A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000

Signalling and Payload Encryption

Administratordokumentation
07/2024

A31003-H34B0-M114-01-00A9

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.

Inhalt

1 Überblick

Anmerkung: Bitte beachten Sie, dass ab OpenScape Assistant V8 die SPE-Administration über den Gateway-Manager erfolgt.

Auf der Registerkarte*Gateway Manager* --> **Signalling and Payload Encryption** (SPE) des OpenScape 4000 Assistant werden APN SecureTrace PassPhrase (Access Point Network) und MEK (Master Encryption Key) festgelegt:

- Die **SecureTrace Passphrase** fungiert als der Schlüssel des Kunden für die SecureTrace-Aktivierung und darf vom Servicepersonal nicht abgerufen werden können.
- Der **APN MEK** dient zum Verschlüsseln von Signalisierungsdaten für IPDA (Internet Protocol Distributed Architecture) zwischen dem Host-System und den AP-Rahmen.

Zertifikatsvalidation

Die MEK-Verteilung erfolgt nur für Baugruppen, wenn ein gültiges Webserver-Zertifikat aktiviert ist. Das Zertifikat wird während der SSL-Initialisierung validiert. Mit dem Dialog **SPE Zertifikatsverwaltung** lassen sich SPE SSL-Stammzertifikate und SPE-SSL-Zertifikate verwalten.

Informationen zu Verwaltung von Webserver-Zertifikaten finden Sie im Dokument "*OpenScape 4000 Assistant/Manager V8 Access Management - Hilfe*" im Kapitel "*Zertifikate für diesen Webserver*".

Die Verteilung von Zertifikaten auf IP-Baugruppen über den Dialog **SPE SSL-Zertifikatsverwaltung** wird im folgenden Kapitel beschrieben.

Wenn das richtige Webserver-Zertifikat nicht aktiviert ist, wird eine Sicherheitsrisikowarnung angezeigt. Die Warnmeldung gibt auch Auskunft darüber, wie das Problem behoben werden kann. Anschließend sind weitere MEK-Verteilungen ohne Zertifikatsvalidation möglich.

Die Gültigkeit des Zertifikats ist von drei Bedingungen abhängig, die alle erfüllt sein müssen:

- Das Zertifikat ist von einer anerkannten Zertifizierungseinrichtung signiert
- Das Zertifikatsdatum ist gültig
- Der Name des Sicherheitszertifikats muss mit der Site übereinstimmen.

2 SPE SSL Zertifikatsverwaltung

Die SPE SSL Zertifikatsverwaltung umfasst Funktionen zur Verwaltung von SSL Sicherheitszertifikaten für die Funktion "Signalling und Payload Encryption (SPE)". Die SPE SSL Zertifikatsverwaltung stellt Werkzeuge bereit, mit deren Hilfe SPE SSL-Stammzertifikate (CA) und PKCS#12-Zertifikate generiert werden können, die für SPE geeignet sind und vom Stammzertifikat signiert werden.

Bevor ein SPE-Zertifikat erstellt werden kann, muss ein SPE-Stammzertifikat (SPE-Root-Zertifikat) vorhanden sein.

Dazu sind die folgenden Funktionen auf der Assistant Startseite als Untereinträge des Menüpukts **Signaling and Payload Encryption** verfügbar:

- SPE-Root-Zertifikat
- SPE-Zertifikat

Verwandtes Thema

Dialog "SPE-Administration"

2.1 SPE-Root-Zertifikat

Mit der Funktion **SPE-Root-Zertifikat** können Sie ein eigenes Stammzertifikat erstellen, das dazu dient, alle SPE Zertifikate zu signieren, die mit der Funktion **SPE-Zertifikat** erstellt werden. Ein bereits erstelltes SPE SSL-Zertifikat kann direkt über die Benutzeroberfläche der Anwendung heruntergeladen werden.

Der Zweck diese Verfahrens ist, dass alle SPE-Zertifikate in einem HiPath 4000/OpenScape 4000-Netzwerk lediglich von einem einzigen, gemeinsamen Stammzertifikat (CA) signiert sind.

Ein Stammzertifikat ist ein spezieller Typ eines selbstsignierenden Zertifikats. Der Unterschied zwischen einem selbstsignierten Zertifikat und einem Stammzertifikat besteht darin, dass bei der Verwendung eines selbstsignierten Zertifikats der Servername angegeben sein muss, während bei der Verwendung eines Stammzertifikats nur der Name des Stammzertifikats (CA) angegeben werden muss. Der Name eines Stammzertifikats bezieht sich nicht auf einen speziellen Server.

Aufruf des Dialogs "SPE-Zertifikatsverwaltung" (für das SPE-Stammzertifikat)

Wählen Sie auf der Assistant-Startseite:

- **Expertenmodus** -> **Signaling and Payload Encryption** -> **SPE-Root-Zertifikat**.
- Der Dialog **SSL Zertifikatsverwaltung** öffnet sich.

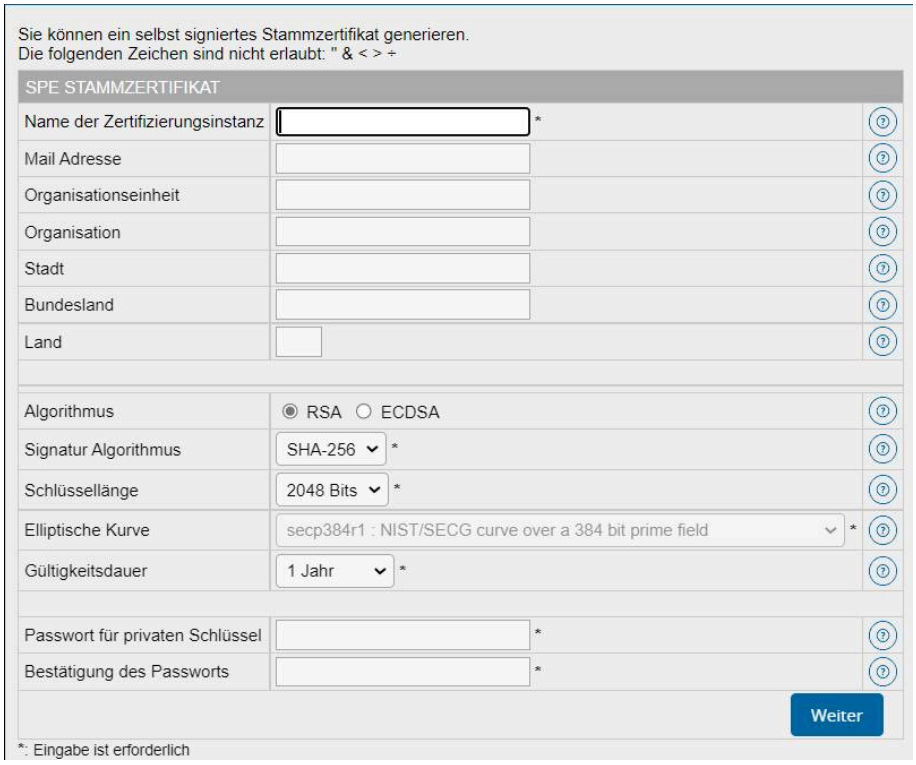
  Abhängig davon, ob bereits ein SPE-Stammzertifikat bereits existiert oder nicht, werden in diesem Dialog unterschiedliche Inhalte angezeigt.

  – Das *SPE-Stammzertifikat existiert nicht*: In diesem Fall sind die Maskenfelder für die Zertifikatsdaten leer.
  – *Das SPE-Stammzertifikat existi*ert: Wenn für diesen Server bereits ein Stammzertifikat generiert wurde, werden die Daten dieses Zertifikats

in den Maskenfeldern ausgegeben und eine diesbezügliche Meldung angezeigt. Das Stammzertifikat kann heruntergeladen werden.

Erstellen eines neuen SPE-Stammzertifikats

1) Wenn noch kein SPE-Stammzertifikat erstellt wurde, wird der Dialog SSL-Zertifikatsverwaltung mit leeren Feldern angezeigt:

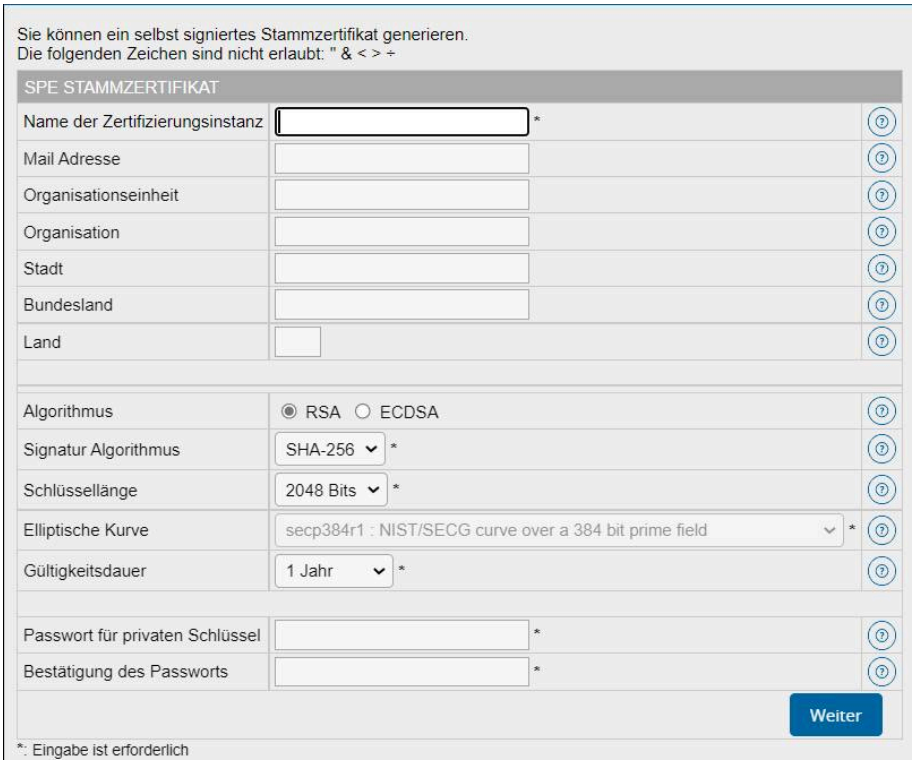


- Geben Sie alle erforderlichen Daten ein.
- Felder, die ausgefüllt werden **müssen**, sind mit einem roten Stern (*) markiert. Nicht erlaubt sind die Zeichen **" & < > ÷** ebenso wie Zeichen mit Akzent.

  Weitere Tooltip-Informationen zu jedem Eingabefeld erhalten Sie durch Klick auf das Fragezeichen "**?**" rechts des jeweiligen Feldes.

  Die kontext-spezifischen Infos werden als "Tooltips" neben den Eingabefeldern eingeblendet.
- Klicken Sie auf die Schaltfläche **Weiter**.

2) Falls ein SPE-Stammzertifikat bereits besteht, wird im Dialog SSL-Zertifikatsverwaltung eine Übersicht mit den Daten des Zertifikats angezeigt:



- Klicken Sie oben in der Zertifikatsübersichtauf die Schaltfläche Neues SPE-Stammzertifikat

  Ein neues Dialogfenster (wie im Fall 1.) öffnet sich. Die Daten des existierenden Stammzertifikats werden in den Eingabefeldern angezeigt und können - wo gewünscht - für das neue SPE-Stammzertifikat übernommen werden.

  – Geben Sie alle erforderlichen Daten ein.

    Felder, die ausgefüllt werden müssen, sind mit einem roten Stern (*) markiert. Nicht erlaubt sind die Zeichen " & < > ÷ ebenso wie Zeichen mit Akzent. Weitere Tooltip-Informationen zu jedem Eingabefeld erhalten Sie durch Klick auf das Fragezeichen "?" rechts des jeweiligen Feldes. Die kontext-spezifischen Infos werden als "Tooltips" neben den Eingabefeldern eingeblendet.

  – Klicken Sie auf die Schaltfläche **Weiter**.

Warnung: Wenn Sie ein neues SPE-Stammzertifikat erstellt wird, obwohl für den Server bereits eines existiert, wird das existierende SPE-Stammzertifikat überschrieben.

Anzeigen/Herunterladen des neu erstellten SPE-Stammzertifikats

Die Daten des neu erstellten SPE-Stammzertifikats werden angezeigt. Sie können nun das Stammzertifikat herunterladen:

- Klicken Sie auf den Link **SPE Root-Zertifikat hier**.

Verwandte Themen

SPE SSL Zertifikatsverwaltung

SPE-Zertifikat

2.2 SPE-Zertifikat

Die Funktion SPE-Zertifikat stellt eine Möglichkeit bereit, ein neues SPE-Zertifikat zu erstellen und es durch das SPE-Stammzertifikat signieren zu lassen. Das mit dieser Funktion erstellte Zertifikat wird immer mit dem SPE-Stammzertifkat signiert, das mit der Funktion **SPE-Root-Zertifikat** erstellt wurde (siehe SPE-Root-Zertifikat auf Seite 7).

Aufruf des Dialogs "SPE-Zertifikatsverwaltung" (für das SPE-Zertifikat)

Wählen Sie auf der Assistant-Startseite:

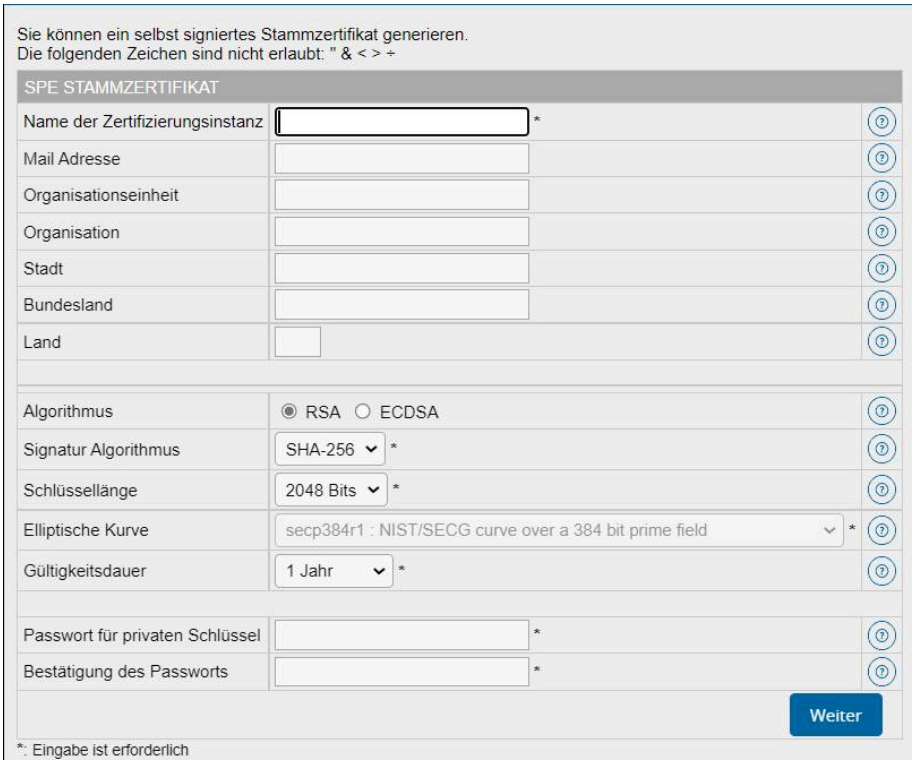
- **Expertenmodus** -> **Signaling and Payload Encryption** -> **SPE-Zertifikat**.
- Der Dialog **SSL Zertifikatsverwaltung** öffnet sich.

  Abhängig davon, ob bereits ein SPE-Stammzertifikat oder ein SPE-Zertifikat existiert oder nicht, werden in diesem Dialog unterschiedliche Inhalte angezeigt.

  – Das *SPE-Zertifikat existiert nicht*: In diesem Fall sind die Maskenfelder für die Zertifikatsdaten leer.
  – *Das SPE-Zertifikat existi*ert: Wenn für diesen Server bereits ein Zertifikat generiert wurde, werden die Daten dieses Zertifikats in den Maskenfeldern ausgegeben und eine diesbezügliche Meldung angezeigt. Das Zertifikat kann heruntergeladen werden.
  – *SPE-Stammzertifikat existiert noch nicht*: Wenn noch kein SPE-Stammzertifikat existiert, werden Sie darauf hingewisen, zuerst ein SPE-Stammzertifikat zu erstellen (siehe Seite 8, Erstellen eines neuen SPE-Stammzertifikats).

Erstellen eines neuen SPE-Zertifikats

1) Wenn noch kein SPE-Stammzertifikat erstellt wurde, wird der Dialog SSL-Zertifikatsverwaltung mit leeren Feldern angezeigt:



- Geben Sie alle erforderlichen Daten ein.

  Felder, die ausgefüllt werden **müssen**, sind mit einem roten Stern (*) markiert. Nicht erlaubt sind die Zeichen **" & < > ÷** ebenso wie Zeichen mit Akzent.

  Weitere Tooltip-Informationen zu jedem Eingabefeld erhalten Sie durch Klick auf das Fragezeichen "**?**" rechts des jeweiligen Feldes.

  Die kontext-spezifischen Infos werden als "Tooltips" neben den Eingabefeldern eingeblendet.
- Klicken Sie auf die Schaltfläche **Weiter**.

2) Falls ein SPE-Zertifikat bereits besteht, wird im Dialog SSL-Zertifikatsverwaltung eine Übersicht mit den Daten des Zertifikats angezeigt:

- Klicken Sie oben in der Zertifikatsübersicht auf die Schaltfläche **Neues SPE-Zertifikat**.

  Ein neues Dialogfenster (wie im Fall 1.) öffnet sich. Die Daten des existierenden Stammzertifikats werden in den Eingabefeldern angezeigt und können - wo gewünscht - für das neue SPE-Zertifikat übernommen werden.

  – Geben Sie alle erforderlichen Daten ein.

    Felder, die ausgefüllt werden **müssen**, sind mit einem roten Stern (*) markiert. Nicht erlaubt sind die Zeichen **" & < > ÷** ebenso wie Zeichen mit Akzent.

    Weitere Tooltip-Informationen zu jedem Eingabefeld erhalten Sie durch Klick auf das Fragezeichen "**?**" rechts des jeweiligen Feldes.

Die kontext-spezifischen Infos werden als "Tooltips" neben den Eingabefeldern eingeblendet.

– Klicken Sie auf die Schaltfläche **Weiter**.

Warnung: Wenn Sie ein neues SPE-Zertifikat erstellt wird, obwohl für den Server bereits eines existiert, wird das existierende SPE-Zertifikat überschrieben.

Anzeigen/Herunterladen des neu erstellten SPE-Zertifikats

Die Daten des neu erstellten SPE-Zertifikats werden angezeigt. Sie können nun das Zertifikat herunterladen:

- Klicken Sie auf den Link **SPE-Zertifikat**.

Verwandte Themen

SPE SSL Zertifikatsverwaltung

SPE-Root-Zertifikat

Dialog "SPE-Administration"

3 Dialog "SPE-Administration"

Im APN-Dialog **SPE-Administration** können Sie die Passphrase-Verteilung für AP-Rahmen und das HHS verwalten.

Starten der Anwendung

Zum Starten der Anwendung SPE-Administration wählen Sie im OpenScape 4000 Assistant Application Launcher folgenden Befehl:

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

Die **SPE-Administration**-Oberfläche wird angezeigt.

In diesem Dialog können die folgenden Aufgaben ausgeführt werden:

- **Aktualisieren und Verteilen einer SecureTrace Passphrase**

  Im Bereich **SecureTrace Passphrase Änderung** können Sie eine Passphrase für alle Baugruppen verteilen. Der Status der Verteilung wird in der Statuszeile (unter **Passphrase ändern Status**) angezeigt.
- **Konfigurieren der manuellen MEK-Verteilung**

  Die manuelle Verteilung wird für ausgewählte Baugruppen ausgeführt und asynchron bearbeitet. Im Abschnitt **Manuelle MEK Verteilung** des Dialogs **SPE-Administration** können Sie die manuelle Verteilung des APN MEK für jede Baugruppe gesondert konfigurieren. Der Status der aktuellen Verteilung wird in einer Statuszeile unter **Manuelle MEK Verteilung Status** angezeigt.

  Bei der manuellen Verteilung wird zunächst der AP-Rahmen mit dem MEK aktualisiert. Wenn die Aktualisierung eines AP-Rahmens fehlschlägt, wird anschließend das HHS mit dem MEK aktualisiert.

  In diesem Fall werden Sie darüber informiert, dass bei der manuellen Verteilung Fehler aufgetreten sind, und angewiesen, den AP-Rahmen über die Web-basierte Oberfläche des CGW (Common Gateway) von Hand mit dem MEK zu aktualisieren.

  Sie können das Ergebnis der manuellen MEK-Verteilung auch in der Tabelle **MEK / Passphrase Verteilung Protokoll** in der rechten unteren Hälfte des Dialogs **SPE-Administration** überprüfen.
- **Konfigurieren der automatischen MEK-Verteilung**

  Die automatische Verteilung kann für alle verfügbaren Baugruppen der NCUI-Familie verwendet werden und für SoftGates, wenn sie nicht in der NCUI-Familie spezifiziert sind.

  Im Abschnitt **Konfiguration Automatische MEK Verteilung** des Dialogs **SPE-Administration** können Sie den Zeitplan für die automatische Verteilung des APN MEK konfigurieren.

- **Anzeigen ausführlicher Protokolle zur SecureTrace Passphrasen-Verteilung**

  Das System speichert die Protokolle einer jeden MEK/SecureTrace Passphrasen-Verteilung. Diese Protokolle können in der Tabelle **MEK / Passphrase Verteilung Protokoll** angezeigt und eingesehen werden.

Felder und Bedienelemente

Abschnitt "SecureTrace Passphrase Änderung"

Abschnitt "Manuelle MEK Verteilung"

Abschnitt "Konfiguration Automatische MEK Verteilung"

Abschnitt "MEK / Passphrase Verteilung Protokoll"

Verwandtes Thema

SPE SSL Zertifikatsverwaltung