IBM Systems MEDIA

What’s New With ICSF HCR77C1

Cryptographic Support for z/OS V2R1 - z/OS V2R3, also known as ICSF FMID HCR77C1 or web deliverable number 17, was released in September 2017.

By Bob Petti

05/01/2018

ICSF Delivers With Its FMID HCR77C1 Release

Cryptographic Support for z/OS V2R1 - z/OS V2R3, also known as ICSF FMID HCR77C1 or web deliverable number 17, was released in September of 2017 and has many things to brag about. The updates contained in this release vary from usability improvements, such as an ISPF-based browser for CKDS key material, to integrated support for a PCI HSM configured CCA coprocessor.

CPACF Enhancements

This latest ICSF release supports the new IBM z14 mainframe, which includes enhancements to the CP Assist for Cryptographic Functions (CPACF) feature:

- Support for SHA-3 hash algorithms, which complements the existing SHA-1 and SHA-2 algorithms. ICSF's One Way Hash (CSNBOWH) callable service now supports the SHA-3 and SHAKE options, taking advantage of the new hashing techniques.
- Support for a True Random Number Generation (TRNG) instruction. ICSF's implementation is transparent, but internally, if ICSF is using CPACF instructions to load its' random number cache, the new TRNG instruction is used when running on the z14. Note: ICSF draws random data from several sources depending on how the system is configured.
- Performance improvements that can improve the throughput of AES GCM encryption. Workloads that use AES GCM encryption may observe a performance improvement here.

Support for a CEX6S Coprocessor and CCA Release 6.0

The CEX6S crypto coprocessor and CCA Release 6.0, which allows a coprocessor to be configured in PCI HSM mode:

• PCI HSM Compliant Mode restricts DES keys to PCI HSM approved usage, for example:

- Multi-use keys (for example, keys of type "DATA") are not eligible for PCI HSM requests.
- Single length (8-byte) DES keys are not eligible for PCI HSM requests.
- Keys must be wrapped using the "enhanced wrap" method. ECB wrapped keys are not eligible for PCI HSM requests.

• To make a key eligible for use in a PCI HSM compliant mode coprocessor, it must be tagged as PCI compliant, for example:

- The DES key token's control vector has been updated to include a flag indicating whether a key is restricted to PCI HSM compliant use.
- New keys can be tagged at the time that they are generated when a coprocessor has been configured in PCI HSM Compliance mode. Existing keys can be tagged using the Key Token Translate 2 (CSNBKTR2) callable service only when a coprocessor is in migrate mode.
- A DES key that is tagged is only usable by a compliant mode coprocessor. When ICSF detects a tagged DES key, it routes the request to an eligible coprocessor or rejects the request with an appropriate error code if no compliant mode coprocessor is available.

• Note that requests that do not contain PCI HSM tagged keys can be routed to any coprocessor. Even a PCI HSM mode coprocessor will satisfy requests that contain non-tagged keys. This is referred to as normal mode. The PCI HSM restrictions only come into play for DES keys that have been tagged as PCI HSM compliant.

• ICSF supports a configuration option keyword, COMPLIANCEWARN, that causes SMF type 82 audit records to be generated for existing workloads, indicating a request's eligibility for PCI HSM compliance, allowing customers to determine what application and key changes are needed to exploit a PCI HSM configured coprocessor.

• A TKE ("Trusted Key Entry") workstation is required to administer a PCI HSM compliant coprocessor.

• In addition to PCI HSM support, CEX6S and CCA 6.0 also introduce the use of x.509 certificates in CCA:

- Certificate validation is done within the coprocessor. A TKE is used to manage root and signing certificates that are installed within the coprocessor.
- The new ICSF callable service, Public Infrastructure Request (CSNDPIC), is available to generate PKCS#10 certificate requests.
- The Digital Signature Verify (CSNDDSV) callable service has been enhanced to accept an x.509

certificate to be used when verifying a signature.

An ISPF-based Browser for the CKDS

The Cryptographic Key Data Set (CKDS) is used to store symmetric key material (DES and AES key tokens). With ICSF FMID HCR77C1, you have access to an ISPF-based key browser that can be used to list and perform basic management operations on key material, including for the first time, the ability to generate a new key from an ISPF panel.

Secure Key Token Support for Format Preserving Encryption

The Field Level Encipher (CSNBFLE) and Field Level Decipher (CSNBFLD) callable services have been updated to accept a key specified as a secure key token. This “protected key” support retains the security of a key that has been encrypted by the CCA coprocessor’s master key, but with the performance advantages of doing the encryption operations on the system’s CPACF feature.

Ability to Monitor Crypto Usage Statistics

System administrators can now monitor their system’s usage of cryptographic resources. Cryptographic usage tracking can be enabled or disabled at ICSF initialization (with the STATS option in CSFPRMxx) or dynamically after ICSF initialization (with the SETICSF OPT,STATS operator command). Cryptographic usage statistics can help you determine:

- The jobs and tasks that are using the various cryptographic engines.
- The cryptographic card types that are getting the most requests.
- If any cryptographic requests are being handled in software.
- The peak periods of cryptographic usage.
- The ICSF services that are being started by other z/OS components.
- The jobs and tasks that are using out-of-date algorithms or key sizes.

Improvements in Auditing for CICS Applications

When the new options dataset keyword CICSAUDIT(YES) is present, ICSF ensures that the SMF records generated by SAF checks made on behalf of the CICS crypto requests contain the CICS client identity and the application id (APPLID).

Key Dataset List (CSFKDSL) Enhancements

The Key Dataset List (CSFKDSL and CSFKDSL6) callable service has been updated to accept a new rule array keyword that allows filtering based on key algorithm as well as a new output format to return more detailed information about the keys that satisfy the input search criteria.

Alleviation of the 2038/2042 Date Restrictions

With ICSF FMID HCR77C1, ICSF removes the restrictions associated with the 2038/2042 timestamps. Where needed, a new timestamp is appended to the bottom of ICSF SMF records containing a full 16-byte timestamp.

Regional Crypto Enablement for International Algorithms

ICSF's support for RCE (Regional Crypto Enablement) was expanded to provide the common international algorithms DES, AES, RSA, and ECC. For more information about the ICSF FMID HCR77C1 release as well as links to its' product publications, see IBM z/OS Downloads (http://ibm.com/systems/z/os/zos/tools/downloads/).

Bob Petti is the z/OS ICSF product owner and has worked on various z/OS projects over the course of his career.

About the author

Bob Petti is the z/OS ICSF Product Owner and has worked on various z/OS projects over the course of his career.