

Install Node Credential Online

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2014, 2016, 2017,2018. 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 Node Credential Online	2





1 Description

This instruction describes how to install a node credential online.

Installation of a node credential online includes an initial online enrollment of the node credential.

As shown in Figure 1, node credential installation with online enrollment consists of the following main steps:

- 1 Enrollment data preparation in the Managed Element (ME).
- 2 The online enrollment starts with a Managed Object (MO) action from the ME. The ME communicates with the enrollment servers at the Certification Authority (CA)/Registration Authority (RA) and installs the node credential. Enrollment action will automatically create chain certificates if they exist in the received enrollment data

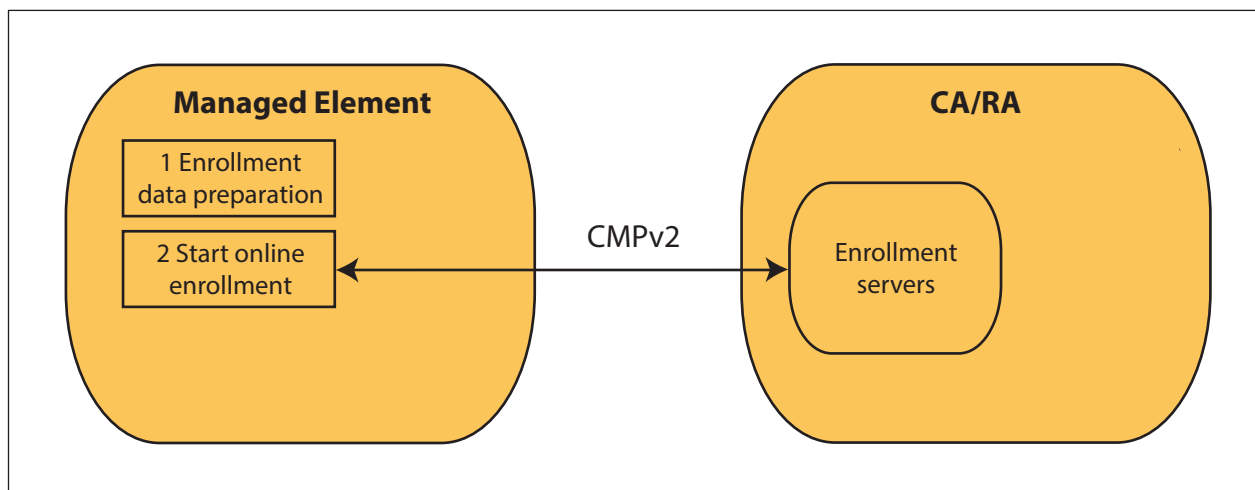


Figure 1 Installation of a Node Credential Online

For more information on how to configure an enrollment server group, refer to [Configure Enrollment Server Group Together with Enrollment Servers](#).



2 Procedure

2.1 Install Node Credential Online

Prerequisites

- This instruction references the following document:
 - [Configure Enrollment Server Group Together with Enrollment Servers](#)
- No tools are required.
- The following conditions must apply:
 - The user has the System Security Administrator role.
 - The challenge password is known.
 - An `EnrollmentAuthority` Managed Object (MO) exists.
 - An `EnrollmentServerGroup` MO with at least one `EnrollmentServer` MO exists.
 - An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.

Steps

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

```
>dn ManagedElement=NODE06ST,SystemFunctions=1,SecM=1,CertM=1
```
2. Enter Config mode:

```
(CertM=1)>configure
```
3. Create the `NodeCredential` MO:

```
(config-CertM=1)>NodeCredential=1
```
4. Set attribute `subjectName`, 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 Distinguished Name (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.

5. Set attribute `keyInfo`, for example:

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

Note: Only RSA keys are supported for online enrollment. Deprecated key types are not recommended for new enrollments.

6. Set attribute `enrollmentServerGroup`, for example:

```
(config-NodeCredential=1)>enrollmentServerGroup="ManagedElement=NODE06ST, SystemFunctions=1, SecM=1, CertM=1, EnrollmentServerGroup=1"
```

7. Set attribute `enrollmentAuthority`, for example:

```
(config-NodeCredential=1)>enrollmentAuthority="ManagedElement=NODE06ST, SystemFunctions=1, SecM=1, CertM=1, EnrollmentAuthority=1"
```

8. Modify the default `enrollmentTimer` value, if needed, for example:

```
(config-NodeCredential=1)>enrollmentTimer=90
```

Note: The default value for attribute `enrollmentTimer` is 60 minutes.

9. 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 certificate author must return the subject alternative name in the enrolled certificate, otherwise the enrollment fails. For example:

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

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.

10. Commit the settings:

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



11. Verify the settings:

```
(NodeCredential=1)>show -v
```

The following is an example output:

```
NodeCredential=1
[...]
  enrollmentAuthority="ManagedElement=NODE06ST,=>
SystemFunctions=1,SecM=1,CertM=1,EnrollmentAuthority=1"
  enrollmentServerGroup="ManagedElement=NODE06ST,=>
SystemFunctions=1,SecM=1,CertM=1,EnrollmentServerGroup=1"
  enrollmentTimer=90
  expiryAlarmThreshold=30 <default>
  keyInfo=RSA_2048
  nodeCredentialId="1"
  renewalMode=MANUAL <default>
  reservedByUser=[] <empty> <read-only>
  subjectAltName="DNS:www.domain.com"
  subjectName="C=SE,O=Ericsson,CN=node06st.ericsson.com"
  userLabel=[] <empty>
  certificateContent=[] <empty> <read-only>
[...]
```

12. Start the enrollment together with parameter challengePassword, for example:

```
(NodeCredential=1)>startOnlineEnrollment --challengePassword
enrollmentChallengePassw
```

The system returns output true or false.

Note: An online initial enrollment requires a shared secret between the node and the enrollment authority. If a challenge password is used as a shared secret, action startOnlineEnrollment must be called together with the password.

13. Verify the result information of the nodeCredentialId enrollment:

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

After a successful online enrollment, the system returns the following:

```
[...]
result=SUCCESS
resultInfo="installed from the online service"
[...]
```

If an error occurs during the execution of the online enrollment, attribute enrollmentProgress shows result=FAILURE and attribute resultInfo shows the cause of the failure. Repair the failure and restart the enrollment if needed.