A Synopsis of System z Crypto Hardware

The IBM System z 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 System z crypto hardware, including the IBM zEnterprise EC12 (zEC12) GA2 (113-119) and IBM zEnterprise BC12 (zBC12) (113-121) announcements from July 23, 2013.

Cryptographic Functions

System z 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 two variations of the wrapping key: one for DES/TDES keys and one for AES keys.

Each of the three types of keys (clear, secure and protected) have different performance characterists 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 (CEX4) coprocessor, 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.

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.

See the TechDoc WP100647, 'A Clear Key/Secure Key/Protected Key Primer' for more details. Also, see the ICSF Systems Programmer's Guide for a description of how the secure key devices support multiple LPARs and protect keys across operating systems and environments.

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 System z 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 System z crypto hardware requires the appropriate microcode to be installed and operational before the export restricted functions can be used. On the z890/z990, z9, z10, z196/z114 and zEC12 machines, this microcode is ordered as no-charge Feature Code #3863. On the CCF machines, the microcode was unique to the CCF on the machine. 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.ibm.com/servers/eserver/zseries/zos/downloads/. 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.

PCI Implementation

Starting with the z890/z990, IBM changed the crypto architecture to move much of the functionality outboard using the PCI (Peripheral Component Interconnect) bus. There were several reasons to move crypto function off the system board and into the I/O cage:

1) Availability: adding crypto functionality to a processor requires an outage of the entire machine. PCI cards are hot-pluggable, and so new function could be added by simply plugging the card with the new functionality into the I/O cage.

2) Scalability: depending on the platform and other cards installed in the I/O cage, up to sixteen cryptographic engines can be installed in a processor. As workload increases, additional features can be ordered and installed, without an outage to the LPAR.

   Although a PCI card is hot-pluggable, to take advantage of the PCI feature without an outage requires that the LPAR be configured for the PCI card. That is, as part of LPAR configuration, you define which features are available to the LPAR in the Activation profile. These devices are defined to the LPAR in two lists in the Activation profile: the candidate list says the device is a candidate to be brought online and the online list controls which devices will be brought online at LPAR activation. If crypto slot 1 is in the online list for an LPAR and if a PCI card resides in Slot 1, that card will be online to the operating system when the LPAR is activated.

   If crypto coprocessor 3 is included in the candidate list, but no coprocessor is installed, obviously that card is not available to the LPAR. However, if a card is installed in slot 3 after the LPAR is activated, that coprocessor can be brought online to the LPAR and made available to the operating system without an outage. If crypto coprocessor 4 is not in the candidate list for the LPAR and a card is installed after the LPAR is activated, that crypto feature cannot be made available without updating the LPAR Activation profile. In this case, on z9s and earlier machines, coprocessor 4 would have to be added to the candidate list and the LPAR deactivated and activated to make it available to the LPAR. Beginning with the z10 machines, there are Dynamic Configuration capabilities for the Crypto Express cards, which avoid the outage to update the profile. See the section below for a description of the new Dynamic Configuration capabilities available beginning with the z10.

3) Cost: Moving the secure hardware support (the ability to detect probes and physical attacks) to the PCI cards allowed IBM to better manage the engineering cost of this additional protection.

Because the PCI 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 PCI 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 awhile for the crypto engines to complete loading after an MCL install.

The PCI cards, beginning with the CEX2 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, new with the CEX4S on the zEC12, there is a new mode, EP11 or PKCS #11 Enterprise mode. In this mode, the card only supports APIs associated with PKCS #11.

Also with the PCI 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

Beginning with the z990 and z890, there are two cryptographic hardware devices available on System z: the CPACF and the PCI crypto cards. The cryptographic hardware on the CCF based machines is discussed in the z800/z900 section of this document.

CP Assist for Cryptographic Function (CPACF)

The CP Assist for Cryptographic Function (or CPACF) was introduced on the z990 and z890. 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 for speed for every CP, IFL, zIIP and zAAP. 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 for the specific machine for the assembler instructions, and the ICSF Application Programmer's Guide for the APIs that are available. For more information on using the CPACF instructions, see the IBM TechDocs web site, www.ibm.com/support/techdocs for documents:

- PRS821 CIPHZ990 – How To Use The New CPACF Crypto Functions
- PRS822 CALCPACF: Callable Routine To Invoke z990 CPACF Crypto Functions

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.

Crypto PCI Cards

As described above, the Cryptographic PCI cards are optional, implementing additional cryptographic function. Using the PCI 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. Beginning with the Crypto Express cards on the z10, 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). Exclusive on the zEC12 is a new function called EP11 mode, which provides support for secure key PKCS #11 operations and is described further in the zEC12 section.

The crypto PCI 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) it's 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 PCI 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
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

Cryptographic hardware has evolved over time, and the hardware on the z900/z800 and 9672 machines is very different from that on the z890/z990, z9, z10, z196/z114 and the zEC12. Following is a description of the cryptographic hardware devices across the System z platforms.

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(xxx-xxx). 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 models. 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 and has the same functionality found on 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 (as well as the z196/z114, z9EC/z9BC and z890/z990) each CP has it's own CPACF available.

Crypto Express4S (zEC12/zBC12 exclusive)

Crypto Express4S represents the newest-generation cryptographic feature. It 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 on the z196. 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 configured as a coprocessor, the card provides data confidentiality, message integrity, financial functions and key security and integrity. The CEX Coprocessor supports secure key DES, TDES and AES encryption as well as PKA encryption. Master keys must be loaded to enable this functionality. The CEX 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 CCA functionality on the CEX 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 Crypto Express Coprocessor performs encryption operations using these keys. This is the same functionality that is found on the CEX3 on the z196/z114 processors.

When 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 Hardware Security Module. 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 Business Class/z9 Enterprise 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).

z890/z990

The cryptographic devices available on the z890/z990 are similar to the devices on the z9.

CP Assist for Cryptographic Function

As on the z9 and z10, the CPACF on a z890/z990 is a clear key device, so no master key is required. As on the z9, there is one CPACF per PU and work is done synchronously with the CP. The z890/z990 CPACF provides the same five native instructions as on the z9 CPACF, and these instructions can be invoked directly from an application or via the ICSF APIs.

The CPACF on the z890/z990 only provides clear key DES/TDES and SHA-1 hashing. It does NOT support AES-128 or SHA-256 but these functions are provided by the ICSF software on the z890/z990, along with AES-192 and -256 bit clear key support. The CPACF on the z890/z990 does not provide a pseudo-random number generator like the CPACF on the z9/z10.

Crypto Express2

The Crypto Express2 feature on a z890/z990 is similar to the CEX2 on a z9, but on a z890/z990 the 4096-bit RSA key support is not available, and the crypto engines cannot be configured as accelerators, but can only operate as a coprocessor. Even though the crypto engine cannot be configured as an accelerator, it does support the PKA APIs, but not at the same volume as the CEX2 configured as an accelerator on the z9/z10. As with the z10 and z9, the cryptographic functions on the CEX2 are only available via the ICSF APIs, and the crypto work on these cards is performed asynchronously, freeing up the general purpose CPs for other work. The Crypto Express2-1P is not supported on the z890/z990.

PCI X Cryptographic Coprocessor

The predecessor to the Crypto Express2 was the PCIXCC feature. This feature contained a single crypto processor that supported secure key DES/TDES, PIN processing for financial APIs, a random number generator and support for the three PKA APIs (for keys up to 2048-bits). The PCIXCC could only support about 1000 handshakes per second. Like the CEX2, it is a secure card and requires that a master key be loaded. The PCIXCC is no longer orderable, but still supported on the z890/z990.

PCI Cryptographic Accelerator (PCICA)

The PCICA feature was a special purpose card that had two cryptographic processors which supported the three PKA APIs. As a clear key device it did not require a master key to be loaded. The PCICA could support approximately 2000 handshakes per second

(1000 on each crypto processor). Like the PCIXCC, it is no longer orderable, but still supported on the z890/z990.

z800/z900 and predecessors

The cryptographic architecture on the z800/z900 and earlier machines was significantly different. Much of the cryptographic functionality was provided on a processor that was available on the system board, like the CPACF, but with more functionality than the CPACF.

Cryptographic Coprocessor Facility

The Cryptographic Coprocessor Facility, like the CPACF, was built onto the system board, but there were a maximum of two CCFs available in a machine. On some of the smaller machines, there was only one CCF available. The CCF was twin-tailed, that is, the CCF was connected to two CPs, but work was only driven through one of the CPs. If the first CP failed, then the hardware would route work to the CCF through the second CP, and if that second CP also failed, the CCF was no longer available. Like the CPACF, the CCF worked synchronously with the CP, so as crypto workload increased, the two CPs that were driving the CCFs might become very busy, possibly even maxing out, even if the other CPs in the machine were not heavily used.

As on the CPACF machines, crypto microcode is required to enable the CCF hardware. On the CCF machines, the microcode is unique to each machine. That is, it contains the server serial number and the crypto module ID of the CCFs.

The CCF provides secure key DES/TDES support, PIN processing for financial APIs, and key management operations. The CCF also supported the three PKA APIs for keys up to 512-bits in length, but at a lower volume than the PCI cards.

The CCF is a secure key only device, and does not support clear key APIs. Applications, such as System SSL, which rely on clear key symmetric algorithms at the record level, would use the secure key APIs even though the secure key protection was not required, simply to take advantage of the hardware. Under the covers, System SSL would create a secure key, and use that on the CCF hardware. The additional security did not incur a performance penalty because the CCF devices were very, very fast (since they were on the system board).

PCI Crypto Coprocessor (PCICC)

The PCI Cryptographic Coprocessor was the first System z crypto device to move to the I/O cage. It is a secure key device, so it requires that a master key be loaded.

Early versions of the PCICC feature had a single cryptographic processor, while later versions had two processors per feature. Like the PCI cards on the z890/z990/z9/z10, the

PCICC card is asynchronous; freeing up the general purpose CPs to do other work while the crypto work is done on the PCI card.

The PCICC provides some of the same functionality as the CCF as well as having additional capabilities. Although it supports the same secure key DES/TDES APIs as the CCF, ICSF will never route these APIs to a PCICC card because the CCF, being on the system board, can process these calls significantly faster. The PCICC provides some additional PIN functions, over and above those supported on the CCF, and it supports the PKA APIs for PKA keys up to 1024-bits in length.

PCI Crypto Accelerator (PCICA)

While the PCICA on the z890/z990 supported three APIs, the PCICA on the z800/z900 only supported a single API, CSNDPKD or Public Key Decrypt. The PCICA feature on the z800/z900 could support approximately 2000 of these APIs per second.

Trusted Key Entry Workstation

The Trusted Key Entry Workstation, or TKE, has two purposes:

- The secure loading and manipulation of master and operational keys into the host cryptographic hardware.
- Managing the configuration of the crypto engines in the host. The crypto coprocessors can provide additional security for selected functions as well as restricting who can manage the configuration

Since a TKE provides a means for securely loading keys on the host, a secure card is required on the host. The TKE is a workstation with a secure cryptographic card which attaches to the host via an Ethernet (TCP/IP) connection. It runs an embedded operating system supporting a single application, so there is no external interface to the TKE and no other applications or products can be installed on the TKE. Like the Hardware Management Console (HMC) the TKE should be considered an appliance, whose sole purpose is to protect the key entry process.

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 based 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 #0841) includes USB ports for the smart card readers and for memory sticks. The TKE 7.2 LIC (FC #0850) which includes both the operating system and application provide the software support to use the USB ports.

When migrating from a lower release of TKE to TKE 7.3, there are now Access Control Points (ACP) that allow the user to choose between warning or prohibiting the loading of a weak Master Key.

- The TKE supports all of the operational keys that are available in ICSF, including the new key types that were introduced on the CEX4S.

The TKE 7.3 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.

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 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 existing

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 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 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.

TKE V5.3 LIC or higher is required to support the z10 BC (unless a CEX3 is installed) and can also connect to the z10 EC, z9 EC, z9 BC and z890/z990. TKE 5.3 LIC added a screen capture utility for documenting key entry instructions.

TKE V5.2 LIC or higher can be used with the z10 EC, z9 EC and z9 BC, z990 and z890. TKE V5.0 was the first to support the z9, but will also support the z800, z900, z890 and z990, as will TKE V5.1.

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 actually be routed.