z/OS

Security Server RACF
APAR OA30560
Support for long distinguished names

Preface

This information applies to APAR OA30560 (RACF).

Overview

APAR OA30560 enhances RACF support for digital certificates in the following ways:

- The RACDCERT ADD and RACDCERT GENCERT commands now support certificates with long distinguished names.
- RACF callable services `R_datalib` and `initACEE` now support certificates with long distinguished names.
- The RACDCERT MAP command now supports IDNFILTER and SDNFILTER values of up to 1024 characters.

With APAR OA30560, RACF changes the way that certificate profile names in the DIGTCERT class are formed and stored in the RACF database.

APAR OA30560 also enhances PKI Services support for digital certificates with APAR OA30952 (PKI). When both OA30560 and OA30952 are installed, PKI Services can generate certificates with long distinguished names.

Software requirements

Support for APAR OA30560 requires one of the following software releases:

- z/OS Security Server RACF Version 1 Release 10 (FMID HRF7750)
- z/OS Security Server RACF Version 1 Release 11 (FMID HRF7760)

Updated RACF publications

The chapters of this document supplement the V1R10 and V1R11 levels of the following RACF publications:

Chapter	Supplements ...
Chapter 1, "Security administration updates," on page 1	*z/OS Security Server RACF Security Administrator's Guide*
Chapter 2, "Command updates," on page 3	*z/OS Security Server RACF Command Language Reference*
Chapter 3, "System programming updates," on page 5	*z/OS Security Server RACF System Programmer's Guide*
Chapter 4, "Messages updates," on page 7	*z/OS Security Server RACF Messages and Codes*
Chapter 5, "RACROUTE macro updates," on page 9	*z/OS Security Server RACROUTE Macro Reference*

Chapter 1. Security administration updates

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

The following topic is added to the chapter called "RACF and digital certificates".

DIGTCERT profile names

The name of a DIGTCERT profile is derived from the certificate's serial number and the issuer's distinguished name (IDN). Any character in either value that would not be valid in a RACF profile name, such as a blank, is replaced with the X'4A' (¢) character.

The format of the profile name is based on the combined length of those values, including the period.

When the combined length of the value of *serial-number.issuer's-distinguished-name* is 246 characters or less, the name of the DIGTCERT profile uses the following format:

serial-number.issuer's-distinguished-name

Example: If the certificate's serial number is `41D87A3B05DE6FBD466C2069661E3872` and the issuer's distinguished name is `OU=VeriSign Class1.O=VeriSign.L=Internet`, the profile name of the DIGTCERT profile is as follows:

```
41D87A3B05DE6FBD466C2069661E3872.OU=VeriSign¢Class1.O=VeriSign.L=Internet
```

When the combined length of the value of *serial-number.issuer's-distinguished-name* exceeds 246 characters, the name of the DIGTCERT profile uses the following format, where the *certificate-hash* value is a hexadecimal representation of the certificate in a hashed form:

serial-number.first-portion-of-IDN.certificate-hash.last-portion-of-IDN

Example: If the certificate's serial number is `0E` and the issuer's distinguished name is as follows, the resulting profile name is as shown:

Issuer's distinguished name:

```
CN=Entrust Certification Authority - L1B.OU=(c) 2008 Entrust,Inc
..OU=www.entrust.net/CPS is incorporated by reference.OU=CPS CON
TAINS IMPORTANT LIMITATIONS OF WARRANTIES AND LIABILITY.OU=AND A
DDITIONAL TERMS GOVERNING USE AND RELIANCE.OU=Entrust,Inc.C=US
```

DIGTCERT profile name:

```
0E.CN:Entrust Certification Authority - L1B.OU:(c) 2008 Entrust,
Inc..OU:www.entrust.net/CPS i de9f2c7fd25e1b3afad3e85a0bd17d9b10
0db4b32fd4e1c67a2d28fced849ee1 ES AND LIABILITY.OU:AND ADDITIONA
L TERMS GOVERNING USE AND RELIANCE.OU:Entrust,Inc.C:US
```

When a DIGTCERT profile name contains a certificate hash value, each occurrence of the equal sign (`=`) delimiter is replaced with a colon (`:`).

Chapter 2. Command updates

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

Longer values for distinguished names

The maximum length of the following operand values is increased to 1024 bytes:

Command	Operand
RACDCERT GENCERT	SUBJECTSDN
RACDCERT MAP	IDNFILTER
	SDNFILTER

Updated information about the RACDCERT ADD command

The following topic is added to the description of the RACDCERT ADD command.

Details about DIGTCERT profile names

The name of a DIGTCERT profile is derived from the certificate's serial number and the issuer's distinguished name (IDN). Any character in either value that would not be valid in a RACF profile name, such as a blank, is replaced with the ¢ character (X'4A').

The maximum length of a DIGTCERT profile name is 246 characters. The format of the profile name is based on the combined length of the certificate's serial number and the issuer's distinguished name (IDN), including the period.

When the combined length of the value of *serial-number.issuer's-distinguished-name* is 246 characters or less, the name of the DIGTCERT profile uses the following format:

```
serial-number.issuer's-distinguished-name
```

When the combined length of the value of *serial-number.issuer's-distinguished-name* exceeds 246 characters, the name of the DIGTCERT profile uses the following format, where the *certificate-hash* value is a hexadecimal representation of the certificate in a hashed form:

```
serial-number.<first-portion-of-IDN><certificate-hash><last-portion-of-IDN>
```

When a DIGTCERT profile name contains a certificate hash value, each occurrence of the equal sign (=) delimiter is replaced with a colon (:).

New restriction for the ISSUERSDN operand

The ISSUERSDN keyword is not supported for lengthy issuer's distinguished names when the name of the certificate's DIGTCERT profile contains a certificate hash value. This restriction applies to the following commands:

- RACDCERT ALTER
- RACDCERT DELETE
- RACDCERT LIST

Chapter 3. System programming updates

This information supplements *z/OS Security Server RACF System Programmer's Guide*.

Updated information about using exits to control shared user IDs

You can use the following exits to check the X500 name (ACEEX5PR) to determine which accesses and privileges a shared user ID should have.

- RACROUTE REQUEST=AUTH preprocessing exit (ICHRCX01)
- RACROUTE REQUEST=FASTAUTH preprocessing exits (ICHRFX01 and ICHRFX03)

The following information about these exits is added in "Chapter 8. RACF installation exits".

The X500 name helps to identify the user of a shared user ID in the cases where a security context (ACEE) was created from a certificate through certificate name filtering or hostid mapping. The X500 name is meaningful for auditing purposes only.

Chapter 4. Messages updates

This information supplements *z/OS Security Server RACF Messages and Codes*.

IRRD108I The certificate does not meet RACF requirements and cannot be used.

Explanation: The certificate being added may be valid, but, RACF® cannot use it for one of the following reasons:

- The issuer's distinguished name is too long. RACF is trying to use the hash algorithm used in the certificate signature to create a DIGTCERT profile name that fits the maximum length of 246, but the hash algorithm is unknown to RACF.
- The combined length of the serial number and issuer's distinguished name is too long to create a DIGTCERT profile name. The combined length should not exceed the maximum length of 246 for a profile name.
- The certificate contains critical extensions that RACF does not recognize.
- The certificate version is greater than 3.

System action: RACDCERT command processing ends.

User response: The digital certificate found in the data set cannot be used by RACF. If you have more than one certificate, be sure that the correct one was placed in the data set. Otherwise, you need to obtain a new certificate containing information that meets RACF requirements. If you cannot obtain another certificate, contact your system programmer.

System programmer response: Check that the certificate being used has been issued by the intended certifying authority. If necessary, report the problem to the IBM® support center.

IRRD109I The certificate cannot be added. Profile *profile-name* is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Use RACDCERT CHECKCERT to determine if the digital certificate is defined for the correct user. A certificate can only exist for one user. You can perform one of the followings actions:

- To add the certificate to a different user perform the following steps:
  1. Use RACDCERT EXPORT to export the certificate and its private key, if any, to a data set.
  2. Use RACDCERT DELETE to delete the certificate.
  3. Issue the RACDCERT ADD command for the correct user.
- To replace the existing certificate, which is typically a self-signed certificate, with a signed copy from your Certificate Authority, or to replace the existing certificate with a renewed version, issue the RACDCERT ADD command for the correct user.
- To enable multiple users to use the same certificate for different applications or servers, you must use a key ring. Using a key ring prevents the need to add the same certificate again. See the chapter on RACF digital certificates in *z/OS Security Server RACF Security Administrator's Guide* for further details.

IRRD203I Subject's name exceeds the maximum allowed (1024 characters).

Explanation: A user is attempting to perform one of the following tasks:

1. Request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions.
2. Preregister a client for a PKI Services digital certificate using the R_PKIServ callable service PREREGISTER.
3. Modify an existing certificate request using the R_PKIServ callable service MODIFYREQS function.

However, the subject's name value provided is too long.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: Reduce the length of the name information for the request such as common name, title, and so on, or contact your system programmer or web page administrator.

Application Programmer Response: Modify the application invoking the R_PKIServ callable service to provide less name information.

Web Page Administrator Response: If R_PKIServ is being invoked from the PKI Services CGIs, modify the certificate template definition in the pkiserv.tmpl file to provide less name information in the <CONSTANT> section.

Chapter 5. RACROUTE macro updates

This information supplements *z/OS Security Server RACROUTE Macro Reference*.

Update to RACROUTE REQUEST=VERIFY

The description of the X500NAME parameter in Chapter 3, "System Macros" is updated as follows.

X500NAME=X500 *name pair addr*
specifies the data structure that contains the X.500 name pair associated with this security environment. Before using the name pair, you need to obtain it from the digital certificate associated with the user ID. You can use the initACEE query function for this task. The name pair must contain both the issuer's name and the subject's name from the certificate.

The X500NAME parameter is valid only for the ENVIR=CREATE function of a REQUEST=VERIFY request. However, the ENVIR=CREATE function ignores the parameter or uses a different name pair in certain circumstances:

- The parameter is ignored if both the ENVRIN parameter and SYSTEM=YES are specified.
- When creating an ACEE from an ENVR object, the ENVR object might already contain an X.500 name pair, which is used.
- If a RACROUTE REQUEST=VERIFY, ENVIR=CREATE creates an ACEE for an undefined user, the X500NAME parameter is ignored.
- If the RACROUTE REQUEST=VERIFY request creates an ACEE for a RACF defined user, the ACEE points to a copy of the X.500 name pair structure in the same subpool as the ACEE. This X.500 name is used in auditing.

When an A-type or RX-type notation is used, *name pair addr* specifies the field name of the data structure. When register notation is used, it specifies the register containing the address of the data structure.

When specifying X500NAME=, you must also specify RELEASE=7705 or later. The data structure of the X.500 name pair is shown in Table 1.

Table 1. Description of X500NAME data structure

Offset	Length (bytes)	Description
0	4	Length of entire X.500 name pair data structure
4	2	Length of issuer's name (1–255)
6	2	Length of subject's name (1–255)
8	1–255	Up to 255 characters of the issuer's distinguished name. Will be truncated if longer.
*	1–255	Up to 255 characters of the subject's distinguished name. Will be truncated if longer.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

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