

Install or Renew Node Credential by PKCS 12

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2014–2018. 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	Description	1
2	Procedure	2
2.1	Install or Renew Node Credential by PKCS#12	2



Install or Renew Node Credential by PKCS 12



1 Description

This instruction describes how to install a node credential manually, directly from a PKCS#12 file containing both a private key and a certificate, or manually renew a node credential.

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

- 1 PKCS#12 certificate container file creation in an external Certification Authority (CA).

The procedures for requesting a PKCS#12 file from the CA, creating the PKCS#12 file at the CA, and receiving the file from the CA are outside the scope of this document. The procedures can vary, depending on the CA.

- 2 Reception of the PKCS#12 file from the CA in an external host.

The way the CA delivers the generated PKCS#12 file is outside the scope of this document. Here it is assumed that the PKCS#12 file is received from the CA and that it is to be copied to host1, which is directly accessible from the ME with the SFTP.

- 3 Certificate container file installation in the Managed Element (ME). During this step, the ME copies the PKCS#12 file from the external host to the ME with the SSH File Transfer Protocol (SFTP) and installs it.

The PKCS#12 certificate container file received from the CA is copied to the ME. This is done with a Managed Object (MO) action that downloads the PKCS#12 file to the ME with the SFTP from an external host (host1) and installs it to the ME.

Enrollment action will automatically create chain certificates if they exists in the received enrollment data

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

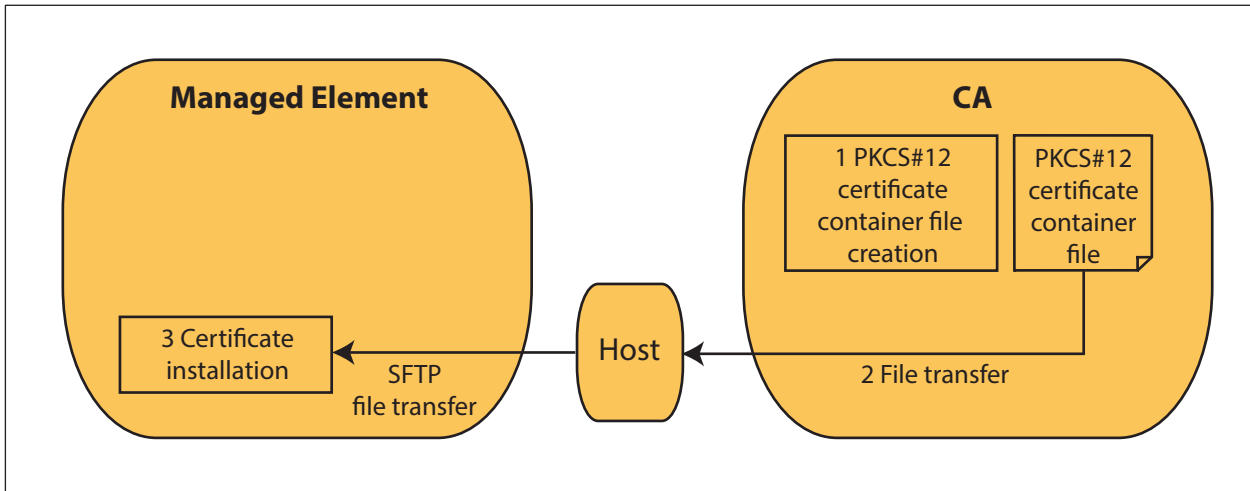


Figure 1 Installation or Renewal of a Node Credential by PKCS#12

2 Procedure

2.1 Install or Renew Node Credential by PKCS#12

Prerequisites

- This instruction references the following document:
 - [Generate Fingerprint for File](#)
 - [View SSH Algorithms](#)
- No tools are required.
- The following conditions must apply:
 - The user has the System Security Administrator role.
 - The address, username, and password for the SFTP server in the external host are known.

In this instruction, the username is `hostuser1` and the password is `hostuser1pw` in `host1`.
 - The name and path to the PKCS#12 file in `host1` are known.

In this instruction, certificate container file `node06stNodeCredential11.p12` is stored in `host1` in the home directory for `hostuser1`.



- The `credentialPassword` password for the PKCS#12 certificate container file has been provided by the Certification Authority (CA) administrator.
- The fingerprint of the PKCS#12 certificate container file has been provided by the CA administrator.

In this instruction, 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` Managed Object (MO) to select is known.
- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.

Steps

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

```
>dn ManagedElement=NODE06S,SystemFunctions=1,SecM=1,CertM=1
```

2. Select the appropriate action:

Installation: Proceed to Step 3.

Renewal: Proceed to Step 6.

3. Enter Config mode:

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

4. Create a `NodeCredential` MO, for example:

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

5. Commit the change:

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

6. Navigate to the `NodeCredential` MO where the PKCS#12 container file is to be installed, for example:

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

7. This is an optional step. You may define the subject alternative name by entering the optional attribute `subjectAltName`, which lets you specify an additional host name into the certificate. The `subjectAltName` can be specified either as an IP address or a domain name, see the managed object model for `NodeCredential` MO. If the `subjectAltName` is specified, the subject alternative name must exist in the enrolled certificate, otherwise the enrollment fails. For example:

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



```
(config-NodeCredential=1)subjectAltName=DNS:www.domain.com
```

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

Note: To verify the subject alternative names of the enrolled certificate view the `extensionContent` field of the `certificateContent` attribute of the `NodeCredential` MO after successful certificate installation.

8. Install the certificate. In this example, the PKCS#12 file is encrypted with password `c_pw`:

```
(NodeCredential=1)>installCredentialFromUri --uri sftp://host
user1@host1/home/hostuser1/node06stNodeCredential1.p12 --uri
Password hostuser1pw --credentialPassword c_pw --fingerprint
ba:41:ac:4f:b3:00:10:98:28:47:36:b1:eb:d9:66:33:69:05:7d:c2
```

The system returns true or false.

If false, proceed with Step 9.

The fingerprint of file `node06stNodeCredential1.p12` 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 seen read from the node with MO action `(CertMCAcapabilities=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 deletes the file `node06stNodeCredential1.p12` from directory certificates.

9. Verify that the certificate installation has been completed successfully:

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

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

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