z/OS

Cryptographic Services Integrated Cryptographic Service Facility Updates to Reference Date Processing APAR OA49503

Contents

Chapter 1. Overview

This document describes changes to the Integrated Cryptographic Service Facility (ICSF) product related to reference date processing.

These changes are available through the application of the PTF for APAR OA49503 and apply to FMID HCR77B1, HCR77B0, and HCR77A1.

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

- *z/OS Cryptographic Services ICSF Administrator's Guide*, SC14-7506-04
- *z/OS Cryptographic Services ICSF System Programmer's Guide*, SC14-7507-04
- *z/OS Cryptographic Services ICSF Application Programmer's Guide*, SC14-7508-04

The technical changes made to the ICSF product by the application of the PTF for APAR OA49503 are indicated in this document by a vertical line to the left of the change.

Chapter 2. 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 1. Resource names for ICSF callable services

Resource name	Callable service names	Callable service description
CSFPRR2	CSNDKRR2 CSNFKRR2	PKDS Key Record Read2

Viewing and Changing System Status

Displaying installation exits

Table 2. Callable Service and its Exit Identifier

Service	Exit Identifier
PKDS Key Record Read2	**CSFPRR2**

Callable services affected by key store policy

Table 3. Callable services that are affected by the no duplicates key store policy controls

ICSF callable service	31-bit name	Parameter checked
PKDS Key Record Read2	CSNDKRR2	token

Callable services that trigger reference date processing

Table 4. Callable services and parameters that trigger reference date processing

ICSF callable service	31-bit name	Parameter checked
PKDS Key Record Read2	CSNDKRR2	label

Chapter 3. 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 5. Exit identifiers and exit invocations

Exit identifiers	**Exit invocations**
CSFPRR2	Gets control during the PKDS Key Record Read2 callable service.

Installation exits

Table 6. Services and their ICSF names

Service	*ICSF name*
PKDS Key Record Read2	**CSFPRR2**

Chapter 4. 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.

CKDS Key Record Read2 (CSNBKRR2 and CSNEKRR2)

Use this callable service to copy an internal fixed-length or variable-length AES, DES, or HMAC key token from the in-storage CKDS to application storage. Other cryptographic services can then use the copied key token directly.

The callable service name for AMODE(64) is CSNEKRR2.

Format

```
CALL CSNBKRR2(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             key_label,
             key_token_length,
             key_token )
```

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 0 or 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.

Table 7. Keywords for CKDS Key Record Read2 control information

Keyword	Meaning
Administrative rules (optional)	
ADMNREAD	The record is being read for administrative purposes. Reference date processing is bypassed. For more information, see the KDSREFDAYS option in *z/OS Cryptographic Services ICSF Administrator's Guide*. This keyword requires the application of the PTF for APAR OA49503 at ICSF FMID HCR77B1 and lower.

key_label

Direction	Type
Direction	String

The 64-byte label of a record in the CKDS to be retrieved.

key_token_length

Direction	Type
Input/Output	Integer

The length of the buffer for the output token. On input, the length of the buffer. The minimum length is 64 bytes and the maximum length is 725 bytes. On output, this parameter will be updated with the length of the token returned in the *key_token* parameter.

key_token

Direction	Type
Output	String

The buffer into which the return key token is written.

Required hardware

No cryptographic hardware is required by this callable service.

PKDS Key Record Read and PKDS Key Record Read2 (CSNDKRR or CSNDKRR2 and CSNFKRR or CSNFKRR2)

Use this callable service to copy a PKA key token or trusted block from the in-storage PKDS to application storage. Other cryptographic services can then use the copied key token directly.

Choosing between CSNDKRR and CSNDKRR2

CSNDKRR and CSNDKRR2 provide identical functions. When choosing which service to use, consider the following:

- CSNDKRR ignores the *rule_array_count* and *rule_array* parameters. The callable service name for AMODE(64) invocation is CSNFKRR.
- CSNDKRR2 processes the *rule_array_count* and *rule_array* parameters. The callable service name for AMODE(64) invocation is CSNFKRR2. This callable service requires the application of the PTF for APAR OA49503 at ICSF FMID HCR77B1 and lower.

Format

```
CALL CSNDKRR(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             label,
             token_length,
             token)
CALL CSNDKRR2(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             label,
             token_length,
             token)
```

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 indicates 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 are supplying in the *rule_array* parameter. This parameter is ignored for CSNDKRR/CSNFKRR. For CSNDKRR2/CSNFKRR2, the value can be 0 or 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. This parameter is ignored for CSNDKRR/CSNFKRR.

Table 8. Keywords for PKDS Key Record Read2 control information

Keyword	Meaning
Administrative rules (optional)	
ADMNREAD	The record is being read for administrative purposes. Reference date processing is bypassed. For more information, see the KDSREFDAYS option in *z/OS Cryptographic Services ICSF Administrator's Guide*.

label

Direction	Type
Input	String

The label of the record to be read. A 64 byte character string.

token_length

Direction	Type
Input/Output	Integer

The length of the area to which the record is to be returned. On successful completion of this service, *token_length* will contain the actual length of the record returned.

token

Direction	Type
Output	String

Area into which the returned record will be written. The area should be at least as long as the record.

Required hardware

No cryptographic hardware is required by this callable service.

PKDS Key Record Read and PKDS Key Record Read2

Printed in USA