Improving the performance and security of your e-business applications

IBM Integrated Cryptographic Coprocessors for IBM @server zSeries 900 and for IBM S/390 Servers

Highlights

- ***Balanced, expandable support for secure Web serving. Greatly improves SSL transaction throughput making secure, high performance, e-business applications easier to implement.***
- ***High speed, secure cryptographic hardware. Add optional PCI Cryptographic Coprocessors alongside CMOS Cryptographic Coprocessors to meet your growth needs.***
- ***Support integrated into z/OS and OS/390® V2. Choice of APIs: IBM CCA, CDSA, and BSAFE.***
- ***Optional Trusted Key Entry (TKE) system. Secure entry and management of master cryptographic keys.***
- ***Tamper-responding design. Cryptographic Coprocessors Certified by NIST at FIPS 140-1 Level 4.***

Securing e-commerce

The protection required to conduct commerce on the Internet, and provide data confidentiality, can be provided only by cryptographic services and techniques. Sensitive information can be encrypted before being transmitted over unsecure networks to ensure its privacy. Cryptographic techniques can be used to detect unauthorized modifications to data in transit. Other cryptographic techniques play a significant role in authenticating participants in a transaction. The efficient and economical protection of enterprise-critical information has become increasingly important in many diverse application environments.

Meeting the Cryptography Challenge

IBM @server zSeries 900 and IBM S/390 integrated cryptographic support provides levels of security and performance for some cryptographic operations that are not possible using software encryption techniques.

Performance

Secure Sockets Layer (SSL) is the predominant method for providing security in today's Internet and e-commerce marketplace. SSL is required for secure Web serving and its performance is a critical factor in designing a solution. z/OS and OS/390 can achieve high levels of SSL performance by offloading complex cryptographic operations to a combination of CMOS Cryptographic Coprocessors and PCI Cryptographic Coprocessors (PCICC).

Highly Secure Solution

Private encryption keys used by applications to authenticate themselves, and to digitally sign data and communications must be protected from loss. The compromise of those keys could lead to loss of trust as well as financial loss. Organizations of credit card issuers, financial institutions, governments, and private industry are increasingly demanding the use of secure hardware cryptographic facilities to ensure trust, privacy, and legality in the emerging e-commerce environment.

The CMOS Cryptographic Coprocessor and the PCICC feature are highly secure, tamper responding designs. Master encryption keys are stored within the hardware boundary and are used, in turn, to encrypt working keys. CMOS Cryptographic Coprocessor has been certified by the US National Institute of Standards and Technology (NIST) at FIPS 140-1 Level 4, the highest level available. PCICC feature is built around specially adapted IBM 4758-2 PCI Cryptographic Coprocessor cards, which like their predecessor, the IBM 4758-1, have also received FIPS 140-1 Level 4 certification.

Integrated Support

Support for cryptographic coprocessors is integrated into z/OS and OS/390 V2.

Each will transparently route application requests for cryptographic services to an appropriate CMOS Cryptographic Coprocessor or PCICC to perform the cryptographic operation. Routing tables internal to z/OS and OS/390 determine which operations will be performed by which type of coprocessor, depending on the function requested or its performance characteristics. As an example, some operations, such as SSL, are supported by, and perform well, on either type of coprocessor and the operating system will spread the workload across all the available coprocessors.

Supporting Financial Applications

Banking, finance, and securities industries have built their systems around hardware encryption for ATM and POS machines (PINs) and secure transactions for over a decade. The requirement for secure, certified, hardware encryption solutions continues to be met by the cryptographic coprocessors.

Support for multiple PR/SM partitions

The Cryptographic Coprocessors can support up to the maximum Processor Resource/Systems Manager™ (PR/SM™) partitions available, each with its own unique master key.

Flexible Functions

PCICC provides support for custom cryptographic functions called User Defined Extensions (UDX). UDX capability can be leveraged by customers who have a specific need for unique functions. Requests for UDX functions to be implemented under contract with IBM will be considered. IBM will test and distribute UDX functions.

High availability

Cryptographic Coprocessors are implemented with the same robust fault tolerant design found throughout zSeries and IBM S/390 enterprise servers. High-availability features on many models include a second CMOS Cryptographic Coprocessor with redundant paths, support for multiple PCICCs, and internal “retries” transparent to the application.

DES Master keys and other long-life cryptographic keys can be updated dynamically without disrupting service to applications using those keys.

z/OS Management

z/OS and OS/390 provide administrative dialogs, security authorization checking of cryptographic function users, and recording of security related events.

Application programming interface

z/OS and OS/390 support IBM Common Cryptographic Architecture (CCA), RSA BSAFE, and Common Data Security Architecture (CDSA) APIs.

Standards compliance

Integrated cryptographic coprocessors support international cryptographic standards for personal identification number (PIN) processing, message authentication and modification detection codes along with hashing algorithms such as the Secure Hash Algorithm (SHA), the Data Encryption Algorithm (DEA) and encryption modes, the Digital Signature Standard and Rivest-Shamir-Adelman (RSA).

z/Series and S/390 Integrated Cryptographic Coprocessors at a glance

Functions

- DES, Triple-DES, CDMF
- MAC, double-key MAC, MDC-2 and MDC-4
- PIN
- SHA-1, MD-5
- 2048-bit Modular Exponentiation (1024-bit w/o PCICC)
- RSA Digital Signature Verification/Generation
- RSA Key Generation and RSA Key Generation with Retained Key (both w/PCICC)
- DSS Key Generation, Signature Verification/Generation
- VISA CVV and MasterCard CVC (track-2 method) Generation and Verification
- SET™ protocol 1.0 (OAEP) (online PIN extensions with PCICC)
- PKCS 1.0, 1.1
- Pseudo Random Number Generator
- Concurrent Synchronous and Asynchronous Execution
- Transparent routing of requests by OS/390 to appropriate cryptographic coprocessors
- Internal non-volatile Memory Arrays
- Tamper Detection and Response
- Robust Fault Tolerant Design
- Export Enablement Control

Hardware requirements

CMOS Cryptographic Coprocessor

- Standard Feature on zSeries 900 and on S/390 Parallel Enterprise Server® Generation 4, Generation 5, Generation 6, and Application StarterPak
- Optional Feature on S/390 Parallel Enterprise Server Generation 3, Multiprise® 2000 and 3000

PCI Cryptographic Coprocessor

- Optional priced feature on zSeries 900 and on S/390 Parallel Enterprise Server Generations 5 and 6. Up to 8 Dual PCICC features, each including two coprocessors, can be installed on a zSeries 900 server. Up to 8 PCICC features, each including one coprocessor, can be installed on a S/390 G5 or G6 server.

Trusted Key Entry workstation

- The Trusted Key Entry workstation is an optional priced feature of zSeries and S/390 Enterprise Servers, and if ordered will be shipped with all hardware and software components installed.

Software requirements

CMOS Cryptographic Coprocessor

- z/OS 1.1 or later, OS/390 V2 R4 or later, or OS/390 V1 + ICSF independent product (5655-120), or MVS™ 5 + ICSF (5655-120)

PCI Cryptographic Coprocessor

- z/OS 1.1 or later, or OS/390 V2 R9 or V2 R10 (V2 R10 for UDX support)

Ordering

To comply with US export regulations, all zSeries and S/390 cryptographic hardware is shipped disabled. To enable it, the proper unpriced enablement feature must be ordered corresponding to the allowed export configuration. An enablement diskette keyed to the specific server system will be shipped for installation.

To learn more

Visit the S/390 security Web site *ibm.com/s390/security*

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

Produced in the United States of America
10-00

G221-9109-00