IBM® z/OS® Version 2 Release 4 System SSL Cryptographic Module

FIPS 140-2

Non-Proprietary Security Policy

Document Version v1.2

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

April 28, 2021

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision.

Table of Contents

1. CRYPTOGRAPHIC MODULE SPECIFICATIONS 3
1.1 SCOPE OF DOCUMENT 3
1.2 CRYPTOGRAPHIC MODULE SPECIFICATION 4
1.3 CRYPTOGRAPHIC MODULE SECURITY LEVEL 5
1.4 DETERMINING MODE OF OPERATION 6
2. PORTS AND INTERFACES 7
2.1 MODULE STATUS 7
3. ROLES, SERVICES AND AUTHENTICATION 8
3.1 ROLES 8
3.2 SERVICES 8
4. PHYSICAL SECURITY 16
5. OPERATIONAL ENVIRONMENT 18
5.1 INSTALLATION AND INVOCATION 18
5.2 MODULE OPERATION 18
6. KEY MANAGEMENT 22
6.1 KEY STORAGE 22
6.2 KEY GENERATION 22
6.3 KEY ESTABLISHMENT 22
6.4 KEY ENTRY AND KEY EXIT 23
6.5 KEY PROTECTION 23
6.6 KEY DESTRUCTION 23
6.7 KEYS AND CSPS LIFE CYCLE 23
7. EMI/EMC 25
8. SELF-TESTS 26
8.1 SYSTEM SSL MODULE 26
8.2 STARTUP SELF-TESTS 26
8.3 STARTUP RECOVERY 26
8.4 PAIR-WISE CONSISTENCY CHECKS 26
8.5 INVOKING FIPS 140-2 SELF-TESTS ON DEMAND. 27
9. OPERATIONAL REQUIREMENTS (OFFICER/USER GUIDANCE) 28
9.1 MODULE CONFIGURATION FOR FIPS 140-2 COMPLIANCE 28
9.2 TESTING/PHYSICAL SECURITY INSPECTION RECOMMENDATIONS 29
10. MITIGATION OF OTHER ATTACKS 30
11. CRYPTOGRAPHIC MODULE CONFIGURATION DIAGRAMS 31
12. GLOSSARY 33
13. REFERENCES 34
14. TRADEMARKS 35

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision.

1. Cryptographic Module Specifications

1.1 Scope of Document

This document is the non-proprietary security policy for the IBM® z/OS® Version 2 Release 4 System SSL Cryptographic Module, and was prepared as part of the requirements for conformance to Federal Information Processing Standard (FIPS) 140-2, Level 1 Software-Hybrid Module.

This document describes the services that the IBM z/OS Version 2 Release 4 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 (i.e. Key Derivation Function (KDF)) and functions to allow the System SSL element to support TLS.

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

1.2 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 4 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 4 ICSF PKCS #11 (hereafter referred to as "ICSF PKCS #11") with FIPS 140-2 Validation #3909 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 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 4 with System SSL level HCPT440/JCPT441 with APAR OA59268
Hardware Components CPACF	Firmware - CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 (aka FC3863) with System Driver Level 32L Hardware – COP chips integrated within processor unit
Documentation	SC14-7495 z/OS System SSL Programming

System SSL module validation was performed using the z/OS Version 2 Release 4 operating system with the following platform configurations:

1. IBM z14® with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 (Base GPC)
2. IBM z14 with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 and optional Crypto Express6 Accelerator (CEX6A) 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 4 on the following platform:

1. IBM z14 with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 and optional Crypto Express5 Accelerator (CEX5A) maybe used by ICSF PKCS #11 for RSA hardware clear key module math cryptography to support RSA digital signature verification and key wrapping.
2. IBM z13® with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 (Base GPC)

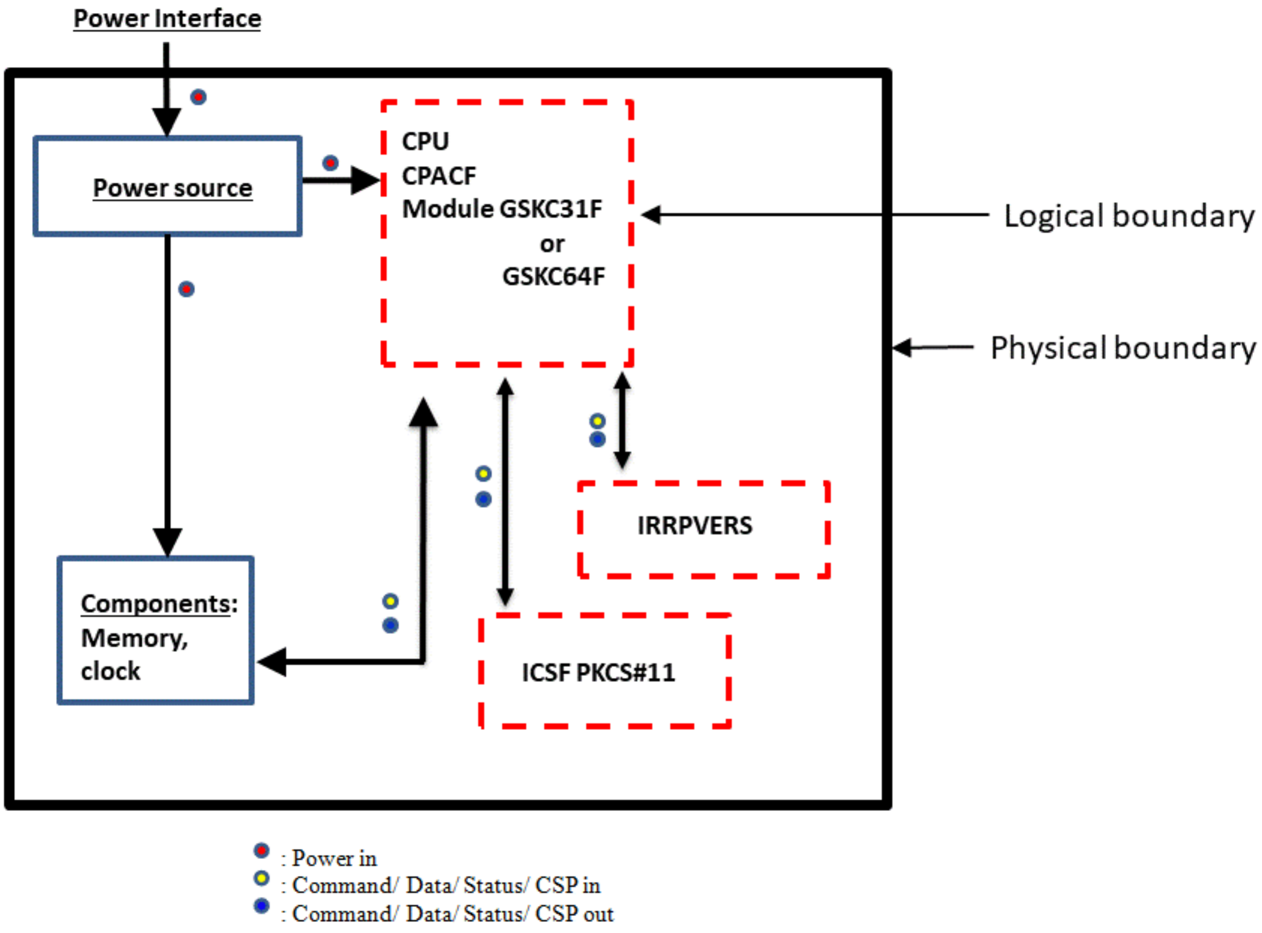
3. IBM z13 with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 and Crypto Express5 accelerator (CEX5A) maybe used by ICSF PKCS #11 for RSA hardware clear key module math cryptography to support RSA digital signature verification and key wrapping.

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 7 in the Cryptographic Module Configuration Diagrams section.

Figure 1: System SSL Cryptographic Module Physical and Logical Boundaries



1.3 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).

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

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

1.4 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 Revision 2. 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.

2. 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	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.

2.1 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.

3. Roles, Services and Authentication

3.1 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)	N/A	N/A
Officer	Module installation and configuration. This role does not involve the use of cryptographic services.	None (Automatic)	N/A	N/A

3.2 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 in FIPS-Approved mode of operation

Service	Roles		CSP	Modes / Notes	Cert #	Access (Read, Write)	Standard
	User	Crypto Officer					

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

Module installation And Configuration		X	N/A	N/A	N/A	N/A	N/A
Self-Tests	X		N/A	N/A	N/A	N/A	N/A
Zeroization	X		All keys and CSPs	N/A	N/A	Write	N/A
Show Status	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	C1664 (31-bit implementation) C1665 (64-bit implementation)	R	FIPS 197 SP 800-38A
Triple-DES Encryption and Decryption	X		Triple DES Symmetric key (192 bit)	CBC	C1664 (31-bit implementation) C1665 (64-bit implementation)	R	SP 800-67
Public Key Algorithms							
DSA Parameter/Key Generation	X		DSA Parameter and asymmetric keys L=2048, N=256	N/A	C1664 (31-bit implementation) C1665 (64-bit implementation)	R,W	FIPS 186-4
DSA Signature Generation	X		DSA Asymmetric Private Key L=2048, N=256 with SHA (224/256)	N/A		R	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		R	FIPS 186-4
RSA Key generation	X		RSA Asymmetric Key 2048 and 3072	N/A	C1664 (31-bit	R,W	FIPS 186-4

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

RSA Signature Generation (FIPS 186-2)	X		RSA Asymmetric Private Key 4096 with SHA (224/256/384/512)	N/A	implementation) C1665 (64-bit implementation)	R	FIPS 186-2
RSA Signature Generation (FIPS 186-4)	X		RSA Asymmetric Private Key 2048/3072 with SHA[1] (1/224/256/384/512)	N/A		R	FIPS 186-4
RSA Signature Verification (FIPS 186-2)	X		RSA Asymmetric Public Key 1024/2048/3072/4096 with SHA (1/224/256/384/512)	N/A		R	FIPS 186-2
RSA Signature Verification (FIPS 186-4)	X		RSA Asymmetric Public Key 1024/2048/3072 with SHA (1/224/256/384/512)	N/A		R	FIPS 186-4
CKG (vendor affirmed)	X		Asymmetric Key Generation	N/A	N/A	R,W	SP800-133
Hash Functions							
SHS Message Digest	X		N/A	SHA -1 SHA-224 SHA-256 SHA-384 SHA-512	C1664 (31-bit implementation) C1665 (64-bit implementation)	N/A	FIPS 180-4
Key Establishment							
Authenticated Encryption (KTS)	X		AES key with HMAC key Triple-DES key with HMAC key	AES-CBC Triple-DES-CBC HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384	See AES, Triple-DES and HMAC certs	R	SP 800-38F

[1] Digital signature generation using SHA-1 is Approved only when used within the TLS protocol, as explained in SP800-52

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

Message Authentication Codes (MACs)							
HMAC Message Authentication	X		Key sizes 112 bits in length and greater[2]	HMAC SHA-1 HMAC SHA-256 HMAC SHA-384	C1664 (31-bit implementation) C1665 (64-bit implementation)	R	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 with SHA (256/384)	N/A	C1664 (31-bit implementation) C1665 (64-bit implementation)	R,W	SP 800-135
CP Assist for Cryptographic Functions							
Symmetric Algorithms							
AES Encryption and Decryption	X		AES Symmetric key (128, 256 bit)	CBC	C79[3]	R	FIPS 197 SP 800-38A
Triple-DES Encryption and Decryption	X		Triple DES Symmetric key (192 bit)	CBC	C79	R	SP 800-67
Hash Function							
SHS Message Digest	X		N/A	SHA -1 SHA-224 SHA-256 SHA-384 SHA-512	C79	N/A	FIPS 180-4
ICSF bound module							
AES	X		AES symmetric keys (128/256-bit keys)	GCM	C1635	R	SP 800-38D

[2] Per FIPS 198-1 and SP 800-107, keys less than 112 bits in length are not approved for HMAC generation.

[3] 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.

RSA Signature verification	X		RSA Asymmetric public keys (1024/2048/3072 -bit keys)	PKCS1.5	C1635	R	FIPS 186-4
			RSA Asymmetric public keys (1024/2048/3072/4096 -bit keys)				FIPS 186-2
Diffie-Hellman shared secret computation (CVL)	X		Diffie-Hellman Asymmetric private keys (L=2048, N=224; L=2048, N=256) shared secret	N/A	C1635	R,W	FIPS 186-4
EC Diffie-Hellman shared secret computation (CVL)	X		EC Diffie-Hellman Asymmetric private keys (keys according to P-224, P-256, P-384 and P-521) shared secret	N/A	C1635	R,W	FIPS 186-4
ECDSA Key generation, Signature generation, Signature verification	X		ECDSA Asymmetric private keys (keys according to P-224, P-256, P-384 and P-521)	N/A	C1635	R,W	FIPS 186-4
DRBG	X		Entropy input, Seed, V, C (Hash-SHA-512)	N/A	C1633	R	SP 800-90A
Authenticated Encryption (KTS)	X		AES key	GCM	See AES-GCM cert	R	SP 800-38F
4768-001 (CEX6A) from ICSF bound module							
Diffie-Hellman shared secret computation (CVL)	X		Diffie-Hellman Asymmetric private keys (L=2048, N=224; L=2048, N=256) shared secret	N/A	C1637	R,W	SP 800-56A, Revision 2
RSA Signature verification	X		RSA Asymmetric public keys (1024/2048/3072 -bit keys)	PKCS1.5	C1637	R	FIPS 186-4
			RSA Asymmetric public keys (1024/2048/3072 /4096-bit keys)				FIPS 186-2
IRRPVERS bound module							

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

RSA Signature Verification	X		RSA Asymmetric public keys (2048-bit keys)	PKCS1.5	C1634	R	FIPS 186-4

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

Table 7: Allowed Services in FIPS-Approved mode of operation

Service	Roles		CSP	Access (Read, Write)	Standard / Mode	Caveat
	User	Crypto Officer				
Public Key Algorithms						
RSA	X		RSA Asymmetric Private Key Modulus size from at least 2048 and up to and including 4096 bits	R	N/A	key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength
Hash Functions						
HMAC-MD5	X		N/A	R	N/A	HMAC-MD5 (when used in the context of the TLS protocol)
ICSF bound module						
Key agreement[4]						
Diffie-Hellman (CVL Certs. #C1635 and #C1637 with Certs. #C1664 and #C1665)	X		Diffie-Hellman Asymmetric private keys (L=2048, N=224; L=2048, N=256)	R,W	SP 800-56A	key agreement; key establishment methodology provides 112 bits of encryption strength
EC Diffie-Hellman (CVL Cert. #C1635 with Certs. #C1664 and #C1665)	X		EC Diffie-Hellman Asymmetric private keys (keys according to P-224, P-256, P-384 and P-521)	R,W	SP 800-56A	key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength

[4] The Key Agreement is a combination of TLS KDF from System SSL and DH/ECDH shared secret computation from the ICSF bound module

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

RSA	X		RSA Asymmetric keys	R	Key wrapping	key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength The modulus size at least 2048 bits and up to 4096 bits (included)
NDRNG	X		N/A	Read Write Execute	N/A	Seeding for the DRBGs

Table 8: Non-approved Services in non-FIPS-Approved mode of operation

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/Verification	Key Parameters L=1024, N=160 not approved
Message Authentication Codes (MACs)	
HMAC	Key sizes less than 112 bits HMAC-MD5 when used outside the context of the TLS protocol
ICSF bound module	
EC Diffie-Hellman shared secret computation	Curve P-192 not approved Brainpool curves (224, 256, 384, 512 bits)
ECDSA Key generation / Digital signature generation	Curve P-192 not approved Brainpool curves (224, 256, 384, 512 bits) Curve25519 and ed448
ECDSA Digital signature verification	Brainpool curves (224, 256, 384, 512 bits)
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.

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

4. 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 2 illustrates an IBM System z14 mainframe computer.

The CP Assist for Cryptographic Function (CPACF) (see Figure 4) 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, Secure Hash Algorithm (SHA) and SP 800-90A DRBG. Security Level 1 is satisfied by the device (CoP) being included within the physical boundary of the module and the device being made of production 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 2: IBM z14 Mainframe Computer

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

Figure 3: Crypto Express6 Card

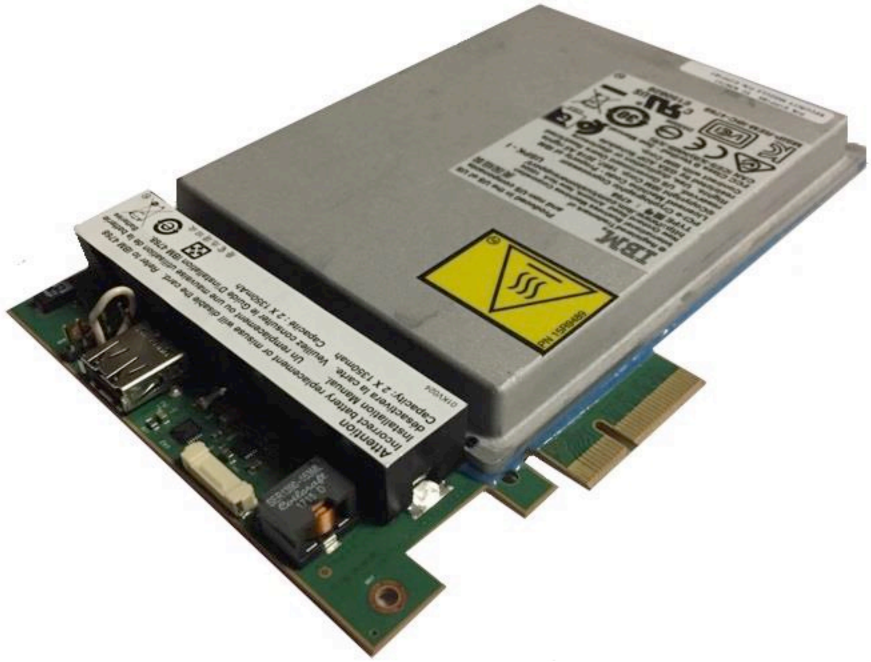
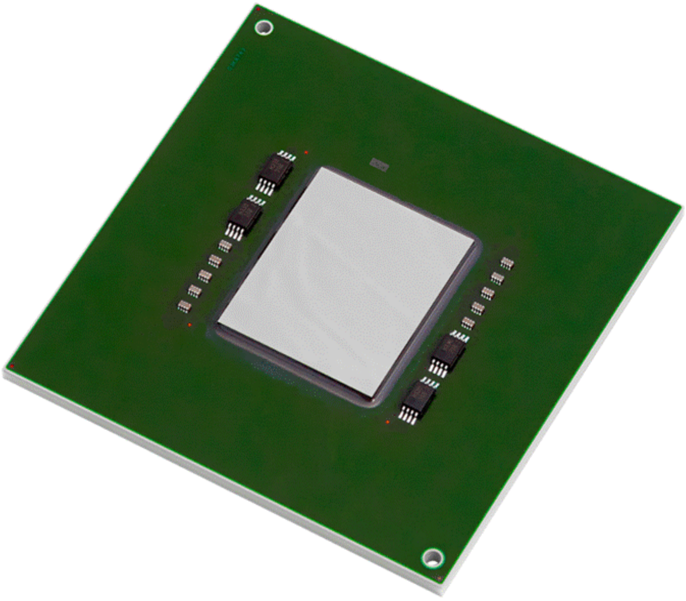


Figure 4: Processor Unit chip



© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

5. Operational Environment

5.1 Installation and Invocation

System SSL element levels HCPT440 and JCPT441 are installed as part of the z/OS Version 2 Release 4 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 OA59268 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.

5.2 Module Operation

The module operates in a modifiable operational environment per FIPS 140-2 level 1 specifications. The module runs on the z/OS operating system executing on the hardware specified in section 2.

The System SSL module is intended to operate within z/OS Version 2 Release 4 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 2[8] ("SP 800-131A Revision 2").

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

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 2. 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 2 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.

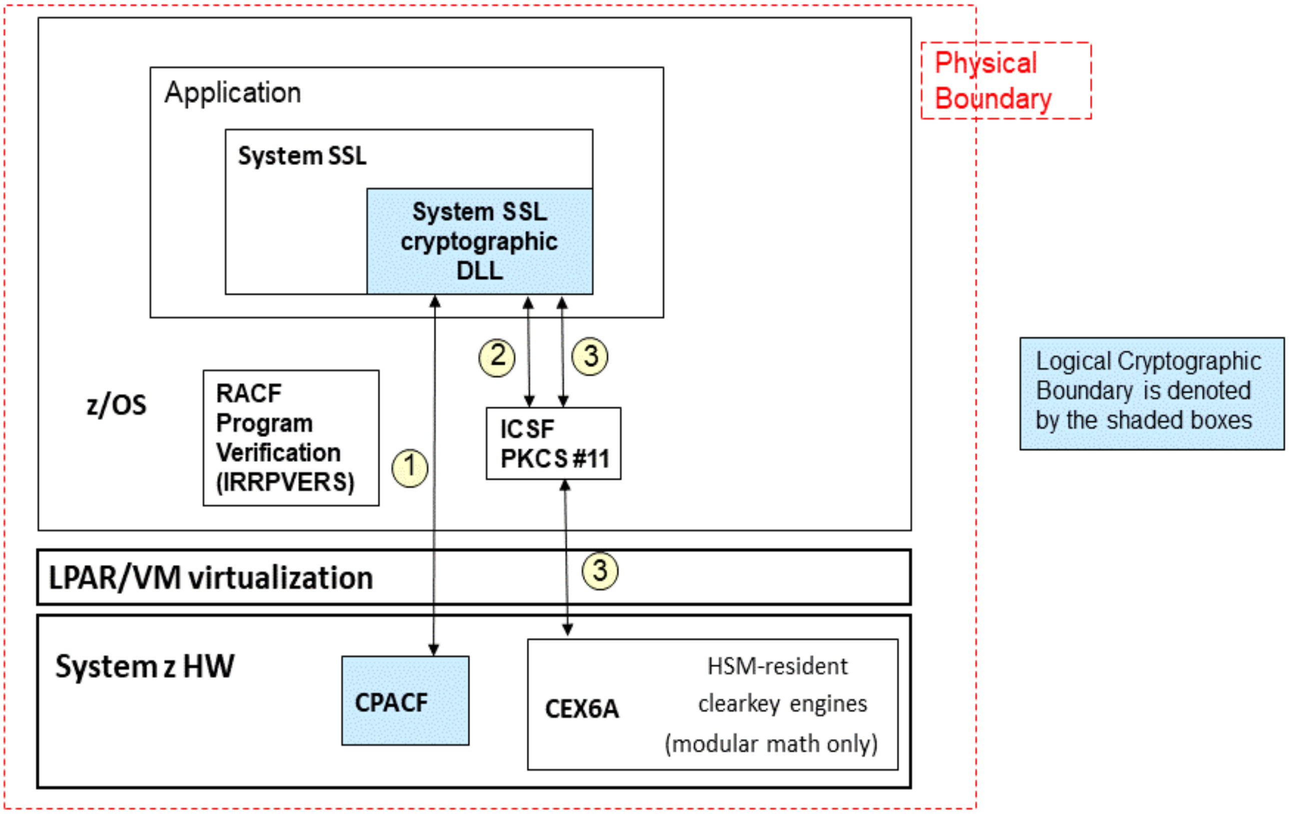
The RACF Signature Verification module (IRRPVERS) is shipped as part of the z/OS Security Server RACF component. IRRPVERS is bound by this module in order to validate the signature on GSKC31F (or GSKC64F). It is not considered part of the cryptographic boundary of this module.

The ICSF PKCS #11 module is shipped as part of the z/OS 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 5, 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.

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

Figure 5: System SSL Cryptographic Module


Physical Boundary
Application
System SSL
System SSL cryptographic DLL
2
3
z/OS
RACF Program Verification (IRRPVERS)
1
ICSF PKCS #11
Logical Cryptographic Boundary is denoted by the shaded boxes
LPAR/VM virtualization
3
System z HW
CPACF
CEX6A
HSM-resident clearkey engines (modular math only)

1 The System SSL Cryptographic DLL is considered within the logical cryptographic boundary. The System SSL DLLs 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.

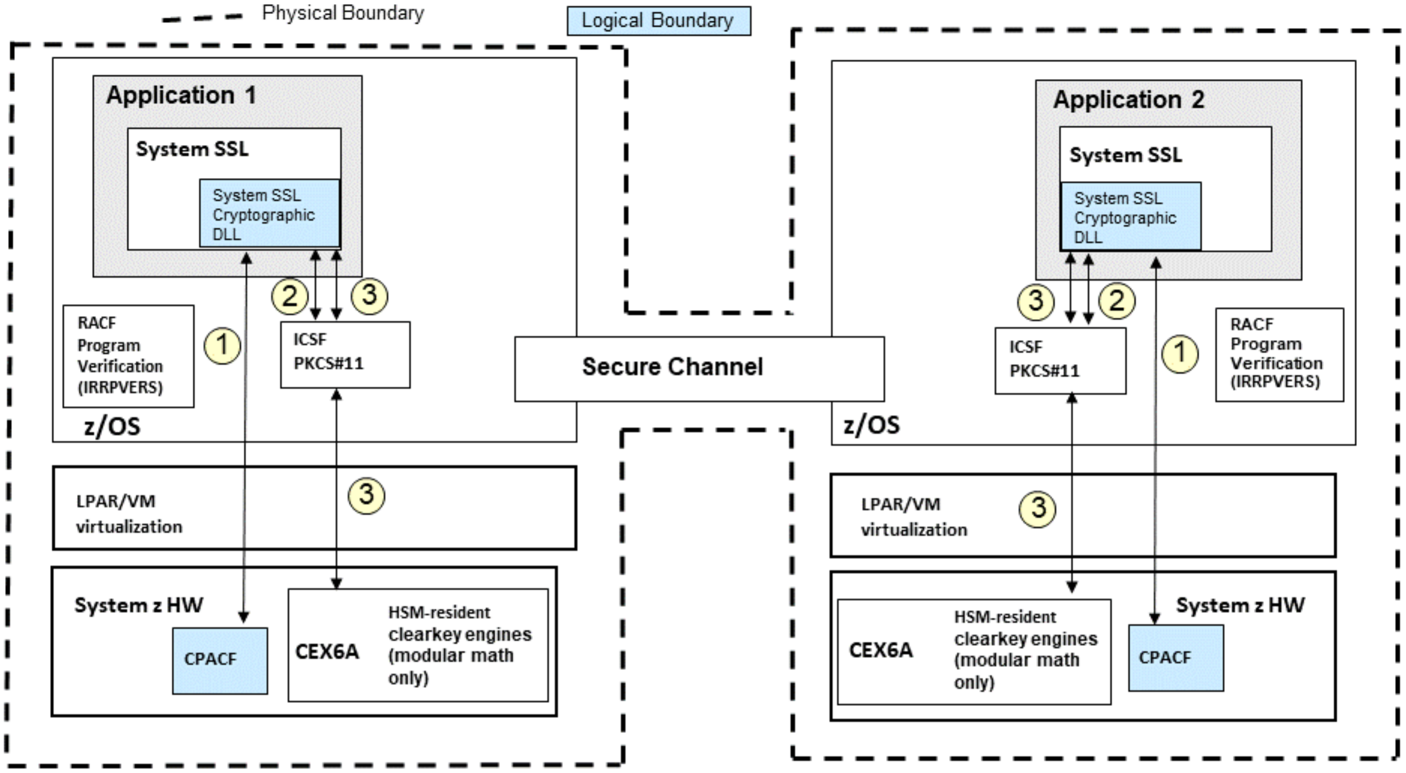
2 System SSL calls the certified ICSF PKCS#11 callable services for random number generation, RSASSA-PSS, AES-GCM and ECC.

3 System SSL calls ICSF PKCS #11 callable services for accelerated modular math RSA services available in the CEX6A card.

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 6, 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 6: System SSL Cryptographic Module – Sysplex


Physical Boundary
Logical Boundary
Application 1
System SSL
System SSL Cryptographic DLL
2
3
RACF Program Verification (IRRPVERS)
1
ICSF PKCS#11
z/OS
LPAR/VM virtualization
3
System z HW
CPACF
CEX6A
HSM-resident clearkey engines (modular math only)
Secure Channel
Application 2
System SSL
System SSL Cryptographic DLL
3
2
ICSF PKCS#11
1
RACF Program Verification (IRRPVERS)
z/OS
LPAR/VM virtualization
3
CEX6A
HSM-resident clearkey engines (modular math only)
System z HW
CPACF

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 CEX6A card

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

6. Key Management

6.1 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.

6.2 Key Generation

The bound ICSF module provides an SP800-90A-compliant Deterministic Random Bit Generator (DRBG) for creation of key components of asymmetric keys, and random number generation. The module performs the health tests for the SP800-90A DRBG as defined per section 11.3 of SP800-90A.

The Key Generation methods implemented in the module for Approved services in FIPS mode is compliant with SP800-133.

For generating RSA and DSA keys, the module implements asymmetric key generation services compliant with **FIPS Pub 186-4**. A seed (i.e. the random value) used in asymmetric key generation is directly obtained from the SP800-90A DRBG.

6.3 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 combined with KDF from System SSL 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 EC Diffie-Hellman in FIPS 140-2 mode, the minimum key size is 224 bits and provides between 112 and 256 bits of encryption strength.

When using RSA Wrapping/Unwrapping in FIPS 140-2 mode, the allowed modulus lengths must be between 2048 and 4096 bits which provides between 112 and 150 bits of encryption strength. Use of modulus lengths less than 2048 bits is not allowed per SP800-131A Revision 2. Applications requiring FIPS adherence must not use modulus lengths less than 2048 bits.

The module provides approved key transport methods compliant to SP 800-38F according to IG D.9. The key transport method is provided by:

- AES-GCM through the bound ICSF module used within the TLS protocol
- AES-CBC with HMAC used within the TLS protocol
- Triple-DES-CBC with HMAC used within the TLS protocol

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

Therefore, the following caveats apply:

- KTS (AES Cert. #C1635; key establishment methodology provides 128 or 256 bits of encryption strength)
- KTS (AES Certs. #C1664 and #C1665 and HMAC Certs. #1664 and #C1665; key establishment methodology provides 128 or 256 bits of encryption strength)
- KTS (Triple-DES Certs. #C1664 and #C1665 and HMAC Certs. #1664 and #C1665; key establishment methodology provides 112 bits of encryption strength)

6.4 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.

6.5 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.

6.6 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 by calling the memset function to set the value to all zeroes.

6.7 Keys and CSPs life cycle

Table 9: CSP Table

Keys/CSPs	Size (in bits)	Generation	Storage	Entry/output	Destruction
TLS premaster secret	N/A	N/A	Address space storage	Input through API parameter	Zeroized when key context is closed

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

TLS master secret	N/A	Derived from premaster secret	Address space storage	Output through API parameters	Zeroized when key context is closed
AES keys	128, 256	TLS key agreement by the SP 800-135 TLS KDF	Address space storage	Input and output through API parameters	Zeroized when key context is closed
Triple-DES keys	192				
HMAC keys	> 112				
DSA private keys	L=2048, N=256	SP 800-90A DRBG as a seed to the FIPS 186-4 key generation methods (compliant to SP 800-133)			
RSA private keys	2048, 3072				
EC keys	P-224, P-256, P-384 and P-521	N/A			

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

7. 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).

8. Self-Tests

8.1 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.

8.2 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 rendered 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. Otherwise, it is performed against the CPACF. 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.

If any of the self-tests fail, the module is rendered unusable (all cryptographic services return an error return code). Any attempts to use the module will fail.

All other cryptographic algorithm provided by the bound modules are self-tested by the corresponding bound module.

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

8.3 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.

8.4 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

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

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.

8.5 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.

9. Operational Requirements (Officer/User Guidance)

9.1 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 2.
- 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.
- According to IG A.13, the same Triple-DES key shall not be used to encrypt more than 2^{16} 64-bit blocks of data.
- **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.

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

    - **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.

9.2 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.

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

10. Mitigation of Other Attacks

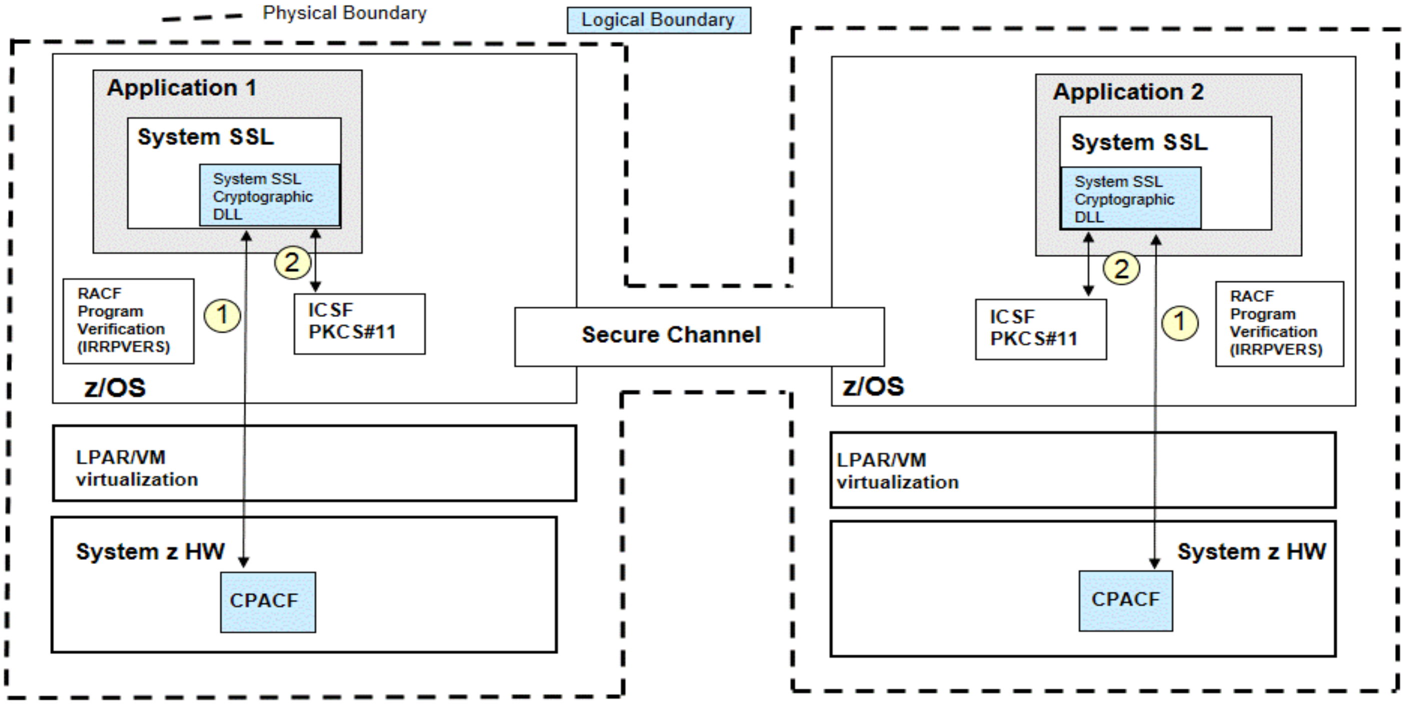
The Mitigation of Other attacks security section of FIPS 140-2 is not applicable to the System SSL cryptographic module.

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

11. 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 z14 with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863.

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

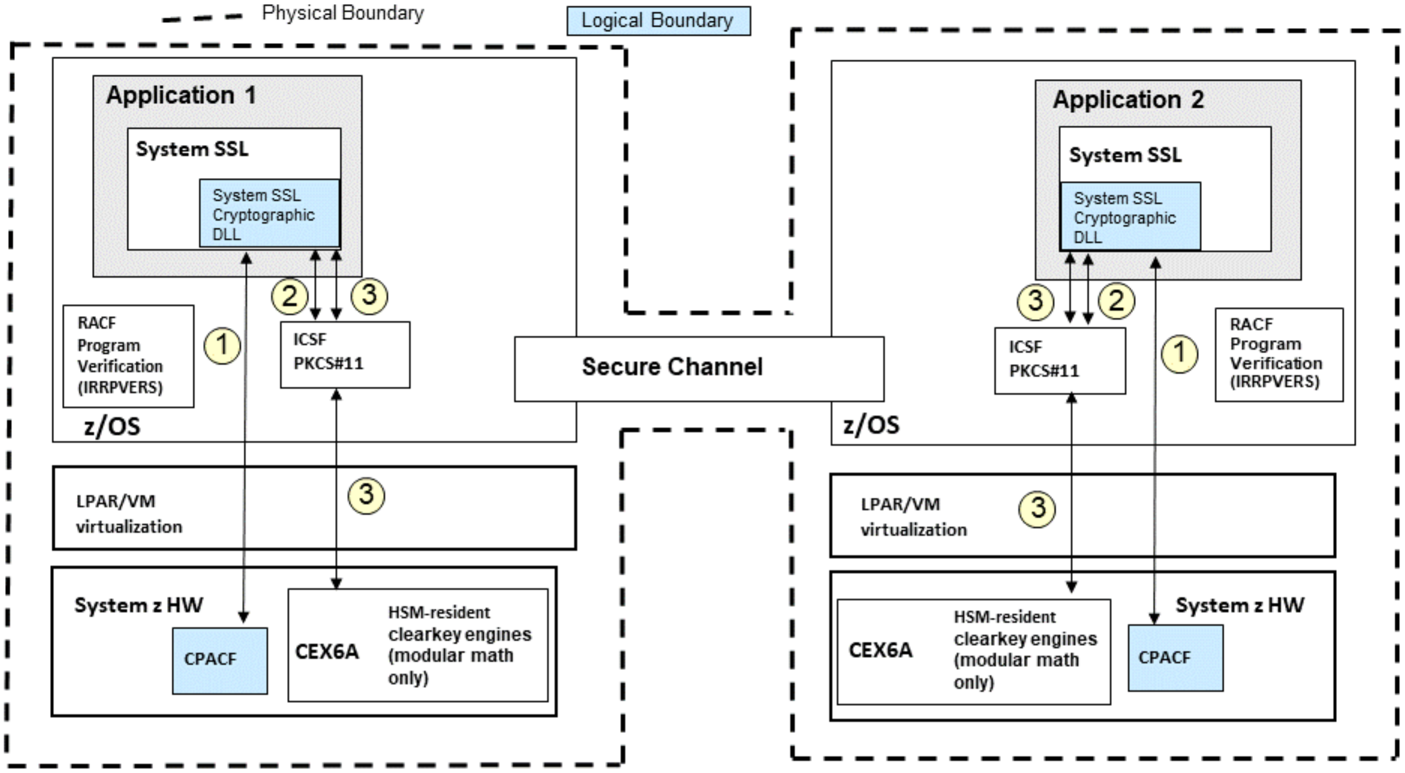


1 System SSL utilizes the CPACF for symmetric (TDES and AES) and hashing (SHA-1, SHA-2) algorithms.

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).

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

Figure 8: Validated Configuration with CPACF, ICSF PKCS #11 and CEX6A card


Physical Boundary
Logical Boundary
Application 1
System SSL
System SSL Cryptographic DLL
2
3
RACF Program Verification (IRRPVERS)
1
ICSF PKCS#11
z/OS
LPAR/VM virtualization
3
System z HW
CPACF
CEX6A
HSM-resident clearkey engines (modular math only)
Secure Channel
Application 2
System SSL
System SSL Cryptographic DLL
3
2
ICSF PKCS#11
1
RACF Program Verification (IRRPVERS)
z/OS
LPAR/VM virtualization
3
CEX6A
HSM-resident clearkey engines (modular math only)
System z HW
CPACF

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 CEX6A card

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

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

12. 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, the IBM Z mainframe server name for the IBM 4767 PCIe Cryptographic Coprocessor 5 hardware security module (HSM), configured as an accelerator

CEX6A Crypto Express6, the IBM Z mainframe server name for the IBM 4768 PCIe Cryptographic Coprocessor 6 hardware security module (HSM) configured as an accelerator

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]

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision

13. References

[1] z/OS Cryptographic Services Secure Sockets Layer Programming (SC14-7495)

[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)

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

[6] IBM z/OS Version 2 Release 4 ICSF PKCS#11 Cryptographic Module

[7] IBM z/OS Version 2 Release 4 Security Server RACF Signature Verification Module

[8] National Institute of Standards and Technology, Special Publication 800-131A Revision 2, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, March, 2019

14. Trademarks

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

- IBM
- RACF
- z/OS
- z13
- z14

© Copyright International Business Machines Corporation 2021
This document may be reproduced only in its original entirety without revision