IBM 4765 Cryptographic Coprocessor for select IBM System x servers -- A security-rich solution for smarter computing

Table of contents

1 Overview
2 Key prerequisites
2 Planned availability date
2 Description
3 Product positioning
4 Product number
4 Publications
5 Technical information
10 Pricing
10 Announcement countries

At a glance

The IBM® 4765 Cryptographic Coprocessor is a security-rich PCIe coprocessor with specialized electronics to support cryptographic functions on select IBM System x® servers with a PCIe slot.

The PCIe Cryptographic Coprocessor is designed to deliver the following functions:

- Rivest-Shamir-Adleman (RSA) algorithm based digital signature generation and verification with keys up to 4096 bits in length
- High throughput SHA, MDS, and Hash-based Message Authentication Code (HMAC), Triple-DES, Single-DES and Advanced Encryption Standard (AES) based encryption for data integrity assurance and confidentiality, including AES Key Wrap (AESKW) conforming to ANS X9.102
- Elliptic Curve Cryptography (ECC) for digital signature and key agreement
- Support for smart card applications and Personal Identification Number (PIN) processing
- Secure time-of-day
- Uninterrupted continuous operation while updating embedded Common Cryptographic Architecture (CCA) application

Overview

The IBM 4765 Cryptographic Coprocessor is designed to provide security-rich features and to deliver high throughput for cryptographic functions on select IBM System x servers. Refer to the ServerProven® website


The cryptographic processes are performed within an enclosure on the board that is certified to the Federal Information Processing Standard (FIPS) 140-2 level 4, the highest level of certification achievable for commercial cryptographic devices.

Support for the following 4765 Cryptographic Coprocessor functions are controlled by an embedded operating system running on two 32-bit PowerPC® microprocessors in lockstep:

- Specialized hardware that performs Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple-Data Encryption Standard (TDES), Rivest-Shamir-Adleman (RSA) algorithm, Secure Hash algorithms (SHA), Elliptic Curve
IBM offers a Common Cryptographic Architecture (CCA) Support Program for the 4765 Cryptographic Coprocessor, at no charge, to the user.

CCA for the 4765 Cryptographic Coprocessor is an enhanced version of the CCA Support Program shipped with the 4764-001 PCI-X Cryptographic Coprocessor.

**Key prerequisites**

- All versions of select IBM System x servers with at least two, or possibly three PCIe slots that are adjacent.

  **Note:** An IBM 4765 Cryptographic Coprocessor can be installed in an end slot, which requires two slots that are adjacent. Otherwise, three slots that are adjacent are required.

- SUSE Linux™ Enterprise Server 11.1 from Novell, 32 bit.
- IBM-supplied, at no charge, support program.

In the future, when the 4765 Cryptographic Coprocessor has been successfully tested with servers other than select IBM System x servers, they will be listed at the 4765 Cryptographic Coprocessor ServerProven website.

When a system is listed as ServerProven, it is considered an IBM-supported environment. The link to the IBM 4765 Cryptographic Coprocessor ServerProven website is


**Planned availability date**

May 31, 2011

Availability of programs with an encryption algorithm in France is subject to French government approval.

**Description**

The tamper-responding hardware and infrastructure firmware of the IBM 4765 Cryptographic Coprocessor meet the most stringent Federal Information Processing Standards Publication (FIPS PUB) 140-2 Level 4 level of security. Specialized hardware performs Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple-Data Encryption Standard (TDES), Rivest-Shamir-Adleman (RSA) algorithm, Secure Hash algorithms (SHA), Elliptic Curve Cryptography (ECC), and other cryptographic processes, relieving the main processor from these tasks.

The 4765 Cryptographic Coprocessor is designed to protect your cryptographic keys and sensitive custom applications. The software running in the coprocessor offers a rich programmable environment to meet unique business needs and can be customized to meet special requirements such as on demand transactions,
automated teller machines (ATMs), and point-of-sale (POS) applications for the banking, finance, and retail industries.

**Design features**: The IBM 4765 Cryptographic Coprocessor has a PCIe local-bus-compatible interface. The coprocessor holds a secure subsystem module, batteries for backup power, and a full-speed USB 2.0 host port available through a mini-A connector. The securely encapsulated subsystem contains two 32-bit PowerPC 405Gr RISC processors running in lockstep with cross-checking to detect malfunctions as well as a separate service processor used to manage self-test and firmware updates, RAM, flash memory and battery-powered memory, secure time-of-day, cryptographic-quality random number generator, AES, DES, TDES, HMAC, MD5, multiple SHA hashing methods, modular-exponentiation (for example, RSA, ECC) hardware, and full-duplex DMA communications.

A secure code-loading arrangement enables control program and application program loading and refreshes after coprocessor installation in your server. IBM offers an embedded subsystem control program and a cryptographic application programming interface (API) which implements the IBM Common Cryptographic Architecture (CCA).

IBM offers support for application programs that use the 4765 Cryptographic Coprocessor in select IBM System x servers and that operate within the Novell SUSE Linux Enterprise Server 11.1 environment. The IBM Common Cryptographic architecture Support Program can be accessed from the Internet at no charge to the user. Refer to the *IBM CCA Basic Services Reference and Guide* which can be found at the IBM 'Cryptocards' website for a full explanation of the CCA API

http://www.ibm.com/security/cryptocards

**Custom programming support**: IBM offers a toolkit, education, consulting, support, and prototyping under custom contracts to allow you to extend the IBM features or use them to create your own on-card application.

Under a special contract with IBM, you will have the flexibility to define and load customized cryptographic functions. This service offering can be requested using the IBM 'Cryptocards' website by selecting the 'Custom programming' link

http://www.ibm.com/security/cryptocards

**Product positioning**

The IBM 4765 Cryptographic Coprocessor is an integral part of the overall security-rich solution for smarter computing, and is designed to provide high security and to deliver high throughput for cryptographic functions on select IBM System x servers.

A cryptographic hardware subsystem is a critical feature required by the vast majority of enterprises in the public sector and the banking and financial industry.

The 4765 Cryptographic Coprocessor is designed to replace the 4764-001 PCI-X Cryptographic Coprocessor which will be withdrawn from marketing December 31, 2011. Refer to Withdrawal Announcement ZG11-0191, dated May 24, 2011.

You may be interested in deploying cryptographic hardware technology in select IBM System x servers if you are:

- Implementing systems that require high security for your cryptographic keys and high assurance the cryptographic processor has not been tampered with or modified in any way
- Implementing applications that process financial transactions including automated teller machine (ATM) Personal Identification Numbers (PINs) and credit card transactions
- Implementing support for EMV (EMVCo) smart card applications
- Implementing secure cryptographic key management
- Implementing card personalization systems
- Using RSA public-key cryptography for digital signatures or key management
- Using Elliptic Curve public-key cryptography for digital signatures
- Using e-commerce applications requiring Secure Electronic Transaction (SET)
- Desiring the security and/or compatibility afforded by an implementation of portions of the IBM Common Cryptographic Architecture

The 4765 Cryptographic Coprocessor provides high throughput for cryptographic operations. Visit the following website for performance details:

http://www.ibm.com/security/cryptocards

### Product number

<table>
<thead>
<tr>
<th>Description</th>
<th>Machine type</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>4765 Crypto Coprocessor</td>
<td>4765</td>
<td>001</td>
</tr>
</tbody>
</table>

### Publications

The following publications are shipped with the product:

- IBM Statement of Limited Warranty - Warranty Information flyer, SC23-6884-00 (Multi-language)
- IBM License Agreement for Machine Code (contains form Z125-5468-04), SC28-6872-01 (Multi-language)
- IBM License Agreement for Machine Code Addendum for Elliptical Curve Cryptography (contains form Z125-8449-00), GC27-2612-00 (Multi-language)
- IBM 4765 PCIe Cryptographic Coprocessor Safety Notices, G325-2638-00 (Multi-language)
- Notice to Users of the IBM 4765 Cryptographic Coprocessor, P/N 80Y2344
- Slot Cover Label Instructions sheet, P/N 46K3930

The **IBM 4765 PCIe Cryptographic Coprocessor Installation Manual** can be downloaded from the following website beginning May 31, 2011:

http://www.ibm.com/security/cryptocards

These publications, in US English versions, can be downloaded over the Internet as PDF files for viewing and printing using Adobe's Acrobat Reader, beginning May 31, 2011.

- IBM 4765 PCIe Cryptographic Coprocessor Installation Manual
- IBM 4765 PCIe Cryptographic Coprocessor CCA Support Program Installation Manual
- IBM CCA Basic Services Reference and Guide for the IBM 4765 PCIe and IBM 4764 PCI-X Cryptographic Coprocessors

For Internet retrieval, visit the following website:

http://www.ibm.com/security/cryptocards

The publications listed can be downloaded from the following website beginning May 31, 2011:

http://www.ibm.com/security/cryptocards

- IBM Statement of Limited Warranty - Warranty Information flyer, SC23-6884-00 (Multi-language)
- IBM License Agreement for Machine Code (contains form Z125-5468-04), SC28-6872-01 (Multi-language)
IBM License Agreement for Machine Code Addendum for Elliptical Curve Cryptography (contains form Z125-8449-00), GC27-2612-00 (Multi-language)
IBM 4765 PCIe Cryptographic Coprocessor Safety Notices, G325-2638-00 (Multi-language)

Displayable softcopy publications

These publications, in US English versions, can be downloaded over the Internet as PDF files for viewing and printing using Adobe's Acrobat Reader, May 31, 2011.

- IBM 4765 PCIe Cryptographic Coprocessor Installation Manual
- IBM 4765 PCIe Cryptographic Coprocessor CCA Support Program Installation Manual
- IBM CCA Basic Services Reference and Guide for the IBM 4765 PCIe and IBM 4764 PCI-X Cryptographic Coprocessors

For Internet retrieval, refer to the following website

http://www.ibm.com/security/cryptocards

Services

Global Technology Services

IBM services include business consulting, outsourcing, hosting services, applications, and other technology management.

These services help you learn about, plan, install, manage, or optimize your IT infrastructure to be an On Demand Business. They can help you integrate your high-speed networks, storage systems, application servers, wireless protocols, and an array of platforms, middleware, and communications software for IBM and many non-IBM offerings. IBM is your one-stop shop for IT support needs.

For details on available services, contact your IBM representative or visit

http://www.ibm.com/services/

For details on available IBM Business Continuity and Recovery Services, contact your IBM representative or visit

http://www.ibm.com/services/continuity

For details on education offerings related to specific products, visit


Select your country, and then select the product as the category.

Technical information

Specified operating environment

Physical specifications
- Length: 167.65 mm (6.60 in)
- Thickness: 14.3 mm (0.57 in)
- Height: 111.15 mm (4.38 in)

The PCIe adapter is a "short type" adapter which complies with the electrical and mechanical requirements defined by:

- PCI Local Bus Specification 2.2
- PCIe Specification 1.1
**Standards**
- Peripheral Component Interconnect (PCI) Local Bus Specification 2.2
- Peripheral Component Interconnect Express (PCIe) Specification 1.1

**Operating environment**
- Temperature: 10° to 35°C (50° to 95°F)
- Relative humidity: 8% to 80%
- Wet bulb: Less than 27°F
- Pressure: 700 mbar minimum

Power requirement:
- 12 volt PCIe domain: 20.13 watts maximum
- 3.3 volt PCIe domain: 3.31 watts maximum (including USB external load)

**Hardware requirements**
All versions of select IBM System x servers with at least two, or possibly three, PCIe slots that are adjacent.

**Note:** A 4765 Cryptographic Coprocessor can be installed in an end slot, which requires two slots that are adjacent. Otherwise, three slots that are adjacent are required.

**Software requirements**
The following operating system is required to support 4765 Cryptographic Coprocessors installed on the supported System x servers:
- SUSE Linux Enterprise Server 11.1 from Novell

For details on future updates to the versions of operating systems that are supported by the 4765 Cryptographic Coprocessor, visit the following website:

http://www.ibm.com/security/cryptocards

The 4765 Cryptographic Coprocessor is supported by the CCA Support Program. Licensed software is required to utilize the 4765 Cryptographic Coprocessor. Only software that the 4765 Cryptographic Coprocessor can internally validate through digital signature techniques can enable the PCIe Cryptographic Coprocessor operations.

The CCA Support Program can be downloaded from the Internet. The hardware and software are subject to the export and import regulations of most countries.

**Compatibility**
Application programs that are designed to work with CCA Support Program versions for 4765 Cryptographic Coprocessor should not require modification.

**Planning information**

**Customer responsibilities**
For instructions or publications, in US English version, visit

http://www.ibm.com/security/cryptocards

**Cable orders**
No cables are required.
Security, auditability, and control

This product uses the security and auditability features of RSA signature generation and verification, generation of RSA key pairs, TDES key management, TDES encryption/decryption, and SHA-1 and SHA-2 generation.

The value of a cryptographic system is largely based on the secrecy and privacy of the keys that are used in cryptographic operations. The design of the IBM 4765 Cryptographic Coprocessor provides very strong protection for the cryptographic keys when it is initialized and used with the appropriate controls to meet your application requirements.

The coprocessor allows you to load sensitive applications along with keys and certificates into a security-rich environment. In addition to providing high speed cryptographic processing, the security-rich environment is designed to protect applications’ data, keys, and code from being compromised.

Your application program should address secure setup and auditing requirements.

The customer is responsible for evaluation, selection, and implementation of security features, administrative procedures, and appropriate controls in application systems and communications facilities.

Global Technology Services

Contact your IBM representative for the list of selected services available in your country, either as standard or customized offerings, for the efficient installation, implementation, and/or integration of this product.

IBM Electronic Services

IBM has transformed its delivery of hardware and software support services to help you achieve higher system availability. Electronic Services is a web-enabled solution that offers an exclusive, no-additional-charge enhancement to the service and support available for IBM servers. These services are designed to provide the opportunity for greater system availability with faster problem resolution and preemptive monitoring. Electronic Services comprises two separate, but complementary, elements: Electronic Services news page and Electronic Services Agent.

The Electronic Services news page is a single Internet entry point that replaces the multiple entry points traditionally used to access IBM Internet services and support. The news page enables you to gain easier access to IBM resources for assistance in resolving technical problems.

The Electronic Service Agent™ is no-additional-charge software that resides on your server. It monitors events and transmits system inventory information to IBM on a periodic, client-defined timetable. The Electronic Service Agent automatically reports hardware problems to IBM. Early knowledge about potential problems enables IBM to deliver proactive service that may result in higher system availability and performance. In addition, information collected through the Service Agent is made available to IBM service support representatives when they help answer your questions or diagnose problems. Installation and use of IBM Electronic Service Agent for problem reporting enables IBM to provide better support and service for your IBM server.

To learn how Electronic Services can work for you, visit

http://www.ibm.com/support/electronic
**Terms and conditions**

**Warranty period**

One year.

Refer to the Statement of Limited Warranty which can be found at the following website:


**Warranty service**

Warranty on the 4765 Cryptographic Coprocessor will be determined by proof of the date of purchase. The customer is responsible to provide proof at the time of service.

Once the warranty has been validated and a determination has been made that the 4765 Cryptographic Coprocessor must be replaced, the exchange is normally done by mail service.

**Customer Replaceable Unit (CRU) Service**

**Warranty service upgrades**

During the warranty period, warranty service upgrades provide an enhanced level of On-site Service for an additional charge. A warranty service upgrade must be purchased during the warranty period and is for a fixed term (duration). It is not refundable or transferable and may not be prorated. If required, IBM will provide the warranty service upgrade enhanced level of On-site Service acquired by the customer. Service levels are response time objectives and are not guaranteed.

IBM will attempt to resolve your problem over the telephone or electronically by access to IBM website

http://www.ibm.com/security/cryptocards

Customers should use these product support pages as a primary source of information concerning the 4765 Cryptographic Coprocessor. The site supports:

- Access to firmware for the 4765 Cryptographic Coprocessor
- Software updates
- Download support for product publications
- Order and warranty support

You must follow the problem determination and resolution procedures that IBM specifies. Scheduling of service will depend upon the time of your call.

Customer Replaceable Units (CRUs) may be provided as part of the machine's standard warranty CRU Service except that you may install a CRU yourself. For additional information on the CRU service, see warranty information.

**Customer Replaceable Units**

If your problem can be resolved with a Customer Replaceable Unit (CRU), and depending upon the warranty service offerings in your geography, IBM will ship the CRU to you for you to install.

Based upon availability, CRUs will be shipped for next business day delivery. IBM specifies, in the materials shipped with a replacement CRU, whether a defective CRU must be returned to IBM. When return is required, 1) return instructions and a container are shipped with the replacement CRU and 2) you may be charged for the
replacement CRU if IBM does not receive the defective CRU within 30 days of your receipt of the replacement.

Customer Replaceable Unit Service is available in your geography. CRUs are designated as being either a Tier 1 or a Tier 2 CRU.

Tier 1 CRUs: Installation of Tier 1 CRUs is your responsibility. If IBM installs a Tier 1 CRU at your request, you will be charged for the installation.

Tier 2 CRUs: You may install a Tier 2 CRU yourself or request IBM to install it.

The following parts have been designated as Tier 1 CRU parts:

- 4765 Cryptographic Coprocessor
- Replacement Batteries
- Multi-battery replacement pack

**Usage plan machine**

No

**IBM hourly service rate classification**

Not applicable

When a type of service involves the exchange of a machine part, the replacement may not be new, but will be in good working order.

**Maintenance service offerings**

Maintenance Service Offerings are not applicable to the IBM 4765 Cryptographic Coprocessor.

**Field-installable features**

No

**Model conversions**

No

**Machine installation**

Customer setup. Customers are responsible for installation according to the instructions IBM provides with the machine.

**Graduated program license charges apply**

No

**Licensed Internal Code and Licensed Machine Code**

This product does not contain Licensed Internal Code or Licensed Machine Code.

**Separately licensed code**

The following technology requires a contract, in addition to the IBM Customer Agreement:

**Elliptical Curve Cryptography:** For machine type and model 4765-001, Elliptical Curve Cryptography (ECC) technology is included with the cryptographic coprocessor. This technology is delivered with the 4765-001 Machine Code, and requires license terms in addition to the standard IBM License Agreement for Machine Code (LMC). These additional terms are delivered through the LMC's
Addendum for Elliptical Curve Cryptography. This ECC Addendum is available at the
time of software download.

The Addendum may be found in multiple languages at

http://www.ibm.com/systems/support/machine_warranties/
machine_code_cryptadd.html

Europe Business Partner terms and conditions
Category: The product is added to Category E.

Pricing

For all local charges, contact your IBM representative.

Announcement countries

All European, Middle Eastern, and African countries except Iran, Sudan, and Syria.

Trademarks

Electronic Service Agent is a trademark of IBM Corporation in the United States,
other countries, or both.

IBM, System x, ServerProven and PowerPC are 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.

Other company, product, and service names may be trademarks or service marks of
others.

Terms of use

IBM products and services which are announced and available in your country
can be ordered under the applicable standard agreements, terms, conditions,
and prices in effect at the time. IBM reserves the right to modify or withdraw this
announcement at any time without notice. This announcement is provided for
your information only. Reference to other products in this announcement does not
necessarily imply those products are announced, or intend to be announced, in your
country. Additional terms of use are located at


For the most current information regarding IBM products, consult your IBM
representative or reseller, or visit the IBM worldwide contacts page

http://www.ibm.com/planetwide/