z/OS

APAR OA28439 (RACF)
RACF support for ICSF PKA Management Extensions

z/OS

APAR OA28439 (RACF)
RACF support for ICSF PKA Management Extensions

Contents

General information

This information applies to APAR OA28439 for RACF. This document also contains data areas changes for SAF APAR OA28437.

Part 1. Overview

Chapter 1. Overview

This document details the RACF support to enhance the ICSF segment for general resource profiles. This support is available on z/OS v1r8 and later supporting the new ICSF function being delivered in APAR OA28855.

The information within this document has been compiled from the separate manuals which make up the RACF library.

Chapter 2. Software

RACF support for PKA management extensions requires APAR OA28439 (RACF). This is in support of new ICSF function being delivered in APAR OA28855.

Part 2. Information updates

The chapters in this part supplement the following books:

Table 1. z/OS Security Server publication updates

Chapter	Supplements...
Chapter 3, “Security administrator considerations,” on page 9	*z/OS Security Server RACF Security Administrator’s Guide*
Chapter 4, “Command considerations,” on page 11	*z/OS Security Server RACF Command Language Reference*
Chapter 5, “Messages considerations,” on page 21	*z/OS Security Server RACF Messages and Codes*
Chapter 6, “RACROUTE considerations,” on page 23	*z/OS Security Server RACROUTE Macro Reference*
Chapter 7, “Data area considerations,” on page 25	*z/OS Security Server RACF Data Areas*
Chapter 8, “Macros and interface considerations,” on page 27	*z/OS Security Server RACF Macros and Interfaces*

Chapter 3. Security administrator considerations

This topic provides information for security administrators about the new ICSF segment. General resource profiles in the CSFKEYS, GCSFKEYS, XCSFKEY, and GXCSFKEY classes can now contain an ICSF segment to provide enhanced export control of ICSF symmetric and asymmetric keys.

The following information supplements *z/OS Security Server RACF Security Administrator's Guide*.

Updated information about field-level access checking

Use *field-level access checking* to control which ICSF segment fields can be accessed by users. To do this, create profiles in the FIELD class and permit users to the profiles.

The format of the profile name for FIELD class profiles that control ICSF segment fields is *class-name*.ICSF.*field-name*, where:

class-name
is one of the following classes:
- CSFKEYS
- GCSFKEYS
- XCSFKEY
- GXCSFKEY

field-name
is the name of the ICSF segment field that corresponds to the command operand that controls the field, as follows:

To control the use of these operands:	Specify this field name:
ASYMUSAGE and NOASYMUSAGE	CSFAUSE
SYMEXPORTABLE and NOSYMEXPORTABLE	CSFSEXP
SYMEXPORTCERTS and NOSYMEXPORTCERTS	CSFSCLBS
SYMEXPORTKEYS and NOSYMEXPORTKEYS	CSFSKLBS

Update information about the RACF database unload utility (IRRDBU00)

Member RACDBULD in SYS1.SAMPLIB creates a DB2® table for each type of RACF database record. The following DB2 tables are now created to support the new database record types.

Record type	Record name	DB2 table name
05G0	General Resource ICSF Data	GENR_ICSF_DATA
05G1	General Resource ICSF Key Label	GENR_ICSF_KEY_DATA
05G2	General Resource ICSF Certificate Identifier	GENR_ICSF_CERT_DATA

Chapter 4. Command considerations

This information supplements *z/OS Security Server RACF Command Language Reference*.

The following commands are updated:

RACDCERT GENCERT (Generate certificate)

The following updates are made to the authorization, syntax, and parameters of this command.

Authorization required

To issue the RACDCERT GENCERT command with the FROMICSF option, you must have the SPECIAL attribute and sufficient authority to the appropriate resource in the CSFKEYS class.

If your installation has established access control over ICSF services, you might also require READ authority to the CSFSERV class resource that controls the ICSF service called CSFPKX.

For details about ICSF authorities, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

Syntax

```
RACDCERT GENCERT[(request-data-set-name)]

[{PCICC[(pkds-label | * )]
        | ICSF[(pkds-label | * )]
        | DSA
        | FROMICSF(pkds-label)}]
```

Parameters

PCICC | ICSF | DSA | FROMICSF
Specifies if RACF should generate a new key pair, and if so, how to generate the key pair and where to store the private key for future use.

FROMICSF(*pkds-label*)
Specifies that no new key pair is to be generated for this new certificate. Instead, RACF uses an existing public key specified by its PKDS label. The public key must reside in the ICSF PKA key data set (PKDS).

When you specify FROMICSF, you must also specify SIGNWITH to sign the new certificate with an existing certificate. The new certificate will contain no private key and therefore cannot be self-signed.

You cannot specify both *request-data-set-name* and FROMICSF.

RALTER (Alter general resource profile)

The following updates are made to the syntax and parameter descriptions of this command.

Syntax

```
[subsystem-prefix]{RALTER | RALT}
          [ ICSF(
            [ ASYMUSAGE(
              [ HANDSHAKE | NOHANDSHAKE ]
              [ SECUREEXPORT | NOSECUREEXPORT ]
              ) ]
            [ SYMEXPORTABLE(BYANY | BYLIST | BYNONE) ]
            [ SYMEXPORTCERTS([qualifier]/label-name ... | *) ]
            [ SYMEXPORTKEYS(ICSF-key-label ... | *) ]
            ) ]
```

Parameters

ICSF | NOICSF

ICSF
Specifies ICSF attributes for the keys that are controlled by this profile. ICSF attributes are valid only for profiles in the CSFKEYS, GCSFKEYS, XCSFKEY, and GXCSFKEY classes.

ASYMUSAGE | NOASYMUSAGE

ASYMUSAGE
Specifies how an asymmetric key that is controlled by this profile is eligible to be used. If you do not specify ASYMUSAGE, the key is eligible for all uses.

SECUREEXPORT | NOSECUREEXPORT
Specifies whether the key is eligible to be used to export or import symmetric keys.

HANDSHAKE | NOHANDSHAKE
Specifies whether the key is eligible to be used to protect communication channels.

NOASYMUSAGE
Resets this option to the default setting. The key is eligible for all uses.

SYMEXPORTABLE | NOSYMEXPORTABLE

SYMEXPORTABLE
Specifies which public keys, if any, are eligible to be used to export a symmetric key that is controlled by this profile. If you do not specify SYMEXPORTABLE, any public key is eligible.

BYANY
Any public key is eligible. The SYMEXPORTCERTS and SYMEXPORTKEYS settings are ignored. This option is the default setting.

BYLIST
Only public keys specified with the SYMEXPORTCERTS or

SYMEXPORTKEYS option are eligible. If neither option is set for this symmetric key, no public key is eligible (as if BYNONE were specified).

BYNONE
No public key is eligible. The SYMEXPORTCERTS and SYMEXPORTKEYS settings are ignored.

NOSYMEXPORTABLE
Resets the SYMEXPORTABLE option to BYANY.

SYMEXPORTCERTS | NOSYMEXPORTCERTS

SYMEXPORTCERTS([*qualifier***]/***label-name ...* **| *)**
Specifies a list of the labels of digital certificates that are eligible to be used to export the symmetric keys controlled by this profile.

Each listed certificate must exist in the ICSF key store (the SAF key ring or PKCS #11 token specified by an ICSF configuration setting). For information about the ICSF key store, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

Specify an asterisk (*) to indicate that any certificate in the ICSF key store is eligible to be used to export the symmetric keys controlled by this profile. Specifying an asterisk (*) overrides any listed labels.

Specify each certificate label using a certificate label string in the form of *qualifier*/*label-name*.

qualifier
Specifies an optional qualifier in the certificate label string when multiple certificates have the same label. If specified, RACF translates the qualifier value to uppercase characters before storing it in the profile. The meaning of the qualifier value depends on where the certificate resides.

When the certificate resides in a ...	The qualifier value is ...
SAF key ring	The RACF user ID of the certificate owner.
PKCS #11 token	The value of the `CKA_ID` attribute of the certificate. The `CKA_ID` value consists of up to 64 hexadecimal characters. Valid characters are `0`–`9` and `A`–`F`.

/label-name
Specifies the certificate label assigned when the certificate was created. You must specify the forward slash character (/) followed by the certificate label.

If the certificate label contains blanks, or special characters that cause problems with TSO/E, such as the comma, parenthesis, or comment delimiter (/*), the entire certificate label string must be enclosed in single quotation marks.

Any leading or trailing blanks specified in *label-name* are removed from this value before storing it in the profile.

Examples of certificate label strings:

```
DENICE/CertForDenice
'ROGERS/Cert for Rogers'
```

```
'/DLR cert'
```

ADDSYMEXPORTCERTS([*qualifier***]/***label-name ...* **| *)**
Adds the specified certificate labels to the current list of labels.

DELSYMEXPORTCERTS([*qualifier***]/***label-name ...* **| *)**
Removes the specified certificate labels from the current list of labels.

NOSYMEXPORTCERTS
Removes the entire list of certificate labels.

SYMEXPORTKEYS | NOSYMEXPORTKEYS

SYMEXPORTKEYS(*ICSF-key-label ...* **| *)**
Specifies a list of the ICSF key labels of public keys that are eligible to be used to export the symmetric keys controlled by this profile. Each listed public key must reside in the ICSF PKA key data set (PKDS).

Specify an asterisk (*) to indicate that any public key in the ICSF PKDS is eligible to be used to export the symmetric keys controlled by this profile. Specifying an asterisk (*) overrides any listed labels.

ICSF-key-label
Specifies the ICSF key label for the public key. The label name cannot exceed 64 characters. The first character must be an alphabetic character or a national character (# , @ , or $). Subsequent characters can be a period character (.) or any alphanumeric or national character.

ADDSYMEXPORTKEYS(*ICSF-key-label ...* **| *)**
Adds the specified key labels to the current list of labels.

DELSYMEXPORTKEYS(*ICSF-key-label ...* **| *)**
Removes the specified key labels from the current list of labels.

NOSYMEXPORTKEYS
Removes the entire list of key labels.

NOICSF
Deletes the ICSF segment.

RDEFINE (Define general resource profile)

The following updates are made to the syntax and parameter descriptions of this command.

Syntax

```
[subsystem-prefix]{RDEFINE | RDEF}
        [ ICSF(
          [ ASYMUSAGE(
            [ HANDSHAKE | NOHANDSHAKE ]
            [ SECUREEXPORT | NOSECUREEXPORT ]
            ) ]
          [ SYMEXPORTABLE(BYANY | BYLIST | BYNONE) ]
          [ SYMEXPORTCERTS([qualifier]/label-name ... | *) ]
          [ SYMEXPORTKEYS(ICSF-key-label ... | *) ]
          ) ]
```

Parameters

ICSF
Specifies ICSF attributes for the keys that are controlled by this profile. ICSF attributes are valid only for profiles in the CSFKEYS, GCSFKEYS, XCSFKEY, and GXCSFKEY classes.

ASYMUSAGE
Specifies how an asymmetric key that is controlled by this profile is eligible to be used. If you do not specify ASYMUSAGE, the key is eligible for all uses.

SECUREEXPORT | NOSECUREEXPORT
Specifies whether the key is eligible to be used to export or import symmetric keys.

HANDSHAKE | NOHANDSHAKE
Specifies whether the key is eligible to be used to protect communication channels.

SYMEXPORTABLE
Specifies which public keys, if any, are eligible for use to export a symmetric key that is controlled by this profile. If you do not specify SYMEXPORTABLE, any public key is eligible.

BYANY
Any public key is eligible. The SYMEXPORTCERTS and SYMEXPORTKEYS settings are ignored. This option is the default setting.

BYLIST
Only public keys specified with the SYMEXPORTCERTS or SYMEXPORTKEYS option are eligible. If neither option is set for this symmetric key, no public key is eligible (as if BYNONE were specified).

BYNONE
No public key is eligible. The SYMEXPORTCERTS and SYMEXPORTKEYS settings are ignored.

SYMEXPORTCERTS([*qualifier***]/***label-name ...* **| *)**

Specifies a list of the labels of digital certificates that are eligible to be used to export the symmetric keys controlled by this profile.

Each listed certificate must exist in the ICSF key store (the SAF key ring or PKCS #11 token specified by an ICSF configuration setting). For information about the ICSF key store, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

Specify an asterisk (*) to indicate that any certificate in the ICSF key store is eligible to be used to export the symmetric keys controlled by this profile. Specifying an asterisk (*) overrides any listed labels.

Specify each certificate label using a certificate label string in the form of *qualifier*/*label-name*.

qualifier

Specifies an optional qualifier in the certificate label string when multiple certificates have the same label. If specified, RACF translates the qualifier value to uppercase characters before storing it in the profile. The meaning of the qualifier value depends on where the certificate resides.

When the certificate resides in a ...	The qualifier value is ...
SAF key ring	The RACF user ID of the certificate owner.
PKCS #11 token	The value of the `CKA_ID` attribute of the certificate. The `CKA_ID` value consists of up to 64 hexadecimal characters. Valid characters are `0`–`9` and `A`–`F`.

/label-name

Specifies the certificate label assigned when the certificate was created. You must specify the forward slash character (/) followed by the certificate label.

If the certificate label contains blanks, or special characters that cause problems with TSO/E, such as the comma, parenthesis, or comment delimiter (`/*`), the entire certificate label string must be enclosed in single quotation marks.

Any leading or trailing blanks specified in *label-name* are removed from this value before storing it in the profile.

Examples of certificate label strings:

```
DENICE/CertForDenice
'ROGERS/Cert for Rogers'
'/DLR cert'
```

SYMEXPORTKEYS(*ICSF-key-label ...* **| *)**

Specifies a list of the ICSF key labels of public keys that are eligible to be used to export the symmetric keys controlled by this profile. Each listed public key must reside in the ICSF PKA key data set (PKDS).

Specify an asterisk (*) to indicate that any public key in the ICSF PKDS is eligible to be used to export the symmetric keys controlled by this profile. Specifying an asterisk (*) overrides any listed labels.

ICSF-key-label

Specifies the ICSF key label for the public key. The label name cannot exceed 64 characters. The first character must be an alphabetic

character or a national character (# , @ , or $). Subsequent characters can be a period character (.) or any alphanumeric or national character.

RLIST (List general resource profile)

The following updates are made to the syntax and parameter descriptions of this command.

Syntax

```
[subsystem-prefix]{RLIST | RL}
                  [ ICSF ]
```

Parameters

ICSF
Specifies that ICSF segment information should be listed for profiles in the CSFKEYS, GCSFKEYS, XCSFKEY, or GXCSFKEY class.

Chapter 5. Messages considerations

This topic provides information about updated or changed messages. This information supplements *z/OS Security Server RACF Messages and Codes*.

New information:

IRRD190I Insufficient authorization to ICSF service *name*.

Explanation: The RACDCERT request could not be performed because there is insufficient authorization to the ICSF service identified by *name*.

System action: RACDCERT command processing ends.

Security Administrator Response: Grant the issuer authorization to the profile in the CSFSERV class that protects the identified service. An ICH408I message might have been issued to the security console identifying the profile and level of access that is required.

IRRD191I Insufficient authorization to ICSF key label.

Explanation: The RACDCERT request could not be performed because there is insufficient authorization to the PKDS label name specified by the issuer.

System action: RACDCERT command processing ends.

Security Administrator Response: Grant the issuer authorization to the profile in the class that protects the specified key label. The specified key label is a resource name covered by a profile in the CSFKEYS, GCSFKEYS, XCSFKEY, or GXCSFKEY class. An ICH408I message might have been issued to the security console identifying the profile and level of access that is required.

IRRD192I The specified key label does not exist.

Explanation: The RACDCERT request could not be performed because the specified label for the required public key in the ICSF PKDS does not exist.

System action: RACDCERT command processing ends.

User response: Reissue the command specifying a valid key label.

IRRD193I You cannot specify a request data set with the FROMICSF keyword. The certificate was not created.

Explanation: The RACDCERT GENCERT command was issued using an existing public key from the ICSF PKDS to define a certificate. A certificate cannot be defined if the RADCERT GENCERT command is issued when a request data set is specified.

System action: RACDCERT command processing ends.

User response: Reissue the command without specifying a request data set.

IRRD194I The key type that corresponds to this PKDS label is not supported.

Explanation: The RACDCERT GENCERT command was issued using an existing public key from the ICSF PKDS to define a certificate. However, the key type is not supported when using FROMICSF.

System action: RACDCERT command processing ends.

User response: Reissue the command specifying a valid key label.

IRRD195I The certificate cannot be generated. The PKDS label is already associated with the certificate contained in the profile identified in message IRRD196I.

Explanation: The PKDS label specified on the FROMICSF operand identifies a key that was created for use with an existing certificate. The certificate is identified by the profile name contained in message IRRD196I, which is displayed after this message.

System action: RACDCERT command processing ends.

User response: Reissue the command specifying a valid key label.

IRRD196I *profile-name*

Explanation: This message is used to display a DIGTCERT class profile name containing a digital certificate. The message that precedes this one provides the context under which the profile name is displayed.

System action: See the message that precedes this one.

User response: See the message that precedes this one.

Changed information:

IRRD130I The *keyword-name* keyword(s) must be specified. The request is not processed.

Explanation: The command that you issued required you to specify keyword *keyword-name*. The required keyword was not specified. For example, the RACDCERT EXPORT and RACDCERT GENREQ functions require a data set name (using the DSN keyword) and a label name (using the LABEL keyword). If either of these keywords is omitted, this message is issued.

The following conditions are additional reasons for the issuance of this message:

- Neither IDNFILTER nor SDNFILTER was specified with MAP. At least one of these keywords is required.
- MULTIID was specified for MAP without criteria.
- CRITERIA or NEWCRITERIA was specified with ID (or defaulting to ID). MULTIID is required.
- ICSF(*) or PCICC(*) was specified without WITHLABEL.
- A PKCS #12 certificate package data set was specified on ADD to replace an existing certificate where the public key has already been stored in ICSF. The PKCS #12 certificate package must be added to ICSF. So the ICSF or PCICC keyword is required.
- FROMICSF was specified for GENCERT without SIGNWITH.

System action: RACDCERT does not process the request.

User response: Specify the required keyword and reissue the command.

Chapter 6. RACROUTE considerations

The following fields have been added to the list for BRANCH=YES of RACROUTE REQUEST=EXTRACT:

- CSFAUSE
- CSFSEXP
- CSFSCLBS
- CSFSCLCT
- CSFSKLBS
- CSFSKLCT

,BRANCH=YES
,BRANCH=NO

specifies whether you want RACF® to use a branch entry.

The following applies to TYPE=EXTRACT with BRANCH=YES:

The RACROUTE REQUEST=EXTRACT macro supports an SRB-compatible branch entry when you specify BRANCH=YES and TYPE=ENCRYPT or BRANCH=YES and TYPE=EXTRACT with no change in function. with TYPE=EXTRACTN.

Cross memory mode is supported to obtain general resource profiles.

- General resource profiles that can be brought into storage are candidates for branch entry EXTRACT.
  - You can use the SETROPTS RACLIST command or RACROUTE REQUEST=LIST, GLOBAL=YES command to create a global listing of profiles in a data space. You can use this list only in the address space it was issued from.
  - You can also use RACROUTE REQUEST=LIST, GLOBAL=NO to create a listing of profiles in the user's address space, but this does not create a global listing of profiles.
- User data that is defaulted from the ACEE is a candidate for branch entry EXTRACT. This occurs when the USER class is specified or CLASS= is not specified, no ENTITY or ENTITYX is specified or ENTITYX is specified with zero for buffer length and zero for the actual entity name length, and no SEGMENT or FIELDS information is specified. The user's ID and default connect group are extracted from the current ACEE.

  If the user's primary and secondary languages are available, they are also extracted from the current ACEE, along with a code (U) indicating that the reported languages are defined in the user's profile. If the user's primary and secondary languages are not available in the user's profile, the installation default primary and secondary languages set by SETROPTS are returned, along with a code (S) indicating that the reported languages are the installation default.

  Additionally, if the user's work attributes (WORKATTR) information is available, it is also extracted from the ACEE. For the format of the WORKATTR information returned from the ACEE, see "RXTW: RACROUTE REQUEST=EXTRACT Result Area Mapping" in *z/OS Security Server RACF Data Areas*.
- RACF can extract the following fields of the general-resource profile:

NOT programming interface information

CATEGORY, IPLOOK, MEMCNT, MEMLST, and NUMCTGY. **Exception:** The MEMCNT and MEMLST fields of the SECLABEL profile are programming interfaces.

End of NOT programming interface information

ACL2, ACL2ACC, ACL2CNT, ACL2NAME, ACL2RSVD, ACL2UID, ACLCNT, APPLDATA, AUDIT, CONVSEC, CSFAUSE, CSFSEXP, CSFSCLBS, CSFSCLCT, CSFSKLBS, CSFSKLCT, GAUDIT, INSTDATA, KEYDATE, KEYINTVL, LEVEL, LOGDAYS, LOGTIME, LOGZONE, NOTIFY, OWNER, SECLABEL, SECLEVEL, SESSKEY, SLSFLAGS, UACC, USERACS, USERID, and WARNING.

- RACF searches RACLISTed profiles in the following order:
  - Those off the ACEE (if ACEE is specified),
  - Those off the TCB ACEE in the PRIMARY address space,
  - Those off the ASXB ACEE in the PRIMARY address space.

  If the profile is not found off any ACEE, RACF searches globally RACLISTed profiles.

To specify the BRANCH keyword, you must specify Release=1.9 or later.

Chapter 7. Data area considerations

This information supplements *z/OS Security Server RACF Data Areas*.

Information for data area ICHPISP is updated to support ICSF segment for general resource profiles:

ISP: RACF In-Storage Profile

Common name:
RACF in-storage profile

Macro ID:
ICHPISP

Size:

Section	Size
4	84 bytes

Offsets			Len	Name (Dim)	Description
Dec	Hex	Type			
0	(0)	STRUCTURE	84	RACRPE	RESOURCE PROFILE ELEMENT
80	(50)	SIGNED	2	RPECSFLN	ICSF SEGMENT INFO LENGTH
82	(52)	UNSIGNED	2	RPECSFOF	ICSF SEGMENT INFO OFFSET
84	(54)	CHARACTER		RPEEND	END OF FIXED PART OF ELEMENT

Offsets			Len	Name (Dim)	Description
Dec	Hex	Type			
0	(0)	CHARACTER	9	RPEICSF	ICSF segment data
0	(0)	UNSIGNED	1	RPEICEXP	Symmetric key export option
1	(1)	UNSIGNED	4	RPEICAUS	Asymmetric key usage options
5	(5)	UNSIGNED	2	RPEICOFF	Offset from RPEICSF to start of certificate label information at RPECLABS
7	(7)	UNSIGNED	2	RPEIKLCT	PKDS label count
9	(9)	CHARACTER	0	RPEIKLBS	Start of PKDS length/label pairs, mapped by RPEILABS

Offsets			Len	Name (Dim)	Description
Dec	Hex	Type			
0	(0)	CHARACTER	*	RPEILABS	Mapping for both PKDS and certificate length/label pairs
0	(0)	UNSIGNED	1	RPEILLN	Label length
1	(1)	CHARACTER	*	RPEILABE	PKDS or certificate label

Offsets			Len	Name (Dim)	Description
Dec	Hex	Type			
0	(0)	CHARACTER	*	RPECLABS	Certificate label information. This data starts immediately after the final PKDS label
0	(0)	UNSIGNED	2	RPEICLCT	Certificate label count
1	(1)	CHARACTER	*	RPEICLBS	Start of certificate length/label pairs, mapped by RPEILABS

Cross Reference

Name	Hex Offset	Hex Value	Level
RPECLABS	0		3
RPECSFLN	50		3
RPECSFOF	52		3
RPEICAUS	1		3
RPEICEXP	0		3
RPEICLBS	1		3
RPEICLCT	0		3
RPEICOFF	5		3
RPEIKLBS	9		3
RPEIKLCT	7		3
RPEILLN	0		3
RPEILABE	0		3
RPEILABS	0		3
RPEICSF	0		2

Chapter 8. Macros and interface considerations

This information supplements *z/OS Security Server RACF Macros and Interfaces*.

New information

General Resource ICSF record (05G0)

The General Resource ICSF record (05G0) defines the ICSF attributes associated with a general resource profile. There is one record per general resource/ICSF data combination:

Table 2. General Resource ICSF Record

		Position		
Field Name	**Type**	**Start**	**End**	**Comments**
GRCSF_RECORD_TYPE	Int	1	4	Record type of the general resource ICSF record (05G0).
GRCSF_NAME	Char	6	251	General resource name as taken from the profile name.
GRCSF_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs .
GRCSF_EXPORTABLE	Char	262	273	Is the symmetric key exportable? Valid values are: BYNONE, BYLIST, and BYANY.
GRCSF_USAGE	Char	275	529	Allowable uses of the asymmetric key. Valid values are: HANDSHAKE, NOHANDSHAKE, SECUREEXPORT, and NOSECUREEXPORT.

General Resource ICSF key label record (05G1)

The General Resource ICSF key label record (05G1) defines the PKDS key labels associated with an ICSF general resource. There is one record per general resource/ICSF key label combination.

Table 3. General Resource ICSF key label Record

		Position		
Field Name	**Type**	**Start**	**End**	**Comments**
GRCSFK_RECORD_TYPE	Int	1	4	Record type of the general resource ICSF key label record (05G1).
GRCSFK_NAME	Char	6	251	General resource name as taken from the profile name.
GRCSFK_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
GRCSFK_LABEL	Char	262	325	ICSF key label of a public key that can be used to export this symmetric key.

General Resource ICSF certificate identifier record (05G2)

The General Resource ICSF certificate identifier record (05G2) defines the certificates associated with an ICSF general resource. There is one record per general resource/certificate combination.

Table 4. General Resource ICSF certificate identifier Record

Field Name	Type	Position		Comments
		Start	End	
GRCSFC_RECORD_TYPE	Int	1	4	Record type of the general resource ICSF certificate identifier record (05G2).
GRCSFC_NAME	Char	6	251	General resource name as taken from the profile name.
GRCSFC_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
GRCSFC_LABEL	Char	262	358	Certificate identifier of a public key that can be used to export this symmetric key.

Changed information

In "Table of data type 6 command-related data", of "Chapter 5. SMF Records", the FROMICSF keyword has been added to byte 3 of the RACDCERT command, event code 66(42):

Event code dec(hex)	Command	Data length	Format	Description
66(42)	**RACDCERT**	4	Binary	Flags for keywords specified: **Bit** **Keyword specified** **Byte 0** **0** ADD **1** ALTER **2** DELETE **3** CONNECT **4** REMOVE **5** SITE **6** CERTAUTH **7** ICSF **Byte 1** **0** TRUST **1** NOTRUST **2** ADDRING **3** DELRING **4** USAGE(PERSONAL) **5** USAGE(SITE) **6** USAGE(CERTAUTH) **7** DEFAULT **Byte 2** **0** CONNECT(SITE) **1** CONNECT(CERTAUTH) **2** GENCERT **3** EXPORT **4** GENREQ **5** SIGNWITH(CERTAUTH... specified **6** SIGNWITH(SITE... specified **7** PASSWORD **Byte 3** **0** MAP **1** ALTMAP **2** DELMAP **3** MULTIID **4** HIGHTRUST **5** PCICC **6** DSA **7** FROMICSF
		8	EBCDIC	User ID (from ID keyword on RACDCERT)
		44	EBCDIC	Data set name
		32	EBCDIC	Label name
		8	EBCDIC	User ID (from ID sub-keyword)
		32	EBCDIC	WITHLABEL
		4	Binary	SIZE
		10	EBCDIC	NOTBEFORE(date) in the format yyyy/mm/dd
		8	EBCDIC	NOTBEFORE(time) in the format hh:mm:ss
		10	EBCDIC	NOTAFTER(date) in the format yyyy/mm/dd
		8	EBCDIC	NOTAFTER(time) in the format hh:mm:ss
		1	Binary	FORMAT **X'01'** CERTB64 **X'02'** CERTDER **X'03'** PKCS12B64 **X'04'** PKCS12DER **X'05'** PKCS7B64 **X'06'** PKCS7DER

Event code dec(hex)	Command	Data length	Format	Description
66(42) (Cont.)	**RACDCERT** (Cont.)	4	Binary	More flags for keywords specified: **Bit** **Keyword specified** **Byte 0** **0** ALTIP **1** ALTEMAIL **2** ALTDOMAIN **3** ALTURI **4** KUHANDSHAKE **5** KUDATAENCR **6** KUDOCSIGN **7** KUCERTSIGN **Byte 1** **0** REKEY **1** ROLLOVER **2** FORCE **3** ADDTOKEN **4** DELTOKEN **5** BIND **6** UNBIND **7** IMPORT **Byte 2** **0–7** Reserved for IBM's use **Byte 3** **0–7** Reserved for IBM's use
		4	Binary	SEQNUM

Updates to the RACF database templates

Template Field name (character data)	Field ID	Flag 1	Flag 2	Field length decimal	Default value	Type	Field being described
The following is the ICSF segment of the GENERAL template.							
ICSF	01	00	00	00000000	00		Start of segment fields for defining ICSF attributes
CSFSEXP	02	00	00	00000001	00	Bin	Symmetric key export option: **Value** **Meaning** **X'80'** BYLIST **X'40'** BYNONE **X'00'** BYANY
CSFSKLCT	03	10	00	00000004	00	Int	Count of PKDS labels
CSFSKLBS	04	80	00	00000000	00	Char	PKDS labels that might be used to export this symmetric key
CSFSCLCT	05	10	00	00000004	0	Int	Count of certificate labels
CSFSCLBS	06	80	00	00000000	00	Char	Certificate labels that might be used to export this symmetric key
CSFAUSE	07	00	00	00000004	55	Bin	Asymmetric key usage. In byte 3: **Value** **Meaning** **X'08'** NOSECUREEXPORT **X'04'** SECUREEXPORT **X'02'** NOHANDSHAKE **X'01'** HANDSHAKE

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

DB2
IBM
ICSF
MVS
RACF
z/OS
zSeries

Other company, product, and service names may be trademarks or service marks of others.

Program Number:

Printed in USA