

Install Trusted Certificate

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2014, 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 |



Install Trusted Certificate



1 Introduction

This document describes how to install a trusted certificate.

As shown in Figure 1, the trusted certificate installation consists of the following main steps:

1. Reception of the certificate file for a trusted CA in an external host.

Note: The procedures how a certificate file is delivered to the operator for installation are outside the scope of this document. The procedures can vary, depending on the CA.

Trusted Certificate is a certificate of CA which the operator trusts. ME uses the CA certificate to verify the CA signature on the peer certificate, before establishing a secure connection.

The peer certificate can have been signed by the CA that the operator trusts or it can be signed by another CA to which the trusted CA trusts (chain of trust). The peer can be a node or a host in the operator's own network, or a node in another operator network.

For the scope of this document, it is sufficient to assume that the peer has a certificate signed by the CA which the operator trusts. That signing CA certificate file has been delivered to the operator and copied to an SSH File Transfer Protocol (SFTP) server (in this document named `host1`), which allows SFTP access from the Managed Element (ME).

2. Trusted certificate installation in the ME. During this step, the ME copies the certificate file from the external host to the ME with the SFTP and installs it as a trusted certificate.

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

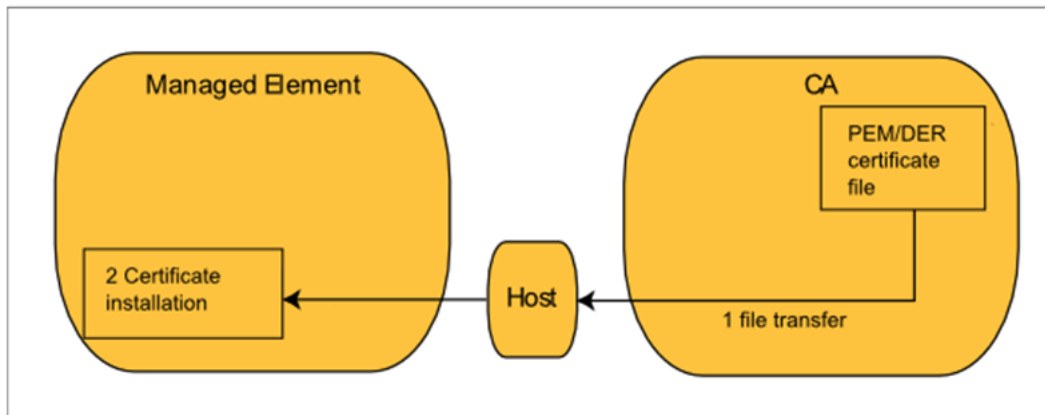


Figure 1 Installation of a Trusted Certificate

The installation is activated in the `CertM=1` context after the X.509 certificate file in Privacy Enhanced Mail (PEM) or Distinguished Encoding Rules (DER) format is uploaded to the node. This procedure automatically creates a *TrustedCertificate* MO, whose attribute `certificateContent` represents the installed certificate.

1.1 Prerequisites

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

1.1.1 Conditions

The following condition must apply:

- The user has the System Security Administrator role.
- The trusted certificate to install is available.
- The name and path to the certificate file in `host1` are known.

In this document, file `trustedCertificate1.pem` is stored in `host1` in the home directory for `hostuser1`.

- The fingerprint for the trusted certificate is known.

In this document, the fingerprint is `c2:91:ac:4f:b3:00:f0:98:28:47:36:b1:eb:d9:66:33:69:05:7d:c4`.

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



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

- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.





2 Procedure

Reception of Certificate File from CA

The way the CA delivers the certificate file is outside the scope of this document. Here it is assumed that the PEM or DER 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.

Trusted Certificate Installation in ME

The certificate file received from the CA is copied to the ME and installed. This is done with an MO action that downloads the certificate file to the ME with the SFTP from an external host (`host1`) and installs it to the ME as a trusted certificate.

The fingerprint, also known as digest, is used in this example procedure to control that a certificate file has not been compromised.

To install a trusted certificate:

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

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

2. Install the trusted certificate, for example:

```
(CertM=1)>installTrustedCertFromUri --uri sftp://ho
stuser1@host1/home/hostuser1/trustedCertificate.pem
--uriPassword hostuser1pw --fingerprint c2:91:ac:4f:b3:
00:f0:98:28:47:36:b1:eb:d9:66:33:69:05:7d:c4
```

The fingerprint of file `trustedCertificate1.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: When referring to files that are relative to user home directory, the syntax of the SFTP Uniform Resource Identifier (URI) format is as follows:

```
sftp://<hostname>/~/cert.pem.
```

The fingerprint is calculated from the whole Certificate Management file, not only from the certificate it contains.

The system returns `true` or `false`.



3. Verify that the certificate installation completed successfully:

```
(CertM=1) > show reportProgress
```

For a successful installation, the system returns the following:

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

If an error occurs during the execution of the action, attribute `reportProgress` shows `result=FAILURE` and `resultInfo` shows the cause of the failure. Repair the failure and restart the installation if needed.

The certificate installation automatically deletes file `trustedCertificate1.pem` in directory `certificates`.