

IBM eServer zSeries 990 Performance of Cryptographic Operations

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

Table of Content

| | |
|--|---------|
| IBM eServer zSeries 990 Performance of Cryptographic Operations | Page 1 |
| (Cryptographic Hardware: CPACF, PCICA, PCIXCC, CEX2C) | Page 1 |
| Preface | Page 3 |
| 2. Cryptographic Hardware supported on zSeries 990 | Page 4 |
| 2.1. CP Assist for Cryptographic Function (CPACF) | Page 4 |
| 2.2. PCI Cryptographic Accelerator (PCICA) Feature | Page 4 |
| 2.3. PCIX Cryptographic Coprocessor (PCIXCC) Feature | Page 5 |
| 2.4. CEX2 Cryptographic Coprocessor (CEX2C) Feature | Page 6 |
| 3. Exploitation of Cryptographic Hardware in z990 | Page 7 |
| 3.1. SSL Protocol based Communication | Page 8 |
| 4. Performance Information | Page 9 |
| 4.1. Definitions | Page 9 |
| 4.2. CP Assist for Cryptographic Function (CPACF) | Page 9 |
| 4.2.1. CP Assist for Cryptographic Function (CPACF) Performance - Architecture Instruction Interface ('Native') | Page 10 |
| 4.2.2. CP Assist for Cryptographic Function (CPACF) Performance - ICSF API Interface | Page 11 |
| 4.3. Symmetric Key Advanced Encryption Standard (AES) Performance - ICSF API Interface | Page 13 |
| 4.4. PCICA Performance | Page 14 |
| 4.5. PCIXCC Performance | Page 16 |
| 4.5.1. PCIXCC Multiple Data Symmetric Key Performance | Page 16 |
| 4.5.2. PCIXCC Symmetric Key Performance - Divers Operations | Page 18 |
| 4.5.3. PCIXCC PKA Performance | Page 19 |
| 4.6. SSL Protocol Handshake Performance | Page 21 |
| 4.6.1. Applicability of SSL Performance Results to a Customer Environment | Page 22 |
| 4.6.2. SSL Protocol Performance - System SSL with z/OS V1.4+E / ICSF level WD2 PID | Page 23 |
| 4.6.3. SSL Protocol Performance - Linux Open SSL | Page 24 |
| 5. January 2005 General Availability Update | Page 25 |
| 5.1 Definitions | Page 25 |
| 5.2 PCIXCC and CEX2C Performance | Page 26 |
| 5.2.2 CEX2C Symmetric Key Performance - Divers Operations | Page 30 |
| 5.2.3. PCIXCC PKA Performance | Page 30 |
| 5.3. SSL Protocol Handshake Performance | Page 33 |
| 5.3.1. Applicability of SSL Performance Results to a Customer Environment | Page 34 |
| 5.3.2. SSL Protocol Performance - System SSL with z/OS V1.6 / ICSF level WD4 PID | Page 35 |
| 5.3.3. SSL Protocol Performance - Linux Open SSL | Page 36 |

Preface

The performance information presented in this publication was measured on IBM eServer® 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

The purpose of this publication is to provide performance information to the user of cryptographic services on IBM eServer zSeries 990 (z990) systems. With the General Availability (GA) of the Crypto Express2 (CEX2C) feature in January, 2005, the zSeries now supports 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. Crypto Express2 (CEX2C) feature.

An earlier publication covered the performance of the cryptographic hardware as available on the zSeries 990 at General Availability in May 2003 (GA1) which consisted of the CPACF and the PCICA. Since most of the measurements that were the base of this publication were repeated on newer levels of internal code, z/OS®, and ICSF it seemed appropriate to present the performance of all cryptographic hardware available for zSeries 990 in one new publication.

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 PCI Cryptographic Accelerator Feature is available on z990 and has been supported on IBM eServer zSeries 900 (z900) already. It may be carried forward on upgrades from z900 to z990. 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 available on z990 since September 2003. The 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 z990 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 990

2.1. CP Assist for Cryptographic Function (CPACF)

zSeries 990 introduces the z990 Message Security Assist (MSA) Architecture along with the new 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 z900 and continues to be supported on z990. 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 6 PCICA features per 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 12 cryptographic accelerator cards in a z990 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 z990 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 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 990 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. PCIX Cryptographic Coprocessor (PCIXCC) Feature

The PCIX Cryptographic Coprocessor Feature was announced in May of 2003 with the zSeries 990 but with a later availability. Customer shipment started in September 2003.

The PCIXCC feature supports:

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

The PCIX Cryptographic Coprocessor (PCIXCC) feature contains one PCIX Cryptographic Coprocessor with its physical implementation on a card.

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 z990 system. The communication mechanism between a z990 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 z990 CP. A special CP task will poll for finished operations of the PCIX Cryptographic Coprocessor, dequeue them, and 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 990 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. CEX2 Cryptographic Coprocessor (CEX2C) Feature

The Cryptographic Express2 Coprocessor Feature was announced in October 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 Cryptographic Express2 Coprocessor (CEX2C) feature contains two cryptographic coprocessors cards. There can be a maximum of 8 CEX2C features in a z990 system for a total of 16 cryptographic coprocessor cards.

The Cryptographic 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 Cryptographic 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 Cryptographic Express2 Coprocessor.

The Cryptographic Express2 Coprocessor executes its cryptographic operations asynchronously to a Central Processor (CP) operation in the z990 system. The communication mechanism between a z990 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 z990 CP. A special CP task will poll at fixed time intervals for finished operations of the Cryptographic Express2 Coprocessor, dequeue them, and 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 Cryptographic Express2 Coprocessor, several operations can be worked on in parallel.

For zSeries 990 systems, the Cryptographic 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 Cryptographic Express2 Coprocessor. For unique customer cryptographic application requirements the Cryptographic Express2 Coprocessor provides for user-defined extensions (UDX) to the Common Cryptographic Architecture interface.

3. Exploitation of Cryptographic Hardware in z990

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 (API) 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. The performance of both modes of operation will be presented in this publication.

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 990 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 z990 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 following environments:

- z/OS
- Linux

- Linux under z/VM®

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 normally provided on the ICSF API level except when stated otherwise. Measurements were performed with the control program z/OS Version 1 Release 4+E (z/OS V1.4 with the z990 Exploitation Support Feature) and ICSF level WD2 PID, except when stated otherwise.

All measurements were performed on an IBM eServer zSeries 990. The internal code level was GA2, October 2003. The exact model of the z990 system used is stated with each measurement. Some of the measurements were run on a z990 Model 2084-304. 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 z990 Model 2084-301 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)

4.2.1. CP Assist for Cryptographic Function (CPACF) Performance - Architecture Instruction Interface ('Native')

All test cases are written in zSeries Assembler Language issuing the zSeries Message Security Assist (MSA) Architecture cryptographic operation instructions as indicated with each group.

The data quoted was from test cases run on a z990 Model 2084-304, however, using only one of the CPs. For each cryptographic operation type quoted, there is a statement on scalability of the

results if multiple CPs are being used. The throughput using N CPs performing the same cryptographic operation is close to N times the throughput of using one CP. The reduction of the measured throughput from N times the throughput of one CP is stated with each measurement.

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)

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

| Native: Single DES CBC Encipher (KMC-DEA) | | |
|---|----------------|------------------|
| Data Length (Bytes) | Operations/sec | x10**6 Bytes/sec |
| 64 | 3347438.0 | 214.2 |
| 256 | 1347711.0 | 345.0 |
| 1024 | 395954.0 | 405.5 |
| 4096 | 104097.0 | 426.4 |
| 64K | 6478.0 | 424.5 |
| 1M | 399.6 | 419.0 |

The KMC-DEA operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 3 percent (with 16 CPs) except for very short data lengths. DEA Cipher Block Chaining Decipher (CBC) with Single Length Key has basically the same performance characteristics as the Encipher operation (reduction is less than 2 percent). DEA Electronic Code Book Encipher (ECB, without chaining) with Single Length Key has basically the same performance characteristics as the corresponding CBC Encipher operation (increase for small data length up to 8 percent, for larger data length about .5 percent).

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

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

| Native: Triple DES CBC Encipher (KMC-TDEA) | | |
|--|----------------|------------------|
| Data Length (Bytes) | Operations/sec | x10**6 Bytes/sec |
| 64 | 1881135.0 | 120.4 |
| 256 | 590479.0 | 151.2 |
| 1024 | 157153.0 | 160.9 |
| 4096 | 39901.0 | 163.4 |
| 64K | 2490.0 | 163.2 |
| 1M | 154.7 | 162.2 |

The KMC-TDEA operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 3 percent (with 16 CPs).

DEA Cipher Block Chaining Decipher with Triple Length Key has basically the same performance characteristics as the Encipher operation (reduction is less than 1 percent).

Compute Message Authentication Code with DEA Single Length Key (56 Bits) (zSeries Message Security Assist Architecture instruction: KMAC-DEA)

| Native: MAC with single DES (KMAC-DEA) | | |
|--|----------------|------------------|
| Data Length (Bytes) | Operations/sec | x10**6 Bytes/sec |
| 64 | 4165152 | 266.6 |
| 256 | 1469222.0 | 376.1 |
| 1024 | 406720.0 | 416.5 |
| 4096 | 104523.0 | 428.1 |
| 64K | 6547.0 | 429.1 |
| 1M | 406.1 | 425.8 |

The KMAC-DEA operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 3 percent (with 16 CPs) except for very short data length.

Compute Message Digest SHA-1

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

| Native: SHA-1(KLMD-SHA-1) | | |
|---------------------------|----------------|------------------|
| Data Length (Bytes) | Operations/sec | x10**6 Bytes/sec |
| 64 | 2053465.0 | 131.4 |
| 256 | 982019.0 | 251.4 |
| 1024 | 318653.0 | 326.3 |
| 4096 | 86526.0 | 354.4 |
| 64K | 5490.0 | 359.8 |
| 1M | 341.0 | 357.6 |

The KLMD-SHA-1 operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 3 percent (with 16 CPs) except for very short data length.

4.2.2. 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 zSeries Message Security Assist (MSA) Architecture as indicated with each group.

The data quoted was from test cases run on a z990 Model 2084-304, however, using only one of the CPs. For each cryptographic operation type quoted there is a statement on scalability of the results if multiple CPs are being used. The throughput using N CPs performing the same cryptographic operation is close to N times the throughput of using one CP. The reduction of the measured throughput from N times the throughput of one CP is stated with each measurement.

As the performance measurement results show all ICSF API interface test cases show lower throughput than the equivalent 'Native' test cases. This is expected 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.

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 | 100598.0 | 6.44 |
| 256 | 95933.0 | 24.56 |
| 1024 | 82133.0 | 84.10 |
| 4096 | 51840.0 | 212.34 |
| 64K | 6072.0 | 397.93 |
| 1M | 397.1 | 416.39 |

The DEA Encipher with Single Length Key operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 15 % for 8 CPs and short data lengths and decreases for higher data lengths to less than 1 percent.

DEA 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 | 97892.0 | 6.27 |
| 256 | 87785.0 | 22.47 |
| 1024 | 62226.0 | 63.72 |
| 4096 | 28763.0 | 117.81 |
| 64K | 2422.0 | 158.73 |
| 1M | 154.2 | 161.69 |

The DEA Encipher with Triple Length Key operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 15 % for 8 CPs and short data lengths and decreases for higher data lengths to less than 1 percent.

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 | 73093.0 | 4.68 |
| 256 | 70108.0 | 17.95 |
| 1024 | 61074.0 | 62.54 |
| 4096 | 40303.0 | 165.08 |
| 64K | 5104.0 | 334.50 |
| 1M | 338.3 | 354.73 |

The Compute message Digest SHA-1 operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 15 % for 8 CPs and short data lengths and decreases for higher data lengths to less than 1 percent.

4.3. Symmetric Key Advanced Encryption Standard (AES) Performance - ICSF API Interface

The Advanced Encryption Standard (AES) is available as a standard for some time and is now emerging in applications. IBM provides software implementations for AES as customers are exploring usage. For this purpose performance information is included in this publication.

AES encryption services are provided in the z/OS environment as API calls to ICSF software routines.

The data quoted was from test cases run on a z990 Model 2084-304, however, using only one of the CPs. For each cryptographic operation type quoted there is a statement on scalability of the results if multiple CPs are being used. The throughput using N CPs performing the same cryptographic operation is close to N times the throughput of using one CP. The reduction of the measured throughput from N times the throughput of one CP is stated with each measurement.

All measurements were performed with z/OS V1.4+E and ICSF level WD2 PID.

AES128 Encipher (128 bit Key Length) - ICSF API

| AES128 Encipher (128 bit key) in software | | |
|---|----------------|------------------|
| Data Length (Bytes) | Operations/sec | x10**6 Bytes/sec |
| 64 | 82884.0 | 5.30 |
| 256 | 59502.0 | 15.23 |
| 1024 | 27712.0 | 28.38 |
| 4096 | 8833.0 | 36.18 |
| 64K | 603.8 | 39.57 |
| 1M | 37.8 | 39.58 |

The AES128 Encipher operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is in the order of 10 % for 8 CPs and short data lengths and decreases for higher data lengths to about 1 percent.

AES128 Decipher (128 bit Key Length) - ICSF API

| AES128 Decipher (128 bit key) in software | | |
|---|----------------|------------------|
| Data Length (Bytes) | Operations/sec | x10**6 Bytes/sec |
| 64 | 74130.0 | 4.74 |
| 256 | 54396.0 | 13.93 |
| 1024 | 26060.0 | 26.69 |
| 4096 | 8474.0 | 34.71 |
| 64K | 582.2 | 38.16 |
| 1M | 36.5 | 38.33 |

The AES128 Decipher operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is in the order of 10 % for 8 CPs and short data length and decreases for higher data length to about 1 percent.

AES256 Encipher (256 bit Key Length) - ICSF API

| AES256 Encipher (256 bit key) in software | | |
|---|----------------|------------------|
| Data Length (Bytes) | Operations/sec | x10**6 Bytes/sec |
| 64 | 78350.0 | 5.01 |
| 256 | 52408.0 | 13.42 |
| 1024 | 22319.0 | 22.85 |
| 4096 | 6785.0 | 27.79 |
| 64K | 454.3 | 29.77 |
| 1M | 28.4 | 29.79 |

The AES256 Encipher operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is in the order of 10 % for 8 CPs and short data lengths and decreases for higher data lengths to about 1 percent.

AES256 Decipher (256 bit Key Length) - ICSF API

| AES256 Decipher (256 bit key) in software | | |
|---|----------------|------------------|
| Data Length (Bytes) | Operations/sec | x10**6 Bytes/sec |
| 64 | 67574.0 | 4.32 |
| 256 | 47272.0 | 12.10 |
| 1024 | 26500.0 | 21.75 |
| 4096 | 6625.0 | 27.14 |
| 64K | 448.3 | 29.38 |
| 1M | 28.1 | 29.46 |

The AES256 Decipher operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is in the order of 10 % for 8 CPs and short data lengths and decreases for higher data lengths to about 1 percent.

4.4. 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 V1.4+E including ICSF level WD2 PID 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 6 PCICA features per system with a maximum of 12 cryptographic accelerator cards in a system

PCICA PKA Performance

| PCICA Public Key Decrypt (PKD) and Public Key Encrypt (PKE) (z/OS V1.4+E ,ICSF: WD2 PID) | | | | |
|--|----------------|----------------|----------------|----------------|
| | 2084-304 | 2084-304 | 2084-304 | 2084-304 |
| PCICA Cryp.Acc.Card | 1 | 1 | 6 | 12 |
| Jobs | 1 | 8 | 48 | 96 |
| | Operations/sec | Operations/sec | Operations/sec | Operations/sec |
| PKD--CRT, 512 bit | 600 | 3566 | 17576 | 27401 |
| PKD--CRT, 1024 bit | 205 | 1093 | 6397 | 12417 |
| PKD--CRT, 2048 bit | 53 | 268 | 1568 | 3053 |
| PKD--ME, 512 bit | 366 | 2189 | 12762 | 23148 |
| PKD--ME, 1024 bit | 103 | 544 | 3184 | 6194 |
| PKE, 512 bit | 855 | 3805 | 15950 | 26890 |
| PKE, 1024 bit | 457 | 3526 | 15477 | 25538 |
| PKE, 2048 bit | 303 | 1681 | 9699 | 16136 |

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 and fourth column of the above table are for measurements where 48 and 96 jobs respectively were continuously executing the same cryptographic operation using 6 and 12 PCICA cryptographic accelerator cards respectively. The results show the maximum and the scalability of the throughput due to multiple PCICA features being used in one z990 system.

4.5. PCIXCC Performance

The PCIX Cryptographic Coprocessor is designed to provide high-security cryptographic operations to be used by the z990 host application programs. The connection of the PCIX Cryptographic Coprocessor feature via the PCIX bus to the z990 Central Processors (CPs) incurs latency and data transmission time. Because of this connection to the z990 CPs the PCIX Cryptographic Coprocessor operates asynchronous to the z990 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 z990 system, each PCIXCC feature containing one PCIXCC card.

4.5.1. 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 z990 Model 2084-304 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 V1.4+E including ICSF level WD2 PID.

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

| PCIXCC (one job): Single DES CBC Encipher | | |
|---|----------------|------------------|
| Data Length (Bytes) | Operations/sec | x10**3 Bytes/sec |
| 64 | 888.89 | 56.9 |
| 256 | 886.40 | 226.9 |
| 1024 | 603.10 | 617.6 |
| 4096 | 454.10 | 1860.0 |
| 64K | 39.65 | 2598.5 |
| 1M | 2.54 | 2661.3 |

The above table provides measurement results for an environment where one job was continuously executing the cryptographic operation using one PCIX 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 | | |
|--|----------------|------------------|
| Data Length (Bytes) | Operations/sec | x10**3 Bytes/sec |
| 64 | 1383.0 | 88.5 |
| 256 | 1327.0 | 339.7 |
| 1024 | 1095.0 | 1121.3 |
| 4096 | 634.9 | 2600.6 |
| 64K | 51.4 | 3371.2 |
| 1M | 3.3 | 3435.1 |

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 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 | | |
|---|----------------|------------------|
| Data Length (Bytes) | Operations/sec | x10**3 Bytes/sec |
| 64 | 886.50 | 56.7 |
| 256 | 790.30 | 202.3 |
| 1024 | 602.80 | 617.3 |
| 4096 | 451.40 | 1848.9 |
| 64K | 39.63 | 2597.2 |
| 1M | 2.54 | 2663.4 |

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 | | |
|---------------------------------------|----------------|------------------|
| Data Length (Bytes) | Operations/sec | x10**3 Bytes/sec |
| 64 | 889.50 | 56.9 |
| 256 | 889.40 | 227.7 |
| 1024 | 888.70 | 910.0 |
| 4096 | 602.30 | 2467.0 |
| 64K | 53.36 | 3497.0 |
| 1M | 3.36 | 3523.2 |

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.

4.5.2. PCIXCC Symmetric Key Performance - Divers Operations

The following table gives the performance in maximum number of operations per second for one PCIX Cryptographic Coprocessor for some selected symmetric key operations.

| PCIXCC Symmetric Key Operations - Examples | Ops/s | Ops/s |
|---|-------|--------|
| | 1 job | 7 jobs |
| Key Generate (operational DES KEYGENKY key) | 604 | 945 |
| Clear PIN Generate Alternate (DES OPINENC + DES PINGEN keys) | 605 | 1,014 |
| Clear PIN Generate (16 digits) (DES PINGEN key) | 819 | 1,442 |
| Encrypted PIN Translation (DES IPINENC key + DES OPINENC key) | 605 | 1,023 |
| Encrypted PIN Translation (2 UKPT enabled KEYGENKY keys) | 308 | 346 |
| Encryp.PIN Verificat. (UKPT enabl.KEYGENKY+DES PINVER keys) | 457 | 509 |

The 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 close to N times the throughput of one PCIXCC card with 7 jobs.

4.5.3. PCIXCC PKA Performance

The PCIX 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 V1.4+E including ICSF level WD2 PID invoking the operation via the ICSF API according to the PKCS-1.2. Standard. Measurements were performed on a z990 Model 2084-304.

PCIXCC PKA Performance

| PCIXCC on z/OS V1.4+E (ICSF level: WD2 PID) | | | | |
|---|----------------|----------------|----------------|----------------|
| Public Key Decrypt (PKD), Public Key Encrypt (PKE) Digital Signature Generate (DSG), Digital Sign. Verify (DSV) Symmetric Key Import (encrypted with RSA key) (SYI) | | | | |
| | 2084-304 | 2084-304 | 2084-304 | 2084-304 |
| PCIXCC cards | 1 | 1 | 2 | 4 |
| Jobs | 1 | 7 | 14 | 28 |
| | Operations/sec | Operations/sec | Operations/sec | Operations/sec |
| PKD--CRT, 512 bit | 834 | 1190 | 2380 | 4745 |
| PKD--CRT, 1024 bit | 600 | 1084 | 2172 | 4223 |
| PKD--CRT, 2048 bit | 264 | 466 | 930 | 1854 |
| PKD--ME, 512 bit | 600 | 1183 | 2369 | 4717 |
| PKD--ME, 1024 bit | 455 | 914 | 1827 | 3645 |
| PKE, 512 bit | 882 | 1295 | 2591 | 5174 |
| PKE, 1024 bit | 847 | 1076 | 2161 | 4312 |
| PKE, 2048 bit | 600 | 801 | 1603 | 3197 |
| DSG--CRT, 512 bit | 847 | 1198 | 2409 | 4510 |
| DSG--CRT, 1024 bit | 600 | 1089 | 2189 | 4344 |
| DSG--CRT, 2048 bit | 264 | 466 | 931 | 1855 |
| DSV--ME, 512 bit | 887 | 1452 | 2912 | 5802 |
| DSV--ME, 1024 bit | 887 | 1379 | 2763 | 5505 |
| SYI--CRT, 512 bit | 601 | 886 | 1775 | 3545 |
| SYI--CRT, 1024 bit | 488 | 836 | 1673 | 3334 |

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 close to N times the throughput of one PCIXCC card with 7 jobs (as stated above) except for DSG-CRT with 512 bit length which gave the factor of 3.8 for four PCIXCC cards.

PKA RSA Key Generate

The PCIX 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 PCIX Cryptographic Coprocessor.

PCIXCC PKA RSA Key Generation Performance

| PCIXCC PKA RSA Key Generate | Operations/sec |
|-----------------------------|----------------|
| External CRT, 512bit | 3.61 |
| External CRT, 1024bit | 1.76 |
| External CRT, 2048bit | 0.78 |
| Internal ME, 512bit | 4.13 |
| Internal ME, 1024bit | 2.00 |

4.6. 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 z990 the PKD operation will be routed for execution to the PCICA or PCIXCC card, 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 z990 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 cipher except when stated otherwise. This SSL data symmetric key encryption for RC4 and MD5 is executed in SSL software, for TDES (168 bits) and SHA in the CPACF hardware.
- 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.

Legend for all SSL Performance Tables:

Caching Session ID: If the SID is cached the initial handshake process is avoided. If the SID is not cached the initial handshake has to be performed for every new connection between Client and Server.

Handshake: If the Session ID is 100 % cached the initial handshake is always avoided. If the handshake has to be performed the compute intensive PKD operation, then necessary on the server, can be performed in System SSL software or with hardware on a PCICA card or PCIXCC card.

Client Authentication: The authentication of the Client is optional in the SSL protocol.

External Throughput Rate (ETR): Number of handshakes performed per second

Utilization: z990 system utilization (average utilization of the z990 Central Processors)

Cryp.Acc.Card: Cryptographic accelerator cards of a PCICA feature (each PCICA feature contains 2 cryptographic accelerator cards)

4.6.1. 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 performance measurement results clearly suggest using cryptographic hardware (either the PCICA card or PCIXCC card) for improved throughput in the transaction rate if more than a few transactions per second are expected to be handled using an SSL protocol transaction. The measurement results show the throughput with one PCICA card being in the same order of magnitude as with one PCIXCC card in the SSL environment. However, the PCICA feature contains two PCICA cards and the PCIXCC feature contains one PCIXCC card. Also, for the z990 server the maximum number of PCICA features is 6 and the maximum number of PCIXCC features is 4 (the total number of PCICA and PCIXCC features cannot exceed 8 features). Thus for high SSL protocol transaction rate environments the PCICA feature is the preferred selection for a z990 system.

The resource consumption in system processing power for one SSL protocol handshake is in the order of 1/11000 of the system (see table below) in the z/OS environment for a z990 Model 2084-316 (16 Central Processors) with 6 PCICA features (12 cryptographic accelerator cards).

In the z/OS environment the transaction rate of a system z990 Model 2084-316 is expected to be typically in the range from 1500 to 5000 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 z990 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:

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.

4.6.2. SSL Protocol Performance - System SSL

with z/OS V1.4+E / ICSF level WD2 PID

z990 Model 2084-304 (4 Central Processors)

| Caching SID | Handshake | Client Authentic. | ETR | Utilization % |
|-------------|------------------|-------------------|-------|---------------|
| 100% | Avoided | no | 4,200 | 100 |
| no | Software | no | 232 | 100 |
| no | 4 Cryp.Acc.Cards | no | 3,355 | 99.9 |
| no | 4 Cryp.Acc.Cards | yes | 1,895 | 100 |

For all of the above measurements the z990 Model 2084-304 system utilization is 100 percent or is close to 100 percent.

Using the PCICA cryptographic hardware compared to using System SSL Software (second and third line in the above table) produces an increase in throughput (number of SSL protocol handshakes) of 14.4 times.

If Client authentication is required the throughput of the server is considerably reduced.

Z990 Model 2084-304 (4 Central Processors) with PCIXCC Cards (no SID caching)

| # PCIXCC Cards | Cipher Suite | Client Authentic. | ETR | Utilization % |
|----------------|--------------|-------------------|-------|---------------|
| 4 | TDES/SHA | no | 3,143 | 100 |
| 4 | RC4/MD5 | no | 3,330 | 99.9 |
| 4 | RC4/MD5 | yes | 1,703 | 75.1 |

Z990 Model 2084-316 (16 Central Processors)

| Caching SID | Handshake | Client Authentic. | ETR | Utilization % |
|-------------|-------------------|-------------------|--------|---------------|
| 100% | Avoided | no | 13,406 | 100 |
| no | Software | no | 908 | 100 |
| no | 8 Cryp.Acc.Cards | no | 8,791 | 82.6 |
| no | 12 Cryp.Acc.Cards | no | 11,042 | 99.5 |
| no | 4 PCIXCC Cards | no | 4,760 | 39 |

For the above measurements the z990 Model 2084-316 system utilization is 100 percent or close to 100 percent when either software or sufficient hardware is used for the PKD operation. Eight PCICA cryptographic accelerator cards of four PCIXCC cards do not provide enough PKD encryption capacity and thus limit the number of SSL operations at a lower system utilization.

There is a 3.3 time increase in throughput comparing the z990 Model 2084-316 (16 CPs) measurement to the z990 Model 2084-304 (4 CPs) when a sufficient number of PCICA cryptographic hardware is used.

Using the PCICA cryptographic hardware there is a 12.2 fold increase in throughput (number of SSL protocol handshakes) compared to using System SSL Software (second and fourth line in the above table).

4.6.3. SSL Protocol Performance - Linux Open SSL

Remark:

The results of all SSL Protocol performance measurements for Linux native and as Guest under VM are based on z990 GAO level internal code (May 2003) whereas all other measurements are based on z990 GA2 level internal code (October 2003). Measurements for Linux Open SSL for GA2 level are not yet available.

For all Linux Open SSL measurements the following applies:

- Linux System Level: SELLS
- Linux Kernel Level: 2.4.19
- Open SSL Code Level: 0.9.6E
- z900Crypt Level: 1.1.2
- No Client Authentication

Linux Open SSL - Native Measurements

| Caching SID | Handshake | # of CPs | ETR | Utilization % |
|-------------|-------------------|----------|--------|---------------|
| no | Software | 4 | 208 | 99.9 |
| no | 8 Cryp.Acc.Cards | 4 | 6,703 | 99.5 |
| no | 12 Cryp.Acc.Cards | 16 | 13,068 | 55.1 |

For the case

e of z990 Model 2048-304 with 4 Central Processors (CPs) (first two lines in the above table) the processing capability is the limiting factor for the throughput as the utilization is close to 100 percent.

Using the PCICA cryptographic hardware provides an increase in throughput (number of SSL protocol handshakes) of 32.4 times the throughput of using Open SSL Software (first and second line in the above table).

Using the z990 Model 2084-316 with 16 Central Processors (CPs) (third line in the above table) the number of available PCICA cryptographic hardware is the limiting factor for the throughput. However, the number of PCICA features on a z990 system is limited to 6 (each PCICA feature contains 2 cryptographic accelerator cards).

Linux Open SSL as a z/VM Guest

This section contains details of the performance measurement results for Linux Open SSL as a z/VM guest. The number of guests in z/VM is as specified in the table of results.

The z/VM system level used for the measurement is 4.3.0 SLU 0000 or, in one case, 4.3.4 SLU 0000. The SSL level is as specified in the previous section.

All measurements are without Client Authentication.

| z/VM System Level | # of z/VM Guests | Handshake | # of CPs | ETR | Utilization % |
|-------------------|------------------|-------------------|----------|-------|---------------|
| 4.3.0 | 30 | Software | 4 | 197 | 100 |
| 4.3.0 | 1 | 8 Cryp.Acc.Cards | 4 | 851 | 14.9 |
| 4.3.0 | 10 | 8 Cryp.Acc.Cards | 4 | 3,470 | 87.7 |
| 4.3.0 | 30 | 8 Cryp.Acc.Cards | 4 | 3,211 | 98 |
| 4.3.0 | 120 | 12 Cryp.Acc.Cards | 8 | 4,456 | 99.4 |
| 4.4.0 | 120 | 12 Cryp.Acc.Cards | 16 | 7,697 | 92.8 |

Using the PCICA cryptographic hardware provides an increase in throughput (number of SSL protocol handshakes) of 16.6 times that of Open SSL Software (first and fourth line in the above table).

5. January 2005 General Availability Update

With the z990 January 2005 General Availability (z990 GA4), the Cryptographic 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 feature in that it includes 2 coprocessors per feature, thereby increasing the total cryptographic capacity. The cryptographic capacity of z990 GA4 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 z990 Central Processors (CPs) incurs latency and data transmission time. Because of this connection to the z990 CPs, the CEX2C operates asynchronous to the z990 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 990. The internal code level was GA4. The exact model of the z990 system used is stated with each measurement. Most of the measurements were run on a z990 Model 2084-304. 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 z990 Model 2084-301 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 for the cryptographic operations using the cryptographic coprocessor 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 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 Section 4.5.

The data quoted is from test cases run on a z990 Model 2084-304 with either one PCIXCC feature or one CEX2C feature. The number of features active for each test is depicted in the table. 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 performance numbers are from measurements with z/OS V1.6 including ICSF level WD4 PID.

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

| Single DES CBC Encipher (one job) | | | | | |
|-----------------------------------|----------------|------------------|----------------|------------------|--|
| | PCIXCC | | CEX2C | | |
| Data Length (Bytes) | Operations/sec | x10**3 Bytes/sec | Operations/sec | x10**3 Bytes/sec | |
| 64 | 881.1 | 56.4 | 871.6 | 55.8 | |
| 256 | 874.2 | 223.8 | 871.4 | 223.1 | |
| 1024 | 599.6 | 614.0 | 865.6 | 886.4 | |
| 4096 | 450.3 | 1844.4 | 448.9 | 1838.7 | |
| 64K | 39.57 | 2593.3 | 39.23 | 2571.0 | |
| 1M | 2.54 | 2659.2 | 2.51 | 2634.0 | |

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 coprocessor 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 enqueuing 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 coprocessor 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 coprocessor.

| Single DES CBC Encipher (multiple jobs) | | | |
|---|------------------|------------------|--------------|
| | 1 PCIXCC, 7 jobs | 1 CEX2C, 14 jobs | Ratio |
| Data Length (Bytes) | Operations/sec | Operations/sec | CEX2C/PCIXCC |
| 64 | 1352 | 2709 | 2.00 |
| 256 | 1301 | 2532 | 1.95 |
| 1024 | 1078 | 2040 | 1.89 |
| 4096 | 632.8 | 1175 | 1.86 |
| 64K | 51.50 | 95.77 | 1.86 |
| 1M | 3.28 | 6.10 | 1.86 |

The throughput with 1 CEX2C feature containing 2 cryptographic coprocessors is in the order of 1.8 to 2.0 times higher than the throughput with 1 PCIXCC feature containing 1 cryptographic coprocessor when enough parallel jobs are executing to keep the cryptographic coprocessors busy.

The throughput with N coprocessors 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 close to N times the throughput of one coprocessor (as exemplified above).

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

| Triple DES CBC Encipher (one job) | | | | | |
|-----------------------------------|----------------|------------------|----------------|------------------|--|
| | PCIXCC | PCIXCC | CEX2C | CEX2C | |
| Data Length (Bytes) | Operations/sec | x10**3 Bytes/sec | Operations/sec | x10**3 Bytes/sec | |
| 64 | 878.4 | 56.2 | 871.6 | 55.8 | |
| 256 | 603.1 | 154.4 | 871.5 | 223.1 | |
| 1024 | 599.6 | 614.0 | 829.0 | 848.9 | |
| 4096 | 449.7 | 1842.0 | 448.9 | 1838.7 | |
| 64K | 39.58 | 2593.9 | 39.23 | 2571.0 | |
| 1M | 2.54 | 2661.3 | 2.51 | 2634.0 | |

The throughput with one CEX2C feature is in the order of 0.99 times the throughput with one PCIXCC feature when only one job is executing the cryptographic operation. For data lengths of 256 bytes and 1024 bytes, the CEX2C feature exhibits approximately 1.4 times the throughput of the PCIXCC feature.

| Triple DES CBC Encipher (multiple jobs) | | | |
|---|------------------|------------------|--------------|
| | 1 PCIXCC, 7 jobs | 1 CEX2C, 14 jobs | Ratio |
| Data Length (Bytes) | Operations/sec | Operations/sec | CEX2C/PCIXCC |
| 64 | 1297 | 2551 | 1.97 |
| 256 | 1250 | 2365 | 1.89 |
| 1024 | 1028 | 1949 | 1.90 |
| 4096 | 615.9 | 1144 | 1.86 |
| 64K | 50.70 | 94.32 | 1.86 |
| 1M | 3.23 | 6.01 | 1.86 |

The throughput with 1 CEX2C feature containing 2 cryptographic coprocessors is in the order of 1.86 to 1.97 times higher than the throughput with 1 PCIXCC feature containing 1 cryptographic

coprocessor when enough parallel jobs are executing to keep the cryptographic coprocessors busy.

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

| MAC with single DES (one job) | | | | | |
|-------------------------------|----------------|------------------|----------------|------------------|-------|
| | PCIXCC | | CEX2C | | CEX2C |
| Data Length (Bytes) | Operations/sec | x10**3 Bytes/sec | Operations/sec | x10**3 Bytes/sec | |
| 64 | 882.3 | 56.5 | 872.1 | 55.8 | |
| 256 | 882.2 | 225.8 | 872.2 | 223.3 | |
| 1024 | 881.4 | 902.6 | 871.4 | 892.3 | |
| 4096 | 599.2 | 2454.3 | 593.0 | 2428.9 | |
| 64K | 54.22 | 3553.4 | 53.10 | 3480.0 | |
| 1M | 3.51 | 3678.4 | 3.39 | 3554.7 | |

The throughput with one CEX2C feature is in the order of 0.98 times the throughput with one PCIXCC feature when only one job is executing the cryptographic operation.

| MAC with single DES (multiple jobs) | | | | |
|-------------------------------------|------------------|------------------|--------------|--|
| | 1 PCIXCC, 7 jobs | 1 CEX2C, 14 jobs | Ratio | |
| Data Length (Bytes) | Operations/sec | Operations/sec | CEX2C/PCIXCC | |
| 64 | 1491 | 2812 | 1.886 | |
| 256 | 1444 | 2709 | 1.876 | |
| 1024 | 1275 | 2359 | 1.850 | |
| 4096 | 857.6 | 1598 | 1.863 | |
| 64K | 63.38 | 118.10 | 1.863 | |
| 1M | 4.01 | 7.48 | 1.866 | |

The throughput with one CEX2C feature containing two cryptographic coprocessors is in the order of 1.8 times the throughput with one PCIXCC feature containing one cryptographic coprocessor when enough parallel jobs are executing to keep the cryptographic coprocessors busy.

5.2.2 CEX2C Symmetric Key Performance - Diverse Operations

The following table gives the performance in maximum number of operations per second for one CEX2C feature (2 cards) for some selected symmetric key operations.

| CEX2C Symmetric Key Operations - Examples | Ops/s | Ops/s |
|---|-------|---------|
| | 1 job | 14 jobs |
| Key Generate (operational DES KEYGENKY key) | 601 | 1,887 |
| Clear PIN Generate Alternate (DES OPINENC + DES PINGEN keys) | 601 | 1,908 |
| Clear PIN Generate (16 digits) (DES PINGEN key) | 884 | 2,678 |
| Encrypted PIN Translation (DES IPINENC key + DES OPINENC key) | 880 | 2,144 |
| Encrypted PIN Translation (2 UKPT enabled KEYGENKY keys) | 307 | 658 |
| Encryp.PIN Verificat. (UKPT enabl.KEYGENKY+DES PINVER keys) | 453 | 943 |

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 close to N times the throughput of one CEX2C feature with 14 jobs.

5.2.3. PCIACC and CEX2C PKA Performance

The PCIACC 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 WD4 PID invoking the operation via the ICSF API according to the PKCS-1.2. Standard. Measurements were performed on a z990 Model 2084-304.

PCIXCC and CEX2C PKA Performance

| PCIXCC and CEX2C on z/OS V1.6 (ICSF level: WD4 PID) | | | |
|--|----------------|----------------|--------------|
| Public Key Decrypt (PKD), Public Key Encrypt (PKE) | | | |
| Digital Signature Generate (DSG), Digital Sign. Verify (DSV) | | | |
| Symmetric Key Import (encrypted with RSA key) (SYI) | | | |
| | 2084-304 | 2084-304 | |
| Crypto Feature | PCIXCC | CEX2C | Ratio |
| Jobs | 1 | 1 | CEX2C/PCIXCC |
| | Operations/sec | Operations/sec | |
| PKD--CRT, 512 bit | 868 | 863 | 0.99 |
| PKD--CRT, 1024 bit | 596 | 590 | 0.99 |
| PKD--CRT, 2048 bit | 263 | 261 | 0.99 |
| PKD--ME, 512 bit | 596 | 590 | 0.99 |
| PKD--ME, 1024 bit | 452 | 448 | 0.99 |
| PKE, 512 bit | 876 | 866 | 0.99 |
| PKE, 1024 bit | 611 | 864 | 1.41 |
| PKE, 2048 bit | 597 | 591 | 0.99 |
| DSG--CRT, 512 bit | 749 | 857 | 1.14 |
| DSG--CRT, 1024 bit | 596 | 590 | 0.99 |
| DSG--CRT, 2048 bit | 263 | 261 | 0.99 |
| DSV--ME, 512 bit | 880 | 870 | 0.99 |
| DSV--ME, 1024 bit | 880 | 870 | 0.99 |
| SYI--CRT, 512 bit | 596 | 590 | 0.99 |
| SYI--CRT, 1024 bit | 483 | 581 | 1.20 |

With only one job executing, CEX2C throughput was 0.99% of PCIXCC throughput for most operations. There were three exceptions: PKE 1024 bit, DSG-CRT 512 bit, and SYI-CRT 1024 bit, where CEX2C throughput was significantly higher than PCIXCC.

Throughput with one CEX2C feature (2 coprocessors) was in the range of 1.83 times to 2.0 times the throughput with one PCIXCC feature.

Throughput with two CEX2C features (4 coprocessors) was twice that of one CEX2C feature.

The PKA cryptographic operation throughput with N CEX2C cards with a sufficient number of jobs repetitively requesting the same cryptographic operation for the examples in the table above is close to N times the throughput of one PCIXCC card with 14 jobs (as stated above).

PKA RSA Key Generate

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 or one CEX2C feature.

PCIXCC and CEX2C PKA RSA Key Generation Performance

| PCIXCC PKA RSA Key Generate on z/OS V1.6 (ICSF level: WD4 PID) | | | |
|--|----------------|----------------|----------------|
| PCIXCC and CEX2C PKA RSA Key Generate | | | |
| Crypto Feature | PCIXCC | CEX2C | CEX2C |
| Jobs | 1 | 1 | 2 |
| | Operations/sec | Operations/sec | Operations/sec |
| External CRT, 512bit | 3.50 | 3.28 | 5.73 |
| External CRT, 1024bit | 1.74 | 1.59 | 2.80 |
| External CRT, 2048bit | 0.69 | 0.63 | 1.09 |
| Internal ME, 512bit | 4.13 | 3.93 | 6.82 |
| Internal ME, 1024bit | 2.00 | 1.86 | 3.38 |

Key Generate performance with one job executing with one CEX2C feature (2 coprocessors) is in the range of 5% to 8% lower than with one PCIXCC feature. When both of the coprocessors available in the CEX2C feature are used, throughput is in the range of 59% to 69% higher than 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 z990 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 z990 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 cipher except when stated otherwise. This SSL data symmetric key

encryption for RC4 and MD5 is executed in SSL software. The SSL data symmetric key encryption for TDES (168 bits) and SHA is executed in the CPACF hardware.

- 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.

Legend for all SSL Performance Tables:

Caching Session ID: If the SID is cached the initial handshake process is avoided. If the SID is not cached the initial handshake has to be performed for every new connection between Client and Server.

Handshake: If the Session ID is 100 % cached the initial handshake is always avoided. If the handshake has to be performed the compute intensive PKD operation, then necessary on the server, can be performed in System SSL software or with hardware on a CEX2C card or PCIXCC card.

Client Authentication: The authentication of the Client is optional in the SSL protocol.

External Throughput Rate (ETR): Number of handshakes performed per second

Utilization: z990 system utilization (average utilization of the z990 Central Processors)

Crypto Card: Cryptographic cards of a CEX2C feature (each CEX2C feature contains 2 cryptographic cards), or PCIXCC feature (each PCIXCC feature contains 1 cryptographic card).

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 by an SSL protocol for the communication between Client and Server.

The performance measurement results clearly suggest using cryptographic hardware (either the CEX2C feature or PCIXCC feature) for improved throughput in the transaction rate if more than a few transactions per second are expected to be handled using an SSL protocol transaction. The measurement results show the throughput with one CEX2C feature (2 coprocessors) being in the same order of magnitude as with one PCIXCC feature (1 coprocessor) in the SSL environment. Also, for the z990 server the maximum number of PCIXCC features is 4 (for a total of 4 PCIX coprocessors) and the maximum number of CEX2C features is 8 (for a total of 16 CEX2C coprocessors). Thus for high SSL protocol transaction rate environments the CEX2C feature is the preferred selection for a z990 system.

The resource consumption in system processing power for one SSL protocol handshake is in the order of 1/3200 of the system (see table below) in the z/OS environment for a z990 Model 2084-304 (4 Central Processors) with 2 CEX2C features (4 cryptographic coprocessors).

In the z/OS environment the transaction rate of a system z990 Model 2084-316 is expected to be typically in the range from 1500 to 5000 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 z990 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:

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 WD4 PID

z990 Model 2084-304 (4 Central Processors)

| Caching SID | Handshake | Cipher | ETR | CPU Util. % | Crypto Util. % |
|-------------|----------------|----------|-------|-------------|----------------|
| 100% | Avoided | RC4,MD5 | 5,303 | 96.61 | NA |
| no | Software | RC4,MD5 | 283 | 100 | NA |
| no | 4 PCIXCC Feat. | RC4,MD5 | 3,960 | 95.58 | 91.07 |
| no | 2 CEX2C Feat. | RC4,MD5 | 4,035 | 98.70 | 97.45 |
| no | 4 PCIXCC Feat. | TDES,SHA | 4,519 | 94.16 | 98.12 |
| no | 2 CEX2C Feat. | TDES,SHA | 4,012 | 85.01 | 97.42 |
| no | 4 CEX2C Feat. | TDES,SHA | 4,995 | 98.29 | 67.94 |

With 100% Session ID Caching (first row of the above table), an SSL handshake is performed during each client’s first transaction. The unique Session ID established for each client during the handshake is cached and re-used for each subsequent transaction, thus handshake processing is avoided.

When Session IDs are not cached (second through sixth rows of the above table), a full SSL handshake is performed for every transaction.

Using the CEX2C cryptographic hardware compared to using System SSL Software produces an increase in throughput (number of SSL protocol handshakes) of 14.4 times (second and fourth rows in the above table).

Throughput with the RC4,MD5 cipher was similar with either CEX2C or PCIX cryptographic coprocessors (third and fourth rows in the above table).

Throughput with TDES,SHA cipher and 2 CEX2C features (4 CEX2C coprocessors) was about 11% lower than with 4 PCIXCC features (4 PCIXCC coprocessors) (fifth and sixth rows in the above table). Throughput for both of these measurements was limited by near 100% utilization of the cryptographic hardware available. The 2 CEX2C features became limited at a lower

© 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.