

Install or Renew Node Credential by PKCS 12

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	3





1 Introduction

This document describes how to manually install a node credential 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).
2. Reception of the PKCS#12 file from the CA in an external host.

Note: 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 depend on the CA.

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.

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

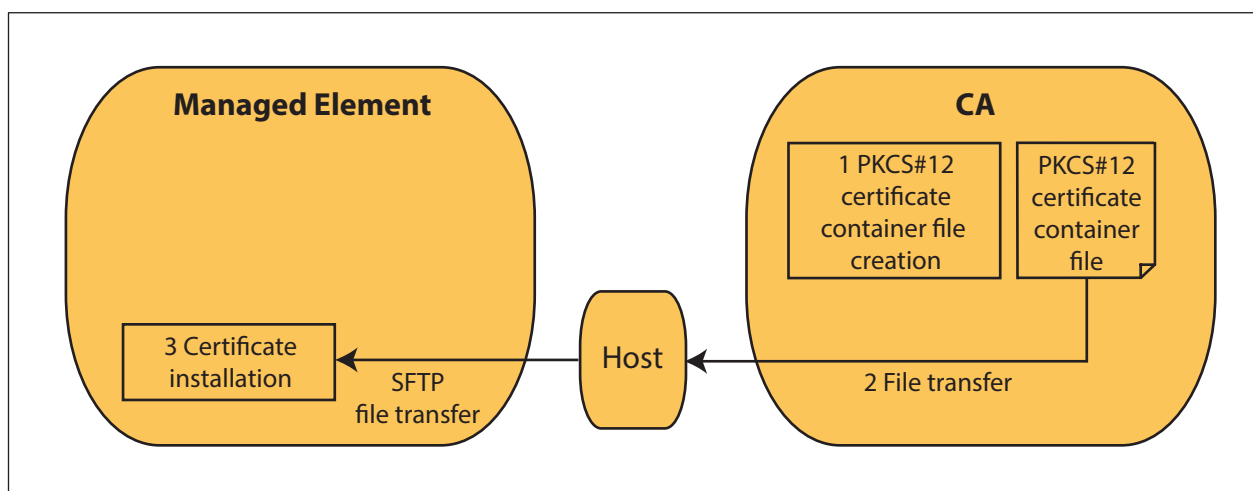


Figure 1 Installation or Renewal of a Node Credential by PKCS#12



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.
- 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 PKCS#12 file in `host1` are known.

In this document, certificate container file `node06stNodeCredential1.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 CA administrator.
- The fingerprint of the PKCS#12 certificate container 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

PKCS#12 Certificate Container File Creation in 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.

Reception of PKCS#12 File from CA

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.

Certificate Container File Installation in ME

The PKCS#12 certificate container file received from the CA is copied to the ME. This is done with an 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.

To install or renew a node credential:

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:

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

5. Commit the change:

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

6. Select the existing *NodeCredential* MO to which the PKCS#12 container file is to be installed:



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

7. This step assumes that the PKCS#12 file is encrypted with password `c_pw`

Install the certificate:

```
(NodeCredential=1) >installCredentialFromUri --uri  
sftp://hostuser1@host1/home/hostuser1/node06st  
NodeCredential1.p12 --uriPassword 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, go to Step 8.

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 `(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.p12` from directory `certificates`.

8. 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.