Creating and Renewing Digital Certificates on z/OS

Chelsea Isaac
Technical Specialist
chelsea.t.jean-mary@ibm.com

Background

This presentation will guide users on how to create and renew digital certificates on z/OS. The steps are organized into the following sections:

Part 1: Create a certificate

- Generate a placeholder certificate
- Download and install the certificates
- Submit certificate request to CA

Part 2: Rekey and rollover a certificate

- Create a certificate request
- Submit certificate request to CA
- Rekey and rollover certificate

Before you start, you must ensure that you have ftp installed on your computer. You should also obtain the instructions for submitting certificates to your organization’s Certificate Authority.

Part 1: Create a Certificate

Generate a placeholder certificate

Generate a placeholder certificate

There are four ways to generate a certificate:

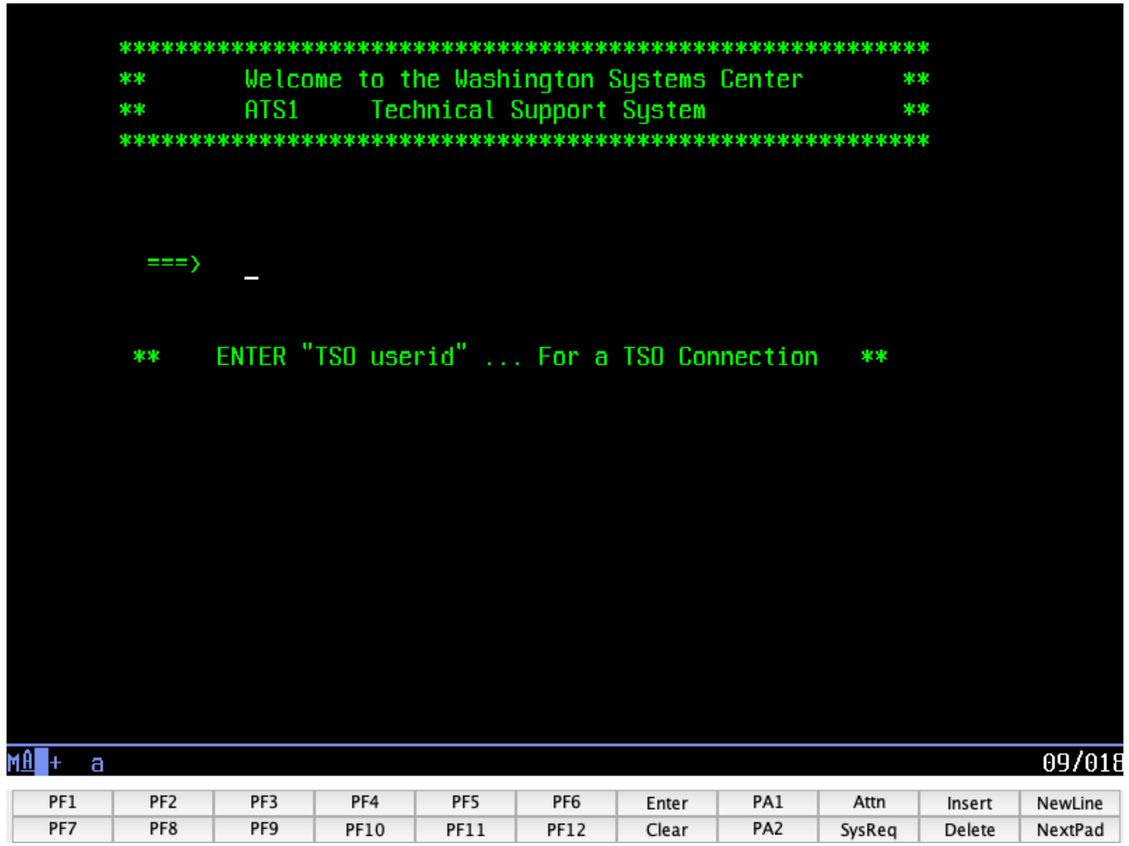
1) RACDCERT commands
2) RACF panels
3) z/OSMF
4) JCL

We'll use the first option.

Generate a placeholder certificate

1. Open PCOMM, tn3270 X, or some TN3270 emulator.

Log into your system.



Generate a placeholder certificate

2. Search for the owner of the application that will use the certificate on SDSF *(ex. TN3270)*.
   After “READY” prompt, type in ISPF.
   After “Option ===>”, type in SDSF.
   After “Command Input ===>”, type in ST to see status of jobs.
   Identify the userid that the application is assigned to (*ex. TCPIP).*

```
SDSF STATUS DISPLAY ALL CLASSES                          LINE 1-17 (83)
COMMAND INPUT ===> _                                       SCROLL ===> PAGE
NP    JOBNAME  JobID    Owner    Prty Queue      C   Pos SAff  ASys Status
      TCPIP    STC14337 TCPIP      15 EXECUTION          ATS1  ATS1 ARMELEM
      TSO      STC14370 STCRACF    15 EXECUTION          ATS1  ATS1
      TN3270   STC14376 TCPIP      15 EXECUTION          ATS1  ATS1
```

Generate a placeholder certificate

3. Follow the process to generate a placeholder certificate using RACDCERT commands:

- Navigate to ISPF/PDF option 6.
- Create a self-signed certificate in RACF as a placeholder.

RACDCERT ID(*certificate-owner*) GENCERT,
SUBJECTSDN(CN('*username*')
T ('*username*''s certificate')
OU('*department*')
O ('*organization*')
L ('*city*')
SP('*state*')
C ('*country*'))
NOTBEFORE(DATE(*start*) TIME(00:00:00))
NOTAFTER (DATE(*finish*) TIME(23:59:59))
WITHLABEL(*self-signed-certlabel*)
SIZE (*key-size*)

```
                                ISPF Command Shell
Enter TSO or Workstation commands below:

 ===> RACDCERT ID(TCPIP) GENCERT SUBJECTSDN(CN('ATS1')OU('Washington Systems Cen
ter')O('IBM')L('Herndon') SP('VA')C('US')) WITHLABEL('ATS1') SIZE(2048) ALTNAME(
IP(9.82.24.230)DOMAIN('ATS1.wsclab.washington.ibm.com'))

Place cursor on choice and press enter to Retrieve command

=> RACDCERT LIST ID (TCPIP)
=> RACDCERT ID(TCPIP) GENCERT SUBJECTSDN(CN('ATS1')OU('Washington Systems Cent
=> RACDCERT DELETE (LABEL('ATS1')) ID(TCPIP) FORCE
=> RACDCERT ID(TCPIP) GENCERT SUBJECTSDN(CN('ATS1')OU('Washington Systems Cent
=> RACDCERT ID(TCPIP) GENCERT, +
=> RACDCERT ID(TCPIP) GENCERT,+
```

Generate a placeholder certificate

4. Issue a “RACDCERT LIST ID(TCPIP)” command to make sure the certificate was created and examine the contents.

- Note that it is a brand-new certificate (Serial Number 00), and that it is self-signed (Issuer’s Name and Subject Name are the same). These will both change when the certificate is signed.

Generate a placeholder certificate

5. Generate a certificate request from the placeholder certificate to send to your external certificate authority using the command below:

RACDCERT ID(*certificate-owner*) GENREQ (LABEL(‘*label*’)) DSN(‘*request.dataset*’)

where label is the placeholder self-signed certificate. RACF saves the certificate request in the data set specified in the DSN parameter.

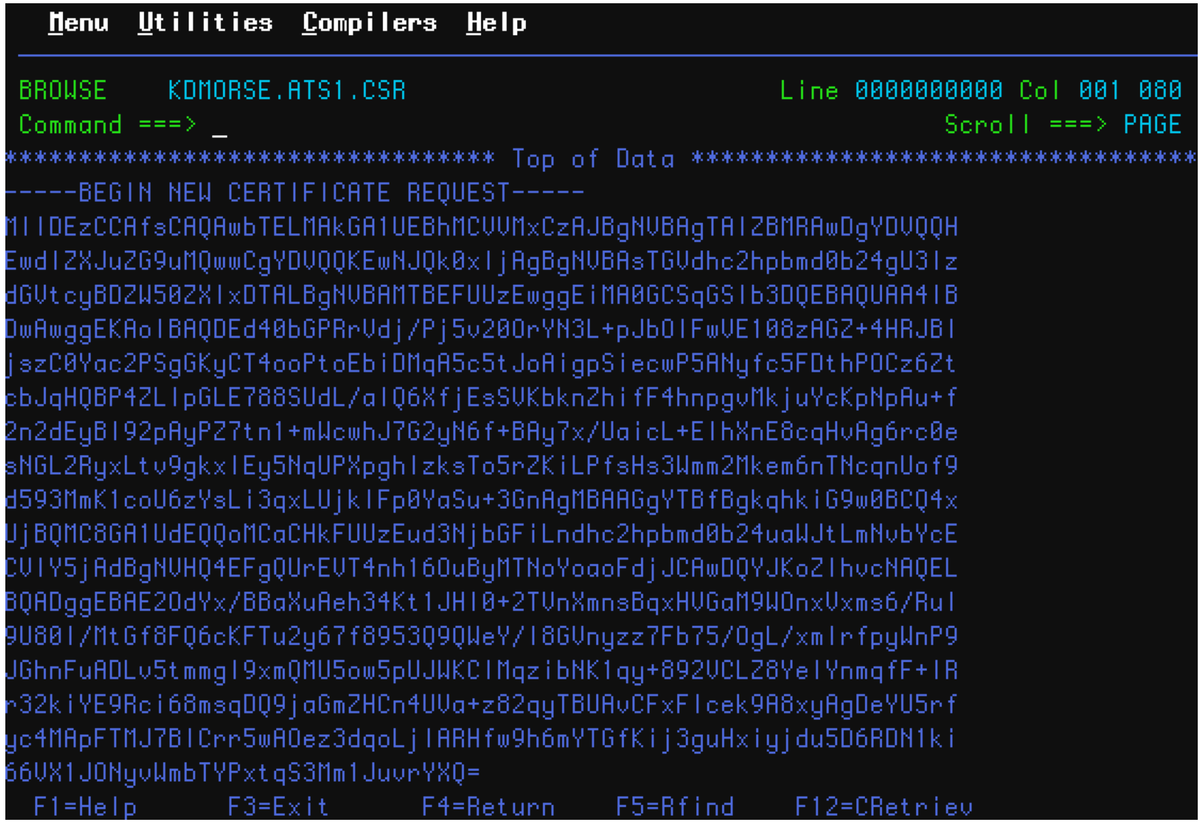
```
                                ISPF Command Shell
Enter TSO or Workstation commands below:

===> RACDCERT ID(TCPIP) GENREQ(LABEL('ATS1'))DSN('KDMORSE.ATS1.CSR')
```

NOTE: We have chosen to stash the certificate in our user high-level qualifier (‘KDMORSE’). Another location may be appropriate for your system.

Generate a placeholder certificate

6. Navigate and view the certificate to ensure it looks like a text file. The format is either .PEM or .DER. This is useful for the transfer to an external CA.

- Privacy Enhanced Mail Certificate file contains ASCII data prefixed with a “-----BEGIN…” line.
- DER is Distinguished Encoding Rules certificates containing a binary representation of the certificate, used for storing X.509 certificates in public cryptography.



NOTE: In our case, our certificate is in PEM format.

Submit certificate request to CA

Submit certificate request to CA

7. We need to upload the certificate request (CSR) to a third-party Certificate Authority so we'll need to download it to a local machine. Sending them via FTP as ASCII files works well.

For Mac Users:

- Open Terminal
- Type in *ftp hostname,* where hostname is the IP address of the mainframe
- Login with your TSO credentials
- To download the file from the mainframe to your local machine, type *get 'request.dataset' certificate-name.csr*
    - For example, we used *get 'KDMORSE.ATS1.CSR' ATS1.csr*
- Type *quit*
- Verify that the information transferred with OpenSSL command (the city, state, alternate names, etc).
    - For example: *openssl req –in ATS1.csr -text*

For Windows Users:

- Open Command Prompt
- Type *ftp hostname*, where hostname is the IP address of the mainframe
- Login with your TSO credentials
- To download the file from the mainframe to your local machine, type *get 'request.dataset' certificate-name.csr* For example: *get 'KDMORSE.ATS1.CSR' ATS1.csr*
- Type *quit* to exit the FTP session
- To verify that the information transferred correctly, you'll need to use OpenSSL. If you don't have OpenSSL installed on your Windows machine:
    - Download and install OpenSSL for Windows
    - Add the OpenSSL bin directory to your system PATH
- Verify the information with the OpenSSL command (the city, state, alternate names, etc).: *openssl req -in ATS1.csr -text*

Submit certificate request to CA

8. Send the certificate request to the certificate authority, using a method that the certificate authority accepts.

Once the certificate request is approved, the certificate is now signed by the CA.

Download and install certificate

Download and install certificate

9. Download and install certificate as a ‘CRT’ file to your local machine, along with the CA Root and Intermediate certificates. Rename your certificate as *certificate-name.crt* (ex. *ATS1.crt*) to start.

For Mac Users:

- Open Terminal and save the certificate in ‘DER’ format by issuing the command: *cp certificate-name.crt certificate-name.der* (ex. *cp ATS1.crt ATS1.der*)
- Read the file by issuing the command: *openssl x509 -inform der -in certificate-name.der -text –noout*
  - For example: *openssl x509 inform der –in ATS1.der –text –noout*
- Type in *ftp hostname,* where hostname is the IP address of the mainframe
- Login with your TSO credentials
- Type ’binary’ to ensure that the file transfer mode is binary and not ASCII.
- To upload the file from the local machine to the mainframe, type *put certificate-name.der ‘response.dataset’*
  - For example, we used *put ATS1.der ‘KDMORSE.ATS1.DER’*
- Upload the CA root and intermediate certificates, type *put carootcert.der ‘caroot.dataset’* and *put caintermediatecert.der ‘caintermediate.dataset’*
- Type *quit* to exit the FTP session.

Download and install certificate

9. Download and install certificate as a ‘CRT’ file to your local machine, along with the CA Root and Intermediate certificates. Rename your certificate as *certificate-name.crt* (ex. *ATS1.crt*) to start.

For Windows Users:

- Open Command Prompt and save the certificate in ‘DER’ format by issuing the command: *cp certificate-name.crt certificate-name.der*
  - For example, *cp ATS1.crt ATS1.der*
- Read the file by issuing the command: *openssl x509 -inform der -in certificate-name.der -text –noout*
  - For example, *openssl x509 inform der –in ATS1.der –text –noout*
- Type *ftp hostname*, where hostname is the IP address of the mainframe
- Login with your TSO credentials
- To upload the file from the local machine to the mainframe, type *put certificate-name.der ‘response.dataset’*
  - For example, we used *put ATS1.der ‘KDMORSE.ATS1.DER’*
- Type *quit* to exit the FTP session.

Download and install certificate

10. On the TN3270 emulator, replace the self-signed certificate with your new CA-signed certificate:

RACDCERT ID(*certificate-owner*) ADD(‘*dataset-name*’) TRUST
For example: *RACDCERT ID(TCPIP) ADD(‘KDMORSE.ATS1.DER’) TRUST*

Check if the certificate is there:
RACDCERT LIST ID(*certificate-owner*)
For example: *RACDCERT LIST ID(TCPIP)*

Check if the chain is complete (it won’t be):
RACDCERT LISTCHAIN ID(*certificate-owner*)
For example: *RACDCERT LISTCHAIN ID(TCPIP)*

Download and install certificate

10. Add the root and intermediate certificates

RACDCERT ADD (‘*response.dataset*’) CERTAUTH WITHLABEL(‘*label*’) TRUST

For example: *RACDCERT ADD(‘KDMORSE.IBMROOT.DER’) CERTAUTH WITHLABEL(‘IBM-ROOT’) TRUST*

RACDCERT ADD(‘KDMORSE.IBMINTER.DER’) CERTAUTH WITHLABEL(‘IBM-Intermediate’) TRUST

Download and install certificate

11. Create a keyring owned by the certificate owner and hang the certificates on it.

First, check if the chain is complete (it should be now):
RACDCERT LISTCHAIN (LABEL(‘*label*’)) ID(*certificate-owner*)
For example: *RACDCERT LISTCHAIN (LABEL(‘ATS1’)) ID(TCPIP)*

Create a key ring.
RACDCERT ADDRING(*name-of-ring*) ID(*certificate-owner*)
For example: *RACDCERT ADDRING(TN3270) ID(TCPIP)*

Add certificates to the ring.
RACDCERT CONNECT (ID(*certificate-owner*) LABEL(‘*label*’) RING(*name-of-ring*) DEFAULT) ID(*certificate-owner*)
For example: *RACDCERT CONNECT (ID(TCPIP) LABEL(‘ATS1’) RING(TN3270) DEFAULT) ID(TCPIP)*

Download and install certificate

12. Check if the certificate is there:

RACDCERT LISTRING(*) ID(*certificate-owner*)

For example: *RACDCERT LISTSTRING(*) ID(TCPIP)*

Add root and intermediate certificates to the ring.

RACDCERT CONNECT (CERTAUTH LABEL(‘*label*’) RING(*name-of-ring*)) ID(*certificate-owner*)

For example: *RACDCERT CONNECT(CERTAUTH LABEL(‘IBM-ROOT’) RING(TN3270)) ID(TCPIP)*

RACDCERT CONNECT(CERTAUTH LABEL(‘IBM-INTERMEDIATE’) RING(TN3270)) ID(TCPIP)

Part 2: Rekey and Rollover Certificate

Create a certificate request

Rekey the certificate

Execute the following RACF command to rekey the existing certificate:
RACDCERT ID(*certificate-owner*) REKEY (LABEL(‘*label*’)) WITHLABEL(‘*label-new*’)
For example: *RACDCERT ID(TCPIP) REKEY (LABEL(’TEC2MVS TN3270’)) WITHLABEL(‘TEC2MVS TN3270 NEW’)*

Create a request for an external CA to sign:
RACDCERT ID(*certificate-owner*) GENREQ(LABEL(‘*label-new*’)) DSN(‘*output-dataset’*)) For example: *RACDCERT ID(TCPIP) GENREQ(LABEL(‘TEC2MVS TN3270 NEW’)) DSN(‘DZROSSI.TN3270N.CSR’)*

Submit certificate request to CA

Submit certificate request to CA

Upload the certificate request (CSR) to a third-party Certificate Authority. First, we'll need to download it to a local machine.

For Mac Users:

- Open Terminal
- Type in *ftp hostname,* where hostname is the IP address of the mainframe
- Login with your TSO credentials
- To download the file from the mainframe to your local machine, type *get 'request.dataset' certificate-name.csr*
  - For example, we used *get 'DZROSSI.TN3270N.CSR' TN3270N.csr*
- Type *quit*
- Verify that the information transferred with OpenSSL command.
  - For example: *openssl req –in TN3270N.csr -text*

For Windows Users:

- Open Command Prompt
- Type *ftp hostname*, where hostname is the IP address of the mainframe
- Login with your TSO credentials
- To download the file from the mainframe to your local machine, type *get 'request.dataset' certificate-name.csr*
  - For example: *get 'DZROSSI.TN3270.CSR' TN3270N.csr*
- Type *quit* to exit the FTP session
- Verify the information with the OpenSSL command:
  - *openssl req -in ATS1.csr -text*

Submit certificate request to CA

Send the certificate request to the certificate authority, using a method that the certificate authority accepts.

Once the certificate request is approved, the certificate is now signed by the CA.

Download and install certificate

Download and install certificate as a ‘CRT’ file to your local machine. Rename your certificate as *certificate-name.crt* (ex. *ATS1.crt*) to start.

For Mac Users:

- Open Terminal and save the certificate in ‘DER’ format by issuing the command: *cp certificate-name.crt certificate-name.der* (ex. *cp TN3270N.crt TN3270N.der*)
- Convert the DER file to PEM format by issuing the following command: *openssl x509 -inform DER -outform PEM -in certificate-name.crt -out certificate-name.pem*
    - For example: *openssl x509 -inform DER -outform PEM -in TEC2MVS.crt -out TEC2MVS.pem*
- Read the file by issuing the command: *openssl x509 -in certificate-name.pem -text -noout*
    - For example: *openssl x509 -in TEC2MVS.pem -text -noout*
- Type in *ftp hostname,* where hostname is the IP address of the mainframe
- Login with your TSO credentials
- Type ’binary’ or ‘bin’ to ensure that the file transfer mode is binary and not ASCII.
- To upload the file from the local machine to the mainframe, type *put certificate-name.der ‘response.dataset’*
    - For example, we used *put TEC2MVSNEW.der ‘DZROSSI.TEC2NEW.DER’*
- Type *quit* to exit the FTP session.

Download and install certificate

Download and install certificate as a ‘CRT’ file to your local machine. Rename your certificate as *certificate-name.crt* (ex. *ATS1.crt*) to start.

For Windows Users:

- Open Command Prompt and save the certificate in ‘DER’ format by issuing the command: *cp certificate-name.crt certificate-name.der*
  - For example, *cp TN3270N.crt TN3270N.der*
- Convert the DER file to PEM format: *openssl x509 -inform DER -outform PEM -in certificate-name.crt -out certificate-name.pem*
  - For example: *openssl x509 -inform DER -outform PEM -in TEC2MVS.crt -out TEC2MVS.pem*
- Read the file by issuing the command: *openssl x509 -in certificate-name.pem -text –noout*
  - For example, *openssl x509 -in TEC2MVS.pem -text -noout*
- Type *ftp hostname*, where hostname is the IP address of the mainframe
- Login with your TSO credentials. Type ’binary’ or ‘bin’ to ensure that the file transfer mode is binary and not ASCII.
- To upload the file from the local machine to the mainframe, type *put certificate-name.der ‘response.dataset’*
  - For example, we used *put TEC2MVSNEW.der ‘DZROSSI.TEC2NEW.DER’*
- Type *quit* to exit the FTP session.

Add the newly signed certificate into RACF

On the TN3270 emulator, add the newly signed certificate into RACF.

RACDCERT ID(*certificate-owner*) ADD(‘*dataset-name*’)
For example: *RACDCERT ID(TCPIP) ADD(‘DZROSSI.TEC2NEW.DER’)*

Check if the certificate is there and marked with TRUST:
RACDCERT LISTRING(*) ID(*certificate-owner*)
For example: *RACDCERT LISTRING(*) ID(TCPIP)*

If not trusted, issue this command to make it trusted:
RACDCERT ID(*certificate-owner*) ALTER(LABEL(‘*label-name*’)) TRUST
For example: *RACDCERT ID(TCPIP) ALTER(LABEL(‘TEC2MVS TN3270 NEW’)) TRUST*

Rekey and Rollover Certificate

Rollover the key

On the TN3270 emulator, add the newly signed certificate into RACF.

RACDCERT ROLLOVER(LABEL(‘*certificate-name*’)) ID(*certificate-owner*) NEWLABEL(‘*new-certificate-name*’)
For example: *RACDCERT ROLLOVER(LABEL(‘TEC2MVS TN3270’)) ID(TCPIP) NEWLABEL(‘TEC2MVS TN3270 NEW’)*

Issue to refresh changes:
SETROPTS RACLIST(DIGTCERT) REFRESH

Check if the keyring contains the new certificate:
RACDCERT LISTRING(*) ID(*certificate-owner*)
For example: *RACDCERT LISTSTRING(*) ID(TCPIP)*

NOTE: Once rollover is complete, the new certificate may be used as if it were the old certificate. The old certificate is retained for historical reasons such as validating signatures on existing certificates, but may no longer be used for any private key operations such as signing other certificates.

Test application is using new certificate

Test the application is using the new certificate. If not, recycle RACF or PAGENT.

Refresh PAGENT with the console command:
/F PAGENT, REFRESH

If the system is not controlled by PAGENT, then the individual services (TN3270, FTPSERV, etc.) do need to be restarted, which may be disruptive.

Delete the old certificate & rename the new certificate

The steps to delete the old certificate and rename the new certificate are optional but keeps things organized.

Delete the old certificate.

RACDCERT DELETE(LABEL(‘*certificate-name*’)) ID(*certificate-owner*)

For example: *RACDCERT DELETE(LABEL(‘TEC2MVS TN3270’)) ID(TCPIP)*

Rename the new certificate.

RACDCERT ALTER(LABEL(‘*certificate-name*’)) ID(*certificate-owner*) NEWLABEL(‘*certificate-name*’)

For example: *RACDCERT ALTER(LABEL(‘TEC2MVS TN3270 NEW’)) ID(TCPIP) NEWLABEL(‘TEC2MVS TN3270’)*

Refresh changes and test application

Issue to refresh changes:

SETROPTS RACLIST(DIGTCERT) REFRESH

Test the application once more.

Thank you

IBM

Appendix

RACDCERT commands manual:
https://www.ibm.com/docs/en/zos/3.1.0?topic=syntax-racdcert-manage-racf-digital-certificates

Requesting a certificate from a certificate authority:
https://www.ibm.com/support/knowledgecenter/en/SSGMCP_5.4.0/security/tcpip/dfht5_requestcert.html