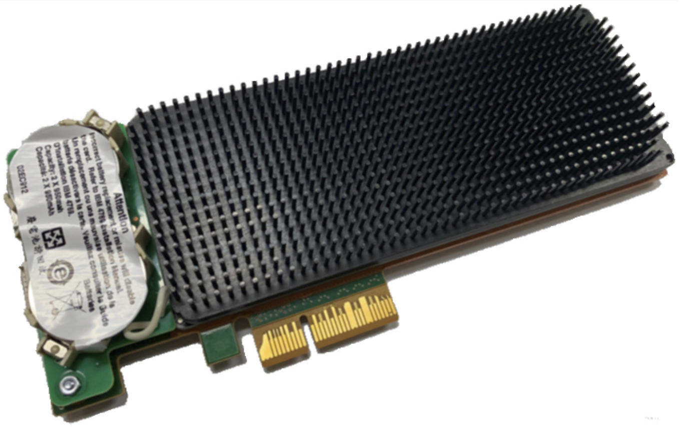
Use the IBM® 4770 hardware security module (HSM) to provide a flexible solution to your high-security cryptographic processing needs.

IBM CEX8S / 4770 PCIe Cryptographic Coprocessor (HSM)



Highlights

- *A high-end secure HSM (Hardware Security Module) implemented on a PCIe card with an IBM designed ASIC, designed to meet the highest level of security certification*
- *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), *SHA-3, 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, Brainpool curves up to 512), Curve25519, Curve448 for Elliptic Curve Diffie-Hellman (ECDH), Key Encapsulation Mechanism (KEM) CRYSTALS-Kyber), and Signature generation/verification (ECDSA , EC-SDSA, EdDSA, CRYSTALS-Dilithium).*
- *Standards-compliant hardware-based random number generator*
- *Secure code load with hardware assisted image verification that enables update of function while installed in application systems*
- *ASC X9 TR-31/X9.143 Key Block support and X9 TR-34 Remote Key Load via asymmetric means*
- *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. Protection against penetration of the secure module, side-channel attacks, power and temperature manipulation is in place from the time of manufacture, destroying secrets and rendering the HSM permanently inoperable on tamper detection.*
- *Reliability, Availability, and Serviceability (RAS) with continuous real-time self-check. Two pairs of PPC-476 processors run in lock step with per-cycle comparison. All interfaces, memory and cryptographic engines are protected using parity, ECC, or CRC.*

Cryptography is ubiquitous in modern systems for protection of the privacy and confidentiality of data, ensuring data integrity, and providing user accountabilit through digital signature techniques.

The IBM 4770 PCIe Cryptographic Coprocessor is a programmable PCIe card HSM that offloads cryptographic processes from the host and performs sensitive tasks unsuitable for general-purpose computers.

The IBM 4770 provides these advantages over previous HSMs:

- Enhanced security algorithms
- Improved position for security certifications
- Improved performance
- Better simulation capabilities
- added cryptographic algorithms
- Quantum Safe and classical algorithm use for code load security and firmware image integrity, as well as HSM status and run-time integrity attestation.

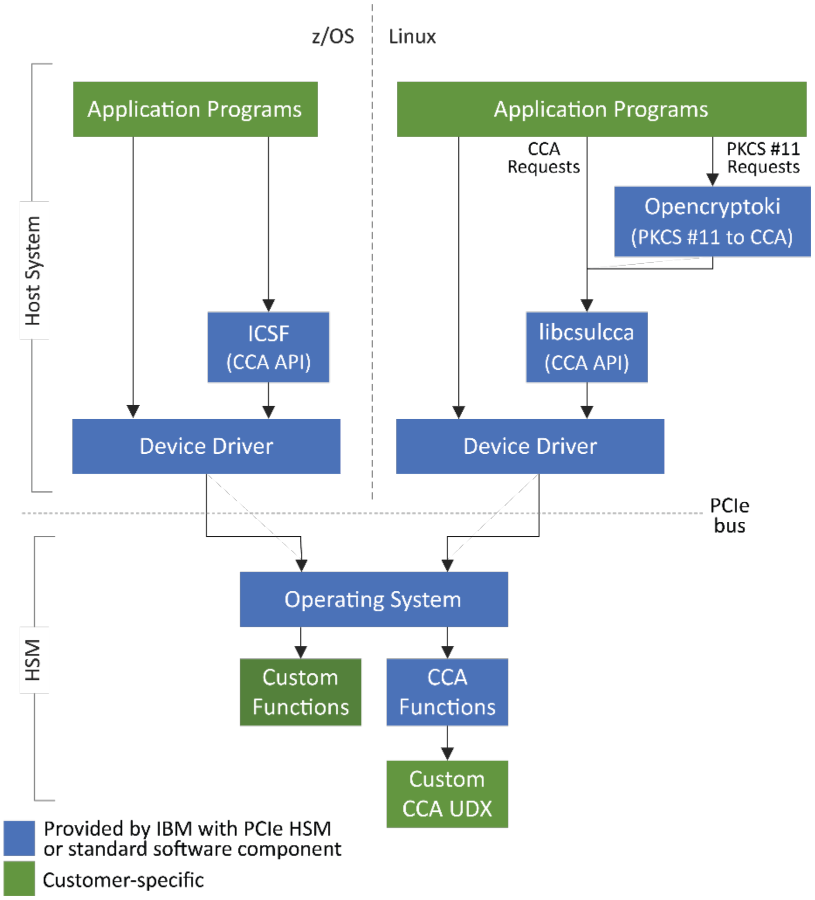
Three Modes of Operation

- Common Cryptographic Architecture (CCA) (financial transaction focus), as well as custom programming
- IBM Enterprise PKCS #11 (EP11) (internet business application focus including FinTech), and
- Accelerator mode for offload of compute-intensive operations in clear key mode

4770 in IBM servers

IBM z16® servers offer an optional Crypto Express8S (CEX8S) feature. On z/OS®, use ICSF cryptographic services. On Linux® on IBM Z, use the CCA for Linux on Z package or the EP11 Support Program, available from CEX8S/4770 Linux on Z.

CCA highlights



CCA includes these capabilities:

- Secure key generation and PCI compliant wrapping with user controlled wrapping keys.
- Data confidentiality using AES, DES/TDES.
- Message integrity using AES, DES and TDES MAC, CMAC, and HMAC.
- Digital signature generation and verification using CRYSTALS-Dilithium, RSA or ECC with formatting 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, Brainpool curves up to 512 bits, Edwards and Koblitz curves. ECSDSA (Schnorr) is also supported.
- Key Encapsulation Mechanism [KEM] CRYSTALS-Kyber.
- Format Preserving Encryption methods FF1, FF2, FF2.1
- Hash using SHA-1, SHA-2, SHA-3.
- PIN processing—several generation and verification processes, AES and many TDES PIN block formats, PIN translation to change keys or formats. TDES and AES DUKPT key management.
- Support for German Banking Industry Committee, *Die Deutsch Kreditwirtschaft* (DK), financial services.
- *Visa Data Secure Platform (DSP) Point-to-Point Encryption (P2PE) including Visa FPE encryption, decryption, and translation*
- Key distribution based on AES, DES, and RSA. Key agreement using Elliptic Curve Diffie-Hellman (ECDH) and a hybrid scheme which uses CRYSTALS-Kyber.
- X9 TR-31/X9.143 native key block support as well as PCI-reviewed proprietary key blocks.
- X9 TR-34 key exchange services for secure remote key load of ATMs.
- 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 4770, with the same security as the other CCA functions.
- Generation of high-quality random numbers that conform to NIST SP800-9A.
- Refined key typing to block attacks through misuse of the key-management functions.
- Secrets stored externally are cryptographically protected against disclosure or modification.
- Non-disruptive transition to PCI PTS HSM mode.
- PCI PTS HSM compliance-tagged DES, AES, and RSA key tokens are usable alongside existing keys and services in a non-disruptive fashion.
- 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 IBM Z CPACF feature for high performance use cases.

If you have additional questions about the IBM 4770 or about CCA, please contact crypto@us.ibm.com.

Custom software support

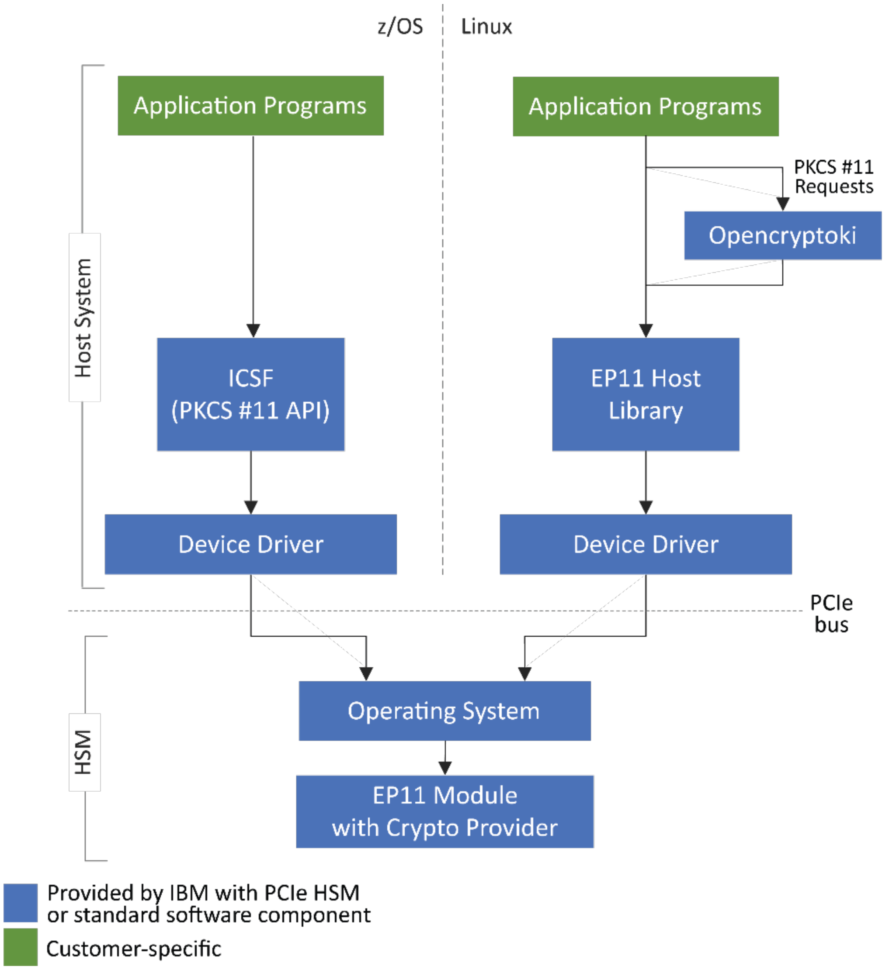
Developing additional functions through User Defined Extensions (UDXs) using CCA as a starting point can be more economical and less time-consuming than creating an entirely new application. Special key management functions and PIN processing routines are typical extensions.

Programming custom applications

IBM offers custom programming services through an experienced IBM team that is familiar with the 4770's specialized programming environment. IBM is pleased to jointly develop specifications and provide quotes on custom solutions.

EP11 highlights

EP11 includes these capabilities:



- Support for PKCS #11 version 2.40.
- 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. RSA keys up to 4096 bits. ECC keys using NIST Prime curves up to 521 bits, Brainpool curves up to 512 bits, Edwards curves ed25519 and ed448 or curve secp256k1.
- Schnorr Signatures (ECSDSA).
- Support for deterministic hierarchical wallet key derivation schemes according to BIP0032 or SLIP0010.
- Hashing using SHA-1, SHA-2, and SHA-3.
- 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.
- Protected key data key import for TDES, AES and EC (private-)keys (Prime, Brainpool and Edwards curves).
- 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, the Secp256k1 curve, and the Edwards curves ed25519 and ed448).
- Key distribution based on AES, DES, and RSA. Key agreement using Diffie-Hellman (DH) and ECDH using standardized key derivation formats (Prime curves, Brainpool curves and the Montgomery curves c25519 and c448).
- Quantum safe cryptography support for the digital-signature algorithm CRYSTALS-Dilithium round 2 (8,7), round 3 (6,5), and round 3 (8,7). It is also the first time that CRYSTALS Kyber for quantum-safe encryption and decryption as well as key encapsulation is supported with security levels 768 and 1024.

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

HSM technical specifications:
IBM 4770 PCIe Cryptographic Coprocessor

Physical characteristics

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

System requirements

The 4770 Cryptographic Coprocessor is only supported on IBM z16 as the Crypto Express8S.

Environmental requirements

From the time of manufacture, the IBM 4770 PCIe Cryptographic Coprocessor card must be shipped, stored, and used within the following environmental specifications. Outside of these specifications, the IBM 4770 tamper sensors can be activated and render the IBM 4770 permanently inoperable.

IBM 4770

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

Temp	-34°C to +60°C
Humidity	5% to 100% RH
Pressure	min 550 mbar (maximum altitude 16 400 feet)

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

Temp	+1°C to +60°C
Humidity	5% to 80% RH
Pressure	min 550 mbar (maximum altitude 16 400 feet)

Operation (ambient in system)

Temp	+5°C to +40°C
Humidity	8% to 85% RH
Pressure / altitude (max)	min 550 mbar (maximum altitude 16 400 feet)
Airflow (minimum)	300 LFM (air velocity over the secure module)

For more information

Documentation and publications, ordering procedures, and news concerning the IBM 4770 PCIe Cryptographic Coprocessor can be found at the IBM CryptoCards product website**. You can also** call IBM DIRECT at 1-800-IBM-CALL in North America 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 2022, updated June 2023

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 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.