

IBM eServer zSeries 890 Performance of Cryptographic Operations

(Cryptographic Hardware: CPACF, PCICA, PCIXCC, CEX2C)

Table of Content

IBM eServer zSeries 890 Performance of Cryptographic Operations	Page 1
Preface	Page 3
1. Introduction	Page 3
2. Cryptographic Hardware supported on zSeries 890	Page 5
2.1. CP Assist for Cryptographic Function (CPACF)	Page 5
2.2. PCI Cryptographic Accelerator (PCICA) Feature	Page 5
2.3. PCIX Cryptographic Coprocessor (PCIXCC) Feature	Page 6
2.4. CEX2C Cryptographic Coprocessor (CEX2C) Feature	Page 7
3. Exploitation of Cryptographic Hardware in z890	Page 8
3.1. SSL Protocol based Communication	Page 9
4. Performance Information	Page 10
4.1. Definitions	Page 10
4.2. CP Assist for Cryptographic Function (CPACF) Performance - ICSF API Interface	Page 10
4.3. PCICA Performance	Page 12
4.4. PCIXCC Performance	Page 13
4.4.1. PCIXCC Multiple Data Symmetric Key Performance	Page 14
4.4.2. PCIXCC PKA Performance	Page 16
4.5. SSL Protocol Handshake Performance	Page 18
4.5.1. Applicability of SSL Performance Results to a Customer Environment	Page 18
4.5.2. SSL Protocol Performance - System SSL with z/OS V1.5/ ICSF level FMID HCR770A	Page 19
5. z890 January 2005 General Availability Performance Update	Page 20
5.1 Definitions	Page 20
5.2 PCIXCC and CEX2C Performance	Page 21
5.2.1 PCIXCC and CEX2C Multiple Data Symmetric Key Performance	Page 21
5.2.2 PCIXCC and CEX2C PKA Performance	Page 24
5.3 SSL Protocol Handshake Performance	Page 27
5.3.1. Applicability of SSL Performance Results to a Customer Environment	Page 27
5.3.2 SSL Protocol Performance - System SSL with z/OS V1.6/ ICSF level FMID HCR7720	Page 28

Preface

The performance information presented in this publication was measured on IBM @server[®] zSeries[®] systems in an unconstrained environment for the specific benchmark with a system control program (operating system) as specified. Many factors may result in variances between the presented information and the information a customer may obtain by trying to reproduce the data. IBM does not guarantee that your results will correspond precisely to the measurement results herein. This information is provided 'as is' without warranty, express or implied.

The performance numbers stated for some of the operations are only for demonstration purposes. When quoting some key length or cryptographic algorithms one may not conclude that IBM implies the key length or cryptographic algorithm are adequate and can therefore be used safely.

The cryptographic functions described here may not be available in all countries and may require special enablement subject to export regulations.

1. Introduction

This publication is an update to an earlier publication and covers the performance of the cryptographic hardware available on the zSeries 890. The original publication covered the cryptographic hardware available as of the General Availability in May of 2004. This update covers the performance of cryptographic hardware available as of the General Availability in January of 2005.

The original performance information contained in the z890 GA1 version of this publication has not been changed. This information is found in Chapter 4. Performance Information.

A new chapter, Chapter 5 z890 January 2005 General Availability Performance Update, has been added which contains performance information for the Crypto Express 2 Coprocessor (CEX2C) feature. Chapter 5 also contains updated performance information for the PCIX Cryptographic Coprocessor (PCIXCC) feature.

Performance information for CP Assist for Cryptographic Function (CPACF) and PCI Cryptographic Accelerator (PCICA) feature was not updated in this version of the document and can be found in Chapter 4.2 and Chapter 4.3.

A separate publication 'IBM eServer zSeries 990 Performance of Cryptographic Operations' covers the performance of the cryptographic hardware as available on the zSeries 990 after the General Availability of the Crypto Express 2 Coprocessor (CEX2C) feature in January 2005.

This publication is available on the Internet with the following URL:

http://www-1.ibm.com/servers/eserver/zseries/security/pdf/Web_z990_Crypto_Rel_01282005.pdf

The present publication for the z890 Performance of Cryptographic Operations follows the same structure as the publication for z990 Performance of Cryptographic Operations. For the convenience of the reader general information is repeated if applicable. The present z890 document is based on measurements on a z890 system. These measurements are performed on current levels of internal code, z/OS[®], and ICSF. Thus results presented in the z890 document

may differ from results of comparable measurements in the z990 document. On the other hand, not all measurements presented in the z990 publication were performed for the z890.

The z890 systems were introduced for those customers requiring a lower-capacity entry point than offered with the z990. The functionality in the crypto area is the same as for the z990.

The zSeries z890 and z990 systems support the following cryptographic hardware functions:

1. CP Assist for Cryptographic Function (CPACF).
2. PCI Cryptographic Accelerator (PCICA) feature.
3. PCIX Cryptographic Coprocessor (PCIXCC) feature.
4. Coprocessor (CEX2C) feature. Crypto Express2

The CP Assist for Cryptographic Function delivers cryptographic support on every Central Processor (CP) with Data Encryption Standard (DES) and Triple DES (TDES) data encryption/decryption and SHA-1 hashing.

The PCICA feature provides hardware support for Public Key operations as are used with Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols which are widely used to help secure e-business applications.

The PCIX Cryptographic Coprocessor (PCIXCC) feature is a replacement of the PCI Cryptographic Coprocessor (PCICC) Feature and the CMOS Cryptographic Coprocessor Facility that were offered on z900. All of the equivalent PCICC functions that are implemented are designed to offer higher performance.

The Crypto Express2 (CEX2C) feature has been available on z890 since January 2005. The Crypto Express2 is a replacement for the PCIXCC and PCICA features. All of the equivalent PCIXCC and PCICA functions are implemented in the Crypto Express2 with equivalent or greater performance (see Section 5).

2. Cryptographic Hardware supported on zSeries 890

2.1. CP Assist for Cryptographic Function (CPACF)

zSeries 890 provides the Message-Security Assist (MSA) Architecture Facility as a model dependent extension of z/Architecture. The implementation is the CP Assist for Cryptographic Function (CPACF). The CPACF delivers cryptographic hardware support on every Central Processor (CP) with DES and TDES data encryption/decryption and SHA-1 hashing. As these cryptographic functions are implemented in each CP the potential throughput scales with the number of CPs in the system. Also, the association of these cryptographic functions to specific CPs in the system, as was with previous generations of zSeries, is eliminated.

The DES and TDES functions of the CPACF use clear key values. The SHA-1 hash functions are shipped enabled. The DES and TDES functions require enablement of the CPACF for export control. The CPACF for DES, TDES, and SHA-1 functions can be invoked by five new problem state instructions defined by an extension of the zSeries architecture. Support is also available via the Integrated Cryptographic Service Facility (ICSF) in z/OS.

The hardware of the CPACF that performs the symmetric key operations (DES; TDES) and SHA-1 functions operates basically synchronous to the CP operations. The CP cannot perform any other instruction execution while a CPACF cryptographic operation is being executed. The CP internal code performs data fetches and stores resultant data while cryptographic operations are executed in the CPACF hardware on a unit basis as defined by the hardware. The hardware has a fixed set up time per request and a fixed operation speed for the unit of operation. Thus maximum throughput can be achieved for larger blocks of data (up to a hardware defined limit).

2.2. PCI Cryptographic Accelerator (PCICA) Feature

The PCI Cryptographic Accelerator Feature is available on z800 and z900 and continues to be supported on z890. Its aim is to provide hardware support to accelerate certain cryptographic operations that occur in the e-business environment. Compute intensive public key operations as used by SSL/TLS protocols can be offloaded from the CP to the PCICA Cryptographic Accelerator and thus increase system throughput.

There can be a maximum of 2 PCICA features in a z890 system. Each PCICA feature contains two cryptographic accelerator cards which can perform cryptographic operations independently from each other. Thus there can be a maximum of 4 cryptographic accelerator cards in a z890 system.

The PCICA Cryptographic Accelerator works in 'clear key' mode only.

The PCICA hardware executes its cryptographic operations basically asynchronously to the CP operation of the z890 CPs. A CP that needs to perform a public key operation uses a message queuing protocol to communicate with the cryptographic accelerator card hardware. After enqueueing a request to the cryptographic accelerator card, the operating system will dispense the task that has enqueued the cryptographic operation, and dispatches another task. Thus the PCICA public key cryptographic hardware will work in parallel to other tasks being executed in the CP. A special CP task will poll at fixed time intervals for finished operations of the cryptographic hardware, dequeue them, and finally 'Post' the application waiting for the result of the cryptographic operation. For the PCICA Cryptographic Accelerator card up to 8 requests can be waiting in the queue either for execution or waiting with the result of the cryptographic operation to be dequeued by a CP. In the PCICA Cryptographic Accelerator card hardware up to 5 operations can be worked on in parallel.

For zSeries 890 systems, the PCICA Cryptographic Accelerator is invoked by the Integrated Cryptographic Support Facility (ICSF) to increase throughput for some PKA services used e.g. in SSL/TLS protocol transaction environments.

2.3. PCI Cryptographic Coprocessor (PCIXCC) Feature

The PCI Cryptographic Coprocessor Feature was announced in May of 2003 with the zSeries 990 with shipment starting in September 2003.

The PCIXCC feature supports:

- Secure cryptographic functions
- Use of secure encrypted key values
- Clear key and secure PKA operations
- User defined Extensions (UDX)

The PCIX Cryptographic Coprocessor (PCIXCC) feature contains one PCIX Cryptographic Coprocessor with its physical implementation on a card. There can be a maximum of 4 PCIXCC features in a z890 system.

The PCIX Cryptographic Coprocessor card provides a high-security cryptographic subsystem. The tamper-responding hardware is designed to qualify at the highest level under the FIPS 140-2 standard. Specialized hardware performs DES, TDES, RSA, and SHA-1 cryptographic operations in a secure environment. The PCIX Cryptographic Coprocessor design protects the cryptographic keys and sensitive custom applications. Security relevant cryptographic keys are encrypted under the Master Key when outside the secure boundary of the PCIXCC card. The Master Keys are always kept in battery backed-up memory within the tamper-protected secure boundary of the PCIXCC card.

The PCIXCC card also supports the ‘clear key’ PKA operations that currently are predominantly used to provide security-rich SSL protocol communications.

The operations in the PCIXCC card are controlled by an on-board microprocessor with memory to hold the controlling program. A secure code-loading process enables control program and application program loading into the PCIXCC card. The Linux based control program together with the application program provides for the IBM Common Cryptographic Architecture (CCA) interface for the applications using the PCIX Cryptographic Coprocessor.

The PCIX Cryptographic Coprocessor executes its cryptographic operations asynchronously to a Central Processor (CP) operation in the z890 system. The communication mechanism between a z890 CP and the PCIXCC card is the same as for the PCICA card. A CP requesting a cryptographic operation from the PCIXCC card uses the message queuing protocol to communicate with the PCIXCC card. After enqueueing a request to the PCIXCC card, the host operating system will dispense the task that has enqueued the cryptographic operation and dispatches another task. Thus processing of the cryptographic operation in the PCIXCC card will work in parallel to other tasks being executed in a z890 CP. A special CP task will poll at fixed time intervals for finished operations of the PCIX Cryptographic Coprocessor, dequeue them, and finally execute the Release function to cause the redispach of the application waiting for the result of the cryptographic operation. For the PCIXCC card up to 8 requests can be waiting in the queue either for execution or waiting with the result of the cryptographic operation to be dequeued by a CP. In the PCIX Cryptographic Coprocessor, several operations can be worked on in parallel.

For zSeries 890 systems, the PCIX Cryptographic Coprocessor works with the Integrated Cryptographic Support Facility (ICSF) and the IBM Resource Access Control Facility (RACF[®]) in a z/OS or OS/390[®] operating environment to provide cryptographic services with the IBM Common Cryptographic Architecture (CCA) secure key management.

The IBM Common Cryptographic Architecture implementation provides a base on which customer programs can request cryptographic services from the PCIX Cryptographic Coprocessor. For unique customer cryptographic application requirements the PCIX Cryptographic Coprocessor provides for user-defined extensions (UDX) to the Common Cryptographic Architecture interface.

2.4. CEX2C Crypto Coprocessor (CEX2C) Feature

The Crypto Express2 Coprocessor Feature was announced in Sept. of 2004 with the zSeries 990 with shipment starting in January 2005.

The CEX2C feature supports:

- Secure cryptographic functions
- Use of secure encrypted key values
- Clear key and secure PKA operations
- User defined Extensions (UDX)

Each Crypto Express2 Coprocessor (CEX2C) feature contains two cryptographic coprocessors cards. There can be a maximum of 8 CEX2C features in a z890 system for a total of 16 cryptographic coprocessor cards.

The Crypto Express2 Coprocessor feature provides a high-security cryptographic subsystem. The tamper-responding hardware is designed to qualify at the highest level under the FIPS 140-2 standard. Specialized hardware performs DES, TDES, RSA, and SHA-1 cryptographic operations in a security-rich environment. The Crypto Express2 Coprocessor design protects the cryptographic keys and sensitive custom applications. Security relevant cryptographic keys are encrypted under the Master Key when outside the secure boundary of the CEX2C card. The Master Keys are always kept in battery backed-up memory within the tamper-protected secure boundary of the CEX2C card.

The CEX2C feature also supports the 'clear key' PKA operations that currently are predominantly used to provide security-rich SSL protocol communications.

The operations in the CEX2C card are controlled by an on-board microprocessor with memory to hold the controlling program. A secure code-loading process enables control program and application program loading into the CEX2C card. The Linux based control program together with the application program provides for the IBM Common Cryptographic Architecture (CCA) interface for the applications using the Crypto Express2 Coprocessor.

The Crypto Express2 Coprocessor executes its cryptographic operations asynchronously to a Central Processor (CP) operation in the z890 system. The communication mechanism between a z890 CP and the CEX2C card is the same as for the PCIXCC card. A CP requesting a cryptographic operation from the CEX2C card uses the message queuing protocol to communicate with the CEX2C card. After enqueueing a request to the CEX2C card, the host operating system will dispense the task that has enqueued the cryptographic operation and dispatches another task. Thus processing of the cryptographic operation in the CEX2C card will work in parallel to other tasks being executed in a z890 CP. A special CP task will poll at fixed time intervals for finished operations of the Crypto Express2 Coprocessor, dequeue them, and

finally execute the Release function to cause the redispach of the application waiting for the result of the cryptographic operation. For the CEX2C card up to 8 requests can be waiting in the queue either for execution or waiting with the result of the cryptographic operation to be dequeued by a CP. In the Crypto Express2 Coprocessor, several operations can be worked on in parallel.

For zSeries 890 systems, the Crypto Express2 Coprocessor works with the Integrated Cryptographic Support Facility (ICSF) and the IBM Resource Access Control Facility (RACF[®]) in a z/OS or OS/390[®] operating environment to provide cryptographic services with the IBM Common Cryptographic Architecture (CCA) secure key management.

The IBM Common Cryptographic Architecture implementation provides a base on which customer programs can request cryptographic services from the Crypto Express2 Coprocessor. For unique customer cryptographic application requirements the Crypto Express2 Coprocessor provides for user-defined extensions (UDX) to the Common Cryptographic Architecture interface.

3. Exploitation of Cryptographic Hardware in z890

In the cryptographic application environment it is quite common that an application will not have direct access to the cryptographic hardware. The application requiring a cryptographic service will call a programming interface which is interpreted by some services of the System Control Program.

In zSeries using the z/OS System Control Program, most cryptographic hardware can only be used through z/OS Integrated Cryptographic Service Facility (ICSF). ICSF is a standard component of z/OS. It provides cryptographic services in the z/OS environment. ICSF provides the Application Programming Interfaces (APIs) by which applications request cryptographic services. Thus ICSF relieves the application from dealing with the complexity of the cryptographic hardware communication. However, these ICSF services are operating software path lengths which have to be added (from an application's point of view) to the execution time of the cryptographic hardware.

As mentioned in the description of the CPACF cryptographic hardware, an application program can use this hardware by invoking any of the 5 new machine instructions. However, there is also an API call interface to ICSF available.

3.1. SSL Protocol based Communication

Secure Sockets Layer (SSL) is a communication protocol that provides highly secure communication over an open communication network, such as the Internet. The SSL protocol is a layered protocol that is intended to be used on top of a reliable transport, e.g. Transmission Control Protocol (TCP/IP). SSL is designed to provide data privacy and integrity by using cryptographic operations and optionally Server and Client authentication based on public key certificates. Once an SSL connection is established between a Client and Server, data

communications between Client and Server are transparent to the encryption and integrity added by the SSL protocol. Transport Layer Security (TLS) is the newer version of the SSL protocol.

Executing the SSL/TLS protocols for a Server (or Client) on a zSeries system will result in a series of cryptographic operations. In the z/OS environment ICSF will either invoke available cryptographic hardware or will execute the cryptographic operation in system software. The SSL/TLS protocol will result in CP path length (due to the protocol itself and due to operating system support), the symmetric key operation's execution time (either hardware assisted or in software executed on a CP), and the execution time of the public key operations (either hardware assisted ((operating in parallel to the CP instruction execution)) or in software on a CP). This publication will state the performance in the SSL environment as the maximum number of SSL handshakes the zSeries 890 can provide as a server within the given system constraints and assess the utilization of the measured system.

The intent for providing capacity information in the SSL environment is to demonstrate the capabilities of a z890 system to act as a Web Server providing highly secure communication to a large number of clients. For this purpose the maximum number of SSL connects and data exchanges per second made between the server and all clients are provided for different environments. There is no intention to provide a more detailed performance analysis for this environment.

In this publication, performance/capacity information will be given for running SSL protocol based communication in the z/OS environment.

As this performance publication primarily deals with performance of cryptographic operations and Web based communication the measurements for the SSL environments include only the processing required for the SSL protocol handshake and some data exchange. Explicitly excluded is the processing for the 'business transaction' that in a normal environment would be initiated in the server on behalf of the client's request. As most SSL protocol-based measurements in this report are limited by the processing capacity of the server, in a 'real life' environment the processing for the business transaction would reduce the number of necessary handshakes considerably.

4. Performance Information

4.1. Definitions

The performance information stated in this publication is provided on the ICSF API level. Measurements were performed with the control program z/OS Version 1 Release 5 (z/OS V1.5) and ICSF level FMID HCR770B, except when stated otherwise.

All measurements were performed on an IBM eServer zSeries 890. The internal code level was GA3. The exact model of the z890 system used is stated with each measurement. Most of the

measurements were run on a z890 Model 2086-A04. This Model contains 4 Central Processors. If, however, the measurement invokes only one single job the performance behavior is the same as if this measurement were run on a z890 Model 2086-A01 which contains only one Central Processor.

For the cryptographic operations that can be used with a variable length of data such as Data Encryption Algorithm (DEA) Standard encryption, the performance is stated for test cases using different data lengths. The length is specified in Bytes ('K' equals 1024, 'M' equals 1,048,576). The resulting data rate is specified in multiples of 1,000,000 Bytes (not 'M').

In order to keep this performance publication at a reasonable length results of measurements are presented using a single cryptographic feature. If multiple cryptographic features are available a statement is made how the performance results scale with usage of multiple features.

4.2. CP Assist for Cryptographic Function (CPACF) Performance - ICSF API Interface

All test cases are written in zSeries Assembler Language issuing an API call to ICSF for the cryptographic operation. ICSF will resolve the API call and issue instructions for the cryptographic operation according to the Message-Security Assist (MSA) Architecture facility as indicated with each group.

On the z890 system performance measurement for the CPACF were only taken at the ICSF API interface level and not on the architecture instruction interface level ('native'). The 'Native' test cases would show lower execution time compared to the ICSF API level test cases because of the additional ICSF path length. As the data length increases, the ICSF path length is a less dominant factor. The throughput is nearly the same as for the 'Native' test cases for large data lengths.

The throughput rate of the 'native' CPACF test cases on z890 are expected to be in the order of .83 times the throughput rate of the 'native' test cases measured on the z990 system.

The data quoted in the following was from test cases running on a z890 Model 2086-A04 a single job which uses only one of the CPs. The throughput using N CPs performing the same cryptographic operations can be expected to be close to N times the throughput of using one CP. As an example, the measured throughput using 4 CPs is in the order of 3.5 to 4 times the throughput using one CP. The smaller factor applies to small block sizes and approaches the factor of 4 with larger block sizes.

Terminology Explanation: The term DEA stands for Data Encryption Algorithm which is a block cipher according to the Data Encryption Standard (DES).

DEA Cipher Block Chaining Encipher with Single Length Key (56 Bits) - ICSF API

(zSeries Message Security Assist Architecture instruction: KMC-DEA)

ICSF API: Single DES CBC Encipher (KMC-DEA)		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	82801.0	5.30
256	79259.0	20.29
1024	67642.0	69.27
4096	42680.0	174.82
64K	4975.0	326.04
1M	326.1	341.94

Decipher with Single Length Key has similar performance characteristics as the Encipher operation.

DEA Cipher Block Chaining Encipher with Triple Length Key (168 Bits) - ICSF API

(zSeries Message Security Assist Architecture instruction: KMC-TDEA)

ICSF API: Triple DES CBC Encipher (KMC-TDEA)		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	80657.0	5.16
256	72265.0	18.50
1024	51201.0	52.43
4096	23580.0	96.58
64K	1987.0	130.22
1M	126.4	132.54

DEA Decipher with Triple Length Key has similar performance characteristics as the Encipher operation.

Compute Message Digest SHA-1 - ICSF API

(zSeries Message Security Assist Architecture instruction: KLMD-SHA-1)

ICSF API: SHA-1(KLMD-SHA-1)		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	59954.0	3.84
256	57808.0	14.80
1024	50265.0	51.47
4096	33139.0	135.74
64K	4190.0	274.60
1M	278.1	291.61

4.3. PCICA Performance

The PCICA Cryptographic Accelerator Feature is designed to offer fast Public Key Algorithm cryptographic (PKA) operations. The PKA performance is listed for RSA key modulus length of 512 bits, 1024 bits (1K bits), and 2048 bits (2K bits). The performance numbers are from

measurements with z/OS V1.5 including ICSF level FMID HCR770B invoking the operation via the ICSF API according to the PKCS-1.2 Standard.

Quoted are the numbers performing the Public Key Decrypt (PKD) cryptographic operation which uses the Private Exponent either through the Chinese Remainder Theorem (CRT) Format or the Modulus Exponent (ME) Format.

For the Public Key Encrypt (PKE) cryptographic operation ICSF always uses an RSA public key with the Modulus Exponent (ME) Format. The modulus is according to the length specified and the (Public) Exponent has the value of 65537 which in hexadecimal notation is X'10001' (with leading zeros up to the length of the modulus).

Each PCICA feature contains two cryptographic accelerator cards which operate independently from each other. There can be a maximum of 2 PCICA features per z890 system with a maximum of 4 cryptographic accelerator cards in a system

PCICA PKA Performance

PCICA Public Key Decrypt (PKD) and Public Key Encrypt (PKE)			
	2086-A04	2086-A04	2086-A04
PCICA Crypt. Acc. Card	1	1	4
Jobs	1	8	32
	Operations/sec	Operations/sec	Operations/sec
PKD--CRT, 512 bit	611	3563	12691
PKD--CRT, 1024 bit	209	1091	4273
PKD--CRT, 2048 bit	53	267	1050
PKD--ME, 512 bit	373	2183	8524
PKD--ME, 1024 bit	105	543	2131
PKE, 512 bit	878	3797	11556
PKE, 1024 bit	458	3651	11970
PKE, 2048 bit	309	1678	6552

The first result column of the above table is for measurements where one job was continuously executing the cryptographic operation using one PCICA cryptographic accelerator card. As mentioned, the execution of the cryptographic operation in the PCICA cryptographic accelerator card is asynchronous to the zSeries Central Processor (CP) execution. As only one job is run on the CP the next cryptographic operation is started only when the result of the previous cryptographic operation has been received by the CP. The single job measurement indicates the delay an application would experience waiting for the result of the cryptographic operation.

The second result column of the above table is for measurements where eight jobs were continuously executing the same cryptographic operation using one PCICA cryptographic accelerator card. The increased throughput is due to the fact that tasks are always available for execution in the PCICA cryptographic accelerator card due to the parallel threads that run in the

zSeries CPs. Thus the full capability of the PCICA cryptographic accelerator card for parallel execution of the cryptographic operation can be utilized.

The third result column of the above table are for measurements where 32 jobs were continuously executing the same cryptographic operation using 4 PCICA cryptographic accelerator cards (2 PCICA features). The results show the maximum and the scalability of the throughput due to multiple PCICA features being used in one z890 system.

4.4. PCIXCC Performance

The PCIX Cryptographic Coprocessor is designed to provide high-security cryptographic operations to be used by the z990 and z890 host application programs. The connection of the PCIX Cryptographic Coprocessor feature via the PCIX bus to the z890 Central Processors (CPs) incurs latency and data transmission time. Because of this connection to the z890 CPs the PCIX Cryptographic Coprocessor operates asynchronous to the z890 CPs. The PCIX Cryptographic Coprocessor (PCIXCC) feature offers the high-security cryptographic operation mode for symmetric key operations and public key operations. In this case the cryptographic keys are encrypted under the corresponding Master Keys when outside the secure boundary of the PCIXCC card.

The PCIXCC feature also offers public key operations in 'clear key' mode. To provide security rich communication for Web site-based applications the SSL/TLS protocol is frequently applied. It is current practice to execute the public key operation incurring in the SSL protocol during the set up of the session in 'clear key' mode.

There can be a maximum of 4 PCIXCC features in a z890 system, each PCIXCC feature containing one PCIXCC cryptographic coprocessor card.

4.4.1. PCIXCC Multiple Data Symmetric Key Performance

This chapter deals with PCIXCC cryptographic operations with a user supplied length of data as e.g. DES operations.

All test cases are written in zSeries Assembler Language issuing an API call to ICSF for the cryptographic operation. ICSF will resolve the API call and handle the communication with the PCIX Cryptographic Coprocessor feature which does the actual cryptographic processing. The symmetric key that is used for the cryptographic operation is encrypted under the corresponding Master Key which in turn is kept in the secure boundary of the PCIXCC card.

The throughput for the cryptographic operations using the PCIXCC card for multiple data symmetric key operations is considerably less than the throughput for the corresponding functions using the CP Assist for Cryptographic Function (CPACF) hardware. For this type of cryptographic operations the PCIX Cryptographic Coprocessor feature should be used only when the security requirements for the application require it. Be aware that in the tables of this chapter the rates are quoted in thousands of bytes, not in millions of bytes as in previous tables.

The data quoted was from test cases run on a z890 Model 2086-A04 using 1 job that performs the cryptographic operation. For each cryptographic operation type quoted there is a statement on scalability of the results if multiple jobs are being used. The increase of measured throughput using 7 jobs is exemplified for the Single DES CBC Encipher operation.

The performance numbers are from measurements with z/OS V1.5 including ICSF level FMID HCR770B.

PCIXCC DEA Cipher Block Chaining Encipher with Single Length Key (56 Bits)

PCIXCC (one job): Single DES CBC Encipher		
Block size B	Operations/sec	x10**3 B/s
64	910.6	58.3
256	900.0	230.4
1024	617.4	632.2
4096	461.8	1891.5
64K	40.5	2656.8
1M	2.6	2725.2

The above table provides measurement results for an environment where one job was continuously executing the cryptographic operation using one PCIXCC Cryptographic Coprocessor card. As mentioned, the execution of the cryptographic operation in the PCIXCC card is asynchronous to the zSeries Central Processor (CP) execution. As only one job is run on the CP the next cryptographic operation is started only when the result of the previous cryptographic operation has been received by the CP. Thus there is a considerable delay before the next cryptographic operation can be initiated by the host CP. This inefficiency is removed when the host program consists of several jobs requesting the same cryptographic operation repetitively. The PCIXCC card's multitasking capability allows for enqueueing and dequeuing of requests in parallel with cryptographic operations being performed. A measurement environment using several parallel jobs highlights better the throughput capacity of the PCIXCC card whereas the 'single job' measurement environment is better suited to highlight the delay an application experiences waiting for the result of the cryptographic operation performed in the PCIXCC card.

PCIXCC (seven jobs): Single DES CBC Encipher		
Block size B	Operations/sec	x10**3 B/s
64	1393.0	89.2
256	1347.0	344.8
1024	1108.0	1134.6
4096	641.9	2629.2
64K	51.8	3398.0
1M	3.3	3453.0

The throughput with N PCIXCC cards with a sufficient number of jobs repetitively requesting the same cryptographic operation for Single DES, Triple DES, and Single DES Message Authentication (MAC) (see the following tables) is expected to be close to N times the throughput of one PCIXCC card with 7 jobs (as exemplified above).

PCIXCC DEA Cipher Block Chaining Encipher with Triple Length Key (168 Bits)

PCIXCC (one job): Triple DES CBC Encipher		
Block size B	Operations/sec	x10**3 B/s
64	906.8	58.0
256	620.9	159.0
1024	617.4	632.2
4096	461.6	1890.7
64K	40.5	2656.8
1M	2.6	2725.2

The throughput for seven jobs for PCIXCC TDES is in the order of 1.3 times to 1.5 times higher than for one job, the lower number applying to large data lengths and the higher to small data lengths

PCIXCC Message Authentication Code with DEA Single Length Key (56 Bits)

PCIXCC (one job): MAC with single DES		
Block size B	Operations/sec	x10**3 B/s
64	911.9	58.4
256	912.0	233.5
1024	911.0	932.9
4096	616.7	2526.0
64K	52.7	3452.4
1M	3.4	3583.0

The throughput for seven jobs for PCIXCC MAC is in the order of 1.2 times to 1.7 times higher than for one job, the lower number applying to large data lengths and the higher to small data lengths.

4.4.2. PCIXCC PKA Performance

The PCIXCC Cryptographic Coprocessor is designed to offer good Public Key Algorithm (PKA) cryptographic operation performance in addition to the high-security environment. The PKA performance is listed for RSA key modulus length of 512 bits, 1024 bits (1K bits), and 2048 bits (2K bits).

The numbers quoted for performing the Public Key Decrypt (PKD) cryptographic operation (using the Private Exponent) are either through the Chinese Remainder Theorem (CRT) Format or the Modulus Exponent (ME) Format. The PKD operation uses the private key in 'clear key' mode.

For the Public Key Encrypt (PKE) cryptographic operation ICSF always uses an RSA public key with the Modulus Exponent (ME) Format. The modulus is according to the length specified and the (Public) Exponent has the value of 65537 which in hexadecimal notation is X'10001' (with leading zeros up to the length of the modulus).

For the Digital Signature Generate (DSG) and the Symmetric Key Import (SYI) cryptographic operations the PKA keys (signature key or encryption key) are encrypted under the corresponding master key.

The performance numbers are from measurements with z/OS V1.5 including ICSF level FMID HCR770B invoking the operation via the ICSF API according to the PKCS-1.2. Standard. Measurements were performed on a z890 Model 2086-A04.

PCIXCC PKA Performance

PCIXCC on z/OS V1.5 (ICSF level: FMID HR770B)		
Public Key Decrypt (PKD), Public Key Encrypt (PKE) Digital Signature Generate (DSG), Digital Sign. Verify (DSV) Symmetric Key Import (encrypted with RSA key) (SYI)		
	2086-A04	2086-A04
PCIXCC cards	1	1
Jobs	1	7
	Operations/sec	Operations/sec
PKD--CRT, 512 bit	615	1199
PKD--CRT, 1024 bit	614	1097
PKD--CRT, 2048 bit	270	465
PKD--ME, 512 bit	614	1199
PKD--ME, 1024 bit	461	918
PKE, 512 bit	902	1291
PKE, 1024 bit	615	1074
PKE, 2048 bit	614	802
DSG--CRT, 512 bit	741	1219
DSG--CRT, 1024 bit	614	1119
DSG--CRT, 2048 bit	270	465
DSV--ME, 512 bit	909	1455
DSV--ME, 1024 bit	908	1389
SYI--CRT, 512 bit	614	927
SYI--CRT, 1024 bit	491	869

The PKA cryptographic operation throughput with N PCIXCC cards with a sufficient number of jobs repetitively requesting the same cryptographic operation for the examples in the table above is expected to be close to N times the throughput of one PCIXCC card with 7 jobs.

PKA RSA Key Generate

The PCIXCC Cryptographic Coprocessor also offers services to generate PKA RSA Keys. The PKA RSA Key Generate performance is listed for RSA key modulus length of 512 bits, 1024 bits (1K bits), and 2048 bits (2K bits) dependent on the Format, either the Chinese Remainder Theorem (CRT) Format or the Modulus Exponent (ME) Format.

PKA Key Generation is a compute intensive operation. The table below specifies the number of Key generations per second provided by one PCIXCC Cryptographic Coprocessor.

PCIXCC PKA RSA Key Generation Performance

PCIXCC PKA RSA Key Generate	Operations/sec
External CRT, 512bit	3.60
External CRT, 1024bit	1.74
External CRT, 2048bit	0.65
Internal ME, 512bit	4.03
Internal ME, 1024bit	2.03

4.5. SSL Protocol Handshake Performance

The SSL handshake protocol is used to negotiate the secure attributes of a session between Client and Server. This process establishes Protocol Version, Session Identification (SID), Authentication (authentication of the Client is optional), and a symmetric key to help protect the data transmitted between Server and Client. The attributes of an established session can be kept as Session Identification in a Client and/or Server cache for later reuse. This may be of interest as establishing a session is a compute intensive process and requires on the Server side a PKA Private Key operation. This Public Key Decrypt (PKD) on the Server can be performed either in software or may be assisted by cryptographic hardware. In the presented measurements on the z890 the PKD operation will be routed for execution to the PCICA or PCIXCC, if available in the configuration. For all presented measurements the PKD operation is in 'clear key' mode which is currently the predominate usage for SSL protocol communications.

For all SSL protocol performance measurements in this publication the following applies:

- Measurements were performed on a z890 system as a Server. The exact model is indicated with the measurement results.
- The performance data is for the server only. The server was driven to a maximum utilization by increasing the number of client systems (on separate systems) until some system resource came to its limits.
- The key length for the Public Key operation is 1024 bits.
- The SSL data encryption is RC4 (128 bits) and MD5 and is executed in SSL software.
- One packet of 2048 Bytes is used as Send Bytes and Receive Bytes.
- The SSL protocol handshake is the pure handshake with the transfer of one 2048 Bytes data packet.

4.5.1. Applicability of SSL Performance Results to a Customer Environment

As mentioned, the measurements for the SSL protocol handshake include the 'pure' handshake and the transfer of one 2048 Bytes encrypted data packet. There is no instruction processing for the application which means there is no instruction processing that results from a 'business transaction' with e.g. a query and potential update of a data base. The performance numbers

provided give guidelines only on the additional system resources required if an existing On-line transaction environment were converted by replacing the 'unchecked' transaction protocol by an SSL protocol for the communication between Client and Server.

The measurement results show the throughput with four PCICA cards being in the same order of magnitude as with four PCIXCC card in the SSL environment. However, the PCICA feature contains two PCICA cards and the PCIXCC feature contains one PCIXCC card.

The resource consumption in system processing power for one SSL protocol handshake is expected to be in the order of 1/3000 of the system (see table below) in the z/OS environment for a z890 Model 2086-A04 (4 Central Processors) with sufficient number of PCICA or PCIXCC features.

In the z/OS environment the transaction rate of a system z890 Model 2086-A04 is expected to be typically in the range from 300 to 1000 transactions per second. The 'heavier' workloads would result in a longer path length and thus yield a lower transaction rate than the 'lighter' workloads. For other z890 Models the numbers would have to be scaled by applying the relative weights as published in the IBM report 'Large System Performance Reference', at the URL:

<http://www-1.ibm.com/servers/eserver/zseries/lspr/>

If the transaction were to be 'secured' by an SSL protocol and the server portion were run on a zSeries system the maximum transaction rate achieved on that server without the SSL protocol would be reduced by the portion of processing capacity that is required for the Server SSL protocol path length.

4.5.2. SSL Protocol Performance - System SSL with z/OS V1.5/ ICSF level FMID HCR770A

All z890 SSL protocol performance numbers are from measurements with z/OS V1.5 including ICSF level FMID HCR770A: The measurements were performed on a z890 Model 2086-A04. For all measurements the full handshake protocol was executed (no SID caching). The encryption method selected in the SSL handshake was RC4, MD5 and performed in software.

z890 Model 2086-A04 (4 Central Processors)

Cryptographic Hardware	ETR	System Utilization %
4 PCICA Crypto Accelerator Cards	2,957	96.2
4 PCIXCC Crypto Coprocessor Cards	3,033	98.9

In both of the above measurements the z890 Model 2086-A04 system utilization is close to 100 percent. Thus the limitation is in both cases on the system capacity and not on the capability of the cryptographic hardware used to perform the compute intensive PKD operation.

5. z890 January 2005 General Availability Performance Update

With the z890 January 2005 General Availability (z890 GA2), the Crypto Express2 Coprocessor (CEX2C) Feature was introduced. The CEX2C feature is a replacement for the PCIXCC feature, providing the same cryptographic operations. The CEX2C feature differs from the PCIXCC in that it includes 2 coprocessors per feature, thereby increasing the cryptographic capacity. The cryptographic capacity has been further increased by allowing installation of up to 8 CEX2C features (16 cards).

The CEX2C feature is designed to provide high-security cryptographic operations to be used by the z990 and z890 host application programs. The connection of the CEX2C feature via the PCIX bus to the z890 Central Processors (CPs) incurs latency and data transmission time. Because of this connection to the z890 CPs the CEX2C operates asynchronous to the z890 CPs. The CEX2C feature offers the high-security cryptographic operation mode for symmetric key operations and public key operations. In this case the cryptographic keys are encrypted under the corresponding Master Keys when outside the secure boundary of the CEX2C card.

The CEX2C feature also offers public key operations in 'clear key' mode. To provide security-rich communication for Web site-based applications the SSL/TLS protocol is frequently applied. It is current practice to execute the public key operation occurring in the SSL protocol during the set up of the session in 'clear key' mode.

5.1 Definitions

The performance information stated in this section is provided on the ICSF API level. Measurements were performed with the control program z/OS Version 1 Release 6 (z/OS V1.6) and ICSF level FMID HCR7720.

All measurements were performed on an IBM eServer zSeries 890 Model 2086-A04. The internal code level was GA2. If, however, the measurement invokes only one single job the performance behavior is the same as if this measurement were run on a z890 Model 2086-A01 which contains only one Central Processor.

For the cryptographic operations that can be used with a variable length of data such as Data Encryption Algorithm (DEA) Standard encryption, the performance is stated for test cases using different data lengths. The length is specified in Bytes ('K' equals 1024, 'M' equals 1,048,576). The resulting data rate is specified in multiples of 1,000,000 Bytes (not 'M').

5.2 PCIXCC and CEX2C Performance

5.2.1 PCIXCC and CEX2C Multiple Data Symmetric Key Performance

This chapter deals with cryptographic operations with a user supplied length of data as e.g. DES operations.

All test cases are written in zSeries Assembler Language issuing an API call to ICSF for the cryptographic operation. ICSF will resolve the API call and handle the communication with the Cryptographic Coprocessor feature which does the actual cryptographic processing. The symmetric key that is used for the cryptographic operation is encrypted under the corresponding Master Key which in turn is kept in the secure boundary of the Cryptographic Coprocessor.

The throughput of multiple data symmetric key operations using the Cryptographic Coprocessor is considerably less than the throughput for the corresponding functions using the CP Assist for Cryptographic Function (CPACF) hardware. For this type of cryptographic operation the Cryptographic Coprocessor feature should be used only when the security requirements for the application require it. Be aware that in the tables of this chapter the rates are quoted in thousands of bytes, as were the PCIXCC measurements in Chapters 4.2 and 4.3.

The data quoted is from test cases run on a z890 Model 2086-A04 with either one PCIXCC feature (1 coprocessor) or one CEX2C feature (2 coprocessors) performing the cryptographic operation. For each cryptographic operation type, data is presented for test results with one job executing the cryptographic operation and with multiple jobs executing the cryptographic operation. The tests with multiple jobs are designed to approximate the maximum throughput capability of the Cryptographic Coprocessor by attempting to keep the Cryptographic Coprocessor queues full with encryption requests.

PCIXCC and CEX2C DEA Cipher Block Chaining Encipher with Single Length Key (56 Bits)

Single DES CBC Encipher (one job)				
Crypto Features	1 PCIXCC	1 PCIXCC	1 CEX2C	1 CEX2C
Block size B	Operations/sec	x10**3 B/s	Operations/sec	x10**3 B/s
64	876.1	56.1	879.1	56.3
256	873.9	223.7	878.8	226.0
1024	597.6	611.9	872.0	892.9
4096	450.9	1846.9	453.2	1856.3
64K	39.55	2591.9	39.68	2600.5
1M	2.54	2659.2	2.54	2666.5

The above table provides measurement results for an environment where one job was continuously executing the cryptographic operation using one Cryptographic Coprocessor feature. As mentioned, the execution of the cryptographic operation in the card is asynchronous to the zSeries Central Processor (CP) execution. As only one job is run on the CP the next cryptographic operation is started only when the result of the previous cryptographic operation has been received by the CP. Thus there is a considerable delay before the next cryptographic operation can be initiated by the host CP. This inefficiency is removed when the host program consists of several jobs requesting the same cryptographic operation repetitively. The CEX2C card's multitasking capability allows for enqueueing and dequeuing of requests in parallel with cryptographic operations being performed. A measurement environment using several parallel jobs highlights better the throughput capacity of the card whereas the 'single job' measurement environment is better suited to highlight the delay an application experiences waiting for the result of the cryptographic operation performed in the card.

Single DES CBC Encipher (multiple jobs)			
Crypto Features/jobs	1 PCIXCC, 7 jobs	1 CEX2C, 14 jobs	Ratio
Block size B	Operations/sec	Operations/sec	CEX2C/PCIXCC
64	1356	2722	2.01
256	1307	2537	1.94
1024	1084	2070	1.91
4096	634.2	1171	1.85
64K	51.48	94.95	1.84
1M	3.27	6.05	1.85

The table above contains measurement results for an environment where enough parallel jobs are executing to keep the cryptographic coprocessors busy. The throughput with 1 CEX2C feature containing 2 cryptographic coprocessors is in the range of 1.84 times to 2.01 times the throughput with 1 PCIXCC feature containing 1 cryptographic coprocessor in this environment.

The throughput with N cryptographic cards with a sufficient number of jobs repetitively requesting the same cryptographic operation for Single DES, Triple DES, and Single DES Message Authentication (MAC) (see the following tables) is expected to be close to N times the throughput of one cryptographic card with 7 jobs (as exemplified above).

PCIXCC and CEX2C DEA Cipher Block Chaining Encipher with Triple Length Key (168 Bits)

Triple DES CBC Encipher (one job)				
Crypto Features	1 PCIXCC	1 PCIXCC	1 CEX2C	1 CEX2C
Block size B	Operations/sec	x10**3 B/s	Operations/sec	x10**3 B/s
64	874.2	55.9	879.1	56.3
256	790.7	202.4	879.0	225.0
1024	597.5	611.8	704.2	721.1
4096	448.3	1836.2	453.2	1856.3
64K	39.53	2590.6	39.67	2599.8
1M	2.54	2659.2	2.54	2666.5

The throughput with 1 CEX2C feature is in the order of 1.00 times to 1.18 times the throughput with 1 PCIXCC feature when only one job is executing the cryptographic operation.

Triple DES CBC Encipher (multiple jobs)			
Crypto Feat./Jobs	1 PCIXCC, 7 jobs	1 CEX2C, 14 jobs	Ratio
Block size B	Operations/sec	Operations/sec	CEX2C/PCIXCC
64	1290	2538	1.97
256	1249	2329	1.86
1024	1028	1966	1.91
4096	615.3	1137	1.85
64K	50.58	93.94	1.86
1M	3.23	5.99	1.86

The throughput with 1 CEX2C feature containing 2 cryptographic coprocessors is in the order of 1.85 times to 1.97 times the throughput with 1 PCIXCC feature containing 1 cryptographic coprocessor when enough parallel jobs are executing to keep the cryptographic coprocessors busy.

PCIXCC and CEX2C Message Authentication Code with DEA Single Length Key (56 Bits)

MAC with single DES (one job)				
Crypto Features	1 PCIXCC	1 PCIXCC	1 CEX2C	1 CEX2C
Block size B	Operations/sec	x10**3 B/s	Operations/sec	x10**3 B/s
64	877.0	56.1	879.9	56.3
256	876.8	224.5	879.7	225.2
1024	875.7	896.7	878.9	900.0
4096	597.0	2445.3	598.7	2452.3
64K	54.42	3566.5	48.26	3162.8
1M	3.52	3686.8	3.01	3155.2

The throughput with 1 CEX2C feature is equivalent to the throughput with 1 PCIXCC feature for data sizes up to 4KB when only one job is executing the cryptographic operation. For 64K and 1M data sizes, PCIXCC throughput is 11% and 14% higher respectively.

MAC with single DES (multiple jobs)			
Crypto Feat./Jobs	1 PCIXCC, 7 jobs	1 CEX2C, 14 jobs	Ratio
Block size B	Operations/sec	Operations/sec	CEX2C/PCIXCC
64	1494	2849	1.91
256	1445	2733	1.89
1024	1279	2388	1.87
4096	860.6	1607	1.87
64K	63.23	117.2	1.85
1M	4.00	7.45	1.86

The throughput with 1 CEX2C feature containing 2 cryptographic coprocessors is in the order of 1.85 times to 1.91 times the throughput with 1 PCIXCC feature containing 1 cryptographic coprocessor when enough parallel jobs are executing to keep the cryptographic coprocessors busy.

5.2.2 PCIXCC and CEX2C PKA Performance

The PCIXCC and CEX2C features are designed to offer good Public Key Algorithm (PKA) cryptographic operation performance in addition to the high-security environment. The PKA performance is listed for RSA key modulus length of 512 bits, 1024 bits (1K bits), and 2048 bits (2K bits).

The numbers quoted for performing the Public Key Decrypt (PKD) cryptographic operation (using the Private Exponent) are either through the Chinese Remainder Theorem (CRT) Format or the Modulus Exponent (ME) Format. The PKD operation uses the private key in 'clear key' mode.

For the Public Key Encrypt (PKE) cryptographic operation ICSF always uses an RSA public key with the Modulus Exponent (ME) Format. The modulus is according to the length specified and the (Public) Exponent has the value of 65537 which in hexadecimal notation is X'10001' (with leading zeros up to the length of the modulus).

For the Digital Signature Generate (DSG) and the Symmetric Key Import (SYI) cryptographic operations the PKA keys (signature key or encryption key) are encrypted under the corresponding master key.

The performance numbers are from measurements with z/OS V1.6 including ICSF level FMID HCR7720 invoking the operation via the ICSF API according to the PKCS-1.2. Standard. Measurements were performed on a z890 Model 2086-A04.

PCIXCC and CEX2C on z/OS V1.6 (ICSF level: FMID HR7720)

Public Key Decrypt (PKD), Public Key Encrypt (PKE)
 Digital Signature Generate (DSG), Digital Signature Verify (DSV)
 Symmetric Key Import (encrypted with RSA key) (SYI)

	2086-A04	2086-A04	
Crypto features	1 PCIXCC	1 CEX2C	
Jobs	1	1	
	Ops/s	Ops/s	Ratio CEX2C/PCIXCC
PKD--CRT, 512 bit	755.5	838.9	1.11
PKD--CRT, 1024 bit	592.9	594.6	1.00
PKD--CRT, 2048 bit	262.6	263.3	1.00
PKD--ME, 512 bit	593.1	594.7	1.00
PKD--ME, 1024 bit	451.0	452.4	1.00
PKE, 512 bit	869.2	872.1	1.00
PKE, 1024 bit	838.5	869.8	1.04
PKE, 2048 bit	594.3	596.0	1.00
DSG--CRT, 512 bit	799.0	856.7	1.07
DSG--CRT, 1024 bit	593.3	594.8	1.00
DSG--CRT, 2048 bit	262.6	263.3	1.00
DSV--CRT, 512 bit	874.4	877.2	1.00
DSV--CRT, 1024 bit	873.9	876.8	1.00
DSV--CRT, 2048 bit	803.1	874.3	1.09
DSV--ME, 512 bit	874.4	876.9	1.00
DSV--ME, 1024 bit	874.3	876.8	1.00
SYI--CRT, 512 bit	593.6	595.4	1.00
SYI--CRT, 1024 bit	559.8	547.1	0.98

Measured throughput with one job using the CEX2C feature was at least equivalent to and sometimes better than measured results using the PCIXCC feature, with the exception of the Symmetric Key Import operation with a 1024 bit modulus which had slightly lower throughput.

	2086-A04	2086-A04	
Crypto Features	1 PCIXCC	1 CEX2C	
Jobs	7	14	
			Ratio
	Ops/s	Ops/s	CEX2C/PCIXCC
PKD--CRT, 512 bit	1179	2166	1.84
PKD--CRT, 1024 bit	1078	1952	1.81
PKD--CRT, 2048 bit	464.8	918.1	1.98
PKD--ME, 512 bit	1177	2123	1.80
PKD--ME, 1024 bit	912.3	1809	1.98
PKE, 512 bit	1282	2410	1.88
PKE, 1024 bit	1093	2063	1.89
PKE, 2048 bit	833.1	1583	1.90
DSG--CRT, 512 bit	1199	2077	1.73
DSG--CRT, 1024 bit	1094	1994	1.82
DSG--CRT, 2048 bit	465.3	918	1.97
DSV--CRT, 512 bit	1436	2682	1.87
DSV--CRT, 1024 bit	1376	2559	1.86
DSV--CRT, 2048 bit	1247	2302	1.85
DSV--ME, 512 bit	1440	2691	1.87
DSV--ME, 1024 bit	1376	2545	1.85
SYI--CRT, 512 bit	908.3	1667	1.84
SYI--CRT, 1024 bit	852.3	1570	1.84

With enough concurrent jobs to keep the coprocessors busy CEX2C throughput is in the range of 1.73 times to 1.98 times the PCIXCC throughput.

The throughput with N CEX2C features with a sufficient number of jobs repetitively requesting the same cryptographic operation for the examples in the table above is expected to be close to N times the throughput of one CEX2C feature with 14 jobs (as exemplified above).

The PCIXCC and CEX2C features also offer services to generate PKA RSA Keys. The PKA RSA Key Generate performance is listed for RSA key modulus length of 512 bits, 1024 bits (1K bits), and 2048 bits (2K bits) dependent on the Format, either the Chinese Remainder Theorem (CRT) Format or the Modulus Exponent (ME) Format.

PKA Key Generation is a compute intensive operation. The table below specifies the number of key generations per second provided by one PCIXCC feature (1 coprocessor) and one CEX2C feature (2 coprocessors). ICSF will only send one key generate operation to a coprocessor at a time, so one job was used with the PCIXCC feature and two jobs with the CEX2C feature.

PCIXCC and CEX2C RSA Key Generation Performance

PCIXCC and CEX2C PKA RSA Key Generate			
Crypto Features	1 PCIXCC	1 CEX2C	
Jobs	1	2	Ratio
	Operations/sec	Operations/sec	CEX2C/PCIXCC
External CRT, 512bit	3.49	4.84	1.39
External CRT, 1024bit	1.70	2.44	1.44
External CRT, 2048bit	0.73	0.95	1.30
Internal ME, 512bit	4.26	5.89	1.38
Internal ME, 1024bit	2.13	2.98	1.40

Throughput with both coprocessors of a CEX2C feature active is in the range of 1.30 times to 1.44 times the throughput with one PCIXCC feature.

5.3 SSL Protocol Handshake Performance

The SSL handshake protocol is used to negotiate the secure attributes of a session between Client and Server. This process establishes Protocol Version, Session Identification (SID), Authentication (authentication of the Client is optional), and a symmetric key to help protect the data transmitted between Server and Client. The attributes of an established session can be kept as Session Identification in a Client and/or Server cache for later reuse. This may be of interest as establishing a session is a compute intensive process and requires on the Server side a PKA Private Key operation. This Public Key Decrypt (PKD) on the Server can be performed either in software or may be assisted by cryptographic hardware. In the presented measurements on the z890 the PKD operation will be routed for execution to the PCIXCC or CEX2C, if available in the configuration. For all presented measurements the PKD operation is in 'clear key' mode which is currently the predominate usage for SSL protocol communications.

For all SSL protocol performance measurements in this publication the following applies:

- Measurements were performed on a z890 system as a Server. The exact model is indicated with the measurement results.
- The performance data is for the server only. The server was driven to a maximum utilization by increasing the number of client systems (on separate systems) until some system resource came to its limits.
- The key length for the Public Key operation is 1024 bits.
- One packet of 2048 Bytes is used as Send Bytes and Receive Bytes.

- The SSL protocol handshake is the pure handshake with the transfer of one 2048 Bytes data packet.

5.3.1. Applicability of SSL Performance Results to a Customer Environment

As mentioned, the measurements for the SSL protocol handshake include the 'pure' handshake and the transfer of one 2048 Bytes encrypted data packet. There is no instruction processing for the application which means there is no instruction processing that results from a 'business transaction' with e.g. a query and potential update of a data base. The performance numbers provided give guidelines only on the additional system resources required if an existing On-line transaction environment were converted by replacing the 'unchecked' transaction protocol with an SSL protocol for the communication between Client and Server.

The measurement results show the throughput with four PCIXCC features (each feature contains 1 coprocessor card) being in the same order of magnitude as with two CEX2C features (each feature contains 2 coprocessor cards).

The resource consumption in system processing power for one SSL protocol handshake is expected to be in the order of 1/3000 of the system (see table below) in the z/OS environment for a z890 Model 2086-A04 (4 Central Processors) with sufficient number of PCIXCC or CEX2C features.

In the z/OS environment the transaction rate of a system z890 Model 2086-A04 is expected to be typically in the range from 300 to 1000 transactions per second. The 'heavier' workloads would result in a longer path length and thus yield a lower transaction rate than the 'lighter' workloads. For other z890 Models the numbers would have to be scaled by applying the relative weights as published in the IBM report 'Large System Performance Reference', at the URL:

<http://www-1.ibm.com/servers/eserver/zseries/lspr/>

If the transaction were to be 'secured' by an SSL protocol and the server portion were run on a zSeries system the maximum transaction rate achieved on that server without the SSL protocol would be reduced by the portion of processing capacity that is required for the Server SSL protocol path length.

5.3.2 SSL Protocol Performance - System SSL with z/OS V1.6/ ICSF level FMID HCR7720

All z890 SSL protocol performance numbers are from measurements with z/OS V1.6 including ICSF level FMID HCR7720. The measurements were performed on a z890 Model 2086-A04. For all measurements the full handshake protocol was executed (no SID caching).

z890 Model 2086-A04 (4 Central Processors)

Cryptographic Hardware	Cipher	ETR	System Utilization %
4 PCIXCC Crypto Coprocessor Features	RC4,MD5	3,158	99.09
2 CEX2C Crypto Coprocessor Features	RC4,MD5	3,150	98.86
4 PCIXCC Crypto Coprocessor Features	TDES,SHA	3,550	92.71
2 CEX2C Crypto Coprocessor Features	TDES,SHA	3,558	93.05

SSL handshake capacity of the z890 system was not affected by the type of cryptographic coprocessor (PCIXCC or CEX2C) that was used.

For all measurements in the above table, the compute intensive SSL handshake PKD operation was executed on the cryptographic hardware. The RC4 cipher with MD5 authentication is always performed in software. The TDES cipher with SHA authentication is executed on the CPACF, resulting in an increase in ETR and a decrease in System CPU Utilization when compared to the RC4,MD5 results.

© Copyright IBM Corporation 2003

IBM Corporation

Marketing Communications, Server Group

Route 100

Somers, NY 10589

U.S.A.

Produced in the United States of America

All Rights Reserved

IBM, IBM @server, IBM eServer, the IBM logo, the e-business logo, HiperSockets, OS/390, RACF, S/390, z/OS, z/VM, and zSeries are trademarks or registered trademarks of International Business Machines Corporation of the United States, other countries or both.

Intel is a registered trademark of the Intel Corporation in the United States, other countries or both.

Linux is a registered trademark of Linux Torvalds.

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

IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Performance is in External Throughput Rate (ETR) based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance rates stated here.