

15 IPsec-VPN-Verbindung zwischen iOS-Client und mGuard-Gerät herstellen



Dokument-ID: 108393_de_02
 Dokument-Bezeichnung: AH DE MGUARD IOS SUPPORT
 © PHOENIX CONTACT 2022-10-27



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 iOS-Client (iPad oder iPhone mit iOS ab Version 8.0) und einem mGuard-Gerät (Server) beschrieben.

15.1	Einleitung.....	115
15.2	Zertifikate verwalten	116
15.3	VPN-Verbindungen konfigurieren	122
15.4	VPN-Verbindungen auf dem iOS-Client starten	127
15.5	VPN-Verbindungen auf dem mGuard überprüfen	128

15.1 Einleitung

Das iOS-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 iOS-Client als auch dem mGuard-Gerät erforderlich

Anforderungen

- mGuard-Gerät mit installierter Firmware ab Version 8.5
- iOS-Gerät mit installierter Firmware ab Version 8.0
- 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.

15.2 Zertifikate verwalten

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

Tabelle 15-1 Erforderliche Zertifikate

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

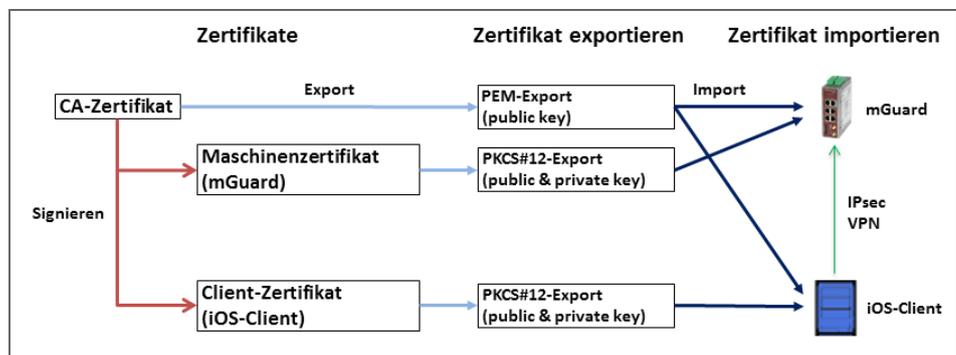


Bild 15-1 Zertifikatsverwaltung für Verbindungen mit Initialisierung durch iOS-Clients

15.2.1 Erforderliche 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 iOS-Clients auf Grundlage der CA-Signatur des vorgezeigten iOS-Client-Zertifikats.
- 2. mGuard-Maschinenzertifikat (PKCS#12)**
Der iOS-Client überprüft die Echtheit des mGuards auf Grundlage der CA-Signatur des mGuard-Maschinenzertifikats. Das signierende CA-Zertifikat muss daher auf dem iOS-Client installiert sein.



ACHTUNG: Die Netzwerkadresse des mGuard-Geräts muss im Zertifikat eingetragen werden

Bei der Erstellung des mGuard-Maschinenzertifikats muss an zwei Stellen die IP-Adresse (oder der Hostname/DNS-Name) eingetragen werden, die der iOS-Client zum Aufbau einer VPN-Verbindung mit dem mGuard-Gerät verwendet (in der Regel die externe Server-IP-Adresse des mGuard-Geräts):

- 1. commonName (CN)** --> siehe Bild 15-2 und Bild 15-3
- 2. X509v3 Subject Alternative Name** --> siehe Bild 15-4

IPsec-VPN-Verbindung zwischen iOS-Client und mGuard-Gerät herstellen

Netzwerk » Interfaces

Allgemein Extern Intern DMZ Sekundäres externes Interface

Netzwerk-Status

Externe IP-Adresse	76.126.21.44
Aktive Standard-Route über	10.0.0.253
Benutzte DNS-Server	Kein

Netzwerk-Modus

Netzwerk-Modus	Router
Router-Modus	Statisch

Netzwerk » Interfaces

Allgemein **Extern** Intern DMZ Sekundäres externes Interface

Externe Netzwerke

Seq.	IP-Adresse	Netzmaske	VLAN verwenden	VLAN-ID
1	76.126.21.44	255.255.255.0	<input type="checkbox"/>	1

Zusätzliche externe Routen

Seq.	Netzwerk	Gateway
+		

Bild 15-2 (Beispiel) Netzwerkeinstellungen am mGuard: Externe IP-Adresse hervorgehoben

Verwaltung Authentifizierung » Zertifikate

Netzwerk

Zertifikateinstellungen **Maschinenzertifikate** CA-Zertifikate Gegenstellen-Zertifikate CRL

Maschinenzertifikate

Seq.	Kurzname	Informationen zum Zertifikat
1	76.126.21.44	<p>Herunterladen <input type="checkbox"/> PKCS#12-Passwort Hochladen</p> <p>Subject: CN=76.126.21.44 OU=TR,O=KBS Incorporation,C=DE</p> <p>Aussteller: CN=KBS12000DE-CA,OU=TR,O=KBS Incorporation,C=DE</p> <p>Gültig von: Sep 8 09:29:20 2016 GMT</p> <p>Gültig bis: Sep 14 09:29:20 2044 GMT</p> <p>Fingerabdruck MD5: E0:84:25:DD:58:27:D0:41:27:E0:6A:16:F4:CF:24:27</p> <p>Fingerabdruck SHA1: 3D:20:14:B1:B7:5C:39:65:CE:D3:CB:2F:A8:F2:7C:11:BF:90</p>

Bild 15-3 Maschinenzertifikat: CN = Externe IP-Adresse oder Hostname/DNS-Name des mGuards

X Certificate and Key management

Create x509 Certificate

Source Subject **Extensions** Key usage Netscape Advanced

X509v3 Basic Constraints

Type: End Entity
Path length:

Key Identifier

Subject Key Identifier
 Authority Key Identifier

Validity

Not before: 2017-07-13 07:59 GMT
Not after: 2018-07-10 14:44 GMT

Time range

2 Years

Midnight Local time No well-defined expiration

X509v3 Subject Alternative Name ✓ IP: 76.125.21.44

X509v3 Issuer Alternative Name

X509v3 CRL Distribution Points

Authority Information Access: OCSP

Bild 15-4 Maschinenzertifikat: Beispiel (XCA) – X509v3 Subject Alternative Name

15.2.2 Erforderliche Zertifikate auf dem iOS-Client

Die folgenden Zertifikate müssen auf dem iOS-Gerät installiert werden (siehe auch Seite 116):

1. CA-Zertifikat (PEM/CER)

Der iOS-Client überprüft die Echtheit des mGuard-Servers auf Grundlage der CA-Signatur des vorgezeigten mGuard-Maschinenzertifikats.

2. iOS-Client-Zertifikat (PKCS#12)

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



Da der iOS-Client die Schlüsselkette (*keychain*) einer PKCS#12-Datei ignoriert, muss das signierende CA-Zertifikat separat auf dem mGuard installiert werden.

15.2.3 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 iOS-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 iOS-Client verwendet werden (siehe “mGuard konfigurieren” , „Registerkarte „Authentifizierung““).

15.2.4 Zertifikate auf dem iOS-Client installieren

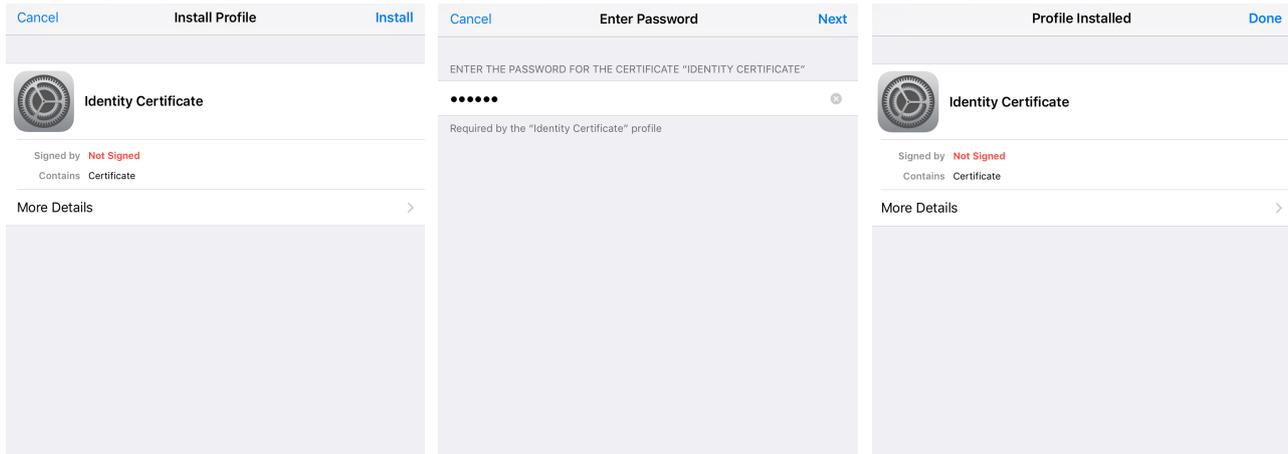


Bild 15-5 Installation der Client-Zertifikate



Bild 15-6 Installierte Zertifikate in der Zertifikate-Liste

Zur Installation des **iOS-Client-Zertifikats** oder des **CA-Zertifikats** auf dem iOS-Client gehen Sie wie folgt vor:

1. Stellen Sie das Zertifikat auf dem iOS-Client zur Verfügung.
2. Öffnen Sie die Datei.
 - ▶ Das Fenster „Identitätszertifikat“ wird angezeigt.
3. Klicken Sie zwei Mal auf „Installieren“.
 - ▶ Wenn das Zertifikat mit einem geheimen Schlüssel (PKCS#12-Dateien) gesichert wurde, wird das Fenster „Passwort“ angezeigt.
4. Geben Sie in diesem Fall das Passwort ein.
5. Klicken Sie auf „Weiter“.
 - ▶ Das Fenster „Profil installiert“ wird angezeigt.
6. Klicken Sie auf „Fertig“, um die Installation des Zertifikats zu beenden.
 - ▶ Das installierte Zertifikat erscheint in der Zertifikate-Liste.

15.3 VPN-Verbindungen konfigurieren

15.3.1 mGuard konfigurieren

Die IPsec-VPN-Verbindung zwischen iOS-Client und mGuard wird über die Erweiterung „XAuth/Mode Config“ hergestellt. Die Konfiguration des iOS-Clients erfolgt über den mGuard und wird dem iOS-Client mitgeteilt.

The screenshot shows the 'Mode Configuration' tab in the mGuard VPN configuration interface. The interface is titled 'IPsec VPN » Verbindungen'. It has four tabs: 'Allgemein', 'Authentifizierung', 'Firewall', and 'IKE-Optionen'. The 'Allgemein' tab is active. The 'Mode Configuration' section includes a dropdown menu for 'Mode Configuration' set to 'Server' and a dropdown for 'Lokal' set to 'Aus der unten stehenden Tabelle'. Below this is a table for 'Netzwerk' with one entry: '1' with a plus icon, a trash icon, and the IP address '176.16.100.0/24'. Below the table are fields for 'Gegenstelle' (set to 'Aus dem unten stehenden Pool'), 'IP-Netzwerk-Pool der Gegenstelle' (set to '176.16.101.0/24'), and 'Abschnittsgröße (Netzwerkgröße zwischen 0 und 32)' (set to '32').

Bild 15-7 mGuard VPN-Konfiguration – Mode Configuration

15.3.1.1 Registerkarte „Allgemein“

Zur Konfiguration einer VPN-Verbindung zum iOS-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 „Verbindungsinitiiierung“ 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 iOS-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 iOS-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 iOS-Clients wird bei Datenverkehr zu Netzwerken, die nicht in der *unten stehenden Tabelle* aufgelistet sind, die VPN-Verbindung umgangen (**Bypass**).

IPsec-VPN-Verbindung zwischen iOS-Client und mGuard-Gerät herstellen

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.

15.3.1.2 Registerkarte „Authentifizierung“

IPsec VPN » Verbindungen

Allgemein Authentifizierung Firewall IKE-Optionen

Authentifizierung 

Authentisierungsverfahren	X.509-Zertifikat	▼
Lokales X.509-Zertifikat	76.126.21.44	▼
Remote CA-Zertifikat	Root CA	▼

Bild 15-8 mGuard VPN-Konfiguration – Authentifizierung

Die VPN-Verbindung zwischen einem iOS-Client und dem mGuard muss durch X.509-Zertifikate autorisiert werden, die auf den entsprechenden Geräten installiert werden müssen (siehe „Zertifikate verwalten“ auf Seite 116).

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**.



Der *Common Name (CN)* und der *Subject Alternative Name* des Zertifikats müssen mit der IP-Adresse (oder dem Hostnamen/DNS-Namen) des mGuard-Geräts übereinstimmen, die der iOS-Client zum Aufbau einer VPN-Verbindung mit dem mGuard-Gerät verwendet (siehe Kapitel 15.2.1).



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

5. Wählen Sie als „*Remote CA-Zertifikat*“ den Namen des CA-Zertifikats das zum Signieren des **iOS-Client-Zertifikats** 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.

15.3.1.3 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.

15.3.1.4 Registerkarte „IKE-Optionen“

IPsec VPN » Connections » KBS12000DEM1061

General Authentication Firewall **IKE Options**

ISAKMP SA (Key Exchange) ?

Seq.	Encryption	Hash	Diffie-Hellman
1	AES-256	All algorithms	All algorithms

IPsec SA (Data Exchange)

Seq.	Encryption	Hash
1	AES-256	SHA-512
2	AES-256	SHA-1

Perfect Forward Secrecy (PFS) (Activation recommended. The remote site must have the same entry.) No

Lifetimes and Limits

ISAKMP SA lifetime	12:00:00	seconds (hh:mm:ss)
IPsec SA lifetime	4:00:00	seconds (hh:mm:ss)

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

15.3.2 iOS-Client konfigurieren

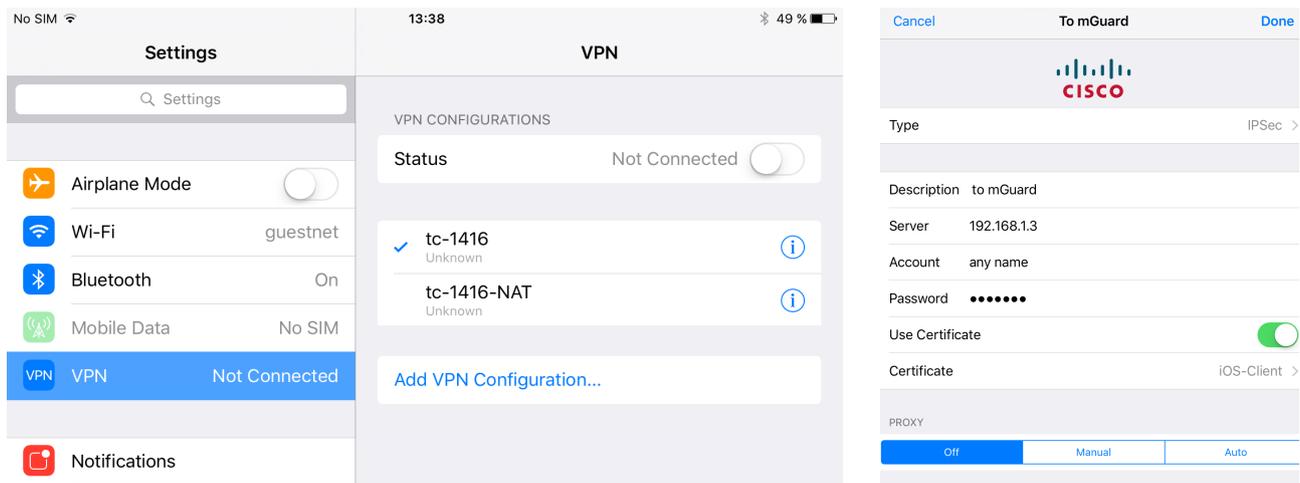


Bild 15-9 iOS-Client: VPN-Konfiguration

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

1. Wählen Sie „Einstellungen >> VPN“.
2. Klicken Sie auf „VPN hinzufügen“.
3. Klicken Sie auf „Typ“.
4. Wählen Sie „IPsec“, und wechseln Sie anschließend zur Konfigurations-Seite.
5. Füllen Sie folgende Eingabefelder aus:
 - *Beschreibung*: Ein beschreibender Name für die VPN-Verbindung
 - *Server*: Externe IP-Adresse oder Hostname/DNS-Name des mGuard-Servers



Diese IP-Adresse bzw. dieser Hostname/DNS-Name muss mit dem *Common Name (CN)* und dem *Subject Alternative Name* des mGuard-Maschinenzertifikats übereinstimmen (siehe Kapitel 15.2.1).

- *Account*: Die Authentifizierung von VPN-Gegenstellen ist von Zertifikaten abhängig. Daher werden der Name und das Passwort des Kontos **durch den mGuard ignoriert**. Geben Sie einen beliebigen Text ein, um weitere Anfragen zu vermeiden.
 - *Passwort*: Das Passwort wird **durch den mGuard ignoriert**. Geben Sie einen beliebigen Text ein.
 - *Zertifikat verwenden*: Aktivieren Sie den Schalter, um ein Zertifikat auszuwählen.
6. Klicken Sie auf „Zertifikat“.
 - ▶ Eine Liste mit allen installierten Zertifikaten erscheint.
 7. Wählen Sie das entsprechende Client-Zertifikat aus, und klicken Sie auf „Zurück“.
 8. Klicken Sie auf „Fertig“, um die Konfiguration zu speichern.
 - ▶ Die VPN-Verbindung ist nun gespeichert und kann gestartet werden.

15.4 VPN-Verbindungen auf dem iOS-Client starten

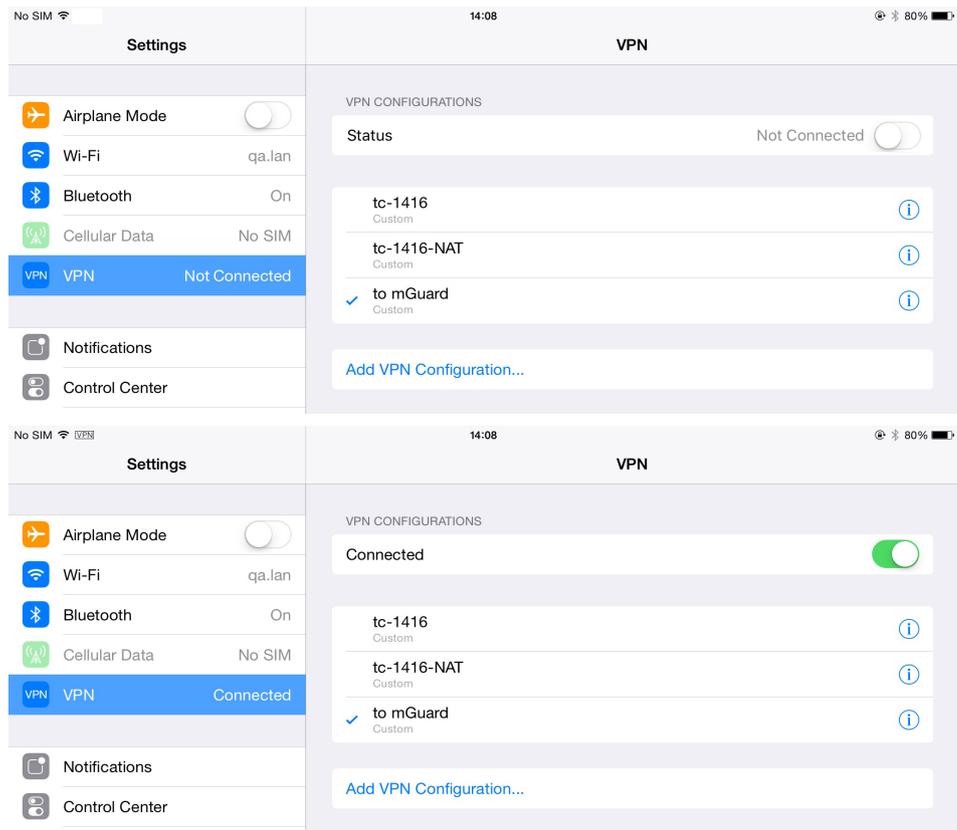


Bild 15-10 VPN-Verbindung auf dem iOS-Client starten

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

1. Wählen Sie „Einstellungen >> VPN“.
2. Klicken Sie auf den Namen der entsprechenden VPN-Verbindung.
3. Klicken Sie im Bereich „VPN CONFIGURATIONEN“ auf die Schaltfläche „Nicht verbunden“.
 - ▶ Die VPN-Verbindung wird hergestellt, und der Status ändert sich von „Nicht verbunden“ zu „Verbunden“.



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

15.5 VPN-Verbindungen auf dem mGuard überprüfen

IPsec VPN » IPsec Status

IPsec Status ?

 **Wartend**

ISAKMP SA	Lokal	76.126.21.44:500 / C=DE, ST=Germany, L=Berlin, O=PHOENIX CONTACT Cyber Security AG, OU=IPsec ModeCfg Test Dept., CN=76.126.21.44, E=mhopf@phoenixcontact.com	aes-256;(sha1 sha2-512);modp-(1024 1536 2048 3072 4096 6144 8192)	
	Gegenstelle	%any:500 / (none)		
IPsec SA		IPsec ModeCfg: 172.16.100.0/24...172.16.101.0/24	aes-256;(sha1 sha2-512)	

 **Im Aufbau**

(no entries)

 **Aufgebaut**

ISAKMP SA	Lokal	76.126.21.44:500 / C=DE, ST=Germany, L=Berlin, O=PHOENIX CONTACT Cyber Security AG, OU=IPsec ModeCfg Test Dept., CN=76.126.21.44, E=mhopf@phoenixcontact.com	main-r3 replace in 7h 58m 14s (active) aes-256;(sha1 sha2-512);modp-(1024 1536 2048 3072 4096 6144 8192)	
	Gegenstelle	76.126.21.44:500 / C=DE, ST=Germany, L=Berlin, O=PHOENIX CONTACT Cyber Security AG, OU=IPsec ModeCfg Test Dept., CN=kbe, E=mhopf@phoenixcontact.com		
IPsec SA		IPsec ModeCfg: 172.16.100.0/24...172.16.101.1/32	quick-r2 replace in 58m 14s (active) aes-256;(sha1 sha2-512) quick-r2 replace in 23m 49s aes-256;(sha1 sha2-512)	  

Bild 15-11 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.