MAINFRAME CRYPTO
www.mainframecrypto.com
gregboyd@mainframecrypto.com
Tel: 240-772-1539

IBM's z13 includes new crypto capabilities

If you are an IBM customer you knew that it was coming. And if you follow IBM-MAIN there were posts here and there that hinted at it. In January, IBM announced its next generation System z … and changed the nomenclature. It's now IBM z Systems, replacing IBM System z. (So is a z13 an IBM z Systems? Or just an IBM z System? Too deep a philosophical question for me.)

The 'big thing' on the z13 is Simultaneous Multithreading support (SMT). Since the CPACF is part of the general purpose engine, environments that can leverage SMT should benefit on clear key crypto as well. But there is also new functionality on the CPACF as well as a new crypto card.

CPACF

On the CP Assist for Cryptographic Function (the CPACF), there is a new instruction for generating random numbers. This new instruction 'provides support for deterministic pseudorandom-number seeding and generation that conforms to the National Institute of Standards and Technology (NIST) special publication 800-90A.' (That statement comes from the IBM zArchitecture Principles of Operations manual, SA22-7832-10, p. 120.) Now you can generate random numbers in compliance with the updated standards!

In the announcement letter (115-001) IBM describes some serious performance improvements for both encryption and decryption (for both TDES and AES) and hashing. It's not clear whether those improvements in speed are due to a faster machine, or code improvement or a combination of those, but the numbers are still impressive.

CEX5S

In addition to the CPACF improvements, there is the brand new Crypto Express5S card, aka the CEX5S. Anyone that's been around IBM for a while knows that IBM hates to pre-announce product capabilities, however they have slipped up in the z13 announcement. Along with this new CEX5S card they announced a new Trusted Key Entry Workstation, and that new TKE includes a new hardware platform, which you can order as FC #0842. But apparently you can also upgrade an older TKE by installing a new crypto card, FC #0894 which is identified as the 4767 TKE Crypto Adapter and is available for the zEC12 or zBC12 after April 14, 2015.

The CEX4S uses the 4765 Crypto Coprocessor, and the older crypto cards used a 4764 Crypto Coprocessor. It looks like this 4767 TKE Crypto Adapter is the latest generation of Crypto Coprocessor, and it would make sense that the CEX5S is also using the new engine, since you need the 4767 in the TKE to manage it.

The new Crypto Express5S also brings new capabilities to the z13. The two most significant are support for Format Preserving Encryption and an expansion in the number of domains or LPARs that a card can support.

Format Preserving Encryption

With the z13, IBM has announced support for VISA Format Preserving Encryption. Format Preserving Encryption (FPE) provides the ability to encrypt data while preserving the format of the original cleartext data. For example, in the U.S. a Social Security Number (SSN) is a nine-digit number. If you encrypt the SSN using FPE, the resulting ciphertext will still be a nine-digit number. Another example is a credit card number (aka PAN or Personal Account Number). A credit card number actually consists of several 'pieces', all numeric. The first part identifies the bank and the last digit is a check digit that can be used to confirm that the credit card number is in fact a legitimate credit card number. The digits in between are the actual account number. By preserving the BIN on the front, and encrypting the actual account number using FPE you can calculate a new check value, based on the BIN and encrypted account number, and now you have a PAN that will pass most edit checks and is also encrypted. So your application doesn't have to change, but the data will still be protected.

There are several new APIs to support FPE. One set (FPE Encipher, FPE Decipher and FPE Translate) will encrypt, in a single call, the data from a credit card: the PAN, Card Holder Name, Track 1 and Track 2 data. Because this data is from the credit card these operations must be performed inside the secure boundary of the Hardware Security Module (HSM) so these APIs are implemented using the secure key technology on the CEX5S card. This set of APIs can handle either ASCII or EBCDIC data as input.

The second set of APIs (Field Level Encipher and Field Level Decipher) are more generic and intended for any type of data, not just data from a credit card. These APIs can use either secure key, clear key or protected key. When using secure key, obviously the work will be done on the CEX5S card. If you pass a clear key to these APIs the FPE work will be done by ICSF using the AES and TDES algorithms on the CPACF hardware. (The Principles of Operations manual for the z13 does not indicate that FPE is supported by any of the native instructions, which implies that ICSF will participate in implementing FPE.) And if you provide a Protected Key to the API, just like with the other APIs, the secure key will be decrypted from under the master key in the CEX5S and then wrapped with the appropriate wrapping key before being passed to ICSF and the CPACF hardware.

More Domains

The other major enhancement on the CEX5S card is support for more than 16 domains. With the CEX4S and all the secure cards before it, a single crypto card could support at most 16 LPARs or virtual guests. There is storage on those cards for a maximum of 16 sets of master keys, each of which can be associated with an LPAR or a virtual guest. Since you could install a maximum of 16 of these crypto card features on a CEC, at most, the CEC could support 256 LPARs or virtual guests (16 domains on each of the 16 crypto cards). Especially for the Linux world that is a pretty significant restriction. With the z13, IBM is introducing support for greater than 16 domains per crypto engine. The announcement letter uses that specific terminology: 'Greater than 16 domain support'. However the draft Redbook SG24-8250-00, IBM z13 Technical Introduction (the Jan. 15 draft) uses the terms '… up to 85 domains support'. And there is at least one VM APAR that says 'z/VM supports an increase in the maximum number of domains per crypto feature from 16 to 256.' (That APAR also mentions the ability to support more than 16 engines on the CEC.) Finally, the ICSF Systems Programmer's Guide (SPG), SC14-7507-03, documents a 256 domain limit in the change highlights, but the 256 limit is never mentioned in the body of the manual. On p. 86 of the SPG is the more generic statement: 'The maximum number of LPARs depends on your server. The maximum number of usage domains matches the maximum number of LPARs available on the server.' So clearly IBM will support more domains, and eventually they will probably support a lot more domains!

A Crypto Performance Whitepaper has not yet been published for the z13, however the IBM z13 Technical Introduction indicates that encryption on the CPACF could be up to 2 times faster than on the zEC12 and SHA-384 and SHA-512 could be up to 3.5 times faster.

Note that both the z13 Announcement Letter and the z13 Technical Introduction manual reference the use of a CEX4S on the z13. However, IBM later published Announcement Letter 115-055 which states that the CEX4S will not be supported on the z13.

As with previous crypto cards, the CEX5S is designed to be FIPS 140-2 Level 4 compliant and apparently has already been submitted for certification. And as with previous machines, the z13 will be submitted for EAL-5 certification as well.

New ICSF - HCR77B0

Along with the new hardware function, there is a new level of ICSF, HCR77B0 which will exploit the new hardware. HCR77B0 will ship with z/OS 2.2 when it becomes available. HCR77B0 provides the ability to exploit the new crypto hardware on the z13 and it also provides other new, non-hardware related functionality too.

The most significant enhancement will help in managing keys. In the previous level of ICSF, HCR77A0, IBM introduced the new KDSR format keystores. Very simply, this standardized the structure of the keystores in a variable length record format with new fields like the Date Last Referenced field. In HCR77B0 the KDSR format adds more date fields, new flags and metadata fields for IBM and/or customer use. The date fields include validity dates as well as date fields to record changes to a record.

With the validity dates, you can now specify a 'Start' and 'Stop' date for a key record. ICSF will honor those dates. Until the start date is reached and after the stop date is reached, ICSF will not allow you to use the key material. This gives you the capability to create a new key record today, but specify a start date in the future and a stop date after that. That provides better control of the key material as you implement key rotation policies. You can create keys well ahead of time, but not allow them to be used until the appropriate dates have been reached. And automatically prevent the key from being used after the period ends.

Of course if you export the key and send it to a partner, that partner may not be using the key in an ICSF environment so there would be no enforcement of your start and stop date. And even if they import it into their ICSF environment, they might change the start and/or stop date. But within your ICSF environment, those dates will be honored. There is also a new z/OS health check for identifying keys that will expire within a specified period.

There is now an archive flag in the key record, giving you the ability to retain a key in the keystore, but prohibit it from being used. IBM had looked at an archive process that would remove a key from the primary keystores (the CKDS/PKDS/TKDS) to an archived keystore. However the problem with that technique is that if that archived key is encrypted under a master key (i.e. a secure key) ICSF would have to support a reencipher of the archive keystore as well as the primary keystore. Instead, IBM chose to simply add an archive flag to the existing record in the primary keystore. If that archive flag is turned on, by default ICSF will not permit use of the key. Along with these new fields, there are a couple of new APIs for reading and writing the new metadata fields in the various keystores. Changes to the metadata will be recorded in the SMF Type 82 records.

It would be easy to imagine a utility that could scan the metadata, looking at fields like the 'Date Last Referenced' field and then mark a key as archived because it has not been used in some minimum time period.

There is a new keystore policy that provides the ability to implement archiving without enforcing it. That is, you can start checking the date last referenced field and flag a key as archived, but still allow those keys to be used while working out the processes and procedures. By creating a RACF profile, CSF.KDS.KEY.ARCHIVE.USE in the XFACILIT class, ICSF will allow a key to be used even if the archive flag is turned on. During a transition period, a utility could check the Date Last Referenced field and for example, if that date is greater than one year ago, turn on the archive bit to prohibit its use. But with the keystore policy defined, the archive would not be enforced.

When an archived key or a key outside of its validity dates is used, an SMF Type 82 Subtype 30 record will be cut. There is a new start-up option, KEYARCHMSG which tells ICSF to issue a message to the joblog the first time an archived key is used. That will provide another way to identify archived keys that are being used allowing you to test your archive policy before enforcing it.

Along with the new APIs for manipulating the metadata, there is a new API for validating the contents of the keystores. The API CSFMPS/6 is the ICSF Multi-Purpose API, but it currently only has a single purpose: to validate the keys in the active CKDS or PKDS. While the master key change process is fairly straightforward, with the ability to add data (i.e. metadata) to the key records, this API provides a way to detect keys that may cause a change master key operation to fail. This key check can be invoked programmatically or executed from the CKDS/PKDS Management panels.

Also from the CKDS/PKDS Management panels there is a Coordinated KDS Conversion option that will convert your keystore from KDS to KDSR format across your ICSFPLEX. It is supported for each of the three ICSF keystores (CKDS, PKDS and TKDS).

HCR77B0 supports a new communication level. With HCR7790, IBM introduced Communication Level 2, which all members of an ICSFPLEX had to be running to support Coordinated Master Key Change operations. With HCR77B0 there is now a Communication Level 3, which is required for all members of an ICSFPLEX before you can perform a Coordinated KDS Conversion (convert to KDSR format).

Crypto Card Labels

HCR77B0 also introduces a new labeling convention for Crypto Cards. The first crypto card, the PCICC was identified with a ‘C’ along with the adjunct processor number. An Accelerator was labeled with an ‘A’ and the PCIXCC with an ‘X’. Starting with the CEX4S, the label was expanded to two characters. The first character was always ‘S’ and the second character was ‘C’ for CCA Coprocessor, or ‘A’ for Accelerator or ‘P’ for PKCS #11 mode. Starting with HCR77B0 the two character convention will be used for all crypto cards, but instead of an ‘S’, the first character will be the generation of Crypto Express card ('2' for a CEX2 all the way up to '5' for a CEX5S). So a CEX4S, configured as a coprocessor will be displayed as 4Cnn, where nn is the AP number. Similarly, a CEX3, configured as an accelerator will be displayed as 3Ann.

HCR77B0 provides a new exit that is available at the completion of all ICSF services. Using CSVDYNEX provides a way to capture statistics on the use of the APIs. This might be a first step toward generating better performance data from ICSF!

If you are using the CICS Attachment Facility (invoking ICSF APIs from CICS applications) be aware that the DFHRPL concatenation in your CICS JCL will need to add the ICSF shared libraries (SIEALNKE). And you'll need to update your WAITLIST with the new APIs that are available on the CEX5S.

There is an interesting new message available with HCR77B0:

CSFM653I kds LOADED num_record RECORDS WITH AVERAGE SIZE average_size

The description of this message indicates that it can be used 'to assist in optimizing VSAM record sizes', but so far there is no guidance from IBM on when and how you would tune those record sizes.

As with all ICSF upgrades, there are toleration APARs that are required if you are porting your existing z/OS system and specifically an older version of ICSF to your z13 system. Those APARs will let that old version of ICSF use the CEX5S, but as either a CEX4S or CEX3 depending the level of ICSF. And there are coexistence APARs that will need to be installed on older versions of ICSF when you will be sharing keystores with an HCR77B0 system. As always, be sure to check the buckets!

The announcement letter is a little bit unclear on the z/VM support for the new CEX5S card, although all the operating systems (z/VM, z/VSE, z/TPF and Linux on z Systems) will at least tolerate the new card. IBM is working with their Linux distribution partners to exploit the new hardware in a future distribution. Because IBM won't pre-announce new hardware technology, they won't provide drivers for the new hardware to their Linux partners until after it becomes generally available. Then it takes a while for the Linux distributors to incorporate those drivers into a new distribution.

TKE 8.0

There is also a new TKE available to support the CEX5S cards. This includes a new workstation with the new 4767 coprocessor as well as new LIC (Licensed Internal Code). As pointed out earlier, you can upgrade your existing TKE by installing a new crypto adapter (the 4767 adapter), but it's not clear from the documentation which old platforms can be upgraded. This upgrade support is likely only for TKE 7 workstations.

The new TKE can connect to either a z13 or a zEC12/zBC12, but it can manage crypto cards back to the CEX2. If you want to use a TKE, then TKE 8.0 LIC is required to manage the CEX5S including the greater than 16 domain support. The TKE LIC also provides usability enhancements as well as improvements to the migration wizards. The migration wizards can greatly reduce the time it takes to migrate your crypto environment to the new hardware (or to your DR site). Finally, the TKE 8.0 also provides printer support on the TKE. Customers have long requested the ability to print key material from the TKE, although that should be used with caution.

With cryptography, you don't want to 'push the envelope'. You want proven algorithms that provide the security and performance to protect your data. The z13 and it new crypto hardware and ICSF do just that!

Did you know?

ICSF can help you review Type 82 records?

IBM provides a sample REXX EXEC and job for printing the SMF Type 82 records in a 'readable' format?

If you don't have access to SAS or MICS or one of the other products for manipulating and managing SMF data, the Type 82 records that are generated by ICSF can be printed using the REXX EXEC CSFSMFR that is provided with ICSF. The sample job CSFSMFJ includes the steps to dump the Type 82 records using IFASMFDP, sort those records on the time and date stamps and finally execute the REXX EXEC in batch.

The EXEC is not very sophisticated. Mostly it simply prints some of the flag fields from the various subtype records, using the headers and nomenclature from the System Programmer's Guide. (For HCR7770 and earlier, the ICSF SMF records were documented in the z/OS System Management Facility manual, but starting with HCR7780 the SMF record layout was moved to the ICSF SPG.)

The EXEC also provides a brief description of each subtype.

In a pinch, you can use the EXEC and job to find an event that was logged by SMF!

How can Mainframe Crypto help you?

Getting started with crypto – If you're just starting to leverage the crypto infrastructure, we can provide guidance in configuring the environment as well as developing the processes and procedures to manage the infrastructure. We can provide guidance on the configuration settings that might impact performance as well as security.

If you're already leveraging the crypto technology, maybe it was implemented some time ago and by a staff member that has moved on to new opportunities. We can help you review and document the configuration, and understand some of the decisions that were made in the initial implementation as well as determining whether those decisions are still appropriate.

If you're dealing with audits and questions from your security team, we can help you document the policies and processes that you are using to provide a secure environment. As appropriate, we can help you "tighten up" those processes to meet your audit requirements.

If you need to implement new crypto solutions we can help extend the current crypto environment to support the new products or applications. That may include evaluating the current workloads to ensure that you have the capacity to support the new workloads.

If you need help in implementing crypto within your internally developed applications, we can help with understanding and implementing the APIs.

zExchange Crypto Webcasts

The zExchange, sponsored by NewEra Software is continuing to offer the monthly crypto sessions in 2015. With the announcement of the z13, we changed the sequence of topics slightly, but we'll cover the crypto hardware in April and May and then talk about ICSF for June through Aug. We'll add new topics during the course of the year.

The schedule will be just like last year's: The last Wednesday of the month at 1PM and that Friday at Noon (ET). You can enroll at http://www.newera-info.com/z-OS-Crypto.html.

This is the third issue of the Mainframe Crypto Newsletter. Its goal is to help you learn about new crypto technology and realize the full-function of the crypto technology that is available on IBM System z. You are receiving this newsletter because you either a) signed up for it on my website, www.mainframecrypto.com or b) you signed up for one of my Crypto Webcasts on the NewEra Software zExchange. Either way, Thank you!

If you would like to continue receiving this newsletter, please sign up at my website www.mainframecrypto.com (from any page except the home page look for "Get Greg's Newsletter"). I plan to phase out the use of the webcast list over time, so the only way to be sure to continue receiving this newsletter is to subscribe.