A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000 Assistant

Signalling Payload Encryption

Administrator Documentation
08/2024

A31003-H34A0-M108-02-76A9

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

1 Overview **4**

2 SPE SSL Certificate Management **5**
2.1 SPE Root Certificate 5
2.2 SPE Certificate 7

3 Signalling and Payload Encryption **11**

Index **12**

1 Overview

NOTICE: Please be aware that from OpenScape Assistant V8 on, the SPE Administration is performed via the Gateway Manager.

In *Gateway Manager* --> **Signalling and Payload Encryption**(SPE) tab sheet on OpenScape 4000 Assistant it is possible to set APN SecureTrace PassPhrase (Access Point Network) and MEK (Master Encryption Key):

- **SecureTrace Passphrase** can be regarded as the customer owned key for activating the SecureTrace and should not be retrievable by the service personal.
- **APN MEK** is used to encrypt signaling data for IPDA (Internet Protocol Distributed Architecture) between the Host System and AP shelves.

Certificate validation

MEK distribution is performed only on boards with the correct web server certificate activated. The certificate is validated during SSL initialization.With the **SPE SSL Certificate Management** dialog it is possible to administrate SPE SSL Root Certificate and SPE SSL Certificate.

Information about web server certificate administration can be found in document *OpenScape 4000 Assistant/Manager V8 Access Management* in chapter *Certificates for this Web Server.*

Distribution of certificates to IP boards using **SPE SSL Certificate Management** dialog is described in chapter below.

If the correct web server certificate is not activated, a warning message about the security risk is displayed. The warning message also gives information on how to correct the issue. Additional MEK distribution is then possible without certificate validation.

Validation of certificate is based on three conditions; in order for the certificate to be valid, all of the following conditions must be true:

- certificate is signed by a valid certification authority
- certificate date is valid
- name of security certificate must match the name of the site.

2 SPE SSL Certificate Management

The SPE SSL Certificate Management comprises features for administering SSL security certificates for Signalling and Payload Encryption feature (SPE). The SPE SSL Certificate Management features provide tools for generation of SPE SSL Root Certificate (CA) and for generation of PKCS#12 certificate suitable for SPE feature which is signed by root certificate.

Before you can generate a new SPE Certificate, an SPE Root Certificate must exist.

For this the following features are available in Assistant's start page entry **Signaling and Payload Encryption** as sub menu items:

- SPE Root Certificate
- SPE Certificate

Related Topic

Signalling and Payload Encryption

2.1 SPE Root Certificate

The feature **SPE Root Certificate** allows you to create your own root certificate which is used to sign all SPE SSL Certificates generated by **SPE Certificate** feature. An already created SPE Root Certificate can be downloaded directly via GUI of the application.

The aim of this feature is to have all SPE certificates within a HiPath 4000/ OpenScape 4000 network signed by just one common root certificate (CA).

A Root Certificate is a special type of self signed certificate. The difference between self signed certificate and root certificate is that when applying a self signed certificates you need to specify the server name, whereas in the case of the root certificate you need to specify a name for the root certificate (CA). The name of the root certificate does not refer to a specific server.

Open the 'SPE SSL Certificate Management' dialog (for the SPE Root Certificate)

In the Assistant start page select:

- **Expert Mode** -> **Signaling and Payload Encryption** -> **SPE Root Certificate**.

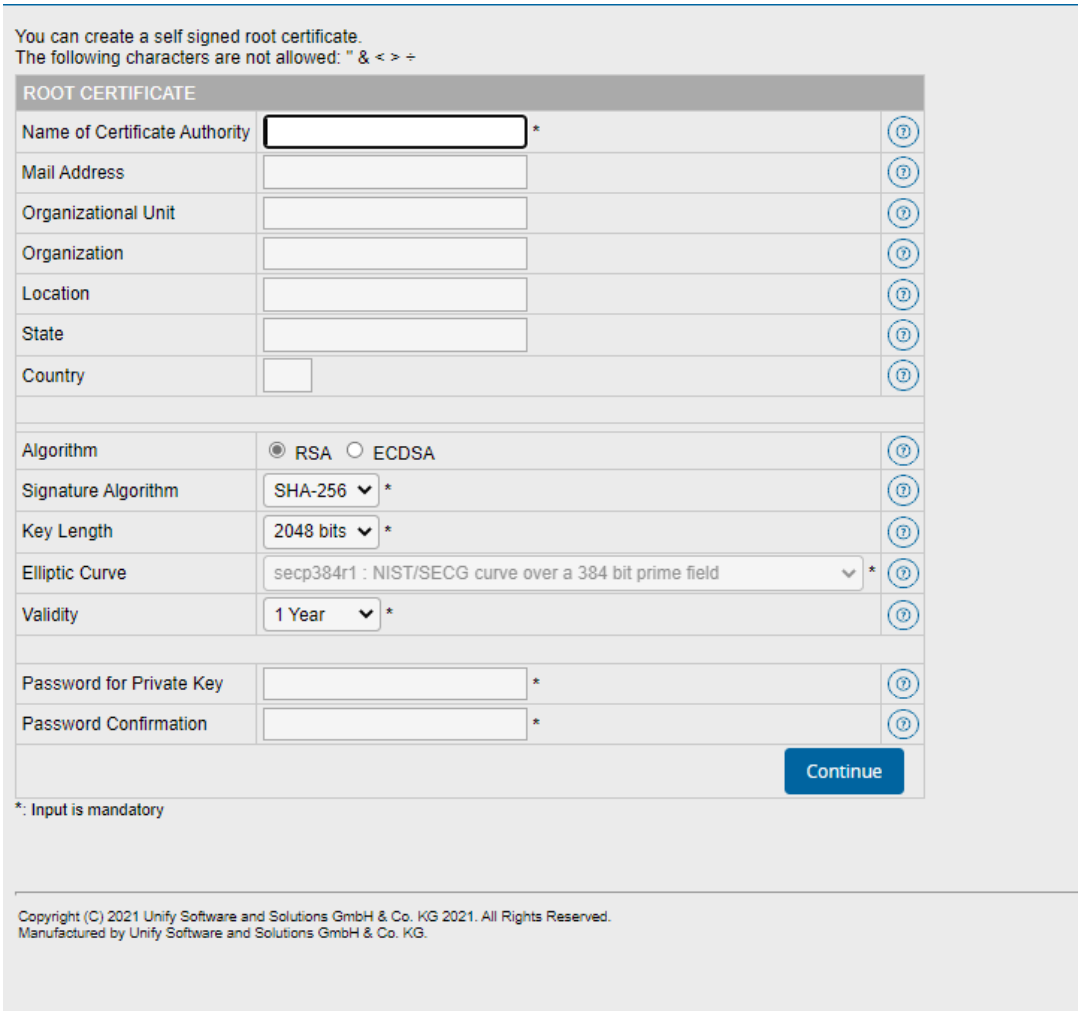
  The **SPE SSL Certificate Management** dialog for the **SPE Root Certificate** opens.

  Depending on whether an SPE Root Certificate exists or not, different contents are displayed in the SPE SSL Certificate Management dialog:

  – *SPE Root Certificate does not exist yet*: If no root certificate has been created yet, the empty root certificate dialog will open.
  – *SPE Root Certificate already exists*: If a root certificate has already been created for this server, the data of the existing certificate will be displayed together with a corresponding note in the root certificate dialog in the browser. It is possible do download root certificate.

Creating a New SPE Root Certificate

1) If no SPE Root Certificate is created yet, the SPE SSL Certificate Management dialog with empty fields is displayed:



- Enter all required data.

  Mandatory fields are flagged with a red asterisk (*). The following characters are not allowed in the entry fields: **" & < > ÷** as well as accented and special characters.

  To get additional context information related the individual entry fields: Click on the **?** icon to the right of each entry field.

  The context-specific information related to the respective field is displayed as a tooltip in the browser.
- Click the **Continue** button.

2) If an SPE Root Certificate was already created an overview of the certificate data is displayed in the SPE SSL Certificate Management dialog:

- Click the **New Root Certificate** button in certificate overview.

  A new dialog screen (such as in case 1.) opens. The data of the existing root certificate are displayed in the entry fields and can be taken over for the new SPE Root Certificate, if desired.

  – Enter all required data.

    Mandatory fields are flagged with a red asterisk (*). The following characters are not allowed in the entry fields: **" & < > ÷** as well as accented and special characters.

    To get additional context information related the individual entry fields: Click on the **?** icon to the right of each entry field. The context-specific information related to the respective field is displayed as a tooltip in the browser.

  – Click the **Continue** button.

WARNING:

If you create a new SPE Root Certificate although a root certificate already exists for this server, the existing SPE Root Certificate will be overwritten.

Displaying/downloading the new created SPE Root Certificate

The data of the new created SPE Root Certificate are displayed. In this case you can download the root certificate:

- Click the link **SPE Root Certificate**.

Related Topics

SPE SSL Certificate Management

SPE Certificate

2.2 SPE Certificate

The SPE Certificate feature provides the method of creating a new SPE Certificate and having it signed by SPE Root Certificate. Certificate created by this feature is always signed by the SPE Root Certificate created in **SPE Root Certificate** feature (see SPE Root Certificate on page 7).

Open the SPE SSL Certificate Management dialog (for the SPE Certificate)

In the Assistant start page select:

- **Expert Mode** -> **Signaling and Payload Encryption** -> **SPE Certificate**.

- The **SPE SSL Certificate Management** dialog for the **SPE Certificate** opens.

  Depending on whether a SPE Certificate or an SPE Root Certificate exists or not, different contents are displayed in the SPE SSL Certificate Management dialog:

  – *SPE Certificate does not exist yet*: If no root certificate has been created yet, the empty root certificate dialog will open.
  – *SPE Certificate already exists*: If a certificate has already been created for this server, the data of the existing certificate will be displayed together with a corresponding note in the certificate dialog in the browser. It is possible do download root certificate.
  – *SPE Root Certificate does not exist yet*: If no root certificate has been created yet, you are informed to create an SPE Root Certificate first (see page 8 Creating a New SPE Root Certificate).

Creating a New SPE Certificate

1) If no SPE Certificate is created yet, the SPE SSL Certificate Management dialog with empty fields is displayed:

2) • Enter all required data.

Mandatory fields are flagged with a red asterisk (*****). The following characters are not allowed in the entry fields: **" & < > ÷** as well as accented and special characters.

To get additional context information related the individual entry fields: Click on the **?** icon to the right of each entry field.

The context-specific information related to the respective field is displayed as a tooltip in the browser.

- Click the **Continue** button.

3) If an SPE Certificate was already created, an overview of the certificate data is displayed in the SPE SSL Certificate Management dialog:

Server	
Common Name	SPECertificate
Country	
Organization	
Organizational Unit	
Mail Address	jan.duda.ext@unify.com
Validity Info	
Version of Certificate	3 (0x2)
Type of Certificate	Server Certificate signed by CA
Serial Number of Certificate	01
Signature Algorithm	sha256WithRSAEncryption
Start of Validity	Jun 29 11:24:54 2015 GMT
End of Validity	Jun 28 11:24:54 2016 GMT
Issuing CA	
Country	
Organization	
Organizational Unit	
Name of CA	SPERootCertificate
Mail Address	jan.duda.ext@unify.com
Encryption Information	
Encryption Algorithm	rsaEncryption
Key Length	2048 bit
MD5 Fingerprint	
SHA1 Fingerprint	08:92:5B:E8:D3:AA:E5:67:3E:51:76:3E:69:EA:34:8E:9C:44:63:C

- Click the **New SPE Certificate** button in certificate overview.

  A new dialog screen (such as in case 1.) opens. The data of the existing root certificate - if one exists - are displayed in the entry fields and can be taken over for the new SPE Certificate.

  – Enter all required data.

  Mandatory fields are flagged with a red asterisk (*). The following characters are not allowed in the entry fields: **" & < > ÷** as well as accented and special characters.

  To get additional context information related the individual entry fields: Click on the **?** icon to the right of each entry field. The context-specific information related to the respective field is displayed as a tooltip in the browser.

  – Click the **Continue** button.

  If you create a new SPE Certificate although a certificate already exists for this server, the existing SPE Certificate will be overwritten.

Displaying/downloading the newly created SPE Certificate

The data of the new created SPE Crtificate are displayed. In this case you can download the certificate:

- Click the link **SPE Certificate**.

Related Topics

SPE SSL Certificate Management

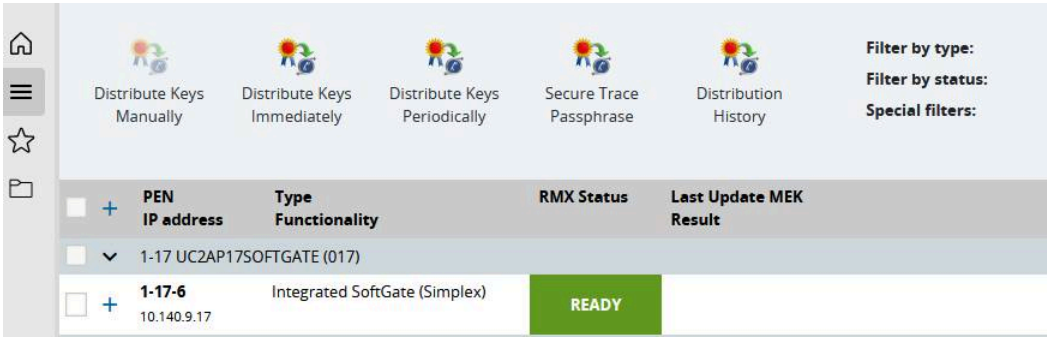
SPE Root Certificate
Signalling and Payload Encryption

3 Signalling and Payload Encryption

The **Signalling and Payload Encryption (SPE)** tab sheet allows you to administrate pass phrase distribution both for AP shelves and HHS.

Signalling and Payload Encryption is available under:

- **Assistant** -> **Expert Mode** -> **Gateway Manager** -> **SPE tab sheet**



The following features are available on this page:

- **Update and distribute a SecureTrace passphrase**

  You can distribute a passphrase for all IP boards using button 'Secure Trace Passphrase'.
- **Configure manual MEK distribution**

  Manual distribution is performed per selected boards and is handled asynchronously. You can configure the manual distribution of the APN MEK per board using 'Distribute Keys Manually' button.

  Manual distribution will start updating AP shelf with the MEK. If updating an AP shelf fails, then it will continue with updating the HHS with the MEK.

  In this case you will be informed that manual distribution is completed with errors and you will be advised to update the AP shelf with the MEK manually from the native web based interface of the Gateway.
- **Immediate MEK distribution**

  You can start random generated MEK distribution to all boards using button 'Distribute Keys Immediately'.
- **Configure automatic MEK distribution**

  You can configure the schedule of the automatic distribution of the APN MEK using 'Distribute Keys Automatically'.

Related Topic

SPE SSL Certificate Management

Index

A

Access Point Network 4
APN 4

C

Certificate validation 4

H

Host System 4

I

Internet Protocol Distributed Architecture 4
IPDA 4

M

Master Encryption Key 4
MEK 4

S

SecureTrace PassPhrase 4