A MITEL
PRODUCT
GUIDE

# Unify OpenScape 4000 V10R1

## vHG 3500 HFA für OpenScape 4000 SoftGate

Administratordokumentation
07/2024

P31003-H31B0-M104-01-00A9

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.

# Contents

# 1 Einleitung und wichtige Hinweise

**OpenScape 4000 SoftGate und vHG 3500 HFA**

OpenScape 4000 SoftGate ist eine IP-Telefonie-Applikation für den Anschluss von HFA- und SIP-basierten Telefonen, z.B. für die Telefonfamilien OpenStage HFA und OpenStage SIP. Sie ermöglicht IP-basierte Kommunikation im gesamten Unternehmen einschließlich kleiner Außenstellen. Der Anschluss an das öffentliche Telefonnetz wird durch SIP-Trunking (SIP-Q oder native SIP) ermöglicht.

Die vHG 3500 HFA (virtuelle HG 3500 HFA = virtuelle STMI) ist im OpenScape 4000 SoftGate die zentrale Steuerung für die IPDA (IP Distributed Architecture).

**Themen in diesem Kapitel**



## 1.1 Zielgruppe dieses Buches

Dieses Buch ist für Mitarbeiter gedacht, die für die Administration der vHG 3500 HFA und OpenScape 4000 SoftGate verantwortlich sind. Sie müssen bereits Erfahrung in der Administration von LANs haben und insbesondere über fundierte Kenntnisse in den folgenden Bereichen verfügen:

- Hardware für die Datenkommunikation
- OpenScape 4000 V10
- Konzepte und Begriffe für Weitbereichsnetze (WAN)
- Konzepte und Begriffe für lokale Netze (LAN)
- Konzepte und Begriffe für das Internet

Sie sollten für vHG 3500 HFA und OpenScape 4000 SoftGate eine Einweisung in den folgenden Bereichen erhalten haben:

- Installation und Inbetriebnahme
- Konfiguration der VoIP-Funktionen
- Einrichtung und Konfiguration der Datenkommunikationsparameter

## 1.2 Inhalt dieses Buches

Dieses Buch beschreibt das WBM (Web-Based Management) der vHG 3500 HFA für OpenScape 4000 SoftGate. Dazu gehören die allgemeine Bedienung des WBMs, Beschreibungen der einzelnen Module für die Administration der vHG 3500 HFA und auch, wie bei der Administration vorzugehen ist.

## 1.3 Hinweis zu Internet Explorer

**IMPORTANT:** Wenn Sie Änderungen an den Internet Explorer Sicherheitseinstellungen für eine WBM-Seite vorgenommen haben (z.B.: die Seite den Trusted Sites hinzugefügt), so wird

empfohlen, den Browser neu zu starten, damit die neuen Einstellungen korrekt verwendet werden.

## 1.4 Verwendete Konventionen

In diesem Buch werden die folgenden typographischen Konventionen verwendet:

| Konvention | Beispiel |
|---|---|
| `Courier` | Eingabe und Ausgabe<br>Beispiel: `LOCAL` als Dateiname eingeben<br>`Befehl nicht gefunden` |
| *Kursiv* | Variable<br>Beispiel: *Name* kann bis zu acht Zeichen lang sein |
| *Kursiv* | Elemente der Benutzeroberfläche<br>Beispiel: Klicken Sie auf die Schaltfläche *OK*. |
| Abschnitt 1.4, "Verwendete Konventionen" | Querverweis |
| *Konfiguration* | Elemente der Benutzeroberfläche als Querverweis |
| **Fett** | Besondere Hervorhebung<br>Beispiel: Dieser Name darf **nicht** gelöscht werden |
| `<Courier>` | Tastenkombinationen<br>Beispiel: `<STRG>+<ALT>+<ESC>` |
| **>** | Menüfolge<br>Beispiel: *WBM* **>** *Konfiguration* |
| | Kennzeichnet Situationen, die Sachschäden und/oder Datenverlust zur Folge haben können. |
| | Kennzeichnet hilfreiche Hinweise. |

# 2 WBM

**WBM**

Das WBM ist die Administrationsoberfläche der vHG 3500 HFA für OpenScape 4000 SoftGate (virtuelle HG 3500 HFA = virtuelle STMI). Sofern der Root-Administrator das WBM aktiviert hat, steht es über jede TCP/IP-Verbindung zur Verfügung, sowohl über das LAN als auch das WAN.

Jeder PC mit TCP/IP-gestützter Netzwerkverbindung, auf dem ein kompatibler Web-Browser läuft, kann nach erfolgreicher Anmeldung am OpenScape 4000 Assistant auf das WBM zugreifen. Das WBM der vHG 3500 HFA verfügt über einen integrierten Web-Server, so dass es über eine HTTP-URL aufrufbar ist.

Die Bedienoberfläche des WBMs ist in den Sprachen Englisch verfügbar.

**Themen in diesem Kapitel**



## 2.1 Hard- und Softwarevoraussetzungen

### 2.1.1 Hardware

Für das WBM benötigen Sie einen Administrations-PC mit folgender Mindestausstattung:

- 128 MB Hauptspeicher (RAM)
- Prozessor-Taktrate 400 MHz

### 2.1.2 Software

Das WBM der vHG 3500 HFA besteht aus HTML/XSL-Seiten mit Frames. Sein Einsatz erfordert:

- Windows NT 4.0, 2000, XP, Vista oder Windows 7
- Microsoft Internet Explorer 10, 11
- Im Internet Explorer sind die unten beschriebenen Einstellungen vorzunehmen, siehe Abschnitt 2.2, "WBM starten und beenden".

  Andere Browser, die Frames, Java und JavaScript unterstützen, sind möglicherweise ebenfalls mit dem WBM kompatibel. Browser, die keine Frames unterstützen, können nicht mit dem WBM verwendet werden.

---

**IMPORTANT:** Wenn auf dem Administrations-PC ein DNS-Server eingerichtet wurde, der aber nicht erreichbar ist, führt dies bei der WBM-Oberfläche zu erheblichen Geschwindigkeitseinbußen. Sollte dies bei Ihnen der Fall sein, überprüfen Sie in den Netzwerkeinstellungen des Administrations-PCs die eingestellten DNS-Server.

Entfernen Sie nicht erreichbare DNS-Server, oder tragen Sie erreichbare Server ein.

## 2.2 WBM starten und beenden

**Zugangsmöglichkeiten**

Zum Starten des WBMs der vHG 3500 HFA für OpenScape 4000 SoftGate gibt es zwei Möglichkeiten. Zum einen über OpenScape 4000 Assistant, zum anderen direkt über einen Web-Browser und die URL des WBMs. Der Zugang über OpenScape 4000 Assistant ist die am häufigsten benutzte Möglichkeit.

**Themen in diesem Abschnitt**

**1)** Abschnitt 2.2.1, "Über OpenScape 4000 Assistant starten" Abschnitt 2.2.2, "Über Web-Browser starten" Abschnitt 2.2.3, "WBM-Sitzung beenden"

## 2.2.1 Über OpenScape 4000 Assistant starten

Führen Sie zum Starten der WBM-Sitzung die folgenden Schritte durch:

**1)** Melden Sie sich mit Ihrem Benutzernamen und Ihrem Kennwort am OpenScape 4000 Assistant an.

**2)** Wählen Sie in der Baumstruktur *OpenScape 4000 Assistant* **>** *Experten-modus* **>** *Gateway Dashboard*. Das Fenster *Gateway Dashboard* mit den vorhandenen Baugruppen wird angezeigt.

**3)** Klicken Sie in der Zeile der gewünschten Baugruppe vHG 3500 HFA (z.B. vHG 3500 - HG 3530) in der Spalte *Remote-Zugang* auf *[WBM] [N/A]*. Die IP-Adresse der entsprechenden Baugruppe muss Ihnen bekannt sein.

**4)** Der Web-Server des WBMs wird kontaktiert. Da er ausschließlich mit HTTPS (gesicherter Datenübertragung) arbeitet, sendet der Server ein Zertifikat.

**NOTICE:** Im Internet Explorer 8 kann die Meldung erscheinen, dass ein Problem mit dem Sicherheitszertifikat der Website besteht. Klicken Sie in diesem Fall auf *Laden dieser Website fortsetzen*.

**5)** Bestätigen Sie den Browser-Dialog mit den Zertifikatsinformationen. Die Startseite des WBMs der vHG 3500 HFA wird angezeigt:


1) Überprüfen Sie, ob Sie sich im WBMs der vHG 3500 HFA (z.B. SoftGate-HFA) befinden.
2) In den Modulen *Konfiguration* und *Wartung* können Sie jetzt die vHG 3500 HFA administrieren.

## 2.2.2 Über Web-Browser starten

**Benutzerkennung**

Für das WBM steht Ihnen die Benutzerkennung âAdministrator" zur Verfügung. Diese Kennung bietet Ihnen Zugang zu den Konfigurationseinstellungen.

Der Standard-Benutzername lautet **TRM** und das Standard-Kennwort **HICOM** (wie im AMO STMIB konfiguriert). Diese Standard-Daten können von Ihnen im AMO STMIB geändert werden.

**WBM-Sitzung starten**

Führen Sie zum Starten der WBM-Sitzung die folgenden Schritte durch:

1) Öffnen Sie Ihren Web-Browser.
2) Geben Sie in die Adresszeile des Web-Browsers die URL des WBMs der vHG 3500 HFA ein, d. h. im Format *https://999.999.999.999*. Der Webserver des WBMs wird kontaktiert. Da er ausschließlich mit HTTPS (gesicherter Datenübertragung) arbeitet, sendet der Server ein Zertifikat.
3) Bestätigen Sie den Browser-Dialog mit den Zertifikatsinformationen. Der Anmeldedialog des WBMs der vHG 3500 HFA wird angezeigt.
4) Geben Sie den Benutzernamen und das Kennwort ein. Klicken Sie auf die Schaltfläche *Login*. Die Startseite des WBMs der vHG 3500 HFA wird angezeigt:


1) In den Modulen *Konfiguration* und *Wartung* können Sie jetzt die vHG 3500 HFAadministrieren.

## 2.2.3 WBM-Sitzung beenden

Führen Sie zum Beenden der WBM-Sitzung die folgenden Schritte durch:

1) Klicken Sie auf das Modul Abmelden. Die Verbindung zum WBM die vHG 3500 HFA wird beendet und die WBM-Sitzung wird geschlossen.

Erläuterungen zum Beenden der WBM-Sitzung finden Sie im Kapitel 6, âAbmelden".

## 2.3 Benutzeroberfläche des WBMs

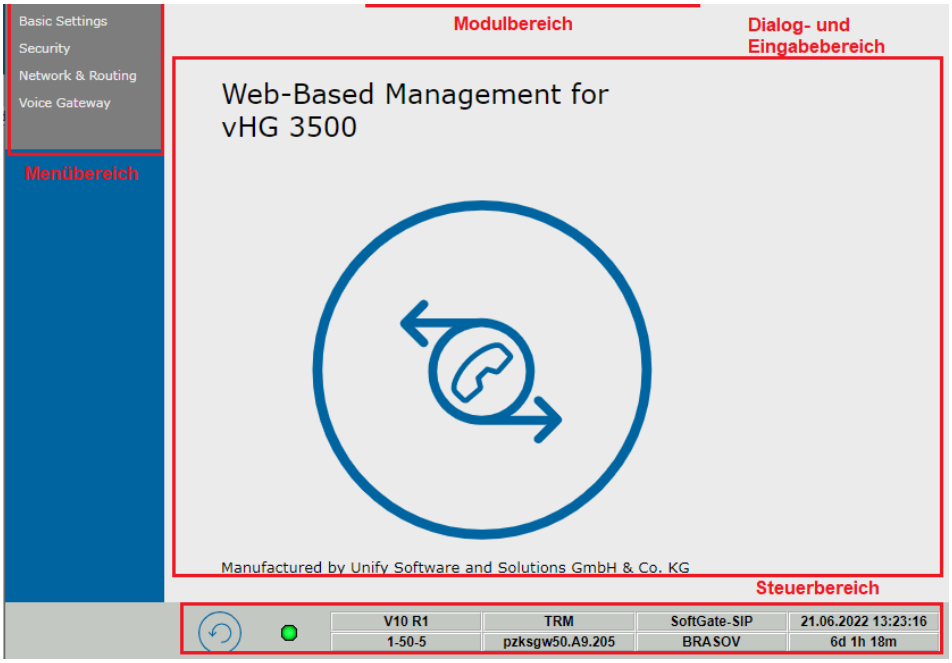
Dieser Abschnitt erklärt den grundsätzlichen Aufbau der Benutzeroberfläche, nennt die einzelnen Bedienelemente und beschreibt deren Benutzung.

**Themen in diesem Abschnitt**

1) Abschnitt 2.3.1, "Einteilung der Benutzeroberfläche" Abschnitt 2.3.2, "Symbole im Steuerbereich des WBM-Fensters" Abschnitt 2.3.3, "Dialogelemente"

## 2.3.1 Einteilung der Benutzeroberfläche

Die Benutzeroberfläche des WBMs lässt sich in die folgenden Bereiche einteilen:




**Menübereich**

Dieser Bereich wird für die Navigation innerhalb eines Moduls verwendet. Welche Menüeinträge dort angezeigt werden, hängt vom gewählten Modul ab.

**Modulbereich**

Dieser Bereich zeigt die zur Verfügung stehenden Module an. Die Module sind: *Konfiguration*, *Wartung*, *Hilfe* und *Abmelden*. Durch Klicken auf den Namen des Moduls erscheinen im Menübereich die zugehörigen Menüeinträge.

**Dialog- und Eingabebereich**

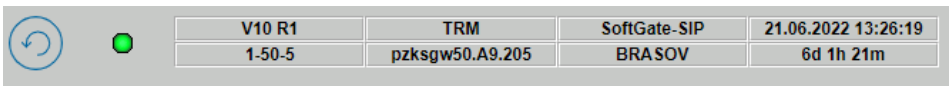
In diesem Bereich erscheinen nach Auswählen des Moduls und des Menüeintrages die jeweiligen Einstellungsdialoge.

**Steuerbereich**

Am unteren Rand finden Sie einige ständig angezeigte Statusinformationen. Zur Bedeutung der Symbole siehe Abschnitt 2.3.2, "Symbole im Steuerbereich des WBM-Fensters".

## 2.3.2 Symbole im Steuerbereich des WBM-Fensters

Im Statusbereich werden laufend Steuer- und Statusinformationen bereitgestellt. Ein Beispiel hierfür zeigt die unten stehende Abbildung:




**Es gibt folgende Steuersymbole:**

Reset-Symbol (1)

Dieses Symbol kann folgende Zustände annehmen:

**Weiß/grau:** Die Dateneingabe ist gesperrt. Der Benutzer kann Daten lesen aber keine Einträge ändern.

**Weiß/schwarz:** Die Dateneingabe ist aktiviert. Durch das Klicken auf dieses Symbol wird ein Neustart der vHG 3500 HFA ausgelöst.

Aktivitäts-Symbol (2)

Das Symbol leuchtet grün, wenn eine Verbindung zum Webserver des WBMs besteht. Wenn keine Verbindung besteht, blinkt das Symbol rot.

**Außerdem werden folgende Statusinformationen angezeigt:**

- Zustandsinformation der ITIL-Version (3),
- Zugangskategorie des Benutzers und Systemversion (4),
- Name der Baugruppe und Aufstellungsort (5),
- Systemdatum und -uhrzeit sowie Zeit seit dem letzten Neustart (6).

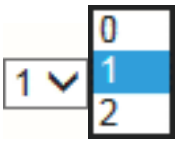
## 2.3.3 Dialogelemente

Im WBM kommen die folgenden Dialogelemente vor:

**Eingabefelder**

Eingaben von numerischen oder alphanumerischen Werten. Vor, hinter oder über dem Feld steht die zugehörige Feldbeschriftung. Bei Passwortfeldern werden zur Sicherheit nur einheitliche Symbole wie Sternchen für jedes eingegebene Zeichen angezeigt. Nicht auf der Tastatur verfügbare Zeichen können unter Microsoft Windows z.B. über die Zeichentabelle eingefügt werden.

**Auswahlfelder**




(im nebenstehenden Bild link geschlosen, rechts geöffnet) Auf den Pfeil klicken, um die Liste zu öffnen oder zu schließen. Den gewünschten Eintrag mit der Maus anklicken.

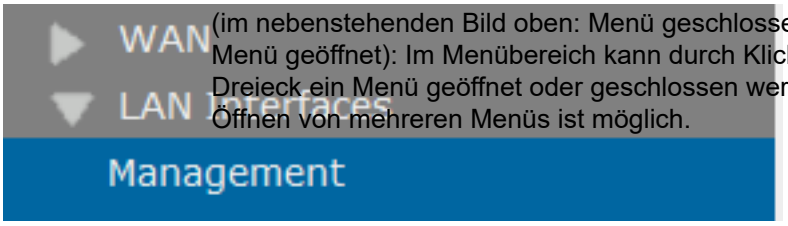
**Kontrollkästchen**

(im nebenstehenden Bild oben ausgeschaltet, unten eingeschaltet): Vor, hinter oder über dem Feld steht die zugehörige Feldbeschriftung. Anklicken, um die entsprechende Option ein- oder auszuschalten. Es können mehrere Kontrollkästchen aktiviert sein.

### Radio-Buttons

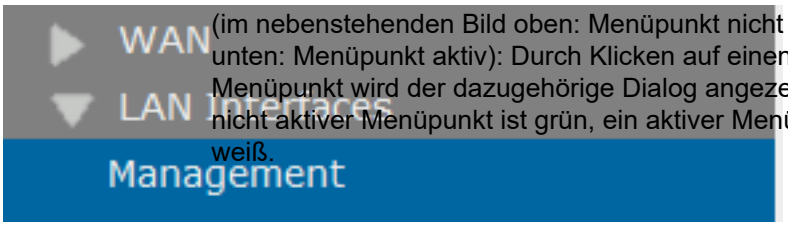
(im nebenstehenden Bild oben ausgeschaltet, unten eingeschaltet): In einer zusammengehörigen Gruppe solcher Elemente ist stets eines eingeschaltet und alle anderen ausgeschaltet. Vor, hinter oder über dem Feld steht die zugehörige Feldbeschriftung. Anklicken, um die entsprechende Funktion einzuschalten.

### Dreiecke




(im nebenstehenden Bild oben: Menü geschlossen, unten: Menü geöffnet): Im Menübereich kann durch Klicken auf ein Dreieck ein Menü geöffnet oder geschlossen werden. Das Öffnen von mehreren Menüs ist möglich.

### Menüpunkte

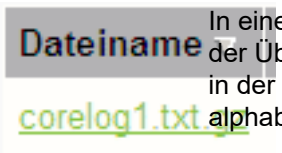



(im nebenstehenden Bild oben: Menüpunkt nicht aktiv, unten: Menüpunkt aktiv): Durch Klicken auf einen Menüpunkt wird der dazugehörige Dialog angezeigt. Ein nicht aktiver Menüpunkt ist grün, ein aktiver Menüpunkt ist weiß.

### Schaltflächen


Bei Anklicken wird die Aktion ausgeführt, die als Text auf der Schaltfläche steht. Die Texte sind selbsterklärend, wie z.B. *Rückgängig* oder *Übernehmen*.

### Sortierreihenfolge




In einer Tabelle kann durch Anklicken des Dreiecks neben der Überschrift in einem Tabellenkopf die Sortierreihenfolge in der darunterliegenden Spalte geändert werden, z.B. alphabetisch aufsteigend oder absteigend.

# 3 Konfiguration

**WBM-Pfad**

*WBM* **>** Konfiguration

Das Modul Konfigurationwird angezeigt

Das Modul Konfiguration dient zum Festlegen der Eigenschaften des vHG 3500 HFA Gateways (Grundeinstellungen) und zum Verwalten des Leistungsmerkmals Signaling & Payload Encryption (SPE).

**Auswahlmöglichkeiten im Modul** Konfiguration

**1)** Grundeinstellungen SPE

## 3.1 Grundeinstellungen

Im Menü Grundeinstellungen können grundsätzliche Daten der vHG 3500 HFA eingegeben werden.

**WBM-Pfad**

*WBM* **>** Konfiguration **>** Grundeinstellungen

Das Menü Grundeinstellungen wird angezeigt.

**Menü** Grundeinstellungen

Die folgenden Optionen werden in diesem Menü angezeigt:

**1)** Gateway

### 3.1.1 Gateway

**WBM-Pfad**

*WBM* **>** Konfiguration **>** Grundeinstellungen **>** Gateway

Der Dialog *Gateway-Eigenschaften* wird angezeigt: In diesem Dialog können Sie Grunddaten eingeben.

**Eingabefelder**

In diesem Dialog gibt es die folgenden Eingabefelder:

- *System-Name*: In dieses Feld ist der Name der vHG 3500 HFA einzugeben, z.B. wenn an einem OpenScape 4000 SoftGate mehrere vHG 3500 HFA betrieben werden.
- *Gateway-Standort*: Schreibgeschützt. In diesem Feld wird der Standort der vHG 3500 HFA angezeigt.

**Schaltflächen**

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Defaultwerte zurückgesetzt.

## 3.2 SPE

Durch SPE (Signaling & Payload Encryption) werden VoIP-Nutz- und Signalisierungsdatenströme von und zur vHG 3500 HFA verschlüsselt. Diese Funktion basiert auf einem asymmetrischen Verschlüsselungsprozess. Öffentliche und private Schlüssel werden für diese Art von Prozess verwendet.

Die einzelnen VoIP-Clients und Gateways, z. B. vHG 3500 HFA, müssen im Kommunikationssystem identifizierbar sein. Dazu werden Zertifikate mit privaten oder öffentlichen Schlüsseln verwendet. Zertifikate werden entweder von einer Kunden-PKI-Zertifizierungsstelle (RA/CA) oder von der internen Zertifizierungsstelle (CA) des DLS-Servers erstellt. Der DLS-Server sendet die Dateien mit diesen Zertifikaten an den Gateway-DLS-Client.

Je nach Anforderung können Sicherheitseinstellungen zur Bewertung der Zertifikate und zur Verschlüsselung von Datenströmen aktiviert oder deaktiviert werden. So wird die Verschlüsselungssicherheit erhöht oder verringert.

**WBM-Pfad**

*WBM* **>** Konfiguration **>** SPE

Das Menü SPE wird angezeigt.

SPE ***Menü***

Die folgenden Optionen werden in diesem Menü angezeigt:

**1)** Keycert importieren Keycert anzeigen Keycert löschen SPE-Sicherheitseinstellung für HFA

### 3.2.1 Keycert importieren

**NOTICE:** Wenn Sie ein Zertifikat zum ersten Mal mit aktivem SPE importieren, wird automatisch ein Neustart durchgeführt.

Unterstützte Public Key Algorithmen für SPE-Zertifikate sind

- **RSA** mit einer Mindestschlüssellänge von 2048 Bit.
- **ECDSA**

**WBM-Pfad**

*WBM* **>** Konfiguration **>** SPE **>** Schlüsselzertifikat importieren

Der Dialog *Laden eines SPE Key Zertifikats über HTTP* wird angezeigt. In diesem Dialog können Sie ein SPE-Schlüsselzertifikat importieren, indem Sie das Entschlüsselungskennwort und den Dateinamen eingeben. Die Datei mit dem Zertifikat stammt von einer Kunden-PKI-Zertifizierungsstelle (RA/CA) oder der internen DLS-Server-Zertifizierungsstelle (CA) und muss im PEM- oder PKCS#12-Format vorliegen.

**Eingabefelder**

In diesem Dialog gibt es die folgenden Eingabefelder:

- *Entschlüsselungskennwort*: Geben Sie in diesem Feld das Kennwort ein, das bei der Erstellung der PEM- oder PKCS#12-Datei verwendet wurde.

- *Datei mit Zertifikat und privatem Schlüssel (PEM oder PKCS#12-Format)*: In dieses Eingabefeld sind der Pfad und der Name der Datei, die das Zertifikat enthält, einzugeben. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

**Schaltflächen**

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Fingerabdruck des Zertifikats anzeigen*: Durch Prüfen des Fingerabdrucks kann festgestellt werden, ob ein unverändertes Zertifikat vorliegt oder ob es verändert wurde.
- *Zertifikat aus Datei importieren*: Das Zertifikat wird aus der im oben genannten Eingabefeld angegebenen Datei importiert.

**Vorgehensweise**

Führen Sie die folgenden Schritte aus, um ein SPE-Zertifikat zu laden:

**1)** Wählen Sie: *WBM* **>** Konfiguration SPE **>** Schlüsselzertifikat importieren. *Laden eines SPE Key Zertifikats über HTTP* wird angezeigt. Folgende Felder können bearbeitet werden:

- *Entschlüsselungskennwort*: Geben Sie in diesem Feld das Kennwort ein, das bei der Erstellung der PEM- oder PKCS#12-Datei verwendet wurde.
- *Datei mit Zertifikat und privatem Schlüssel (PEM oder PKCS#12-Format)*: Geben Sie den Pfad und den Dateinamen der Datei ein, die die zu importierenden Zertifikatsdaten enthält. Klicken Sie auf *Durchsuchen*, um einen Dialog zur Suche nach der Datei zu öffnen.

**2)** Klicken Sie auf *Fingerabdruck des Zertifikats anzeigen*. Ein Fenster mit dem Fingerabdruck des zu importierenden Zertifikats wird angezeigt:

**a)** Überprüfen Sie den Fingerabdruck (Hexadezimalzahl). Wenn das Zertifikat geändert wird, ändert sich immer der Fingerabdruck. Nur ein unveränderter Fingerabdruck ist eine Gewähr für ein unverändertes Zertifikat. Sind die beiden Fingerabdrücke nicht identisch, dann liegt wahrscheinlich ein Angriffsversuch vor. In diesem Fall darf der Schlüssel nicht mehr verwendet werden; darüber hinaus sind die festgelegten Maßnahmen zu ergreifen.

**b)** Klicken Sie auf *OK*, um das Fenster mit dem Fingerabdruck zu schließen.

**3)** Klicken Sie auf *Zertifikat aus Datei importieren*, wenn Sie mit der Prüfung des Fingerabdrucks zufrieden sind. Importieren Sie das Zertifikat nicht, falls der Fingerabdruck nicht Ihren Erwartungen entspricht.

## 3.2.2 Keycert anzeigen

**WBM-Pfad**

*WBM* **>** Konfiguration **>** SPE **>** Keycert anzeigen

Der Dialog *Zertifikatsinformationen* wird angezeigt. In diesem Dialogfeld können Sie das SPE-Zertifikat sehen, z. B. um es zu testen.

**Angezeigte Daten**

Die folgenden Zertifikatsdaten werden angezeigt:

- Allgemeine Daten: *Name des Zertifikats*, *Zertifikatstyp*, *Seriennummer des Zertifikats*, *Seriennummer des Zertifikats (hex)*, *Signatur-Algorithmus-Typ*,

*Beginn der Zertifikatsgültigkeit (GMT)*, *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*
- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name*: *(CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name*: *(CN)*
- *Alternativer Antragstellername*
- *Verschlüsselungsdaten mit öffentlichem Schlüssel*: *Länge des öffentlichen Schlüssels*, *Öffentlicher Schlüssel*, *Fingerabdruck*

## 3.2.3 Keycert löschen

**WBM-Pfad**

*WBM* **>** Konfiguration  SPE **>** Keycert löschen

Der Dialog *Zertifikat für SPE löschen* wird angezeigt. In diesem Dialogfeld können Sie das SPE-Zertifikat entfernen, z. B. wenn ein neues Zertifikat benötigt wird.

**Schaltflächen**

Dieser Dialog enthält folgende Schaltflächen:

- *Löschen*: Das SPE-Zertifikat kann nach einer Warnung gelöscht werden.
- *Abbrechen* Der Löschvorgang wird abgebrochen.

**Vorgehensweise**

Führen Sie die folgenden Schritte aus, um ein SPE-Zertifikat zu entfernen:

**1)** Auswählen: *WBM* **>** Konfiguration SPE **>** Keycert löschen. Eine Warnung wird angezeigt. Zu Prüfzwecken wird außerdem der Name des Zertifikats angegeben.
**2)** Klicken Sie auf *Löschen* und im Bestätigungsdialog auf *OK*.

## 3.2.4 SPE-Sicherheitseinstellung für HFA

**WBM-Pfad**

*WBM* **>** Konfiguration **>** SPE **>** SPE-Sicherheitseinstellung für HFA

Der Dialog *SPE-Sicherheitseinstellung ändern* wird angezeigt. In diesem Dialog können die Sicherheitseinstellungen für Signalling und Payload Encryption (SPE) an die Sicherheitsanforderungen des Kunden angepasst werden. Dies betrifft die Verschlüsselung der Signalisierungs- und der Nutzdaten bei der Kommunikation zwischen der vHG 3500 HFA/vHG 3500 HFA und den VoIP-Clients sowie zwischen zwei vHG 3500 HFA.

**Dropdownlisten, Eingabefelder, Kontrollkästchen**

In diesem Dialog werden folgende Einstellungen angezeigt:

- *Minimale Länge der RSA-Schlüssel*: Sie können *512*, *1024* und *2048*auswählen. Je größer dieser Wert ist, desto sicherer ist der Schlüssel.
- *Maximales Intervall für Schlüssel-Neuverhandlung [Stunden]*: Dieser Wert gibt an, wie lange ein bestimmter Schlüssel für die Verschlüsselung der

Signalisierungs- und Nutzdaten verwendet werden soll. Wenn diese Zeit verstrichen ist, wird ein neuer Schlüssel definiert.

- *Sichere Neuaushandlung erzwingen (RFC 5746)*: Aktivieren durch Kontrollkästchen.
- *TLS-Protokollversion:* Sie können *TLS 1.2 mit Fallback auf TLS 1.0 (Standardeinstellung), Nur TLS 1.0* oder *Nur TLS 1.2 auswählen.*

**TLS 1.2 Chiffrenauswahl**

- *Schlüsselvereinbarung*: Wählen Sie *mit* oder *ohne Perfect Forward Secrecy*.
- *Verschlüsselung*: Wählen Sie *AES-128 mit Fallback* auf AES-256 oder *Nur AES-256.*
- *AES-Betriebsmodus*: Wählen Sie *GCM bevorzugt, mit Fallback auf CBC, Nur GCM* oder *Nur CBC.*

**TLS-Parameter**

- *Zertifikatsprüfungsstufe*: *Keine*, *vertrauenswürdig* oder *vollständig*
- *Zertifikatsprüfung mit CRL-Prüfung erforderlich*: *Aktivieren/Deaktivieren*
- *Prüfung des Antragstellers*: Aktivieren / Deaktivieren

**Schaltflächen**

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Defaultwerte zurückgesetzt.

**Vorgehensweise**

Um die SPE-Sicherheitseinstellungen zu ändern, gehen Sie wie folgt vor:

**1)** Auswählen: *WBM* **>** Konfiguration SPE **>** SPE-Sicherheitseinstellung für HFA. Der Dialog *SPE-Sicherheitseinstellung ändern* wird angezeigt.

**2)** Nehmen Sie die gewünschten Einstellungen vor, siehe Abschnitt âDropdownlisten, Eingabefelder, Kontrollkästchen".

**3)** Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.
Die geänderten Daten werden in die Konfiguration übernommen.

# 4 Wartung

Das Modul *Wartung* stellt Funktionen für die Wartung und Administration der vHG 3500 HFA zur Verfügung. Dazu gehören das Durchführen von Software-Updates, das Sichern der Konfiguration und das Erstellen eines Secure Trace.

**WBM-Pfad**

*WBM* **>** *Wartung*

Das Modul *Wartung* wird geöffnet.

**Auswahlmöglichkeiten im Modul** *Wartung*

**1)** SW-Update Backup/Restore Secure Trace DLS Client

## 4.1 SW-Update

Im Menü *SW-Update* (SW: Software) werden Funktionen zum Anzeigen der Software-Version, für das Software-Update und für die Software-Aktivierung der vHG 3500 HFA zur Verfügung gestellt.

**WBM-Pfad**

*WBM* **>** *Wartung* **>** *SW-Update*

Das Menü *SW-Update* wird geöffnet.

**Menü** *SW-Update*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

**1)** SW-Version anzeigen

### 4.1.1 SW-Version anzeigen

**WBM-Pfad**

*WBM* **>** *Wartung* **>** SW-Update **>** *SW-Version anzeigen*

Der Dialog *Softwareversion* wird angezeigt. Dieser Dialog enthält Details über die momentan installierten Software- und Hardwareversionen.

**Angaben**

Im Einzelnen werden folgende Angaben gemacht:

- System Version (PBX): Dieser Bereich zeigt die OpenScape 4000 Version unter:
- *System Version*
- Plattform Version: Dieser Bereich zeigt an, auf welcher Hardware der vHG 3500 HFA läuft, z.B. OpenScape Access 500. Die Angaben dazu sind:
- *Hardware*, *Platform Deployment*, *Platform Version*, *Importierte Platform Version*, *OS-Update Status*
- SoftGate Version: Dieser Bereich zeigt die installierten Software und Loadwareversionen an. Das sind:
- *Softwareversion*, *Loadwarename*, *Loadwarevariante*, *APS-Version*

- SoftGate Komponentenversionen: Dieser Bereich zeigt die installierten SoftGate-Komponenten ihre Versionen. Das sind:
- *IMS SVN Version*, *SoftGate SVN Version*, *CLA Version*, *Soco-common Version*, *OpenSIPS Version*
- Zusätzliche Packageversionen: Dieser Bereich zeigt zusätzlich benötigte Software und ihre Versionen. Das ist:
- *Java Version*

## 4.2 Backup/Restore

Im Menü *Backup/Restore* kann die Konfiguration und die Sicherheitskonfiguration der vHG 3500 HFA lokal gesichert (exportiert) werden. Diese lokale Sicherung kann geladen (importiert) und anschließend aktiviert werden.

**WBM-Pfad**

*WBM* **>** *Wartung* **>** *Backup/Restore*

Das Menü *Backup/Restore* wird geöffnet.

**Menü** *Backup/Restore*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

**1)** Export Konfiguration Export Sicherheitskonf. Import Konfiguration Import Sicherheitskonf.

### 4.2.1 Export Konfiguration

**WBM-Pfad**

*WBM* **>** *Wartung* **>** Backup/Restore **>** *Export Konfiguration*

Der Dialog *Konfiguration exportieren* wird angezeigt. In diesem Dialog kann die Konfiguration der vHG 3500 HFA lokal gesichert (exportiert) werden.

**Schaltflächen**

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Das Exportieren der Konfiguration wird gestartet.
- *Rückgängig:* Das Exportieren der Konfiguration wird abgebrochen.

**Vorgehen**

Führen Sie zum Exportieren der Konfiguration die folgenden Schritte durch:

**1)** Klicken Sie auf die Schaltfläche *Übernehmen*. Die Konfiguration wird in eine zip-Datei exportiert. Es erscheint ein Fenster *Dateidownload* mit einer Abfrage, ob die zip-Datei geöffnet oder gespeichert werden soll.
**2)** Klicken Sie auf die Schaltfläche *Speichern* und wählen Sie den gewünschten Ordner für die Datei aus. Klicken Sie dann auf die Schaltfläche *OK*. Die zip-Datei wird gespeichert.

## 4.2.2 Export Sicherheitskonf.

**WBM-Pfad**

*WBM* > *Wartung* > Backup/Restore > *Export Sicherheitskonf.*

Der Dialog *Sicherheitskonfiguration exportieren* wird angezeigt. In diesem Dialog kann die Sicherheitskonfiguration der vHG 3500 HFA lokal gesichert (exportiert) werden.

**Schaltflächen**

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Das Exportieren der Sicherheitskonfiguration wird gestartet.
- *Rückgängig:* Das Exportieren der Sicherheitskonfiguration wird abgebrochen.

**Vorgehen**

Führen Sie zum Exportieren der Sicherheitskonfiguration die folgenden Schritte durch:

1) Klicken Sie auf die Schaltfläche *Übernehmen*. Die Sicherheitskonfiguration wird in eine zip-Datei exportiert. Es erscheint ein Fenster *Dateidownload* mit einer Abfrage, ob die zip-Datei geöffnet oder gespeichert werden soll.
2) Klicken Sie auf die Schaltfläche *Speichern* und wählen Sie den gewünschten Ordner für die Datei aus. Klicken Sie dann auf die Schaltfläche *OK*. Die zip-Datei wird gespeichert.

## 4.2.3 Import Konfiguration

**WBM-Pfad**

*WBM* > *Wartung* > Backup/Restore > *Import Konfiguration*

Der Dialog *Konfiguration importieren* wird angezeigt. In diesem Dialog kann die zuvor lokal gesicherte Konfiguration der vHG 3500 HFA wieder importiert werden.

**Eingabefeld**

In diesem Dialog gibt es das folgende Eingabefeld:

- *Dateiname:* In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die zu importierende Konfiguration enthält. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

**Schaltflächen**

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Laden:* Die angegebene Konfigurationsdatei wird geladen.
- *Rückgängig:* Der eingegebene Pfad und der Dateiname werden gelöscht.

**Vorgehen**

Führen Sie zum Importieren einer Konfigurationsdatei die folgenden Schritte durch:

1) Geben Sie den Pfad und den Namen der Konfigurationsdatei ein oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus.
2) Klicken Sie auf die Schaltfläche *Laden*. Die Konfigurationsdatei wird geladen.

---

**IMPORTANT:** Damit alle Konfigurationsänderungen wirksam werden, muss vHG 3500 HFA neu gestartet werden.

---

## 4.2.4 Import Sicherheitskonf.

**WBM-Pfad**

*WBM* **>** *Wartung* **>** Backup/Restore **>** *Import Sicherheitskonf.*

Der Dialog *Sicherheitskonfiguration importieren* wird angezeigt. In diesem Dialog kann die zuvor lokal gesicherte Sicherheitskonfiguration der vHG 3500 HFA wieder importiert werden.

**Eingabefeld**

In diesem Dialog gibt es das folgende Eingabefeld:

- *Dateiname:* In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die zu importierende Sicherheitskonfiguration enthält. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

**Schaltflächen**

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Laden:* Die angegebene Datei wird geladen.
- *Rückgängig:* Der eingegebene Pfad und der Dateiname werden gelöscht.

**Vorgehen**

Führen Sie zum Importieren einer Sicherheitskonfiguration die folgenden Schritte durch:

1) Geben Sie den Pfad und den Namen der Datei ein, welche die zu importierende Sicherheitskonfiguration enthält oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus.
2) Klicken Sie auf die Schaltfläche *Laden*. Die Datei wird geladen.

---

**IMPORTANT:** Damit alle Konfigurationsänderungen wirksam werden, muss vHG 3500 HFA neu gestartet werden.

---

## 4.3 Secure Trace

Ein Secure Trace dient zum Ermitteln von Störungen im Kommunikationssystem. Durch den Secure Trace werden Aufzeichnungen über verschlüsselte VoIP-Nutz- und Signalisierungsdatenströme vom und zum vHG 3500 HFA angefertigt.

Der Secure Trace enthält verschlüsselte Aufzeichnungen. Diese Aufzeichnungen können vom Entwickler durch einen Schlüssel entschlüsselt werden.

### WBM-Pfad

*WBM* > Wartung > Secure Trace

Das Menü *Secure Trace* wird geöffnet.

### Menü *Secure Trace*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

**1)** Zertifikat importieren Zertifikat anzeigen Status Trace starten Trace stoppen

### Prinzipieller Ablauf der Secure Trace-Erstellung

Zum Erstellen eines Secure Trace ist der folgende Ablauf einzuhalten:

**1)** Der Servicetechniker stellt ein Problem im Netzwerk des Kunden fest. In einer Besprechung mit dem Entwickler wird die Notwendigkeit erkannt, einen Secure Trace zu erzeugen.

**2)** Der Kunde wird von der Notwendigkeit informiert und muss bestätigen, dass er informiert wurde. Danach gibt der Kunde eine Bestellung zum Erzeugen eines Secure Trace auf, in der Beginn und Ende (mit Datum und Uhrzeit) der Überwachung genannt sind.

**3)** Die Entwicklung erstellt ein Schlüsselpaar, das aus dem öffentlichen Schlüssel und dem privaten Schlüssel besteht. Mit dem Schlüsselpaar kann nur ein einziger Secure Trace erstellt werden. Die Zertifikate werden folgendermaßen verwendet:

**4)**
- Das Zertifikat mit dem privaten Schlüssel ist streng geheim und kann nur von autorisierten Entwicklern benutzt werden (Whitelist).
- Das Zertifikat mit dem öffentlichen Schlüssel wird an den Servicetechniker übergeben bzw. kann von der HiSat Homepage (https://hisat.global-intra.net/wiki/index.php/SecureTrace) heruntergeladen werden.

**5)** Der Servicetechniker informiert den Kunden über den Beginn der Trace-Aktivitäten. Der Kunde muss die betroffenen Teilnehmer informieren.

---

**IMPORTANT:** Das Aufzeichnen von Gesprächen und Verbindungsdaten ist ein Straftatbestand, wenn die betroffenen Teilnehmer nicht informiert wurden!

---

**1)** Der Servicetechniker stellt den Gateways vHG 3500 HFA, für die ein Secure Trace zu erstellen ist, das Zertifikat zur Verfügung, siehe Abschnitt 4.3.1, "Zertifikat importieren".

**2)** Der Servicetechniker aktiviert die Secure Trace-Funktion, siehe Abschnitt 4.3.4, "Trace starten". Ein Secure Trace wird erstellt. Die Aktivierung und die spätere Deaktivierung (Abschnitt 4.3.5, "Trace stoppen") werden von den beteiligten Kommunikationssystemen protokolliert.

**3)** Nachdem der Secure Trace erstellt wurde, wird der Kunde über das Ende der Trace-Aktivitäten informiert. Der Servicetechniker entfernt das Zertifikat vom System.

**4)** Der Secure Trace wird dem Entwickler zur Verfügung gestellt.

**5)** Der Entwickler entschlüsselt den Secure Trace, indem er den privaten Schlüssel anwendet. Danach analysiert er die entschlüsselten Aufzeichnungen.

6) Nach dem Ende der Analyse müssen alle relevanten Materialien und Daten auf eine sichere Art und Weise zerstört werden. Dies beinhaltet auch das Zerstören des privaten Schlüssels, damit eine eventuell angefertigte unerlaubte Kopie des Secure Trace nicht mehr entschlüsselt werden kann.

## 4.3.1 Zertifikat importieren

**WBM-Pfad**

*WBM* **>** Wartung **>** Secure Trace **>** Zertifikat importieren

Der Dialog *Laden des Secure Trace Zertifikats über HTTP* wird angezeigt. In diesem Dialog kann ein Secure Trace-Zertifikat importiert werden. Dieses Zertifikat ist die Voraussetzung dafür, dass ein Secure Trace erstellt werden kann. Der Servicetechniker bekommt es vom Entwickler. Es enthält den öffentlichen Schlüssel und muss im PEM- oder im binären Format vorliegen. Das Zertifikat ist maximal einen Monat gültig.

**Eingabefeld**

Dieser Dialog enthält das folgende Eingabefeld:

- *Datei mit dem Zertifikat (PEM- oder Binär-Format)*: In dieses Eingabefeld sind der Pfad und der Name der Datei, die das Zertifikat enthält, einzugeben. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

**Schaltflächen**

Dieser Dialog enthält die folgenden Schaltflächen:

- *Fingerabdruck des Zertifikats anzeigen*: Durch Prüfen des Fingerabdrucks kann festgestellt werden, ob ein unverändertes Zertifikat vorliegt oder ob es verändert wurde.
- *Zertifikat aus Datei importieren*: Das Zertifikat wird aus der im oben genannten Eingabefeld angegebenen Datei importiert.

**Vorgehen**

Führen Sie zum Importieren des Zertifikats die folgenden Schritte durch:

1) Wählen Sie: *WBM* **>** Wartung **>** Secure Trace **>** Zertifikat importieren. Der Dialog *Laden des Secure Trace Zertifikats über HTTP* wird angezeigt.
2) Wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus, die das Zertifikat enthält und bestätigen Sie mit *Öffnen*. Die Datei wird geladen.
3) Klicken Sie auf *Fingerabdruck des Zertifikats anzeigen*. Ein Fenster mit dem Fingerabdruck des zu importierenden Zertifikats wird angezeigt:
4) **a)** Prüfen Sie den Fingerabdruck (hexadezimale Zahl). Wenn ein Zertifikat verändert wurde, ändert sich immer der Fingerabdruck. Nur ein unveränderter Fingerabdruck ist eine Gewähr für ein unverändertes Zertifikat. Sind die beiden Fingerabdrücke nicht identisch, dann liegt wahrscheinlich ein Angriffsversuch vor. In diesem Fall darf der Schlüssel nicht mehr verwendet werden; darüber hinaus sind die festgelegten Maßnahmen zu ergreifen.

   Klicken Sie auf *OK*, um das Fenster mit dem Fingerabdruck zu schließen.
5) Klicken Sie auf *Zertifikat aus Datei importieren*, wenn Sie mit der Prüfung des Fingerabdrucks zufrieden sind. Importieren Sie das Zertifikat nicht, falls der Fingerabdruck nicht Ihren Erwartungen entspricht.

Das Erstellen des Secure Trace ist nun möglich.

## 4.3.2 Zertifikat anzeigen

**WBM-Pfad**

*WBM* > Wartung > Secure Trace > Zertifikat anzeigen

Der Dialog *Zertifikatsinformationen* wird angezeigt. In diesem Dialog kann das Secure Trace-Zertifikat angezeigt werden, z.B. um es zu überprüfen.

**Angezeigte Daten**

Es werden die folgenden Daten aus dem Zertifikat angezeigt:

- Allgemeine Daten: *Name des Zertifikats*, *Zertifikatstyp*, *Seriennummer des Zertifikats*, *Seriennummer des Zertifikats (hex)*, *Signatur-Algorithmus-Typ*, *Beginn der Zertifikatsgültigkeit (GMT)*, *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*
- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Alternativer Antragstellername*
- *Daten des öffentl. Schlüssels*: *Länge des öffentl. Schlüssels*, *Öffentlicher Schlüssel*, *Fingerabdruck*

## 4.3.3 Status

**WBM-Pfad**

*WBM* > Wartung > Secure Trace > Status

Der Dialog *Secure Trace Status* wird angezeigt. In diesem Dialog können Sie feststellen, ob gerade ein Secure Trace erstellt wird.

**Angezeigte Daten**

Es werden die folgenden Daten angezeigt:

- *Secure Trace aktiviert*: Diese Zeile zeigt an, ob gerade ein Secure Trace erstellt wird.
- *Automatischer Deaktivierungszeitpunkt*: Diese Zeile zeigt an, wann der Secure Trace voraussichtlich erstellt ist und die Secure Trace-Funktion automatisch deaktiviert wird.
- *Secure Trace für folgende Protokolle*: Diese Zeile zeigt an, für welche Protokolle der Secure Trace erstellt wird. Das kann sein: Media Server (SRTP).

## 4.3.4 Trace starten

**WBM-Pfad**

*WBM* > Wartung > Secure Trace > Trace starten

Der Dialog *Secure Trace einschalten* wird angezeigt. In diesem Dialog kann der Secure Trace gestartet werden. Dazu müssen die folgenden Voraussetzungen vorliegen:

- Der Secure Trace ist noch nicht aktiviert.
- Der Kunde hat die Erstellung des Secure Trace veranlasst und möchte seine *Secure Trace Aktivierungs-Passphrase* in das WBM eingeben.
- Sie haben einen öffentlichen Schlüssel vom Entwickler bekommen und in das WBM geladen.

**Eingabefelder und Kontrollkästchen**

- *Start Parameter*:
- – *Secure Trace Aktivierungs-Passphrase*: Um die Nutzung der Secure Trace-Funktion zu begrenzen, wird die Aktivierung durch eine besondere Passphrase, die nur der Kunde kennt, geschützt. Somit ist diese Passphrase der Schlüssel des Kunden und das Zertifikat der Schlüssel des Servicetechnikers. Beide Schlüssel sind notwendig, um die Secure Trace-Funktion zu aktivieren.

  Eine Passphrase ist ein aus mehreren Wörtern bestehendes Passwort mit einer maximalen Länge von 20 Zeichen.

  – *Dauer des Secure Trace (Min.)*: Das Eingeben der Dauer des Secure Trace (in Minuten) ist unbedingt erforderlich.
- *Secure Trace für folgende Protokolle*:
- – *MediaServer (SRTP)*: Der Secure Trace für MediaServer wird erstellt. Das Protokoll SRTP (Secure Real-Time Transport Protocol) dient der verschlüsselten Übertragung über IP-basierte Netze und verwendet AES (Advanced Encryption Standard) für die Verschlüsselung.

**Schaltfläche**

In diesem Dialog gibt es die folgende Schaltfläche:

- *Secure Trace einschalten*: Der Secure Trace wird gestartet. Die oben genannten Voraussetzungen für das Starten des Secure Trace müssen vorliegen.

**Vorgehen**

Führen Sie zum Starten des Secure Trace die folgenden Schritte durch:

1) Prüfen Sie, ob die oben genannten Voraussetzungen vorliegen.
2) Wählen Sie: *WBM* **>** Wartung **>** Secure Trace **>** Trace starten. Der Dialog *Secure Trace einschalten* wird angezeigt.
3) Geben Sie im Bereich *Start Parameter* die *Secure Trace Aktivierungs-Passphrase* und die *Dauer des Secure Trace (Min.)* ein.
4) Aktivieren Sie das Protokoll *MediaServer (SRTP)*.
5) Klicken Sie auf die Schaltfläche *Secure Trace einschalten*. Der Secure Trace wird für die angegebene Zeitdauer erstellt.

## 4.3.5 Trace stoppen

**WBM-Pfad**

*WBM* **>** Wartung **>** Secure Trace **>** Trace stoppen

Der Dialog *Secure Trace beenden* wird angezeigt. In diesem Dialog kann ein laufender Secure Trace gestoppt werden, wenn die unter Trace starten festgelegte Zeitdauer noch nicht abgelaufen ist.

#### Schaltfläche

In diesem Dialog gibt es die folgende Schaltfläche:

- *Secure Trace beenden*: Der Secure Trace wird gestoppt.

## 4.4 DLS Client

Der DLS-Client dient der Administration von PKI-Daten und der QDC-Konfiguration (DLS: **D**ep**l**oyment **S**ervice oder **D**eployment- und **L**icencing **S**erver, PKI: **P**ublic **K**ey **I**nfrastructure, QDC: **Q**uality of Service **D**ata **C**ollection).

#### WBM-Pfad

*WBM* **>** Wartung **>** DLS Client

Das Menü *DLS Client* wird geöffnet.

#### Menü *DLS Client*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

**1)** DLS Einstellungen PIN Eingabe Bootstrapping zurücksetzen DLS kontaktieren

#### Bootstrapping

Durch das Bootstrapping soll eine auf Zertifikaten basierende zuverlässige SSL-Verbindung zwischen DLS-Server und DLS-Client aufgebaut werden.

Ausgehend von einer Verbindungsanfrage des DLS-Clients an einen DLS-Server sowie der darauffolgenden Antwort â“also einer noch unzuverlässigen Verbindungâ“, wird über die wechselseitige Authentifizierung und den Austausch von Zertifikaten eine zuverlässige Verbindung aufgebaut (d. h. Bootstrapping = ein einfaches System entwickelt sich zu einem komplexen System aus sich selbst heraus).

Da sich auf die Verbindungsanfrage des DLS-Clients anstatt des gewollten DLS-Servers auch ein anderer DLS-Server melden könnte, um die gewünschte Verbindung an sich zu ziehen, sind Sicherungsmaßnahmen notwendig. Mittels AMO kann der DLS-Server (d. h. dessen IP-Adresse und Port) administriert werden, den der DLS-Client kontaktieren soll.

Es wird empfohlen, den DLS-Client gegenüber dem DLS-Server durch Eingeben einer Bootstrap-PIN am WBM des vHG 3500 HFA, die zuvor vom DLS-Server per Zufall generiert wurde, zu autorisieren. Die Autorisierung des DLS-Clients kann auch mit einer nicht einzugebenden systeminternen Standard-PIN erfolgen, oder auf die Autorisierung mittels PIN kann auch ganz verzichtet werden. Diese beiden Möglichkeiten werden jedoch nicht empfohlen.

Nach dem Herstellen der zuverlässigen Verbindung werden die Zertifikate ausgetauscht, s. u.

**Zertifikatsgenerierung und -verteilung für die Kommunikation zwischen DLS-Client und DLS-Server:**

Alle Zertifikate und privaten Schlüssel für die verschlüsselte Kommunikation zwischen DLS-Client und DLS-Server werden durch eine selbst-signierende Zertifizierungsstelle (CA) des DLS-Servers erzeugt und durch den DLS-Server während des Bootstrappings zum DLS-Client gesendet.

Die vom DLS-Server zum DLS-Client gesendete PKCS#12-Datei enthält das DLSC Client-Zertifikat, den darin enthaltenen privaten Schlüssel und das Zertifikat der Zertifizierungsstelle des DLS-Servers (DLSC CA-Zertifikat). Der DLS-Server kann alle von ihm gelieferten Zertifikate zurücklesen, jedoch nicht den privaten Schlüssel.

**Zertifikatsgenerierung und -verteilung für die sichere Verbindung des WBM zum DLS-Server:**

Der Administrator sendet manuell das von der Kunden PKI-Zertifizierungsstelle erstellte WBM-Zertifikat, das den privaten Schlüssel enthält, zum OpenScape 4000 Assistant. Der OpenScape 4000 Assistant sendet dann automatisch sein WBM-Zertifikat zu allen gateways. Mit diesem Zertifikat weist sich dann der DLS-Client gegenüber dem DLS-Server aus.

## 4.4.1 DLS Einstellungen

Außer dem automatischen Registrieren des DLS-Client am DLS-Server mittels der ContactMe-Antwort kann der DLS-Client auch manuell registriert werden. Dafür müssen Ihnen vom DLS-Server die IP-Adresse und der Port für den Bootstrapping-Modus bekannt sein. Die IP-Adresse und der Port des DLS-Servers können mittels AMO konfiguriert werden. Diese Änderung wird erst nach einem Neustart des vHG 3500 HFA wirksam.

Nach Setzen von IP-Adresse und Port des DLS-Servers erfolgt beim Neustart (und jedem weiteren Neustart) ein einmaliger Versuch, durch Senden einer Verbindungsanfrage das Bootstrapping einzuleiten.

Unter dem Menüpunkt *DLS kontaktieren* können manuell weitere Verbindungsversuche eingeleitet werden. Falls noch kein Bootstrapping durchgeführt wurde, wird dies dabei automatisch eingeleitet, andernfalls wird lediglich geprüft, ob der DLS erreichbar ist.

**WBM-Pfad**

*WBM* **>** Wartung **>** *DLS Client* **>** *DLS Einstellungen*

Der Dialog *DLS Client Grundeinstellung ändern* wird geöffnet.

**Eingabefeld**

Im Bereich *Aktuelle DLS Client Grundeinstellung* gibt es folgendes Eingabefeld:

- *Zeitintervall für ContactMe-Antwort*: Zeit, die der DLS-Client nach Absenden seiner Verbindungsanfrage wartet, um die ContactMe-Antwort vom DLS-Server zu erhalten. Die Wartezeit muss begrenzt sein, damit ContactMe-Antworten von ungewollten DLS-Servern nicht empfangen werden können.

**Anzeigen**

In diesem Dialog gibt es die folgenden Anzeigen:

- *Aktuelle DLS Client Grundeinstellung*:
- – *PIN für DLS-Bootstrapping erforderlich*: Die PIN kann unter dem Menüpunkt *PIN Eingabe* eingegeben werden. *Ja*: Es wurde eine PIN eingegeben. *Nein*: es wurde keine PIN eingegeben.
  – *Sichere Kommunikation mit DLS-Server*: *Aktiviert* oder *Deaktiviert*
- *Aktuelle DLS Client Server Einstellung*:
- – *IP-Adresse des DLS-Servers*: IP-Adresse des DLS-Servers für den Bootstrapping-Modus kann mittels AMO konfiguriert werden. Ein Neustart des vHG 3500 HFA ist erforderlich.
  – *Port des DLS-Servers*: Port des DLS-Servers für den Bootstrapping-Modus kann mittels AMO konfiguriert werden. Ein Neustart des vHG 3500 HFA ist erforderlich.
  – *Port für sichere Verbindung zum DLS-Server*: Port des vHG 3500 HFA für eine sichere Verbindung zum DLS-Server

**Schaltflächen**

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.

## 4.4.2 PIN Eingabe

**WBM-Pfad**

*WBM* **>** Wartung **>** *DLS Client* **>** *PIN Eingabe*

Der Dialog *Eingabe der Bootstrap PIN* wird geöffnet. In diesem Dialog kann die vom DLS-Server per Zufall generierte Bootstrap PIN eingegeben werden.

**Eingabefeld**

In diesem Dialog gibt es folgendes Eingabefeld:

- *Bootstrap PIN*: Wenn in dieses Eingabefeld eine PIN eingegeben und durch Klicken auf *Übernehmen* gespeichert wurde, wird im Dialog *DLS Client Grundeinstellung ändern* (Menüpunkt *DLS Einstellungen*) angezeigt, dass für das DLS-Bootstrapping eine PIN erforderlich ist.

**Schaltflächen**

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.

## 4.4.3 Bootstrapping zurücksetzen

**WBM-Pfad**

*WBM* **>** Wartung **>** *DLS Client* **>** *Bootstrapping zurücksetzen*

Der Dialog *DLS Client Bootstrapping zurücksetzen* wird geöffnet.

**Schaltfläche**

In diesem Dialog gibt es die folgende Schaltfläche:

- *Bootstrapping zurücksetzen*: Das Bootstrapping des DLS-Clients wird zurückgesetzt.

## 4.4.4 DLS kontaktieren

Unter dem Menüpunkt *DLS kontaktieren* können manuell weitere Verbindungsversuche zum DLS-Server eingeleitet werden. Falls noch kein Bootstrapping durchgeführt wurde, wird dies dabei automatisch eingeleitet, andernfalls wird lediglich geprüft, ob der DLS erreichbar ist.

**WBM-Pfad**

*WBM* **>** Wartung **>** *DLS Client* **>** *DLS kontaktieren*

Der Dialog *DLS kontaktieren* wird geöffnet.

**Menü *DLS kontaktieren***

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

**1)** DLSC Client-Zertifikate DLSC CA-Zertifikate

**Dialog *DLS kontaktieren***

In diesem Dialog gibt es folgende Schaltfläche:

- *Kontaktieren*: Der DLS-Server wird kontaktiert, um zu überprüfen, ob er noch verfügbar ist.

### 4.4.4.1 DLSC Client-Zertifikate

Unter diesem Menüpunkt befinden sich die DLSC Client-Zertifikate mit dem privaten Schlüssel. Mit diesen Zertifikaten weist sich der DLS-Client gegenüber dem DLS-Server aus. Während des Bootstrapping-Modus bekommt der DLS-Client das Zertifikat vom DLS-Server.

**WBM-Pfad**

*WBM* **>** Wartung **>** *DLS Client* **>** *DLSC Client-Zertifikate*

Das Menü *DLSC Client-Zertifikate* wird geöffnet.

**Menü** *DLSC Client-Zertifikate*

Unter diesem Menüpunkt sind die einzelnen DLSC Client-Zertifikate auswählbar:

1. DLSC Client-Zertifikat

### 4.4.4.2 1. DLSC Client-Zertifikat

**WBM-Pfad**

*WBM* **>** Wartung **>** *DLS Client* **>** *DLSC Client-Zertifikate* **>** *1. DLSC Client-Zertifikat*

Der Dialog *Zertifikatsinformationen* wird geöffnet.

**Angezeigte Daten**

Es werden die folgenden Daten aus dem Zertifikat angezeigt:

- Allgemeine Daten: *Zertifikatstyp*, *Seriennummer des Zertifikats*, *Seriennummer des Zertifikats (hex)*, *Signatur-Algorithmus-Typ*, *Beginn der Zertifikatsgültigkeit (GMT)*, *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*
- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Alternativer Antragstellername*
- *Daten des öffentl. Schlüssels*: *Länge des öffentl. Schlüssels*, *Öffentlicher Schlüssel*, *Fingerabdruck*

### 4.4.4.3 DLSC CA-Zertifikate

Dieser Ordner enthält die vom DLS-Server während des Bootstrapping-Modus gelieferten DLSC CA-Zertifikate.

**WBM-Pfad**

*WBM* **>** Wartung **>** *DLS Client* **>** *DLSC CA-Zertifikate*

Das Menü *DLSC CA-Zertifikate* wird geöffnet.

**Menü** *DLSC CA-Zertifikate*

Unter diesem Menüpunkt sind die einzelnen DLSC Client-Zertifikate auswählbar:

â1. CA-Zertifikat", â2. CA-Zertifikat"

### 4.4.4.4 â1. CA-Zertifikat", â2. CA-Zertifikat"

**WBM-Pfad**

*WBM* **>** Wartung **>** *DLS Client* **>** *DLSC Client-Zertifikate* **>** *â1. CA-Zertifikat", â2. CA-Zertifikat"*

Der Dialog *Zertifikatsinformationen* wird geöffnet.

**Angezeigte Daten**

Es werden die folgenden Daten aus dem Zertifikat angezeigt:

- Allgemeine Daten: *Zertifikatstyp*, *Seriennummer des Zertifikats*, *Signatur-Algorithmus-Typ*, *Beginn der Zertifikatsgültigkeit (GMT)*, *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*
- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Alternativer Antragstellername*
- *Daten des öffentl. Schlüssels*: *Länge des öffentl. Schlüssels*, *Öffentlicher Schlüssel*, *Fingerabdruck*

# 5 Hilfe

Im Modul *Hilfe* werden Informationen über das WBM angezeigt.

**WBM-Pfad**

*WBM* **>** *Hilfe*

# 6 Abmelden

Nach Klicken auf *Abmelden* wird die Verbindung zur vHG 3500 HFA beendet und die WBM-Sitzung geschlossen.

**WBM-Pfad**

*WBM* **>** *Abmelden*

# Index

## V



## W



## Z