A Synopsis of z Systems Crypto Hardware

Version 2 Release 4

Author:

Hank Meetze

Changes:

V2R4 – Addition of z15-T01 and z15-T02 cryptographic features and the addition of TKE 9.2. Removal of processor information for the z990/z890.

V2R3 – Addition of z14 cryptographic features and the addition of TKE 9.0.

V2R2 – Addition of z13s and z13 GA2 updates. Removal of processor information for the z900/z800. Addition of TKE 8.1 and improvements with the TKE section.

A Synopsis of z Systems Crypto Hardware

The IBM z Systems cryptographic hardware provides a rich array of encryption capabilities. The functionality available depends on the specific platform and the hardware that has been installed. This document begins with a brief introduction of crypto functions and issues common to all the platforms, and then provides a synopsis of the z Systems crypto hardware, including the IBM z15 announcement (120-006 from April 14, 2020.

Cryptographic Functions

z Systems cryptographic hardware supports four cryptographic capabilities. These include:

- data confidentiality (encrypting/decrypting data using symmetric and/or asymmetric algorithms)
- message integrity (message authentication, modification detection, non-repudiation)
- financial functions (using symmetric algorithms to protect PINs associated with credit cards and financial transactions)
- key management (security and integrity of keys)

Clear Key vs Secure Key vs Protected Key

IBM Crypto hardware can use clear key, secure key or protected key. No matter which you choose, there is no difference in the crypto algorithms and the resulting ciphertext is the same if the underlying key is the same. The difference is the protection provided for the key value that protects the data.

The secure hardware includes tamper detecting technology to protect against attacks involving probe penetration, power sequencing and radiation and temperature manipulation consistent with FIPS requirements. If a tamper is detected the circuitry will zeroize the card wiping out the keys so they cannot be compromised. When a secure key is created, that key is encrypted under a master key, and the underlying key value is never exposed, in the clear, outside of the secure hardware. When that key needs to leave the secure hardware (for example to be stored in a repository) the encrypted version of the key is stored. That encrypted key must itself be decrypted before it can be used to encrypt or decrypt data. (For transport purposes, a key can be encrypted under a key encrypting key instead of the master key, but in no instance will a secure key exist in the clear outside of the secure hardware.)

A clear key is not protected (encrypted) by another key. The actual key value may exist in a file or on the network during key entry or in an address space when in use by an application. Operational procedures and other security mechanisms provide protection for clear keys.

Beginning with Driver 79 (Nov. 2009 LIC on the z10) IBM hardware adds support for protected keys. A protected key does not rely on the tamper resistant secure hardware but is an operational key that is encrypted under a wrapping key associated with the LPAR. When the protected key is brought into the CPACF it is unwrapped and the clear value is used to perform the crypto operation.

A protected key never exists, in the clear, in system storage. A protected key is encrypted under a wrapping key that is uniquely created each time the LPAR is activated or reset. That wrapping key is stored in the Hardware Storage Area (HSA) and cannot be accessed by an application or the operating system. The wrapping key does not have the protection of tamper resistant hardware, but it is only available to firmware. There are three variations of the wrapping key: one for DES/TDES keys, one for AES keys and one for ECC keys.

Each of the three types of keys (clear, secure and protected) have different performance characteristics and thus different costs. In addition to the hardware costing more, there are performance and CPU costs, so customers must make a business decision about whether their security requirements warrant the cost of secure key support.

Of the three types of symmetric keys (clear, secure and protected), clear keys provide the best performance. Clear key operations are done on the CPACF, which is associated with the general purpose CP and so operations are completed synchronously, at machine speeds.

Secure key operations are routed out to the PCI card on the Self-Timed Interface, so effectively you’re executing an I/O operation to get the data and keys out to the card. While the crypto work is offloaded to the card, there is still some CPU costs in getting the work formatted for and routed to the card and then in receiving the results back from the card and passing those results back to the caller. But the real impact on performance is the asynchronous operation to the card. Secure key operations will take longer than clear key operations.

Protected keys fall in between clear keys and secure keys in terms of performance. Performance is closer to that of clear keys, although they do have some additional overhead. It is expected that most protected keys will be stored as secure keys in the CKDS. That key will need to be brought into the Crypto Express3 (CEX3) or Crypto Express4S (CEX4S), Crypto Express5S (CEX5S), Crypto Express6S (CEX6S) or Crypto Express7S (CEX7S) adapters, decrypted from under the master key and then re-encrypted under the wrapping key. The actual encryption and decryption of the data, done on the CPACF, will then have similar performance characteristics to a clear key operation.

Clear keys would be appropriate when there are procedures in place to protect the key values while they are in use, or when the additional cost of secure key protection outweighs the risk to the data (as when a short-lived key is required, such as with System SSL). If the amount and/or value of the data being protected is low, the additional cost of secure key protection may not be worthwhile. If operational procedures protect the clear key values (i.e. dumps that might contain passwords are shredded or disposed in a secure manner), then secure key encryption may not be required. If the data being protected is segmented in such a way that an attacker would have to invest significantly to capture all the relevant pieces, clear key may provide sufficient protection.

Protected keys would be appropriate for applications that require better performance than secure key, but don't have the strict requirement of a Hardware Security Module (HSM).

Protected keys can begin life as a secure key or a clear key. That is, a protected key may use a secure key which is decrypted from under the master key and then wrapped for use in the CPACF. Or, a protected key may be generated as a clear key within an application and then wrapped for use in the CPACF.

Secure key hardware requires that a master key be loaded to enable that hardware. Since it provides protection for other keys, the master key must be available to use the crypto functions on the card. Clear key hardware does not require a master key, but it's important to note that secure key hardware may be a superset of clear key hardware. That is, clear key work may be performed on secure hardware, but secure key work will only be executed on secure key hardware.

The private key of an RSA key pair can also be a secure key, encrypted under the asymmetric master key or ASYM-MK. The public key, since it will be published, is stored in the clear.

Symmetric Algorithms, Symmetric Keys

Symmetric keys are used with symmetric algorithms (Data Encryption Standard or DES; Triple DES or TDES; Advanced Encryption Standard or AES) and both parties (the encrypter and decrypter) must have a copy of the key, which must be a secret between the two. Anyone who has a copy of the symmetric key can decrypt the data enciphered with that key.

Asymmetric Algorithms, Public/Private Keys

Don't confuse clear key/secure key with public/private keys used by asymmetric algorithms. Asymmetric algorithms or Public Key Architecture (PKA) use a key pair to protect data. With PKA, two different, but mathematically related keys are used. One, the public key, is made available publicly and can be used by anyone who wants to send data securely to the owner of the private key. Data that has been encrypted using a public key can ONLY be decrypted using the corresponding private key. Anyone who has a copy of the public key can encrypt their own data to send, but they cannot use that public key to decrypt data that was encrypted using the same public key. That is, if both you and your neighbor have my public key, each of you can encrypt a message to me and I can decrypt it with the corresponding private key. But you can't decrypt your neighbor's message with that public key. Since the private key must be used to decrypt the data encrypted by the public key, that private key should be well protected and only available to the owner of the public/private key pair. The secure hardware along with the asymmetric master key can provide that level of protection.

Export Restrictions

The U.S. Government considers encryption technology to be a munition, and therefore strictly controls the ability to export the technology. Since the z Systems includes crypto technology within the machine, IBM controls access to the crypto hardware via microcode, and the U.S. Government limits where that microcode can be exported. All of the z Systems crypto hardware requires the appropriate microcode to be installed and operational before the export restricted functions can be used. On the zEC12/zBC12, z13/z13s,z14/z14 ZR1 and z15-T01/z15-T02 machines, this microcode is ordered as no-charge Feature Code #3863. IBM software that implements encryption will also check for the presence of this feature code before performing encryption in software.

Cryptographic Software

The Integrated Cryptographic Service Facility, ICSF, is the system software that provides the interface to the hardware. As new functions are implemented in the hardware, new versions of ICSF will be available to invoke those functions. ICSF is available as a component of and packaged with z/OS, however the most current versions are available via web download at:

http://www-03.ibm.com/systems/z/os/zos/tools/downloads/index.html.

See TechDoc TD103782, ‘z/OS: ICSF Version and FMID Cross Reference’ for a summary of the hardware support in the various versions of ICSF.

Later in the document we’ll see that there are crypto instructions that are available directly to an application, but most of the crypto hardware can only be accessed by using the cryptographic Application Programming Interfaces (APIs). Invoking the APIs in application code or in a product will pass the crypto request to ICSF which will determine what hardware is available and which device can best service the request. Some APIs may be supported by a single crypto device which implies that that device must be installed and available to service the API. If the appropriate device is not available, ICSF will fail the operation with a return code and reason code indicating the device was not available. Other APIs can be serviced on several different devices and ICSF will make the decision where best to route each call. The ICSF Application Programmer’s Guide provides a table for each API that describes the hardware required to support the API.

Application code can also affect how the cryptographic hardware is used. The application determines which APIs or cryptographic instructions are invoked, and what parameters are passed to the API. Specific parameters may be supported on a particular cryptographic hardware device, but not on another. So, the parameters can impact how the work is routed. In addition, some applications may perform the cryptographic functions using software routines, never routing the work to the hardware or ICSF.

Native Peripheral Component Interconnect Express (PCIe)

Since the PCIe cards use the Self-Timed Interface, the crypto work done on the cards is asynchronous. That is, once ICSF routes the work to the card the application waits for the operation to complete and the general purpose CPs are free to handle other work (both crypto and non-crypto work) in the system. The PCIe cards perform the crypto function and queue the results back to ICSF which then provides the results back to the calling application.

Installing new crypto microcode takes longer than installing non-crypto MCLs. Crypto MCLs are installed on the CEC just like any other MCL, but that microcode must then be loaded into the crypto engines. And once the microcode is loaded, the crypto engine will perform a number of tests to insure it is operating properly. These include 'known-answer' tests where the crypto engine will perform an operation expecting to get a specific result. If that specific result is not returned, the card will issue a hardware check and the card will not be available to perform crypto work. These 'known-answer' tests can take a while to perform, especially as tests are added to meet FIPS compliance. Therefore, be aware that it does take a while for the crypto engines to complete loading after an MCL install.

The PCIe cards can be configured in different modes. By default the card is a coprocessor and can support all of the crypto functions as defined at the beginning of this document. Alternatively, the card can be configured as an accelerator. In this mode, the card only supports three cryptographic APIs, all associated with System SSL handshakes. Because of this smaller microcode load, the performance for these APIs is significantly better than when configured as a coprocessor. Finally, with the CEX4S on the zEC12/zBC12, the CEX5S on the z13/z13s, the CEX6S on the z14/z14 ZR1 and CEX7S on the z15-T01/z15-T02, there is support for EP11 or PKCS #11 Enterprise mode. In this mode, the card only supports APIs associated with PKCS #11.

Also with the PCIe implementation, the secure hardware supports User Defined Extensions (UDX). A UDX provides the ability to load customer specific code into the secure hardware giving the ability to manipulate data securely within the hardware protection of the card. UDX's are custom written, and while customers can write their own on other platforms, it is strongly recommended that IBM Global Services be engaged as they are experienced in developing and writing custom implementations that communicate with ICSF without introducing covert channels.

Cryptographic Hardware

There are two cryptographic hardware devices available on the zEC12/zBC12, z13/z13s, z14/z14 ZR1 and z15: the CPACF and the PCIe crypto cards.

CP Assist for Cryptographic Function (CPACF)

The CP Assist for Cryptographic Function (or CPACF) was introduced in 2003. Each generation of the machine introduces new function as well as improved performance on the CPACF. The CPACF is associated with the general purpose engines on the machine and provides assembler instructions that perform crypto operations. These instructions are called Message Security Assist (MSA) instructions. They are synchronous instructions that run at processor speed for every CP, IFL and zIIP. So when the CPACF is processing a cryptographic request the PU passing that work to the CPACF is busy and unavailable for other work.

The CPACF is accessible through native assembler instructions, or via the clear key APIs available with ICSF. See the Principles of Operations in ResourceLink for the specific machine for the assembler instructions, and the ICSF Application Programmer's Guide for the APIs that are available.

Prior to the implementation of Protected Key described above, the CPACF was clear key hardware. That is, when you invoke an assembler instruction to perform a symmetric encryption operation, the instruction expects to receive the cryptographic key via an address pointer to the key value. That key value will either be in the clear or when using protected key, the CPACF expects the pointer to be to a wrapped key (the operational key is encrypted, or wrapped) not a clear key. However, the CPACF is not considered a secure key device. That is, it does not include any tamper resisting technology.

Cryptographic PCIe Cards

As described above, the Cryptographic PCIe cards are optional, implementing additional cryptographic function. Using the PCIe infrastructure provide advantages in terms of availability, scalability and cost. In the earliest machines, there were two variations of the cards, a secure key device that implements a multitude of capabilities or a clear key device that implements only a limited set of functions, but provides a significant performance benefit for those functions. In 2008 the Crypto Express cards, IBM provided a single feature, with multiple engines that could be independently configured as either a coprocessor (secure key device) or an accelerator (clear key device). Starting with the zEC12/zBC12 there is a new function called EP11 mode, which provides support for secure key PKCS #11 operations and is described further in the zEC12/zBC12 section.

The crypto PCIe cards have tamper resistant technology on the cards which meets the FIPS 140-2 Level 4 requirements. As defined in FIPS 140-2, the cards are packaged with tamper detecting and tamper responding technology, such that, if an attacker tries to determine the contents of the card the hardware will detect the attack and wipe out (or zeroize) its contents before they can be captured. The technology protects against attacks involving probe penetration, power sequencing and radiation and temperature manipulation consistent with FIPS requirements

When configured as a coprocessor, the cryptographic engine must have a master key loaded. That master key will be used to encrypt operational keys that will leave the secure tamper resistant boundary of the card. When you store your operational key in a key repository, the secure keys will be encrypted using the appropriate master key from the card. To use the operational key in the future it would have to be loaded back into a coprocessor and the same master key would have to be used to decrypt the key and recover the actual operational key value.

On the most current PCIe card there are five different master keys available, although you only need to load the ones that you plan to use. Those are:

AES-MK or AES Master Key for encrypting AES keys
DES-MK or DES Master Key for encrypting DES/TDES keys
ECC-MK or Elliptic Curve Master Key for encrypting ECC private keys and certain RSA key pats in type 30 and 31 RSA keys.
RSA-MK or Rivest-Shamir-Adelman Master Key for encrypting RSA private keys
P11-MK for EP11 Master Key for encrypting PKCS #11 secure key material

The following is a description of the cryptographic hardware devices across the z Systems platforms, N (z15) through N-6 (z9 EC/z9 BC).

IBM z15

The IBM z15-T01 was announced on September 12, 2019 (119-027) and the z15-T02 was announced on April 14, 2020 (120-006). There have been many enhancements protecting data residing on this platform and beyond the z15 using Data Privacy Passports (220-062).

CP Assist for Cryptographic Function

The CPACF is on available on every core just like the previous z14 processor. There have enhancements with the ICSF call to the CPACF. New instructions have been added on the z15 for ECC operations. These are, key generation, key derivation and digital signatures generation and verification using NIST curves. For the z15 the CPACF hardware supports the following cryptographic services:

- DES
- Triple-DES
- AES-128
- AES-102
- AES-256 (clear and protected keys)
- SHA-1
- SHA-256 (SHA-2 and SHA-3 standard)
- SHA-384 (SHA-2 or SHA-3 standard)
- SHA-512 (SHA-2 or SHA-3 standard)
- SHAKE-128
- SHAKE-256
- PRNG
- DRNG
- TRNG
- Edwards Elliptic Curves Ed25519 and Ed448
- NIST Prime curves P-256, P-384, and P-521

It provides high-performance hardware encryption, decryption, hashing, and random number generation support. The following instructions support the cryptographic assist function:

- KMAC: Compute Message Authentic Code
- KM: Cipher Message
- KMC: Cipher Message with Chaining
- KMF: Cipher Message with CFB
- KMCTR: Cipher Message with Counter
- KMO: Cipher Message with OFB
- KIMD: Compute Intermediate Message Digest
- KLMD: Compute Last Message Digest
- PCKMO: Provide Cryptographic Key Management Operation

PKCS #11 enhancements

The z15 continues to make enhancements to support of PKCS #11 for clients requiring open standards and enhanced security. Listed are these new enhancements:

- EP11 interface similar to the industry standard PKCS #11 API.
- Design enhancements to meet requirements for BSI (Federal Office for Information Security in Germany)
- Support for SHA-3 EdDSA
- EP11 4.7 support for the Crypto Express7S adapter
- Protected mode WrapKey, the secure EP11 key is returned to the host caller reenciphered under the CPACF wrapping key for direct usage in a CPACF encryption instruction.

BM z14/z14 ZR1

The IBM z Systems z14 was announced on July 17, 2017 (117-044) and the IBM z Systems z14 Model ZR1 was announced on April 10, 2018 (118-018). This processor has made significant performance enhancements to the CP Assist for Cryptographic Function (CPACF) over previous generations of z Systems processors. To build on these performance enhancements a new Crypto Express6S (CEX6S) adapter has been designed exclusive to the z14/z14 ZR1 processor. As with the prior crypto adapter support, the CEX6S adapter can be configured as an accelerator or as an IBM Common Cryptographic Architecture (CCA) coprocessor (this is the default) or IBM Enterprise Public-Key Cryptography Standards (PKCS) #11 (EP11) coprocessor. The performance enhanced cryptographic features of the CPACF and CEX6S allow pervasive encryption to encrypt/decrypt data in flight and at rest with minimal overhead.

CP Assist for Cryptographic Function

With the z14/z14 ZR1, the CPACF is enhanced to support pervasive encryption to provide faster encryption and decryption than previous servers. For every Processor Unit defined as a Central Processor (CP) or an Integrated Facility for Linux (IFL) it offers the following enhancements over z13:

- Reduced overhead on short data (hashing and encryption)
- Up to 4x throughput for AES
- New hashing algorithms, e.g. SHA-3
- Support for authenticated encryption (combined encryption and hashing, e.g. AES-GCM)
- True random number generator (e.g. for session keys)

Crypto Express6S (z14/z14 ZR1 exclusive)

Crypto Express6S represents the newest generation of cryptographic features. Cryptographic performance improvements with new Crypto Express6S (FC #0893) allow more data to be securely transferred across the Internet. Crypto Express6S is designed to complement the cryptographic capabilities of the CPACF. It is an optional feature of the z14/z14 ZR1 server generation.

The Crypto Express6S feature is designed to provide granularity for increased flexibility with one PCIe adapter per feature. Although installed in the PCIe I/O drawer, Crypto Express6S features do not perform I/O operations. That is, no data is moved between the CPC and any externally attached devices. For availability reasons, a minimum of two features is required.

The z14/z14 ZR1 servers allow sharing of a cryptographic coprocessor across 85 domains (the maximum number of LPARs on the system for z14/z14 ZR1 is 85).

The Crypto Express6S is a state-of-the-art, tamper-sensing, and tamper-responding programmable cryptographic feature that provides a secure cryptographic environment. Each adapter contains a tamper-resistant hardware security module (HSM). The HSM can be configured as a Secure IBM CCA coprocessor, as a Secure IBM Enterprise PKCS #11 (EP11) coprocessor, or as an accelerator:

- A Secure IBM CCA coprocessor is for secure key encrypted transactions that use CCA callable services (default).
- A Secure IBM Enterprise PKCS #11 (EP11) coprocessor implements an industry standardized set of services that adhere to the PKCS #11 specification v2.20 and more recent amendments. This new cryptographic coprocessor mode introduced the PKCS #11 secure key function.
- An accelerator for public key and private key cryptographic operations is used with Secure Sockets Layer/Transport Layer Security (SSL/TLS) acceleration.

The Crypto Express6S is designed to meet these cryptographic standards, among others:

- FIPS 140-2 Level 4

- Common Criteria EP11 EAL4
- ANSI 9.97
- Payment Card Industry (PCI) HSM
- German Banking Industry Commission (GBIC), (formerly DK, Deutsche Kreditwirtschaft)

The Crypto Express6S coprocessor with CCA 6.0 is designed to comply with the Payment Card Industry (PCI) Pin Transaction Security (PTS) Hardware Security Module (HSM) standard, Version 3.0, dated June 2016 (PCI-compliant mode). PCI security standards are developed by the Payment Card Industry Security Standards Council to help ensure security in the payment card industry with guidance and direction to HSM vendors to help meet the security needs of the financial payments industry.

The requirements in PCI PTS HSM standards are intended to enhance security for operations that process sensitive data with requirements in key management, HSM API functions, device physical security, controls during manufacturing and delivery, device administration, and a number of other areas.

The Crypto Express6S manufacturing and delivery processes are enhanced with IBM z14/z14 ZR1 to comply with PCI PTS HSM and with CCA 6.0 introduces several new capabilities both for PCI-HSM compliance mode and for general use:

- A new derived key hierarchy so that PCI-HSM compliance-tagged key tokens may be used alongside existing keys and services in a nondisruptive fashion -- with existing master keys.
- Nondisruptive transition to PCI-HSM mode: Using TKE 9.0, a domain of the Crypto Express6S coprocessor with CCA 6.0 may be placed in PCI PTS HSM compliant mode with no disruption to other domains or to normal/legacy services using the domain that is moved to PCI-HSM compliant mode.
- Secure Audit Log hosted from the Crypto Express6S coprocessor with CCA 6.0. Required by the PCI PTS HSM standard, this audit log covers all administrative actions and is managed by TKE 9.0. The new audit log is nondisruptive to normal application processing for domains where it is active.
- Secure public key infrastructure: The Crypto Express6S coprocessor with CCA 6.0 adds native X.509 certificate support including PKCS #10 certificate request generation through a new PKI hosted from the coprocessor. Trust chain certificates are managed via TKE 9.0.
- Migration planning assistance through active application reporting. The Crypto Express6S coprocessor with CCA 6.0 can report in real time what operations and keys will need attention if they are planned for use with PCI-HSM tagged keys. Report details and activity depend on host access library/operating system configuration.
- CPACF exportable AES cipher key support added for AES cipher keys created using new options in CCA 6.0.
- IF the TKE is used for managing your CCA card in normal mode, TKE 9.0 is required.
- TKE 9.0 is required to manage CCA domains in imprint and pci-compliant

mode. All CCA domains are initially in normal mode.

IBM z13 / IBM z13s

The IBM z Systems z13 was announced on January 14, 2015 (115-001) and the z Systems z13s was announced on February 16, 2016 (116-002). The z13/z13s continues to use CP Assist for Cryptographic Function (CPACF) but the CPACF has been redesigned, providing significant performance enhancements over the previous processors. New on the z13/z13s are the Crypto Express5S (CEX5S) cards. These cards also have been designed to have significant performance improvements over the previous Crypto Express cards. The Crypto Express5S cards are exclusive to the z13/z13s processors. The Crypto Express4S cards will not be available on the z13/z13s processors either as a net new feature or carry forward.

CP Assist for Cryptographic Function

The CPACF has been redesigned from the “ground up” for the z13/z13s processors. There are significant performance enhancements over the previous processors. These include a reduction in overhead for coprocessor start/end, cache effects and enhanced performance for large blocks of data resulting in increased throughput for AES, TDES and SHA processing. One coprocessor is dedicated for data compression and encryption functions for each core. The compression unit is integrated with the CP assist for cryptographic function (CPACF), benefiting from combining (or sharing) the use of buffers and interfaces. The CPACF continues to provide clear and protected symmetric key cryptography and hashing functions. Symmetric algorithms include DES, TDES and AES. DES uses single length (8-byte) keys, while TDES can use single, double (16-byte) or triple (24- byte) length keys. The CPACF supports AES keys of 128-, 192- or 256-bit lengths.

There are no changes to the hashing algorithms between the z13/z13s and the zEC12/zBC12 but the execution performance of the hashing algorithms has been greatly improved. For the z13/z13s processors, hashing algorithms are 3.5 times faster than on the zEC12/zBC12 processors. Hashing algorithms SHA-1 and SHA-2 (SHA-224, SHA-256, SHA-384 and SHA-512) continue to be supported in the CPACF hardware.

Crypto Express5S (z13/z13s exclusive)

The Crypto Express5S feature (FC 0890) is an optional z13/z13s exclusive feature and resides in the Peripheral Component Interconnect Express Gen 3 (PCIe Gen 3) I/O drawer. Each feature has one PCIe cryptographic adapter. This feature provides a secure programming and hardware environment on which crypto processes are run. Each cryptographic coprocessor includes a general-purpose processor, non-volatile storage, and specialized cryptographic electronics. The Crypto Express5S feature provides tamper-sensing and tamper-responding, high-performance cryptographic operations.

The Crypto Express5S card has added L2 Cache, new Crypto ASIC and processor upgrade. These enhancements have doubled the performance over the previous generation Crypto Express4S card.

Each Crypto Express5S PCI Express adapter can be in one of these configurations:

- Secure IBM CCA coprocessor (CEX5C) for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification. This configuration includes secure key functions. It is optionally programmable to deploy more functions and algorithms by using UDX.

- Secure IBM Enterprise PKCS #11 (EP11) coprocessor (CEX5P) implements an industry-standardized set of services that adhere to the PKCS #11 specification V2.20 and more recent amendments. It was designed for extended FIPS and Common Criteria evaluations to meet public sector requirements.

  A TKE workstation is required to support the administration of the Crypto Express5S when it is configured in EP11 mode.

- Accelerator (CEX5A) for acceleration of public key and private key cryptographic operations that are used with SSL/Transport Layer Security (TLS) processing.

Greater than 16 Domain support:

z13s has support for up to 40 LPARs and the z13 has support for up to 85 LPARs. The z Systems crypto architecture was designed to support 16 domains (which matched the LPAR maximum at the time). Prior to z13 and z13s, in customer environments where the number of LPARs was larger than 16, crypto workload separation could be complex. These customers had to map a large set of LPARs to a small set of crypto domains.

Now, in z13s and z13, with the adjunct processor (AP) extended addressing (APXA) facility that is installed, the z Systems crypto architecture can support up to 256 domains in an AP. As such, the Crypto Express cards are enhanced to handle 256 domains, and the z Systems firmware provides up to 40 (on z13s) respectively 85 (on z13) domains to customers (to match the current LPAR maximum). Customers have the flexibility of mapping individual LPARs to unique crypto domains or continuing to share crypto domains across LPARs.

Here are the requirements to support 40 respectively 85 domains:

Hardware requirements:

- z13s and Crypto Express5S with CCA V5.2 firmware
- z13 and Crypto Express5S with CCA V5.0 or above firmware

Software requirements:

- z/OS V2.2
- z/OS V2.1 and z/OS V1.13 with the Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77B0)
- Also available with HCR7780, HCR7790, HCR77A0, and HCR77A1 (previous WDs with PTFs)
- z/VM V6.2 and Version 6.3 with PTFs for guest use

Standards supported on the Crypto Express5S

DES/TDES w DES/TDES MAC/CMAC:

The Data Encryption Standard is a widespread symmetrical encryption algorithm. DES and also the double-length and triple length key DES (TDES) today is considered to be not sufficiently secure for many applications and has been replaced by the Advanced Encryption Standard (AES) as the official US standard, but it is still used in the industry, together with the Message Authentication Code (MAC) and the Cipher-Based Message Authentication Code (CMAC) for verifying the integrity of messages.

AES, AESKW, AES GMAC, AES GCM, AES XTS mode, CMAC

The Advanced Encryption Standard (AES) replaced DES as the official US standard in October 2000. Also the enhanced standards for AES Key Wrap (AESKW), the AES Galois Message Authentication Code (AES GMAC) and Galois/Counter Mode (AES GCM), as well as the XEX-based tweaked-codebook mode with ciphertext stealing (AES XTS) and also CMAC are supported.

MD5, SHA-1, SHA-2 (224, 256, 384, 512), HMAC

The Secure Hash Algorithm (SHA-1 and the enhanced SHA-2 for different block sizes) as well as the older message-digest (MD5) algorithm and the advanced keyed-hash message authentication code (HMAC) are used for verifying both the data integrity and the authentication of a message.

Visa Format Preserving Encryption (VFPE)

A method of encryption where the resulting cipher text has the same form as the input clear text, developed for usage with credit cards.

RSA (512, 1024, 2048, 4096)

RSA was been published in 1977 and was named with the initial letters of the surnames of its authors Ron Rivest, Adi Shamir and Leonard Adleman. It is widely used asymmetric public-key algorithm, which means that the encryption key is public while the decryption key is kept secret. It is based on the difficulty of factoring the product of two large prime numbers. The number describes the length of the keys.

ECDSA (192, 224, 256, 384, 521 Prime/NIST)

Elliptic Curve Cryptography (ECC) is a family of asymmetric cryptographic algorithms based on the algebraic structure of elliptic curves. ECC can be used for encryption, pseudo-random number generation and digital certificates. The Elliptic Curve Digital Signature Algorithm (ECDSA) Prime/NIST method is used for ECC digital signatures which are recommended for government use by the National Institute of Standards and Technology (NIST).

ECDSA (160, 192, 224, 256, 320, 384, 512 BrainPool)

ECC Brainpool is a workgroup of companies and institutions which engage on developing ECC algorithms. The ECDSA algorithms recommended by this group are supported.

ECDH (192, 224, 256, 384, 521 Prime/NIST)

Elliptic curve Diffie–Hellman (ECDH) is an asymmetric protocol used for key agreement between two parties using ECC based private keys. The recommendations by NIST are supported.

ECDH (160, 192, 224, 256, 320, 384, 512 BrainPool)

ECDH according to the Brainpool recommendations.

Montgomery Modular Math Engine

The Montgomery Modular Math Engine is a method for fast modular multiplication. Many crypto systems like RSA and Diffie-Hellman key Exchange can use this method.

RNG (Random Number Generator)

The generation of random numbers for cryptographic key generation is supported.

PNG (Prime Number Generator)

Also is the generation of prime numbers.

Clear Key Fast Path (Symmetric and Asymmetric)

That mode of operations gives a direct hardware path to the cryptographic engine and provides very high performance for public-key cryptographic functions.

IBM zEnterprise EC12 (zEC12) / IBM zEnterprise BC12 (zBC12)

The IBM zEnterprise EC12 (zEC12) was announced on August 28, 2012 (112-155) followed by the IBM zEnterprise BC12 (zBC12) announcement on July 23, 2013 (113-121). Both processors continue to use the CP Assist for Cryptographic Function (CPACF) that was available on earlier machines.

The Crypto Express4S is a new feature introduced with this processor and is exclusive to the zEC12/zBC12 processors. It contains the latest cryptographic function designed to complement the cryptographic functions of CPACF. The Crypto Express3 card is still available on the zEC12/zBC12 as a carry forward feature from the z196/z114.

CP Assist for Cryptographic Function

The CPACF continues to provide clear and protected symmetric key cryptography and hashing functions. Symmetric algorithms include DES, TDES and AES. DES uses single length (8-byte) keys, while TDES can use single, double (16-byte) or triple (24-byte) length keys. The CPACF supports AES keys of 128-, 192- or 256-bit lengths.

There are no changes to the hashing algorithms between the z196/z114 and the zEC12. Hashing algorithms SHA-1 and SHA-2 (SHA-224, SHA-256, SHA-384 and SHA-512) continue to be supported in the CPACF hardware.

The CPACF also provides the ability to generate a random number via a pseudo-random number generator.

On the zEC12/zBC12 each CP has its own CPACF available.

Crypto Express4S (zEC12/zBC12 exclusive)

Crypto Express4S resides in the Peripheral Component Interconnect Express Generation 2 (PCIe Gen 2) I/O drawer, a native PCIe Gen 2 environment that was first introduced in July 2011. The Crypto Express4S has been designed for port granularity providing increased flexibility with one PCI Express cryptographic adapter per feature.

Crypto Express4S remains a tamper-sensing and tamper-responding, programmable cryptographic feature providing a secure cryptographic environment. Each adapter can be configured through the HMC as a Secure IBM Common Cryptographic Architecture (CCA) coprocessor, as a Secure IBM Enterprise PKCS #11 (EP11) coprocessor or as an accelerator.

When the Crypto Express4S is configured as an IBM CCA coprocessor, the card provides data confidentiality, message integrity, financial functions and key security and integrity. The coprocessor supports secure key DES, TDES and AES encryption as well as PKA encryption. Master keys must be loaded to enable this functionality. The coprocessor supports PIN processing for financial APIs, a random number generator and it provides the ability to create, delete, update and store DES, TDES, AES and PKA keys (both RSA and ECC keys). The coprocessor functionality includes ECC key generation and key management along with digital signature generation and verification. This functionality was extended to include the Elliptic Curve Diffie-Hellman (ECDH) algorithm. In addition to generating and managing RSA and ECC keys, the coprocessor performs encryption operations using these keys.

When the Crypto Express4S is configured as an accelerator, the card is a clear key device that only supports three cryptographic APIs, all associated with System SSL handshakes. The three APIs are public key operations that rely on very large prime numbers and are very expensive in terms of CPU utilization when implemented in software.

The Crypto Express4S has improved the wrapping key strength to comply with cryptographic standards, including ANSI X9.24 Part 1 and PCI-HSM, where a key must not be wrapped with a key weaker than itself. With this release, CCA allows you to configure the coprocessor to ensure that your system meets these key wrapping requirements. It can be configured to respond in one of three ways when a key is wrapped with a weaker key: ignore weak wrapping (the default, which is consistent with earlier crypto cards), complete the requested operation but return a warning message, or prohibit weak wrapping altogether. This stronger wrapping also applies to keys stored in the CKDS, so the CEX4S can support a 24-byte DES-MK.

AES key-encrypting keys (KEKs) can be used to wrap TDES keys. All of the TDES key wrapping functions are still available, but a parallel set of AES wrapping functions are now available for use. This provides stronger security for key material.

Diversified Key Generation Cipher Block Chaining (CBC) is used during the Europay, Mastercard and Visa (EMV) smart card personalization process. Session keys are derived and then used to secure messages to the EMV cards. Some EMV card personalization specifications require the use of TDES CBC mode to derive these session keys. This enhancement adds that capability to the existing key derivation options in CCA.

EMV support has also been enhanced to return the Initial PIN Encrypting Key (IPEK) to a calling application. An IPEK is the initial key that is loaded into a point-of-sale (POS) terminal before it is deployed for use. This is only for terminals that will use the DUKPT key protocol. CCA has added a function that allows the HSM to securely derive an IPEK and return it to the application program in an encrypted key token, which can then be securely installed in a POS terminal.

Remote Key Export (RKX) provides stronger key wrapping using a proprietary enhanced mode algorithm. This includes the ability to set a default preference for the wrapping method to be used as well as options to override the CCA default functions.

Several commonly used UDX’s have been incorporated into the IBM Common Cryptographic Architecture on the Crypto Express4S cards. As described earlier in this document a UDX allows a customer to execute custom code inside the tamper resistant boundary of the HSM. There are several functions that have been requested by multiple customers in a UDX:

- Recover PIN from Offset
- Symmetric Key Export with Data
- Authentication Parameter Generate

These functions will now be available to all customers without the need to install and maintain a UDX.

Derived Unique Key Per Transaction (DUKPT) provides a method in which a separate key is used for each transaction or message sent from a device. This is compliant with the standards described in ANSI X9.24 Part 1: "Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques". A key is derived from a base key that is initially loaded into the device. This newly created key will be used for a single transaction or message and erased when the communication has completed. The cycle continues with another new key being derived from the base key for the next transaction or message which will be erased when that communication has completed. Since this methodology uses a derived key, an attacker could only acquire information for a single transaction and not for any past or future transactions. DUKPT for PIN keys has been supported for some time, but on the CEX4S it is extended to Message Authentication and data keys.

Secure Cipher Text Translate2 (CTT2) is a new data encryption service that takes as input data encrypted with one key and returns the same data encrypted under a different key. This service has the advantage that it provides the ability to securely change the encryption key for cipher text without exposing the intermediate plain text. The decryption of data and re-encryption of data happens entirely inside the secure module on the Crypto Express4S feature.

The standards for Random Number Generation have been updated and strengthened. The Crypto Express4S coprocessor function has been updated to support methods compliant with these new standards. Now, random number generation in the Crypto Express4S feature when defined as a coprocessor conforms to the Deterministic Random Bit Generator (DRBG) requirements defined in NIST Special Publication 800-90/90A, using the SHA-256 based DBRG mechanism.

Changes have been made to the CCA application programming interface (API) to help improve support of payment card applications for American Express EMV cards. The Transaction Validation service is used to generate and verify American Express card security codes (CSCs). This release adds support for the American Express CSC version 2.0 algorithm. The PIN Change/Unblock verb is used for PIN maintenance. It prepares an encrypted message portion for communicating an original or replacement PIN for an EMV smart card. The verb embeds the PINs in an encrypted PIN block using information supplied.

A new configuration option is available when defining the Crypto Express4S feature as a coprocessor. This option is called IBM Enterprise Public-Key Cryptography Standards (PKCS) #11 (or simply EP11) mode. In EP11 mode, keys now can be generated and securely wrapped under the EP11 Master Key. The secure keys never leave the secure coprocessor boundary unencrypted. This firmware is designed to meet the rigorous FIPS 140-2 Level 4 and Common Criteria EAL 4+ certifications. The Crypto Express4S with EP11 configuration is known as CEX4SP. A Trusted Key Entry (TKE) workstation is required for management of the Crypto Express4S when defined as an EP11 coprocessor.

PKCS #11 v2.1 Probabilistic Signature Scheme (PSS) is the latest algorithm to be used in digital signature applications with enhanced security characteristics over prior digital signature algorithms.

The EP11 supported Key algorithms:

- Diffie-Hellman: 1024-bit, 2048-bit
- Elliptic Curve Diffie-Hellman
- National Institute of Standards and Technology (NIST): 192-bit, 224-bit, 256-bit, 384-bit, 521-bit
- Brainpool: 160-bit, 192-bit, 224-bit, 256-bit, 320-bit, 384-bit, 512- bit

Offload Generation of Domain Parameters are necessary inputs for the creation of Digital Signature Algorithm (DSA) and Diffie-Hellman key pairs. This enhancement is designed to provide the ability to offload the task of generating domain parameters to EP11. This will help reduce the consumption of CPU resources. These domain parameters can then be used to create key pairs.

When the Crypto Express4S feature is configured as an accelerator it is used for System SSL handshakes processing. When configured as an accelerator only three instructions are supported: PKA Encrypt, PKA Decrypt and Digital Signature Verification. With a limited number of instructions, processing on the accelerator is very fast. These three APIs are public key APIs that rely on very large prime numbers and are very expensive in terms of CPU utilization when implemented in software. The CEX4A provides only limited cryptographic function, but it supports very high volume PKA workloads.

The zEC12/zBC12 continues to support Elliptic Curve Cryptography (ECC). This public key algorithm has a much shorter key length and therefore requires less computing resources than RSA keys. This technology is appropriate in resource-constrained environments such as mobile phones and smart cards which may have limited power for processing longer RSA keys. Additional standards for the banking and finance industry, such as ANSI and ISO, are also supported by the zEC12/zBC12.

Crypto Express3 (Carry forward only)

Crypto Express3 is an optional feature on the zEC12/zBC12 and only available when carried forward from a z196, z114 or z10. It cannot be ordered on a zEC12/zBC12 processor. The minimum number of carry forward features is two with a maximum support of eight features. Each Crypto Express3 feature holds two PCI Express cryptographic adapters. The Crypto Express3 (CEX3) contains two cryptographic engines, which can be configured independently from the HMC as either a coprocessor or accelerator. The Crypto Express3 feature on the zEC12 has the same functionality as found on the z196/z114 processors.

As stronger algorithms and longer keys become increasingly common, security requirements dictate that these keys must be wrapped using key encrypting keys (KEKs) of sufficient strength. This feature added support for AES key encrypting keys. These AES wrapping keys have adequate strength to protect other AES keys for transport or storage. The new AES key types are EXPORTER, IMPORTER and for use in the encryption and decryption services, CIPHER. These new AES key types may use a variable length key token. New APIs have been added or modified to manage and use these new keys.

ANSI TR-31 defines a method of cryptographically protecting TDES cryptographic keys and their associated usage attributes. CCA has added functions that can be used to import and export CCA TDES keys in TR-31 formats. These functions are designed primarily as a secure method of wrapping TDES keys for improved and more secure key interchange between CCA and non-CCA devices and systems.

To help avoid a decimalization table attack to learn a personal identification number (PIN), a solution is now available in the CCA to thwart this attack by protecting the decimalization table from manipulation. PINs are most often used for automated teller machines (ATMs) but are increasingly used at point-of sale, for debit and credit cards. With this support, the PIN decimalization table is protected inside the secure tamper resistant boundary of the card.

The CEX3 now supports Optimal Asymetric Encryption Padding with RSA Encryption. RSA-OAEP is a public-key encryption scheme or method of encoding messages and data in combination with the RSA algorithm and a hash algorithm.

Elliptic Curve Cryptography (ECC) Digital Signature Algorithm support is capable of providing digital signature functions and key agreement functions. This new CCA function provides ECC key generation, key management and digital signature generation and verification functions compliant with the ECDSA method described in ANSI X9.62 “Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)”. ECC uses keys that are shorter than RSA keys for equivalent strength-per-key-bit. RSA is impractical at key lengths with strength-per-key-bit equivalent to AES-192 and AES-256.

The CCA has been extended to include the Elliptic Curve Diffie Hellman (ECDH) algorithm. Elliptic Curve Diffie Hellman (ECDH) is a key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. This shared secret may be directly used as a key, or to derive another key which can then be used to encrypt subsequent communications using a symmetric key cipher such as AES KEK.

Licensing: Elliptical Curve Cryptography technology (ECC) is delivered through the machine's Machine Code (also called Licensed Internal Code, or LIC), and requires license terms in addition to the standard IBM License Agreement for Machine Code (LMC). These additional terms are delivered through the LMC's Addendum for Elliptical Curve Cryptography. This ECC Addendum will be delivered with the machine along with the LMC when a cryptography feature is included in the zEnterprise CPC order, or when a cryptography feature is carried forward as part of an MES order into zEnterprise CPC.

z196/z114

The z196 was announced on July 22, 2010 (110-170) and was followed by the announcement of the z114 on July 12, 2011 (111-136). The zEnterprise systems continue to use the CP Assist for Cryptographic Function (CPACF) that were available on earlier machines, but with additional capabilities. These processors continue to use the Crypto Express3 (CEX3) that was announced in October, 2009 (109-678) but have additional functionality over the z10 machines.

CP Assist for Cryptographic Function

The CPACF provides clear and protected key cryptography and hashing functions on the z196/z114. This crypto engine provides support for clear key, symmetric algorithms DES, TDES and AES. DES uses single length (8-byte) keys, while TDES can use single, double (16-byte) or triple (24-byte) length keys. The CPACF also supports AES keys of 128-, 192- or 256-bit lengths. This encryption support is provided by assembler instructions, documented in the Principles of Operations manual.

The CPACF on the z196/z114 continues support for the Protected Key function that was introduced with the Crypto Express3 and the CPACF on the z10 machines.

The z196/z114 also supports SHA-1, SHA-256 and SHA-512 hashing algorithms in the CPACF hardware. ICSF extends that hashing support to the full suite of SHA-2 algorithms (adding SHA-224 and SHA-384).

On the z196/z114, the CPACF provides new instructions for symmetric encryption with cipher feedback, and a new operand for the Compute Intermediate and Compute Last Message Digest instructions.

The CPACF also provides the ability to generate a random number via a pseudo-random number generator.

On the z196/z114, as well as the z10, a CPACF is shared by two general purpose engines.

Crypto Express3 / Crypto Express3-1P

The Crypto Express3 (CEX3) and Crypto Express3-1P (CEX3-1P) are the only secure key devices supported on the z196/z114. First announced in October, 2009, this device is very similar to the CEX2 in terms of functionality, but provides several enhancements in terms of performance, reliability and availability. The CEX3-1P is identical to the CEX3 in functionality but only has a single engine versus two on the CEX3 and is only supported on the z114, not the z196. These functions are only available via the ICSF APIs.

The CEX3 has duplicate symmetric processors available which are used to run operations in parallel, the results of which are compared to ensure the integrity of the cryptographic operation. The CEX3 has implemented dynamic power management to maximize RSA performance. The card will monitor the heat being generated on the card and enable or disable RSA engines to maximize performance and throughput within the limits of the tamper responding hardware.

The CEX3 uses the PCI-E bus versus the PCI-X bus on the CEX2, which is one factor in improving performance. The CEX3 also has more (4MB) battery backed memory (BBRAM) than the CEX2.

The Crypto Express3, like the Crypto Express2, contains two cryptographic engines, which can be configured from the HMC as either a coprocessor or accelerator. When configured as a coprocessor, the CEX3C provides all of the cryptographic function described in the Cryptographic Functions section on page 1 (data confidentiality, message integrity, financial functions and key security and integrity). As with the CEX2C, the CEX3C supports secure key DES, TDES and AES encryption as well as PKA encryption. Master keys must be loaded to enable this functionality. The CEX3 supports PIN processing for financial APIs, a random number generator and it provides the ability to create, delete, update and store DES, TDES, AES, PKA and ECC keys. The CEX3C also supports PKA encryption, although not at the same volume as when configured as an accelerator (CEX3A).

Performance on the coprocessor depends on which functions are being executed and depending on the mix it can support from 1800 to 3200 operations per second.

When configured as an accelerator, no master key is loaded and it is a clear key device that only supports three cryptographic APIs, all associated with System SSL handshakes.

The three APIs are public key APIs that rely on very large prime numbers and are very expensive in terms of CPU utilization when implemented in software. When configured as an accelerator the CEX3A can support approximately 6000 handshakes per second providing significant relief in CPU utilization. So, the CEX3A provides only limited cryptographic function, but it supports very high volume PKA workloads.

For availability reasons, if a CEX3 feature will be installed, at least two features must be ordered, to provide redundancy, and a maximum of eight can be installed (depending on what other devices are in the I/O cage). The cryptographic functions on the CEX3 are only available via the ICSF APIs.

New on the CEX3 on the z196/z114 is support for Concurrent Driver Upgrade and Concurrent Patch Apply. With this support, segment 3 updates to the card (which provide CCA or the Common Cryptographic Architecture) can be performed without any performance impact or outage. Some levels of CCA or hardware changes still require the crypto coprocessor to be varied offline and back online to get the microcode loaded onto the card.

With the July 12 announcement of z114 there were several new enhancements to the Crypto Express3 and Crypto Express3 – 1P cards exclusive to z196 and z114 processors.

As stronger algorithms and longer keys become increasingly common, security requirements dictate that these keys must be wrapped using key encrypting keys (KEKs) of sufficient strength. This feature adds support for AES key encrypting keys. These AES wrapping keys have adequate strength to protect other AES keys for transport or storage. The new AES key types are EXPORTER, IMPORTER and for use in the encryption and decryption services, CIPHER. These new AES key types use a variable length key token. New APIs have been added or modified to manage and use these new keys.

ANSI TR-31 defines a method of cryptographically protecting Triple Data Encryption Standard (TDES) cryptographic keys and their associated usage attributes. CCA has added functions that can be used to import and export CCA TDES keys in TR-31 formats. These functions are designed primarily as a secure method of wrapping TDES keys for improved and more secure key interchange between CCA and non-CCA devices and systems.

To help avoid a decimalization table attack to learn a personal identification number (PIN), a solution is now available in the CCA to thwart this attack by protecting the decimalization table from manipulation. PINs are most often used for automated teller machines (ATMs) but are increasingly used at point-of sale, for debit and credit cards.

RSA Encryption Scheme – Optimal Asymmetric Encryption Padding (RSA OAEP) is a public-key encryption scheme or method of encoding messages and data in combination with the RSA algorithm and a hash algorithm. Currently, the Common Cryptographic Architecture and z/OS Integrated Cryptographic Service Facility (ICSF) provide key management services supporting the RSA OAEP method using the SHA-1 hash algorithm, as defined by the Public Key Cryptographic standards (PKCS) #1 V2.0 standard. These services can be used to exchange AES or DES/TDES key values securely between financial institutions and systems. However, PKCS#1 V2.1 extends the OAEP method to include the use of the SHA-256 hashing algorithm to increase the strength of the key wrapping and unwrapping mechanism. The CCA key management services have been enhanced so that they can use RSA OAEP with SHA-256 in addition to RSA OAEP with SHA-1.

The Common Cryptographic Architecture has been extended to include the Elliptic Curve Diffie Hellman (ECDH) algorithm. Elliptic Curve DiffieHellman (ECDH) is a key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. This shared secret may be directly used as a key, or to derive another key which can then be used to encrypt subsequent communications using a symmetric key cipher such as AES KEK.

z10 Enterprise Class/z10 Business Class

The z10 Enterprise Class machine (z10 EC) was announced on February 26, 2008 (108-154). Additional cryptographic capabilities for the z10 EC were announced along with the z10 Business Class (z10 BC) machine on October 21, 2008 (108-754). The October,

2009 announcement (109-678) of the z10 GA3 introduced support for the new PCI card, the Crypto Express3 which works with the CPACF to provide the new protected key function. The z10 crypto hardware supports several new crypto functions as well as making it easier to manage the crypto devices. There are three crypto hardware devices available on the z10: the CP Assist for Cryptographic Function (CPACF) is integrated into the PU in the host, and the Crypto Express2 and Crypto Express3 are PCI devices installed in the I/O cage.

CP Assist for Cryptographic Function

The CPACF provides clear key cryptography and hashing functions on the z10. This crypto engine provides support for clear key, symmetric algorithms DES, TDES and AES. DES uses single length (8-byte) keys, while TDES can use single, double (16-byte) or triple (24-byte) length keys. The z10 CPACF supports AES keys of 128-, 192- or 256-bit lengths. Support for AES-192 and AES-256 bit keys and SHA-512 are new on the z10 (i.e. not available on the z9 or earlier) and are referred to as ‘Enhancements to CP Assist for Cryptographic Function’.

The z10 also supports SHA-1, SHA-256 and SHA-512 hashing algorithms in the CPACF hardware. ICSF extends that hashing support to the full suite of SHA-2 algorithms (adding SHA-224 and SHA-384). The National Institute of Standards and Technology (NIST) recommends that users migrate to the stronger SHA-2 family of hash functions for digital signature applications, however the SHA-1 algorithm is still widely used and required for certain protocols and applications.

With the November, 2009 MCL (Driver 79) the CPACF supports protected key operations. This microcode also provides a new assembler instruction for use with protected keys. The availability of this new instruction for protected keys can be enabled or disabled via the Support Element.

On the z10, the CPACF is available to every processor unit (CP, IFL, zIIP or zAAP).

Crypto Express2 / Crypto Express2-1P

The Crypto Express2 (CEX2) on the z10 is a PCI feature, physically identical to the Crypto Express2 on the z9, z990 and z890, however the microcode on the z10 provides several new capabilities.

The CEX2 feature includes two cryptographic processors, each of which can be configured independently as either a cryptographic coprocessor (the default) or as a cryptographic accelerator. The Crypto Express2-1P (CEX2-1P) is identical to the Crypto Express2 in functionality however it only has a single cryptographic processor and is only supported on the BC model. For availability reasons, if a CEX2 feature will be installed, at least two features must be ordered and a maximum of eight can be installed (depending on what other devices are in the I/O cage). On the BC model those two features can be two CEX2-1Ps or two CEX2s or one of each, but two features are required to provide redundancy. The cryptographic functions on the CEX2 are only available via the ICSF APIs.

When the CEX2 is configured as an accelerator (CEX2A), it is a clear key device that only supports three cryptographic APIs. The three APIs are public key APIs that rely on very large prime numbers and are very expensive in terms of CPU utilization when implemented in software. When configured as an accelerator the CEX2A can support approximately 2000 handshakes. Like the CEX3A, it provides only limited cryptographic function, but supports very high volume PKA workloads.

When the CEX2 is configured as a coprocessor (CEX2C) it is a secure key device that requires a master key be loaded. As a coprocessor it supports all the crypto functions identified at the beginning of this article: data confidentiality, message integrity, financial functions and key management. The CEX2 supports secure key DES and TDES encryption and PKA encryption and with Driver 76, announced on October 21, 2008 the CEX2 coprocessor supports AES secure key encryption. This new secure key support requires a new master key to be loaded, called the AES-MK. The AES-MK is used to protect AES data keys. The SYM-MK is now known as the DES-MK, and continues to protect secure DES/TDES operational keys. While the CEX2C supports the same three APIs as the accelerator, it can only drive about 1000 APIs per second. The CEX2C also supports PIN processing for financial APIs, a random number generator and it provides the ability to create, delete, update and store DES, TDES, AES and PKA keys.

The other new hardware support announced in October 2008 is the ability to use 13- through 19-digit PANs when calculating the VISA Card Verification Value (CVV) or

Mastercard Card Verification Code (CVC). Prior to this announcement, the hardware supported the early industry standards of 13-digit, 16-digit and 19-digit Personal Account Numbers however with the CEX2C on the z10, the PAN can be from 13- to 19-digits in length to meet new industry standards.

The CEX2C on the z10 includes support for several new functions that were made available on the z9 via new microcode. The CEX2C includes support for RSA keys up to 4096-bits for key management operations, digital signatures and query services. Retained keys for key management functions are not supported on the CEX2C on the z10.

The CEX2C supports ISO Format 3 PIN blocks as defined in the ISO 9564-1 standard. This PIN format provides added security by padding the PIN block with random data before it is encrypted, rather than padding with predictable values as used in other formats. The CEX2C also provides the ability to generate random numbers up to 8192 bytes in length.

On the z10 (and the z9), a crypto engine can be dynamically changed (from accelerator to coprocessor or coprocessor to accelerator) via the Hardware Management Console (HMC) without taking an outage of ICSF, the operating system or the LPAR. This means that as workload changes you can reconfigure the crypto devices to take advantage of the performance and throughput characteristics of each without incurring an outage to implement the change

In addition, the z10 provides the ability to dynamically add (and remove crypto devices) in an LPAR. For a crypto engine to be used by an LPAR, that engine must be defined in the Candidate List of the LPAR Activation Profile. (Adding the engine to the list makes it a 'Candidate' to be brought online while the LPAR, and operating system, is active.) Prior to the z10, changes to the Activation Profile would only be picked up by a Deactivate/Activate of the LPAR, which meant you had to add these crypto devices to the candidate list even before they were installed to avoid an outage of the LPAR. The z10 provides the ability to dynamically add or remove the device from the LPAR and/or update the Activation Profile to make the change permanent. So crypto devices can be added or moved between LPARs without requiring an outage.

Crypto Express3 / Crypto Express3-1P

The Crypto Express3 (CEX3) and Crypto Express3-1P (CEX3-1P) are the newest secure key devices for the z10. Announced in October, 2009, these devices are very similar to the CEX2 in terms of functionality, but provide several enhancements in terms of performance, reliability and availability. The CEX3 uses the PCI-E bus which is expected to provide four times the performance of the PCI-X bus. The CEX3 and CEX3-1P both have duplicate processors installed which provide additional integrity over the CEX2 as the extra processors validate the results of operations. The new features also have more (4MB) Battery Backed Ram (BBRAM) than the CEX2.

The CEX3 and CEX3-1P have implemented dynamic power management to maximize RSA performance. The card will monitor the heat being generated on the card and enable or disable RSA engines to maximize performance and throughput within the limits of the tamper responding hardware.

z9 Enterprise Class/z9 Business Class

The crypto hardware architecture on the z9 is similar to the z10.

CP Assist for Cryptographic Function

The CP Assist for Cryptographic Function provides clear key and SHA functions on the z9 Business Class (BC) and z9 Enterprise Class (EC). The CPACF on the z9 provides additional functionality over the CPACF on the z890/z990, but not all of the functions available on the z10.

On the z9, the CPACF is part of every PU or processor unit (CP, IFL, zIIP, zAAP). On a 10-way machine there will be 10 CPACFs available. As on the z10, it provides synchronous cryptographic support, so when the CPACF is processing a cryptographic request, the corresponding general purpose PU is busy, and cannot be doing other work.

On the z9 machines, the CPACF provides DES/TDES and AES 128-bit clear key symmetric encryption, along with supporting the SHA-1 and SHA-256 hashing algorithms and it also provides a pseudo-random number generator. The functions are available either via native assembler instructions, or they can be invoked using the clear key APIs available through ICSF. See the Principles of Operations for the specific machine for the assembler instructions, and the ICSF Application Programmer's Guide for the APIs that are available. Support for AES-192 and AES-256 clear key is not available in the CPACF on the z9, but is provided by the ICSF software. As mentioned above, see the IBM TechDocs website for more information on using the CPACF instructions.

Crypto Express2 and Crypto Express2-1P

The Crypto Express2 feature is installed in the I/O cage on the z9, just like the z10.

The Crypto Express2 (CEX2) feature includes two cryptographic processors, and on the z9, each of those two can be configured independently as either a cryptographic coprocessor (the default) or as a cryptographic accelerator. The Crypto Express2-1P (CEX2-1P) feature has a single cryptographic processor and is supported on the z9 BC, but not the z9 EC. That single engine can be configured as either a coprocessor (the default) or as a cryptographic accelerator.

For availability, if a Crypto Express2 will be installed, at least two must be installed. On the z9 EC two of the original Crypto Express2 features must be installed. The z9 BC also requires two features, but those can be any combination of the CEX2 and the CEX2-1P.

When the CEX2 is configured as a coprocessor (CEX2C), it is a secure key device that requires a master key be loaded. The CEX2C supports secure key DES/TDES, PIN processing for financial APIs, a random number generator and it will support the generation and management of keys, including PKA keys up to 2048-bits in length. In November, 2007 the CEX2 was enhanced to provide support for 4096-bit RSA keys via new microcode. With this latest microcode and the appropriate version of ICSF these longer keys are supported for key management, digital signatures and query services. In addition, the CEX2C will support the same PKA APIs supported by the CEX2A, but it can only support about 1000 handshakes per second. With new microcode on the z9 the CEX2C also supports ISO Format 3 PIN blocks and provides a long random number generator.

In addition, the support for 13 through 19-digit PANs and secure AES key that was previously available on the z10 has been made available on the z9 CEX2C by installing new microcode. This support became available in April, 2009 and requires System Driver 67L, EC# G40942 plus MCL bundle 42B. See TechDoc TD103782, ‘z/OS: ICSF Version and FMID Cross Reference’ for the versions of ICSF which support the new hardware functionality.When the CEX2 is configured as an accelerator (CEX2A), it is a clear key device that supports the same three cryptographic PKA APIs as it supports on the z10, and at the same throughput as the z10 (approximately 3000 per second).

Trusted Key Entry Workstation

The Trusted Key Entry (TKE) product is an appliance used to provision (manage) host crypto modules on and IBM Z or LinuxONE servers. The most important configuration task is to load master keys into host crypto module domains. In many cases, the master keys must be managed according to strict polices, standards, or even laws. In many cases these polices, standards, and laws require:

- The master key must be built from a series of parts combined inside the target crypto module domain. (Split knowledge)
- Key parts must be stored in secure hardware outside the target domains. (Hardware-based master key part protection.)
- Key parts must be encrypted while in transit to a target domain. (Hardware-based master key part protection)
- Each key part must be loaded by a different individual (Dual controls)

TKE is the only product that provides compliant-level IBM Z and LinuxONE host cryptographic module management features. The TKE provides features to:

1. Managing all the administrative settings of an IBM Z or LinuxONE host crypto module. In general, you configure your host crypto modules by:
   - Creating the user’s that manage your module. You grant privilege and set limits.
   - Securely loading your master keys using compliant-level management techniques.
   - Manage the list of services you will allow your applications to use.
2. Securely collect all host crypto module administrative settings from a host crypto module on an IBM Z or LinuxONE and apply it to another module on the same or different server.
3. Allow you to treat a set of domains as if they are one. This allows you to send module-wide administrative commands to a set of modules at the same time and it allows you to send domain-specific administrative commands to a set of domains at the same time.

Compliant-level key management features are only available if you also purchase the smart card readers and smart cards feature of the TKE.

On the TKE, the customer configures a stand-alone security environment, restricting who can use the key entry application on the workstation and controlling the authority to load both operational and master keys and to manipulate the secure hardware. With the proper authorities a key officer or team of security officers can create and change master keys and operational keys. These keys can then be loaded into the host cryptographic hardware using a secure connection (relying on the Diffie-Hellman key exchange protocol) so that the key values never exist in the clear in an address space or on the network.

Beginning with TKE V5.3 and the z10, up to ten TKEs can be ordered per CEC, providing the ability to order additional TKEs for redundancy, Disaster Recovery or testing purposes.

The TKE actually incorporates two features, the hardware and the LIC (Licensed Internal Code) which includes the operating system and application software. The TKE version is closely associated with the host platforms that it will support.

The TKE is runs on an Intel platform and is the same platform as the Hardware Management Console (HMC). Each version of the TKE hardware is slightly different in terms of the configuration (DVD drive, monitor, floppy drive, etc.) and associated with each hardware feature is a version of the operating system and application (LIC). For example, the latest TKE hardware (FC #0847) includes TKE 9.0 LIC (FC #0878) and USB ports for the smart card readers and for memory sticks. FC #0847 does not support floppy drivers.

TKE 9.2

The TKE workstation is an optional feature that offers key management functions. It can be a TKE tower workstation (FC 0088) or TKE rack-mounted workstation (FC 0087) for z15-T01/z15-T02 systems to manage Crypto Express7S, Crypto Express6S, or Crypto Express5S.

TCP/IP port in the host transaction program to use AT-TLS, you must select the new check box in your TKE workstation host definition to specify you are using a TLS connection.

• TKE 9.2 can be used to exploit the following enhancements available in various releases of Common Cryptographic Architecture (CCA) firmware levels:

> – TKE 9.2 will allow you to create AES operational key parts with the PCI compliant tag turned on. You can use these parts when you load your AES operational keys, if the CCA level supports the tag.
>
> – When you display Access Control Point (ACP) tracking information, tracking interval information will be included if the CCA firmware level returns the

information. You will be able to tell when tracking was turned on, if or when tracking was turned off, and the number of times tracking was turned off and back on from the last time tracking data was cleared.

– When you display master key information, you will have new options for selecting how the verification pattern is calculated if the CCA firmware supports the ENC-0 and CMAC calculations.

• With TKE 9.2, you can now select the IBM Enterprise PKCS #11 Transport Wrapping Key Policy. This policy is used to select the EP11 transport wrapping key strength. Select this policy if you require the EP11 transport wrapping key to be a true 256-bit AES key. If the policy is selected, the transport wrapping key is derived using Diffie-Hellman Key Exchange of 521-bit Elliptic Curve (EC) public keys between the TKE and the host crypto module running IBM Enterprise PKCS #11 (EP11). You can only select this policy when:

– All your EP11 smart cards are at the minimum part level 00RY790 (Blue smart cards).

– All your EP11 smart cards are at the minimum applet version V0.6. (The minimum applet support first appeared in TKE 9.2.)

– All your host IBM Enterprise PKCS #11 modules are at API version 6.02 or later.

• TKE 9.2 has new features that simplify existing management tasks:

– You can configure your host definition so that it will automatically accept modules that are successfully authenticated. You can select the option to automatically accept modules when you create a host definition or add the option to existing host definitions through the change host function.

– The utility that allows you to copy key parts in binary files onto smart cards will allow you to select more than one file at a time. This will simplify the process of moving from binary key part files to smart card key part management.

– With any attempt to delete a role or authority from a Common Cryptographic Architecture (CCA) mode host crypto module from inside of a TKE domain group, the delete will be attempted on every module included in the group. Previously the operation would stop the first time the role or authority was not found on a module in the group.

– When TKE 9.2 detects that a Linux host supports long user IDs you will be able to enter user IDs with up to 32 characters.

– The TKE Workstation Logon Wizard includes a new step that encourages you remove excess authority from the DEFAULT role after your TKE Workstation administrator profiles have been created.

• The following are important notes about upgrading existing TKE Workstations to TKE 9.2:

– TKE workstations with feature codes 0847 and 0849 cannot be upgraded to TKE 9.2 LIC.

– TKE workstations with feature code 0080, 0081, 0085, or 0086 can be upgraded to TKE 9.2 LIC only if the TKE Workstation feature is assigned to a z14 server or later.

– You will have to buy a new local adapter crypto feature for the TKE if your TKE is at a pre-TKE 9.0 LIC level.

TKE 9.0

The TKE provides a secure, remote, and flexible method of providing Master Key Part Entry, and to remotely manage PCIe cryptographic coprocessors. Up to 10 TKE workstations can be ordered. TKE FCs #0085 and #0086 can be used to control the Crypto Express6S or Crypto Express5S cards on z14 servers. They also can be used to control the Crypto Express5S on z13 and z13s servers, and the Crypto cards on older still supported servers.

This are the enhancements for the new TKE 9.0 LIC:

Key material copy to alternate zone

TKE 9.0 allows you to copy key material from smart cards in one TKE zone to smart cards in another zone. You might have old 1024 bit strength TKE zones, and may wish to move/copy the key material in those zones into a new, stronger TKE zone. To use this new feature you create new TKE and/or EP11 smart cards on your TKE 9.0 system. You enroll the new TKE and/or EP11 smart cards in an alternate zone. This allows you to copy smart card content from a smart card enrolled in the alternate zone.

Save TKE data directory structure with files to USB

TKE data can be saved to, or restored from, removable media in the same directory structure they were found on the TKE.

Create key parts without opening a host

The TKE application now has the ability for administrators to create key parts without opening a host. This allows the key administrator to create key parts while being offline or before any hosts are defined.

New TKE Audit Log application

There is a new TKE Audit Log application available for the Privileged Mode Access ID of AUDITOR. This application provides a new, easy-to-use interface to view the TKE workstation security audit records from the TKE workstation.

Heartbeat audit record

TKE workstations cuts an audit record when the TKE boots or when no audit events have occurred during a client-configured duration of time. The record shows the serial number of the TKE local crypto adapter and indicates if the local crypto adapter has been changed since the last check.

Performance improvements for domain groups

With CCA version 5.3, depending on the size of a domain group, you may experience performance improvements when doing a Load, Set, or Clear operation from inside a domain group. For example, if you group all 85 domains on a Host Crypto Express 5, and issue a Clear New Master Key register operation, the number of commands issued to the module will drop from 85 to 1.

Secure key entry on EP11

TKE 9.0 EP11 smart card applet now supports secure key entry of EP11 master key parts.

New certificate manager for domains

Every domain will now have the ability to manage a set of parent X. 509 certificates for validating operating X.509 certificates used by applications running in the domain. The following features are related to support for the Crypto Express6S with CCA 6.0. The Crypto Express6S with CCA 6.0 is designed to meet the PCI-HSM PIN Transaction Security v3.0, 2016 standard.

Domain mode management

With CCA 6.0, individual domains are in one of the following modes:

- Normal Mode
- Imprint Mode
- Compliant Mode

Imprint and compliant mode were added to indirectly and directly meet PCI-HSM PIN Transaction Security v3.0, 2016 requirement. TKE is required to manage Host Crypto Module domains in imprint and compliant mode.

Set clock

With TKE 9.0, there is the ability to set the host crypto module's clock. The clock must be set before a domain can be placed in imprint mode.

Domain-specific Host Crypto Module Audit Log management

Domains in imprint mode or compliant mode on a Crypto Express6S maintain a domain-specific module audit log. The TKE provides a feature for downloading the audit records so they can be viewed.

Domain-specific roles and authorities

Domains in imprint mode or compliant mode on a Crypto Express6S must be managed using domain-specific roles and authorities. The TKE provides new management features for the domain-specific roles and authorities. The roles are subject to forced dual control policies which prevent roles from being able to both issue and cosign a command. Refer to the TKE

Setup PCI Environment Wizard

To simplify the management of a compliant domain, the TKE provides a setup wizard that will create a minimum set of forced dual control roles and authorities needed to manage a compliant domain.

TKE 8.1

TKE 8.1 is available to order with z13/z13s and is supported on the zEC12 and zBC12. The following is the list of new features available in TKE 8.1:

- Domain Cloning: The ability to collect data from one domain and push it to a set of domains. This is extremely valuable for deploying new domains.
- Ability to launch Coordinated Master Key roll from the TKE.
- Three new wizard-like features: Create new TKE zone, Create new Migration Zone, Configure Host Roles and Authorities.
- Operational Key Option: This allows the client to decide if operational key commands are limited to the master domain or sent all domains in the group.
- HMAC key: Support for HMAC key has been added. The key is limited to 3 specific sizes: 128, 192, and 256.
- TKE enables Save Customized Data feature. This simplifies the way that a client can save and restore client data to a TKE.
- TKE can be configured to prevent auto-logon. If configured, a password is required to “launch the Trusted Key Entry Console web application”.
- Binary Key Part File Utility: This allows the client to copy a key part from a binary file to a smart card.
- ACP Usage Information: This feature allows clients to determine which Domain Controls (Access Control Points) are actually “checked/used” on a domain. The utility allows to activate and deactivate tracking and create reports.
- Display Crypto Module Settings: This feature allows clients to build a report that

shows the settings of a crypto module.

TKE 8.0

TKE 8.0 is available to order with zEC12/zBC12 and is supported on the z13 and z13s. TKE 8.0 and greater is required to manage a Crypto Express5S host crypto coprocessor. The following is the list of new features available in TKE 8.0:

- Support for managing the new Crypto Express5S coprocessor. You must have a minimum level of TKE 8.0 to manage this new coprocessor. The Crypto Express5S contains 85 domains for the z13 and 40 domains for the z13s.
- There is a new wizard-like feature to load all master keys through a single process. During the process, all first parts are loaded before moving to the middle or last parts. This process is designed to reduce the amount of smart card swapping during a key load ceremony.
- You can now configure how much of a key or key part verification patter is displayed.
- There is now full function migration wizard support for host crypto coprocessors running in EP11 mode.
- Support for Crypto Module Groups was removed. There is a utility for converting Crypto Module Groups to Domain Groups.
- A new FIPS certified smart card (FC #0892) was released with TKE 8.0. The new cards have the part number 00JA710 printed on them. The previous smart card can be carried forward and used on TKE 8.0. However, if an Injection Authority (IA) smart card or Key Part Holder (KPH) smart card is created on TKE 8.0, the smart card must be a 74Y0551 or 00JA710 smart card part. The 45D3398 cannot be initialized as an IA or KPH smart card on TKE 8.0.
- There is now an indicator on the top window of TKE applications that lets you know if the application has access to the smart card readers.
- The owner of a TKE workstation passphrase profile can now change their own passphrase during the sign-on process.

The TKE provides the capability to collect data from one host crypto coprocessor and apply that data to another host crypto coprocessor. These tasks are done from the Configuration Migration Tasks application of the TKE. There are new considerations when a Crypto Express5S coprocessor is involved in the collect or apply process:

- You can collect or apply data to or from a Crypto Express5S coprocessor from a TKE 8.0 system.
- Data, collected from any type of crypto coprocessor, can only be applied to a Crypto Express5S coprocessor if the data was collected using Key Part Holder Certificates from KPH smart cards that are created on a TKE 8.0 system.
- Any time you collect data that will be applied to a Crypto Express5S coprocessor, the collect must be done from a TKE 8.0 system.
- If data is applied to a Crypto Express5s coprocessor, the Injection Authority smart

cards used during the apply process must be created on a TKE 8.0 system.

TKE 7.3

The TKE 7.3 is supported on the following processors: zEC12, zBC12, z196 and z114. It has been enhanced to support EP11 when using the full function migration wizard. This enhancement provides the ability to quickly and accurately collect and apply data to the Crypto Express features configured as EP11 coprocessors.

The TKE 7.3 now has a workstation setup wizard. This setup wizard performs the most common TKE workstation initialization functions, ensuring speed and accuracy of new TKE hardware deployment. It simplifies the process while greatly reducing errors. The wizard can also be run to verify the TKE workstation has been configured correctly.

The TKE 7.3 allows the set of the Master Key from the TKE workstation. Prior to this support, the master key could be loaded from the TKE, but an additional step was required to be performed from the ICSF panels. With this new support, the entire operation of setting the master key can be performed from the TKE. The TKE workstation will allow you to set any master key from the TKE workstation.

The latest CCA enhancements are designed to allow users to prevent the automatic generation of certain PIN values, or the replacement of existing PINs with certain PIN values that might be considered weak. The TKE 7.3 LIC includes a new tab for specifying these restricted PIN values.

Five new AES operational keys can be managed from the TKE 7.3 workstation. The key types are MAC, PINCALC, PINPROT, PINPRW and DKYGENKY.

The TKE 7.3 has been enhanced with two new functions, the Close Host and Unload Authority Signature Key. The Close Host enhancement is designed to allow the user to explicitly sign off a host. The Unload Authority Signature Key enhancement allows the user to explicitly remove the current authority signature key without ending the TKE application. Having many users with different roles, users no longer have to end the TKE application before the TKE workstation is utilized by another user.

The TKE 7.3 workstation profile role has a new access control point to create, change, or delete a host list entry. This is designed to provide stronger separation of duties between users of a host list entry and users that manage the entries.

In TKE 7.3, when creating or changing a domain group, a domain can only be included in the group once. This ensures that domain commands are only sent to a domain once.

The TKE 7.3 has been enhanced to manage a 'module-scoped role' from inside a domain group. If a host crypto module role is managed from a domain group, the user must explicitly select which Domain Access Control Points are to be set. The user either specifies that every domain access control point is selected for every crypto module in the group or only the domain access control points for the domains in the group are selected.

When TKE 7.3 is used to manage CCA or EP11 Domain Control Points, the user can save the settings to a file which can then later be applied to other domains. This enhancement allows for fast and accurate deployment of new or recovered domains.

When using the latest version of smart cards on a TKE 7.3 workstation, a 256-bit AES session key will be used for all smart card operations.

TKE 7.2

The TKE 7.2 supports the Crypto Express4S feature when the PCIe adapter is configured as an EP11 coprocessor. The TKE workstation is required in order to manage a Crypto Express4S feature that is configured as an EP11 coprocessor. The TKE smart card reader (#0885) is mandatory. This feature code includes two smart card readers and 10 smart cards. Additional smart cards can be ordered in groups of 10 via feature code #0884.

The TKE 7.2 master key support by default is a DES master key 16 bytes in length. Additional support has been added which is exclusive to TKE 7.2 for a 24-byte DES master key. The DES master key length for a domain is determined by setting Access Control Points (ACPs) from the TKE.

The TKE 7.2 can now support four smart card readers. The TKE workstation supports two, three, or four smart card readers when smart cards are being used. It is expected that PKCS #11 mode will require more keys when generating and managing key material Adding card readers will help reduce the amount of swapping of smart cards into and out of the readers. The additional smart card readers are optional as EP11 mode can be managed with only two smart card readers. Although designed for EP11 mode, the additional smart card readers can also be used by the CCA coprocessors as well. (The additional readers are ordered using feature code #0885.)

TKE 7.1

TKE 7.1 now has a wizard-like feature that takes users through the entire key loading procedure for a master or operational key. The feature preserves all of the exiting separation of duties and authority requirements for clearing, loading key parts, and completing a key.

From the TKE 7.1 workstation crypto module notebook, users will be able to display the current status of the host cryptographic module that is being managed.

TKE 7.0

TKE 7.0 LIC also provides an improved host adapter configuration migration wizard which supports migrating master keys between host adapter cards.

TKE 7.0 LIC, which requires the latest TKE hardware with the new 4765 PCIe Cryptographic Coprocessor (FC #0841) is required for managing Host Cryptographic adapters (CEX3s) on the z196/z114. TKE 7.0 LIC requires HCR7740 or later plus the CEX3 toleration APAR, OA29839 on the z196. TKE 7.0 will also support the management of Host Cryptographic Adapters and on the z9 (CEX2s) and z10 (CEX2s and/or CEX3s).

TKE 6.0

TKE 6.0 LIC provided several usability enhancements and introduced two new functions:

- Host adapter domain grouping which means that multiple domains can be grouped and managed together
- Host adapter configuration migration wizard which assists in migrating security data between PCI cards

TKE 6.0 LIC can be used to manage cryptographic adapters installed on a z10. The operating system must be running HCR7740 or later, and if there is a CEX3 installed then the CEX3 toleration APAR OA29839 must be installed. In addition, TKE 6.0 LIC can be used to manage Host Cryptographic adapters on z9 EC and BC, and z890 and z990 systems.

Optionally, the TKE can store keys, key parts and provide access authorization via smart cards. The Smart Card Reader is a separately orderable feature that includes 20 smart cards. The smart cards resemble credit cards in size and shape but contain an embedded microprocesor and memory for data storage. Additional smart cards can also be ordered. Beginning with TKE 6.0, new smart cards and readers are available supporting longer (2048-bit) RSA keys which provide stronger security. The new smart cards also have a newer chip, providing better performance. The new smart card reader can still read the older smart cards for purposes of backing up a CA smart card, or copying a TKE smart card, but the older smart cards cannot be used for any other TKE operations.

In Summary

There is some overlap in the crypto functionality across the crypto hardware on each platform. Your hardware platform will determine what hardware is available to you, but your application or program product controls which APIs are invoked, and so the application determines which crypto functions you need. Your performance and security requirements dictate which of those crypto functions must be implemented in hardware, and which can be implemented in software. ICSF is the interface to the crypto hardware, and it determines where the work will be routed.