z/OS: ICSF Version and FMID Cross Reference

Abstract: This document describes the relationship between ICSF Web Deliverables, z/OS Releases, and IBM Z cryptographic hardware support, highlights the new functions available in each ICSF web deliverable, and provides a glimpse into the past history of ICSF and IBM Z.

ICSF and z/OS have different release cycles, so it can be confusing trying to determine which release of ICSF matches up with which release of z/OS, especially when you consider that each ICSF release supports multiple z/OS releases, but only one version of ICSF is included in the base z/OS release. Confusing, right? If you throw IBM Z cryptographic hardware releases into the mix, the challenge to make sense of the combinations is daunting.

In brief, ICSF has a generally available (GA) release of a new "web deliverable" in conjunction with every IBM Z hardware release that introduces new cryptographic support. The z/OS release cycle is not the same. While z/OS strives to include the most recently GA'ed version of ICSF, there are times when ICSF will ship new function beyond the point where it is possible to be included with the z/OS base release, thus it is made available separately as a downloadable "web deliverable" (at http://www.ibm.com/systems/z/os/zos/downloads/). These web deliverables will support multiple versions of z/OS and multiple IBM Z hardware systems.

The chart below shows at least two rows for most releases of ICSF: one for the web download and one for the version incorporated into the z/OS base. For example, ICSF FMID HCR77B0 was made available as a web deliverable in February 2015 and supported on the then current operating systems and hardware. There is a separate row for HCR77B0 on z/OS 2.2 since that is the version of ICSF that was shipped with the base release of z/OS 2.2 in September 2015. Note that the planned End of Service column reflects the End of Service for the last release of the operating system that supports the specific level of ICSF.

Remember, although a specific level of ICSF supports multiple IBM Z hardware releases and z/OS releases, do not assume that every combination will be functionally equivalent. The rule of thumb is:

- Newer ICSF FMIDs will typically run on older hardware and exploit the capabilities of that older hardware fully.
    - For example, HCR77C1 was released in conjunction with the z14 system, but can also run on prior systems such as a zEC12 and fully exploit all cryptographic features of that system.
- Older ICSF releases can often run on newer hardware platforms but will typically not exploit the new features of that hardware.
    - For example, HCR77C0 was released alongside the second GA of z13, but can also run on a z14 system. When on z14, however, HCR77C0 has only toleration support for the new CEX6S cryptographic coprocessor. From the HCR77C0's

perspective, the CEX6 is functionally equivalent to the CEX5 that was available in the z13. The new features of the z14 and CEX6 are only available with ICSF HCR77C1 and later web deliverables.

NOTE: Be aware that HCR77A1 or later FMIDs of ICSF no longer support z800/z900 machines when running z/OS V1R13 or later.

As always, be sure to check the appropriate PSP buckets for the latest information when installing ICSF either from a web download, or a part of the z/OS base. Upgrading the ICSF version will always require an IPL because of its reliance on control block information specific to the hardware.

Current ICSF Versions

FMID	External Name	Support Highlights	Applicable z/OS Releases*	Availability	Planned EoS	Supported Servers
HCR77B0	Enhanced Cryptographic Support for z/OS V1R13 - z/OS V2R1	z13 & CEX5 Support, including support for sharing cryptographic coprocessors across a maximum of 85 domains; VISA Format Preserving Encryption (VFPE) services; DK AES PIN and AES MAC Generate and Verify Services; Support for exploitation of counter mode (CTR) for AES-based encryption on z196 and later processors; Enhanced random number generation exploiting CPACF Deterministic Random Number Generate (DRNG) instruction along with the ability to disable the RNG Cache; Services and support for key archiving and key material validity; Enhancement to the ICSF Multi-Purpose service, CSFMPS, for change master key operation dry run	z/OS 1.13; z/OS 2.1	Feb 2015	TBD	z890; z990; z9; z10; z196; z114; zEC12; zBC12; z13; z14**; z15**
	z/OS 2.2		z/OS 2.2	Sep 2015		

HCR77B1	**Cryptographic Support for z/OS V1R13 - z/OS V2R2**	**ICSF Console command support; Regional Cryptographic Enablement*; Support for EMV Simplification services;** Support for **RSAES-OAEP formatting in PKA Decrypt and Encrypt services, Support in Key Generate for CIPHER, DATAC and DATAM keys in OP, IM or EX form; Operational Key Load support for HMAC keys loaded from the TKE; additional DK AES PIN support**	**z/OS 1.13; z/OS 2.1; z/OS 2.2**	**Nov 2015**	TBD	**z890; z990; z9; z10; z196; z114; zEC12; zBC12; z13; z14**; z15****
HCR77C0	**Cryptographic Support for z/OS V2R1 - z/OS V2R2**	Key Lifecycle and Usage Auditing, FIPS mode Auditing, Options Dataset Refresh, Enhanced PKCS #11 Secret Key Encrypt and PKCS #11 Secret Key Decrypt callable services to support clear key AES ciphertext stealing, specifically CS1, No longer requiring the CKDSN and PKDSN keywords to be supplied in the Installation Options Data Set, New ICSF Health Check - ICSF_UNSUPPORTED_CCA_KEYS, Enhanced Digital Signature Generate and Digital Signature Verify callable services to take as input the message to be signed or verified as well as the prehashed message. ICSF enhancements for the Crypto Express5S updates - Note: The following support requires Firmware/MCL updates to both the TKE and the z13 processor. These are considered co-requisites. See the Driver-27 Exception Letter for the latest MCL bundle requirements	**z/OS 2.1; z/OS 2.2**	**Oct 2016**	TBD	**z9; z10; z196; z114; zEC12; zBC12; z13; z14**; z15****
	z/OS 2.3	• Digital Signature Generate, Digital Signature Verify, and PKA Key Token Build callable services for RSA-PSS Signatures • PKA Key Generate and PKA Key Token Build callable services expanded to support selectable public exponents in the generation of RSA private/public key pairs	**z/OS 2.3**	**Sept. 2017**		
HCR77C1	**Cryptographic Support for z/OS V2R1 - z/OS V2R3**	Support for z14 processors and Crypto Express6S include support for a PCI HSM ("Payment Card Industry Hardware Security Module") configured CCA coprocessor: • A TKE ("Trusted Key Entry") workstation is required to administer a PCI HSM-compliant CCA coprocessor. In addition to PCI HSM support, CEX6S also introduces the use of X.509 certificates in CCA. • A TKE is used to manage root and signing certificates installed within the coprocessor. • A new ICSF callable service Public Infrastructure Request (CSNDPIC) is available to generate PKCS#10 certificate requests. • The Digital Signature Verify (CSNDDSV) service has been updated to support the use of an X.509 certificate when verifying a signature. Additional enhancements to ICSF available in this download provide	**z/OS 2.1; z/OS 2.2; z/OS 2.3**	**Sept 2017**	**TBD**	**z9; z10; z196; z114; zEC12; zBC12; z13; z14; z15****

support for:

- New z14 CPACF instructions for SHA-3 hashing, TRNG (True Random Number Generation), and improved performance of AES GCM encryption.
- A new ability to monitor crypto usage tracking.
  - New SMF Type 82 Subtype 31 records to indicate use of:
    - Specific hardware or software crypto engines
    - Cryptographic algorithms
    - ICSF callable services
- An improvement to Key Dataset List (CSNKDSL) service to provide additional search criteria and more details on the returned output. (**Note:** This improvement is available on ICSF HCR77C0 with APAR OA52145.)
- An ISPF-based browser for the Crypto Key Dataset (CKDS).
- Improvements to the auditing of CICS applications that make use of ICSF resources. (**Note:** This improvement is only available on z/OS V2.3.)
- The ability to use secure key tokens for the Field Level Encipher and Field Level Decipher (CSNBFLE, CSNBFLD) services. (**Note:** This function is also available on ICSF HCR77B1 and HCR77C0 with APAR OA51102.)
- Support for standard international cryptographic algorithms such as DES, AES, RSA, and ECC via ICSF's Regional Cryptographic Enablement with the implementation of those algorithms provided by IBM approved RCE vendor hardware.*

HCR77D0	**Cryptographic Support for z/OS V2R2 – z/OS V2R3**	ICSF enhancements for Crypto Express5S (CCA Release 5.4 and later) and Crypto Express6S (CCA Release 6.1 and later): • ISO-4 format PIN blocks as described in the ISO-9564-4 standard. In addition to a new service, PIN Translate 2 (CSNBPTR2), the following services will be updated to support ISO-4 format PIN blocks: Clear PIN Encrypt (CSNBCPE), DK PIN Verify (CSNBDKPV), DK PIN Change (CSNBDKPC), DK PAN Modify in Transaction (CSNBDKMT). • Three-key TDES Keys. Currently, only DATA key types are available in 3-key TDES key types. This enhancement allows for the following key types to be operational as a 3-key TDES key: CIPHER, ENCIPHER, DECIPHER, EXPORTER, IMPORTER, MAC, MACVER, IPINENC, OPINENC, PINGEN, PINVER. • DK Key Diversification. The German Banking Industry Committee (GBIC) has introduced a new key diversification scheme such that a single diversification key can be used to generate keys with different key usage attributes. A new key type is introduced, KDKGENKY, as well as a new callable service Diversify Directed Key (CSNBDDK). The following callable services are updated in support of DK Key Diversification: Diversified Key Generate 2 (CSNBDKG2), Key Token Build 2 (CSNBKTB2), Key Generate 2 (CSKBKGN2). • ISO-20038 Key Wrapping. In support of the ISO-20038 standard, the TR-31 Import (CSNBT31I) and TR-31 Export (CSNBT31X) callable services will be updated to use AES IMPORTER and EXPORTER key types for key wrapping. ICSF enhancements for Crypto Express6S (CCA Release 6.2), in addition to those above: • Symmetric keys can now be restricted from being eligible for CPACF protected key. With updated flags in the control vector, it is possible to mark a key as either eligible or ineligible for being exported for CPACF use as a protected key. In addition, CCA 6.2 provides the ability for 3-key TDES	**z/OS 2.2; z/OS 2.3**	**Dec 2018**	**TBD**	**z10; z114; z196; zEC12; zBC12; z13; z14; z15****

	z/OS 2.4	keys to be “tagged” such that they are restricted to PCI HSM compliance usage.
		Additional enhancements to ICSF available in this download provide support for:
		• CCA redirection for Regional Crypto Enablement. Certain CCA callable services will have the ability to direct the request to a regional crypto device. This enhancement introduces the concept of "RCS Redirection" through a new XFACILIT resource, and adds the concept of an "RCS Token" to existing symmetric key token types.*
		• ChaCha20 and Poly1305 algorithms. These new algorithms will be available via the PKCS#11 interfaces and clear key only.
		• Applying service to a running ICSF instance without causing an interruption to their applications. When ICSF service is available on a system, ICSF will have a new operator command that will allow running requests to finish, pause incoming requests, prepare to restart with the service libraries, and then stop ICSF. Through system automation (preferred), ICSF will be restarted and the paused requests will be resumed without a visible interruption.
		• Early ICSF. ICSF will now be able to start much earlier in the IPL process, such that ICSF should be available for work as early as full function start. ICSF is also adding new ways to provide installation options via a more standard PARMLIB interface.
		• KGUP. KGUP can be made to honor CSFKEYS resource profiles, configured to require higher permission when performing destructive operations on an existing key (such as UPDATE or DELETE), permit a user or group to a CSFKEYS resource but only for specific callable services, and have ICSF prepend a system name to a CSFKEYS resource prior to the SAF check.
		• A new ISPF browser added for the PKDS.
		• The 32-byte limit on the CKA_LABEL attribute of PKCS#11 key objects
		  ○ The limit has been lifted.
		• Providing a CKDS label of a clear key to the CSNBKYT service.
		• The key verification pattern written to SMF records after a successful Operational Key Load function.
		  ○ Will honor the MASTERKCVLEN keyword in the ICSF installation options dataset.
		• The Operational Key Load ISPF Panel utility.
		  ○ Allows the specification of the key wrapping scheme when importing the key.
		• A new BSI mode. BSI 2017 has been added to the EP11 Coprocessor.
		• Callable services PKCS#11 Wrap Key (CSFPWPK) and PKCS#11 Unwrap Key (CSFPUWK)
		  ○ Updated to accept AES-GCM as a key wrapping mechanism for secret and private clear keys
		• A new DISPLAY ICSF, MKVPs operator command.
		  ○ Used to display the master key verification patterns recorded in the ICSF key data stores in comparison with the same MKVPs in online crypto coprocessors in such a way that discrepancies can be detected.
			z/OS 2.4	**Sep. 2019**		

HCR77D1	**Cryptographic Support for z/OS V2R2 – z/OS V2R3**	• The new Crypto Express7S adapter, configured as a CCA coprocessor, an EP11 coprocessor, or as an accelerator. With the IBM z15, a system can host three generations of crypto express coprocessors simultaneously—the CEX5,	**z/OS 2.2; z/OS 2.3;**	**Sep. 2019**	**TBA**	**z10; z114; z196; zEC12;**

	CEX6, and the CEX7. • The ability to use CP Assist for Cryptographic Functions (CPACF) for certain clear key ECC operations. ICSF can now call CPACF instructions to perform ECC key generation, key derivation, and digital signature generation and verification using a subset of the NIST curves. The CPACF on IBM z15 also supports the ED448 and EC25519 curves. • A new SMF record whenever a master key is changed. Certain compliance regulations mandate the periodic rotation of encryption keys, including the master keys loaded into coprocessors. As part of the master key change process, an SMF record will now be written every time the new master key is promoted to the current master key as part of the change master key ceremony. • A health check that verifies a system's ability to use the NIST recommended PKCS PSS signature algorithms. It is not obvious that the ECC master key is required when generating and using RSA keys enabled for PKCS PSS signatures, so a health check will help convey the need for this additional master key to exploit the recommended algorithms. • New quantum safe algorithms for signing and verification operations. With this release of ICSF, it is now possible to use quantum safe encryption algorithms for digital signature operations, which also includes the ability to generate and store new keys. These algorithms will be clear key only and available via the PKCS#11 interfaces only at this time. • ICSF enhancements for Crypto Express5S (CCA Release 5.5) and Crypto Express6S (CCA Release 6.3): o New services in support of ANSI TR-34 Remote Key Loading o PCI Compliance for AES and RSA keys o New PIN services for the DK customers o NOTE: These functions were made available on HCR77D0 with PTFs for APAR OA57089	**z/OS 2.4**		**zBC12; z13; z14; z15**

Pink => Older version, but still available for download	****Older versions of ICSF may need toleration maintenance installed to support newer hardware** *** For China market only.**
Yellow => planned	
Light blue => Version shipped with z/OS	
Green => Most current version, available via web download	

Historical ICSF Versions (No longer supported)

FMID	External Name	Support Highlights	Applicable z/OS Releases*	Availability	EoS	Supported Servers
HCR7740	Cryptographic Support for z/OS V1R6/R7 and z/OS.e V1R6/R7 z/OS 1.9	PKCS #11 APIs	z/OS 1.9	Sep 2007	Sep 2010	z800; z900; z890; z990; z9; z10**, z196**
HCR7750	Cryptographic Support for z/OS V1R7-z/OS V1R9 and z/OS.e V1R7-V1R8 z/OS 1.10	Support ISO Format 3 PIN Blocks and RSA Keys up to 4096-bits; Enhanced TKE Auditing Support; New Random Number Generate Long API; Enhancements to CPACF; CEX2 Dynamic Add; Add support for AES-192 & AES-256, SHA-512	z/OS 1.7; z/OS 1.8; z/OS 1.9; z/OS.e 1.7; z/OS.e 1.8 z/OS 1.10	Nov 2007 Sep 2008	Sep 2011	z800; z900; z890; z990; z9; z10**, z196**, z114**, zEC12***
HCR7751	Cryptographic Support for z/OS V1R8-z/OS V1R10 and z/OS.e V1R8 z/OS 1.11	Support for 13-Digit through 19-Digit PAN data; New Crypto Query Service; Keystore Policy; Secure Key AES; TKE 5.3	z/OS 1.8; z/OS 1.9; z/OS 1.10 z/OS 1.11	Nov 2008 Sep 2009	Sep 2012	z800; z900; z890; z990; z9; z10**, z196**, z114**, zEC12***
HCR7770	Cryptographic Support for z/OS V1R9-V1R11 z/OS 1.12	Protected Key CPACF; Crypto Express3; Extended PKCS #11 Support; Elliptic Curve Cryptography (ECC) Support	z/OS 1.9; z/OS 1.10; z/OS 1.11 z/OS 1.12	Nov 2009 Sep 2010	Sep 2014	z800; z900; z890; z990; z9; z10, z196**, z114**, zEC12**
HCR7780	Cryptographic Support for z/OS V1R10-V1R12 z/OS 1.13	z196 Support (MSA-4 Instructions); CCA Elliptic Curve (ECDSA, ECDH); ANSI X9.8 & ANSI X9.24 Enhancements; HMAC (with OA33260); TKE 7.0; 64-bit support for all APIs; Enhance logging for PCI Audit; CKDS constraint relief	z/OS 1.10; z/OS 1.11; z/OS 1.12 z/OS 1.13	Sep 2010 Sep 2011	Sep 2016	z800#; z900#; z890; z990; z9; z10; z196 ; z114; zEC12**; zBC12**; z13** # Variable Length CKDS is not supported on z800 or z900
HCR7790	Cryptographic Support for z/OS V1R11-V1R13	Coordinated KDS Administration; Expanded CCA key support for AES algorithm; Enhanced ANSI TR-31 Interoperable secure key exchange; PIN block decimalization table protection; PKA RSA OAEP with SHA-256 algorithm; Additional ECC functions; TKE 7.1	z/OS 1.11; z/OS 1.12; z/OS 1.13	Sep 2011	Sep 2016	z800#; z900#; z890; z990; z9; z10; z196 ; z114; zEC12**; zBC12**; z13** # Variable Length CKDS is not supported on z800 or z900
HCR77A0	Cryptographic Support for z/OS V1R12-V1R13	zEC12 & CEX4S Support, including Enterprise PKCS #11 (EP11); KDS Administration support for the PKDS (RSA-MK/ECC-MK) and TKDS (P11-MK) including improved I/O performance on these key datasets; 24-byte DES Master Key support; New controls for weak key wrapping; DUKPT for MAC and Encryption	z/OS 1.12; z/OS 1.13	Sep 2012	Sept 2018	z800; z900; z890; z990; z9; z10; z196; z114; zEC12; zBC12; z13**; z14** # Variable Length CKDS is not supported on z800 or on z900

		Keys; **FIPS compliant RNG and Random Number cache;** **Secure Cipher Text Translate;** **EMV Enhancements for Amex cards**				**Note:** **z/OS 2.1 will only run on a z9 or later machine, however HCR77A0 is supported all the way back to the z800/z900**
	z/OS 2.1		**z/OS 2.1**	**Sep 2013**		
HCR77A1	**Cryptographic Support for z/OS V1R13 - z/OS V2R1**	**AP Configuration Simplification including new Health Checker;** **KDS Key Utilization Statistics;** **Dynamic SSM; UDX Reduction & Simplification; EMV Enhancements;** **SAF checks for OWH & RNG;** **SAF ACEE Selection;** **Non-SAF Protected IQF;** **RKX Key Export Wrapping;** **AES MAC Enhancements;** **PKCS #11 (EP11) Enhancements;** **Improved CTRACE support**	**z/OS 1.13;** **z/OS 2.1**	**Sep 2013**	**Sept 2018**	**z890; z990; z9; z10; z196; z114; zEC12; zBC12; z13**;z14****