z/OS

Cryptographic Services System Secure Sockets Layer Programming Changes to support NIST FIPS 140-2 Level 1 criteria - APAR OA50589 Documentation for V2R1

Contents

Chapter 1. Overview

This document describes the changes to System SSL information to support NIST FIPS 140-2 Level 1 criteria previously presented in *z/OS Cryptographic Services System Secure Sockets Layer Programming*, SC14-7495-00.

The preceding book documents capabilities provided in support of z/OS Version 2 Release 1.

Technical changes or additions related to the changes to support NIST FIPS 140-2 Level 1 criteria in this document are indicated by a vertical line to the left of the change.

These changes are available through the application of the PTFs for APAR OA50589.

Chapter 2. Updates to System SSL and FIPS 140-2

Algorithms and key sizes

When executing in FIPS mode, System SSL continues to take advantage of the CP Assist for Cryptographic Function (CPACF) when available. Hardware cryptographic functions allowed in FIPS mode support clear keys (requires at least one cryptographic card to be defined as an accelerator and online prior to the startup of ICSF) and secure PKCS #11 keys. Secure keys stored in the PKDS are not supported.

RSA digital signature verification, encryption, and decryption

When running in FIPS mode, if System SSL detects during runtime initialization that ICSF is available and that there is a cryptographic card available that is defined as an accelerator, System SSL attempts to call the ICSF callable services to perform clear key RSA digital signature verification, encryption, and decryption. The accelerator card must be online before the startup of ICSF. If ICSF is unable to perform the RSA cryptographic operation, System SSL performs the cryptographic operation in its software implementation. If the ICSF invocation returns with a severe error, software is used for the RSA operations until the System SSL runtime is reinitialized. If access to the ICSF services is being protected by the CSFSERV class profile, the application user ID must be authorized to the CSFPPD2, CSFPPE2, and CSFPPV2 services.

Function	ICSF PKCS #11 callable services	CSFSERV resources required - Read Access
RSA Decrypt	CSFPPD2	CSFPKD
RSA Encrypt	CSFPPE2	CSFPKE
RSA Digital Signature Verify	CSFPPV2	CSFDSV

System SSL module verification setup

The System SSL modules that support FIPS 140-2 are signed by using an IBM key during the build process. After System SSL is installed, more steps are required before the execution of a FIPS enabled System SSL application.

Chapter 3. Updates to API reference

gsk_environment_init()

Initializes an SSL environment.

Results

The function return value will be 0 (**GSK_OK**) if no error is detected. Otherwise, it will be one of the return codes listed in the **gskssl.h** include file.

[GSK_INTERNAL_ERROR]
An internal processing error has occurred.

Chapter 4. Updates to Certificate Management Services (CMS) API reference

gsk_add_record()

Adds a record to a key or request database.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_change_database_password()

Changes the database password.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_create_certification_request()

Creates a PKCS #10 certification request as described in PKCS #10, Version 1.7: *Certification Request*.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_create_database_renewal_request()

Creates a PKCS #10 certification renewal request.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_create_database_signed_certificate()

Creates a signed certificate as part of a set of certificates.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_create_renewal_request()

Creates a PKCS #10 certification renewal request.

This function is deprecated. Use **gsk_create_database_renewal_request()** instead.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_create_self_signed_certificate()

Creates a self-signed certificate.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_create_signed_certificate_set()

Creates a signed certificate as part of a set of certificates.

This function is deprecated. Use **gsk_create_database_signed_certificate()** instead.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_encode_export_key()

Encodes an X.509 certificate and its private key into a PKCS #12 data stream.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_export_key()

Exports a certificate and the associated private key.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_import_key()

Imports a certificate and associated private key.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_make_enveloped_data_content()

Create PKCS #7 EnvelopedData content information

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file. These are some possible errors:

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

[CMSERR_WEAK_KEY]
Triple DES (3DES) key parts are not unique.

Usage

When executing in FIPS mode, if a 3DES session key is supplied, the three key parts are checked for key uniqueness.

gsk_make_enveloped_data_content_extended()

Create PKCS #7 EnvelopedData content information.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

[CMSERR_WEAK_KEY]
Triple DES (3DES) key parts are not unique.

Usage

When executing in FIPS mode, if a 3DES session key is supplied, the three key parts are checked for key uniqueness.

gsk_make_enveloped_data_msg()

Creates a PKCS #7 EnvelopedData message from application data.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

[CMSERR_WEAK_KEY]
Triple DES (3DES) key parts are not unique.

Usage

When executing in FIPS mode, if a 3DES session key is supplied, the three key parts are checked for key uniqueness.

gsk_make_enveloped_data_msg_extended()

Creates a PKCS #7 EnvelopedData message from application data.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

[CMSERR_WEAK_KEY]
Triple DES (3DES) key parts are not unique.

Usage

When executing in FIPS mode, if a 3DES session key is supplied, the three key parts are checked for key uniqueness.

gsk_open_keyring()

Opens a SAF digital certificate key ring or z/OS PKCS #11 token.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_perform_kat()

Conducts a set of known answer tests for the System SSL algorithms validated by NIST. The caller must set FIPS mode (see 'gsk_fips_state_set()') before calling this function.

Usage

The **gsk_perform_kat()** routine can be used whenever an application, in order to meet security requirements, needs to check the correctness of cryptographic algorithms that are part of the product. The routine performs Known Answer Tests on the following cryptographic algorithms:

- AES CBC 128-bit and AES CBC 256-bit encryption and decryption
- DSA signature generation and verification
- RSA encrypt and decrypt
- RSA signature generation/verification and encryption/decryption
- SHA Digest Algorithms: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-384
- TLS V1.0, V1.1 and V1.2 key derivation function
- TripleDES encryption and decryption

If an error is encountered during testing, the **gsk_perform_kat()** routine will terminate and return the appropriate error code.

The **gsk_perform_kat()** routine will test software or hardware cryptographic algorithms depending on the value of the GSK_HW_CRYPTO environment variable.

gsk_replace_record()

Replaces a record in a key or request database.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

gsk_set_default_key()

Sets the default key.

Results

The function return value will be 0 if no error is detected. Otherwise, it will be one of the return codes listed in the **gskcms.h** include file.

[CMSERR_INTERNAL_ERROR]
An internal processing error has occurred.

Chapter 5. Updates to Deprecated Secure Socket Layer (SSL) APIs

gsk_initialize()

Initializes the System SSL runtime environment.

Results

The function return value will be 0 (**GSK_OK**) if no error is detected. Otherwise, it will be one of the return codes listed in the **gskssl.h** include file.

[GSK_ERROR_INTERNAL]
An internal processing error has occurred.

Chapter 6. Updates to Messages and codes

This topic lists the messages and codes issued by System SSL.

SSL function return codes

3 An internal error has occurred.

Explanation: The System SSL runtime library detected an internal processing error.

User response: Retry the operation. If the problem persists, collect a System SSL trace containing the error and then contact your service representative.

9 Cryptographic processing error.

Explanation: An error is detected by a cryptographic function. This error might also occur while running in FIPS mode when negotiating a secure connection and a non-FIPS key size is used or a triple DES cipher is used and the negotiated triple DES session key does not have three unique key parts.

User response: If the error occurred while executing in FIPS mode, check that only FIPS key sizes are used. If the error occurred during the establishment of a secure connection in FIPS mode using a triple DES cipher, retry the connection.

If the problem persists, collect a System SSL trace containing the error and then contact your service representative.

For more information about FIPS key sizes, see Chapter 4, “System SSL and FIPS 140-2”, in *z/OS Cryptographic Services System Secure Sockets Layer Programming*, SC14-7495-00.

Deprecated SSL function return codes

-29 An internal error has occurred.

Explanation: The System SSL runtime library detected an internal processing error.

User response: Retry the operation. If the problem persists, collect a System SSL trace containing the error and then contact your service representative.

-36 Cryptographic processing error.

Explanation: An error is detected by a cryptographic function. This error might also occur while running in FIPS mode when negotiating a secure connection and a non-FIPS key size is used or a triple DES cipher is used and the negotiated triple DES session key does not have three unique key parts.

User response: If the error occurred while executing in FIPS mode, check that only FIPS key sizes are used. If the error occurred during the establishment of a secure connection in FIPS mode using a triple DES cipher, retry the connection.

If the problem persists, collect a System SSL trace containing the error and then contact your service representative.

For more information about FIPS key sizes, see Chapter 4, “System SSL and FIPS 140-2”, in *z/OS Cryptographic Services System Secure Sockets Layer Programming*, SC14-7495-00.

CMS status codes

03353036 **Encryption key is weak**

Explanation: A small subset of the possible DES and Triple DES encryption keys are weak and can be broken more easily than the rest of the keys. For this reason, the weak keys should be avoided when generating a DES or Triple DES key. The error can also occur while running in FIPS mode with a user supplied Triple DES session key when the key does not contain 3 unique key parts.

User response: A user supplied triple DES key was found to be weak or a Triple DES key was specified that did not have three unique key parts. Ensure the key being used is valid and retry the operation. If the problem persists, collect a System SSL trace containing the error and then contact your service representative.

0335306C **Attempt to execute in FIPS mode failed.**

Explanation: A request to execute in FIPS mode failed because the required System SSL DLLs could not be loaded.

User response: Ensure that the Cryptographic Services Security Level 3 FMID is installed and that module verification has been setup correctly. See 'System SSL module verification setup' in Chapter 4 'System SSL and FIPS 140-2', in *z/OS Cryptographic Services System Secure Sockets Layer Programming*, SC14-7495-00, for module verification information. Module verification failures may also result in RACF messages (for example, ICH440I) being written to the console with information about the failure. If the module verification problem persists, collect a System SSL trace containing the error and then contact your service representative.

033530A9 **An internal error has occurred**

Explanation: The System SSL runtime library detected an internal processing error.

User response: Retry the operation. If the problem persists, collect a System SSL trace containing the error and then contact your service representative.

SSL started task messages (GSK01nnn)

GSK01051E *Jobname/ASID* **Hardware encryption error. ICSF hardware encryption processing is unavailable**

Explanation: The specified job encountered a severe hardware encryption error during ICSF hardware processing. Encryption functions are processed in software. See message GSK01052W in the system log for algorithm-specific detail. This message can also be issued when the job is running in FIPS mode if during System SSL runtime initialization, it was determined that a cryptographic card that is configured as an accelerator was available and a later call to ICSF for an RSA operation resulted in a severe error.

User response: Ensure that ICSF hardware encryption services are installed and functioning correctly. Restart the SSL application or process to reinitialize the SSL DLLs.

GSK01052W *Jobname/ASID* **Hardware encryption error.** *Algorithm* **encryption processing switched to software**

Explanation: The specified job encountered a severe ICSF or hardware encryption error. ICSF or hardware processing for the specified algorithm has been disabled. Any future encryption or decryption using this algorithm is performed in software for the particular SSL application or process.

User response: Ensure that ICSF hardware encryption services are installed and functioning correctly. Restart the SSL application or process to reinitialize the SSL DLLs.

Printed in USA