z/OS: ICSF Version and FMID Cross Reference

Abstract: ICSF is a component of z/OS and ships with the base product. It is the software component that provides access to the System z crypto hardware. As new hardware becomes available, updates and functionality are added to ICSF outside of the z/OS release cycle. This document provides a history of the ICSF versions, the supported hardware and operating system releases and highlights the new capability within each version, through Cryptographic Support for z/OS V1R13-V2R1, HCR77A1.

ICSF is a software component of z/OS providing cryptographic support either in its own software routines or through access to the cryptographic hardware available on the platform. Updates to ICSF outside of the z/OS release cycle are available as web downloads (at http://www.ibm.com/systems/z/os/zos/downloads/). With each new release of z/OS, a version of ICSF is incorporated as part of the base, but it may not be the latest version available, leading to confusion.

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, HCR77A0 was made available as a web download in September, 2012 and supported on the then current operating systems and hardware. There is a separate row for HCR77A0 on z/OS 2.1 since the FMID was shipped with z/OS 2.1 in September, 2013. 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.

Just because a specific level of ICSF is supported on a particular hardware platform and operating system, does not imply that it will take advantage of all the hardware capability. ICSF is very robust and to some extent, very upward and downward compatible. That is, new ICSF FMIDs will usually run on old hardware, and old ICSF FMIDs will generally run on new hardware. However, the old levels of ICSF will not take advantage of new hardware functions, and new levels of ICSF cannot use functions that are not available in the hardware where it runs. For example, HCR77A0 introduces support for the Crypto Express4S card, however this version of ICSF will also run on the z9 and z10 which do not support the CEX4S. Obviously, the functionality of the CEX4S is not available on these machines even when running HCR77A0. Also be aware that HCR77A1 will 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.

The TechDoc WP100810, ‘A Synopsis of System z Crypto Hardware’ provides an introduction to the crypto hardware capabilities.

Current ICSF Versions

FMID	External Name	Support Higlights	Applicable z/OS Releases*	Availability	Planned EoS	Supported Servers
HCR7770	Cryptographic Support for z/OS V1R9-V1R11	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	Nov 2009	Sep 2014	z800; z900; z890; z990; z9; z10, z196**, z114**, zEC12**
	z/OS 1.12		z/OS 1.12	Sep 2010		
HCR7780	Cryptographic Support for z/OS V1R10-V1R12	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	Sep 2010	Sep 2016	z800#; z900#; z890; z990; z9; z10; z196 ; z114, zEC12** #Variable Length CKDS is not supported on z800 or z900
	z/OS 1.13		z/OS 1.13	Sep 2011		
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** #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 Keys; FIPS compliant RNG and Random Number cache; Secure Cipher Text Translate; EMV Enhancements for Amex cards	z/OS 1.12; z/OS 1.13	Sep 2012	Sep 2018	z800; z900; z890; z990; z9; z10; z196; z114; zEC12 #Variable Length CKDS is not supported on z800 or on z900 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	Sep 2018	z890; z990; z9; z10; z196; z114; zEC12

Pink => Older version, but still available for download

Orange => Web download, or z/OS release no longer available

Yellow => planned

Light blue => Version shipped with z/OS

Green => Most current version, available via web download

**Older versions of ICSF may need toleration maintenance installed to support newer hardware

z/OS: ICSF Version and FMID Cross Reference

Historical ICSF Versions

FMID	External Name	Support Higlights	Applicable z/OS Releases	Availability	Planned EoS	Supported Servers
HCR7706	z/OS 1.3	New ISPF Panels	z/OS 1.3	Mar 2002	Mar 2005	G5; G6; z800; z900
	z/OS 1.4		z/OS 1.4	Sep 2002	Mar 2007	G5; G6; z800; z900
HCR7708	z990 Cryptographic CP Assist Support for z/OS V1.3	z990 Compatability	z/OS 1.3	Jun 2003	Mar 2005	G5; G6; z800; z900
	z/OS V1.4 z990 Compatibility Support Feature		z/OS 1.4	Jun 2003	Mar 2007	G5; G6; z800; z900; z890; z990
	z/OS V1.4 z990 Exploitation Support Feature		z/OS 1.4	Oct 2003	Mar 2007	
	z/OS 1.4		z/OS 1.4	Oct 2003	Mar 2007	
	z/OS 1.5		z/OS 1.5	Mar 2004	Sep 2007	
HCR770A	z990 Cryptographic Support	Support PCIXCC feature; New ISPF Panels	OS/390 2.10; z/OS 1.2; z/OS 1.3	Sep 2003	Mar 2005	G5; G6; z800; z900; z890; z990
	z990/z890 Cryptographic Support		z/OS 1.4; z/OS 1.5	Sep 2003	Mar 2007	G5; G6; z800; z900; z890; z990; z9
	z/OS 1.6		z/OS 1.6	Sep 2004	Sep 2007	z800; z900; z890; z990; z9
HCR770B	z990 and z890 Enhancements to Cryptographic Support *	Operational Key Entry; CSFIQF API; z890/z990 PKE/PKD Enhancements; DUKPT; EMV 2000 Support	OS/390 2.10; z/OS 1.2; z/OS 1.3; z/OS 1.4; z/OS 1.5; z/OS 1.6; z/OS.e 1.3-1.6	May 2004	Sep 2007	G5; G6; z800; z900; z890; z990; z9
HCR7720	ICSF 64-bit Virtual Support for Z/OS V1R6 and z/OS.e V1R6	64-bit support; Support CEX2 (in the default configuration of a coprocessor, i.e. CEX2C); Card Verification Value for 19-digit PANs	z/OS 1.6	Dec 2004	Sep 2007	z800; z900; z890; z990; z9
	z/OS 1.7		z/OS 1.7	Sep 2005	Sep 2008	z800; z900; z890; z990; z9; z10
HCR7730	Cryptographic Support for z/OS V1R6/R7 and z/OS.e V1R6/R7	z9 (AES-128 & SHA-256 on CPACF); SYSPLEXCKDS; Support configuration of CEX2 accelerator (CEX2A)	z/OS 1.6; z/OS 1.7	Sep 2005	Sep 2008	z800; z900; z890; z990; z9; z10
HCR7731	Enhancements to Cryptographic Support for z/OS and z/OS.e V1R6/R7	ATM Remote Key	z/OS 1.6; z/OS 1.7	May 2006	Sep 2008	z800; z900; z890; z990; z9; z10**, z196**
	z/OS 1.8		z/OS 1.8	Sep 2006	Sep 2009	
HCR7740	z/OS 1.9 (aka Cryptographic Support for z/OS V1R6/R7 and z/OS.e V1R6/R7)	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	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	Nov 2007	Sep 2011	z800; z900; z890; z990; z9; z10**, z196**, z114**, zEC12***
	z/OS 1.10		z/OS 1.10	Sep 2008	Sep 2011	
HCR7751	Cryptographic Support for z/OS V1R8-z/OS V1R10 and z/OS.e V1R8	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	Nov 2008	Sep 2012	z800; z900; z890; z990; z9; z10**, z196**, z114**, zEC12***
	z/OS 1.11		z/OS 1.11	Sep 2009		
	Orange => Web download, or z/OS release no longer available					