Updates for SA23-2292 z/OS Security Server RACF Command Language Reference

RALTER command.

The ENCRYPTKEY keyword is added to the SSIGNON segment to request conversion of a PassTicket key to a KEYENCRYPTED key with a key label.

The KEYLABEL keyword is added to the SSIGNON segment to specify use of a key which exists in the ICSF CKDS which was not created by RACF.

...

[SSIGNON(

[KEYMASKED(key-value)

| KEYENCRYPTED(key-value)

| ENCRYPTKEY

| KEYLABEL(label-value)]

)

| NOSSIGNON]

…

Note, the KEYMASKED, KEYENCRYPTED, ENCRYPTKEY and KEYLABEL keywords all work against the same field in the RACF database. Use of any of these RALTER keywords replaces the previous PassTicket key (or its label) in the RACF database.

ENCRYPTKEY

If the existing key is KEYMASKED, it is converted to a KEYENCRYPTED key and the data in the RACF database is replaced with the ICSF key label. Knowledge of the existing key value is not necessary.

If the existing key is KEYENCRYPTED in the form of a key token, it is moved into the ICSF CKDS and data in the RACF database is replaced with a key label. Knowledge of the existing key value is not necessary.

If the existing key is KEYENCRYPTED and already referenced by a key label, message **IRR52254I** is issued and ENCRYPTKEY is ignored.

RACF generates key label names in the form IRR.SSIGNON.*sysname.mmddyyyy.hhmmss.nnnnnn.* The key label name is not user configurable. RLIST has been updated in this apar to display the key label name. *Sysname* indicates the name of the system on which the ENCRYPTKEY operation was

performed.

Before using ENCRYPTKEY, please understand ALL of the following:

There is no way to revert back to a masked key after using ENCRYPTKEY, other than by redefining the key using KEYMASKED which requires knowledge and re-specification of the key value.

There is no way to revert back to an ICSF key token

Your RACF database will contain a key token if creation of a key label failed. Creation of the key label could have failed due to the defect described by apar OA56729, or due to lack of authorization to ICSF services or keys at the time the KEYENCRYPTED(xx) keyword was specified.

ICSF key tokens which are stored in the RACF database are usable in environments where the ICSF CKDS is not shared, as long as all systems sharing the RACF database have the same master key. Key tokens are no less secure than key labels. The advantage of key tokens stored in the ICSF CKDS, referenced by key labels, is that ICSF re-enciphers them automatically when the master key changes.

If a key token is stored in the RACF database instead of a key label, RACF updates the key token when a master key change is detected. RACF only updates a key token when it is used in a PassTicket operation. If the master key is changed twice between use of a specific key token, the key token is rendered unusable.

The user specifying ENCRYPTKEY requires READ access to the CSFCKI, CSFKRC and CSFKRW services via profiles in the CSFSERV class. READ access to CSFKRD is optional, and is only used to clean up in the event an error occurs in CSFKRW.

The user specifying ENCRYPTKEY requires READ access to keys in the form *IRR.SSIGNON.sysname.** using profiles in the CSFKEYS class. *Sysname* is the name of the system where the ENCRYPTKEY keyword was specified.

Use of ENCRYPTKEY requires that ICSF be installed and active at the time the ENCRYPTKEY keyword is used.

When sharing the RACF database, please understand ALL of the following:

If the RACF database is shared between systems which do not also share the ICSF CKDS and master key, PassTickets modified using ENCRYPTKEY will no longer work on any systems other than the system on which ENCRYPTKEY was issued because RACF is unable to add the key to the CKDS on the other systems.

ICSF services must be used to export the key, using its key label, from the system on which ENCRYPTKEY was issued to the ICSF CKDS of all other systems which share the RACF database. The same key label must be used on all systems.

The key label which is displayed when using the RLIST command to view the profile in the PTKTDATA class contains the system name of the system on which ENCRYPTKEY was originally specified.

The ICSF CSNDSYX and CSNDSYI services can be used to export and import PassTicket keys from the ICSF CKDS. The ICSF CSNBKEX and CSNBKIM services

can also be used to export and import PassTicket keys from the ICSF CKDS.

Ensure you are able to copy keys from one ICSF CKDS to the others BEFORE using the ENCRYPTKEY keyword.

KEYLABEL(label value)

Specifies the name of an ICSF key label to be used when generating or evaluating a PassTicket. ICSF must be installed and active, and the key must be defined in the ICSF CKDS at the time of use. However, this is not checked when the KEYLABEL keyword is specified.

When using KEYLABEL, RACF does not make any calls to ICSF. The key label is saved in the RACF database, and it is up to the installation to ensure that the key is added to the ICSF CKDS before any PassTicket operations occur which need it. The key must refer to a DES key with a type of DATA with length of 8 bytes.

Note: The KEYLABEL(x) operand cannot be used to override the key label generated by RACF when KEYENCRYPTED() or ENCRYPTKEY is specified.

RDEFINE command

The KEYLABEL keyword is added to the SSIGNON segment to specify use of a key which exists in the ICSF CKDS which was not created by RACF.

...

[SSIGNON(

[KEYMASKED(key-value)

| KEYENCRYPTED(key-value)

| KEYLABEL(label-value)]

)

| NOSSIGNON]

…

KEYLABEL(x)

Specifies the name of an ICSF key label to be used when generating or evaluating a PassTicket. ICSF must be installed and active, and the key must be defined in the ICSF CKDS at the time of use. However, this is not checked when the KEYLABEL keyword is specified.

When using KEYLABEL, RACF does not make any calls to ICSF. The key label is saved in the RACF database, and it is up to the installation to ensure that the key is added to the CKDS before any PassTicket operations occur which need it. The key must refer to a DES key with a type of DATA.

Note: The KEYLABEL(x) operand cannot be used to override the key label generated by RACF when KEYENCRYPTED() is specified.

RLIST command

The RLIST command is enhanced to provide more information about the nature of encrypted keys in the SSIGNON segment.

When the SSIGNON segment contains a PassTicket key, RLIST displays:

```
SSIGNON INFORMATION
-------------------
```

When a masked key exists, the following will be displayed:

```
KEYMASKED DATA NOT DISPLAYABLE
```

When a key token exists, the following will be displayed:

```
KEYTOKEN DATA NOT DISPLAYABLE
```

And when a key label exists, the following (for example) will be displayed:

```
KEYENCRYPTED LABEL: IRR.SSIGNON.SY1.07192018.185056.915782
```

z/OS Security Server RACF Messages and Codes SA23-2291

IRR52140I – deleted...

IRR52141I Mutually exclusive keywords specified in the SSIGNON segment. Command processing is terminated.

Explanation: You specified some combination of the KEYMASKED, KEYENCRYPTED, KEYLABEL, and ENCRYPTKEY suboperands, which are mutually exclusive. You can specify only one operand at a time.

System action: Command processing stops.

User response: Reenter the command with only one of the suboperands.

IRR52142I The *operand* sub-operand was specified but RACF was unable to load cryptocraphic module *module*. Reason code is *code*. Command Processing is terminated.

Explanation: RACF failed to load ICSF module *module*. The z/OS LOAD macro returned *code*.

System action: Command processing stops.

User response: Use the return *code* from z/OS LOAD to determine why RACF was unable to load *module*. Fix the problem and try the command again. Or contact IBM support.

IRR52251I Cryptographic service *service-name* failed with return code *rc*, reason code *rsn*. Command processing is terminated.

Explanation: An unexpected error was encountered when calling the cryptographic service *service-name*. The return and reason codes are displayed.

System action: If the failing *service-name* is something other than CSNBCKI, the command was partially successful and an ICSF key token is saved in the RACF database. If the failing *service-name* is CSNBCKI, the command stops.

User response: Using the documentation for the *service-name*, try to determine if the error is caused by an ICSF setup problem. Otherwise, contact IBM. Once the problem has been corrected, retry the command.

IRR52252I An incorrect value was specified for the ENCRYPTKEY operand. Command processing is terminated.

Explanation: You specified an incorrect suboperand of the ENCRYPTKEY operand.

System action: Command processing stops.

User response: Remove or correct the value and issue the command again.

IRR52253I A valid key was not found in the *profile-name* profile in the *class-name* class. Diagnostic code is *diag-code*. Command processing is terminated.

Explanation: You specified the ENCRYPTKEY operand to encrypt the secured signon key contained in the profile named *profile-name* in the *class-name* class. However, the format of the of the data in the key field (SSKEY) is not recognized by RACF. The key is unusable.

System action: Command processing stops.

User response: If diag-code is 1 or 5, then there is no key in the profile. Assign a new key using the KEYENCRYPTED or KEYLABEL keyword. For other values of diag-code, you can either assign a new value to replace the unusable key or contact IBM to try to determine how the data became corrupted.

IRR52254I The encrypted key found in the *profile-name* profile in the *class-name* class cannot be further encrypted using ENCRYPTKEY. Command processing is terminated.

Explanation: You specified the ENCRYPTKEY operand to encrypt the secured signon key contained in the profile named *profile-name* in the *class-name* class. However, the key is already encrypted and saved in the ICSF CKDS. No further processing is possible for this key.

System action: Command processing stops.

User response: None.

IRR52255I Only one profile may be specified when specifying the ENCRYPTKEY operand. Command processing is terminated.

Explanation: You specified the ENCRYPTKEY operand to encrypt a secured signon key. However, multiple profile names were specified on the RALTER command. This is not allowed when specifying ENCRYPTKEY.

System action: Command processing stops.

User response: Split the command into several commands, each of which specify a single profile name.