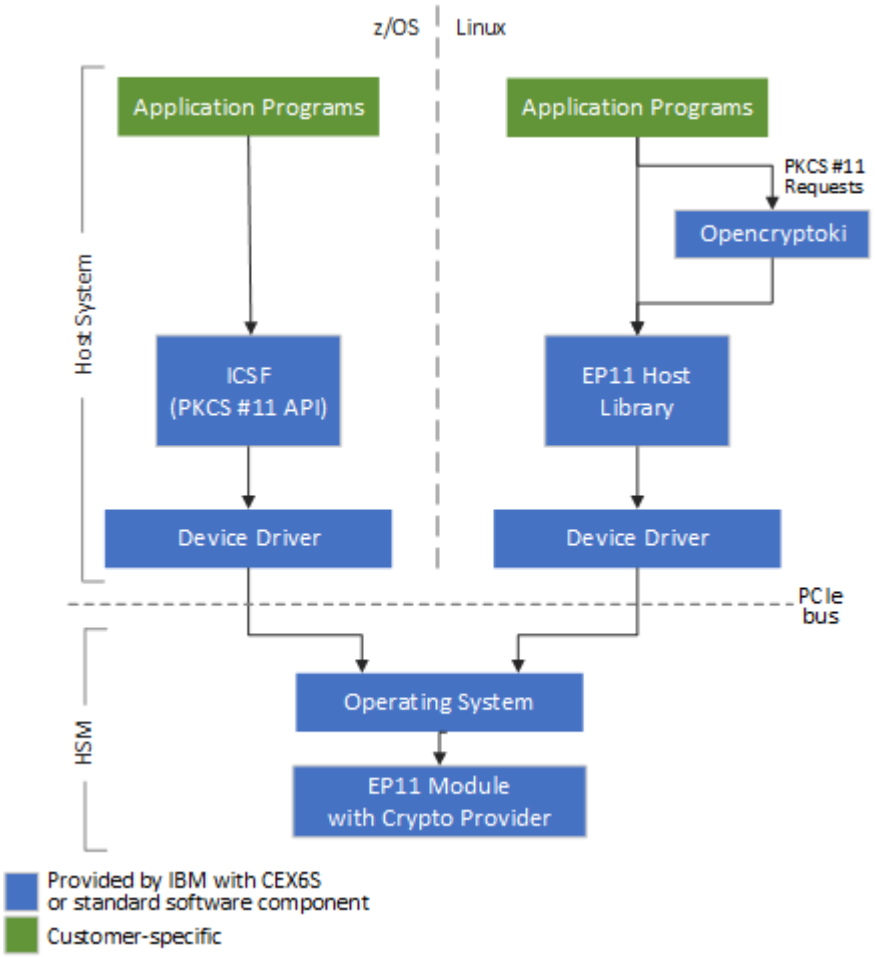
The CEX6S HSM contains firmware to manage its specialized hardware and uses hardware and firmware to control loading of additional software based on HSM-validated digital signatures. Software support includes the embedded Linux operating system and special device drivers, which provide the platform for 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.

Programming custom applications

IBM offers custom programming services through an experienced IBM team that is familiar with the CEX6S' specialized programming environment, tools, debug aids, and code release procedures. IBM is pleased to jointly develop specifications and provide quotes on custom solutions.

EP11 highlights

EP11 includes these capabilities:



- Support for PKCS #11 version 2.20.
- Data confidentiality using AES and TDES.
- Message integrity using AES and TDES MAC, CMAC, and HMAC.
- Digital signature generation and verification using RSA or ECC with formatting according to PKCS #1, RSA-PSS, and RSA-OAEP (SHA-1 only). 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 and SHA-2.
- EP11 login sessions – bind objects to a specific user to allow for fine-grained usage control of objects.
- Attribute-bound keys – transport secrets securely without losing attributes between different systems.
- Secure Wrapping Key (WK) cloning and domain or card state export and import.
- Enforcing usage policies and support for binding objects to specific operational modes.
- Secure audit facility.
- Generation of high-quality random numbers.
- Trustable public keys through integrity-protected SPKIs with MAC.
- Secrets stored externally are cryptographically protected against disclosure or modification.
- Wrapped content is authenticated with a MAC key that is derived from the WK.
- Wrapping keys can only be loaded encrypted using importer keys.
- Administrative commands are signed by M-of-N administrators before the command is accepted by the HSM.
- Allows binding of objects to specific operational modes enforcing using objects only on backends where specific policies are activated.
- The system is stateless, keeping most of the secrets outside the HSM in wrapped and MACed form, allowing maximizing throughput and a potential unlimited number of users.
- The transport protocol that is used between the backend and the host library is documented and published.
- Secure generation of symmetric and asymmetric keys for AES, TDES, DH, DSA, RSA (up to 4096 bits), and ECC (Prime curves up to 521 bits, Brainpool curves up to 512 bits, and the Secp256k1 curve).
- Key distribution based on AES, DES, and RSA. Key agreement using Diffie-Hellman (DH) and ECDH.

If you have additional questions about EP11, please contact EP11SUPP@de.ibm.com.

HSM technical specifications:
IBM CEX6S PCIe Cryptographic Coprocessor

Physical characteristics

Card type:	Half-length PCIe x4 card PCI Local Bus Specification 2.2 PCIe specification 1.1
Voltage / Power consumed: Required:	+3.3 VDC ± 10% 23.44 W max 25 W min

System requirements

The 4768 Cryptographic Coprocessor is only supported on IBM z14 as the Crypto Express6S.

Environmental requirements	From the time of manufacture, the IBM CEX6S PCIe Cryptographic Coprocessor card must be shipped, stored, and used within the following environmental specifications. Outside of these specifications, the IBM CEX6S tamper sensors can be activated and render the IBM CEX6S permanently inoperable.

IBM CEX6S

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 CEX6S PCIe Cryptographic Coprocessor can be found at the IBM CryptoCards product website**.** You can also 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
August 2019