



Tales From the Frontlines:

SecureZIP® and IBM System z® Integrated
Cryptographic Services Facility

TECHNICAL WHITE PAPER

Table of Contents

Contents	2
Introduction	3
What is Hardware Crypto on System z?	4
Crypto Overview - Passphrase and Digital Certificates	4
Types of Encryption Algorithms	4
SecureZIP Crypto Interoperability	4
ICSF Operating Environment	5
System z Machines the Support Hardware Crypto	5
Enabling System z Hardware Crypto	6
Determining Available ICSF Facilities	6
Leveraging your System z Investment	7
Summary	8

Tales From the Frontlines: SecureZIP® and IBM System z® Integrated Cryptographic Services Facility

IBM's Integrated Cryptographic Services Facility (ICSF) allows organizations to increase processing efficiencies within their environment. Organizations can also increase productivity by applying SecureZIP to mainframe processes, facilitating cross-platform data exchange.

SecureZIP leverages IBM's System z ICSF, enabling organizations to take advantage of significant cost resource savings when encrypting data. SecureZIP maximizes the investment made by customers in hardware cryptography by utilizing the least expensive processor capabilities within a system, while maintaining the data security and portability that the standard ZIP file format provides. SecureZIP leverages the performance advantages of hardware-assisted cryptography on System z.

What is Hardware Crypto on System z?

Crypto Overview – Passphrase and Digital Certificates

A summary of cryptography outlines a few basic elements. There are two categories of encryption algorithms: symmetric and asymmetric. A symmetric key algorithm relies solely on private keys, such as a password or passphrase. Asymmetric encryption uses a private key and a public key, such as a digital certificate.

Passphrase-based encryption requires less setup, but sharing keys is difficult. By using only a single passphrase for both encryption and decryption, it makes it difficult to keep the data secure if more than one person is involved in the encryption and decryption process.

Certificate-based encryption is considered more secure but it takes increased setup. You need to obtain a certificate, which consists of a public and private key. The benefit of a digital certificate is that everyone can use your public key to encrypt data for you, and only you have the private key to decrypt that data. These certificates could be obtained by a number of Certificate Authorities (CA) such as Comodo, VeriSign, GeoTrust, and Entrust. PKWARE has several whitepapers describing the mechanics of how digital certificates work.

SecureZIP supports both passphrase- and certificate-based encryption; it can even support a combination of both methods.

Types of Encryption Algorithms

The two most frequently used encryption algorithms are Triple DES (3DES) and Advanced Encryption Standard (AES). Both are considered to be secure for the foreseeable future. 3DES builds on DES implementations and is readily available in many cryptographic products and protocols. The AES algorithm is well-established in many cryptographic applications, but it may be several years before the AES algorithm is as pervasive as 3DES.

The smallest AES key size is 128 bits. SecureZIP supports AES key sizes of 128, 192, and 256 bits. The recommended key size for 3DES is 168 bits. The smaller key size means that fewer resources are needed for the generation, exchange, and storage of key bits.

Therefore, when using SecureZIP, it is possible to encrypt data with 3DES, AES-128, 192, and 256 bit algorithms using either passphrase- or certificate- based encryption—or a combination of both methods.

SecureZIP Crypto Interoperability

An added benefit of SecureZIP is that secured archives (ZIP files) can be used not only on the platform that they were created on, but also any platform that SecureZIP runs on. The ZIP standard is platform independent and portable across all major computing systems. Encrypted ZIP archives created on System z could be transferred to System i, UNIX (HP/UX, Solaris, AIX), Linux, Windows Server, or Windows Desktop and could be decrypted on any of those platforms, or vice versa. digest, used in digital signing and authentication. Pseudo Random Number Generation is used in encryption and digital signing.






Not all ICSF functions are available in hardware on all System z platforms. Whether the ICSF functions are available in hardware or software depends on the platform, the hardware crypto cards installed on

those platforms, and the specific machine models.

ICSF Operating Environment

System z machines that support Hardware Crypto

Not all ICSF functions are available in hardware on all System z platforms. As seen in the table below, whether the ICSF functions are available in hardware or software depends on the platform, the hardware crypto cards installed on those platforms, and the specific machine models.

Machine	z990 2084	z890 2086	z9-EC 2094	z9-BC 2096	z10-EC 2097	z10-BC 2098
						
Algorithm Supported	DES 3DES	DES 3DES	DES 3DES AES128	DES 3DES AES128	DES 3DES AES128, 192, 256	DES 3DES AES128, 192, 256
Crypto Hardware	CPACF PCIXCC CEX2C	CPACF PCIXCC CEX2C	CPACF CEX2C	CPACF CEX2C	CPACF CEX2C	CPACF CEX2C

The z890, z990, z9 EC, z9 BC, z10-EC and z10-BC all support CP Assist for Cryptographic Functions or CPACF and Cryptographic Express2 Coprocessor or CEX2C.

CPACF provides hardware cryptographic capabilities such as 3DES, AES and SHA algorithms. The purpose of CPACF is to provide high performance operations of encryption, decryption, digital signing, and authentication.

CPACF is a set of cryptographic instructions available on all CPs. CPACF on the z9-EC and z9-BC machines has been enhanced to include support of the Advanced Encryption Standard (AES) for 128-bit keys along with Secure Hash Algorithm-256 (SHA-256), and Pseudo Random Number Generation (PRNG). CPACF on the z10-EC and z10-BC machines has been expanded to also support AES-192 and AES-256 algorithms as well as SHA-384 and SHA-512.

SecureZIP supports CPACF on the z990, z890, z9 EC, z9 BC, z10 EC and z10 BC. These machines also support FIPS 140-2 validated cryptographic algorithms, specifically the PCIXCC and the CEX2C.

The z890 and z990 support the PCI XCryptographic Coprocessor or PCIXCC. The z890, z990, z9 EC, z9 BC, z10 EC and z10 BC all support Cryptographic Express2 Coprocessor or CEX2C.

PCIXCC is an asynchronous cryptographic coprocessor. Both DES/3DES and RSA key functions are supported.

CEX2C provides equivalent function to the PCIXCC, but is packaged differently. The Crypto Express2 feature has two PCI-X adapters, and each can be defined as either a Coprocessor or as an Accelerator.

Like the PCIXCC, both DES/3DES and RSA key functions are supported.

Enabling System z Hardware Crypto

Here is a summary of steps for preparing a system for Hardware Crypto.

Even when using CPACF, where crypto functions exist on the CP itself and no additional hardware needs to be purchased, Hardware Crypto still needs to be enabled to comply with crypto export restrictions. It is also necessary to define and activate the coprocessors to the LPAR's and activate.

The Cryptographic Key Data Set (CKDS) is the data storage for the symmetric (DES) keys, and the Public Key Data Set (PKDS) is the data storage for the public keys. Keys stored in the CKDS and PKDS are not stored in the clear, but are encrypted using EDE (Encipher/Decipher/Encipher) which is an ANSI standard. ICSF uses ISPF panels to administer the cryptographic hardware and keys.

ICSF is the system software (comes as part of the base OS) that provides the interface to the hardware, and must be active to use the hardware. ICSF runs as a started task and provides the key management interfaces and access to the CKDS and PKDS, as well as the APIs for applications to invoke the hardware functions.

Determining Available ICSF Facilities

The first phase of planning for SecureZIP's use of ICSF is to map targeted cryptographic functionality into facilities that are made available across the platform environments.

Cryptographic Service	z/890 & z/990	z9 BC/EC	z10 BC/EC
DES/TDES Hardware Acceleration	CPACF HCR7720	CPACF HCR7730	CPACF HCR7750
AES ICSF Software	CPACF HCR7720	CPACF HCR7730	CPACF HCR7750
AES128 Hardware Acceleration	Not available	CPACF HCR7730	CPACF HCR7750
AES192, 256 Hardware Acceleration	Not available	Not available	CPACF HCR7750
SHA-1 Hardware Acceleration	CPACF HCR7720	CPACF HCR7730	CPACF HCR7750
SHA-256 Hardware Acceleration	Not available	CPACF HCR7730	CPACF HCR7750
SHA-384, 512 Hardware Acceleration	Not available	Not available	CPACF HCR7750
Pseudo Random Data Generation	PCIXCC/CEX2C HCR7720	CPACF/CEX2C HCR7730	CPACF/CEX2C HCR7750

The left-hand column of the above table defines the primary functional ICSF services required for SecureZIP processing. The primary hardware facility available for each required service--Cryptographic Coprocessor Facility or CP Assist for Cryptographic Functions is mapped into the matrix for each platform.

PKWARE researched the required ICSF software level required to access the hardware facility (listed by SMP/E FMID). Although an internal binary release level is available from the major ICSF control block, it is not shown here to avoid confusion with operating system release levels.

Leveraging your System z Investment

Taking advantage of your System z Hardware Crypto with SecureZIP

SecureZIP can use several facilities for crypto algorithms, including data encryption algorithms. Originally SecureZIP only used the RSA BSAFE crypto algorithms, but in version 9, ICSF integration was introduced and SecureZIP could use one of three difference facilities to encrypt data: IBM Hardware, IBM Software, and RSA BSAFE.

Below is a typical SecureZIP job for encrypting data using passphrased based encryption on a z9:

```
//ZIPTXT EXEC PGM=SECZIP
//STEPLIB DD DISP=SHR,DSN=PROD.PKWARE.LOAD
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
-ENCRYPTION_METHOD(AES128)
-PWD(PASSWORD)
-ARCHIVE_DSN(PROD.TEXT.LIB.ZIP)
-ACTION(ADD)
PROD.TEXT.LIB
/*
```

SecureZIP is taking the dataset PROD.TEXT.LIB and encrypting it using AES128 encryption into a ZIP archive named PROD.TEXT.LIB.ZIP. To take advantage of Hardware Crypto on this z9, the only command that is needed is already in the Defaults Module (ACZDFLT):

```
-FACILITY_ENCRYPTDATA(IBMHardware,IBMSoftware,SECUREZIP)
```

The command FACILITY_ENCRYPTDATA describes the choice of cryptographic facility (service) available to accomplish the requested encryption/decryption process. The values specify, in order of preference, the facility types that SecureZIP should attempt to use. Because IBMHardware is listed first, and because AES128 is available on the z9, ICSF Cryptographic Services will be engaged to use the hardware-accelerated cryptography.

If this command is listed in the Defaults Module (ACZDFLT), then no JCL changes are required for the sample job listed above; it will simply take advantage of hardware crypto.

Upgrading PKZIP or SecureZIP to take advantage of hardware crypto

Below is a sample JCL from PKZIP v5.6 demonstrating the syntax required to encrypt:

```
//ZIPTXT EXEC PGM=PKZIP
//STEPLIB DD DISP=SHR,DSN=PROD.PKWARE.LOAD
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
-ENCRYPTION_METHOD(AES128)
-PWD(PASSWORD)
-ARCHIVE_DSN(PROD.TEXT.LIB.ZIP)
-ACTION(ADD)
PROD.TEXT.LIB
/*
```

The only difference between this sample job and the previous sample job is the PGM name, PKZIP vs. SECZIP.

After PKZIP 5.6 is upgraded to SecureZIP v10, assuming SecureZIP v10 uses the same load library (PROD.PKWARE.LOAD), the exact same JCL that was used in PKZIP 5.6 could be used to perform hardware crypto using SecureZIP version 10. Because PKZIP is an alias for SECZIP, the program name does not have to change. SecureZIP strives to stay backward compatible with previous versions of our PKZIP/SecureZIP products to preserve your investment in existing Batch Jobs, but also allows you to take advantage of your investment in System z Hardware Crypto without having to change your existing JCL.

If the ENCRYPTION_METHOD used in the PKZIP version 5.6 job was AES256 instead of AES128, after the upgrade, the job will still execute. The only difference is that hardware crypto would not be utilized because AES256 is not supported on the z9 with CPACF. AES256 is supported on the z10 with CPACF where by hardware crypto would be utilized.

Summary

PKWARE leverages the power of IBM's System z Integrated Cryptographic Services Facility (ICSF) with its SecureZIP Mainframe products. SecureZIP provides a cross platform security solution that offers data encryption, digital signing, and authentication. SecureZIP supports both passphrase and digital certificate-based encryption capabilities, or a combination of both methods.

PKWARE's SecureZIP leverages the System z hardware and software facilities, regardless of the hardware features enabled in a specific installation. Secured archives (ZIP files) can be used not only on the platform they were created on, but also any platform that SecureZIP runs on. In addition, SecureZIP maximizes the investment made by customers in hardware cryptography by utilizing the least expensive processor capabilities within a system, while maintaining the data security and portability that the standard ZIP file format provides.

As a result of the flexible application of PKWARE's SecureZIP Mainframe products, leveraging IBM's ICSF will enable organizations to take advantage of significant cost and resource savings when encrypting data.

United States

648 N. Plankinton Ave. Suite220
Milwaukee, WI 53203
1.888.4.PKWARE
www.pkware.com

UK/EMEA

Crown House
72 Hammersmith Road
London W14 8TH
United Kingdom
ph: +44 (0) 207 470 2420

© 2008 PKWARE, Inc. All rights reserved. PKWARE, PKZIP, SecureZIP, and SecureZIP Mail Gateway are trademarks or registered trademarks in the U.S.A. and other countries. Any other trademarks are used for identification purposes only and remain the property of their respective owners.