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

Did You Know?

24-Byte DES Master Key Support on the CEX4S

The Crypto Express4S can support a 24-byte DES master key. When IBM first implemented crypto technology, 8-byte keys were the norm, although Triple DES was just arriving. So the early hardware and ICSF versions used a double-length, 16-byte DES master key to protect those 8-byte operational keys.

24-Byte DES-MK to meet Key Wrapping requirements

Now that DES is no longer considered secure, Triple-DES keys are the norm. And unfortunately, that 16-byte DES-MK is not long enough to secure your 24-byte operational keys. (The weak-point, where you would mount a brute-force attack is now the 16-byte master key, not the 24-byte operational key.) This new 24-byte DES-MK support helps meet the ANSI key wrapping standards.

HCR77A0 was the first version of ICSF to support the longer DES-MK. Once you migrate to the longer DES-MK, you wouldn't want to inadvertently switch back to the 16-byte DES-MK, so the process for implementing 24-byte DES-MK requires a Trusted Key Entry Workstation to enable the Access Control Point (the hardware "switch") that implements the longer master key.

If you are subject to the ANSI key-wrapping standards you might want to consider implementing the new 24-byte DES master key.

Crypto Resolutions for the New Year!

In the December webcast for the zExchange (sponsored by NewEra Software), I mentioned four things that I think you should be doing now in your crypto environment. They included:

- Rotate your keys
- Secure your crypto resources
- Capture your performance data
- Know your users

Rotate your keys

Good crypto hygiene includes changing your keys periodically. You don't need to change your keys every thirty or ninety days like you do a password, but you should have corporate guidelines that proscribe changing them. And that includes both master keys and application keys, as well as public and private keys.

The rotation period will be different, depending on the type of key and how it is used. For example, private keys in a public/private key pair will be locked away securely in your PKA keystore and encrypted under the RSA-MK or ECC-MK. So they should be very secure (see Secure your crypto resources), and therefore the rotation period can be somewhat longer than for symmetric

© Mainframe Crypto, LLC

keys that you share with a partner. (How good is your partner's security for that key material?)

Your master key will also be on its own cycle, whether it be yearly or biennially or every five years. And if you have to reload those master keys, say as part of your Disaster Recovery exercise, then once the DR exercise is finished might be a good time to change those master keys.

And of course you should have documented procedures for changing each type of key that can be executed at any time. If there is any kind of "event", where a key could be compromised (for example, if a trusted key officer leaves the organization), then you want to have a crisp procedure for changing the key on demand.

Secure your crypto resources

You should SAF protect your crypto resources. Start with your keystores (the CKDS, PKDS and TKDS) which may contain key material in the clear. The only address space that requires access to the keystores is ICSF. That is, all requests for keys should come via the ICSF APIs and those will be serviced by the ICSF address space. So no other user-id needs read access to these keystores. (There are cases where a fire-call userid may need access, but every one of those should be logged.)

You should also protect individual keys in both production and test environments. It's easy to see that production keys should only be used by production applications, but you should consider protecting keys in your test environment as well. Some customers have opened up the ability to create and use keys in the test environment, thinking that they want their developers to be able to create keys whenever they need them for testing purposes. However that has led to having many, many keys defined and no clear idea of who is using those keys nor whether those keys are still needed.

Of course that implies a strong naming convention for your keys, and then using group profiles to secure keys.

Finally, you should also protect the individual ICSF APIs. Strong separation of duties requires that production applications should have authority to use a particular key, but not be able to create or change that key. And key officers should be able to generate or change keys, but not be able to decrypt production data using one of those keys.

Capture your performance data

The performance data that is currently provided by ICSF and the crypto hardware is not sufficient to do serious performance reporting nor effective capacity planning. However it's all you've got. So you should at least be capturing that data and at least monitoring trends. The RMF Crypto Hardware Activity report (from the RMF Type 70 records) will report the utilization on your Crypto Express cards, but it won't

© Mainframe Crypto, LLC

provide any detail as to whether the crypto workload is primarily public/private key encryption or DES/TDES or AES encryption or MAC operations or whatever. And it won't tell you whether the workload is coming from LPAR 3 or LPAR 7. But if you monitor the utilization over time, hopefully you'll notice the utilization rising over time and that will give you an indication of when you'll need to add more resources.

The SMF Type 113 records, generated by the CPU Measurement Facility can be used to count the number of crypto operations performed by the CPACF hardware. Theoretically you can use those numbers to calculate the impact of those crypto operations on your total CPU utilization. Again, monitoring those counters over time could provide an indication of when your crypto workload is changing and the need for more crypto resources.

And don't forget that there are other SMF records with crypto related fields: SMF Type 30 and 72.

Know your users

Finally, you should try to understand your unique crypto workload. In your environment, you might only be using the crypto infrastructure for securing your communications using System SSL. In that case, you should at least try to learn whether that is primarily TN3270 or CICS communications or FTPs with your partners.

Or possibly you've installed the Infosphere Guardium Data Encryption Tool for DB2 and IMS and your primary crypto work is encrypting rows in your DB2 tables.

Plus you could have "stealth crypto" users. That is, it's fairly easy for an application programmer to invoke the ICSF APIs and start performing crypto operations. And even sneakier, those developers could use the assembler instructions to perform encryption or hashing

Your crypto workload might be any one of those (or several others) or it could be a combination of multiple. And every shop will have their own unique mix and crypto workload.

So this is the fuzziest of the four recommendations, but you should try to understand your own unique environment and the workload that your applications and developers are driving. Talk to your developers and your communications team to understand whether they are using the crypto infrastructure.

What Mainframe Crypto can provide

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.

© Mainframe Crypto, LLC

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, will continue to offer the monthly crypto sessions in 2015. We'll start the year with some of the crypto basics that we covered last year (Intro to Crypto, Crypto Hardware and ICSF), updated as appropriate. We'll also 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 second 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.

Happy New Year!

© Mainframe Crypto, LLC