



**IBM System z9 Business Class  
Performance of Cryptographic  
Operations  
(Cryptographic Hardware: CPACF,  
CEX2C, CEX2A)**

## Table of Contents

<b>Preface</b> .....	Page 2
<b>1. Introduction</b> .....	Page 2
<b>2. Cryptographic Hardware supported on z9 BC</b> .....	Page 3
2.1. <i>CP Assist for Cryptographic Function (CPACF)</i> .....	Page 3
2.2. <i>Crypto Express2 (CEX2) Feature</i> .....	Page 3
2.3. <i>Crypto Express2-1P (CEX2-1P) Feature</i> .....	Page 5
<b>3. Exploitation of Cryptographic Hardware in z9 BC</b> .....	Page 5
3.1. <i>SSL Protocol based Communication</i> .....	Page 6
<b>4. Performance Information</b> .....	Page 7
4.1. <i>Definitions</i> .....	Page 7
4.2. <i>CP Assist for Cryptographic Function (CPACF)</i> .....	Page 8
4.2.1. CP Assist for Cryptographic Function (CPACF) Performance - Architecture Instruction Interface ('Native') .....	Page 8
4.2.2. CP Assist for Cryptographic Function (CPACF) Performance - ICSF API Interface .....	Page 11
4.3. <i>Symmetric Key Advanced Encryption Standard (AES) Performance - ICSF API Interface</i> .....	Page 14
4.4. <i>Crypto Express2 Performance</i> .....	Page 16
4.4.1. CEX2 Coprocessor Multiple Data Symmetric Key Performance .....	Page 16
4.4.2. CEX2 Coprocessor Symmetric Key Performance - Diverse Operations .....	Page 19
4.4.3. CEX2 Coprocessor PKA Performance .....	Page 20
4.4.4. CEX2 Accelerator Performance .....	Page 22
4.5. <i>SSL Protocol Handshake Performance</i> .....	Page 24
4.5.1. Applicability of SSL Performance Results to a Customer Environment .....	Page 25
4.5.2. SSL Protocol Performance - System SSL with z/OS V1.7 / Enhancements to Cryptographic Support for z/OS and z/OS.e V1R6/R7 (ICSF) .....	Page 26
<b>5. May 2007 Performance Update for CEX2-1P</b> .....	Page 26
5.1. <i>CEX2-1P Coprocessor Multiple Data Symmetric Key Performance</i> .....	Page 27
5.2. <i>CEX2-1P Coprocessor Symmetric Key Performance - Diverse Operations</i> .....	Page 30
5.3. <i>CEX2-1P Coprocessor PKA Performance</i> .....	Page 30
5.4. <i>CEX2-1P Accelerator Performance</i> .....	Page 32
5.5. <i>SSL Protocol Handshake Performance</i> .....	Page 34
5.5.1. <i>Applicability of SSL Performance Results to a Customer Environment</i> .....	Page 35
5.5.2. SSL Protocol Performance - System SSL with z/OS V1.8 / z/OS Integrated Cryptographic Service Facility (ICSF) .....	Page 36
5.5.3. SSL Protocol Performance - Linux Open SSL .....	Page 36

## Preface

The performance information presented in this publication was measured on IBM System z9™ Business Class (z9 BC) 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 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 is adequate or can 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 System z9 BC systems. The z9 BC supports the following cryptographic hardware features:

1. *CP Assist for Cryptographic Function (CPACF).*
2. *Crypto Express2 (CEX2) feature.*
3. *Crypto Express2-1P (CEX2-1P) feature.*

The CP Assist for Cryptographic Function delivers cryptographic support on every Central Processor (CP) with Data Encryption Standard (DES), Triple DES (TDES), and Advanced Encryption Standard (AES)-128 bit data encryption/decryption, as well as Secure Hash Algorithm (SHA-1) and SHA-256 hashing.

The Crypto Express2 (CEX2) feature combines the functions of Coprocessor (for secure key encrypted transactions) and Accelerator (for Secure Sockets Layer [SSL] acceleration) modes in a single optional feature with two PCI-X adapters. New on System z9, using the HMC console, the PCI-X adapters can be customized as having either two Coprocessors, two Accelerators or one of each. The Crypto Express2 is a follow-on to the PCIXCC and PCICA features. All of the analogous PCIXCC and PCICA functions are implemented in the Crypto Express2 with equivalent or greater performance.

Introduced in May 2007, the Crypto Express2-1P (CEX2-1P) feature provides the same functions as the CEX2, but contains only one PCI-X adapter. The PCI-X adapter can be configured as a Coprocessor or Accelerator. May 2007 Performance Update for CEX2-1P was added to this document to provide the performance characteristics of CEX2-1P. All other performance information contained in this document remains unchanged from the original publication.

## **2. Cryptographic Hardware supported on z9 BC**

### *2.1. CP Assist for Cryptographic Function (CPACF)*

The z9 BC supports the Message Security Assist (MSA) Architecture along with the CP Assist for Cryptographic Function (CPACF). The CP Assist for Cryptographic Function delivers cryptographic support on every Central Processor (CP) with Data Encryption Standard (DES), Triple DES (TDES), and Advanced Encryption Standard (AES) data encryption/decryption, as well as SHA-1 and SHA-256 hashing. As these cryptographic functions are implemented in each CP the potential throughput scales with the number of CPs in the system.

The DES, TDES and AES-128 functions of the CPACF use clear key values. The SHA-1 and SHA-256 hash functions are shipped enabled. The DES, TDES and AES functions require enablement of the CPACF for export control. The CPACF for DES, TDES, AES, SHA-1, and SHA-256 functions can be invoked by problem state instructions defined by an extension of the z9 architecture. Support is also available via Enhancements to Cryptographic Support for z/OS<sup>®</sup> and z/OS.e V1R6/R7 (ICSF) in z/OS.

The hardware of the CPACF that performs the symmetric key operations (DES; TDES; AES-128) and SHA 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. Crypto Express2 (CEX2) Feature*

The Crypto Express2 (CEX2) feature combines the functions of Coprocessor (for secure key encrypted transactions) and Accelerator (for SSL acceleration) modes in a single optional feature with two PCI-X adapters. New on System z9, using the HMC console, the PCI-X adapters can be customized as having either two Coprocessors, two Accelerators or one of each. The Crypto Express2 is a follow on to the PCIXCC and PCICA features previously available on

IBM eServer™ zSeries® 900 (z900) and IBM eServer zSeries 990 (z990) systems. All of the analogous PCIXCC and PCICA functions are implemented in the Crypto Express2 with equivalent or greater performance.

There can be a maximum of 8 CEX2 features in a z9 BC system for a total of 16 PCI-X adapters.

When configured in Coprocessor mode, the CEX2 feature supports:

- *Cryptographic functions*
- *Use of encrypted key values*
- *Clear key and encrypted PKA operations*
- *User defined Extensions (UDX)*

The CEX2 in Coprocessor mode provides a security-rich cryptographic subsystem. The tamper-responding hardware has been certified at the highest level under the FIPS 140-2 standard, Level 4. Specialized hardware performs DES, TDES, RSA, and SHA-1 cryptographic operations in a security-rich environment. The CEX2 Coprocessor is designed to protect the cryptographic keys and sensitive custom applications. Security relevant cryptographic keys are encrypted under the Master Key when outside the secure boundary of the CEX2 card. The Master Keys are always kept in battery backed-up memory within the tamper-protected boundary of the CEX2 Coprocessor, and are destroyed if the hardware module detects an attempt to penetrate it.

The CEX2 Coprocessor also supports the ‘clear key’ PKA operations that currently are often used to provide SSL protocol communications.

When configured in Accelerator mode, the CEX2 feature provides 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 Central Processor (CP) to the CEX2 Accelerator, potentially increasing system throughput. The CEX2 in Accelerator mode works in ‘clear key’ mode only.

The operations in the CEX2 are controlled by an on-board microprocessor with memory to hold the controlling program. A security-rich code-loading process enables control program and application program loading into the CEX2. The control program together with the application program provides for the IBM Common Cryptographic Architecture (CCA) interface for the applications using the CEX2 feature.

The Crypto Express2 executes its cryptographic operations asynchronously to a CP operation in the z9 BC system. A CP requesting a cryptographic operation from the CEX2 uses the

message queuing protocol to communicate with the CEX2. After enqueueing a request to the CEX2, the host operating system will dispense the task that has enqueue the cryptographic operation and dispatches another task. Thus, processing of the cryptographic operation in the CEX2 will work in parallel to other tasks being executed in a z9 BC CP. A special CP task will poll at fixed time intervals for finished operations of the Cryptographic Express2, dequeue them, and execute the Release function to cause the redispach of the application waiting for the result of the cryptographic operation. For each PCI-X adapter in the CEX2, 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, several operations can be worked on in parallel.

For z9 BC systems, the Crypto Express2 feature works with Enhancements to Cryptographic Support for z/OS and z/OS.e 1.6/1.7 (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) interface.

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

### *2.3. Crypto Express2-1P (CEX2-1P) Feature*

Introduced in May 2007, the Crypto Express2-1P (CEX2-1P) feature provides the same functions as the CEX2, but contains only one PCI-X adapter. The PCI-X adapter can be configured as a Coprocessor or Accelerator.

## **3. Exploitation of Cryptographic Hardware in z9 BC**

In the cryptographic application environment it is not unusual that an application will not have direct access to the cryptographic hardware. Instead, the application requiring a cryptographic service will call an Application Programming Interface (API) which is interpreted by some services of the System Control Program.

In the z9 BC using the z/OS System Control Program, most cryptographic hardware can only be used through Enhancements to Cryptographic Support for z/OS and z/OS.e 1.6/1.7 (ICSF). ICSF is a standard component of z/OS. It provides cryptographic services in the z/OS environment. ICSF provides the 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 available to ICSF. 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 was designed to facilitate 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/Internet 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 z9 BC 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 an increase in transaction execution time compared to an unsecure protocol. Some factors contributing to the increase are 1) CP path length (due to the protocol itself and due to operating system support); 2) the symmetric key operation's execution time (either hardware assisted or in software executed on a CP); and 3) 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 z9 BC can provide as a server within the given system constraints and assess the utilization of the measured system, assuming no other work is executing.

The intent for providing capacity information in the SSL environment is to demonstrate the capabilities of a z9 BC system to act as a Web Server providing SSL-compliant 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 and Linux<sup>®</sup> for IBM eServer zSeries environments.

As this performance publication primarily deals with performance of cryptographic operations and Web based communication, the measurements for the SSL environment 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 7 (z/OS 1.7) and Enhancements to Cryptographic Support for z/OS and z/OS.e 1.6/1.7 (ICSF), except when stated otherwise.

All measurements were performed on an IBM System z9 BC. The exact model of the z9 BC system used is stated with each measurement. Most of the measurements were run on a z9 BC Model S04 with 4 Central Processors. (Details of the configuration are available on request.) If, however, the measurement invokes only one single job the performance behavior is the same as if this measurement were run on a z9 BC Model S04 with 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 are presented for only a subset of the cryptographic operations supported by System z9 BC. Measurements for many other operations have been made, and in some cases a statement is included comparing the results of these operations to those presented in the tables. Unless otherwise stated, the tables contain results of measurements using only one PCI-X card in a CEX2 feature. In many cases, measurements were also taken with multiple cryptographic features available. Results with multiple cryptographic features are not presented in the tables, however, 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 System z9 Assembler Language issuing the System z9 Message Security Assist (MSA) Architecture cryptographic operation instructions as indicated with each group.

The data quoted was from test cases run on a z9 BC Model S04, however, using only one of the CPs. Measurements were also taken with multiple jobs using up to 4 CPs (not shown). For each cryptographic operation type quoted, there is a statement on scalability of the results if up to 4 CPs (the maximum for System z9 BC) are being used.

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)**

(System z9 Message Security Assist Architecture instruction: KMC-DEA)

Native: Single DES CBC Encipher (KMC-DEA)		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	3978560	254.6
256	1756920	449.8
1024	525822	538.4
4096	140581	575.8
64K	8754	573.7
1M	536.9	563.0

The KMC-DEA operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 1 percent (with 4 CPs).

DEA Cipher Block Chaining Decipher (CBC) with Single Length Key has similar performance characteristics to the Encipher operation.

DEA Electronic Code Book Encipher (ECB, without chaining) with Single Length Key has similar performance characteristics as the corresponding CBC Encipher operation (increase for small data length up to 14 percent, for larger data length less than 1 percent).

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

(System z9 Message Security Assist Architecture instruction: KMC-TDEA)

Native: Triple DES CBC Encipher (KMC-TDEA)		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	2362248	151.1
256	722674	185.0
1024	194550	199.2
4096	49388	202.3
64K	3069	201.2
1M	190.4	199.7

The KMC-TDEA operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 1 percent (with 4 CPs).

DEA Cipher Block Chaining Decipher with Triple Length Key has similar performance characteristics to the Encipher operation.

**AES Cipher Block Chaining Encipher with Single Length Key (128 Bits)**

(System z9 Message Security Assist Architecture instruction: KMC-AES)

Native: AES CBC Encipher (KMC-AES)		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	2806742	179.6
256	948926	242.9
1024	258402	264.6
4096	66092	270.7
64K	4106	269.1
1M	254.4	266.8

The KMC-AES operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 1 percent (with 4 CPs).

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

(System z9 Message Security Assist Architecture instruction: KMAC-DEA)

Native: MAC with single DES (KMAC-DEA)		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	5641447	361.1
256	1993068	510.2
1024	552241	565.5
4096	142199	582.4
64K	8877	581.8
1M	547.7	574.4

The KMAC-DEA operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 1 percent (with 4 CPs).

**Compute Message Digest SHA-1**

(System z9 Message Security Assist Architecture instruction: KLMD-SHA-1)

Native: SHA-1(KLMD-SHA-1)		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	2526807	161.7
256	1294635	331.4
1024	440435	451.0
4096	120246	492.5
64K	7630	500.1
1M	471.4	494.4

The KLMD-SHA-1 operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 1 percent (with 4 CPs).

## Compute Message Digest SHA-256

(System z9 Message Security Assist Architecture instruction: KLMD-SHA-256)

Native: SHA-256(KLMD-SHA-256)		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	1930146	123.5
256	901712	230.8
1024	289203	296.1
4096	78207	320.3
64K	4964	325.3
1M	307.6	322.6

The KLMD-SHA-256 operation scales with the number of CPs executing multiple jobs with the same operation. The reduction is less than 1 percent (with 4 CPs).

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

All test cases are written in System z9 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 System z9 Message Security Assist (MSA) Architecture as indicated with each group.

The data quoted was from test cases run on a z9 BC Model S04, however, using only one of the CPs. Measurements were also taken with multiple jobs using up to 4 CPs (not shown). For each cryptographic operation type quoted there is a statement on scalability of the results if 4 CPs (the maximum for System z9 BC) are being used.

As the performance measurement results show, all ICSF API interface test cases have 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 and the throughput is similar to the 'Native' test cases for large data lengths.

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

(System z9 Message Security Assist Architecture instruction: KMC-DEA)

ICSF API: Single DES CBC Encipher (KMC-DEA) 1 job		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	85464.0	5.47
256	82970.0	21.24
1024	74909.0	76.71
4096	53660.0	219.79
64K	7869.0	515.73
1M	532.4	558.29

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 11 % for 4 CPs and 64 byte data length and decreases for higher data lengths.

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**

(System z9 Message Security Assist Architecture instruction: KMC-TDEA)

ICSF API: Triple DES CBC Encipher (KMC-TDEA) 1 job		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	83781.0	5.36
256	77489.0	19.84
1024	60007.0	61.45
4096	31415.0	128.68
64K	2952.0	195.83
1M	189.5	198.76

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 11 % for 4 CPs and 64 byte data length and decreases for higher data lengths.

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

**Compute Message Digest SHA-1 - ICSF API**

(System z9 Message Security Assist Architecture instruction: KLMD-SHA-1)

ICSF API: SHA-1(KLMD-SHA-1) 1 job		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	66761.0	4.27
256	65136.0	16.67
1024	59134.0	60.55
4096	43570.0	178.47
64K	6829.0	447.61
1M	467.2	489.90

The Compute message Digest SHA-1 operation scales with the number of CPs (up to the maximum of 4 CPs in the z9 BC) executing multiple jobs with the same operation. The reduction is less than 12 % for 4 CPs and 64 byte data length and decreases for higher data lengths.

**Compute Message Digest SHA-256 - ICSF API**

(System z9 Message Security Assist Architecture instruction: KLMD-SHA-2)

ICSF API: SHA-256(KLMD-SHA-256)		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	65825.0	4.21
256	63277.0	16.20
1024	55170.0	56.49
4096	36342.0	148.86
64K	4602.0	301.60
1M	305.4	320.28

The Compute message Digest SHA-2 operation scales with the number of CPs (up to the maximum of 4 CPs in the z9 BC) executing multiple jobs with the same operation. The reduction is less than 12 % for 4 CPs and 64 byte data length and decreases for higher data lengths.

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

With System z9, AES-128 encryption services are provided in the CPACF. IBM continues to provide AES-256 encryption services in the z/OS environment as API calls to ICSF software routines.

The data quoted was from test cases run on a z9 BC Model S04, however, using only one of the CPs. Measurements were also taken with multiple jobs using up to 4 CPs (not shown). For each cryptographic operation type quoted there is a statement on scalability of the results if up to 4 CPs are being used.

All measurements were performed with z/OS V1.7 and Enhancements to Cryptographic Support for z/OS and z/OS.e V1R6/R7 (ICSF).

**AES128 Encipher (128 bit Key Length) - ICSF API (CPACF)**

AES128 Encipher (128 bit key) 1 job		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	82947.0	5.31
256	77953.0	19.96
1024	64125.0	65.66
4096	37152.0	152.18
64K	3896.0	255.37
1M	253.1	265.40

The AES128 Encipher operation scales with the number of CPs (up to the maximum of 4 CPs in the z9 BC) executing multiple jobs with the same operation. The reduction is approximately 11% for 4 CPs and 64 byte data length and decreases for higher data lengths.

**AES128 Decipher (128 bit Key Length) - ICSF API (CPACF)**

AES128 Decipher (128 bit key) 1 job		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	82486.0	5.28
256	77786.0	19.91
1024	63895.0	65.43
4096	37099.0	151.96
64K	3893.0	255.15
1M	253.1	265.42

The AES128 Decipher operation scales with the number of CPs (up to the maximum of 4 CPs in the z9 BC) executing multiple jobs with the same operation. The reduction is approximately 11% for 4 CPs and 64 byte data length and decreases for higher data lengths.

**AES256 Encipher (256 bit Key Length) - ICSF API (Software)**

AES256 Encipher (256 bit key) in software		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	70667.0	4.52
256	51132.0	13.09
1024	23995.0	24.57
4096	7686.0	31.48
64K	522.6	34.25
1M	32.8	34.38

The AES256 Encipher operation scales with the number of CPs (up to the maximum of 4 CPs in the z9 BC) executing multiple jobs with the same operation. The reduction is approximately 8% for 4 CPs and 64 byte data length and decreases for higher data lengths.

**AES256 Decipher (256 bit Key Length) - ICSF API (Software)**

AES256 Decipher (256 bit key) in software		
Data Length (Bytes)	Operations/sec	x10**6 Bytes/sec
64	62894.0	4.03
256	45692.0	11.70
1024	21576.0	22.09
4096	6936.0	28.41
64K	473.2	31.02
1M	29.7	31.13

The AES256 Decipher operation scales with the number of CPs (up to the maximum of 4 CPs in the z9 BC) executing multiple jobs with the same operation. The reduction is approximately 7% for 4 CPs and 64 byte data length and decreases for higher data lengths.

## *4.4. Crypto Express2 Performance*

The Crypto Express2 feature is designed to address high-end server security requirements. The Crypto Express2 feature, with two PCI-X adapters, is configurable and can be defined for secure key encrypted transactions (Coprocessor – the default) or SSL acceleration (Accelerator). Crypto Express2 executes the functions that were previously offered by the PCICA and PCIXCC features, performing hardware acceleration for SSL transactions and clear key RSA operations. Like its predecessors, the Crypto Express2 feature has been designed to address the security requirements of an enterprise server. The PCIXCC, PCICC, and PCICA features are not supported on z9 BC.

When configured as a Coprocessor, the PCI-X adapter is designed to provide security-rich cryptographic operations to be used by System z9 host application programs. The Coprocessor mode offers security features for symmetric key and public key operations. In this case the cryptographic keys are encrypted under the corresponding Master Keys when outside the secure boundary of the PCI-X adapter.

When configured as an Accelerator, the PCI-X adapter is designed to provide high speed acceleration of RSA operations in ‘clear key’ mode, providing security rich communication for Web site-based applications which utilize the SSL or TLS protocol. Some implementers execute the public key operation, incurred during set up of an SSL session, in ‘clear key’ mode.

The connection of the CEX2 feature via the PCI-X bus to the z9 BC Central Processors (CPs) incurs latency and data transmission time. Because of this connection to the z9 BC CPs, the CEX2 operates asynchronous to the z9 BC CPs.

There can be a maximum of 8 CEX2 features in a z9 BC system, each CEX2 feature containing two PCI-X adapters.

### *4.4.1. CEX2 Coprocessor Multiple Data Symmetric Key Performance*

This chapter deals with CEX2 Coprocessor cryptographic operations with a user supplied length of data as, e.g., DES operations.

All test cases are written in System z9 Assembler Language issuing an API call to ICSF for the cryptographic operation. ICSF will resolve the API call and handle the communication with the CEX2 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 PCI-X adapter.

The throughput for the cryptographic operations using the CEX2 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 CEX2 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 z9 BC Model S04 using 1 job that performs the cryptographic operation. Measurements were also taken with multiple jobs using up to 4 CPs. Results with multiple jobs are not always included in tables, however, for each cryptographic operation type quoted there is a statement on scalability of the results if multiple jobs are 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 1.7 including Enhancements to Cryptographic Support for z/OS and z/OS.e 1.6/1.7 (ICSF).

**CEX2 Coprocessor DEA Cipher Block Chaining Encipher with Single Length Key (56 Bits)**

CEX2C (one job): Single DES CBC Encipher			
Data Length (Bytes)	Operations/sec	x10**3 Bytes/sec	
64	908.60	58.15	
256	908.20	232.5	
1024	899.40	921.0	
4096	612.10	2507.2	
64K	60.77	3982.7	
1M	3.94	4130.1	

The above table provides measurement results for an environment where one job was continuously executing the cryptographic operation using one CEX2 Coprocessor card. As mentioned, the execution of the cryptographic operation in the CEX2 Coprocessor card is asynchronous to the z9 BC 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 CEX2 Coprocessor adapter'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 CEX2 Coprocessor adapter 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 CEX2 Coprocessor.

CEX2C (seven jobs): Single DES CBC Encipher		
Data Length (Bytes)	Operations/sec	x10**3 Bytes/sec
64	1388.0	88.85
256	1293.0	331.1
1024	1043.0	1068.7
4096	812.1	3326.5
64K	78.31	5132.1
1M	5.06	5306.5

The throughput with 4 CEX2 Coprocessor adapters 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 4 times the throughput of one CEX2 Coprocessor adapter with 7 jobs (as exemplified above).

#### **CEX2 Coprocessor DEA Cipher Block Chaining Encipher with Triple Length Key (168 Bits)**

CEX2C (one job): Triple DES CBC Encipher		
Data Length (Bytes)	Operations/sec	x10**3 Bytes/sec
64	908.7	58.16
256	908.6	232.6
1024	624.4	639.4
4096	610.9	2502.3
64K	55.73	3652.7
1M	3.59	3759.7

The throughput for seven jobs for CEX2 Coprocessor TDES is approximately 1.2 times to 1.6 times higher than for one job.

CEX2 Coprocessor Message Authentication Code with DEA Single Length Key (56 Bits)

CEX2C (one job): MAC with single DES		
Data Length (Bytes)	Operations/sec	x10**3 Bytes/sec
64	909.2	58.19
256	909.4	232.8
1024	907.9	929.8
4096	899.8	3685.9
64K	86.23	5651.4
1M	5.85	6129.0

The throughput for seven jobs for CEX2 Coprocessor MAC is approximately 1.2 to 1.5 times higher than for one job, the lower number applying to large data length and the higher to small data lengths.

4.4.2. CEX2 Coprocessor Symmetric Key Performance - Diverse Operations

The following table gives the performance in maximum number of operations per second for each of the two PCI-X cards in a CEX2 feature for some selected symmetric key operations.

The following table gives the performance in maximum number of operations per second for each of the two PCI-X cards in a CEX2 feature for some selected symmetric key operations.

CEX2 Coprocessor Symmetric Key Operations - Examples	Ops/s	Ops/s
	1 job	7 jobs
Key Generate (operational DES KEYGENKY key)	617	932
Clear PIN Generate Alternate (DES OPINENC + DES PINGEN keys)	671	990
Clear PIN Generate (16 digits) ( DES PINGEN key)	910	1,394
Encrypted PIN Translation (DES IPINENC key + DES OPINENC key)	909	1,101
Encrypted PIN Translation (2 UKPT enabled KEYGENKY keys)	313	332
Encryp.PIN Verificat. (UKPT enabl.KEYGENKY+DES PINVER keys)	458	483

The throughput with 4 CEX2 Coprocessor adapters with a sufficient number of jobs repetitively requesting the same cryptographic operation for the examples in the table above is close to 4 times the throughput of one CEX2 Coprocessor adapter with 7 jobs.

### 4.4.3. CEX2 Coprocessor PKA Performance

The CEX2 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 lengths 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 (DSC) and the Symmetric Key Import (SYI) cryptographic operations the PKA private keys (signature key or encryption key) are encrypted under the corresponding master key.

The performance numbers are from measurements with z/OS 1.7 including Enhancements to Cryptographic Support for z/OS and z/OS.e 1.6/1.7 (ICSF) invoking the operation via the ICSF API according to the PKCS-1.2. standard. Measurements were performed on a z9 BC Model S04 with 4 CPs.

**CEX2 Coprocessor PKA Performance**

<b>CEX2C on z/OS V1.7 (ICSF level: WD#6)</b>				
Public Key Decrypt (PKD), Public Key Encrypt (PKE)				
Digital Signature Generate (DSG), Digital Sign. Verify (DSV)				
Symmetric Key Import (encrypted with RSA key) (SYI)				
	2096-S04	2096-S04	2096-S04	2096-S04
CEX2C	1	1	2	4
Jobs	1	7	14	28
	Operations/sec	Operations/sec	Operations/sec	Operations/sec
PKD--CRT, 512 bit	878	1104	2202	4413
PKD--CRT, 1024 bit	611	996	1990	3975
PKD--CRT, 2048 bit	268	466	931	1860
PKD--ME, 512 bit	612	1082	2165	4344
PKD--ME, 1024 bit	463	925	1847	3688
PKE, 512 bit	901	1214	2422	4840
PKE, 1024 bit	854	991	1986	4012
PKE, 2048 bit	612	769	1534	3078
DSG--CRT, 512 bit	865	1115	2233	4329
DSG--CRT, 1024 bit	612	997	2000	4034
DSG--CRT, 2048 bit	268	466	932	1860
DSV--ME, 512 bit	906	1349	2695	5396
DSV--ME, 1024 bit	906	1256	2513	5071
SYI--CRT, 512 bit	612	842	1681	3362
SYI--CRT, 1024 bit	473	795	1588	3178

The PKA cryptographic operation throughput with 4 CEX2 Coprocessor adapters with a sufficient number of jobs repetitively requesting the same cryptographic operation for the examples in the table above is close to 4 times the throughput of one CEX2 Coprocessor adapter with 7 jobs (as stated above) except for DSG-CRT with 512 bit length which gave the factor of 3.8 for four CEX2 Coprocessor adapters.

#### PKA RSA Key Generate

The CEX2 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 CEX2 Coprocessor.

#### **CEX2 Coprocessor PKA RSA Key Generation Performance**

CEX2C PKA RSA Key Generate	
	Operations/sec
External CRT, 512bit	3.39
External CRT, 1024bit	1.64
External CRT, 2048bit	0.61
Internal ME, 512bit	3.93
Internal ME, 1024bit	1.95

#### 4.4.4 CEX2 Accelerator Performance

The CEX2 Accelerator configuration mode is designed to offer fast Public Key Algorithm (PKA) cryptographic 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 V1.7 including Enhancements to Cryptographic Support for z/OS and z/OS.e 1.6/1.7 (ICSF) 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)

**CEX2 Accelerator PKA Performance**

<b>CEX2A Public Key Decrypt (PKD) and Public Key Encrypt (PKE) (z/OS V1.7 ,ICSF: WD#6)</b>			
2096 CPs	4	4	4
CEX2A Adapters	1	1	4
Jobs	1	8	32
	Operations/sec	Operations/sec	Operations/sec
PKD--CRT, 512 bit	1713	10216	38107
PKD--CRT, 1024 bit	1708	3334	12723
PKD--CRT, 2048 bit	374	456	1821
PKD--ME, 512 bit	1715	3369	12417
PKD--ME, 1024 bit	614	920	3673
PKE, 512 bit	1740	13262	49254
PKE, 1024 bit	1740	13262	49368
PKE, 2048 bit	1737	11660	41726

The first result column of the above table is for measurements where one job was continuously executing the cryptographic operation using one CEX2 Accelerator card. As mentioned, the execution of the cryptographic operation in the CEX2 Accelerator is asynchronous to the z9 BC 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 CEX2 Accelerator card. The increased throughput is due to the fact that tasks are always available for execution in the CEX2 Accelerator card due to the parallel threads that run in the z9 BC CPs. Thus the full capability of the CEX2 Accelerator card for parallel execution of the cryptographic operation can be utilized.

The third column of the above table is for measurements where 32 jobs were continuously executing the same cryptographic operation using 4 CEX2 Accelerator cards. The results show the scalability of the throughput when multiple CEX2 Accelerator adapters are used in one z9 BC system.

## 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 z9 BC, the PKD operation will be routed for execution to the CEX2 Coprocessor or CEX2 Accelerator adapter, if available in the configuration. For all presented measurements the PKD operation is in 'clear key' mode.

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

- *Measurements were performed on a z9 BC system with 4 CPs as a Server.*
- *The performance data is for the server only. The server was driven to a maximum utilization by increasing the number of client threads (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 Triple DES (168 bits) and SHA cipher except when stated otherwise. This SSL data symmetric key encryption for TDES and SHA is executed in 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 CEX2 Accelerator or CEX2 Coprocessor adapter.

#### **Client Authentication:**

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

### **External Throughput Rate (ETR):**

Number of handshakes performed per second.

### **CPU Utilization %:**

Average utilization of the z9 BC system Central Processors as reported by Resource Measurement Facility (RMF™).

### **Crypto Utilization %:**

Average utilization of the CEX2 Accelerator or CEX2 Coprocessor adapters as reported by RMF.

#### 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 performance measurement results clearly suggest using cryptographic hardware 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. Furthermore, the measurement results show the throughput with one CEX2 Accelerator adapter being in the order of three times the throughput as with one CEX2 Coprocessor adapter in the SSL environment. Thus for high SSL protocol transaction rate environments, CEX2 Accelerator is the preferred configuration mode for a System z9 BC server.

The resource consumption in system processing power for one SSL protocol handshake is in the order of 1/5000 of the system (see table below) in the z/OS environment for a z9 BC Model S04 with 4 Central Processors and 2 CEX2 features (4 CEX2 Accelerator cards).

If the transaction were to be ‘secured’ by an SSL protocol and the server portion were run on a System z9 BC server, 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 1.7 / Enhancements to Cryptographic Support for z/OS and z/OS.e 1.6/1.7 (ICSF)

**z9 BC Model S04 (4 Central Processors)**

Caching SID	Handshake	Client Auth.	ETR	CPU Util. %	Crypto Util. %
100%	Avoided	no	6,920	97.8	NA
no	Software	no	345	99.9	NA
no	6 CEX2C	no	5,109	96.6	85.3
no	4 CEX2A	no	5,248	97.3	42.4
no	4 CEX2A	yes	3,693	99.2	37.4

Using the CEX2 Coprocessor 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 14.8 times.

The 5,109 ETR (third row) was achieved with 3 CEX2 features available to the system, providing 6 adapters which were all configured as Coprocessors. The average utilization of the 6 CEX2 Coprocessor adapters was 85.3% in this test, indicating that the 6 CEX2 Coprocessor adapters could potentially process almost 6,000 SSL handshakes before reaching 100% utilization.

The fourth row shows that a similar throughput rate can be achieved with CEX2 Accelerator adapters. With the CEX2 Accelerator configuration mode, only 4 adapters were used and the average utilization of the CEX2 Accelerator adapters was 42.4%, indicating that the 4 CEX2 Accelerator adapters could potentially process more than 12,000 SSL handshakes before reaching 100% utilization.

If Client authentication is required the throughput of the server is considerably reduced, as shown in row 5 of the above table.

**5. May 2007 Performance Update for CEX2-1P**

The CEX2-1P feature is designed to address high-end server security requirements. The CEX2-1P feature contains one PCI-X adapter which is configurable and can be defined for secure key encrypted transactions (Coprocessor – the default) or SSL acceleration (Accelerator). CEX2-1P executes the same functions as the CEX2 feature and is only supported on z9 BC.

When configured as a Coprocessor, the PCI-X adapter is designed to provide security-rich cryptographic operations to be used by System z9 host application programs. The Coprocessor mode offers security features for symmetric key and public key operations. In this case the cryptographic keys are encrypted under the corresponding Master Keys when outside the boundary of the PCI-X adapter.

When configured as an Accelerator, the PCI-X adapter is designed to provide high speed acceleration of RSA operations in 'clear key' mode, providing security rich communication for Web site-based applications which utilize the SSL or TLS protocol. Some implementers execute the public key operation, incurred during set up of an SSL session, in 'clear key' mode.

The connection of the CEX2-1P feature via the PCI-X bus to the z9 BC Central Processors (CPs) incurs latency and data transmission time. Because of this connection to the z9 BC CPs, the CEX2-1P operates asynchronous to the z9 BC CPs.

There can be a maximum of 8 CEX2-1P features in a z9 BC system, each CEX2-1P feature containing one PCI-X adapter.

### *5.1. CEX2-1P Coprocessor Multiple Data Symmetric Key Performance*

This chapter deals with CEX2-1P Coprocessor cryptographic operations with a user supplied length of data (for example, DES encryption of n bytes of data).

All test cases are written in System z9 BC Assembler Language issuing an API call to ICSF for the cryptographic operation. ICSF will resolve the API call and handle the communication with the CEX2-1P 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 PCI-X adapter.

The throughput for the cryptographic operations using the CEX2-1P 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 CEX2-1P 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.

The data quoted was from test cases run on a z9 BC Model S04 using 1 job that performs the cryptographic operation. Measurements were also taken with multiple jobs using up to 4 CPs. Results with multiple jobs are not always included in tables, however, for each cryptographic

operation type quoted there is a statement on scalability of the results if multiple jobs are 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 V1.8 including z/OS Integrated Cryptographic Service Facility (ICSF).

**CEX2-1P Coprocessor DEA Cipher Block Chaining Encipher with Single Length**

CEX2C-1P (one job): Single DES CBC Encipher		
Data Length (Bytes)	Operations/sec	x10**3 Bytes/sec
64	920.90	58.94
256	921.10	235.8
1024	914.20	936.2
4096	620.00	2539.7
64K	66.46	4356.1
1M	4.31	4525.6

**Key (56 Bits)**

The above table provides measurement results for an environment where one job was continuously executing the cryptographic operation using one CEX2-1P Coprocessor. As mentioned, the execution of the cryptographic operation in the CEX2-1P Coprocessor is asynchronous to the z9 BC 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 CEX2-1P Coprocessor'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 CEX2-1P 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 CEX2-1P.

CEX2C-1P (seven jobs): Single DES CBC Encipher		
Data Length (Bytes)	Operations/sec	x10**3 Bytes/sec
64	1442.0	92.30
256	1351.0	345.9
1024	1083.0	1109.8
4096	857.8	3513.7
64K	79.62	5218.3
1M	5.13	5386.7

The throughput with 2 CEX2-1P Coprocessor features 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 2 times the throughput of one CEX2-1P Coprocessor feature with 7 jobs (as exemplified above).

**CEX2-1P Coprocessor DEA Cipher Block Chaining Encipher with Triple Length Key (168 Bits)**

CEX2C-1P (one job): Triple DES CBC Encipher		
Data Length (Bytes)	Operations/sec	x10**3 Bytes/sec
64	921.1	58.95
256	921.1	235.8
1024	874.2	895.2
4096	619.6	2538.0
64K	56.30	3690.0
1M	3.62	3796.9

The throughput for seven jobs for CEX2-1P Coprocessor TDES is approximately 1.2 times to 1.5 times higher than for one job (as measured in this example).

**CEX2-1P Coprocessor Message Authentication Code with DEA Single Length Key (56 Bits)**

CEX2C (one job): MAC with single DES		
Data Length (Bytes)	Operations/sec	x10**3 Bytes/sec
64	921.5	58.97
256	921.4	235.8
1024	920.6	942.7
4096	917.2	3756.8
64K	87.27	5719.8
1M	5.91	6200.5

The throughput for seven jobs for CEX2-1P Coprocessor MAC is approximately 1.2 to 1.6 times higher than for one job (as measured in this example), the lower number applying to large data length and the higher to small data lengths.

*5.2. CEX2-1P Coprocessor Symmetric Key Performance - Diverse Operations*

The following table gives the throughput in number of operations per second on a CEX2-1P feature for some selected symmetric key operations.

CEX2-1P Coprocessor Symmetric Key Operations - Examples	Ops/s 1 job	Ops/s 7 jobs
Key Generate (operational DES KEYGENKY key)	666	988
Clear PIN Generate Alternate (DES OPINENC + DES PINGEN keys)	624	945
Clear PIN Generate (16 digits) ( DES PINGEN key)	923	1,472
Encrypted PIN Translation (DES IPINENC key + DES OPINENC key)	921	1,129
Encrypted PIN Translation (2 UKPT enabled KEYGENKY keys)	316	336
Encryp.PIN Verificat. (UKPT enabl.KEYGENKY+DES PINVER keys)	470	494

The throughput with 2 CEX2-1P Coprocessor features with a sufficient number of jobs repetitively requesting the same cryptographic operation for the examples in the table above is close to 2 times the throughput of one CEX2-1P Coprocessor feature with 7 jobs.

*5.3. CEX2-1P Coprocessor PKA Performance*

The CEX2-1P 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 lengths 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 private keys (signature key or encryption key) are encrypted under the corresponding master key.

The performance numbers are from measurements with z/OS V1.8 including z/OS Integrated Cryptographic Service Facility (ICSF) invoking the operation via the ICSF API according to the PKCS-1.2. standard. Measurements were performed on a z9 BC Model S04 with 4 CPs.

**CEX2-1P Coprocessor PKA Performance**

<b>CEX2C-1P on z/OS V1.8 (ICSF level: WD#6)</b>			
Public Key Decrypt (PKD), Public Key Encrypt (PKE) Digital Signature Generate (DSG), Digital Sign. Verify (DSV) Symmetric Key Import (encrypted with RSA key) (SYI)			
	2096-S04	2096-S04	2096-S04
CEX2C-1P	1	1	2
Jobs	1	7	14
	Operations/sec	Operations/sec	Operations/sec
PKD--CRT, 512 bit	909	1183	2364
PKD--CRT, 1024 bit	619	1062	2121
PKD--CRT, 2048 bit	271	466	931
PKD--ME, 512 bit	619	1158	2311
PKD--ME, 1024 bit	468	930	1858
PKE, 512 bit	913	1289	2579
PKE, 1024 bit	912	930	2167
PKE, 2048 bit	619	809	1614
DSG--CRT, 512 bit	911	1202	2400
DSG--CRT, 1024 bit	619	1079	2154
DSG--CRT, 2048 bit	271	466	931
DSV--ME, 512 bit	918	1438	2839
DSV--ME, 1024 bit	918	1363	2717
SYI--CRT, 512 bit	619	882	1762
SYI--CRT, 1024 bit	610	833	1662

The PKA cryptographic operation throughput with 2 CEX2-1P Coprocessor features with a sufficient number of jobs repetitively requesting the same cryptographic operation for the examples in the table above is close to 2 times the throughput of one CEX2-1P Coprocessor feature with 7 jobs.

**PKA RSA Key Generate**

The CEX2-1P 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 CEX2-1P Coprocessor.

**CEX2-1P Coprocessor PKA RSA Key Generation Performance**

CEX2C-1P PKA RSA Key Generate	
	Operations/sec
External CRT, 512bit	3.31
External CRT, 1024bit	1.66
External CRT, 2048bit	0.65
Internal ME, 512bit	3.90
Internal ME, 1024bit	1.92

*5.4 CEX2-1P Accelerator Performance*

The CEX2-1P Accelerator configuration mode is designed to offer fast Public Key Algorithm (PKA) cryptographic 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 V1.8 including z/OS Integrated Cryptographic Service Facility (ICSF) 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)

**CEX2-1P Accelerator PKA Performance**

<b>CEX2A Public Key Decrypt (PKD) and Public Key Encrypt (PKE) (z/OS V1.8 ,ICSF: WD#6)</b>			
2096 CPs	4	4	4
CEX2A-1P Features	1	1	2
Jobs	1	8	16
	Operations/sec	Operations/sec	Operations/sec
PKD--CRT, 512 bit	1747	10233	20068
PKD--CRT, 1024 bit	1744	3334	6664
PKD--CRT, 2048 bit	377	455	911
PKD--ME, 512 bit	1748	3370	6720
PKD--ME, 1024 bit	621	919	1838
PKE, 512 bit	1772	13600	26039
PKE, 1024 bit	1771	13602	25583
PKE, 2048 bit	1768	11646	21598

The first result column of the above table is for measurements where one job was continuously executing the cryptographic operation using one CEX2-1P Accelerator. As mentioned, the execution of the cryptographic operation in the CEX2-1P Accelerator is asynchronous to the z9 BC 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 CEX2-1P Accelerator. The increased throughput is due to the fact that tasks are readily available for execution in the CEX2-1P Accelerator due to the parallel threads that run in the z9 BC CPs. Thus the full capability of the CEX2-1P Accelerator for parallel execution of the cryptographic operation can be utilized.

The third column of the above table is for measurements where 16 jobs were continuously executing the same cryptographic operation using 2 CEX2-1P Accelerators. The results show the scalability of the throughput when multiple CEX2-1P Accelerator features are used in one z9 BC system.

### *5.5. 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 z9 BC, the PKD operation will be routed for execution to the CEX2-1P Coprocessor or CEX2-1P Accelerator feature, if available in the configuration. For all presented measurements the PKD operation is in 'clear key' mode.

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

- *Measurements were performed on a z9 BC system with 4 CPs as a Server.*
- *The performance data is for the server only. The server was driven to a maximum utilization by increasing the number of client threads (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 Triple DES (168 bits) and SHA cipher except when stated otherwise. This SSL data symmetric key encryption for TDES and SHA is executed in 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 CEX2-1P Accelerator or CEX2-1P Coprocessor adapter.

##### **Client Authentication:**

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

**External Throughput Rate (ETR):**

Number of handshakes performed per second.

**CPU Utilization %:**

Average utilization of the z9 BC system Central Processors as reported by Resource Measurement Facility (RMF).

**Crypto Utilization %:**

Average utilization of the CEX2-1P Accelerator or CEX2-1P Coprocessor adapter as reported by RMF.

### *5.5.1. 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 that results from a ‘business transaction’ (for example: 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 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. Furthermore, the measurement results show the throughput with one CEX2-1P Accelerator feature being in the order of three times the throughput as with one CEX2-1P Coprocessor feature in the SSL environment. Thus for high SSL protocol transaction rate environments, CEX2-1P Accelerator is the preferred configuration mode for a System z9 BC server.

The resource consumption in system processing power for one SSL protocol handshake is in the order of 1/5000 of the system (see table below) in the z/OS environment for a z9 BC Model S04 with 4 Central Processors and 2 CEX2-1P features configured in Accelerator mode.

If the transaction were to be ‘secured’ by an SSL protocol and the server portion were run on a System z9 BC server, 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.

5.5.2. SSL Protocol Performance - System SSL with z/OS 1.8 / z/OS Integrated Cryptographic Service Facility (ICSF)

z9 BC Model S04 (4 Central Processors)

Caching SID	Handshake	Client Auth.	ETR	CPU Util. %	Crypto Util. %
100%	Avoided	no	7,000	97.5	NA
no	Software	no	346	100	NA
no	2 CEX2C-1P	no	2,336	44.3	100
no	2 CEX2A-1P	no	5,370	97.5	83.8
no	2 CEX2A-1P	yes	3,514	93.4	68.5

With only 2 CEX2-1P Coprocessor features available (third row), the throughput was limited by the 100% Crypto Utilization. Installing additional CEX2-1P Coprocessor features would allow higher throughput.

Using the CEX2-1P Accelerator cryptographic hardware compared to using System SSL Software (second and fourth rows) produces an increase in throughput (number of SSL protocol handshakes) of 15.5 times (as measured in this example).

The 5,370 ETR (fourth row) was achieved with 2 CEX2-1P features available to the system, which were both configured as Accelerators. The average utilization of the 2 CEX2-1P Accelerator features was 83.8% in this test, indicating that the 2 CEX2-1P Accelerator features could potentially process more than 6,000 SSL handshakes before reaching 100% utilization.

If Client authentication is required the throughput of the server is considerably reduced, as shown in row 5 of the above table.

5.5.3. SSL Protocol Performance - Linux Open SSL

For all Linux Open SSL measurements the following applies:

- *Linux System Level: SLES9 SP3*
- *Linux Kernel Level: 2.6.5*
- *Open SSL Code Level: 0.9.7d*
- *System z9 Crypt Level: 1.3.3*
- *No Client Authentication*

**Linux Open SSL - Native Measurements**

Caching SID	Handshake	ETR	CPU Utilization %
no	2 CEX2C-1P	2,433	33.1
no	2 CEX2A-1P	6,640	91.9

With only 2 CEX2-1P features available, both measurements were limited by the crypto configuration. Installing additional CEX2-1P features would allow higher throughput.

When configured as a Coprocessor, each CEX2-1P supports approximately 1,200 SSL Handshakes per second.

When configured as an Accelerator, each CEX2-1P supports approximately 3,300 SSL Handshakes per second.



Copyright IBM Corporation 2007

IBM Corporation  
New Orchard Rd.  
Armonk, NY 10504  
U.S.A

Produced in the United States of America, 04/07

All Rights Reserved

IBM, IBM logo, OS/390, RACF, RMF, System z, System z9, z/OS, and zSeries are trademarks or registered trademarks of International Business Machines Corporation of the United States, other countries or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Information concerning non-IBM products was obtained from the suppliers of their products or their published announcements. Questions on the capabilities of the non-IBM products should be addressed with the suppliers.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

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.

Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY, 10504-1785 USA.

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 Internal Throughput Rate (ITR) ratio 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 ratios stated here.

ZSO03009-USEN-00