z/OS

Cryptographic Services Integrated Cryptographic Service Facility CSFKDSL Label Filtering and Output Updates APAR OA52145

Contents

Chapter 1. Overview

This document describes changes to the Integrated Cryptographic Service Facility (ICSF) product to enable you to filter key labels by their key algorithm, use up to seven wild cards, and output label metadata all in one step.

These changes are available through the application of the PTF for APAR OA52145 and apply to FMID HCR77C0 and HCR77B1.

This document contains alterations to information previously presented in *z/OS Cryptographic Services ICSF Application Programmer's Guide*, SC14-7508-06.

The technical changes made to the ICSF product by the application of the PTF for APAR OA52145 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, SC14-7508-06, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF Application Programmer's Guide*, SC14-7508-06, for the new support for Key Data Set List (CSFKDSL and CSFKDSL6) provided by this APAR. Refer to this source document if background information is needed.

Key Data Set List (CSFKDSL and CSFKDSL6)

Use the key data set list callable service to generate a list or count of CKDS and PKDS labels or TKDS object handles. The list can be refined by search criteria for metadata or key algorithm. The list can display the key labels in addition to the metadata associated with each label.

The KDSR format of the key data sets (introduced in ICSF FMID HCR77A1) contains metadata that can be used for the search criteria. The older key data set formats have only the record create and update dates available. When the search criteria contains metadata that is not supported by the format of key data set, the service returns a return code 4 and does not generate a list or count. See "Coordinated KDS Administration callable service (CSFCRC and CSFCRC6)" to convert your key data sets to KDSR format.

For the CKDS and PKDS, the label is a character string up to 64 bytes long. Wild cards are allowed in the filter for labels. See the Usage Notes for information. The search criteria is applied to records that match the label filter.

For the TKDS, the name is the 32-byte name of a token. Wild cards are not allowed. The search criteria is applied to the objects of the token specified. Only PKCS #11 objects have metadata. While the token has a record in the TKDS, it does not have metadata.

Tokens in the TKDS cannot be listed by using this service. The token record list service is used to generate a list of tokens.

The callable service name for AMODE(64) is CSFKDSL6.

Format

```
CALL CSFKDSL (
              return_code,
              reason_code,
              exit_data_length,
              exit_data,
              rule_array_count,
              rule_array,
              label_filter_length,
              label_filter,
              search_criteria_length,
              search_criteria,
              label_count,
              output_list_length,
              output_list,
              reserved1_length,
```

```
reserved1,
reserved2_length,
reserved2,
continuation_area )
```

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
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. The value can be 3 or 4.

rule_array

Direction	Type
Input	Character

The *rule_array* parameter 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 1. Keywords for KDS list control information

Keyword	Meaning
Key data set (Required)	
CKDS	Specifies that the active CKDS is to be searched.
PKDS	Specifies that the active PKDS is to be searched.
TKDS	Specifies that the active TKDS is to be searched.
Key algorithm (Optional)	
DES	Specifies that DES key algorithms are to be added to the search criteria. Only valid with CKDS.
AES	Specifies that AES key algorithms are to be added to the search criteria. Only valid with CKDS.
PKA	Specifies that PKA key algorithms are to be added to the search criteria. Only valid with PKDS. Labels with either RSA or ECC key algorithms are returned.
Output format (Required)	
LABELS	Specifies that a list of labels that meet the search criteria is to be returned.
COUNT	Specifies that a count of labels that meet the search criteria is to be returned.
DETAILED	Specifies that a list of labels that meet the search criteria is to be returned along with the metadata associated with each label.
State of record (Required)	
ACTIVE	Specifies that only records that are not archived and within the start/end dates if specified are checked. If the start and end dates have not been set for a record, the record is considered active.
INACTIVE	Specifies that only records that are not archived and not within the start/end dates are checked.
ARCHIVED	Specifies that only records that have been archived are checked.
ALL	Specifies that all records are checked.

label_filter_length

Direction	Type
Input	Integer

The *label_filter_length* parameter specifies the length in bytes of the *label_filter* parameter.

For the CKDS and PKDS, the value can be between zero and 80 inclusive. When the length is zero, no filtering is used.

For the TKDS, the value must be 32.

label_filter

Direction	Type
Input	Character

The *label_filter* parameter contains the information that is used to filter on the key data set records by label or handle.

For the CKDS and PKDS, the filter is for the 64-byte label. Wild cards are allowed. Blank characters are not allowed. See the Usage Notes for details.

For the TKDS, the filter must be the 32-byte name of a token. Wild cards are not allowed. Trailing blanks are allowed. The search criteria is applied to the objects of the specified token.

search_criteria_length

Direction	Type
Input	Integer

The *search_criteria_length* parameter is the length in bytes of the *search_criteria* parameter. The value can be zero if no search criterion is to be applied. The maximum value is 500.

search_criteria

Direction	Type
Input	String

The *search_criteria* parameter is a list of search criterion to be applied to the search. The *search_criteria* is a block of entries in contiguous storage.

Each list entry identifies a single search criterion and any additional data. All of the criterion in the list is applied to each record matching the label filter in the key data set. Each entry in the list uses the structure that is shown in Table 2.

Table 2. Search criteria entry

Offset (Decimal)	Number of bytes	Description
0	2	Search criterion: **Value** **Meaning** **X'0001'** Criterion is for a date. **X'0002'** Criterion is a metadata tag. **X'0003'** Criterion is a TKDS object type. **X'0004'** Criterion is a CKDS key type. **X'0005'** Criterion is a metadata flag. **X'0006'** Criterion is an unsupported CCA key.
2	2	Length of structure. The length includes the search criterion and this length field.
4		Additional information (Required): • For dates, see Table 3 on page 7. • For metadata tag, see Table 4 on page 7. • For TKDS object type, see Table 5 on page 8. • For CKDS key type, see Table 6 on page 8. • For metadata flags, see Table 7 on page 10. • For unsupported CCA keys, see Table 8 on page 10.

- To use a date as a search criterion, select the date type you want to use, a comparison operator, and a date in YYYYMMDD format or binary zero. Binary zero means that the date has not been set.
- When searching for dates equal to zero, the record matches if the date is zero or the metadata block is not present. The date the record is archived or recalled is stored in a metadata block.
- When searching for dates being less than, or less than or equal to a non-zero date, the record matches only if there is a non-zero date for that type in the record.
- Searching for dates being less than or equal to zero are treated in the same manner as a request for dates equal to zero.

Table 3. Search criteria with date tag

Offset (Decimal)	Number of bytes	Value (Decimal)	Description
0	2	1	Search criterion is date.
2	2	14	Length of the entry.
4	1		Date type: **Value** **Date** **X'01'** Date the record was created. **X'02'** Date the record was last updated. **X'03'** Last date the record was referenced. **X'04'** Date the record was archived. **X'05'** Key material validity start date. **X'06'** Key material validity end date. **X'07'** Date the record was recalled.
5	1		Date comparison: **Value** **Meaning** **X'01'** Dates that are less than the specified date. **X'02'** Dates that are greater than the specified date. **X'03'** Dates that are equal to the specified date. **X'04'** Dates that are less than or equal to the specified date. **X'05'** Dates that are greater than or equal to the specified date.
6	8		Date in YYYYMMDD format (EBCDIC numeric characters) or binary zero.

To use a metadata tag as a search criterion, select a valid tag.

Table 4. Search criteria with metadata tag

Offset (Decimal)	Number of bytes	Value (Decimal)	Description
0	2	2	Search criterion is metadata tag.
2	2	6	Length of the entry.

Table 4. Search criteria with metadata tag (continued)

Offset (Decimal)	Number of bytes	Value (Decimal)	Description
4	2		Metadata tag: **Value** **Meaning** **X'0001'** Installation user data. **X'0002'** Service that referenced the record. **X'0003'** Record archive date. **X'0004'** Record recall date. **X'0005'** Key fingerprint. **X'0006'** Retained RSA key information. **X'0007'-X'7FFF'** Reserved for IBM use. **X'8000'-X'FFFF'** Installation metadata.

To use a TKDS object type as a search criterion, specify the type of objects required.

Table 5. Search criteria with TKDS object type

Offset (Decimal)	Number of bytes	Value (Decimal)	Description
0	2	3	Search criterion is TKDS object type.
2	2	5	Length of the entry.
4	1		Object type: **Value (EBCDIC)** **Meaning** **'T'** The key material of the object is in the clear. **'Y'** The key material of the object is wrapped by the EP11 master key.

To use a CKDS key type as a search criterion, specify the type of keys required.

Table 6. Search criteria with CKDS key type

Offset (Decimal)	Number of bytes	Value (Decimal)	Description
0	2	4	Search criterion is CKDS key type.
2	2	12	Length of the entry.

Table 6. Search criteria with CKDS key type (continued)

Offset (Decimal)	Number of bytes	Value (Decimal)	Description
4	8		CKDS key type in the label (bytes 65-72): **Value (EBCDIC)** **Meaning** **ADATA** DES ANSI X9.17 DATA keys. **AKEK** DES ANSI X9.17 key-encrypting keys. **CIPHER** AES CIPHER keys. **CV** Any of the following DES key types: CIPHER, CIPHERXI, CIPHERXL, CIPHERXO, CVARDEC, CVARENC, CVARPINE, CVARXCVL, CVARXCVR, DATAC, DATAM, DATAMV, DECIPHER, DKYGENKY, ENCIPHER, IKEYXLAT, KEYGENKY, OKEYXLAT, SECMSG. **DATA** AES and DES DATA keys (encrypted and clear). **DATAXLAT** DES data-translating keys. **DKYGENKY** AES DKYGENKY. **EXPORTER** AES and DES exporter keys. **IMPORTER** AES and DES importer keys. **IMP-PKA** DES limit authority importer keys. **IPINENC** DES input PIN encrypting keys. **MAC** AES, DES, and HMAC MAC keys. **MACD** DES double-length MAC key (DATAM). **MACVER** DES and HMAC MAC verification keys. **NULL** Records with no key material. **OPINENC** DES output PIN encrypting keys. **PINGEN** DES PIN generation keys. **PINCALC** AES PIN calculation keys. **PINPROT** AES PIN protection keys. **PINPRW** AES PIN reference value keys.

Table 6. Search criteria with CKDS key type (continued)

Offset (Decimal)	Number of bytes	Value (Decimal)	Description
4	8		**PINVER** DES PIN verification keys.

To use a metadata flag as a search criterion, specify the flag and value to be used.

Table 7. Search criteria with a metadata flag

Offset (Decimal)	Number of bytes	Value (Decimal)	Description
0	2	5	Search criterion is a metadata flag.
2	2	6	Length of the entry.
4	1	1	Flag type: **Value** **Date** **X'01'** Prohibit archive flag.
5	1		**Value (Decimal)** **State of the flag** **1** Enabled. **0** Disabled.

To use an unsupported CCA key as a search criterion, specify the type of keys required. Any number of bits can be set to 1.

- When bit 0 is set to 1 for the CKDS, all DES ANSI X9.17 keys are listed.
- When bit 1 is set to 1 for the CKDS, all DES DATAXLAT keys are listed.
- When bit 0 is set to 1 for the PKDS, all DSS keys are listed.

Table 8. Search criteria with an unsupported CCA key

Offset (Decimal)	Number of bytes	Value (Decimal)	Description
0	2	6	Search criterion is an unsupported CCA key.
2	2	5	Length of the entry.
4	1		Unsupported keys: **Bit** **Meaning** **0** CKDS: ANSI X9.17 keys PKDS: DSS keys **1** CKDS: DATAXLAT keys PKDS: Reserved **2-7** Reserved.

label_count

Direction	Type
Output	Integer

The number of labels or handles that are found that match the search criteria. The number of entries in the list in the *output_list* parameter when the LABEL keyword is specified in the rule array. This is the total number of matches found in the KDS when the COUNT keyword is specified in the rule array.

output_list_length

Direction	Type
Input/Output	Integer

The *output_list_length* parameter is the length in bytes of the *output_list* parameter. On input, the value is the size of the buffer for the output. On output, the value is the actual length of the data that is returned in the *output_list* parameter.

This parameter is ignored when the COUNT keyword is specified in the rule array.

output_list

Direction	Type
Output	Character

The output area for the list of labels or handles meeting the search criteria. When the output format rule array keyword is LABELS, the labels are returned in an array where each entry is a fixed length as follows:

- CKDS - 72 bytes
- PKDS - 64 bytes
- TKDS - 44 bytes

When the DETAILED rule is specified, the output area data is formatted as shown in Table 9 for both the CKDS and the PKDS.

Table 9. Output area data when DETAILED rule is specified

Offset (Decimal)	Number of bytes	Field name	Description
0	64	Key label	The label that is used to identify the key in the CKDS and PKDS.
64	8	Label type	Key type. Blank for the PKDS.
72	8	Key algorithm	Encrypting algorithm of the key. **Contained in the CKDS** DES/AES/HMAC. **Contained in the PKDS** RSA/ECC/DSS/TBLK. **When the key algorithm rule is not specified, DETAILED returns:** HMAC/DSS/TBLK. This field is left justified and padded with blanks after the value.
80	8	Creation date	Date of the key's creation, expressed as *YYYYMMDD*.

Table 9. Output area data when DETAILED rule is specified (continued)

Offset (Decimal)	Number of bytes	Field name	Description
88	8	Creation time	Time of the key's creation, expressed as Coordinated Universal Time (UTC) in the format *hhmmssth*.
96	8	Update date	Date that this key was last updated, expressed as *YYYYMMDD*.
104	8	Update time	Time that this key was last updated, expressed as Coordinated Universal Time (UTC) in the format *hhmmssth*.

The number of labels that are returned is determined by the *output_list_length* parameter and the length of the label by KDS. The *label_count* parameter contains the number of labels in this list.

If there is not enough room to fit all the labels, the return code is 4 and the reason code is 3033. The *continuation_area* is used to continue the list for subsequent calls.

This parameter is not returned when the COUNT keyword is specified in the rule array.

Note: The CKDS label consists of a 64-byte label and an 8-byte key type. The key type is used for key separation.

reserved1_length

Direction	Type
Input	Integer

This parameter is reserved. The value must be zero.

reserved1

Direction	Type
Input	String

This parameter is ignored.

reserved2_length

Direction	Type
Input	Integer

This parameter is reserved. The value must be zero.

reserved2

Direction	Type
Input	String

This parameter is ignored.

continuation_area

Direction	Type
Input/Output	String

This parameter is ignored when the COUNT keyword is specified in the rule array.

This is a 100-byte work area that the calling application must supply. The *continuation_area* is a work area that allows the service to be called multiple times to get the complete list of all labels that meet the search criteria.

For the first request, initialize this area to binary zero.

For subsequent requests, your application must not change the data in this string. The return code indicates whether the list is complete.

Usage Notes

SAF is invoked to verify that the caller is authorized to use this callable service. No checking is done of the CSFKEYS or CRYPTOZ profiles.

ICSF system keys in the CKDS will not be listed by this service.

Specifying the label filter for the CKDS and PKDS

A label can consist of up to 64 characters. The first character must be alphabetic or a national character (#, $, @). The remaining characters can be alphanumeric, a national character (#, $, @), or a period (.).

The *label_filter* parameter is a character string that can contain the following:

- Character strings containing valid characters for labels.
- Wild cards (* (asterisk)):
  - A wild card means 0 or more characters are to be ignored in the filtering process.
  - The number of characters to be ignored can be specified as *(*nn*), where *nn* is the number (1 –63) of characters to be ignored in the filtering process.
  - You can specify from 0 to 4 wild cards in the filter. When you do not have a wild card in the string, you are checking for the existence of the label in the key data set.
- Blanks are not allowed anywhere in the filter.

Examples:

***** All labels.

***ABC** All labels ending with ABC.

DEF All labels with DEF anywhere within the label.

GHI* All labels starting with GHI.

JKL*MNO
All labels starting with JKL and ending with MNO.

(20)PQR
All labels with PQR at character 21.

STU*(6)VWX*
All labels starting with STU and with VWX at character 10.

***(15)YZ1*234**
All labels with YZ1 at character 16 and ending with 234.

$5*6*7 All labels that start with $5, have a 6 anywhere in the label, and end with 7.

.APPL*.AES*.*.KEK*.*.
All labels that have APPL followed by anything, AES followed by anything, and KEK followed by anything after an initial prefix before APPL.

Examples of search criteria:

- Dates:
  - Using binary zero as a value to compare against allows a search to find records where a date field has not been set. If the search date is zero:

    Record creation date
    Cannot be zero.

    Record update date
    The record has not been updated.

    Key material validity start date
    The date was not set.

    Key material validity end date
    The date was not set.

    Last used reference date
    The record has not been used in a cryptographic operation.

    Record archive date
    If the record has been archived, the date cannot be zero. If the record has not been archived, the date is zero.

    Record recall date
    If the record has been recalled, the date cannot be zero. If the record has not been recalled, the date is zero.

Required hardware

No cryptographic hardware is required by this callable service.

Printed in USA