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

IBM z13s and Crypto

In February, IBM announced their new IBM z13s machines. Since this announcement also includes GA2 for the z13, it's sometimes hard to differentiate what is new on the platform vs what is carried over to GA2. Most of the z13s announcement rehashes what was already available on the z13 and the Crypto Express5, but there are a couple of items worthy of mention.

Probably the two most significant crypto related capabilities are improved performance and support for new operator commands.

The Redbook, IBM z13 and IBM z13s Technical Introduction, SG24-8250, claims that the CPACF hardware is up to 2.3 times faster for encryption functions and 3.9 times faster for hashing functions versus previous platforms. In addition, the announcement letter, 116-002, says that the Crypto Express5s performance has been 'improved to support the mobile world.' The numbers for the z13 were pretty dramatic, but IBM doesn't update its Performance of Crypto Operations document for the Business Class machines, so there aren't any details.

HCR77B1, the most recent version of ICSF and which provides support for the z13 and z13s includes two new operator commands. The Display ICSF command will show information about the cards that are installed, the KDS, and selected options. Most of these options provide status that is available on the ISPF ICSF panels, however now the information is available to operators at the console. There is also a LIST option which displays the members of a SYSPLEX that are eligible to participate in the LIST and SETICSF commands.

The SETICSF command will perform specific administrative functions such as activating/deactivating a card, enabling/disabling updates to a KDS or changing a subset of ICSF options.

Prior to these commands being available, the functions had to be performed from the ISPF ICSF panels, which meant that operators had to have TSO access and the appropriate authorities. The new commands are documented in the ICSF SPG for HCR77B1.

This new version of ICSF and the z13 hardware also adds new CCA support:

- New key check value using CMAC algorithm for the CSNBKYT2 API
- Support for AES Galois/Counter Mode (GCM) for the CSNBSAE/ CSNBSAD (Symmetric Algorithm Encipher/Decipher) APIs
- Support for a new key derivation algorithm for CSNDEDH (EC Diffie-Hellman) API

- New API, Encrypted PIN Translate Enhanced (CSNBPTRE) to support an FPE encrypted PAN
- A new ICSF Option, MASTERKCVLEN, to control the length of the verification/hash patterns displayed (to comply with ISO11568)

Another potentially significant capability is the new Remote Device support. There is a new ICSF Option, REMOTEDEVICE, which allows you to define 'standalone devices that perform geography-specific cryptography'. You can define up to 16 of these remote devices, via IP address and port number. Basically this allows you to route work, from ICSF, to a specialized device delivering a unique algorithm.

Currently the support is only for devices that provide the 'Chinese SMx family of algorithms'. I suspect that this is not a new direction for IBM, allowing ICSF to route work to distributed devices, but more an acknowledgement of the realities of supporting crypto in China.

There is also a new level of the Trusted Key Entry Workstation, TKE 8.1. TKE 8.0 was introduced with the z13 and TKE 8.1 adds new capabilities while still running on the same TKE hardware (which includes the new CEX5S coprocessor in the workstation).

If you are using a TKE, then some of the new capabilities on the TKE 8.1 will be of interest:

- Support for coordinated master key change function (previously only available via the ISPF ICSF panels)
- Support for domain-only apply (ability to apply domain settings to target domains, without changing module settings)
- Several new 'wizard-like' features (to create roles and authorities, to create the smart cards used to implement a TKE zone or a migration zone)
- Support for HMAC operational keys
- New option on domain groups to clear and load operational key registers for all domains in the group
- Support for access control tracking
- New function to copy key parts from binary file to smart card
- New admin settings to require

enhanced password encryption for host connections and to disable automatic host logons

What Mainframe Crypto can provide

No matter whether you're just getting started with crypto on System z or you've got an established crypto environment, Mainframe Crypto can help!

If you're just dipping your toe into leveraging the crypto infrastructure, we can help you hit the ground running. There may be a new requirement to encrypt your databases, or to secure your network communications. Either way, you'll need to get ICSF up and running, and the defaults aren't always the best. (See the DEFAULTWRAP start-up option.) And if you've installed Crypto Express cards, you'll need to get the master keys loaded. The easiest method is PassPhrase Initialization, but that's not really secure. And you have to make sure you can recover those master keys on your Disaster Recovery machines. We have plenty of experience in helping customers get that infrastructure working the right way!

There may be even more opportunities to help customers who have had their crypto infrastructure in place for years. First, do you know why crypto is configured the way it is? Are the old-timers that originally set up the environment still around? And do they remember why parameters were set the way they are? Second, are you leveraging the capabilities and functions that are available with the latest versions of ICSF and the crypto hardware? Third, have your procedures and processes kept up with the latest standards and best practices?

The crypto infrastructure on System z provides a huge amount of functionality. It's not just for hiding data! Are you leveraging all of that functionality across all of the products that need security and integrity? With the increased functionality, comes increased complexity. And every product is different in how it leverages the crypto functionality. Database encryption works very differently from securing network communications. And those work differently than IBM's Service Delivery. If you implemented the crypto infrastructure to meet one specific requirement, why not use it with all the other products that can take advantage of crypto!

Mainframe Crypto can provide assistance with reviewing your environment as well as customized education on all aspects of Crypto on z/OS.

Did You Know?

DES requires an odd parity key!

If you didn't realize it, the specification for the DES algorithm requires an odd-parity key value. And ICSF will enforce that for you, even if you weren't expecting it. There was a case where a customer was performing single-DES encryption using a key value of ABCD1234. They then decrypted the data but mistakenly used a key value of ABCD1224. And the data was successfully recovered! They were a little perplexed.

Let's look at why:

ABCD1234 in hex is C1C2C3C4F1F2F3F4.

And in binary that is

C1	11000001
C2	11000010
C3	11000011
C4	11000100
F1	11110001
F2	11110010
F3	11110011
F4	11110100

Notice that the third (C3) and seventh (F3) bytes each have an even number of bits. ICSF will kindly flip the last bit to change the parity, resulting in:

11000001	C1
11000010	C2
11000010	C2
11000100	C4
11110001	F1
11110010	F2
11110010	F2
11110100	F4

Now consider the 2nd key, ABCD1224, which in hex is C1C2C3C4F1F2F2F4

And in binary that is

C1	11000001
C2	11000010
C3	11000011
C4	11000100
F1	11110001
F2	11110010
F2	11110010
F4	11110100

In this case, only the third byte has even parity, so only one bit is flipped:

11000001	C1
11000010	C2
11000010	C2
11000100	C4
11110001	F1
11110010	F2
11110010	F2
11110100	F4

Which now looks a lot like the second key. Of course you shouldn't be using 8-byte single DES keys. And you shouldn't be hard coding clear keys, but be aware that ICSF will adjust the parity of DES keys when necessary, and you may not even realize it

NewEra zExchange

NewEra Software is continuing to offer the zExchange Crypto sessions, but in 2016 we're doing them bi-monthly. The first session, in January, was on the Trusted Key Entry Workstation. In March we covered Application Coding. The sessions are generally on the last Wednesday of the month at 1PM. You can enroll at http://www.newera-info.com/z-OS-Crypto.html.