z/OS

Cryptographic Services Integrated Cryptographic Service Facility New PKCS #11 Key Structure Callable Services APAR OA50113

Contents

Chapter 1. Overview 1

Chapter 2. Update of z/OS Cryptographic Services ICSF Application Programmer's Guide, SC14-7508-05, information. . . . 3

PKCS #11 Services 3

Using the PKCS #11 key structure callable services . 3

PKCS #11 Private Key Structure Decrypt (CSFPPD2 and CSFPPD26). 4

PKCS #11 Private Key Structure Sign (CSFPPS2 and CSFPPS26) 7

PKCS #11 Public Key Structure Encrypt (CSFPPE2 and CSFPPE26) 9

PKCS #11 Public Key Structure Verify (CSFPPV2 and CSFPPV26) 12

PKCS #11 Private Key Sign (CSFPPKS and CSFPPKS6) 14

Parameters 15

Chapter 3. Update of z/OS Cryptographic Services ICSF Administrator's Guide, SC14-7506-05, information 17

Setting up profiles in the CSFSERV general resource class 17

Chapter 4. Update of z/OS Cryptographic Services ICSF System Programmer's Guide, SC14-7507-05, information 19

Callable services 19

CICS attachment facility 19

Chapter 5. Update of z/OS Cryptographic Services ICSF Writing PKCS #11 Applications, SC14-7510-03, information 21

Key types and mechanisms supported 21

Chapter 1. Overview

This document describes changes to the Integrated Cryptographic Service Facility (ICSF) product in support of the new PKCS #11 key structure callable services:

- PKCS #11 Private key structure decrypt (CSFPPD2 and CSFPPD26)
- PKCS #11 Private key structure sign (CSFPPS2 and CSFPPS26)
- PKCS #11 Public key structure encrypt (CSFPPE2 and CSFPPE26)
- PKCS #11 Public key structure verify (CSFPPV2 and CSFPPV26)

These changes are available through the application of the PTF for APAR OA50113 and apply to FMID HCR77B1, HCR77B0, HCR77A1, and HCR77A0.

This document contains alterations to information previously presented in the following books:

- *z/OS Cryptographic Services ICSF Application Programmer's Guide*, SC14-7508-05
- *z/OS Cryptographic Services ICSF Administrator's Guide*, SC14-7506-05
- *z/OS Cryptographic Services ICSF System Programmer's Guide*, SC14-7507-05
- *z/OS Cryptographic Services ICSF Writing PKCS #11 Applications*, SC14-7510-03

The technical changes made to the ICSF product by the application of the PTF for APAR OA50113 are indicated in this document by a vertical line to the left of the change.

Chapter 2. Update of z/OS Cryptographic Services ICSF Application Programmer's Guide, SC14-7508-05, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF Application Programmer's Guide*, SC14-7508-05, for the new PKCS #11 key structure callable services provided by this APAR. Refer to this source document if background information is needed.

PKCS #11 Services

ICSF provides callable services that offer a fast-path alternative to some of the traditional PKCS #11 callable services. The following table summarizes these callable services. For complete syntax and reference information, refer to "Using the PKCS #11 key structure callable services."

Table 1. Summary of PKCS #11 callable services that offer a fast-path alternative

Verb	Service Name	Function
CSFPPD2	PKCS #11 Private key structure decrypt	Decrypt data using an RSA private key structure.
CSFPPE2	PKCS #11 Public key structure encrypt	Encrypt data using an RSA public key structure.
CSFPPS2	PKCS #11 Private key structure sign	Sign data using an RSA private key structure.
CSFPPV2	PKCS #11 Public key structure verify	Verify data using an RSA public key structure.

Using the PKCS #11 key structure callable services

This topic describes the PKCS #11 key structure callable services which offer a fast-path alternative to some of the traditional PKCS #11 callable services. Under the standard PKCS #11 callable services, a key must first be established as an object before it may be used for a cryptographic operation. When that key is no longer needed, that key should be deleted to prevent it from consuming resources unnecessarily.

The PKCS #11 key structure callable services allow you to specify the key structure (rather than the key handle) as an in-memory parameter. This eliminates the need to create and delete the key object.

The PKCS #11 key structure callable services support the ASN.1 clear key structures:

The PKCS #8 PrivateKeyInfo structure

This key structure is defined in section 5 of RFC 5208 *Public-Key Cryptography Standards (PKCS) #8: Private-Key Information Syntax Specification Version 1.2.*

```
Private-Key Information Syntax

This section gives the syntax for private-key information.

Private-key information shall have ASN.1 type PrivateKeyInfo:
```

```
PrivateKeyInfo ::= SEQUENCE {
  version                   Version,
  privateKeyAlgorithm       PrivateKeyAlgorithmIdentifier,
  privateKey                PrivateKey,
  attributes           [0]  IMPLICIT Attributes OPTIONAL }
Version ::= INTEGER
PrivateKeyAlgorithmIdentifier ::= AlgorithmIdentifier
PrivateKey ::= OCTET STRING
Attributes ::= SET OF Attribute
```

The SubjectPublicKeyInfo structure

This key structure is defined in section 4.1 of RFC 3820 *Internet X.509 Public Key Infrastructure*.

```
SubjectPublicKeyInfo  ::=  SEQUENCE  {
   algorithm            AlgorithmIdentifier,
   subjectPublicKey     BIT STRING  }
```

See each PKCS #11 key structure callable service for information on which key structure is supported:

- "PKCS #11 Private Key Structure Decrypt (CSFPPD2 and CSFPPD26)"
- "PKCS #11 Private Key Structure Sign (CSFPPS2 and CSFPPS26)" on page 7
- "PKCS #11 Public Key Structure Encrypt (CSFPPE2 and CSFPPE26)" on page 9
- "PKCS #11 Public Key Structure Verify (CSFPPV2 and CSFPPV26)" on page 12

PKCS #11 Private Key Structure Decrypt (CSFPPD2 and CSFPPD26)

Use the PKCS #11 private key structure decrypt callable service to decrypt data using a clear RSA private key. PKCS #1 v1.5 formatting is used. The key must be a DER encoded PrivateKeyInfo structure as specified by PKCS #8.

The callable service can be invoked in AMODE(24), AMODE(31), or AMODE(64). 64-bit callers must use CSFPPD26.

Format

```
CALL CSFPPD2(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             cipher_value_length,
             cipher_value,
             reserved,
             clear_value_length,
             clear_value,
             private_key_info_length,
             private_key_info)
```

Parameters

return_code

Direction	Type
Output	Integer

The return code specifies the general result of the callable service.

reason_code

Direction	Type
Output	Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems.

exit_data_length

Direction	Type
Ignored	Integer

This field is ignored. It is recommended to specify 0 for this parameter.

exit_data

Direction	Type
Ignored	String

This field is ignored.

rule_array_count

Direction	Type
Input	Integer

The number of keywords you supplied in the *rule_array* parameter. This value must be 1.

rule_array

Direction	Type
Input	String

Keywords that provide control information to the callable service. Table 2 lists the keywords. Each keyword is left-justified in an 8-byte field and padded on the right with blanks. All keywords must be in contiguous storage.

Table 2. Keywords for Private Key Structure Decrypt

Keyword	Meaning
Mechanism (The following must be specified)	
RSA-PKCS	Mechanism is RSA decryption using PKCS #1 v1.5 formatting.

cipher_value_length

Direction	Type
Input	Integer

The length of the *cipher_value* parameter in bytes. Must be the size of the modulus of the key.

cipher_value

Direction	Type
Input	String

The value to be decrypted.

reserved

Direction	Type
Ignored	String

This field is currently not used.

clear_value_length

Direction	Type
Input/Output	Integer

The length in bytes of the *clear_value* parameter. On input, this must be at least the size of the RSA modulus in bytes. On output, this is updated to be the actual length of the decrypted value.

clear_value

Direction	Type
Output	String

This field contains the decrypted value.

private_key_info_length

Direction	Type
Input	Integer

Length in bytes of the *private_key_info* parameter. The maximum size you can specify is 3000 bytes.

private_key_info

Direction	Type
Input	String

The DER encoded PrivateKeyInfo structure as specified by PKCS #8. The *privateKeyAlgorithm* field of this structure must indicate that the key is an RSA key.

Authorization

The CSFSERV resource name that protects this service is CSFPKD, and it is the same resource name that is used to protect the PKA Decrypt service.

Usage notes

- This service always enforces FIPS restrictions.
- This service requires an IBM eServer zSeries 990 or later machine type.
- The *attributes* field in the key structure is ignored.

PKCS #11 Private Key Structure Sign (CSFPPS2 and CSFPPS26)

Use the PKCS #11 private key structure sign callable service to sign data using a clear RSA private key. PKCS #1 v1.5 formatting is used. The key must be a DER encoded PrivateKeyInfo structure as specified by PKCS #8.

The callable service can be invoked in AMODE(24), AMODE(31), or AMODE(64). 64-bit callers must use CSFPPS26.

Format

```
CALL CSFPPS2(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             hash_length,
             hash,
             reserved,
             signature_length,
             signature,
             private_key_info_length,
             private_key_info)
```

Parameters

return_code

Direction	Type
Output	Integer

The return code specifies the general result of the callable service.

reason_code

Direction	Type
Output	Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems.

exit_data_length

Direction	Type
Ignored	Integer

This field is ignored. It is recommended to specify 0 for this parameter.

exit_data

Direction	Type
Ignored	String

This field is ignored.

rule_array_count

Direction	Type
Input	Integer

The number of keywords you supplied in the *rule_array* parameter. This value must be 1.

rule_array

Direction	Type
Input	String

Keywords that provide control information to the callable service. Table 3 lists the keywords. Each keyword is left-justified in an 8-byte field and padded on the right with blanks. All keywords must be in contiguous storage.

Table 3. Keywords for Private Key Structure Sign

Keyword	Meaning
Mechanism (The following must be specified)	
RSA-PKCS	Mechanism is RSA signature generation using PKCS #1 v1.5 formatting.

hash_length

Direction	Type
Input	Integer

The length of the *hash* parameter in bytes.

hash

Direction	Type
Input	String

The value to be signed. This is expected to be a DER encoded DigestInfo structure.

reserved

Direction	Type
Ignored	String

This field is currently not used.

signature_length

Direction	Type
Input/Output	Integer

The length in bytes of the *signature* parameter. On output, this is updated to be the actual length of the generated signature.

signature

Direction	Type
Output	String

This field contains the generated signature.

private_key_info_length

Direction	Type
Input	Integer

Length in bytes of the *private_key_info* parameter. The maximum size you can specify is 3000 bytes.

private_key_info

Direction	Type
Input	String

The DER encoded PrivateKeyInfo structure as specified by PKCS #8. The *privateKeyAlgorithm* field of this structure must indicate that the key is an RSA key.

Authorization

The CSFSERV resource name that protects this service is CSFDSG, and it is the same resource name that is used to protect the PKA Digital Signature Generate service.

Usage notes

- This service always enforces FIPS restrictions.
- This service requires an IBM eServer zSeries 990 or later machine type.
- The *attributes* field in the key structure is ignored.

PKCS #11 Public Key Structure Encrypt (CSFPPE2 and CSFPPE26)

Use the PKCS #11 public key structure encrypt callable service to encrypt data using an RSA public key. PKCS #1 v1.5 formatting is used. The key must be a DER encoded SubjectPublicKeyInfo structure as specified by RFC 3280.

The callable service can be invoked in AMODE(24), AMODE(31), or AMODE(64). 64-bit callers must use CSFPPE26.

Format

```
CALL CSFPPE2(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             clear_value_length,
             clear_value,
             reserved,
             cipher_value_length,
             cipher_value,
             subject_public_key_info_length,
             subject_public_key_info)
```

Parameters

return_code

Direction	Type
Output	Integer

The return code specifies the general result of the callable service.

reason_code

Direction	Type
Output	Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems.

exit_data_length

Direction	Type
Ignored	Integer

This field is ignored. It is recommended to specify 0 for this parameter.

exit_data

Direction	Type
Ignored	String

This field is ignored.

rule_array_count

Direction	Type
Input	Integer

The number of keywords you supplied in the *rule_array* parameter. This value must be 1.

rule_array

Direction	Type
Input	String

Keywords that provide control information to the callable service. Table 4 lists the keywords. Each keyword is left-justified in an 8-byte field and padded on the right with blanks. All keywords must be in contiguous storage.

Table 4. Keywords for Public Key Structure Encrypt

Keyword	Meaning
Mechanism (The following must be specified)	
RSA-PKCS	Mechanism is RSA signature encryption using PKCS #1 v1.5 formatting.

clear_value_length

Direction	Type
Input	Integer

The length in bytes of the *clear_value* parameter.

clear_value

Direction	Type
Input	String

The signature value to be encrypted.

reserved

Direction	Type
Ignored	String

This field is currently not used.

cipher_value_length

Direction	Type
Input/Output	Integer

The length of the *cipher_value* parameter in bytes. On output, this is updated to be the actual length of the encrypted value.

cipher_value

Direction	Type
Output	String

This field contains the encrypted value.

subject_public_key_info_length

Direction	Type
Input	Integer

Length in bytes of the *subject_public_key_info* parameter. The maximum size you can specify is 3000 bytes.

subject_public_key_info

Direction	Type
Input	String

The DER encoded SubjectPublicKeyInfo structure as specified by RFC 3280. The *algorithm* field of this structure must indicate that the key is an RSA key.

Authorization

The CSFSERV resource name that protects this service is CSFPKE, and it is the same resource name used to protect the PKA Encrypt service.

Usage notes

- This service always enforces FIPS restrictions.
- This service requires an IBM eServer zSeries 990 or later machine type.

PKCS #11 Public Key Structure Verify (CSFPPV2 and CSFPPV26)

Use the PKCS #11 public key structure verify callable service to verify data using an RSA public key. PKCS #1 v1.5 formatting is used. The key must be a DER encoded SubjectPublicKeyInfo structure as specified by RFC 3280.

The callable service can be invoked in AMODE(24), AMODE(31), or AMODE(64). 64-bit callers must use CSFPPV26.

Format

```
CALL CSFPPV2(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             signature_length,
             signature,
             reserved,
             hash_length,
             hash,
             subject_public_key_info_length,
             subject_public_key_info)
```

Parameters

return_code

Direction	Type
Output	Integer

The return code specifies the general result of the callable service.

reason_code

Direction	Type
Output	Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems.

exit_data_length

Direction	Type
Ignored	Integer

This field is ignored. It is recommended to specify 0 for this parameter.

exit_data

Direction	Type
Ignored	String

This field is ignored.

rule_array_count

Direction	Type
Input	Integer

The number of keywords you supplied in the *rule_array* parameter. This value must be 1.

rule_array

Direction	Type
Input	String

Keywords that provide control information to the callable service. Table 5 lists the keywords. Each keyword is left-justified in an 8-byte field and padded on the right with blanks. All keywords must be in contiguous storage.

Table 5. Keywords for Public Key Structure Verify

Keyword	Meaning
Mechanism (The following must be specified)	
RSA-PKCS	Mechanism is RSA signature verification using PKCS #1 v1.5 formatting.

signature_length

Direction	Type
Input	Integer

The length in bytes of the *signature* parameter.

signature

Direction	Type
Input	String

The signature value to be validated.

reserved

Direction	Type
Ignored	String

This field is currently not used.

hash_length

Direction	Type
Input	Integer

The length of the *hash* parameter in bytes.

hash

Direction	Type
Input	String

The value to be verified. This is expected to be a DER encoded DigestInfo structure.

subject_public_key_info_length

Direction	Type
Input	Integer

Length in bytes of the *subject_public_key_info* parameter. The maximum size you can specify is 3000 bytes.

subject_public_key_info

Direction	Type
Input	String

The DER encoded SubjectPublicKeyInfo structure as specified by RFC 3280. The *algorithm* field of this structure must indicate that the key is an RSA key.

Authorization

The CSFSERV resource name that protects this service is CSFDSV, and it is the same resource name used to protect the PKA Digital Signature Verify service.

Usage notes

- This service always enforces FIPS restrictions.
- This service requires an IBM eServer zSeries 990 or later machine type.

PKCS #11 Private Key Sign (CSFPPKS and CSFPPKS6)

Use the PKCS #11 Private Key Sign callable service to:

- Decrypt or sign data using an RSA private key using zero-pad or PKCS #1 v1.5 formatting.
- Sign data using a DSA private key.
- Sign data using an Elliptic Curve private key in combination with DSA.

The key handle must be a handle of a PKCS #11 private key object. When the request type keyword DECRYPT is specified in the rule array, CKA_DECRYPT attribute must be true. When no request type is specified, the CKA_SIGN attribute must be true.

The callable service can be invoked in AMODE(24), AMODE(31), or AMODE(64). 64-bit callers must use CSFPPKS6.

Parameters

return_code

Direction	Type
Output	Integer

The return code specifies the general result of the callable service.

reason_code

Direction	Type
Output	Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes that indicate specific processing problems.

exit_data_length

Direction	Type
Ignored	Integer

This field is ignored. It is recommended to specify 0 for this parameter.

exit_data

Direction	Type
Ignored	String

This field is ignored.

rule_array_count

Direction	Type
Input	Integer

The number of keywords you supplied in the *rule_array_parameter*. This value may be 1 or 2.

rule_array

Direction	Type
Input	String

Keywords that provide control information to the callable service.

Table 6. Keywords for private key sign

Keyword	Meaning
Mechanism (One of the following must be specified)	
RSA-ZERO	Mechanism is RSA decryption or signature generation using zero-pad formatting
RSA-PKCS	Mechanism is RSA decryption or signature generation using PKCS #1 v1.5 formatting
DSA	Mechanism is DSA signature generation

Table 6. Keywords for private key sign (continued)

Keyword	Meaning
ECDSA	Mechanism is Elliptic Curve with DSA signature generation
Request type (optional)	
DECRYPT	The request is to decrypt data. This type of request requires the CKA_DECRYPT attribute to be true. If DECRYPT is not specified, the CKA_SIGN attribute must be true. Valid with RSA only.

cipher_value_length

Direction	Type
Input	Integer

Length of the *cipher_value* parameter in bytes.

cipher_value

Direction	Type
Input	String

For decrypt, this is the value to be decrypted. Otherwise this is the value to be signed. For RSA-PKCS signature requests, the data to be signed is expected to be a DER encoded DigestInfo structure. For DSA and ECDSA signature requests, the data to be signed is expected to be a SHA1, SHA224, SHA256, SHA384 or SHA512 digest.

key_handle

Direction	Type
Input	String

The 44-byte handle of a private key object.

clear_value_length

Direction	Type
Input/Output	Integer

Length of the *clear_value* parameter in bytes. On input, this must be at least the size of the RSA modulus in bytes. On output, this is updated to be the actual length of the decrypted value or the generated signature.

clear_value

Direction	Type
Output	String

For decrypt, this field will contain the decrypted value. Otherwise this field will contain the generated signature.

Chapter 3. Update of z/OS Cryptographic Services ICSF Administrator's Guide, SC14-7506-05, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF Administrator's Guide*, SC14-7506-05, for the new PKCS #11 key structure callable services provided by this APAR. Refer to this source document if background information is needed.

Setting up profiles in the CSFSERV general resource class

Table 7. Resource names for ICSF callable services

Resource name	Callable service names	Callable service description
CSFDSG	CSNDDSG CSNFDSG CSFPPS2 CSFPPS26	Digital Signature Generate PKCS #11 Private key structure sign
CSFDSV	CSNDDSV CSNFDSV CSFPPV2 CSFPPV26	Digital Signature Verify PKCS #11 Public key structure verify
CSFPKD	CSNDPKD CSNFPKD CSFPPD2 CSFPPD26	PKA Decrypt PKCS #11 Private key structure decrypt
CSFPKE	CSNDPKE CSNFPKE CSFPPE2 CSFPPE26	PKA Encrypt PKCS #11 Public key structure encrypt

Chapter 4. Update of z/OS Cryptographic Services ICSF System Programmer's Guide, SC14-7507-05, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF System Programmer's Guide*, SC14-7507-05, for the new PKCS #11 key structure callable services provided by this APAR. Refer to this source document if background information is needed.

Callable services

The following table summarizes the new and changed callable services for ICSF FMID HCR77A0. For complete reference information on these callable services, refer to *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

Table 8. Summary of new and changed ICSF callable services

Callable service	FMID	Description
PKCS #11 Private Key Structure Decrypt	HCR77A0	**New**: Decrypt data using a clear private key structure.
PKCS #11 Private Key Structure Sign	HCR77A0	**New**: Sign data using a clear private key structure.
PKCS #11 Public Key Structure Encrypt	HCR77A0	**New**: Encrypt data using a public key structure.
PKCS #11 Public Key Structure Verify	HCR77A0	**New**: Verify a signature using a public key structure.

CICS attachment facility

If you have the CICS Attachment Facility installed and you specify your own CICS wait list data set, you need to modify the wait list data set to include the new callable services.

Modify and include:

HCR77A0
CSF1PD2, CSF1PE2, CSF1PS2, CSF1PV2.

Chapter 5. Update of z/OS Cryptographic Services ICSF Writing PKCS #11 Applications, SC14-7510-03, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF Writing PKCS #11 Applications*, SC14-7510-03, for the new PKCS #11 key structure callable services provided by this APAR. Refer to this source document if background information is needed.

Key types and mechanisms supported

The following table lists the algorithms and uses (by mechanism) that are not allowed when operating in compliance with FIPS 140-2. For more information about how the z/OS PKCS #11 services can be configured to operate in compliance with the FIPS 140-2 standard, refer to

Table 9. Restricted algorithms and uses when running in compliance with FIPS 140-2

Algorithm	Mechanisms	Usage disallowed
Triple DES	CKM_DES3_ECB, CKM_DES3_CBC, CKM_DES3_CBC_PAD	Two key Triple DES. Three key Triple DES encryption or key wrap where the individual DES key parts are not unique.

Printed in USA