

Install or Renew Node Credential by CSR

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2014, 2015, 2016. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

| | | |
|----------|---------------------|----------|
| 1 | Introduction | 1 |
| 1.1 | Prerequisites | 2 |
| 2 | Procedure | 5 |





1 Introduction

This document describes how to install or renew a node credential manually with Certificate Signing Request (CSR), PKCS#10.

As shown in Figure 1, the installation or renewal consists of the following main steps:

1. Enrollment data preparation in the Managed Element (ME).
2. CSR file creation in the ME.
3. Transferring the CSR file from the ME to an external host with the SSH File Transfer Protocol (SFTP).

Note: SSH File Transfer Protocol (SFTP) uses system-wide Secure Shell (SSH) algorithm setting defined in *Ssh* Managed Object (MO), see *View SSH Algorithms*.

4. Submitting the CSR file from the external host to an external Certification Authority (CA) and requesting the CA to generate a certificate file in Privacy Enhanced Mail (PEM) or Distinguished Encoding Rules (DER) format.
5. Certificate file creation in the CA.
6. Receiving the certificate file from the CA.

Note: The procedures for sending the CSR file to the CA, creating the certificate at the CA, and receiving the certificate file from the CA are outside the scope of this document. The procedures can depend on the CA.

7. Certificate file installation in the ME. During this step, the ME copies the certificate file to the ME with the SFTP and installs it.

Note: SSH File Transfer Protocol (SFTP) uses system-wide Secure Shell (SSH) algorithm setting defined in *Ssh* MO, see *View SSH Algorithms*.

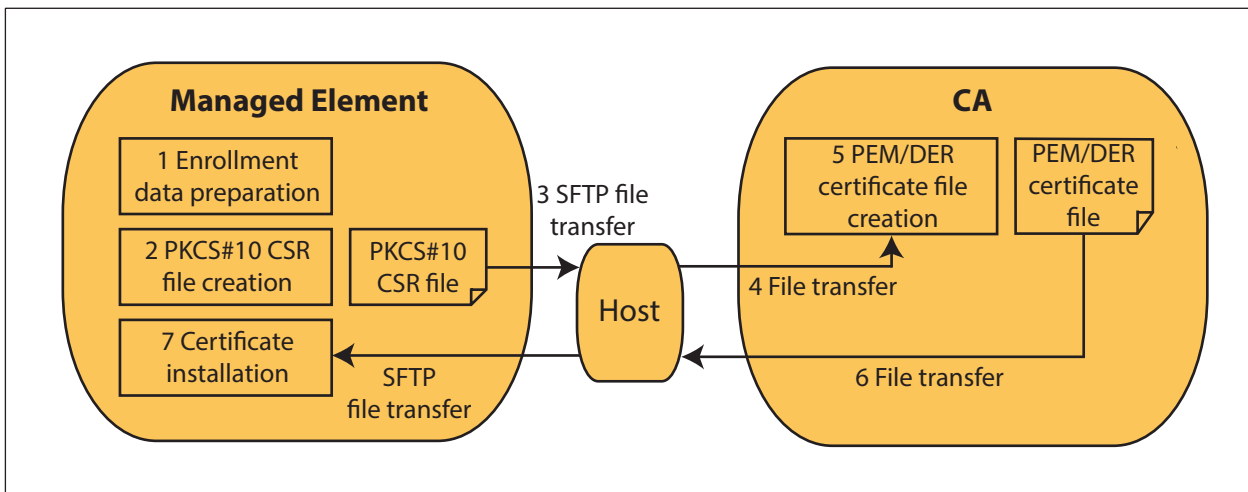


Figure 1 CSR-Based Offline Enrollment

1.1 Prerequisites

This section describes the prerequisites, which must be fulfilled before using the procedure.

1.1.1 Conditions

The following conditions must apply:

- The user has the System Security Administrator role.
- A user account for accessing the ME with the SFTP and downloading the CSR file from the ME is available.

In this document, the corresponding username is `me_user1`.

- The address, username, and password for the SFTP server in the external host are known.

In this document, the username is `hostuser1` and the password is `hostuser1pw` in `host1`.

- The name and path to the certificate file in `host1` are known.

In this document, the external host is `host1`, the username is `hostuser1`, and the password is `hostuser1pw`. The certificate file `node06stNodeCredential1.pem` is stored in `host1` in the home directory for `hostuser1`.

- The user has read access to the certificate file in the external host to be able to download it to the ME with the SFTP.



- The CA used for certificates and the procedures for requesting certificates from the CA are known.
- The fingerprint of the certificate file (PEM or DER file) has been provided by the CA administrator.

In this document, the fingerprint is `ba:41:ac:4f:b3:00:10:98:28:47:36:b1:eb:d9:66:33:69:05:7d:c2`.

- For a renewal, the *NodeCredential* MO to select is known.
- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.





2 Procedure

Enrollment Data Preparation in ME

To install or renew a node credential:

1. Navigate to the *CertM* MO, for example:

```
>dn ManagedElement=NODE06ST, SystemFunctions=1, SecM=1, CertM=1
```

2. Select the appropriate action:

Installation: Proceed with Step 3.

Renewal: Proceed with Step 7.

3. Enter Config mode:

```
(CertM=1) >configure
```

4. Create a *NodeCredential* MO:

```
(config-CertM=1) >NodeCredential=1
```

5. Specify the X.501 Distinguished Name (DN) name to be used in the subject field of the requested certificate, for example:

```
(config-NodeCredential=1) subjectName="C=SE, O=Ericsson, CN=node06st.ericsson.com"
```

Note: The only mandatory Relative Distinguished Name (RDN) required in the DN is the Common Name (CN).

The value `CN=node06st.ericsson.com` is an example value. From a certificate syntax point of view, also other values such as `CN=NODE06ST` are valid. The value that is to be configured in the CN depends on the security policy in the organization for which the ME is installed. It also depends on the information the peer expects to receive in a certificate from the ME when the peer tries to connect to the ME using the service for which this node credential is used.

6. Proceed with Step 9.
7. Select the existing *NodeCredential* MO:

```
(CertM=1) >NodeCredential=1
```

8. Enter Config mode:



```
(NodeCredential=1)>configure
```

9. Select the appropriate key type and length, for example, `RSA_2048` that corresponds to 2048-bit long key generated for the RSA algorithm:

```
(config-NodeCredential=1)keyInfo=RSA_2048
```

10. Commit the changes:

```
(config-NodeCredential=1)commit
```

CSR File Creation in ME

11. Start the enrollment by creating a CSR file in the given local Uniform Resource Identifier (URI). The simplest case is to provide only the filename, for example:

```
(NodeCredential=1)>startOfflineCsrEnrollment --uri  
node06stNodeCredential1.csr
```

The system returns `true` when successfully triggered else `false`.

Starting the enrollment creates the CSR file in the directory referred to by read-only attribute `localFileStorePath` in the *CertM* MO, namely directory `certificates`.

Transferring CSR File from ME with SFTP

The CSR file is copied from the ME to the external host (`host1`). In the example, the user starts from the shell in `host1`, logs in with the SFTP to the ME using username `me_user1`, and retrieves the CSR file from the ME to `host1` with SFTP operation `get`.

12. Open an SFTP session from the external host to the ME, for example:

```
shell$ sftp me_user1@node06st
```

13. Navigate to the folder containing the file, for example:

```
>cd certificates
```

14. Copy the CSR file from the ME by using SFTP operation `get` and specifying the full filename, for example:

```
sftp>get node06stNodeCredential1.csr
```

15. Exit the SFTP session:

```
sftp>exit
```



Certificate File Creation in CA

The procedures for sending the CSR file to the CA, creating the certificate at CA, and receiving the certificate file from the CA are outside the scope of this document. The procedures can depend on the CA.

For the scope of this document, it is sufficient to assume that the CSR file copied with the SFTP to `host1` can be sent further to the CA for signing, and that the certificate file received from the CA is to be copied to `host1`, which is directly accessible from the ME with the SFTP.

Certificate File Installation in ME

The certificate file received from the CA is copied to the ME. This is done with an MO action that downloads the file to the ME with the SFTP from `host1` and installs it to the ME.

16. Navigate to the *CertM* MO, for example:

```
>dn ManagedElement=NODE06ST, SystemFunctions=1, SecM=1
, CertM=1
```

17. Select the node credential:

```
(CertM=1) >NodeCredential=1
```

18. Install the certificate in the same *NodeCredential* MO where the corresponding CSR file was created:

```
(NodeCredential=1) >installCredentialFromUri --uri
sftp://hostuser1@host1/home/hostuser1/node06stNodeCred
ential1.pem --uriPassword hostuser1pw --fingerprint ba:4
1:ac:4f:b3:00:10:98:28:47:36:b1:eb:d9:66:33:69:05:7d:c2
```

The credential password is not needed as the certificate is installed in PEM or DER format (option `--credentialPassword` is not used).

The fingerprint of file `node06stNodeCredential1.pem` is checked. The fingerprint must be entered in the defined format for the algorithm that the ME supports for calculating the fingerprint. The supported format for fingerprint can be read from the node with MO action `(CertMCapabilities=1) >show fingerprintSupport`. For more information on fingerprint, refer to *Generate Fingerprint for File*.

Note: The fingerprint is calculated from the whole file, not only from the certificate it contains.

The credential installation automatically deleted file `node06stNodeCredential1.pem` from directory `certificates`.

The system returns `true` when successfully triggered else `false`.



19. Check that the certificate installation has been completed successfully:

```
(NodeCredential=1) > show enrollmentProgress
```

```
result=SUCCESS  
resultInfo="installed from the certificate file"
```

If an error occurs during the execution of the action, attribute `enrollmentProgress` shows `result=FAILURE` and `resultInfo` shows the cause of the failure.