

Did You Know?

New ICSF Related Health Checks!

IBM has added a couple of new health checks and updated an existing check. Technically, these are RACF health checks but they are related to ICSF and Crypto.

log even successful operations.

In addition, the RACF_SENSITIVE_RESOURCES health check has been updated to include the three ICSF keystores as

If you're not protecting these resources (CSFSERV and CSFKEYS), you should be.

RACF_CSFSERV_ACTIVE and RACF_CSFKEYS_ACTIVE are new health checks that will verify the resource classes for protecting ICSF APIs (CSFSERV) and key material (CSFKEYS) are active. If you are not protecting these resources, you should be. Not just anyone should be allowed to create key material on a production system. You can use the CSFSERV class to restrict who can issue APIs that generate key material. Not just anyone should have access to key material, especially on the production system. On a test system, the access rules might be different, but I would still encourage you to limit authority and

sensitive resources. These data sets should all have UACC(NONE), because they only need to be read by ICSF, on behalf of your application. These health checks are available via APAR OA44696.

Service Offering – Master Key Management

Do you include cryptography as part of your Disaster Recovery process? Do you know the passphrase or the key parts that were used to set up your crypto environment? Could you reload them in case of a disaster? Or in an emergency (i.e. you had to

This is the first of what will hopefully be many newsletters to come from Mainframe Crypto! As most of you are aware, I retired from IBM in April of this year, with plans to open my own consulting business. I hope to continue doing similar work to what I did at IBM: helping customers understand and implement crypto technology on System z. One way that I hope to do that is via this newsletter, with notes about new technology and things that you may not have considered before.

If you are on this distribution then you fall into one of two groups: First, you have already signed up for the newsletter. If so, Thank you! Second, you signed up for one of the Crypto webcasts sponsored by NewEra Software and the zExchange. Thank you for attending those as well, but 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 to receive this newsletter is to subscribe.

install a new crypto card to support additional capacity)? Have you successfully exercised the process for loading your

master keys? If so, Good for You! That means you have access to the appropriate key material and you know the procedures to follow to get them reloaded. But are those procedures documented, so your backup could perform them?

If you have not exercised the key loading procedure recently, what will you do in an emergency?

Mainframe Crypto can help you gain familiarity with the process and document it as you go. At the end of the engagement you will a) know your master key material and b) have a documented process that you can use either at your Disaster Recovery site or in your production environment to get those keys reloaded!

Education – I need your help

Mainframe Crypto is teaming up with Mulder Training and Consultancy to offer a course on IBM's Common Cryptographic Architecture (CCA) and ICSF Implementation.

Similarly to me, Andries Mulder retired from IBM and now offers training and consulting in Europe on the IBM Cryptographic environment. He has been working with the IBM CCA since it was introduced in 1989 on the Transaction Security System. He runs several classes on the IBM family of products and is an Authorized Service Provider for the IBM 4764 and 4765 Software Development Toolkit (UDX toolkits).

The IBM CCA/ICSF Implementation Course familiarizes students with IBM's ICSF and CCA. The course provides experience in configuring, programming, testing, and operating ICSF.

After attending the course students should be able to configure, program, and use ICSF in CCA mode. In addition, participants should be able to design solutions that use IBM's other CCA products.

We are currently looking for opportunities to

deliver this training in the United States. That is, we are looking to bring the class to a city near you! If you are interested in attending and more importantly, think your organization will fund the \$3100 fee (per student), please let us know. We'd like to find a central site, near, but not in, a major US city. We'll need at least six students to make it cost effective for you as well as us.

If your organization would like a private class we would be more than happy to offer it onsite at a reduced price!

If you'd like more information, please send a note to gregboyd@mainframecrypto.com.

