z/OS

Cryptographic Services Integrated Cryptographic Service Facility Key Encryption Translate (CSNBKET and CSNEKET) Service APAR OA49443

Contents

Chapter 1. Overview

This document describes changes to the Integrated Cryptographic Service Facility (ICSF) product in support of the new Key Encryption Translate (CSNBKET and CSNEKET) service used to change the encryption of key material in a key token wrapped with ECB (legacy method) and key material wrapped CBC.

These changes are available through the application of the PTF for APAR OA49443 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*, SC14-7508-04
- *z/OS Cryptographic Services ICSF Administrator's Guide*, SC14-7506-04
- *z/OS Cryptographic Services ICSF System Programmer's Guide*, SC14-7507-04

The technical changes made to the ICSF product by the application of the PTF for APAR OA49443 are indicated in this document by a vertical line to the left of the change.

Chapter 2. Update of z/OS Cryptographic Services ICSF System Programmer's Guide, SC14-7507-04, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF System Programmer's Guide*, SC14-7507-04, for the updates provided by this APAR. Refer to this source document if background information is needed.

Installation, initialization, and customization

Table 1. Exit identifiers and exit invocations

Exit identifiers	Exit invocations
CSFKET	Gets control during the Key Encryption Translate callable service.

Migration

Callable services

The following table summarizes the new and changed callable services for ICSF FMID HCR77B1. For complete reference information on these callable services, refer to *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

Table 2. Summary of new and changed ICSF callable services

Callable service	FMID	Description
Key Encryption Translate	HCR77B1	**New:** Change the method of encryption of DES key material.

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
CSFKET

Installation exits

Table 3. Services and their ICSF names

Service	*ICSF name*
Key Encryption Translate	**CSFKET**

Chapter 3. Update of z/OS Cryptographic Services ICSF Application Programmer's Guide, SC14-7508-04, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF Application Programmer's Guide*, SC14-7508-04, for the updates provided by this APAR. Refer to this source document if background information is needed.

Introducing symmetric key cryptography and using symmetric key callable services

DES key types

The DES keys are 64-bit, 128-bit, and 192-bit keys that use the DES algorithm to perform the cryptographic function. A 64-bit key is referred to as a single-length key. A 128-bit key is referred to as a double-length key. Triple-length keys are 192-bits in length. Only DATA keys can be triple-length.

For installations that do not support double-length key-encrypting keys, effective single-length keys are provided. For an effective single-length key, the clear key value of the left key half equals the clear key value of the right key half.

Table 4. Descriptions of DES key types and service usage

DES key type	Usable with services
Key-encrypting key class These keys are used to wrap other keys. The keys are double-length keys.	
EXPORTER	Control Vector Translate, Data Key Export, Derive ICC MK, ECC Diffie-Hellman, Generate Issuer MK, Key Encryption Translate, Key Export, Key Generate, Key Test2, Key Test Extended, Key Translate, Key Translate2, PKA Key Generate, PKA Key Translate, Prohibit Export Extended, Remote Key Export, Secure Messaging for Keys, Symmetric Key Generate, TR-31 Export, TR-31 Import, Unique Key Derive
IMPORTER	Control Vector Translate, Data Key Import, ECC Diffie-Hellman, Generate Issuer MK, Key Encryption Translate, Key Generate, Key Import, Key Test2, Key Test Extended, Key Translate, Key Translate2, Multiple Secure Key Import, PKA Key Generate, PKA Key Import, PKA Key Translate, Prohibit Export Extended, Remote Key Export, Restrict Key Attribute, Secure Key Import, Secure Messaging for Keys, Symmetric Key Generate, TR-31 Export, TR-31 Import

Key Encryption Translate Callable Service (CSNBKET and CSNEKET)

Use the Key Encryption Translate service to change the method of encryption of the key material.

Summary of callable services

Table 5 lists the callable services described in this publication, and their corresponding verbs. The figure also references the topic that describes the callable service.

Table 5. Summary of ICSF callable services

Service	Service name	Function
Chapter 5, "Managing Symmetric Cryptographic Keys"		
CSNBKET CSNEKET	Key Encryption Translate	Change the encryption of DES key material in a key token wrapped with ECB (legacy method) and key material wrapped CBC.

Managing Symmetric Cryptographic Keys

Key Encryption Translate (CSNBKET and CSNEKET)

Use the Key Encryption Translate service to change the method of encryption of DES key material. The input key can be a double-length external DES CCA DATA key token, or a double-length CBC-encrypted key. The return key is encrypted using CBC encryption or CCA (ECB) encryption. The CCA DATA key must be double-length and have an all-zero control vector. The CBC-encrypted key is treated as a 16-byte string encrypted with an all-zero initialization vector.

Note: This service does not handle keys wrapped using the enhanced method.

The callable service name for AMODE(64) invocation is CSNEKET.

Format

```
CALL CSNBKET(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             kek_key_identifier_length,
             kek_key_identifier,
             key_in_length,
             key_in,
             key_out_length,
             key_out)
```

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
Input/Output	Integer

The length of the data that is passed to the installation exit. The data is identified in the *exit_data* parameter.

exit_data

Direction	Type
Input/Output	String

The data that is passed to the installation exit.

rule_array_count

Direction	Type
Input	Integer

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

rule_array

Direction	Type
Input	String

The *rule_array* contains keywords that provide control information to the callable service. The keywords must be in contiguous storage with each of the keywords left-justified in its own 8-byte location and padded on the right with blanks.

The *rule_array* keywords are:

Table 6. Keywords for Key Encryption Translate

Keyword	Meaning
Key translation method (one required)	
CBCTOECB	Specifies decryption of a 16-byte string and CCA encryption of the resulting clear-key value as an external CCA DATA key.
ECBTOCBC	Specifies decryption of a CCA DATA key and the CBC encryption of the resulting clear key.

kek_key_identifier_length

Direction	Type
Input	Integer

The length of the *kek_key_identifier* parameter in bytes. The value must be 64.

kek_key_identifier

Direction	Type
Input/Output	String

The key-encrypting key used to decrypt the input key and to encrypt the output key. This is an internal token or the 64-byte label of a key in the CKDS. For the CBCTOECB keyword, the key must be a DES IMPORTER key. For the ECBTOCBC keyword, the key must be a DES EXPORTER key.

If the token supplied was encrypted under the old master key, the token will be returned encrypted under the current master key.

key_in_length

Direction	Type
Input	Integer

The length of the *key_in* parameter in bytes. The value must be 16 for a **CBCTOECD** translation or 64 for an **ECBTOCBC** translation.

key_in

Direction	Type
Input	String

The key material or key token to be translated. This is either a CCA external key token or a 16–byte CBC-encrypted key.

key_out_length

Direction	Type
Input/Output	Integer

The length of the *key_out* parameter in bytes. On input, set value must be:

- At least 16 for the ECBTOCBC translation.
- At least 64 for the CBCTOECB translation.

Upon successful completion, the parameter is set to the length of the value returned in the *key_out* parameter.

key_out

Direction	Type
Output	String

The translated key material or key token.

Usage notes

SAF may be invoked to verify the caller is authorized to use this callable service, the key label, or internal secure key tokens that are stored in the CKDS.

Access control points

The following access control points in the domain role control the function of this service:

Table 7. Required access control points for Key Encryption Translate

Rule array keyword	Access control point
CBCTOECB	Key Encryption Translate – CBC to ECB
ECBTOCBC	Key Encryption Translate – ECB to CBC

Note: These access controls are not enabled in the domain role. A TKE workstation is required to enable them.

Required hardware

This table lists the required cryptographic hardware for each server type and describes restrictions for this callable service.

Table 8. Key Encryption Translate required hardware

Server	Required cryptographic hardware	Restrictions
IBM eServer zSeries 990 IBM eServer zSeries 890		This service is not supported.
IBM System z9 EC IBM System z9 BC		This service is not supported.
IBM System z10 EC IBM System z10 BC	Crypto Express2 Coprocessor	This service is not supported.
	Crypto Express3 Coprocessor	
IBM zEnterprise 196 IBM zEnterprise 114	Crypto Express3 Coprocessor	
IBM zEnterprise EC12 IBM zEnterprise BC12	Crypto Express3 Coprocessor Crypto Express4 CCA Coprocessor	
IBM z13	Crypto Express5 CCA Coprocessor	

Access control points and callable services

Table 9. Access control points – Callable Services

Access control point name	Callable service	Usage
Key Encryption Translate – CBC to ECB	CSNBKET / CSNEKET	DD
Key Encryption Translate – ECB to CBC	CSNBKET / CSNEKET	DD

Access control points and callable services

Chapter 4. Update of z/OS Cryptographic Services ICSF Administrator's Guide, SC14-7506-04, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF Administrator's Guide*, SC14-7506-04, for the updates provided by this APAR. Refer to this source document if background information is needed.

Controlling who can use cryptographic keys and services

Setting up profiles in the CSFSERV general resource class

Table 10. Resource names for ICSF callable services

Resource name	Callable service names	Callable service description
CSFKET	CSNBKET CSNEKET	Key Encryption Translate

Callable services affected by key store policy

Table 11. Callable services and parameters affected by key store policy

ICSF callable service	31-bit name	Parameter checked
Key Encryption Translate	CSNBKET	KEK_key_identifier

Printed in USA