IBM® z/OS® Version 2 Release 1 System SSL Cryptographic Module

FIPS 140-2

Non-Proprietary Security Policy

Policy Version v1.2

IBM Systems & Technology Group
System z Development
Poughkeepsie, New York

January 27, 2017

Table of Contents

1. SCOPE OF DOCUMENT 3
2. CRYPTOGRAPHIC MODULE SPECIFICATION 3
3. CRYPTOGRAPHIC MODULE SECURITY LEVEL 5
4. PORTS AND INTERFACES 6
5. ROLES, SERVICES AND AUTHENTICATION 7
5.1 ROLES 7
5.2 SERVICES 7
6. OPERATIONAL ENVIRONMENT 12
7. KEY MANAGEMENT 16
8. PHYSICAL SECURITY 17
9. EMI/EMC 20
10. SELF-TESTS 20
10.1 SYSTEM SSL MODULE 20
11. OPERATIONAL REQUIREMENTS (OFFICER/USER GUIDANCE) 21
11.1 MODULE CONFIGURATION FOR FIPS 140-2 COMPLIANCE 21
11.2 DETERMINING MODE OF OPERATION 22
11.3 TESTING/PHYSICAL SECURITY INSPECTION RECOMMENDATIONS 23
12. MITIGATION OF OTHER ATTACKS 23
13. CRYPTOGRAPHIC MODULE CONFIGURATION DIAGRAMS 23
14. GLOSSARY 24
15. REFERENCES 25
16. TRADEMARKS 26

1. Scope of Document

This document describes the services that the z/OS System SSL cryptographic module ("System SSL module" or "module") provides to security officers and end users, and the policy governing access to those services by the z/OS System SSL element. It complements official z/OS System SSL element documentation, which concentrates on application programming interface (API) level usage and environmental setup [1].

The z/OS System SSL cryptographic module provides cryptographic functionality, ASN.1 processing, x.509 certificate, PKCS #7 and data conversion functionality for use by the System SSL element of z/OS (hereafter referred to as "System SSL element"). The z/OS System SSL cryptographic module in its FIPS 140-2 configuration consists of a single shared library (DLL). The shared library binary is either a 31 or 64-bit version. The deployed version consists of the following modules:

Table 1: System SSL Library Modules

31-bit	64-bit
GSKC31F	GSKC64F

The z/OS System SSL cryptographic module is packaged within the System SSL element of z/OS. The System SSL element contains external application programming interfaces (APIs) which allows host applications to utilize functionality within the System SSL element and the z/OS System SSL cryptographic module. Communication to the z/OS System SSL cryptographic module is through C-language applications programming interfaces (APIs) known only to the System SSL element's DLLs and executables. These DLLs and executables are not part of the cryptographic module. All interfaces to the System SSL module are through the System SSL element.

The z/OS System SSL cryptographic module does not implement the TLS protocol. It provides the cryptographic primitives (ie. Key Derivation Function (KDF)) and functions to allow the System SSL element to support TLS.

2. Cryptographic Module Specification

The z/OS System SSL cryptographic module is classified as a *multi-chip standalone software-hybrid module* for **FIPS Pub 140-2** purposes. The actual cryptographic boundary for this FIPS 140-2 module validation includes the System SSL module running in configurations supplemented by hardware cryptography. The System SSL module consists of software-based cryptographic algorithms, as well as symmetric and hashing algorithms provided by the CP Assist for Cryptographic Function (CPACF).

The System SSL module uses the z/OS Version 2 Release 1 Security Server RACF Signature Verification (hereafter referred to as "IRRPVERS") with FIPS 140-2 Validation #2691 for module integrity checking services.

The System SSL module uses the z/OS Version 2 Release 1 ICSF PKCS #11 (hereafter referred to as "ICSF PKCS #11") with FIPS 140-2 Validation #2763 for certified cryptographic algorithms not available within the System SSL module (ie. random number generation) and hardware RSA signature verification and key wrapping.

The IRRPVERS and ICSF PKCS #11 are also known as "bound" modules.

Table 2: System SSL Module Components

Type/Name	Version
Software Components System SSL DLLs (GSKC31F and GSKC64F)	z/OS Version 2 Release 1 with System SSL level HCPT410/JCPT411 with APAR OA50589
Hardware Components CPACF	Firmware - CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 (aka FC3863) with System Driver Level 22H Hardware – COP chips integrated within processor unit
Documentation	APAR OA50589 PDF SC14-7495-00 *z/OS System SSL Programming*

System SSL module validation was performed using the z/OS Version 2 Release 1 operating system with the following platform configurations:

1. IBM z13 with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 (Base GPC)

2. IBM z13 with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 and optional Crypto Express5 card (Accelerator (CEX5A)) - CEX5A card maybe used by ICSF PKCS#11 for RSA hardware clear key module math cryptography to support RSA digital signature verification and key wrapping.

The System SSL module running on the above platforms met all **FIPS Pub 140-2** Level 1 security requirements.

See Section 13, Cryptographic Module Configuration Diagrams, for more information about the validated platforms.

In addition to the configurations tested by the laboratory, vendor-affirmed testing was performed using z/OS Version 2 Release 1 on the following platforms:

1. IBM System zEnterprise™ EC12 (zEC12) with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 (Base GPC)

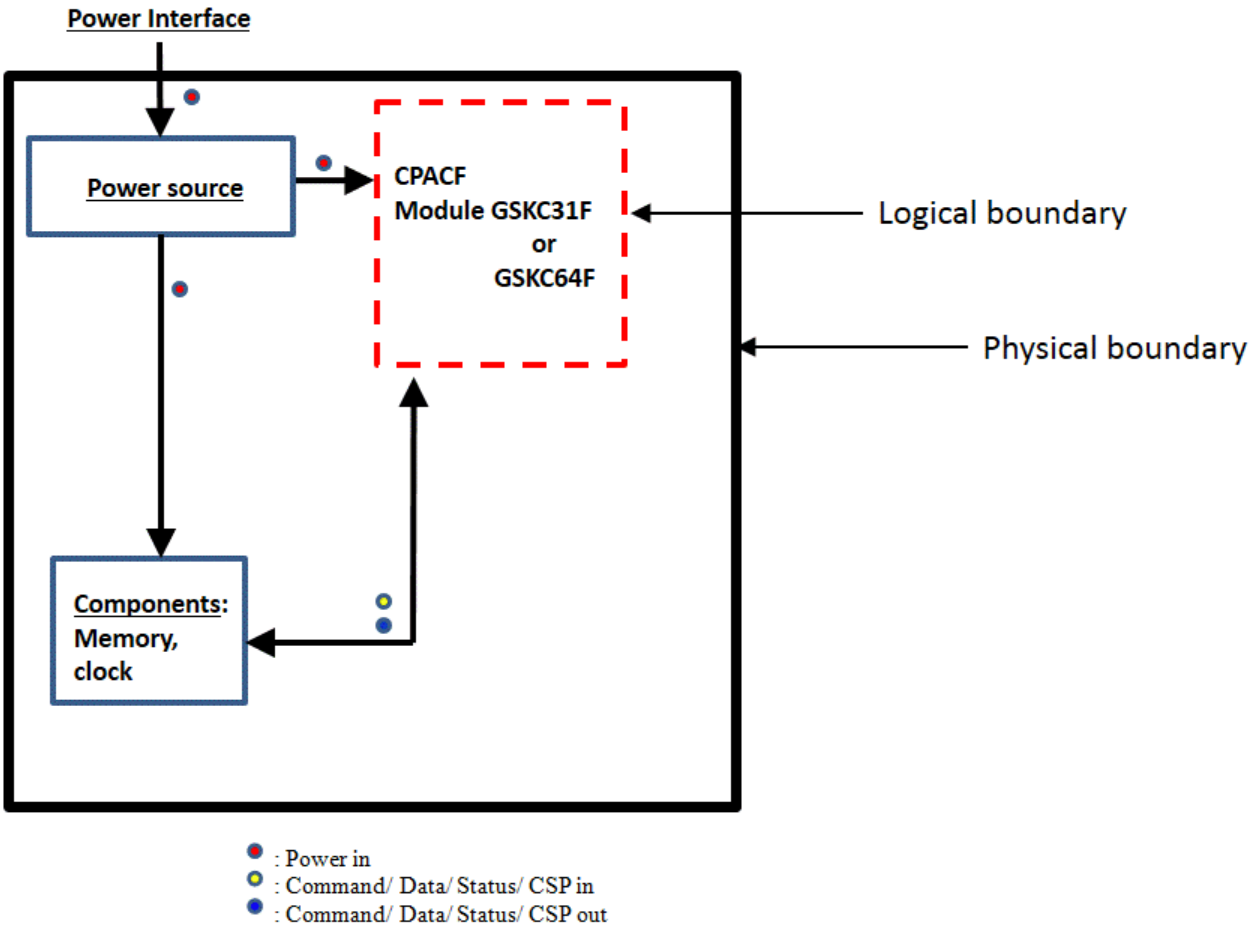
2. IBM System zEnterprise™ BC12 (zBC12) with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 (Base GPC).

Note (IG G.5): the CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported and executed in an operational environment not listed on the validation certificate.

Security level: This document describes the security policy for the z/OS System SSL module with Level 1 overall security as defined in **FIPS Pub 140-2** [2].

Figure 1 below shows the physical boundary of the System z machine as well as the logical boundary of the module. A more detailed view consisting of the module and bound modules is shown Figure 2 in the Cryptographic Module Configuration Diagrams section.

Figure 1: System SSL Cryptographic Module Physical and Logical Boundaries



3. Cryptographic Module Security Level

The System SSL module is intended to meet requirements of Security Level 1 overall, with certain categories of security requirements not applicable (Table 3).

Table 3: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	1

Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of other attacks	N/A
Overall	1

4. Ports and Interfaces

As a multi-chip standalone module, the System SSL module physical interfaces are the boundaries of the host running System SSL module code. The underlying logical interfaces of the module are internal application programming interfaces (APIs) to the System SSL element and logical interfaces to the ICSF PKCS #11 module.

Table 4: Data input, data output, control input and status output

Interfaces into and out of the Module		
FIPS 140-2 Interface	**Logical Interface**	**Description**
Data Input	API	Input variables are passed on the internal application programming interface (API)
Data Output	API	Output results are passed back through the API
Control Input	API function calls and environment variable	Setting of GSK_HW_CRYPTO environment variable
Status Output	API return codes	Status output is provided in return codes
Power	Not applicable	Not applicable
Interface between module and ICSF PKCS #11		
FIPS 140-2 Interface	**Logical Interface – ICSF PKCS #11 APIs (CSFPPD2, CSFPPE2, CSFPPV2)**	**Description**
Data Input	API	Input variables passed on the ICSF PKCS #11 API invocation
Data Output	API	Output results passed back by the ICSF PKCS #11 API
Control Input	API	ICSF PKCS #11 vendor defined PKCS #11 attribute CKA_IBM_FIPS140 passed on API invocation
Status Output	API return and reason codes	Status output returned from ICSF PKCS #11 API as return and reason codes

Cryptographic bypass capability is not supported by the System SSL module.

Module Status: The System SSL module communicates any error status synchronously through the use of return codes to the System SSL element which then surfaces them to the calling application. A complete list of return codes returned by the System SSL element are provided in the System SSL element documentation. It is the responsibility of the application to handle exceptional conditions in a FIPS 140-2 appropriate manner.

The System SSL module is optimized for library use and does not contain any terminating assertions or exceptions. Any internal error detected by the System SSL module and not induced by user data will be reflected back to the application

with an appropriate return code. The calling application must examine the return code and act in a FIPS 140-2 appropriate manner to such failures and reflect this error in a fashion consistent with this application.

User-induced or internal errors do not reveal any sensitive material to callers. Return codes and error conditions surfaced by the System SSL element are fully documented in the System SSL element's programming documentation.

5. Roles, Services and Authentication

5.1 Roles

The module supports two roles: a cryptographic officer (Officer) role and a User role (Table 5). The module does not support user identification or authentication that would allow the module to distinguish between the two supported roles. Each of the roles is authenticated through the operating system prior to using any system services.

The Officer role is a purely administrative role that does not involve the use of cryptographic services. The role is not explicitly authenticated but assumed implicitly on implementation of the module's installation and configuration.

The User role has access to all of the module's services. The role is not explicitly authenticated, but assumed implicitly on access of any of the non-Officer services. An operator is implicitly in the User or Officer role based upon the service(s) chosen. If any of the User-specific services are called, then the operator is in the User role; otherwise the operator is in the Officer role.

Table 5: Roles and Authentication Mechanisms

Role	Purpose/Permitted Actions	Type of Authentication	Authentication Data	Strength of Mechanism
User	Request the cryptographic algorithms list in tables 6 and 7	None (Automatic)	None	N/A
Officer	Module installation and configuration. This role does not involve the use of cryptographic services.	Implicit	N/A	N/A

5.2 Services

The module provides commands (services - Tables 6, 7 and 8) and queries (Table 9). Queries return status of commands or command groups; commands exercise cryptographic functions or services. Officers perform queries; Users may perform both queries and commands..

Services are accessed through System SSL element API interfaces from the calling host application.

The System SSL module provides both non-cryptographic and cryptographic services. The non-cryptographic services can be utilized by the calling application (i.e. x.509 certificate encoding/decoding) without causing any impact to the module's cryptographic support.

Cryptographic primitives (i.e. Key Derivation Function (KDF), AES encrypt/decrypt) provide the required cryptographic primitives for the System SSL element to support the TLS protocol. The cryptographic algorithms associated with the TLS ciphers are restricted to FIPS approved algorithms only.

Additional services and processing are provided by bound modules IRRPVERS and ICSF PKCS #11. The System SSL module utilizes the module integrity checking services provided by IRRPVERS and the cryptographic services provided by ICSF PKCS #11.

Table 6: Approved Services

(There are algorithms that have been CAVS tested with key sizes and block chaining modes for which the module does not provide interfaces. Only the algorithms' key sizes and block chaining modes present in this table are made available by the module.)

Service	Roles		CSP	Modes / Notes	Cert #	Access (Read, write, execute)	Standard
	User	Crypto Officer					
Module installation And Configuration		X	N/A	N/A	N/A	N/A	N/A
Software							
Symmetric Algorithms							
AES Encryption and Decryption	X		AES Symmetric key (128, 256 bit)	CBC	4083 4084	Read Write Execute	FIPS 197 SP 800-38A
Triple DES Encryption And Decryption	X		Triple DES Symmetric key (192 bit)	CBC	2230 2231	Read Write Execute	SP 800-67
Public Key Algorithms							
DSA Parameter/Key Generation	X		DSA Parameter And Asymmetric keys L=2048, N=256	N/A	1108 1109	Read Write Execute	FIPS 186-4
DSA Signature Generation	X		DSA Asymmetric Private Key L=2048, N=256 with SHA[2](1/224/256)	SHA-1 affirmed for use with protocols only.	1108 1109	Read Write Execute	FIPS 186-4
DSA Signature Verification	X		DSA Asymmetric Public Key L=1024,N=160 with SHA(1/224/256) L=2048,N=256 with SHA (1/224/256)	N/A	1108 1109	Read Execute	FIPS 186-4
RSA Key generation	X		RSA Asymmetric Key 2048 and 3072	N/A	2210 2211	Read Write Execute	FIPS 186-4
RSA Signature Generation	X		RSA Asymmetric Private Key	SHA-1 affirmed for use	2210 2211	Read Write	FIPS 186-4

			2048 and 3072 with SHA[2] (1/224/256/384/512)	with protocols only.		Execute	
RSA Signature Verification	X		RSA Asymmetric Public Key 2048 and 3072 with SHA (1/224/256/384/512)	N/A	2210 2211	Read Execute	FIPS 186-4
Hash Functions							
SHS Message Digest	X		N/A	SHA -1 SHA-224 SHA-256 SHA-384 SHA-512	3361 3362	N/A	FIPS 180-4
Message Authentication Codes (MACs)							
HMAC Message Authentication	X		Key sizes 112 bits in length and greater[1]	HMAC SHA-1, HMAC SHA-256 HMAC SHA-384	2665 2666	Read Write Execute	FIPS 198-1
Component							
TLS Key Derivation	X		TLS V1.0, V1.1, V1.2 premaster secret, read MAC key, read key, read IV, write MAC key, write key and write IV	N/A	901 902	Read Write Execute	SP 800-135
CP Assist for Cryptographic Functions							
Symmetric Algorithms							
AES Encryption and Decryption	X		AES Symmetric key (128, 256 bit)	CBC	3958	Read Write Execute	FIPS 197 SP 800-38A
Triple DES Encryption And Decryption	X		Triple DES Symmetric key (192 bit)	CBC	2214	Read Write Execute	SP 800-67
Hash Function							
SHS Message Digest	X		N/A	SHA -1 SHA-224 SHA-256 SHA-384 SHA-512	3196	Read Write Execute	FIPS 180-4
Hybrid							
Public Key Algorithms							
DSA Signature Generation	X		DSA Asymmetric Private Key L=2048, N=256 with	SHA-1 affirmed for use with protocols only	1119 1120	Read Write Execute	FIPS 186-4

			SHA[2] (1/224/256)				
DSA Signature Verification	X		DSA Asymmetric Public Key L=1024,N=160 with SHA(1/224/256) L=2048,N=256 with SHA (1/224/256)	N/A	1119 1120	Read Execute	FIPS 186-4
RSA Signature Generation System SSL RSA with CPACF SHA	X		RSA Asymmetric Private Key 2048 and 3072 with SHA[2] (1/224/256/384/512)	SHA-1 affirmed for use with protocols only.	2231 2232	Read Write Execute	FIPS 186-4
RSA Signature Verification Various combination of ICSF PKCS #11 RSA with either System SSL or CPACF SHA	X		2048 and 3072 with SHA[2] (1/224/256/384/512)	N/A	2231 2232 2240 2241 2242 2243 2244 2245 2246 2247	Read Execute	FIPS 186-4
Message Authentication Codes (MACs)							
Message Authentication Codes (MACS) CPACF SHA	X		Key sizes 112 bits in length and greater[1]	HMAC SHA-1, HMAC SHA-256 HMAC SHA-384	2697 2698	Read Write Execute	FIPS 198-1
Component							
TLS Key Derivation CPACF SHA	X		TLS V1.0, V1.1, V1.2 premaster secret, read MAC key, read key, read IV, write MAC key, write key and write IV	N/A	934 935	Read Write Execute	SP 800-135

Notes:
1. Per FIPS 198-1 and SP 800-107, keys less than 112 bits in length are not approved for HMAC generation.
2. Use of SHA1 for digital signature generation is deprecated and should not be used.

Table 7: Allowed Services

Service	Roles		CSP	Access (Read, write, execute)	Standard	Caveat
	User	Crypto Officer				
RSA Key Wrapping	X		RSA Asymmetric Private Key	Read Write	N/A	key wrapping; key establishment methodology

			Modulus size from at least 2048 and up to 4096 bits	Execute		provides between 112 and 150 bits of encryption strength
RSA Digital Signature Generation	X		RSA Asymmetric Private Key Modulus size 2048 and up to 4096 bits (except 2048 and 3072 bits)	Read Write Execute	FIPS 186-4	N/A
RSA Digital Signature Verification	X		RSA Asymmetric Public Key Modulus size between 1024 and 4096 bits (except 2048 and 3072 bits)	Read, Execute	FIPS 186-2 FIPS 186-4	N/A
RSA Key Generation	X		RSA Asymmetric Private and Public Key Key lengths multiple of 16 bits between 2048 and 4096 bits (except 2048 and 3072 bits)	Read, Write, Execute	FIPS 186-4	N/A
Message Authentication Codes (MACs)						
HMAC Message Authentication	X		HMAC key Key sizes 112 bits in length and greater	Read Write Execute	IETF RFC 2104	HMAC with MD5 (Part of TLS Specific service)
Hash Functions						
MD5	X		N/A	Read Write Execute	N/A	MD5 (Part of TLS Specific service)

Table 8: Non-approved Services

Service	Notes
Software	
Public Key Algorithms	
RSA Key Generation, Key Wrapping, Digital Signature Generation	Key bit sizes less than 2048 not approved (non-compliant less than 112 bits of encryption strength)

DSA Parameter Generation, Key Generation, Digital Signature Generation	Key Parameters L=1024, N=160 not approved
Message Authentication Codes (MACs)	
HMAC	Key sizes less than 112 bits HMAC-MD5 usage outside of the TLS protocol
Message Digest	
MD5	MD5 usage outside of the TLS protocol
Hybrid	
Public key Algorithms	
RSA Key Wrapping, Digital Signature Generation	Key bit sizes less than 2048 not approved (non-compliant less than 112 bits of encryption strength)

Note: When any of the services in table 8 are utilized, the module will be in non-FIPS mode.

Table 9: Queries

Service	Notes	Roles	
Module Status		**Officer**	**User**
Error	When the System SSL module has entered the error state, one of the following return codes is presented when an attempt is made to use the module: CMSERR_KATPW_FAILED, CMSERR_KATPW_ICSF_FAILED or CMSERR_FIPS_KEY_PAIR_CONSISTENCY	No	Yes
Integrity Checks			
Power-up Tests	Automatic before first use	Yes	No
Self-Tests	Application can call the “perform KAT” function any time after the System SSL module has been loaded	Yes	Yes
Operational Correctness Checks			
Pair-wise consistency	Continuously performed (automatic)	Yes	Yes

6. Operational Environment

Installation and Invocation

System SSL element levels HCPT410 and JCPT411 are installed as part of the z/OS Version 2 Release 1 ServerPac using the “Installing Your Order” documentation provided with the ServerPac (prepackaged tailored z/OS installation including z/OS System SSL). The evaluated configuration requires the installation of service provided through System SSL APAR OA50589 and is bound to the IRRPVERS and ICSF PKCS #11 modules.

The System SSL module requires that a copy of both IRRPVERS and ICSF PKCS #11 be installed and operational on the system for the System SSL module to operate in a validated mode.

The CPACF Enablement Feature 3863 must be installed prior to loading the System SSL DLL. This feature code may be ordered from IBM then downloaded through RETAIN and installed using the Hardware Management Console (HMC).

The System SSL cryptographic module can only be used in conjunction with the System SSL element of z/OS. The System SSL element provides external APIs and accesses the System SSL module through internal C language APIs.

Module Operation

The System SSL module is intended to operate within z/OS Version 2 Release 1 in a single-user mode of operation.

Using the System SSL module in a FIPS 140-2 approved manner assumes that the following defined criteria are followed:

- The Operating System enforces authentication method(s) to prevent unauthorized access to Module services.
- All host system components that can contain sensitive cryptographic data (main memory, system bus, disk storage) must be located within a secure environment.
- The application using the module services through the System SSL element must consist of one or more processes in which each process is utilizing a separate copy of the executable code.
- The application designer must be sure that the application is designed correctly and does not corrupt the storage in the address space where the instance of System SSL module is loaded.
- An instance of the System SSL module must be accessed only by a single process (address space). This means that each process has its own instance of the System SSL element hence one instance of the System SSL module.
- The System SSL module setup procedures documented in the programming documentation must be followed and setup done correctly.
- The CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 must be installed and enabled.
- IRRPVERS module is installed and configured according to its Security Policy [7].
- ICSF PKCS #11 module is installed and configured according to its Security Policy [6].
- Applications requiring FIPS adherence must follow the recommendations found in NIST Special Publication 800-131A Revision 1[8] (“SP 800-131A Revision 1”).

This module implements both approved and non-approved services. The calling application controls the invocation of the services and the cryptographic material being supplied or used by the services. When the module is loaded, the module will allow non-approved algorithms and key sizes to be used. The module also offers non-approved but allowed RSA key establishment and exchange services even when operating FIPS restricted.

Note: The module does not enforce the more recent restrictions introduced by SP 800-131A Revision 1. In some cases, it's not possible for the module to do the enforcement since the context of the request is not known. Therefore, all applications requiring FIPS adherence must explicitly follow the recommendations found in SP800-131A Revision 1 and self-enforce.

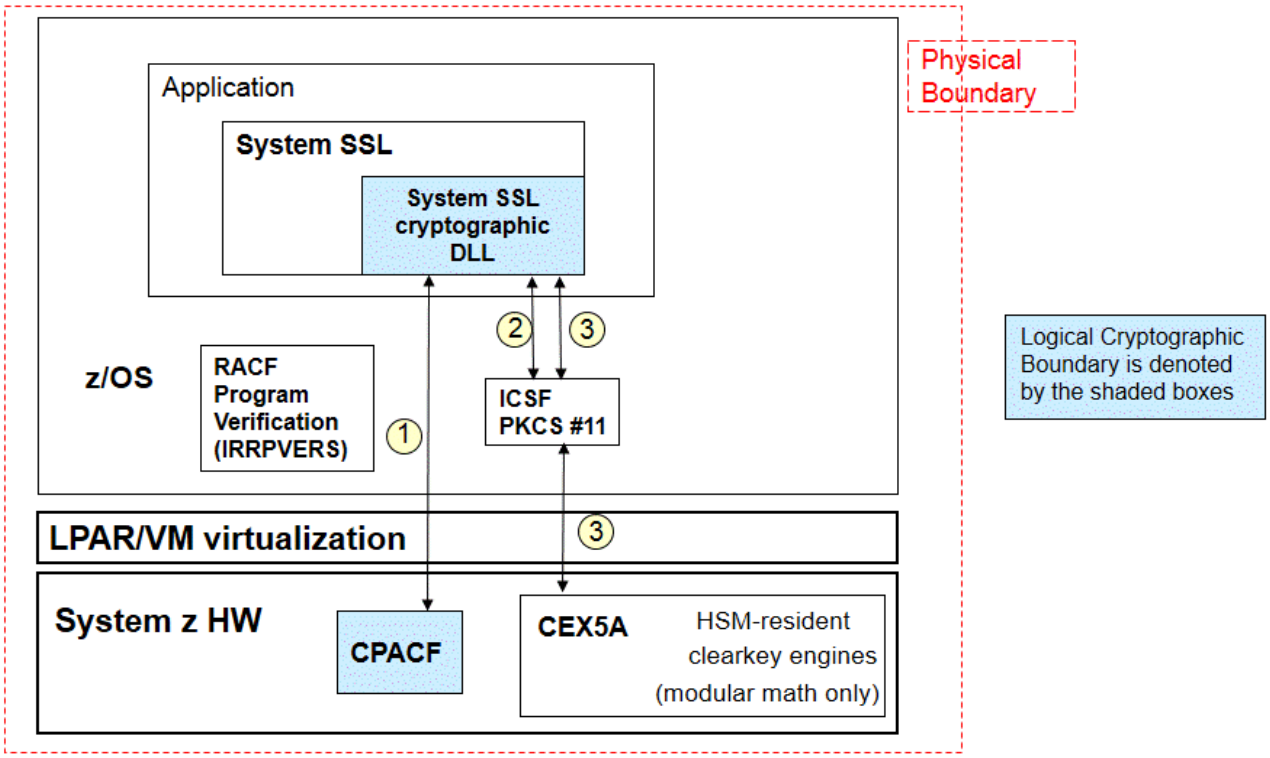
The System SSL module and CPACF represent the logical boundary. The physical cryptographic boundary for the module is defined as the enclosure of the host on which the cryptographic module is to be executed.

The RACF Signature Verification module (IRRPVERS) is shipped as part of the Security Server RACF component. IRRPVERS is bound by this module in order to validate the signature on GSKC31F (or GSKC64F). It is not considered part of the cryptographic boundary of this module.

The ICSF PKCS #11 module is shipped as part of the Integrated Cryptographic Services Facility (ICSF) component. ICSF PKCS #11 is bound by this module for basic cryptographic services. It is not considered part of the cryptographic boundary of this module.

As shown in Figure 2, System SSL Cryptographic Module, the cryptographic module's DLL is instantiated within an application's address space by System SSL element. Each application or operating system component that utilizes the System SSL element support will create a new instance of the z/OS System SSL cryptographic module. Usage of the FIPS certified ICSF PKCS#11 module provides support for certified cryptographic algorithms not available within the System SSL module (i.e. random number generation) and hardware RSA signature verification and key wrapping. The FIPS certified RACF Signature Verification (IRRPVERS) module performs the initial integrity power-up tests.

Figure 2: System SSL Cryptographic Module

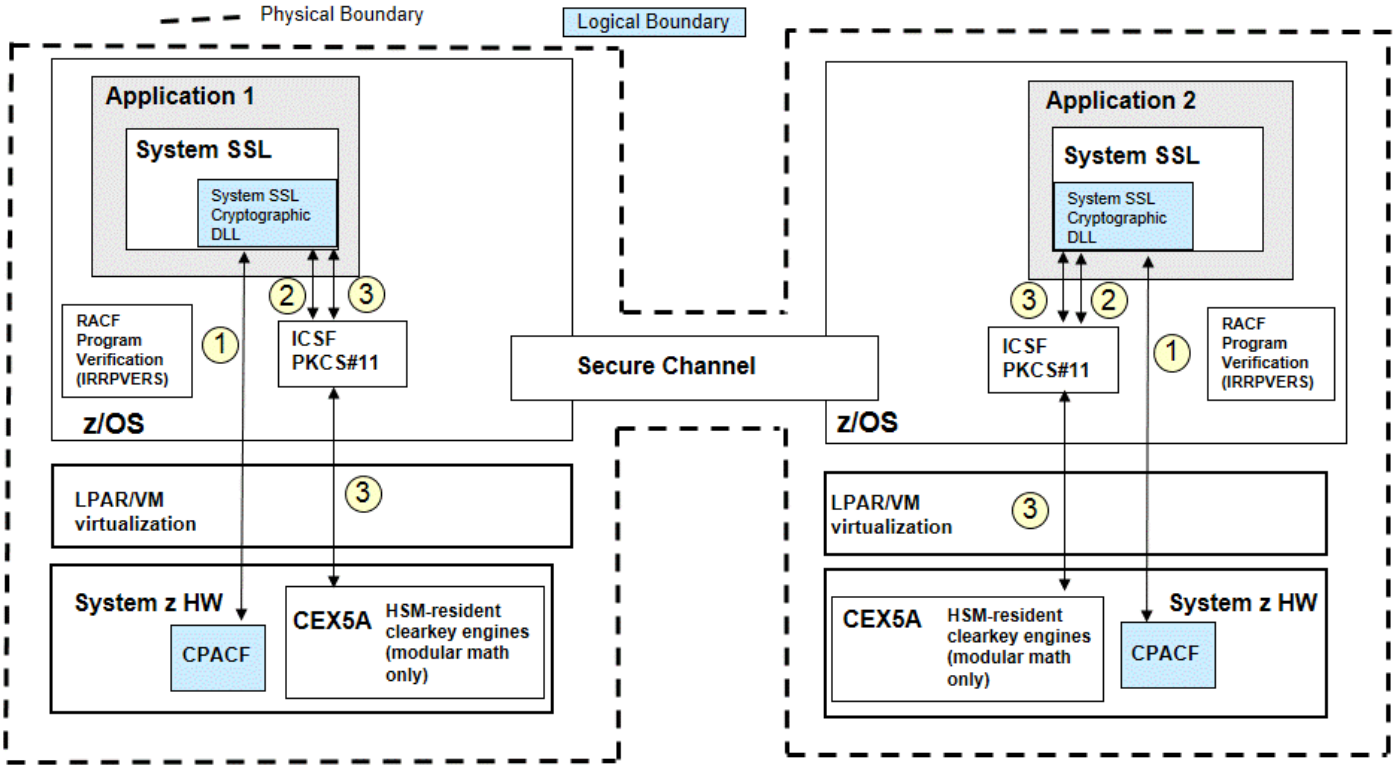


1. The System SSL Cryptographic DLL is considered within the logical cryptographic boundary. The System SSL DLL may issue the System z CPACF machine instructions to perform symmetric encryption and hashing cryptographic functions that are provided by these machine instructions. The CPACF is considered within the logical cryptographic boundary.
2. System SSL calls the certified ICSF PKCS#11 callable services for certified crypto algorithms not available within the System SSL module. (ie. random number generation)
3. System SSL calls ICSF PKCS #11 callable services for accelerated modular math RSA services available in the CEX5A cards.

Note: RACF Program Verification handles ensuring the integrity of the System SSL module during the load process. IRRPVERS is a separately certified module.

As shown in Figure 3, System SSL Cryptographic Module in a z/OS Sysplex Environment, a System SSL cryptographic module may be deployed in a high availability environment where the application may in effect be instantiated on multiple z/OS system instances configured in a “clustered” environment known as a parallel sysplex. A parallel sysplex makes these systems behave like a single, logical computing facility. The underlying structure of the parallel sysplex remains virtually transparent to users, networks, applications, and even operations.

Figure 3: System SSL Cryptographic Module – Sysplex



1. System SSL utilizes the CPACF for symmetric (TDES and AES) and hashing (SHA-1, SHA-2) algorithms.
2. System SSL calls the certified ICSF PKCS#11 module via ICSF callable services for certified crypto algorithms not available within the System SSL module. (ie. random number generation) .
3. System SSL DLL calls ICSF PKCS #11 callable services for accelerated modular math RSA services available in the CEX5A cards

Note: RACF IRRPVERS, ICSF PKCS #11 are bound certified modules to the System SSL module

7. Key Management

Key Storage: The System SSL module provides key generation, import and export services to applications to be used in conjunction with cryptographic services. It is the responsibility of applications using the services to ensure that these services are used in a FIPS 140-2 compliant manner.

In particular, see table 6 and the footnotes of table 6 for information on deprecated key sizes/usages.

Keys managed or generated by applications or libraries may be passed from applications to the module in the clear, provided that the sending application or library exists within the physical boundary of the host computer.

Key material resides in application memory as clear data or in a standard key store format. The most frequently used standard formats, using passphrase-derived keys such as PKCS#12, are classified as clear-key storage according to **FIPS Pub 140-2** guidelines.

Key Generation Key Generation uses an approved DRBG algorithm provided as an approved service through bound module ICSF PKCS #11.

DSA key generation is done according to **FIPS Pub 186-4**[3]**.**

RSA key generation implements the **FIPS Pub 186-4** key generation method.

Key Establishment The module provides support for asymmetric key establishment methods as allowed by Annex D in the **FIPS Pub 140-2**. The supported asymmetric key establishment methods are RSA Wrapping/Unwrapping, Diffie-Hellman key agreement and ECDH key agreement. Diffie-Hellman and ECDH key agreement uses approved services through bound ICSF PKCS #11 module.

When using Diffie-Hellman in FIPS 140-2 mode, the allowed modulus length is 2048 bits, which provides 112 bits of encryption strength.

When using RSA Wrapping/Unwrapping in FIPS 140-2 mode, the allowed modulus lengths must be between 1024 and 4096 bits which provides between 80 and 150 bits of encryption strength. Use of modulus lengths less than 2048 bits is not allowed per SP800-131A Revision 1. Applications requiring FIPS adherence must not use modulus lengths less than 2048 bits.

Key Entry and Key Exit The module does not support manual key entry or intermediate key generation key output.

The module does not output or input keys outside of the physical boundary.

Key Protection To enforce compliance with **FIPS Pub 140-2** key management requirements on the System SSL module itself, code issuing calls must manage keys in a **FIPS Pub 140-2** compliant method. Keys managed or generated by applications may be passed from the application to the module in the clear in the **FIPS Pub 140-2** validated configuration.

The management and allocation of memory is the responsibility of the operating system. It is assumed that a unique process is allocated for each request, and that the operating system and the underlying hardware control access to the address space which contains the process that uses the module. Each instance of the cryptographic module is self-contained within a process; the module relies on such process separation and address separation to maintain confidentiality of secrets. All platforms used during **FIPS Pub 140-2** validation provided per-process protection for user data. Keys stored internally within the address range of System SSL module are similarly separated logically (even if they reside in the same address space).

All keys are associated with the User role. It is the responsibility of application program developers to protect keys exported from the System SSL module.

Key Destruction Applications must destroy persistent key objects and similar sensitive information using **FIPS Pub 140-2** compliant procedures. The System SSL module itself does not destroy externally stored keys and secrets, as it does not own or discard persistent objects. Objects, when released on behalf of a caller, are erased before they are released.

8. Physical Security

The System SSL module installation inherits the physical characteristics of the host running it. The System SSL module has no physical security characteristics of its own. Figure 4 illustrates an IBM System z13 mainframe computer.

The CP Assist for Cryptographic Function (CPACF) (see Figure 6) is also a hardware device – part of the CoProcessor Unit (CoP) and offers the full complement of the Triple DES algorithm, Advanced Encryption Standard (AES) algorithm

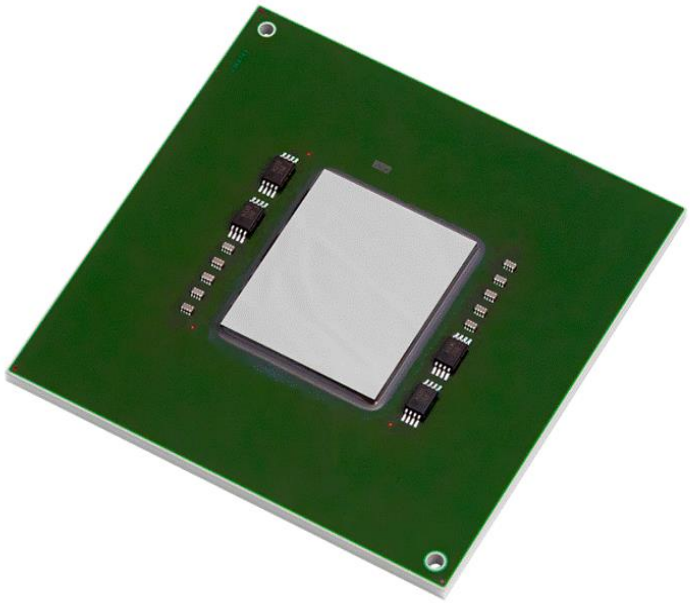
and Secure Hash Algorithm (SHA). Security Level 1 is satisfied by the device (CoP) being included within the physical boundary of the module and the device being made of commercial-grade components.

CPACF Physical Design: Each microprocessor (core) on the 8-core chip has its own dedicated CoP, which implements the crypto instructions and also provides the hardware compression function. The compression unit is integrated with the CP Assist for Cryptographic Function (CPACF), benefiting from combining (sharing) the use of buffers and interfaces.

Figure 4: IBM z13 Mainframe Computer

Figure 5: Crypto Express5 Card

Figure 6: Processor Unit chip



9. EMI/EMC

Systems utilizing the module's services have their overall EMI/EMC ratings determined by the host system, which includes the CPACF. The validation environments meet the requirements of 47 CFR FCC PART 15, Subpart B, Class A (Business use).

10. Self-Tests

10.1 System SSL Module

The System SSL module implements a number of self-tests to check proper functioning of the module including power-up self-tests and conditional self-tests. Conditional tests are performed when asymmetric keys are generated. These tests include pair-wise consistency tests of the generated DSA or RSA keys.

Startup Self-Tests "Power-up" self-tests consist of software integrity test(s) and known-answer tests of algorithm implementations. The module integrity test is automatically performed during loading. The integrity of the module is performed by bound cryptographic module IRRPVERS based on the verification of the module's RSA/SHA-256 based-digital signature prior to the module being utilized. Module signatures are generated during the final phase of the build process. Initialization will only succeed if the utilized module signature is verified successfully. The integrity verification starts with bound module IRRPVERS verifying its own digital signature. Once verified, IRRPVERS verifies the digital signature of either GSKC31F or GSKC64F.

Algorithm known answer tests (KAT) are invoked automatically upon loading the System SSL module. The initialization function is executed via DEP (default entry point) as specified in FIPS 140-2 Implementation Guidance 9.10. If any of the known answer tests fail, the module is render unusable (all cryptographic services return an error return code). Any attempts to use the module will fail.

Prior to the execution of the power-up self-tests, the System SSL module checks whether environment variable GSK_HW_CRYPTO has been set. If not set, AES, TDES, SHA-1 and SHA-2 KAT tests are performed using the CPACF. If GSK_HW_CRYPTO is set, AES, TDES, SHA-1 and SHA-2 CPACF cryptographic algorithms can be disabled for use by the System SSL through bit settings within the specified value. If the cryptographic algorithm has been disabled, the KAT is run against the software version within the System SSL module. Only one version of the algorithm is supported for the entire instance of the System SSL module.

The module tests the following cryptographic algorithms:

CPACF: AES encryption/decryption, Triple DES encryption/decryption, SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512.

System SSL module software: AES encryption/decryption, Triple DES encryption/decryption, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RSA (2048-bit key sign/verify, wrapping/unwrapping), DSA (2048-bit prime sign/verify), HMAC-SHA-1, HMAC-SHA256 and HMAC-SHA384.

During the self-test processing, all data output is inhibited until the self-tests are completed.

Startup Recovery If any of the startup self-tests fail, the System SSL module will terminate FIPS 140-2 processing and enter into error state. The System SSL element's calling application must recognize this error and handle it in a FIPS 140-2 appropriate manner, for example, by reinitializing the module instance.

Pair-wise Consistency Checks This test is run whenever the module generates a RSA or DSA public/private key-pair. If the pair-wise consistency check fails, the module enters an error state and returns an error status code. The System SSL element's calling application must recognize this error and handle it in a FIPS 140-2 appropriate manner, for example, by reinitializing the module instance.

Invoking FIPS 140-2 self-tests on demand. If a user can access System SSL services, the module has passed its integrity and power-up self-tests. During regular operations, a host application can ask the System SSL element to repeat the known answer tests on demand for algorithms within the System SSL module. The System SSL element invokes internal API "perform KAT" function. If these tests pass, the module is working properly.

If a KAT failure is encountered, the module enters an error state and returns an error status code. The calling application must recognize this error and handle it in a FIPS 140-2 appropriate manner, for example, by reinitializing the module instance.

11. Operational Requirements (Officer/User Guidance)

11.1 Module Configuration for FIPS 140-2 Compliance

To ensure FIPS 140-2 compliant usage, the following requirements must be observed:

- IRRPVERS must be configured to execute in FIPS 140-2 mode according to its Security Policy [7] and be operational prior to System SSL module being utilized.

- ICSF PKCS #11 must be configured to execute in FIPS 140-2 mode according to its Security Policy [6] and be operational prior to System SSL module being utilized.

- Crypto officers of System SSL must verify that the correct Security Manager Profiles have been defined to ensure that startup integrity tests are performed. Each System SSL module DLL contains an RSA/SHA-256 signature. The startup integrity tests ensure that the signature matches the expected value. See z/OS System SSL element documentation [1] for Security Manager Profile settings.

- Applications using System SSL element features must observe **FIPS Pub 140-2** rules for key management and provide their own self-tests.

  For proper operations, the crypto officer or users must verify that applications comply with this requirement. While details of these application requirements are outside of the scope of this policy, they are mentioned here for completeness.

- The Operating System (OS) hosting the library must be set up in accordance with **FIPS Pub 140-2** rules. It must provide sufficient separation between processes to prevent inadvertent access to data of different processes. (This requirement was met for all platforms tested during validation.)

- An instance of the module must not be used by multiple callers simultaneously such that they might interfere with each other. Note that for keys retained in caller-provided storage, this requirement is automatically met if the OS provides sufficient process separation (since the ownership of each memory region, therefore, each object, is uniquely determined.)

- Applications using System SSL module services must verify that ownership of keys is not compromised, and keys are not shared between different users of the calling application.

Note that this requirement is not enforced by the System SSL module itself, but by the application providing the keys to System SSL.

- Applications utilizing System SSL services must avoid using non-approved algorithms or modes of operation. If not feasible, the application must indicate that they use utilize non-approved cryptographic services. Applications must also comply with the key size and algorithm requirements specified in the latest version of NIST Special Publication 800-131A Revision 1.

- To be in FIPS 140-2 mode, the System SSL installation must run on a host with commercial grade components and must be physically protected as prudent in an enterprise environment.

- **Physical assumptions**
    - The module is intended for application use in user areas that have physical control and monitoring. It is assumed that the following physical conditions will exist:
        - **LOCATION**
            - The processing resources of the module will be located within controlled access facilities that will prevent unauthorized physical access.
        - **PROTECTION**
            - The module hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
            - Any sysplex communications shall be configured so that unauthorized physical access is prevented.
- **Personnel assumptions**
    - It is assumed that the following personnel conditions will exist:
        - **MANAGE**
            - There will be one or more competent individuals assigned to manage the module and the security of the information it contains.
        - **NO EVIL ADMINISTRATOR**
            - The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the Crypto Officer documentation.
        - **CO-OPERATION**
            - Authorized users possess the necessary authorization to access at least some of the information managed by the module and are expected to act in a cooperative manner in a benign environment.

11.2 Determining Mode of Operation

The FIPS mode for this module is enforced by policy.

The application utilizing services must enforce key management compliant with **FIPS Pub 140-2** requirements. This should be indicated in an application-specific way that is directly observable by crypto officers and end-users.

While such application-specific details are outside the scope of the validation, they are mentioned here for completeness.

The user application must comply with the key size requirements specified in the latest revision of the NIST Special Publication 800-131A. If the services defined in table 6 and 7 are utilized, the module is then FIPS mode. If the services defined in table 8 are utilized, the module will be considered not in FIPS mode.

11.3 Testing/Physical Security Inspection Recommendations

In addition to automatic tests, which are described elsewhere in this document, a System SSL element application may invoke FIPS 140-2 mode self-tests at any time. These self-tests are initiated through a dedicated function “perform KAT” function, which is invoked automatically at startup. Continuous tests reside within their respective functions and are called implicitly during the function processing. These tests are not observable unless a failure is detected.

Apart from prudent security practice of server applications and those of security-critical embedded systems, no further restrictions are placed on hosts utilizing these services.

12. Mitigation of Other Attacks

The Mitigation of Other attacks security section of FIPS 140-2 is not applicable to the System SSL cryptographic module.

13. Cryptographic Module Configuration Diagrams

The following diagrams illustrate the different validated configurations. These validated configurations can consist of a single z/OS System instance or multiple z/OS System instances. Figure 7 illustrates IBM z13 with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863

Figure 7: Validated Configuration with CPACF and ICSF PKCS #11

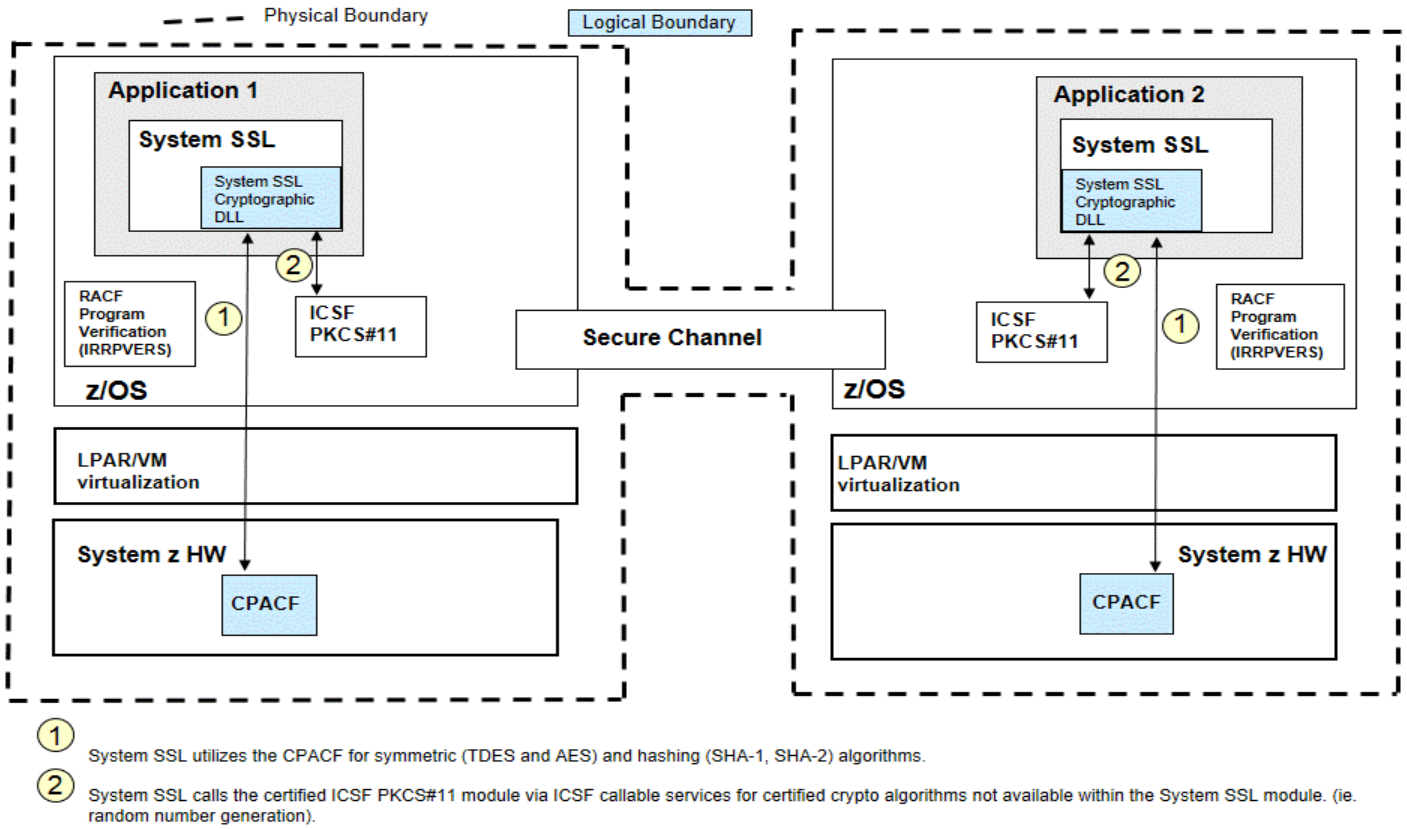
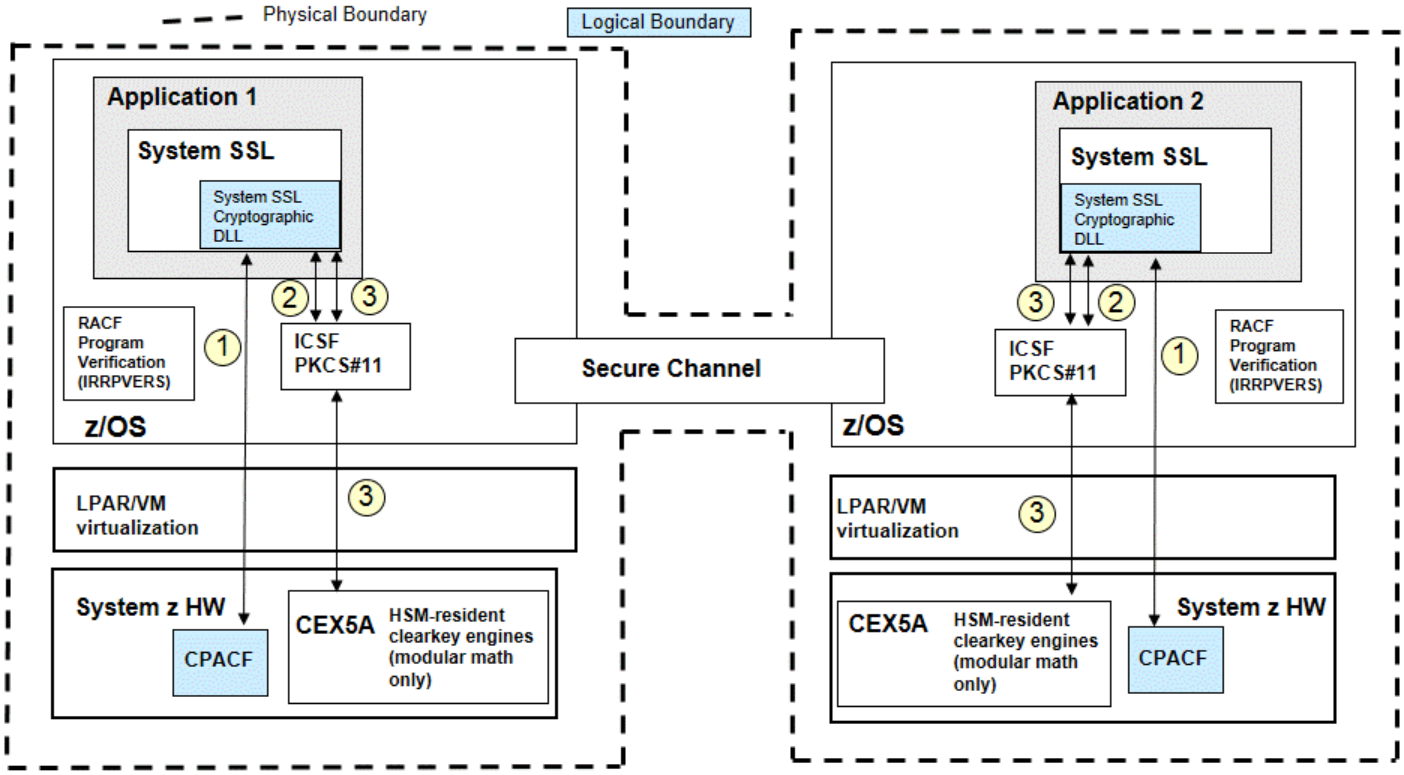


Figure 8 illustrates IBM z13 with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 and optional Crypto Express5 cards (Accelerator (CEX5A)) configuration.

Figure 8: Validated Configuration with CPACF, ICSF PKCS #11 and CEX5A card



1. System SSL utilizes the CPACF for symmetric (TDES and AES) and hashing (SHA-1, SHA-2) algorithms.
2. System SSL calls the certified ICSF PKCS#11 module via ICSF callable services for certified crypto algorithms not available within the System SSL module. (ie. random number generation) .
3. System SSL DLL calls ICSF PKCS #11 callable services for accelerated modular math RSA services available in the CEX5A cards

Note: RACF IRRPVERS, ICSF PKCS #11 are bound certified modules to the System SSL module

14. Glossary

Address space A set of contiguous virtual addresses available to a program and its data. The address space is a container for enclaves and processes. [4] [5]

API Application Programming Interface

CEX5A Crypto Express5 Accelerator, mainframe name for IBM Hardware Security Modules (HSMs).

CP Central Processor, aka CPU

CPACF CP Assist for Cryptographic Function, clear key on-chip accelerator integrated into mainframe processors. CPACF functionality is restricted to symmetric and hashing operations.

DLL	Dynamic Link Library, shared program library instantiated separately from binaries using it. FIPS 140-2 configurations of System SSL DLLs are never statically linked.
DRBG	Deterministic Random Bit Generator
Enclave	In the z/OS Language Environment, a collection of routines, one of which is named as the main routine. The enclave contains at least one thread. Multiple enclaves may be contained within a process. [4] [5]
ICSF	Integrated Cryptographic Service Facility
KAT	Known Answer Test
OS	Operating System
Process	A collection of resources; both program code and data, consisting of at least one enclave. [4] [5]
RACF	Resource Access Control Facility
RETAIN	IBM database system shared by IBM and its customers
ServerPac	Prepackaged version of the z/OS Operating System
Thread	An execution construct that consists of synchronous invocations and terminations of routines. The thread is the basic runtime path within the z/OS Language Environment program management model, and is dispatched by the operating system with its own run-time stack, instruction counter and registers. Thread may exist concurrently with other threads within an address space. [4] [5]

15. References

[1] z/OS Cryptographic Services Secure Sockets Layer Programming (SC41-7495-00) with OA50589 APAR documentation

[2] National Institute of Standards and Technology, Security Requirements for Cryptographic Modules (FIPS 140-2), 2002

[3] National Institute of Standards and Technology, Federal Information Processing Standards, Digital Signature Standard (FIPS 186-4), 2013

[4] ABCs of z/OS System Programming Volume 1 (SG24-6981-01)

[5] ABCs of z/OS System Programming Volume 2 (SG24-6982-02)

[6] IBM® z/OS® Version 2 Release 1 ICSF PKCS#11 Cryptographic Module

[7] IBM® z/OS® Version 2 Release 1 Security Server RACF® Signature Verification Module

[8] National Institute of Standards and Technology, Special Publication 800-131A Revision 1, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, November 6, 2015

16. Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

- IBM
- RACF
- zEnterprise
- z/OS
- zEC12
- z13