1 IPsec-VPN-Verbindung zwischen Android-Client und mGuard-Gerät herstellen

Dokument-ID: 108394_de_00
Dokument-Bezeichnung: AH DE MGUARD ANDROID SUPPORT

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

Inhalt dieses Dokuments

In diesem Dokument werden die notwendigen Schritte zur Konfiguration einer VPN-Verbindung zwischen einem Android-Client (Tablet-PC oder Mobiltelefon mit Android OS Version 6.0) mit einem mGuard-Server beschrieben.

1.1 Einleitung

Das Android-Gerät dient als Remote-Client zur Initialisierung der IPsec-VPN-Verbindung. Der mGuard übernimmt die Funktion des lokalen Servers sowie zur Konfiguration und Bereitstellung des lokalen Netzwerkes für die Clients über die XAuth/Mode-Config-Erweiterung.

Für die VPN-Verbindungen ist die Installation von X.509-Zertifikaten und Schlüsseln sowohl bei dem Android-Client als auch dem mGuard-Gerät erforderlich.

Allgemeine Informationen zur Konfiguration von VPN-Verbindungen finden Sie unter „Software-Referenzhandbuch – mGuard-Firmware“, online verfügbar oder im PHOENIX CONTACT Webshop unter: phoenixcontact.net/products. Weiterführende Informationen zum Android-Client finden Sie auf den entsprechenden Webseiten des Herstellers.

Das Aussehen der Einstellungen und Bedienoberflächen unterscheidet sich deutlich bei Android-Geräten unterschiedlicher Modelle und Hersteller. Das vorliegende Dokument wurde auf Grundlage des Geräts *SAMSUNG SM-T580* mit installierter Android-Version 6.0.1 erstellt.

1.1.1 Anforderungen

- mGuard-Gerät mit installierter Firmware ab Version 8.5
- Android-Gerät mit installierter Firmware ab Version 6.0
- Sämtliche erforderlichen und signierten Zertifikate

Wie erstelle ich X.509-Zertifikate?

Weiterführende Informationen zur Zertifikatsverwaltung finden Sie als Anwenderhinweis in dem Dokument „AH DE MGUARD APPNOTES“, verfügbar im PHOENIX CONTACT Webshop unter: phoenixcontact.net/products.

1.1.2 Haftungsausschluss

Dieses Dokument stellt keinen Ersatz für die Anwenderhandbücher der betreffenden Produkte dar.

1.2 Zertifikate verwalten

Für den Aufbau einer IPsec-VPN-Verbindung zwischen einem Android-Client und einem mGuard-Server müssen sich die Geräte über X.509-Zertifikate gegenseitig authentifizieren.

Tabelle 1-1 Erforderliche Zertifikate

Gerät	Erforderliches Zertifikat	Format
mGuard	CA-Zertifikat	**PEM / CER**
	mGuard-Maschinenzertifikat (von CA signiert)	**PKCS#12**
Android-Client	mGuard-Maschinenzertifikat (von CA signiert)	**PEM / CER**
	Android-Client-Zertifikat (von CA signiert)	**PKCS#12**

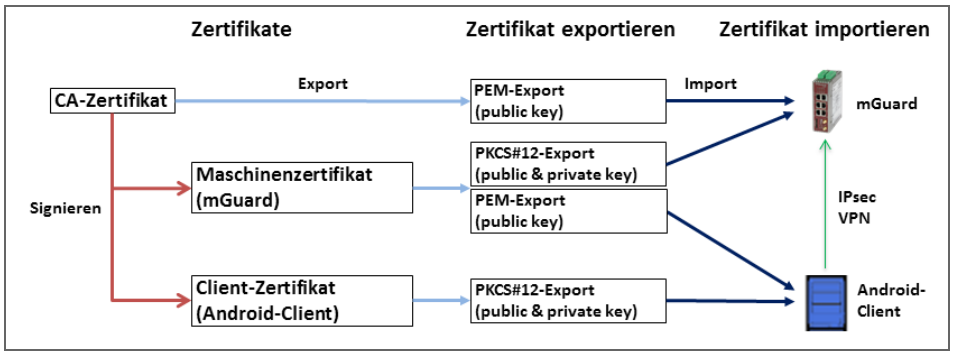


Bild 1-1 Zertifikathandhabung für Verbindungen mit Initialisierung durch **Android-Clients**

Die Begriffe „Maschinenzertifikat“ und „Client-Zertifikat“ bezeichnen ein X.509-Zertifikat und den zugehörigen privaten Schlüssel (*private key*), über den sich die Maschine bzw. der Client gegenüber den Gegenstellen identifiziert.

1.2.1 Erforderlichen Zertifikate auf dem mGuard-Gerät

Die folgenden Zertifikate müssen auf dem mGuard-Gerät installiert werden:

1. **CA-Zertifikat (PEM / CER)**

   Der mGuard überprüft die Echtheit des Android-Clients auf Grundlage der CA-Signatur des vorgezeigten Android-Client-Zertifikats.

2. **mGuard-Maschinenzertifikat (PKCS#12)**

   Der **Android-Client** überprüft die Echtheit des mGuards auf Grundlage des vorgezeigten mGuard-Maschinenzertifikats. Das mGuard-Maschinenzertifikat muss daher auch auf dem Android-Client installiert sein.

1.2.2 Erforderliche Zertifikate auf dem Android-Client

Die folgenden Zertifikate müssen auf dem Android-Gerät installiert werden (siehe auch Seite 3):

1. **mGuard-Maschinenzertifikat (PEM/CER)**

   Der Android-Client überprüft die Echtheit des mGuard-Servers auf Grundlage des vorgezeigten mGuard-Maschinenzertifikats.

2. **Android-Client-Zertifikat (PKCS#12)**

   Der mGuard überprüft die Echtheit des Android-Clients auf Grundlage der CA-Signatur des vorgezeigten Android-Client-Zertifikats. Das signierende CA-Zertifikat muss daher auf dem mGuard installiert sein.

1.2.3 Zertifikate auf dem mGuard-Gerät installieren

Maschinenzertifikat

Zum Hochladen des mGuard-Maschinenzertifikats auf den mGuard gehen Sie wie folgt vor:

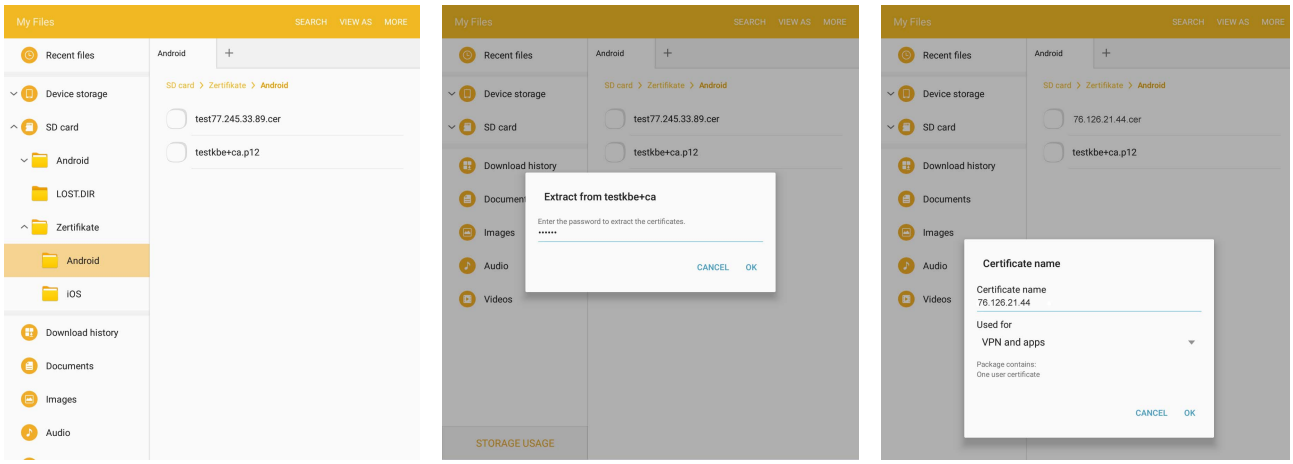
1. Wählen Sie **Authentifizierung >> Zertifikate >> Maschinenzertifikate**.
2. Klicken Sie auf das Icon ⊕, um eine neue Tabellenzeile zu erstellen.
3. Klicken Sie auf das Icon 🗀.
4. Wählen Sie das Maschinenzertifikat aus (PKCS#12-Datei), und klicken Sie auf „Öffnen“.
5. Geben Sie das Passwort ein, mit dem der geheime Schlüssel des Zertifikats gesichert wurde.
6. Klicken Sie auf die Schaltfläche „Hochladen“.
   ► Das hochgeladene Zertifikat erscheint in der Zertifikate-Liste.
7. Klicken Sie auf das Icon 💾, um die Einstellungen zu speichern.
   ► Das mGuard-Maschinenzertifikat wurde hochgeladen und kann zur Authentifizierung gegenüber dem Android-Client verwendet werden (siehe “mGuard konfigurieren” , Registerkarte „Authentifizierung“).

CA-Zertifikat

Zum Hochladen des CA-Zertifikats auf den mGuard gehen Sie wie folgt vor:

1. Wählen Sie **Authentifizierung >> Zertifikate >> CA-Zertifikate**.
2. Klicken Sie auf das Icon ⊕, um eine neue Tabellenzeile zu erstellen.
3. Klicken Sie auf das Icon 🗀.
4. Wählen Sie das CA-Zertifikat aus (PEM- oder CER-Datei), und klicken Sie auf „Öffnen“.
5. Klicken Sie auf die Schaltfläche „Hochladen“.
   ► Das hochgeladene Zertifikat erscheint in der Zertifikate-Liste.
6. Klicken Sie auf das Icon 💾, um die Einstellungen zu speichern.
   ► Das CA-Zertifikat wurde hochgeladen und kann zur Authentifizierung des Android-Client verwendet werden (siehe “mGuard konfigurieren” , Registerkarte „Authentifizierung“).

1.2.4 Zertifikate auf dem Android-Client installieren



Zur Installation des **Android-Client-Zertifikats** (PKCS#12-Datei mit signierendem CA-Zertifikat) und des **mGuard-Maschinenzertifikats** (PEM-/CER-Datei) auf dem Android-Client gehen Sie wie folgt vor:

1. Um die VPN-Funktion auf dem Android-Gerät nutzen zu können, müssen Sie das Bildschirm-Sperrmuster, den PIN oder das Passwort setzen.
2. Stellen Sie die Zertifikatsdateien auf dem Android-Client zur Verfügung.
3. Öffnen Sie die PKCS#12-Datei (**.p12),* um den Android-Client und die signierenden CA-Zertifikate zu extrahieren und zu installieren.
   ► Das Fenster „Zertifikat extrahiere“ erscheint.

   Falls das Fenster nicht erscheint und das Gerät stattdessen den Inhalt der Datei anzeigt, laden Sie die Datei in den Speicher Ihres Geräts herunter oder stellen sie über eine SD-Karte zur Verfügung. Öffnen Sie die Datei in dem entsprechenden Verzeichnis.
4. Geben Sie das Passwort ein, und klicken Sie auf „OK“.
   ► Das Fenster „Zertifikatsname“ erscheint.
5. Optional: Weisen Sie dem Zertifikat einen neuen Namen zu, um das Zertifikat einfacher in der Zertifikate-Liste finden zu können.
6. Klicken Sie auf „OK“, um die Installation des Android-Client-Zertifikats und des signierenden CA-Zertifikats zu beenden.
   ► Die installierten Zertifikate erscheinen in der Zertifikate-Liste des Anwenders (Einstellungen >> Gerätesicherheit >> Andere Sicherheitseinstellungen >> Benutzerzertifikate).
7. Öffnen Sie die PEM- oder CER-Datei (**.pem / *.cer*), um das mGuard-Maschinenzertifikat zu installieren.
   ► Das Fenster „Zertifikatsname“ erscheint.

   Falls das Fenster nicht erscheint und das Gerät stattdessen den Inhalt der Datei anzeigt, laden Sie die Datei in den Speicher Ihres Geräts herunter oder stellen sie über eine SD-Karte zur Verfügung. Öffnen Sie die Datei in dem entsprechenden Verzeichnis.
8. Klicken Sie auf „OK“, um die Installation des mGuard-Maschinenzertifikats zu beenden.

► Das installierte Zertifikat erscheint in der Zertifikate-Liste des Anwenders (Einstellungen >> Gerätesicherheit >> Andere Sicherheitseinstellungen >> Benutzerzertifikate).

1.3 VPN-Verbindungen konfigurieren

1.3.1 mGuard konfigurieren

Die IPsec-VPN-Verbindung zwischen Android-Client und mGuard wird über die Erweiterung „XAuth/Mode Config“ hergestellt.

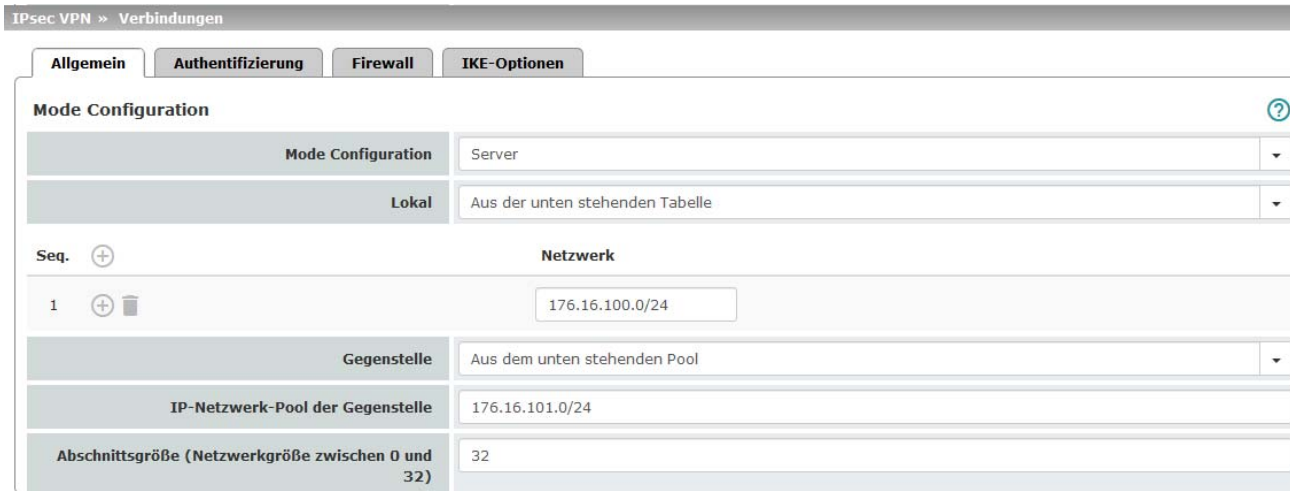


Bild 1-2 mGuard VPN-Konfiguration – Mode Configuration

1.3.1.1 Registerkarte „Allgemein“

Zur Konfiguration einer VPN-Verbindung zum Android-Client auf dem mGuard gehen Sie wie folgt vor:

1. Wählen Sie **IPsec VPN >> Verbindungen >> Allgemein**.
2. Klicken Sie auf das Icon ⊕, um eine neue Tabellenzeile zu erstellen.
3. Klicken Sie auf das Icon ✎.
   ► Die Registerkarte „**Allgemein**“ erscheint.
4. Geben Sie einen beschreibenden Namen für die Verbindung ein, und ändern Sie optional weitere Einstellungen.

   Überprüfen Sie, ob das Eingabefeld „Adresse des VPN-Gateways der Gegenstelle“ den Wert „**%any**“ enthält und „Verbindungsinitiierung“ auf „**Warte**“ gesetzt ist (Standardwerte).

5. **Mode Configuration**: Wählen Sie die Option „**Server**“.
6. **Lokal**: Geben Sie alle lokalen Netzwerke (1 oder mehrere) auf Server-Seite (mGuard) ein, auf die über die VPN-Verbindung durch den Android-Client zugegriffen werden soll.
   – **Fest**: Das *„Lokale IP-Netzwerk“* muss auf 0.0.0.0/0 gesetzt werden. In diesem Fall wird der gesamte Datenverkehr vom Android-Client über die VPN-Verbindung übertragen.

– **Aus der unten stehenden Tabelle**: Nur der Datenverkehr zu den in der *unten stehenden Tabelle* aufgelisteten Netzwerken wird über die VPN-Verbindung übertragen.

Bei Android-Clients wird die Funktion „*Aus der unten stehenden Tabelle*“ nicht vollständig unterstützt. **Datenverkehr** von Android-Clients zu Netzwerken, die nicht in der *unten stehenden Tabelle* definiert sind, **wird blockiert!**

7. **Gegenstelle**: Definieren Sie den Netzwerk-Pool (**Aus dem unten stehenden Pool**), aus dem der mGuard einen variablen Abschnitt (**Abschnittsgröße**) zur Nutzung durch das Netzwerk des Remote-Clients zuweist.

1.3.1.2 Registerkarte „Authentifizierung“

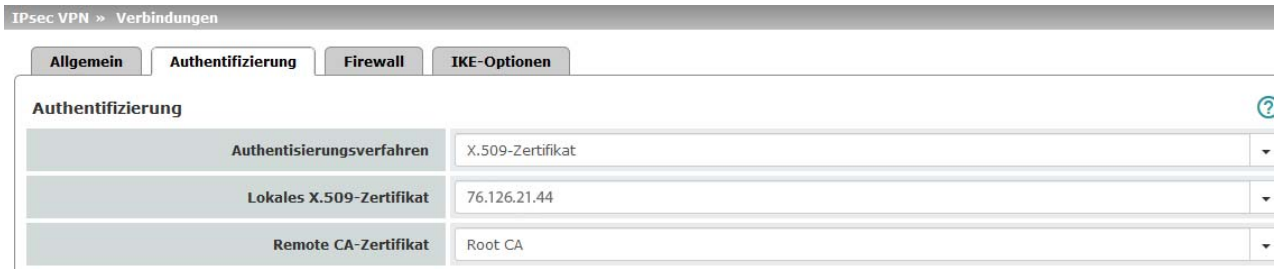


Bild 1-3 mGuard VPN-Konfiguration – Authentifizierung

Die VPN-Verbindung zwischen einem Android-Client und dem mGuard muss durch X.509-Zertifikate autorisiert werden, die auf den entsprechenden Geräten installiert werden müssen (siehe „Zertifikate verwalten“ auf Seite 3).

Um der VPN-Verbindung die erforderlichen Zertifikate zuzuweisen, gehen Sie wie folgt vor:

1. Wählen Sie **IPsec VPN >> Verbindungen**.
2. Bearbeiten Sie die gewünschte VPN-Verbindung (Registerkarte „Authentifizierung“).
3. Wählen Sie „**Authentisierungsverfahren**: X.509 Certificate“.
4. Wählen Sie als *„Lokales X.509-Zertifikat“* das **mGuard-Maschinenzertifikat**.

   Das lokale Zertifikat muss mit dem CA-Zertifikat signiert worden sein, das auf dem Android-Client installiert wurde.

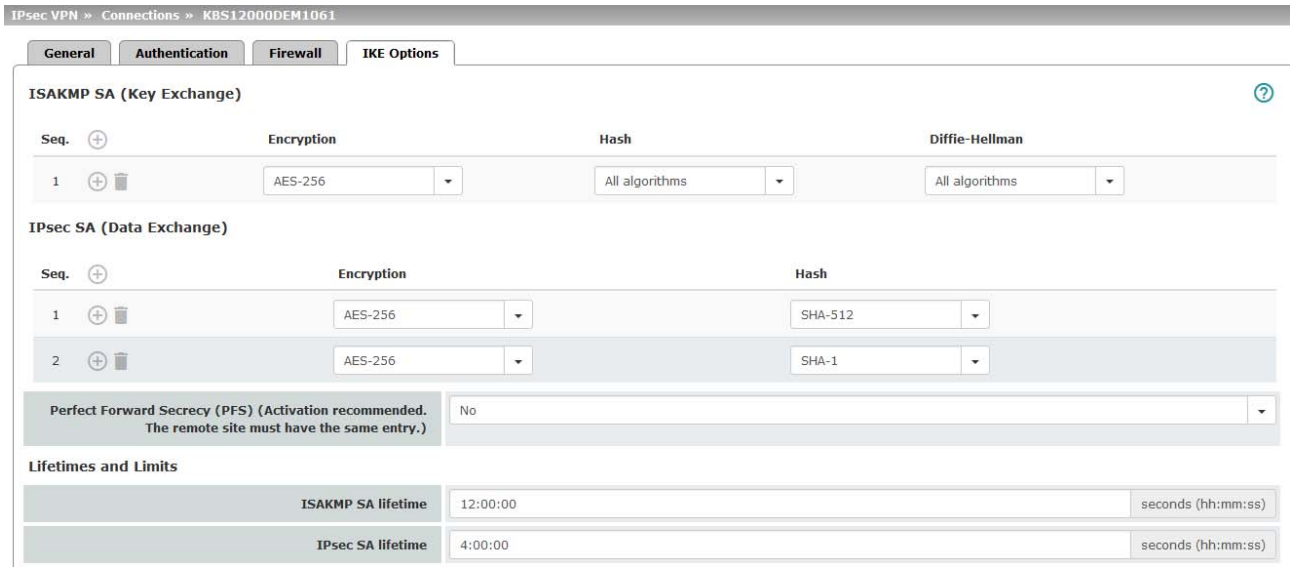
5. Wählen Sie als *„Remote CA-Zertifikat“* den Namen des CA-Zertifikats das zum Signieren des **Android-Client-Zertifikat** verwendet wurde.
6. Klicken Sie auf auf das Icon , um die Einstellungen zu speichern.
   ► Die VPN-Verbindung wird nach einer Initialisierung durch den Client hergestellt.

1.3.1.3 Registerkarte „Firewall“

Die VPN-Firewall beschränkt den Zugriff über den VPN-Tunnel. Sie können die VPN-Firewall bei Bedarf konfigurieren.

In der werkseitigen Voreinstellung wird **jeglicher eingehender** und **ausgehender** Datenverkehr zugelassen**.**

1.3.1.4 Registerkarte „IKE-Optionen“



Die werkseitig voreingestellten IKE-Optionen müssen geändert werden:

1. Wählen Sie **IPsec VPN >> Verbindungen**.
2. Bearbeiten Sie die gewünschte VPN-Verbindung (Registerkarte „IKE-Optionen“).
3. Konfigurieren Sie die folgenden Einstellungen (und behalten Sie bei allen anderen Einstellungen die werkseitige Voreinstellung bei).

ISAKMP-SA (Schlüsselaustausch)

- Verschlüsselung: AES-256
- Prüfsumme: Alle Algorithmen
- Diffie-Hellman: Alle Algorithmen

IPsec-SA (Datenaustausch)

- Klicken Sie auf das Icon ⊕, um zwei Tabellenzeilen zu erzeugen und die folgenden Einstellungen zu verwenden:
  - (Zeile 1) Encryption: AES-256 | Hash: SHA-512
  - (Zeile 2) Encryption: AES-256 | Hash: SHA-1

Perfect Forward Secrecy (PFS)

- Die PFS muss deaktiviert werden.

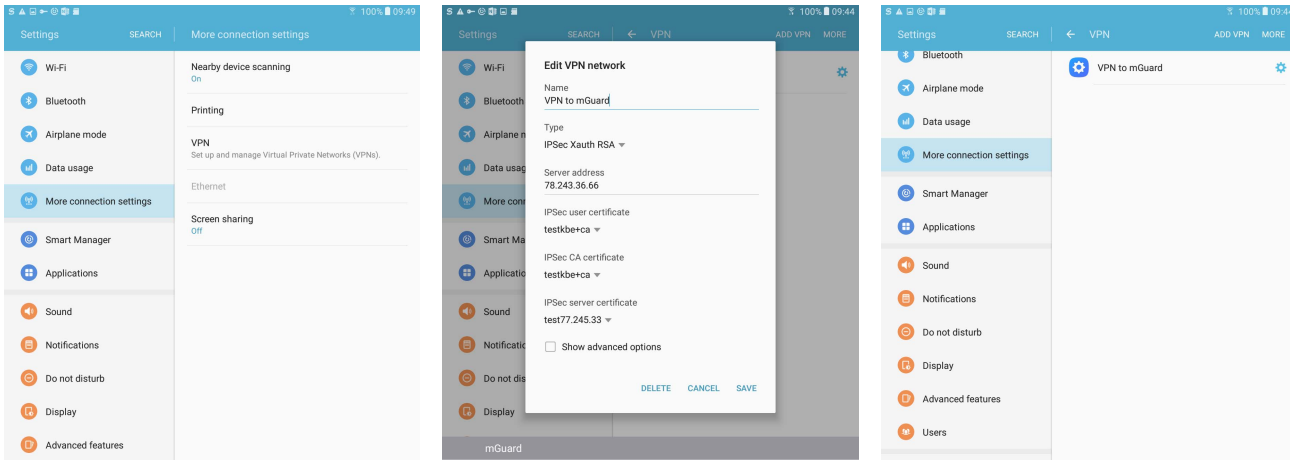
ISAKMP-SA-Lebensdauer

- 12:00:00 (hh:mm:ss)

IPsec-SA-Lebensdauer

- 04:00:00 (hh:mm:ss)

1.3.2 Android-Client konfigurieren



Um eine IPsec-VPN-Verbindung auf dem Android-Client zu konfigurieren, gehen Sie wie folgt vor:

1. Wählen Sie das „Einstellungen >> Weitere Verbindungseinstellungen >> VPN“.
2. Klicken Sie auf „VPN HINZUFÜGEN “ oder „+“.
   ► Das Fenster „VPN hinzufügen“ erscheint.
3. Konfigurieren Sie folgende Einstellungen:
   – *Name*: Ein beschreibender Name für die Verbindung
   – *Typ*: IPSec Xauth RSA
   – *Server-Adresse*: Die externe IP-Adresse oder der DNS-Name des mGuard-Servers
   – *IPSec-Benutzerzertifikat*: Wählen Sie den Namen, den Sie dem Android-Client-Zertifikat aus der PKCS#12-Datei zugewiesen haben.
   – *IPSec-CA-Zertifikate*: Wählen Sie den Namen, den Sie dem Android-Client-Zertifikat aus der PKCS#12-Datei zugewiesen haben.
   – *IPSec-Serverzertifikat*: Wählen Sie den Namen, den Sie dem mGuard-Maschinenzertifikat des mGuard-Servers (VPN-Gateway) zugewiesen haben.
4. Klicken Sie auf „SPEICHERN“, um die Konfiguration zu speichern.
   ► Die VPN-Verbindung ist nun gespeichert und kann gestartet werden.

1.4 VPN-Verbindungen auf dem Android-Client starten

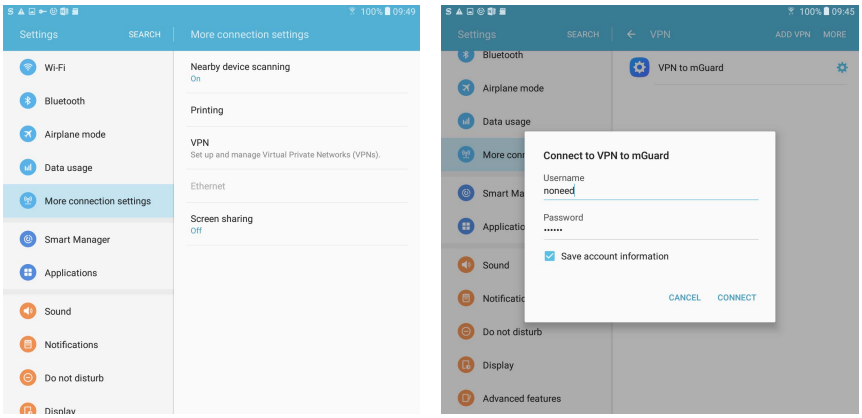


Bild 1-4 VPN-Verbindung auf dem Android-Client starten

Zum Starten einer IPsec-VPN-Verbindung auf dem Android-Client gehen Sie wie folgt vor:

1. Wählen Sie „Einstellungen >> Weitere Verbindungseinstellungen >> VPN“.
2. Klicken Sie auf den Namen der entsprechenden VPN-Verbindung.
   ► Das Fenster „Mit <Verbindungsname> verbinden“ erscheint.

> Benutzername und Passwort für XAuth werden durch den mGuard ignoriert. Geben Sie eine kurze, beliebige Zeichenfolge ein, und speichern Sie die Kontoinformationen.

3. Klicken Sie auf „VERBINDEN“, um die Verbindung herzustellen.
   ► Die VPN-Verbindung wird hergestellt, und der Status ändert sich von „Nicht verbunden “ zu „Verbinden...“ und anschließend zu „Verbunden“.

> Wenn die Verbindung fehlschlägt, klicken Sie auf das „Zahnrad“-Icon der VPN-Verbindung, um die Konfiguration auf Fehler oder den Status Ihrer Internetverbindung zu überprüfen.

1.5 VPN-Verbindungen auf dem mGuard überprüfen

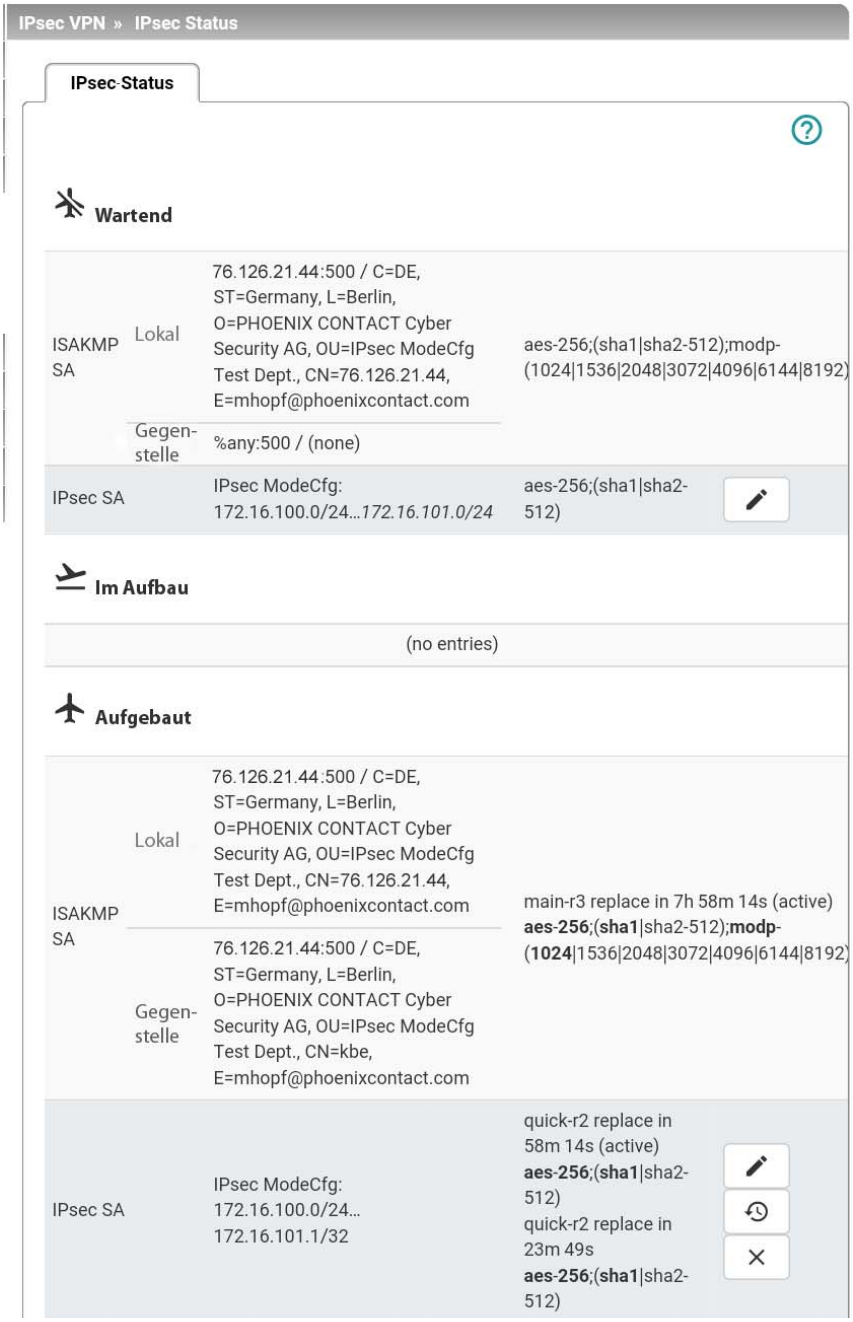


Bild 1-5 IPsec-VPN-Status

Zur Überprüfung des Status einer IPsec-VPN-Verbindung gehen Sie wie folgt vor:

- Wählen Sie **IPsec VPN >> IPsec-Status**.
  - ► Eine hergestellte IPsec-VPN-Verbindung wird im Bereich „Aufgebaut“ angezeigt.