VPN - Tutorial

Stationäres eHealth-Kartenterminal ORGA 6141 online und ORGA Neo ab Firmware 3.9.2



Inhaltsverzeichnis

1. Version Historie 3
2. Herausgeber / Editor 4
3. Copyrights....4
4. Motivation 5
5. Mitgeltende Dokumente....5
6. Systemvoraussetzung 5
7. Kartenterminal 6
8. Konfiguration des Kartenterminals 6
   Konfiguration über die lokalen Menüfunktionen am eHKT 6
   Aktivierung des VPN-Tunnels 6
   Status des VPN-Tunnels bei IPSec 7
   Status des VPN-Tunnels bei WireGuard 7
   Informationen zu Zugangsdaten bei IPSec....8
   Erzeugung eines Certification-Signing-Request (CSR) bei IPSec....9
9. Ablauf des USB Import / Export....12
   Use Case: Import 12
   Use Case: Export 12
   Import der Konfigurationsdatei....13
   Konventionen zum Dateinamen....13
10. Unterstützte Parameter 14
11. Beschreibung der wesentlichen VPN-Client Parameter....15
   Beispiele für den USB-Stick Import / Export 17
12. Konfiguration über das Remote Management Interface (RMI) 22
   Vorbemerkungen zur VPN-Konfiguration....22
13. Konfiguration über die Web-Applikation zum Remote Management Interface (RMI) 30
   Erstellen einer WireGuard VPN-Konfiguration....30
   Erstellen einer StrongSwan VPN-Konfiguration über die Web-Applikation 33
14. VPN SICCT Unicast Adresse (optional) 36
15. Konfigurationen im Testumfeld....37
   VPN-Gateway 38
   Kartenterminal....39
16. Erstellung und Umwandlung eines PKCS#12-Containers 40
17. Quellenverweise 43

Version Historie

Version	Datum	Editor	Änderung zur Vorgängerversion
0.1	12.01.2021	THS	• Initial
0.2	25.01.2021	THS	• Korrekturen und Bilder ergänzt
0.3	25.01.2021	THS	• Korrekturen
0.4	28.01.2021	THS	• Erläuterungen bzgl. der base64-Kodierung von Zertifikaten
0.5	14.07.2021	THS	• Ergänzung für FW V3.8.1 • Authentisierung mit Public-Key
0.6	19.8.2021	THS	• Aktualisierung der Public-Key Beispiel
22.1	22.12.2021	JBA	• Redaktionelle Korrekturen • Worldline Schema
23.10.1	12.10.2023	THE	• Ergänzungen für FW v3.9.x
23.10.2	13.10.2023	MPE	• Review und Ergänzungen
23.10.2	18.10.2023	JBA	• Umsetzen ins WL-Design • UseCase Import aktualisiert
23.11.1	03.11.2023	MPE	• Review, Verweise, Referenzen • Umgestaltung des Dokumentenaufbaus
23.11.2	13.11.2023	JBA	• Vorbemerkungen zur VPN-Konfiguration hinzugefügt
23.12.1	14.12.2023	THE	• Erläuterung bzgl. Authentifizierungsmethode PSK ohne CA-Zertifikat
24.05.1	06.05.2024	KPF	• Layout
24.12.1	16.12.2024	THE	• Ergänzungen zur FW v3.9.1 – WireGuard
25.4.1	02.04.2025	JBA	• Ergänzungen zur FW v3.9.1 – VPN-Konfiguration von WireGuard und IPSec/IKEv2 über die Web-Applikation
25.6.1	02.06.2025	JBA	• Anpassung des VPN-Konfigurationsprozesses an die finale Firmwareversion
25.6.2	10.06.2025	JBA	• VPN-Prozess: Review mit finalen Anpassungen

Herausgeber / Editor

Worldline Healthcare GmbH
Konrad-Zuse-Ring 1
24220 Flintbek
WEEE DE 32266764

Tel.: 04347 90 11 111
E-Mail: kontakt.whc@worldline.com
Internet: www.worldline.com/de/healthcare

Copyrights

Copyright© 2023/2024/2025
Worldline Healthcare GmbH - Alle Rechte vorbehalten.
Alle Produkte oder Dienstleistungen, die in diesem Dokument genannt werden, sind Marken, Dienstleistungsmarken, eingetragene Marken oder eingetragene Dienstleistungsmarken der entsprechenden Eigentümer.

Kein Teil dieser Dokumentation darf ohne schriftliche Genehmigung der Worldline Healthcare GmbH kopiert, gesendet, übertragen, elektronisch gespeichert oder in eine andere Sprache übersetzt werden.

Die Worldline Healthcare GmbH behält sich das Recht auf die Änderung von Funktionen, Eigenschaften und technischen Angaben zu jeder Zeit und ohne vorherige Benachrichtigung vor.

Motivation

Das stationäre eHealth-Kartenterminal ORGA 6141 online unterstützt seit der Firmwareversion 3.8.0 den Aufbau einer VPN-Netzwerkverbindung bzw. eines VPN-Tunnels nach IPSec/IKEv2[i]. Mit der Firmwareversion 3.9.1 ist optional das WireGuard[ii] VPN-Protokoll mit aufgenommen worden. Dieses Tutorial dient als Leitfaden für die Erstellung und das Importieren der entsprechenden Konfigurationen ins Kartenterminal sowie für die Aktivierung der VPN-Netzwerkverbindung ab der Firmwareversion 3.9.x.

Darüber hinaus wird in diesem Tutorial der Im- & Export von weiteren Konfigurationseinstellungen erklärt.

Mitgeltende Dokumente

Folgende Dokumente beinhalten ebenfalls wichtige Informationen zum Aufbau und zur Aktivierung von VPN-Verbindungen inklusive der Wertebereichen der einzelnen Parameter:

- Bedienungsanleitung ORGA 6141 online[3] [AGD]
- Dokumentation Remote Management Interface ORGA 6141 online[4] [RMI]

Die jeweils aktuelle Version finden Sie auf unserer Homepage unter:

ORGA Neo | Worldline Deutschland

Systemvoraussetzung

Für die Erstellung einer VPN-Verbindung werden folgende Hard- und Software-Komponenten benötigt:

VPN-Gateway

- **IPsec-Server (z.B. StrongSwan[iii])**
  - öffentlich zugängliche IP-Adresse bzw. Domainnamen
  - offene Netzwerk-Ports 500 und 4500
  - Unterstützung der Authentifizierungsmethoden PreSharedKey (PSK), EAP-MSCHAPv2 zur Authentifizierung der Clients mittels Benutzername- / Kennung, Passwort, EAP-TLS und Public-Key
  - Routing von Broadcast-Nachrichten
- **WireGuard-Server**
  - öffentlich zugängliche IP-Adresse bzw. Domainnamen
  - offene Netzwerk-Ports (entsprechend der verwendeten Konfiguration)
  - Terminal Hardwareversion >= v2.0.0



Hinweis
Die Konfiguration des **VPN-Gateways** wird in diesem Tutorial nicht näher beschrieben und obliegt dem **Administrator** des **VPN-Gateways**.

Hinweise können dem Kapitel Konfigurationen im Testumfeld - Seite 30 entnommen werden.

Kartenterminal

- **IPsec-Client (z.B. strongSwan[iv])**
  - Benutzername- / Kennung und Passwort, den PSK oder ein entsprechendes Client-Zertifikat
  - CA-Zertifikat des VPN-Gateways (bei PSK optional)
  - USB-Stick für dem Import der erstellten Konfiguration
  - Uhrzeit setzen via NTP

Wird kein CA-Zertifikat für die Authentifizierungsmethode PSK konfiguriert, wird der Pre-Shared Key auch für die serverseitige Authentifizierung verwendet.

- **WireGuard-Client**
  - Zugang zum Remote-Management-Interface für die Konfiguration
  - Konfigurationsdatei

Wie die aktuell im Kartenterminal hinterlegten Zugangsdaten ausgelesen werden können, erfahren Sie im Kapitel Informationen zu Zugangsdaten - Seite 8.

Konfiguration des Kartenterminals

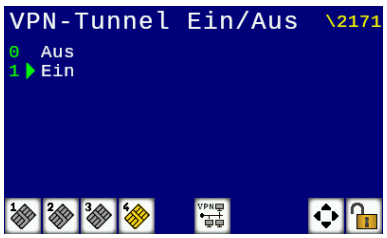
Die Konfiguration des Kartenterminals inkl. des VPN-Clients kann über das lokale Gerätemenü in Kombination mit einem Datenimport über einen USB-Stick oder direkt über das Remote-Management-Interface (RMI) bzw. die Web-Browser Applikation erfolgen.

> **Hinweis**
> Die Konfiguration von WireGuard steht nur über die Web-Applikation bzw. per RMI-Interface zur Verfügung.

In diesem Dokument wird der Fokus zwar auf die, für die VPN-Client-Konfiguration erforderlichen, Parameter gelegt, jedoch ermöglichen die neuen Bezeichner (siehe Unterstützte Parameter - Seite 13) der Konfigurationsdatei eine deutlich erweiterte, an das Remote Management Interface angelehnte Konfiguration über den USB-Stick oder das RMI-Interface.

Konfiguration über die lokalen Menüfunktionen am eHKT

Aktivierung des VPN-Tunnels

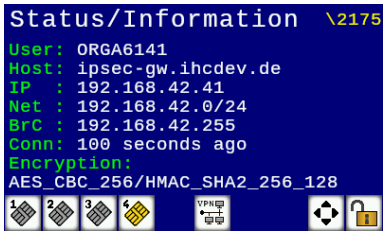


Für die Aktivierung des VPN-Tunnels gehen Sie ins Menü [*IPSec VPN* \217]. Sind alle benötigten Daten für die jeweilige Authentifizierungsmethode vorhanden, können Sie den Tunnel einschalten.

Nach Aktivierung verändert sich zudem das Status-Icons der Netzwerkverbindung in der Anzeige.

Diese werden mit dem Zusatz [VPN] versehen. Ein orangefarbener Schriftzug zeigt an, dass der VPN-Tunnel aktiviert wurde, aber zurzeit keine Verbindung besteht. Bei einem schwarzen Schriftzug wurde der Tunnel aufgebaut und die Verbindung besteht. Bzgl. WireGuard steht diese Funktionalität, nach erfolgter Konfiguration über die Web-Applikation bzw. per RMI-Interface, ebenfalls zur Verfügung.

Status des VPN-Tunnels bei IPSec

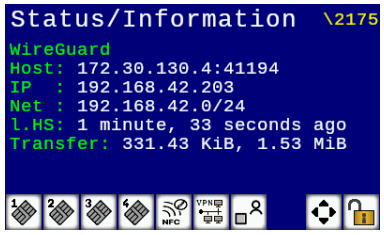


Der Status des VPN-Tunnels kann am Kartenterminal unter [Einstellungen/LAN Parameter/VPN Konfiguration/Status/Information \2175] während des Betriebes eingesehen werden.

Angezeigt werden im Betrieb mit strongSwan:

- **User** Benutzername- / Kennung bzw. Authentifizierungsmethode
- **Host** URL / Adresse des VPN-Gateways
- **IP** eigene IP im VPN
- **Net** VPN-Netzwerk
- **BrC** ermittelte Broadcast-Adresse
- **Conn** Dauer der Verbindung bzw. ob gerade eine Verbindung im Aufbau ist
- **Encrypt.** ausgehandelte Verschlüsselungsmethoden

Status des VPN-Tunnels bei WireGuard



Der Status des WireGuard VPN-Tunnels kann am Kartenterminal unter [Einstellungen/LAN Parameter/VPN/Konfiguration/Status/ Information \2175] während des Betriebes ebenfalls eingesehen werden. Der aktuelle Status kann ebenfalls über die Web-Applikation unter Info oder per RMI-Interface abgefragt werden.

Angezeigt werden im Betrieb mit WireGuard:

- **Host** URL / Adresse des VPN-Gateways
- **IP** eigene IP im VPN
- **Net** VPN-Netzwerk
- **l.HS** Zeitpunkt des letzten Handshake der VPN-Verbindung
- **Transfer** empfangenes und gesendetes Datenvolumen

Im Falle eines Fehlers bzw. einer Störung wird…



… im Display bei IPSec folgendes angezeigt:

- **User** Benutzername- / Kennung bzw. Authentifizierungsmethode
- **Host** URL / Adresse des VPN-Gateways
- **Error** Fehlerbeschreibung

> **Hinweis**
> Bei Verwendung von WireGuard steht eine Fehlerbeschreibung nicht zur Verfügung

Informationen zu Zugangsdaten bei IPSec



Unter dem Menüpunkt [Einstellungen/LAN Parameter/VPN/ Konfiguration/Zugangsdaten/ Info zu den Zugangsdaten \21741] können Informationen bzgl. der aktuell verwendeten Zugangsdaten abgefragt werden.

Angezeigt werden im Betrieb:



- **Host** URL / IP des VPN-Gateways
- **Cert** Common Name (CN) des Client-Zertifikates
- **Cert-CXD** Ablaufdatum des Client-Zertifikates
- **Cert-#** Seriennummer des Client-Zertifikates
- **CACert** Common Name (CN) des CA-Zertifikates
- **CACert-CXD** Ablaufdatum des CA-Zertifikates
- **CACert-#** Seriennummer des CA-Zertifikates

Bei Verwendung von WireGuard steht diese Funktionalität nicht zur Verfügung.

Erzeugung eines Certification-Signing-Request (CSR) bei IPSec



Soll die Authentifizierung mittels Public-Key erfolgen, kann für das Clientzertifikat ein entsprechender Schlüssel generiert werden. Aus Gründen der Sicherheit generiert das Kartenterminal diesen Schlüssel selbst und erzeugt einen CSR für die Erstellung eines Clientzertifikates durch die herausgebende Stelle des VPN-Betreibers.



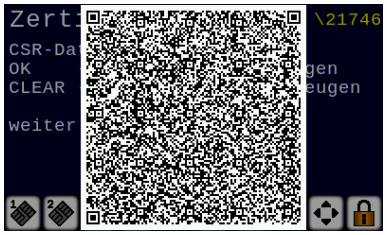
Mit Menüpunkt [21746] wird die Erzeugung eines CSR gestartet. Ist kein zuvor generierter Schlüssel vorhanden, wir automatisch ein **ECC-Schlüssel auf Basis der „brainpool256r1“-Kurve** generiert. Andernfalls erfolgt eine Auswahl



Wird der vorhandene Schlüssel erneut gewählt und es existiert bereits ein CSR, erfolgt eine weitere Auswahl.

Als X509-Subjekt für den CSR werden standardmäßig folgende Werte gesetzt:

- C = DE
- ST = Schleswig-Holstein
- L = Flintbek
  = Worldline Healthcare GmbH
- CN = (Seriennummer des Kartenterminals)@orga6141.online



Zum Schluss wird der CSR per QR-Code angezeigt. Der im QR-Code enthaltene CSR kann entweder eingescannt bzw. über das RMI (net_vpn_client_csr) abgefragt und für die Erstellung eines Clientzertifikates durch die herausgebende Stelle des VPN-Betreibers benutzt werden.

Das erstellte Clientzertifikat wird anschließend per USB-Stick oder über das RMI (net_vpn_client_certificate) ins Kartenterminal importiert.

Hinweis
Bei Verwendung von WireGuard steht eine Fehlerbeschreibung nicht zur Verfügung

CSR-Daten:

```
$ openssl req -text -in csr_file
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = DE, ST = Schleswig-Holstein, L = Flintbek, O = Worldline Healthcare GmbH, CN =
01400000003144@orga6141.online
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:1f:27:07:5b:51:b2:3d:ea:f0:2a:14:36:45:3c:
                    01:bd:17:c3:11:89:2b:b5:06:e3:0d:9c:7d:76:0f:
                    75:b9:13:09:3a:af:4f:b8:d5:02:35:62:bd:f1:72:
                    0a:96:d2:bb:fe:a7:8a:12:f1:6e:41:bd:d5:85:37:
                    eb:13:4c:c3:9a
                ASN1 OID: brainpoolP256r1
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                email:01400000003144@orga6141.online
    Signature Algorithm: ecdsa-with-SHA256
         30:44:02:20:2c:f9:db:c9:ad:60:83:e7:bf:8a:ae:37:09:18:
         1a:a8:f9:fa:39:ce:e3:2c:8b:21:ac:39:ad:e3:46:3a:3b:13:
         02:20:42:83:a5:f9:12:13:58:34:3f:b1:f2:9d:9e:21:c3:e5:
         2f:91:13:c7:a3:82:67:82:a9:6b:0c:b7:89:e8:8e:6f
-----BEGIN CERTIFICATE REQUEST-----
MIIBgzCCASoCAQAwgYoxCzAJBgNVBAYTAkRFMRswGQYDVQQIDBJTY2hsZXN3aWct
SG9sc3RlaW4xETAPBgNVBAcMCEZsaW50YmVrMSIwIAYDVQQKDBlXb3JsZGxpbmUg
SGVhbHRoY2FyZSBHbWJIMScwJQYDVQQDDB4wMTQwMDAwMDAwMzE0NEBvcmdhNjE0
MS5vbmxpbmUwWjAUBgcqhkjOPQIBBgkrJAMDAggBAQcDQgAEHycHW1GyPerwKhQ2
RTwBvRfDEYkrtQbjDZx9dg91uRMJOq9PuNUCNWK98XIKltK7/qeKEvFuQb3VhTfr
E0zDmqA8MDoGCSqGSIb3DQEJDjEtMCswKQYDVR0RBCIwIIEeMDE0MDAwMDAwMDMx
NDRAb3JnYTYxNDEub25saW5lMAoGCCqGSM49BAMCA0cAMEQCICz528mtYIPnv4qu
NwkYGqj5+jnO4yyLIaw5reNGOjsTAiBCg6X5EhNYND+x8p2eIcPlL5ETx6OCZ4Kp
awy3ieiObw==
-----END CERTIFICATE REQUEST-----
```

Beispielaufruf zur Erstellung des Clientzertifikates:

```
$openssl x509 -req -in ${CSR_FILE} -CA ${CA_CERT} -CAkey ${CA_KEY} -CAcreateserial -out ${CN}-cert.pem -
days 365
```

Clientzertifikat:

```
$ openssl x509 -text -noout -in 01400000003144@orga6141.online-cert.pem
 Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4a:ca:f5:f8:1d:08:17:29:89:55:48:1c:78:6c:62:3f:f6:07:e7:fa
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = DE, O = Worldline Healthcare GmbH, CN = WHC-CA01 TEST
        Validity
            Not Before: Oct 11 12:23:14 2023 GMT
            Not After : Oct 10 12:23:14 2024 GMT
        Subject: C = DE, ST = Schleswig-Holstein, L = Flintbek, O = Worldline Healthcare GmbH, CN =
01400000003144@orga6141.online
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:1f:27:07:5b:51:b2:3d:ea:f0:2a:14:36:45:3c:
                    01:bd:17:c3:11:89:2b:b5:06:e3:0d:9c:7d:76:0f:
                    75:b9:13:09:3a:af:4f:b8:d5:02:35:62:bd:f1:72:
                    0a:96:d2:bb:fe:a7:8a:12:f1:6e:41:bd:d5:85:37:
                    eb:13:4c:c3:9a
                ASN1 OID: brainpoolP256r1
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client
            X509v3 Subject Key Identifier:
                BF:70:62:97:AF:33:97:56:B6:9F:82:C8:17:E5:94:E3:B2:B4:F7:0D
            X509v3 Authority Key Identifier:
                keyid:1B:34:7F:D9:D6:1E:38:F8:C8:14:44:25:FD:00:D5:0D:A3:E2:17:09

            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Subject Alternative Name:
                email:01400000003144@orga6141.online
    Signature Algorithm: ecdsa-with-SHA256
         30:64:02:30:5b:22:93:4e:41:7a:50:9e:31:4e:5e:20:e2:5b:
         54:ce:eb:de:75:fe:a8:9e:3d:de:cf:e8:90:1b:f0:43:1a:2d:
         6e:0c:34:7c:e6:d6:51:18:6c:2c:a8:43:20:fe:c9:fd:02:30:
         53:1a:85:b2:ac:63:fc:e9:60:70:4a:83:4f:d2:ab:3e:40:8d:
         bc:34:ec:38:61:e8:81:5d:d4:c4:19:d8:f1:f9:bf:89:4d:65:
         79:14:aa:7b:ca:4b:b0:1d:45:9b:94:84
```

Ablauf des USB Import / Export

In diesem Abschnitt sind die notwendigen Schritte eines Daten-Imports und -Exports stichpunktartig in Use Cases zusammengefasst. Grundsätzlich ist diese Import / Export Funktion direkt über die RMI-Schnittstelle als auch direkt am Kartenterminal über den USB Import / Export verfügbar.

Use Case: Import

- Erstellen der Konfigurationsdatei (im UTF-8 Zeichensatz) und Speicherung auf einem USB-Stick (Verzeichnis: Seriennummern oder Root)
- Administrator wählt nachfolgende Menüpunkte (Eingabe der Admin-PIN erforderlich):
  Service | Konfiguration | Import von USB-Stick
- Administrator wird zum Stecken des USB-Sticks aufgefordert
- Applikation wartet auf den USB-Stick
- Applikation sucht nach Konfigurationsdatei auf dem USB-Stick im Ordner mit der Seriennummer des Terminals bzw. im Root-Verzeichnis
- der Name der Konfigurationsdatei für den Import wird angezeigt
- Administrator wird um Bestätigung gebeten
- Applikation startet den Import
- Applikation zeigt jeden verarbeiteten Parameter mit Ergebnis auf dem Display und erzeugt eine Log-Datei auf dem USB-Stick
  Name: Konfigurationsdatei mit Endung „.log“ im Ursprungsverzeichnis.
- am Ende des Importes wird der USB-Stick aus dem System entfernt
- der Administrator wird zum Ziehen des USB-Sticks aufgefordert

Use Case: Export

- Administrator wählt nachfolgende Menüpunkte (Eingabe der Admin-PIN erforderlich):
  Service | Konfiguration | Export auf USB-Stick
- Administrator wird zum Stecken des USB-Sticks aufgefordert
- Applikation warten auf den USB-Stick
- sobald der USB-Stick eingebunden ist, startet der Export.
- Applikation legt eine Datei im Ordner mit der Seriennummer des Terminals (sofern vorhanden) bzw. im Root-Verzeichnis des USB-Sticks an
- Applikation zeigt die verarbeiteten Parameter im Display an
- am Ende des Exports wird der USB-Stick aus dem System entfernt
- der Administrator wird zum Ziehen des USB-Sticks aufgefordert



Hinweis
Das Erstellen einer initialen Export-Datei kann als Vorlage und Hilfe für die Erstellung einer Konfigurationsdatei für den Import genutzt werden. Es sind dann lediglich die relevanten Parameter anzupassen.

Import der Konfigurationsdatei

Nachdem die erstellte Konfigurationsdatei, auf einen FAT32 formatierten USB-Stick, ins Stammverzeichnis oder in einen Ordner mit der Seriennummer des Kartenterminals kopiert wurde, kann der Import gestartet werden.



Wählen Sie dazu den Menüpunkt [*Import von USB-Stick* \361] und folgen Sie den Anweisungen bzw. stecken Sie den USB-Stick in die entsprechende Buchse an der Unterseite des Kartenterminals. Der Dateiname wird im Display angezeigt und Sie werden zur Bestätigung mit der ‚OK'-Taste aufgefordert. Anschließend startet der Import.



Der Fortschritt und das Resultat des Imports werden in der Anzeige dargestellt. Zudem wird eine Log-Datei auf dem USB-Stick angelegt. In dieser können Sie den Import der einzelnen Parameter überprüfen.

Sie können nun den USB-Stick wieder aus dem Gerät entfernen.

War der Import erfolgreich startet das Kartenterminal automatisch neu und die Parameter werden übernommen! Im Fehlerfall ist die Konfiguration zu korrigieren und neu zu laden (Details hierzu siehe Log-Datei).

Konventionen zum Dateinamen

Beim Importieren von Konfigurationsdaten wird von der Applikation nur eine Datei im Ordner mit der Seriennummer des Terminals bzw. im Root-Verzeichnis des USB-Sticks eingelesen. Der Dateiname setzt sich aus einer, vom Administrator, freiwählbaren Bezeichnung (im Beispiel blau ge'x'te) und einer festen Dateiendung (_import.cfg) zusammen.

Beispiel: xxxxxx_import.cfg

Beim Export setzt sich der Dateiname aus dem Gerätenamen und einer festen Dateiendung (_export.cfg) zusammen. Ist ein Ordner mit der Seriennummer des Kartenterminals auf dem USB-Stick vorhanden, wird die Dateien dort, sonst im Root-Verzeichnis des USB-Sticks geschrieben.

Beispiel: orga6141-014000000003144_export.cfg

Unterstützte Parameter

In der nachfolgenden Tabelle sind die für die Konfiguration des VPN-Clients erforderlichen bzw. relevanten Parameter und ihre Bezeichner aufgeführt. Hierbei sind die alten Bezeichner der Firmware Versionen 3.8.x sowie die neuen Bezeichner der erweiterten Konfigurationsmöglichkeit ab Firmware Version 3.9.0 sowie die Möglichkeiten zum Im- und Export aufgelistet. Die Exportfunktion wird ausschließlich über die neuen Bezeichner unterstützt.

Bezeichner (v3.8.x)	Bezeichner (v3.9.x)	Import	Export
welcome_message	gui_idleMessage	x	x
dhcp_enabled	net_lan_dhcpEnabled	x	x
ip_addr	net_lan_ipAddr	x	x
netmask	net_lan_subnetMask	x	x
gateway_ip	net_lan_gatewayIpAddr	x	x
domain_name_server	net_dns	x	x
	net_vpn_client_name		x
	net_vpn_client_enabled	x	x
	net_vpn_client_authMode	x	x
vpn_account_user	net_vpn_client_userId	x	x
	net_vpn_client_passwd	x	
	net_vpn_client_preSharedKey	x	
	net_vpn_client_dpdDelaySeconds	x	x
ipsec_private	net_vpn_client_privateKey	x	
	net_vpn_client_privateKeyHash		x
ipsec_cert	net_vpn_client_certificate	x	x
	net_vpn_client_certificateHash		x
	net_vpn_client_certificateIssuer		x
	net_vpn_client_certifitateSubject		x
	net_vpn_client_certificateSerial		x
	net_vpn_client_certificateCxd		x
	net_vpn_client_csr		x
ipsec_conf	net_vpn_client_configuration	x	x
vpn_gateway_addr	net_vpn_server_gateway	x	x
ipsec_cacert	net_vpn_server_caCertificate	x	
	net_vpn_server_caCertificateHash		x
	net_vpn_server_caCertificateIssuer		x
	net_vpn_server_caCertificateSubject		x
	net_vpn_server_caCertificateSerial		x
	net_vpn_server_caCertificateCxd		x
	net_vpn_server_caCertificateCounter		x
	net_vpn_pkcs12	x	
	net_vpn_pkcs12_passwd	x	
	net_vpn_ipAddrSicctUnicast	x	x
	rmi_sessionEnabled	x	x
	rmi_tcpport	x	x
	rmi_timeout	x	x
	rmi_smcb_pinEnabled	x	x
	rmi_server_certificate	x	x
	rmi_server_csr		x

Bezeichner (v3.8.x)	Bezeichner (v3.9.x)	Import	Export
	rmi_server_new_cert_country	x	
	rmi_server_new_cert_state	x	
	rmi_server_new_cert_org	x	
	rmi_server_new_cert_name	x	
	rmi_server_new_cert_email	x	
	rmi_server_new_cert_nota	x	
	rmi_server_new_cert_notb	x	
admin_session	sicct_adminSessionEnabled	x	x
mct_ntp_enabled	sys_ntp_enabled	x	x
ntp_addr	sys_ntp_serverIpAddr	x	x
timezone	sys_locale_timeZone	x	x
device_name	sys_terminalName	x	x
import_filename	***not supported***	-	-

Beschreibung der wesentlichen VPN-Client Parameter

Der Im- und Export von Konfigurationsparametern via USB-Stick ist im Kapitel 7.3.6 der Bedienungsanleitung ORGA 6141 online[3] auf Seite 91 dieses Dokumentes beschrieben.

Im Folgenden werden die wesentlichen Elemente bzgl. des VPN-Tunnels detaillierter dargestellt. Aus Gründen der Kompatibilität zur FW V3.8.x können auch die alten Konfigurationsparameter und deren Syntax für den Import verwendet werden. Es wird aber empfohlen, den erweiterten neuen Parametersatz sowie die neue Syntax zu verwenden.

Bezeichner	Format*	Beschreibung	Alter Bezeichner
net_vpn_client_enabled	Boolean	Aktivierung und Deaktivierung des VPN-Services im Kartenterminal	
net_vpn_client_name	String	Auswahl des zu verwendeten VPN-Clients „StrongSwan“ oder „WireGuard“	
net_vpn_client_authMode	String	psk | mschap | pub | eap-tls	
net_vpn_client_userId	String	Benutzername- / Kennung zur Authentifizierung des Kartenterminals bei EAP-MSCHAPv2	vpn_account_user
net_vpn_client_passwd	String	Passwort zur Authentifizierung des Kartenterminals bei EAP-MSCHAPv2	
net_vpn_client_preSharedKey	String	Zeichenfolge zur Authentifizierung des Kartenterminals PSK	
net_vpn_client_privateKey	PEM	Privater Schlüssel bei Zertifikats-basierenden Authentifizierungsmethoden	
net_vpn_client_certificate	PEM	Client-Zertifikat des Kartenterminals bei Zertifikats-basierenden Authentifizierungs-methoden	ipsec_cert
net_vpn_client_configuration	String	Alternative Konfiguration des VPN-Clients im Kartenterminal	ipsec_conf
net_vpn_server_gateway	String	IP-Adresse oder Domainname des VPN-Gateways	vpn_gateway_addr
net_vpn_server_dpdDelay	Number	Intervall in Sekunden für die Überprüfung der Aktivitätsbereitschaft eines Peers	
net_vpn_server_cacertificate	PEM	CA-Zertifikat des VPN-Gateways	ipsec_cacert
net_vpn_pkcs12	Base64	Verschlüsselter PKCS#12 Container, der den Privaten Schlüssel enthalten muss und Client-Zertifikate und CA-Zertifikat enthalten kann	
net_vpn_pkcs12_passwd	String	Passwort für den verschlüsselten PKCS#12 Container	
sys_ntp_enabled	Boolean	Aktivierung und Deaktivierung des NTP-Services im Kartenterminal	mct_ntp_enabled

Bezeichner	Format*	Beschreibung	Alter Bezeichner
sys_ntp_serverIpAddr	IPv4		ntp_addr

*) weitere Details zum Format können Sie dem Dokument „Remote Management Interface - ORGA 6141online“[4] entnehmen

Für den Betrieb des VPN-Tunnels muss die Uhrzeit im Kartenterminal gesetzt sein. Das Setzen erfolgt automatisch via NTP. Falls dieser Dienst noch nicht über das Menü (\218) aktiviert wurde, kann das auch per Konfigurationsdatei erfolgen.

sys_ntp_serverIpAddr
IP-Adresse des bevorzugten NTP-Servers. Das kann ein Server im lokalen Netz oder ein öffentlicher Server z.B. von der Physikalisch-Technische Bundesanstalt in Braunschweig sein:

ptbtime1.ptb.de = 192.53.103.108
ptbtime2.ptb.de = 192.53.103.104
ptbtime3.ptb.de = 192.53.103.103

sys_ntp_enabled
Startet den NTP-Dienst bei jedem Neustart des Kartenterminals.

Bezeichner, die im PEM-Format importiert werden sollen, bedürfen einer kleinen Anpassung in der Formatierung. Im Normalfall besteht das PEM-Format aus einer öffnenden Blockzeile „----- BEGIN xxx -----", den mehrzeilig, base64-kodierten Nutzdaten und einer abschließenden Blockzeile „----- END xxx -----".

Hinweis
Für den Import ist dies in einer Zeile darzustellen. Als Zeilenumbruch ist ein ‚\n' zu verwenden.
Die Zeilenumbrüche in den base64-kodierten Nutzdaten müssen entfernt werden.

Beispiel:
-----BEGIN CERTIFICATE-----
MIIDojCCAwugAwIBAgIJAMLM0CJRzPyzMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
…
..
h8b4FYTVCg/l6TP5SWgei4VWgRfxgA==
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----\nMIIDojCCAw…4VWgRfxgA==\n-----END CERTIFICATE-----

Bezeichner, die im BASE64-Format importiert werden sollen, müssen zuvor entsprechend umgewandelt werden.

Der PKCS#12 Container (*.pfx, *.p12) ist eine binäre Datei und kann so nicht direkt in die Konfiguration übernommen werden. Zur Formatumwandlung kann auf einem Linux-System, beispielsweise das Kommandozeilen-Programm **base64** benutzt werden.

Beispiel:
cat terminal.pfx | base64 -w 0 > terminal.pfx.b64

Die erzeugte Datei terminal.pfx.b64 enthält die umgewandelten Daten aus terminal.pfx. Diese können dann in die Konfigurationsdatei übernommen werden.

Beispiele für den USB-Stick Import / Export

Konfiguration VPN – Authentifizierung mit EAPMSChapV2

```
# setup network
net_lan_dhcpEnabled=false
net_lan_ipAddr=192.168.1.100
net_dns=192.168.1.1
net_lan_subnetMask=255.255.255.0
net_lan_gatewayIpAddr=192.168.1.1

# ntp ptbtime1.ptb.de
sys_ntp_enabled=true
sys_ntp_serverIpAddr=192.168.1.1

# idle screen
#
gui_idleMessage="WHC VPN-Test"

# remove existing secure data
#
net_vpn_server_caCertificate=
net_vpn_client_certificate=
net_vpn_client_privateKey=
net_vpn_client_preSharedKey=

# vpn gateway
#
net_vpn_client_authMode="EapMsChapV2"
net_vpn_server_gateway="vpngw-dev.ihcdev.de"
net_vpn_client_userId="ORGA6141"
net_vpn_client_passwd="123456"
net_vpn_server_caCertificate="-----BEGIN CERTIFICATE-----
\nMIICBzCCAY2gAwIBAgIIBB+O58qc/icwCgYIKoZIzj0EAwMwSTELMAkGA1UEBhMCREUxIjAgBgNVBAoTGVdvcmxkbGluZSBIZWFsdGhj
YXJlIEdtYkgxFjAUBgNVBAMTDVdIQy1DQTAxIFRFU1QwHhcNMjMwMTMwMTA1NTIzWhcNMjYwMTI5MTA1NTIzWjBJMQswCQYDVQQGEwJERT
EiMCAGA1UEChMZV29ybGRsaW5lIEhlYWx0aGNhcmUgR21iSDEWMBQGA1UEAxMNV0hDLUNBMDEgVEVTVDB2MBAGByqGSM49AgEGBSuBBAAi
A2IABKAIuOojdUSkutasiKvmY3XzUOzrOlq+uZpB9HZ71W6Yh5LT6mY7LvNnCV8bUUNWYlj129qt40OyNN8ZI7r5wrEMq9yM8Tu/HmVwnt
Zi+cvBf5kD95uyCHtFPfZ6L9Nbc6NCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFBs0f9nWHjj4yBRE
Jf0A1Q2j4hcJMAoGCCqGSM49BAMDA2gAMGUCMQD6f5oDDGgF41/wgbg9nXzJU0OrBV5N6yrp7HuxdnZzDzN/aGaeg3KTtkYi9L9pBfYCMA
s5LpKJOJCHXZ6rMBSLIQkletycMGFMVjECzAMYx5hMDhuKimNJy2x5QkkMXd1T7A==\n-----END CERTIFICATE-----"
```

Konfiguration VPN – Client-Authentifizierung mit PSK und zertifikatsbasierende Server-Authentifizierung

```
net_lan_dhcpEnabled=false
net_lan_ipAddr=192.168.1.100
net_dns=192.168.1.1
net_lan_subnetMask=255.255.255.0
net_lan_gatewayIpAddr=192.168.1.1

# ntp ptbtime1.ptb.de
sys_ntp_enabled=true
sys_ntp_serverIpAddr=192.53.103.108

# idle screen
#
gui_idleMessage="WHC VPN-Test"

# remove existing secure data
#
net_vpn_server_caCertificate=
net_vpn_client_certificate=
net_vpn_client_privateKey=
net_vpn_client_preSharedKey=

# vpn gateway
#
net_vpn_client_authMode="Psk"
net_vpn_server_gateway="vpngw-dev.ihcdev.de"
net_vpn_client_userId="01400000003144@orga6141.online"
net_vpn_client_preSharedKey="HALLO_VPNGW"
net_vpn_server_caCertificate="-----BEGIN CERTIFICATE-----
\nMIICBzCCAY2gAwIBAgIIBB+O58qc/icwCgYIKoZIzj0EAwMwSTELMAkGA1UEBhMCREUxIjAgBgNVBAoTGVdvcmxkbGluZSBIZWFsdGhj
YXJlIEdtYkgxFjAUBgNVBAMTDVdIQy1DQTAxIFRFU1QwHhcNMjMwMTMwMTA1NTIzWhcNMjYwMTI5MTA1NTIzWjBJMQswCQYDVQQGEwJERT
EiMCAGA1UEChMZV29ybGRsaW5lIEhlYWx0aGNhcmUgR21iSDEWMBQGA1UEAxMNV0hDLUNBMDEgVEVTVDB2MBAGByqGSM49AgEGBSuBBAAi
A2IABKAIuOojdUSkutasiKvmY3XzUOzrOlq+uZpB9HZ71W6Yh5LT6mY7LvNnCV8bUUNWYlj129qt40OyNN8ZI7r5wrEMq9yM8Tu/HmVwnt
Zi+cvBf5kD95uyCHtFPfZ6L9Nbc6NCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFBs0f9nWHjj4yBRE
Jf0A1Q2j4hcJMAoGCCqGSM49BAMDA2gAMGUCMQD6f5oDDGgF41/wgbg9nXzJU0OrBV5N6yrp7HuxdnZzDzN/aGaeg3KTtkYi9L9pBfYCMA
s5LpKJOJCHXZ6rMBSLIQkletycMGFMVjECzAMYx5hMDhuKimNJy2x5QkkMXd1T7A==\n-----END CERTIFICATE-----"
```

Hinweis
Wird der Parameter net_vpn_server_caCertificate nicht mit konfiguriert, wird der Pre-Shared Key auch für die serverseitige Authentifizierung verwendet.

Konfiguration VPN – Authentifizierung mit PubKey

```
# setup network
net_lan_dhcpEnabled=false
net_lan_ipAddr=192.168.1.100
net_dns=192.168.1.1
net_lan_subnetMask=255.255.255.0
net_lan_gatewayIpAddr=192.168.1.1

# ntp ptbtime1.ptb.de
sys_ntp_enabled=true
sys_ntp_serverIpAddr=192.53.103.108

# idle screen
#
gui_idleMessage="WHC VPN-Test"

# remove existing secure data
#
net_vpn_server_caCertificate=
net_vpn_client_certificate=
net_vpn_client_privateKey=
net_vpn_client_preSharedKey=

# vpn gateway
#
net_vpn_client_authMode="PubKey"
net_vpn_server_gateway="vpngw-dev.ihcdev.de"
net_vpn_client_privateKey="-----BEGIN EC PRIVATE KEY-----
\nMHcCAQEEIMgexI607yiZiqbRZUBjphGC3PClY2y4dconUuoPomtAoAoGCCqGSM49AwEHoUQDQgAEzS9RpkFQehffPMwy19sKn+3UJhz1
3AFfxwWgW326PKypBsAdFbeB7J0/YsFIf4HsIlYw7rmuuTouwFXSt9q3rw==\n-----END EC PRIVATE KEY-----"
net_vpn_client_certificate="-----BEGIN CERTIFICATE-----
\nMIICWjCCAeGgAwIBAgIUSsr1+B0IFymJVUgceGxiP/YH6DQwCgYIKoZIzj0EAwIwSTELMAkGA1UEBhMCREUxIjAgBgNVBAoTGVdvcmxk
bGluZSBIZWFsdGhjYXJlIEdtYkgxFjAUBgNVBAMTDVdIQy1DQTAxIFRFU1QwHhcNMjMwODI0MTA1MTQ4WhcNMjQwODIzMTA1MTQ4WjBTMQ
swCQYDVQQGEwJERTEbMBkGA1UECgwSV29ybGRsaW5lIE1UUyBHbWJIMScwJQYDVQQDDB4wMTQwMDAwMDAwMzE0NEBvcmdhNjE0MS5vbmxp
bmUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATNL1GmQVB6F988zDLX2wqf7dQmHPXcAV/HBaBbfbo8rKkGwB0Vt4HsnT9iwUh/gewiVj
Duua65Oi7AVdK32revo4GcMIGZMAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBBAQDAgeAMB0GA1UdDgQWBBQCoFzzamhEQ75SIewK4yuxoEht
jzAfBgNVHSMEGDAWgBQbNH/Z1h44+MgURCX9ANUNo+IXCTAOBgNVHQ8BAf8EBAMCBeAwKQYDVR0RBCIwIIEeMDE0MDAwMDAwMDMxNDRAb3
JnYTYxNDEub25saW5lMAoGCCqGSM49BAMCA2cAMGQCMFWvPc4sPr+rv5dgGcqkRUqyr9t8dvI6GTPPs32tv/geICcFqFj/NFjVflpxE08f
gQIwT5DYeHvSWJWmQ9udHUteXWxhKUm4qLTvl2FdRZp4NebPHgSizMP9I53xM4ER5o8Y\n-----END CERTIFICATE-----"
net_vpn_server_caCertificate="-----BEGIN CERTIFICATE-----
\nMIICBzCCAY2gAwIBAgIIBB+O58qc/icwCgYIKoZIzj0EAwMwSTELMAkGA1UEBhMCREUxIjAgBgNVBAoTGVdvcmxkbGluZSBIZWFsdGhj
YXJlIEdtYkgxFjAUBgNVBAMTDVdIQy1DQTAxIFRFU1QwHhcNMjMwMTMwMTA1NTIzWhcNMjYwMTI5MTA1NTIzWjBJMQswCQYDVQQGEwJERT
EiMCAGA1UEChMZV29ybGRsaW5lIEhlYWx0aGNhcmUgR21iSDEWMBQGA1UEAxMNV0hDLUNBMDEgVEVTVDB2MBAGByqGSM49AgEGBSuBBAAi
A2IABKAIuOojdUSkutasiKvmY3XzUOzrOlq+uZpB9HZ71W6Yh5LT6mY7LvNnCV8bUUNWYlj129qt40OyNN8ZI7r5wrEMq9yM8Tu/HmVwnt
Zi+cvBf5kD95uyCHtFPfZ6L9Nbc6NCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFBs0f9nWHjj4yBRE
Jf0A1Q2j4hcJMAoGCCqGSM49BAMDA2gAMGUCMQD6f5oDDGgF41/wgbg9nXzJU0OrBV5N6yrp7HuxdnZzDzN/aGaeg3KTtkYi9L9pBfYCMA
s5LpKJOJCHXZ6rMBSLIQkletycMGFMVjECzAMYx5hMDhuKimNJy2x5QkkMXd1T7A==\n-----END CERTIFICATE-----"
```

Konfiguration VPN – Authentifizierung mit PubKey (PKCS#12)

```
# setup network
net_lan_dhcpEnabled=false
net_lan_ipAddr=192.168.1.100
net_dns=192.168.1.1
net_lan_subnetMask=255.255.255.0
net_lan_gatewayIpAddr=192.168.1.1

# ntp ptbtime1.ptb.de
sys_ntp_enabled=true
sys_ntp_serverIpAddr=192.53.103.108

# idle screen
#
gui_idleMessage="WHC VPN-Test"

# remove existing secure data
#
net_vpn_server_caCertificate=
net_vpn_client_certificate=
net_vpn_client_privateKey=
net_vpn_client_preSharedKey=

# vpn gateway
#
net_vpn_client_authMode="PubKey"
net_vpn_server_gateway="vpngw-dev.ihcdev.de"
net_vpn_pkcs12_passwd="123456"
net_vpn_pkcs12="MIIHWwIBAzCCByEGCSqGSIb3DQEHAaCCBxIEggcOMIIHCjCCBa8GCSqGSIb3DQEHBqCCBaAwggWcAgEAMIIFlQYJKo
ZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQIiVvEALTFJ+wCAggAgIIFaKfQfOjM/7H3Luimgnfd83EpqMrEwIM3VZrS0q+RHOT+brbakVPH
g02a/HdAr5rYSRTCmEqZvsSf+yiGJ/xnEvfrKq9QET+CCTTWmTA7ilbVaIosURGP1Udb3a6FVDj/sX8D4H46l2xdDW4e4se5iz4Z3no0EZ
llE7bRT9W06OVsk+jM4Zrtjc3P0pIttMEzzBaeONCgLO97R357m1dzTSBHCbaubf2nko7fFqpG1dsPnImmeVwL6FnGQNjAZmR3vP8g0gmX
qWLNfiZvQunI2anLid9chcVaVWVGcDedVkN6+qVfyRXSIe4FhtQY3V/B+y1jHVbSQcxmeGQEVnyRhbpDIl98Z7EeuUTFtbLmY4J+XHplEX
t6DsQ0XbJonLZr8w7YEAxHwdsotA5Mqpo0sJ8tBhRbqavLRJGjGB93MpibZG1OGm99l+SyNxjbUxRpFgfcJ6u6VquORRmtE249Aizye2O6
uTUzFtpBZ7WAmLUgqDCoXjgXRpdS7CXNBWQDGWQQXZWOBfeSN+bW56QisqwAge8dgxglLIv/i0EifPZhmXv8net5yFoYAK80DSDFp/xheD
Eh9pNhJRDuQyW4ISrtb0/Gz2Z4mx0eNQtqYrYfMep9mcBhSki+7jO7rxuhbRY4bPa6fMpIM5lm38qyZ55niw3ZBIZVT85Quy0eoJOXxUj1
3Y9Lx38wvlIN6quH2V+F+yzGHFH8fz8DclweqZMWCvpxEPwyj2DT3bTlK/IvF+LjoEGOg+5WOUbe77C5uS/2/fbMIKjypiNXWht9XUMI+s
NuEiCvmO5ggDF7RwBBcMEgfVUojbFBnwvc+34kFK+1ByuaO22+PY9YwPhN56EIKDl8J5HkOeWKA3fFhI8bLRuz0bFHas4GqieJygHcsOP0
f0kBecSrQWtVJ/1nqIRef+ZklzeOhhfP97KhutVIwcmXx235LE+ciZ0u9wOtAY1oHn4A/XfvRqEg7O8SElcjQ68irBGLAYLE1ocZD/d1x4
X59BW8/ErvUN9jrs6kLzXRLSLlziVVQCaNT8BikHcu+PszuRtJ9grkPl8yhly2Tdu7h+0SquKliOX6hAiQn8VIaABrJZa4R83ZLQTwkfEJ
qj6nI//Zeq2WaqYddJlrI8suymElU2bR3OPDiUBFmiPmzZeNeoeUGedDwZq5NIRxHQsQ9Z7B1iIKWnmsFlcD+9IumiM2gl1TJkpBrodydz
hn4lf14r0GXfAK7yzixRSQcVFRWuTF1AaXv1Xep2VBLZD+CMCpSbRYm3IqVYJzNBfwzaveajNd+BBaEEwaRtVjLm11QOfdn9lyoOhngpx9
Jrt4lwMb22MZzKTd0RZPNTS8QXlsbqJK7hG44Nq7FC+03Ul9zqg++iLYiI2YwsAsSJS/ydvdRTFWgR9BG/bHSgXhCGEFlq2UwepKg4trjX
WXQpHrrYaupdlCR4GS0kgTVKDDkKEhsXKz+lcfMdWb2boEpz2C7j82AaTQeZoBSwm0oOAXei4VZ60ljrd0NjDdGeZhm8A5fvqL52qw74aj
u0ogg60APUska+eQN1YRhw6d9HdHo0NWdlUN379C755FoI2RjZJ+VE0/UW0G+pUcLYcIH3OELOiby0yP55ebCfJaF0iBmiQpwFg/4tIvly
uOS53TgQKwLSq20V2C0SZq1jR5SsV4CkqnOGNtiOGCI1Czb28+xKQHZGNjs8xQLpFDrf8/TCt+RY6fyLEhPoNOqNoSCO3VJHg5jLTkw37u
YDHJ8thlLJGKh3dyHsNXBYbEATvqZM/cdJ2sTDQnAlHt5HmgK1r6JwuOL8D2rThHvl3OCQTfSbHmpk03VvmJg2Y3HY4e0DKThbQwggFTBg
kqhkiG9w0BBwGgggFEBIIBQDCCATwwggE4BgsqhkiG9w0BDAoBAqCBtDCBsTAcBgoqhkiG9w0BDAEDMA4ECKl26Uc0cduuAgIIAASBkAqT
nt/ysDeb3mIvotgoq4Ac4s+ivLwGw+wiSOQifkKgpjqj3fyUIf1cV0Hu+CvQNXKxVRonE+ycrehM2HsY7rbiF0jsqgktajT4w7K6qlFb7g
eA4AVvkf2Zl6yzrfCauJIIh8PlC+w5WEIwYQJLcq5+zVuemEuBotFIoVUZbzhC9ZvDfmo/4hmWoyGZrBHQDjFyMCMGCSqGSIb3DQEJFTEW
BBQFYKtq+bPILAvP2ruIj47mWGFr2DBLBgkqhkiG9w0BCRQxPh48ADAAMQA0ADAAMAAwADAAMAAwADAAMwAxADQANABAAG8AcgBnAGEANg
AxADQAMQAuAG8AbgBsAGkAbgBlMDEwITAJBgUrDgMCGgUABBQ5ercLN2RMWE2Tk+ArAfsWVABbYgQIclp0jf3U3iICAggA"
```

Exportdatei

```
gui_idleMessage="WHC VPN-Test"
net_lan_dhcpEnabled=false
net_lan_ipAddr="192.168.1.100"
net_lan_subnetMask="255.255.255.0"
net_lan_gatewayIpAddr="192.168.1.1"
net_dns="192.168.1.1"
net_vpn_client_name="strongSwan U5.9.11"
net_vpn_client_enabled=false
net_vpn_client_authMode="PubKey"
net_vpn_client_userId=""
net_vpn_client_passwd="read-only"
net_vpn_client_preSharedKey="read-only"
net_vpn_client_dpdDelaySeconds=25
net_vpn_client_privateKey="read-only"
net_vpn_client_privateKeyHash="36:DD:88:07:4F:CE:A0:07:2A:0F:DA:35:14:F6:3F:FA:B7:5C:BE:92:DB:74:9B:C0:EE:
15:3E:D2:59:84:08:65"
net_vpn_client_certificate="read-only"
net_vpn_client_certificateHash="4E:2E:67:26:AE:D2:15:56:FE:C0:FE:EC:C8:CB:B9:4D:BD:FE:4B:51:46:16:6B:1B:DF
:73:D7:03:A2:FC:F8:CC"
net_vpn_client_certificateIssuer="/C=DE/O=Worldline Healthcare GmbH/CN=WHC-CA01 TEST"
net_vpn_client_certificateSubject="/C=DE/O=Worldline Healthcare GmbH/CN=01400000003144"
net_vpn_client_certificateSerial="4A:CA:F5:F8:1D:08:17:29:89:55:48:1C:78:6C:62:3F:F6:07:E8:59"
net_vpn_client_certificateCxd="04.10.2024 13:33"
net_vpn_client_csr=""
net_vpn_client_configuration=""
net_vpn_server_gateway="vpngw-dev.ihcdev.de"
net_vpn_server_caCertificate="read-only"
net_vpn_server_caCertificateHash="D8:46:84:A7:9C:70:EC:4F:07:03:70:FE:FE:D3:9D:8A:DE:3C:A1:81:D6:D4:5F:09:
65:43:6B:AA:A3:E2:AB:D6"
net_vpn_server_caCertificateIssuer="/C=DE/O=Worldline Healthcare GmbH/CN=WHC-CA01 TEST"
net_vpn_server_caCertificateSubject="/C=DE/O=Worldline Healthcare GmbH/CN=WHC-CA01 TEST"
net_vpn_server_caCertificateSerial="04:1F:8E:E7:CA:9C:FE:27"
net_vpn_server_caCertificateCxd="29.01.2026 10:55"
net_vpn_server_caCertificateCounter=1
net_vpn_pkcs12="read-only"
net_vpn_pkcs12_passwd="read-only"
rmi_sessionEnabled=true
rmi_tcpport=443
rmi_timeout=300
rmi_smcb_pinEnabled=false
rmi_server_certificate="-----BEGIN CERTIFICATE-----
\nMIIClTCCAjqgAwIBAgIBAzAKBggqhkjOPQQDAjCBmjELMAkGA1UEBhMCREUxGzAZ\nBgNVBAgMElNjaGxlc3dpZy1Ib2xzdGVpbjEiMC
AGA1UECgwZV29ybGRsaW5lIEhl\nYWx0aGNhcmUgR21iSDEgMB4GA1UEAwwXT1JHQTYxMDAtMDE0MDAwMDAwMDMxNDQx\nKDAmBgkqhkiG
9w0BCQEWGWtvbnRha3Qud2hjQHdvcmxkbGluZS5jb20wHhcNMjMx\nMDAzMDAwMDAwWhcNNDMxMDAzMDAwMDAwWjCBmjELMAkGA1UEBhMC
REUxGzAZBgNV\nBAgMElNjaGxlc3dpZy1Ib2xzdGVpbjEiMCAGA1UECgwZV29ybGRsaW5lIEhlYWx0\naGNhcmUgR21iSDEgMB4GA1UEAw
wXT1JHQTYxMDAtMDE0MDAwMDAwMDMxNDQxKDAm\nBgkqhkiG9w0BCQEWGWtvbnRha3Qud2hjQHdvcmxkbGluZS5jb20wWTATBgcqhkjO\n
PQIBBggqhkjOPQMBBwNCAAT0I47Ex5mA9gJP2hpjaTy0hVXZlpP7yXQGE2vF8BVp\nDcsYHSm+A7GTIow8bTK1Zsn1sc0cEEv4Al98bYCX
7WuQo28wbTAJBgNVHRMEAjAA\nMB0GA1UdDgQWBBTcZNaX33sIuVpSGXewhD95njcfATAfBgNVHSMEGDAWgBTcZNaX\n33sIuVpSGXewhD
95njcfATATBgNVHSUEDDAKBggrBgEFBQcDATALBgNVHQ8EBAMC\nA6gwCgYIKoZIzj0EAwIDSQAwRgIhAOIC4j/LNCtt1aGOdwRcR/bEBn
ojTUrwxbWZ\nCd2shx96AiEAxsu+XBCSBsB/VCKJ0wiyw1rcs7PdnuVM426DVMVvFJA=\n-----END CERTIFICATE-----\n"
rmi_server_csr=""
sicct_adminSessionEnabled=true
sys_ntp_enabled=true
sys_ntp_serverIpAddr="192.53.103.108"
sys_locale_timeZone="MEZ-1MEZ-2,M3.5.0,M10.5.0"
sys_terminalName="ORGA6100-01400000003144"
```

Konfiguration über das Remote Management Interface (RMI)

In diesem Abschnitt werden die für die Konfiguration des VPN-Clients erforderlichen Schritte und Einstellungen über das RMI benannt und beschrieben.

Für eine ausführliche Beschreibung des Remote Management Interfaces sowie die Verwendung der WEB-Browser basierten Konfiguration verweisen wir auf das Dokument Remote Management Interface - ORGA 6141 online (in der aktuellen Fassung)[4].

Vorbemerkungen zur VPN-Konfiguration

Bei der Veränderung von VPN-Parametern wird in der Web-Applikation der Remote Management Schnittstelle nach dem Abspeichern zu einem Geräte-Neustart aufgefordert, um einen möglichen Verbindungsverlust zum Kartenterminal zu vermeiden. Bei einer direkten Anbindung der RMI-Schnittstelle an ein eigenes Management-System wird der gleiche Prozess empfohlen, technisch notwendig ist jedoch nur das Setzen des Parameters VPN Client - Aktivierungsstatus.

Des Weiteren ist darauf zu achten, dass der entsprechenden VPN-Client (StrongSwan oder WireGuard) über den Parameter „net_vpn_client_name“ [VPN Client Name] ausgewählt wurde.

Beispiel-Request für die Konfiguration des VPN-Gateways:

Request: VPN-Tunnel einschalten

```
>>[362]: {
    "request": {
        "token": "4b7f9b5b-2a95-41ac-8798-66305e7c27db",
        "service": "Settings",
        "method": {
            "setProperties": {
                "sessionId": "6169efa1-096e-4c67-b24f-d616e468bbe1",
                "properties": {
                    "net_vpn_client_enabled": "true"
                }
            }
        }
    }
}
<<[114]: {
    "response": {
        "token": "4b7f9b5b-2a95-41ac-8798-66305e7c27db",
        "service": "Settings",
        "result": null
    }
}
```

Request: VPN-Tunnel für Authentifizierung PSK konfigurieren

```
>>[1436]: {
    "request": {
        "token": "e3c6fd3c-f3a8-44ca-ab9b-61c617087fb1",
        "service": "Settings",
        "method": {
            "setProperties": {
                "sessionId": "3fbb42d7-e93e-4774-92c6-25cf9d26856e",
                "properties": {
                    "net_vpn_client_authMode": "Psk",
                    "net_vpn_server_gateway": "vpngw-dev.ihcdev.de",
                    "net_vpn_client_dpdDelaySeconds": 20,
                    "net_vpn_client_preSharedKey": "HALLO_VPNGW",
                    "net_vpn_server_caCertificate": "-----BEGIN CERTIFICATE-----
\nMIICBzCCAY2gAwIBAgIIBB+O58qc/icwCgYIKoZIzj0EAwMwSTELMAkGA1UEBhMC\nREUxIjAgBgNVBAoTGVdvcmxkbGluZSBIZWFsdG
hjYXJlIEdtYkgxFjAUBgNVBAMT\nDVdIQy1DQTAxIFRFU1QwHhcNMjMwMTMwMTA1NTIzWhcNMjYwMTI5MTA1NTIzWjBJ\nMQswCQYDVQQG
EwJERTEiMCAGA1UEChMZV29ybGRsaW5lIEhlYWx0aGNhcmUgR21i\nSDEWMBQGA1UEAxMNV0hDLUNBMDEgVEVTVDB2MBAGByqGSM49AgEG
BSuBBAAiA2IA\nBKAIuOojdUSkutasiKvmY3XzUOzrOlq+uZpB9HZ71W6Yh5LT6mY7LvNnCV8bUUNW\nYlj129qt40OyNN8ZI7r5wrEMq9
yM8Tu/HmVwntZi+cvBf5kD95uyCHtFPfZ6L9Nb\nc6NCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYE\n
FBs0f9nWHjj4yBREJf0A1Q2j4hcJMAoGCCqGSM49BAMDA2gAMGUCMQD6f5oDDGgF\n41/wgbg9nXzJU0OrBV5N6yrp7HuxdnZzDzN/aGae
g3KTtkYi9L9pBfYCMAs5LpKJ\nOJCHXZ6rMBSLIQkletycMGFMVjECzAMYx5hMDhuKimNJy2x5QkkMXd1T7A==\n-----END
CERTIFICATE-----",
                    "gui_idleMessage": "WHC PSK"
                }
            }
        }
    }
}
<<[114]: {
    "response": {
        "token": "e3c6fd3c-f3a8-44ca-ab9b-61c617087fb1",
        "service": "Settings",
        "result": null
    }
}
```

Hinweis
Wird der Parameter net_vpn_server_caCertificate nicht mit konfiguriert, wird der Pre-Shared Key auch für die serverseitige Authentifizierung verwendet.

Request: VPN-Tunnel für Authentifizierung EAPMSChapV2 konfigurieren

```
>>[1502]: {
    "request": {
        "token": "c57768fd-85d3-4592-896c-f1938feecd1c",
        "service": "Settings",
        "method": {
            "setProperties": {
                "sessionId": "342c25a1-cf97-46af-a42e-02bb841a128e",
                "properties": {
                    "net_vpn_client_authMode": "EapMsChapV2",
                    "net_vpn_server_gateway": "vpngw-dev.ihcdev.de",
                    "net_vpn_client_dpdDelaySeconds": 10,
                    "net_vpn_client_userId": "ORGA6141-THS",
                    "net_vpn_client_passwd": "123456",
                    "net_vpn_server_caCertificate": "-----BEGIN CERTIFICATE-----
\nMIICBzCCAY2gAwIBAgIIBB+O58qc/icwCgYIKoZIzj0EAwMwSTELMAkGA1UEBhMC\nREUxIjAgBgNVBAoTGVdvcmxkbGluZSBIZWFsdG
hjYXJlIEdtYkgxFjAUBgNVBAMT\nDVdIQy1DQTAxIFRFU1QwHhcNMjMwMTMwMTA1NTIzWhcNMjYwMTI5MTA1NTIzWjBJ\nMQswCQYDVQQG
EwJERTEiMCAGA1UEChMZV29ybGRsaW5lIEhlYWx0aGNhcmUgR21i\nSDEWMBQGA1UEAxMNV0hDLUNBMDEgVEVTVDB2MBAGByqGSM49AgEG
BSuBBAAiA2IA\nBKAIuOojdUSkutasiKvmY3XzUOzrOlq+uZpB9HZ71W6Yh5LT6mY7LvNnCV8bUUNW\nYlj129qt40OyNN8ZI7r5wrEMq9
yM8Tu/HmVwntZi+cvBf5kD95uyCHtFPfZ6L9Nb\nc6NCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYE\n
FBs0f9nWHjj4yBREJf0A1Q2j4hcJMAoGCCqGSM49BAMDA2gAMGUCMQD6f5oDDGgF\n41/wgbg9nXzJU0OrBV5N6yrp7HuxdnZzDzN/aGae
g3KTtkYi9L9pBfYCMAs5LpKJ\nOJCHXZ6rMBSLIQkletycMGFMVjECzAMYx5hMDhuKimNJy2x5QkkMXd1T7A==\n-----END
CERTIFICATE-----",
                    "gui_idleMessage": "WHC EapMsChapV2"
                }
            }
        }
    }
}
<<[114]: {
    "response": {
        "token": "c57768fd-85d3-4592-896c-f1938feecd1c",
        "service": "Settings",
        "result": null
    }
}
```

Request: VPN-Tunnel für Authentifizierung PubKey konfigurieren

```
>>[4801]: {
    "request": {
        "token": "72695ef8-84ea-4aa4-82c7-be156ae841bd",
        "service": "Settings",
        "method": {
            "setProperties": {
                "sessionId": "1bb002a7-3126-4dd7-809d-cd77f291864e",
                "properties": {
                    "net_vpn_client_authMode": "PubKey",
                    "net_vpn_server_gateway": "vpngw-dev.ihcdev.de",
                    "net_vpn_client_dpdDelaySeconds": 25,
                    "net_vpn_pkcs12":
"MIIMKgIBAzCCC/AGCSqGSIb3DQEHAaCCC+EEggvdMIIL2TCCCs8GCSqGSIb3DQEHBqCCCsAwggq8AgEAMIIKtQYJKoZIhvcNAQcBMBwGCiqGSIb3
DQEMAQYwDgQI26Ryazpmwsc CAggAgIIKiNU/D6qApf637g1eMbBg7V56F4WNMicDNA8mhPABjIgUE9Rbcd/evVFGZr6xsJypnEs80B/CBb/wI9huA
+j1uGqXfQY+jie41493T0G80MdtulvEMSmIKN9qgG0x3Ov2QqjcfDHxH68e1WuC9c2uAIKs1W1pi8OV3U2H2UAyDzOcMjg4dhqVlluHnq6sdSdmxq
ZNdPj7kM9Qglsb6JtqCOhCh0X58u5zak5PLoFSkO/7rkwO9H/RamFzhljrTcGAmzhJX0PKy/Mb2DY/+pD17XOKDI/Uq0Y2wW8dGep20RFsL2pFVs5
EzbaL59cHVFeOrrJlcrWGhwmPv0/MX9f2VPTrDOr+NGg39PL8w6GsZJb+pb++KtVIvq1WiwxlmGheKLWfyzPIA+EKw5eQiwMqzr5SkbvWdLDMMqy2
shjiQ9jYjA4eHOKLKaqJIsU37ygs6CjhA98+KYrVXV+Nt7mnxRuGqKC6QPGl3wjAfK3HRmH0t87fdQLIIdvE3vTK1hyZI/lQJnmcO8DR0f1AQpnak
DFqiTGMVwJVfG62BeS5guzZI6sujKffUZ4MNrQTRrI09U0CXVEvQZpKxZ3WF+fZU7tv/Lw3M1M+/qXlLibAURqpUut8H+bTkFCVCI1ASxmOVs3ht7
ADMapgVuAN48HVgHwLYQFd4SZ6gOvR+r8R/RijlQbRF3CDz8OgOzPD1pGrVWfMKWG+ckgKvw58p01lMMnCqxxjN7KGtWBrO5t+g8Qg2NYfj4sslYT
oolHz9gp+28whybHru92WU4AkKNuDNTm5Q/Rs7VX6P4PU5ur2MTZaWsey5D3VRGgaEeHDLXX3ba6cPZ+TS7CVgbkcu7NAygIe7ivAQTDbcajwbWTj
l25CUbR8yQu6r5hqsRXQs016iWkiuUUHSqQ1AJx4MWAmRgy4kT2XRYKYH3KcRdobN9eT8MQe1DqUIET+TsVwpiCJdY8r02dae7FoXEYtoGxYh8wzM
owaBaVr7Zk+YkoOX3A/SQgpxX68KQSc9HLEuostYBQsz+Z0OdvU95CKkrXAI2cHVsjTHNMGvR7a97Tpm9mfaQTI0WJs8r+fLFPBL25x6gGqRhWsOx
UEX8Dzm+BncKixaFmdpkQHY5mLoTBRkE4oeGOBb8Orht5Idl7WUsyMv54swFMME7jN8c9K1//9wLsEVsF+ZTrSZPonjdLJhkPgWGf8vUzD+t+j3wf
dAvoJnP6+RK1r5M/RTJspllRDOEMQxmPnFT8OFoUjieTk/9txMRlp4xZv9OZHpWmEAolO9LXN3SKEh+TsqUoIoofF/VOyji5MkYzq3pWReVUrxDvb
3pwf0aJtWwivsJiKV6/KSCspBHEuaULKJ5OwfJoNAY3TIxuQB+Xlmf3apGBPY4iM+zXY1k0yRURyaGvXMbdK2uGQzkoidF7BrFqs8o9+YmHGUbMP5
Ccv29csywEyTSdz3DIakPZLCt/Vw7PQINJjqWTHMHaD7zqjGfQS/7x0auXe+urVM41Cb6Iks7cX80M51Aeyo66B1hY2/mjicC8S6fT5+hhpJZE7Dt
q38XRtkPsM9LPW4FUTPTZoF08Jjm8+OjGHyttgtEj25Trb/PeE5pemA0t4ONLItbC7iCuD97QaKOciB0sdcAlAQOsJgq7TttdKhtu0SEW0GILRqZ/
s0atfcWx3RD0ENDwIKtRDheonswXx9hORSW9BGxI5w1WJw1Mwvqfspws3ld/YjMz7jVRsqnblldr8vmNls+CFdUz1/eNXDE+7+WmFqztBJmIe+GJj
mj1KnTK0qSjdS/G7wgXqfHMH336u5Dw+TX8lwv7+vPta78P91javz6xgPa2NKDIUtOLnIsCjy6Sc+KUxoGXH//0VjKGk7Rqh4eDP9M53xizZEdqsd
MpY8laLvPn/4lVywagr7d5nPjIe31lY3D4zmF/uqZlf9q3oghABB8pAgfRoYWo6R01Vj3EKDB+csERbJ1ftdf5iaPZSVqR1GQ/cKiezSFAMDkvnqQ
gbgmoIw+goerjAvrQQJj0nw/iSh0hwvp9UB504J9Hh092zA0KkJkkJKZGBX0It3CDP5XSbibG5PKViDill9PY5Z9EDBUQ58XWs1DLlOlcI/3uDoxS
kyagX3UHSNfqwDGbdWfE+oksDG8YQia7QtFPFjpMvE83M8U1zvLHXFL3RwnOMweiDe2cjlXxNw/gnnuPE67L/6unW2V6orFvrizRQ3iACXP78nUw+
JfMJxYhXGTCCYus1DGvXOleGHqPIiVAiwzq733H3keqivQ7dlNJrU7dCb96Uve61jdKoxU7msJrRXThPUpdKKH02pkd0U9DeZchfWDN/lSJbSbF/7
WN4zTIrjWEV/l3l8EmnFG078g1vjAwaTgyAvTiZgD5kkPquoue5+GBb1ApOC/s74D7jxy+mbe1pHneu1Rt2PDuOlnazN5vyI7QuVDMwFd5X5j0UgI
n016somNTZLqkvxpaXAPNXiWzulHhGTmr6882NrV3MHT9XcxgHMzg66UNy/fKzrsWpl6a88tU6xn90Ul4D0PILRxFIbrZnUz+cv9iZHae5WPvV9iE
Z+85XIBikkgSN43B6LpapEdAzyfyyqJgoPoJzVVUxHfcxKCO1K6DvuX/60Ujz4eHWivjCKQ1Jmu9rItbsDJSQlaUGmPKsVsnd6R6TiY+VhRZtZL/I
2gqAvJR2YMV53eRvclM0CAEwVhkBGLtu+05jq42e0dDwtXrv8IS6r10hKrlALAL2DQY29r7e3EiJBRH//BlgUB2HmEUjvfXGQQiNXYbfnrUO+kQuG
9cAZ3XM9k0qATzUv76fmXqoOeJECirieKZwWyCc1XrC8/YmM96Hycv86fH60dhLXgSU5pFyr9K8s3P90K0YLlQSMNz2L2l2rWmGXRmmpxTOuxyU8S
yyIOXHi5CzlQ86o4DJ2gGarHnS2eYsh0OjF41x34KUeLqLFtKqaqfCUcsHnXULgr7d42NX3IyBrI2Js8504bekVUbaDWGC7AZo+dSYpjtNLXxQJg9
7+9lNi1lFpyvtfuilGXr+EpdNmk8wJqCYR4EoLS1v/v0l1zZIdajURX+XWCJIUEEf4tmfcCjiDAugnXdeU8Jr6OiPJ0ShSKxU9dnLhobzczaPGA1L
nVJjcSy+sRtb2HsKK1zUcl6aYrhodWw/RRumGhEWYsC930dU3MADFcLfJAmLHCYZZUJlTrIWbsT+dVZBE3qugoggr3FFJJnXNbczR6aTX+RaUWRRh
spPm7Lw8fE+EQBCQwG3cmQJcetoImlq+bU6YXwrcZwhXhUWkEF/SRV/rR0g681ikDZR1ps5nrdr/uGta411D1rszeTE158mWPEGNQhV83+ZhMFg9D
ZwiVei0AbLmHgBRWPeNtZiT3BReS3zT3z/mHPh31ffXnS30BMMKISZRg4lwfTZbPrUALw2Otkfqod1Dy9NsJ8UeycIPs9znlLQoBbDgEfDrPU4obO
QKB2YwxK8GT42YSSYZfBLCKTI9/hjhy9pvelTVzVaBLSONE1UuqKQ+YF7Inghjo0kubOtec0PdM1vAjtLd5UjPYtgj40Fdg5ESFpSoQUdSXj1Uu5Z
gqfCg047yat1MIIBAgYJKoZIhvcNAQcBoIH0BIHxMIHuMIHrBgsqhkiG9w0BDAoBAqCBtDCBsTAcBgoqhkiG9w0BDAEDMA4ECNcQ0RZEK9COAgIIA
ASBkPKUuxiUsiUy0mfYa/shxD/5nZIC4bO9512j6Ey16iKz3Om6nwABJYH+P3/FYaTFSlI2HPXC2RsgpkQfGdgq5GL9AP/cerrPAEjzKJ0ZKNeTfh
g6SftmbhXhfFubOi3yriSeNSgkscDQZPtU6TAER6SYeReaCMxk8LFiKyxGkfmaW84ADqLBlQcS6o1kE1p92DElMCMGCSqGSIb3DQEJFTEWBBRBUcD
O6f4vA3BJwLXJ6ZsieNLcfjAxMCEwCQYFKw4DAhoFAAQUQ8BzhSWGOwX08/ItJkcZNOi+eH0ECJRo3xy2yilyAgIIAA==",
                    "net_vpn_pkcs12_passwd": "123456",
                    "gui_idleMessage": "WHC PubKey"
                }
            }
        }
    }
}

<<[114]: {
    "response": {
        "token": "72695ef8-84ea-4aa4-82c7-be156ae841bd",
        "service": "Settings",
        "result": null
    }
}
```

Request: VPN-Tunnel Konfiguration löschen

```
>>[1047]: {
    "request": {
        "token": "407e3605-fcbc-4a10-a6a8-8029504635ac",
        "service": "Settings",
        "method": {
            "setProperties": {
                "sessionId": "a1634594-369b-49f4-bb0d-fc3c2175a9c9",
                "properties": {
                    "net_vpn_client_enabled": "false",
                    "net_vpn_client_authMode": "None",
                    "net_vpn_client_userId": "",
                    "net_vpn_client_passwd": "",
                    "net_vpn_client_preSharedKey": "",
                    "net_vpn_client_certificate": "",
                    "net_vpn_client_privateKey": "",
                    "net_vpn_client_dpdDelaySeconds": 20,
                    "net_vpn_server_gateway": "",
                    "net_vpn_server_caCertificate": "",
                    "net_vpn_pkcs12": "",
                    "net_vpn_pkcs12_passwd": "",
                    "net_vpn_client_configuration": "",
                    "gui_idleMessage": "WHC ohne VPN-CFG"
                }
            }
        }
    }
}
<<[114]: {
    "response": {
        "token": "407e3605-fcbc-4a10-a6a8-8029504635ac",
        "service": "Settings",
        "result": null
    }
}
```

Request: VPN-Tunnel Konfiguration Server auslesen

```
>>[699]: {
    "request": {
        "token": "1028f500-ae5a-4da3-9f84-01da62bdf6e4",
        "service": "Settings",
        "method": {
            "getProperties": {
                "sessionId": "fec79018-042a-426c-927c-5de74b7d5000",
                "propertyIds": [
                    "net_vpn_server_caCertificateHash",
                    "net_vpn_server_caCertificateIssuer",
                    "net_vpn_server_caCertificateSubject",
                    "net_vpn_server_caCertificateSerial",
                    "net_vpn_server_caCertificateCxd",
                    "net_vpn_server_gateway",
                    "net_vpn_server_caCertificateCounter"
                ]
            }
        }
    }
}
<<[697]: {
    "response": {
        "token": "1028f500-ae5a-4da3-9f84-01da62bdf6e4",
        "service": "Settings",
        "result": {
            "properties": {
                "net_vpn_server_caCertificateCxd": "29.01.2026 10:55",
                "net_vpn_server_caCertificateHash":
"D8:46:84:A7:9C:70:EC:4F:07:03:70:FE:FE:D3:9D:8A:DE:3C:A1:81:D6:D4:5F:09:65:43:6B:AA:A3:E2:AB:D6",
                "net_vpn_server_caCertificateIssuer": "/C=DE/O=Worldline Healthcare GmbH/CN=WHC-CA01
TEST",
                "net_vpn_server_caCertificateSerial": "04:1F:8E:E7:CA:9C:FE:27",
                "net_vpn_server_caCertificateSubject": "/C=DE/O=Worldline Healthcare GmbH/CN=WHC-CA01
TEST",
                "net_vpn_server_caCertificateCounter": 1,
                "net_vpn_server_gateway": "vpngw-dev.ihcdev.de"
            }
        }
    }
}
```

Request: VPN-Tunnel Konfiguration Client auslesen

```
>>[1034]: {
    "request": {
        "token": "71acad3b-dc1d-4b9f-8bfa-9be40c2bb2ff",
        "service": "Settings",
        "method": {
            "getProperties": {
                "sessionId": "fec79018-042a-426c-927c-5de74b7d5000",
                "propertyIds": [
                    "net_vpn_client_enabled",
                    "net_vpn_client_authMode",
                    "net_vpn_client_dpdDelaySeconds",
                    "net_vpn_client_userId",
                    "net_vpn_client_privateKeyHash",
                    "net_vpn_client_certificateHash",
                    "net_vpn_client_certificatePubKeyHash",
                    "net_vpn_client_certificateIssuer",
                    "net_vpn_client_certificateSubject",
                    "net_vpn_client_certificateSerial",
                    "net_vpn_client_certificateCxd",
                    "net_vpn_client_certificateCommonName",
                    "net_vpn_client_csr",
                    "net_vpn_client_name"
                ]
            }
        }
    }
}
<<[1260]: {
    "response": {
        "token": "71acad3b-dc1d-4b9f-8bfa-9be40c2bb2ff",
        "service": "Settings",
        "result": {
            "properties": {
                "net_vpn_client_authMode": "PubKey",
                "net_vpn_client_certificateCommonName": "01400000003144@orga6141.online",
                "net_vpn_client_certificateCxd": "24.04.2024 10:14",
                "net_vpn_client_certificateHash":
"76:15:1E:F6:73:F4:12:F9:59:26:5D:CA:DC:A6:95:66:9A:FB:8D:60:55:E3:BC:2D:16:CD:7E:BE:4F:30:55:B4",
                "net_vpn_client_certificatePubKeyHash":
"EC:69:8D:AE:5D:B9:EF:D4:5E:1F:25:87:65:0C:D6:34:16:C9:BE:C5:55:EC:17:B4:45:0E:36:DD:17:C4:9F:A9",
                "net_vpn_client_certificateIssuer": "/C=DE/O=Worldline Healthcare GmbH/CN=WHC-CA01 TEST",
                "net_vpn_client_certificateSerial":
"4A:CA:F5:F8:1D:08:17:29:89:55:48:1C:78:6C:62:3F:F6:07:E7:F4",
                "net_vpn_client_certificateSubject": "/C=DE/O=Worldline Healthcare
GmbH/CN=01400000003144@orga6141.online",
                "net_vpn_client_csr": "",
                "net_vpn_client_dpdDelaySeconds": 15,
                "net_vpn_client_enabled": false,
                "net_vpn_client_name": "strongSwan U5.9.11",
                "net_vpn_client_privateKeyHash":
"EC:69:8D:AE:5D:B9:EF:D4:5E:1F:25:87:65:0C:D6:34:16:C9:BE:C5:55:EC:17:B4:45:0E:36:DD:17:C4:9F:A9",
                "net_vpn_client_userId": "01400000003144@orga6141.online"
            }
        }
    }
}
```

Request: VPN-Tunnel WireGuard


```
>>[1320]: {
    "request": {
        "token": "7ae6cfd9-1bce-4c90-a528-52f7e5b1742b",
        "service": "Settings",
        "method": {
            "setProperties": {
                "sessionId": "fa6fb584-be5c-4db6-a349-ebe7c9f4625c",
                "properties": {
                    "gui_idleMessage": "WHC WireGuard",
                    "net_vpn_client_name": "Wireguard",
                    "net_vpn_client_configuration": "# automated generated Tue Dec  3 10:47:02 AM CET
2024\n[Interface]\n# client private key\nPrivateKey = qP8AL4tl8GzYogLt4Bl0I5Et4T+TClmLFJ8Trgjm5m4=\n#
client ip in vpn net\nAddress = 192.168.42.201/24\n\n[PEER]\n# server public key\nPublicKey =
D3RpJVXkO7bFE06rUci21vesWMNpHU116CEEjewU6F0=\n# pre-shared key\n# PresharedKey =
mkI9YdmqRHGDM26KG9xGZ0lkRBZuXLbo7oTJMGVarwY=\n# set ACL (Access Control List)\nAllowedIPs =
192.168.42.0/24\n# server public ip adress and port\nEndpoint = 172.30.130.4:41194\n# keep connection
alive\nPersistentKeepalive = 15\n\n# # server configuration part\n# [PEER]\n# # client public key serial:
01400000003144\n# PublicKey = 0TLWR51VmqhmTXC1EvpIOI1hEyvNqsdBWiXDdYCLaw4=\n# # pre-shared key\n#
PresharedKey = mkI9YdmqRHGDM26KG9xGZ0lkRBZuXLbo7oTJMGVarwY=\n# # client ip in vpn net\n# AllowedIPs =
192.168.42.201/32\n"
                }
            }
        }
    }
}
```

Konfiguration über die Web-Applikation zum Remote Management Interface (RMI)

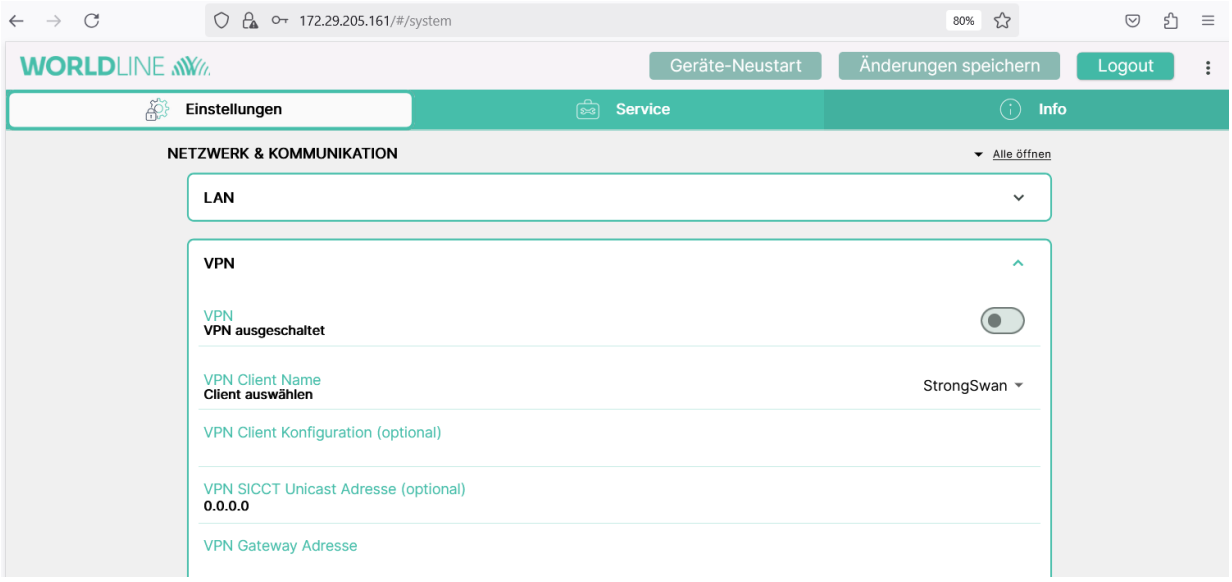
In diesem Abschnitt werden die für die Konfiguration des VPN-Clients erforderlichen Schritte und Einstellungen über die Web-Applikation zum RMI beschrieben.

Für die grundsätzliche Beschreibung der Web-Applikation zum Remote Management Interface wird auf das Dokument Remote Management Interface - ORGA 6141 online (in der aktuellen Fassung) [4] verweisen. Hier werden in Kapitel 5 - Web-Applikation – die wesentlichen Voraussetzungen, Rollen, der grundsätzliche Aufbau, die grundsätzliche Handhabung sowie der Initialstart der Web-Applikation beschrieben.

Bei der Veränderung von VPN-Parametern wird in der Web-Applikation der Remote Management Schnittstelle nach dem Abspeichern zu einem Geräte-Neustart aufgefordert, um einen möglichen Verbindungsverlust zum Kartenterminal zu vermeiden, technisch notwendig ist jedoch nur, den jeweiligen Eintrag über den Button **Änderungen speichern** ins Kartenterminal zu übernehmen und den VPN-Tunnels über den Schiebregler **VPN** einzuschalten. Sollte die Konfiguration bei einem eingeschalteten VPN-Tunnel nicht vollständig oder von der Syntax falsch sein, so wird die Speicherung abgelehnt.

Erstellen einer WireGuard VPN-Konfiguration

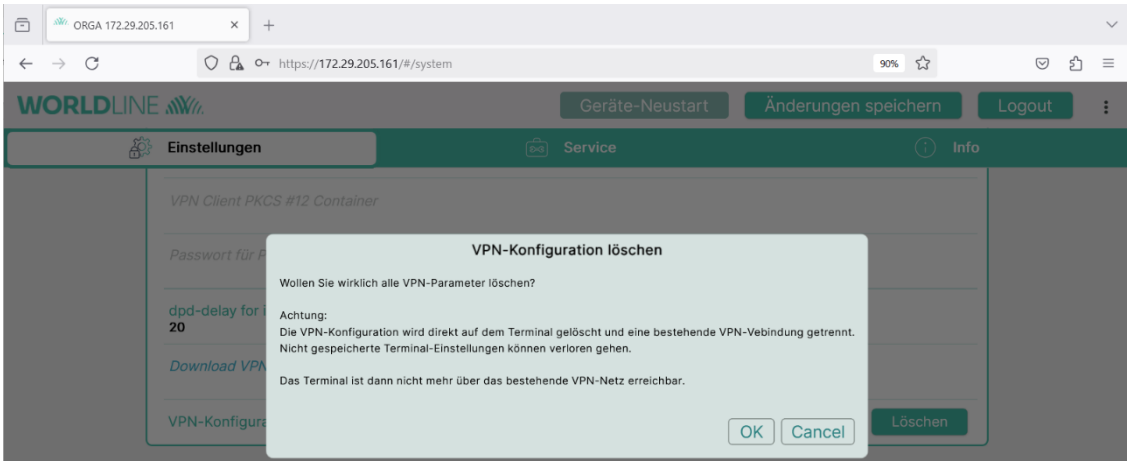
Nachdem Sie die Web-Applikation gestartet haben, öffnen Sie im Bereich **Einstellungen** mit einem Klick das **VPN**-Fenster:
Für die WireGuard Konfiguration gehen Sie jetzt grundsätzlich wie folgt vor:



- Wählen Sie unter VPN Client Name das **WireGuard** VPN Protokoll aus.
  Es sind nun viele Konfigurationsfenster ausgegraut, die für die WireGuard Konfiguration nicht benötigt werden. Trotzdem müssen diese Felder leer sein.

- Scrollen Sie durch das ganze VPN-Auswahlfenster und prüfen, ob hier schon eine Konfiguration angelegt wurde. Im Ausgangszustand finden Sie folgende Default Einstellungen:
  - VPN SICCT Unicast Adresse: 0.0.0.0
  - Anzahl der importierten CA-Zertifikate: 0
  - VPN Authentifizierung steht auf: None
  - dpd-delay for ipsec connection [s]: 20

  Alle anderen Felder müssen leer sein. Ist dieses nicht der Fall, liegt bereits eine Konfiguration komplett oder teilweise vor. Das kann dann der Fall sein, wenn z.B. der lokale Admin über das Kartenterminal bereits eine VPN-Konfiguration ins Gerät geladen hat. Klären Sie die Ursache für diese (Teil-)Konfiguration und entscheiden, ob diese Konfiguration gelöscht werden kann.
- Es wird grundsätzlich empfohlen, eine vorhandene Konfiguration – so Ihnen diese nicht bekannt ist – zu löschen.
- Um eine VPN-Konfiguration zu löschen, gehen Sie in die letzte Zeile des VPN-Fensters auf den Button **Löschen**.
  Bitte beachten Sie den Hinweistext vor dem Löschen:



  Wenn Sie sich sicher sind, dass Sie das Kartenterminal hinterher noch erreichen, löschen Sie die Konfiguration und führen Sie einen **Geräte-Neustart** durch.

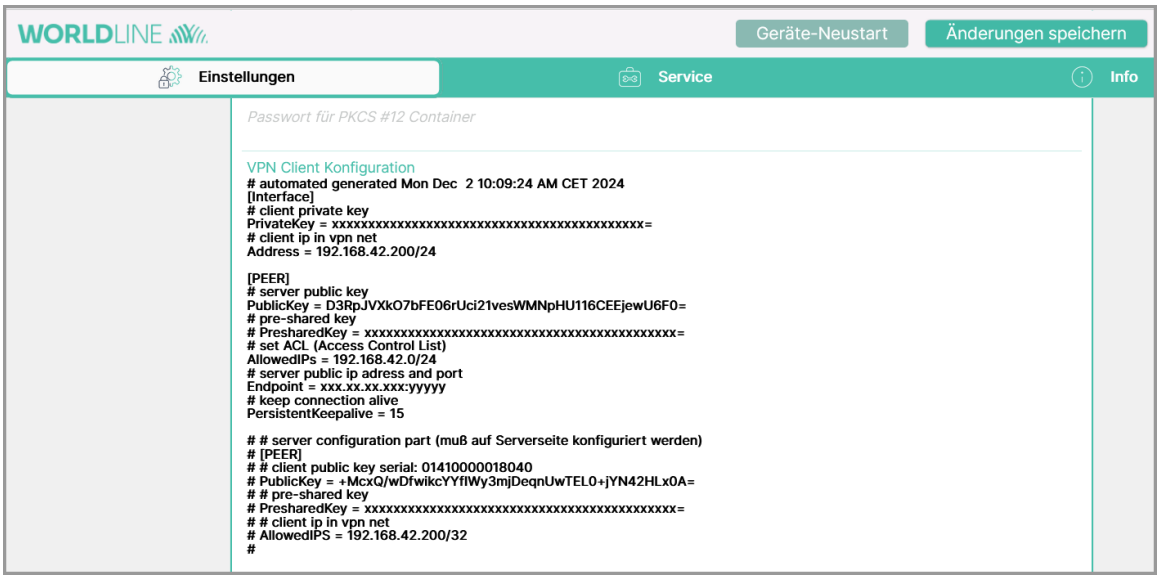
- Gehen Sie nun wieder in das VPN-Fenster und öffnen dieses durch Anklicken.
- Lassen Sie den **VPN**-Client **ausgeschaltet**.
- Gehen Sie **noch nicht** auf den **Änderungen Speichern-Button**.
- Gehen Sie unter **VPN Client Name** wieder in die Auswahl **WireGuard.**
- Gehen Sie jetzt auf die **VPN Client Konfiguration**
- Geben Sie hier die von Ihrem Administrator erhaltene WireGuard Konfiguration per Copy & Paste ein. Weitere Hinweise finden Sie z.B. auch im Internet unter
  https://www.wireguard.com/quickstart/:

```
# automated generated Mon Dec  2 10:09:24 AM CET 2024
[Interface]
# client private key
PrivateKey = xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx=
# client ip in vpn net
Address = 192.168.42.200/24

[PEER]
# server public key
PublicKey = D3RpJVXkO7bFE06rUci21vesWMNpHU116CEEjewU6F0=
# pre-shared key
# PresharedKey = xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx=
# set ACL (Access Control List)
AllowedIPs = 192.168.42.0/24
# server public ip adress and port
Endpoint = xxx.xx.xx.xxx:yyyyy
# keep connection alive
PersistentKeepalive = 15

# # server configuration part (muß auf Serverseite konfiguriert werden)
# [PEER]
# # client public key serial: 01410000018040
# PublicKey = +McxQ/wDfwikcYYfIWy3mjDeqnUwTEL0+jYN42HLx0A=
# # pre-shared key
# PresharedKey = xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx=
# # client ip in vpn net
# AllowedIPS = 192.168.42.200/32
#
```

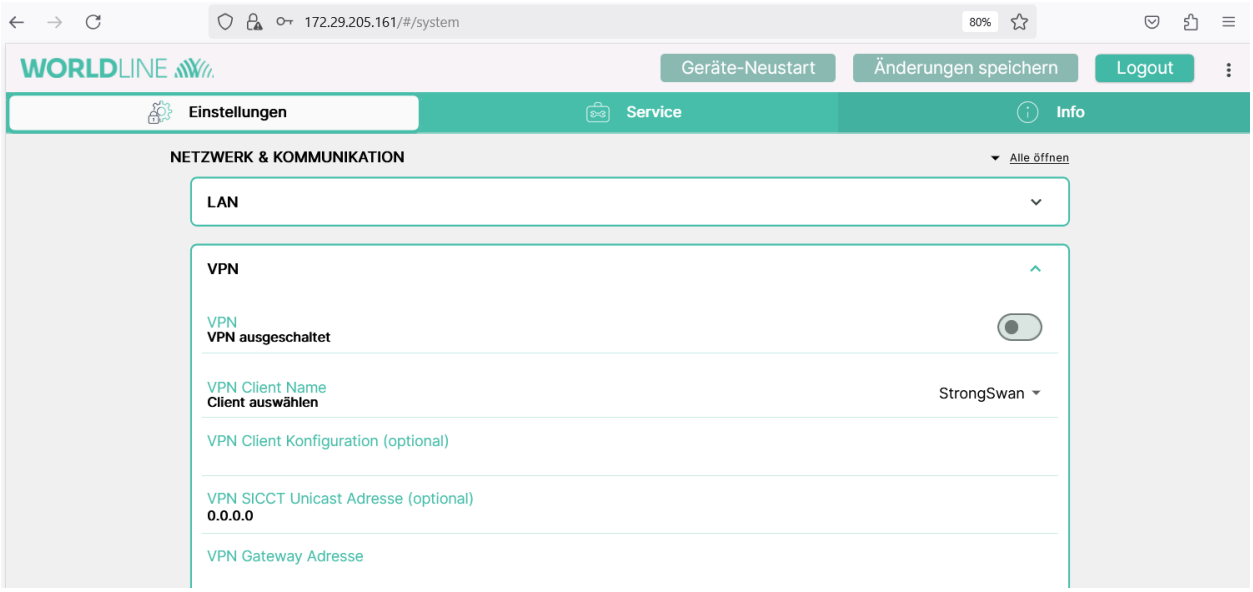
- Mit der gespeicherten Konfiguration ergibt sich dann folgendes Ergebnis in der Web-Applikation:



- Optional können Sie nun eine **VPN SICCT Unicast Adresse** vom dazugehörigen Konnektor angeben, so dass das eHKT sein Announcement jetzt auch gerichtet an den Konnektor senden kann.
- Abschließend bestätigen Sie die Konfiguration mit dem Button **Änderungen Speichern** oben rechts.
- Setzen Sie nun den **VPN** Schieberegler ggf. auf **VPN eingeschaltet** und gehen noch einmal auf **Änderungen Speichern**
- Damit ist – wenn die Konfigurationen von Client und Server aufeinander abgestimmt und richtig sind - eine WireGuard VPN-Verbindung aufgebaut.
- In der Web-Applikation kann jetzt der Status im Betrieb im Bereich **Info/VPN** eingesehen werden.

Erstellen einer StrongSwan VPN-Konfiguration über die Web-Applikation

Nachdem Sie die Web-Applikation gestartet haben, öffnen Sie im Bereich **Einstellungen** mit einem Klick das **VPN**-Fenster:

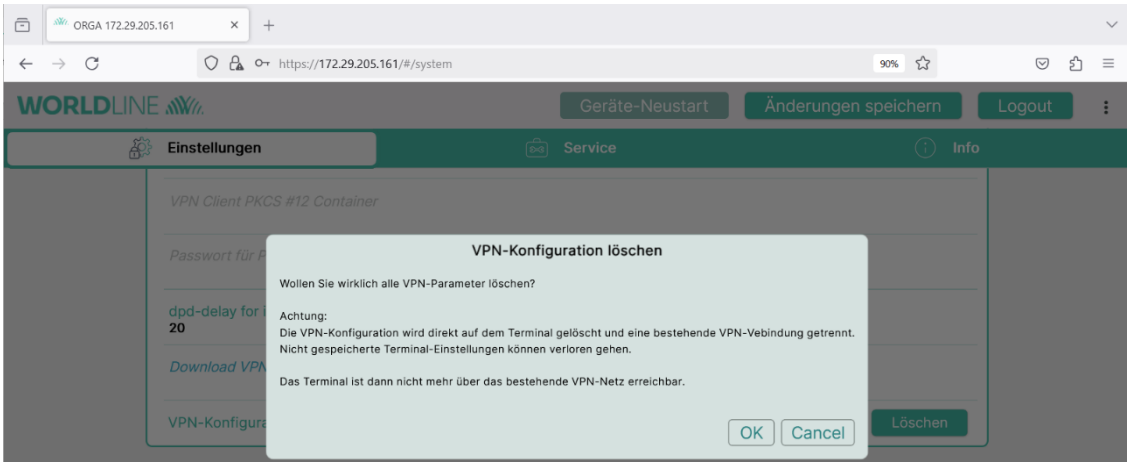


Für die StrongSwan Konfiguration gehen Sie jetzt grundsätzlich wie folgt vor:

- Wählen Sie zunächst unter VPN Client Name das **StrongSwan** VPN Protokoll aus.
- Scrollen Sie durch das ganze VPN-Auswahlfenster und prüfen, ob hier schon eine Konfiguration angelegt wurde. Im Ausgangszustand finden Sie folgende Default Einstellungen:
  - VPN SICCT Unicast Adresse: 0.0.0.0
  - Anzahl der importierten CA-Zertifikate: 0
  - VPN Authentifizierung steht auf: None
  - dpd-delay for ipsec connection [s]: 20

  Alle anderen Felder müssen leer sein. Ist dieses nicht der Fall, liegt bereits eine Konfiguration komplett oder teilweise vor. Das kann dann der Fall sein, wenn z.B. der lokale Admin über das Kartenterminal bereits eine VPN-Konfiguration ins Gerät geladen hat. Klären Sie die Ursache für diese (Teil-)Konfiguration und entscheiden, ob diese Konfiguration gelöscht werden kann.
- Prüfen Sie insbesondere die beiden optionalen Parameter **VPN Client Konfiguration (optional)** und den Parameter **VPN SICCT Unicast Adresse (optional).** Beide Parameter müssen leer sein, denn diese beiden Parameter werden auch für die WireGuard Konfiguration verwendet.
- Es wird grundsätzlich empfohlen, die vorhandene Konfiguration – so Ihnen diese nicht bekannt ist – zu löschen.
- Um eine VPN-Konfiguration zu löschen, gehen Sie in die letzte Zeile auf den **Löschen** Button.

Bitte beachten Sie den Hinweistext vor dem Löschen:



Wenn Sie sich sicher sind, dass Sie das Kartenterminal hinterher noch erreichen, löschen Sie die Konfiguration und führen Sie einen **Geräte-Neustart** durch.

Öffnen Sie nun wieder im Bereich **Einstellungen** mit einem Klick das **VPN**-Fenster:

- Gehen Sie **noch nicht** auf den **Änderungen Speichern-Button**.
- Gehen Sie unter **VPN Client Name** jetzt wieder in die Auswahl **StrongSwan**

Die folgende Tabelle gibt einen Überblick über die generellen Konfigurationsmöglichkeiten beim StrongSwan VPN-Tunnel sowie seinen 4 Authentifizierungsmöglichkeiten:

VPN Client Name	**StrongSwan**			
VPN Client Konfiguration (optional)	***optional***, als Alternative für die Eingabe der Einzelparameter kann hier auch eine komplette Konfiguration reingeladen werden.			
VPN SICCT Unicast Adresse (optional)	***optional***, Wertebereich IP-v4-Addr, Beschreibung auf Seite 35			
VPN Server Gateway Adresse	***mandatory***, Wertebereich: IP-v4-Addr oder gültige Domain Adresse mit maximal 255 Zeichen			
CA Zertifikat	***mandatory***, für die PSK-Authentifizierung jedoch optional. ein Beispiel finden Sie auf Seite 35			
VPN Authentifizierung	**Pre-Shared Key**	**EAP-MSCHAPv2**	**Public Key**	**EAP-TLS**
Benutzer Kennung	***optional***	***mandatory***	***optional***	***optional***
Pre-Shared Key (PSK)	***mandatory***			
Benutzer Passwort		***mandatory***		
Private Key			***mandatory***	***mandatory***
Client Zertifikat			***mandatory***	***mandatory***
VPN Client PKCS#12 Container			***mandatory***	***mandatory***
Passwort für PKCS#12 Container			***mandatory***	***mandatory***

- Die Parameter CA Zertifikat, Privat Key und das Client Zertifikat können auch einzeln konfiguriert werden.

- Wählen Sie nun die **VPN Authentifizierung**(s) Methode aus. Es stehen vier Methoden zur Auswahl: **Pre-Shared Key / EAP-MSCHAPv2 / Public-Key / EAP-TLS**
- Geben Sie unter der **Benutzer Kennung** die Gateway IP-Adresse oder die entsprechende URL-Adresse des Gateways ein.
- Beim **Pre-Shared Key** geben sie das Geheimnis ein, welches Sie im Vorwege mit dem Administrator des VPN-Gateways ausgetauscht haben.
- Bei der **Pre-Shared Key** Authentifizierung können Sie optional auch ein **CA-Zertifikat** eingeben. Wird das CA-Zertifikat nicht mit konfiguriert, wird der **Pre-Shared Key** auch für die serverseitige Authentifizierung verwendet. Bei allen anderen drei Authentifizierungsmethoden muss ein CA-Zertifikat angegeben werden. Die blau hinterlegten Felder aktualisieren sich dann beim nächsten Neustart.
- Geben Sie unter **Benutzer Passwort** das zur **Benutzer Kennung** gehörende Passwort ein.
- Einen **Private Key** geben Sie per Copy & Paste im gleichnamigen Feld ein**.** Hier ein Beispiel:
    - -----BEGIN EC PRIVATE KEY-----
\nMHcCAQEEIMgexI607yiZiqbRZUBjphGC3PCIY2y4dconUuoPomtAoAoGCCqGSM49AwEHoUQDQgAEzS9RpkFQehffPMwy19sKn+3UJhz13AFfxwWgW326PKypBsAdFbeB7J0/YsFIf4HsIIYw7rmuuTouwFXSt9q3rw==\n-----END EC PRIVATE KEY-----
- Mit einem **Client – Zertifikat** wird die Identität des Kartenterminal verifiziert und dient dazu, eine sichere Verbindung zwischen dem Client und dem Server zu etablieren. Hier ein Beispiel:
    - -----BEGIN CERTIFICATE-----
\nMIICWjCCAeGgAwIBAgIUSsr1+B0IFymJVUgceGxiP/YH6DQwCgYIKoZIzj0EAwIwSTELMAkGA1UEBhMCREUxIjAgBgNVBAoTGVdvcmxkbGluZSBIZWFsdGhjYXJlIEdtYkgxFjAUBgNVBAMTDVdIQy1DQTAxIFRFU1QwHhcNMjMwODI0MTA1MTQ4WhcNMjQwODIzMTA1MTQ4WjBTMQswCQYDVQQGEwJERTEbMBkGA1UECgwSV29ybGRsaW5lIE1UUyBHbWJIMScwJQYDVQQDDB4wMTQwMDAwMDAwMzE0NEBvcmdhNjE0MS5vbmxpbmUwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATNL1GmQVB6F988zDLX2wqf7dQmHPXcAV/HBaBbfbo8rKkGwB0Vt4HsnT9iwUh/gewiVjDuua65Oi7AVdK32revo4GcMIGZMAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBBAQDAgeAMB0GA1UdDgQWBBQCoFzzamhEQ75SIewK4yuxoEhtjzAfBgNVHSMEGDAWgBQbNH/Z1h44+MgURCX9ANUNo+IXCTAOBgNVHQ8BAf8EBAMCBeAwKQYDVR0RBCIwIIEeMDE0MDAwMDAwMDMxNDRAb3JnYTYxNDEub25saW5lMAoGCCqGSM49BAMCA2cAMGQCMFWvPc4sPr+rv5dgGcqkRUqyr9t8dvI6GTPPs32tv/geICcFqFj/NFjVflpxE08fgQIwT5DYeHvSWJWmQ9udHUteXWxhKUm4qLTvl2FdRZp4NebPHgSizMP9I53xM4ER5o8Y\n-----END CERTIFICATE-----

- Der **PKCS #12 Container** beinhaltet den privaten Schlüssel, das X.509-Zertifikat für den Client und ein oder mehrere CA-Zertifikate für den Server. Wie Sie diese Container Datei erstellen, ist im Kapitel Erstellung und Umwandlung eines PKCS#12-Containers auf Seite 40 beschrieben.

  In der Web-Applikation haben Sie nun zwei Eingabemöglichkeiten. Entweder Sie laden sich die Base64 Daten per Copy & Paste in das Eingabefeld und bestätigen diese mit dem Button **Eingabe übernehmen** oder Sie laden sich einfach die PKCS#12 Datei (.pfx, .PFX, .p12, .P12) über den Button **PKCS#12 Datei laden** von Ihrem Rechner direkt ins Kartenterminal. Zum Abschluss geben Sie dann noch das dazugehörige **Passwort für den PKCS#12 Container** ein.
- Optional können Sie nun eine **VPN SICCT Unicast Adresse** vom dazugehörigen Konnektor angeben, so dass das eHKT sein Announcement jetzt auch gerichtet an den Konnektor senden kann.
- Abschließend bestätigen Sie die Konfiguration mit dem Button **Änderungen Speichern** oben rechts.
- Setzen Sie nun den **VPN** Schieberegler ggf. auf **VPN eingeschaltet** und gehen noch einmal auf **Änderungen Speichern**
- Damit ist – wenn die Konfigurationen von Client und Server aufeinander abgestimmt und richtig sind - eine StrongSwan VPN-Verbindung aufgebaut.
- In der Web-Applikation kann jetzt der Status im Betrieb im Bereich **Info/VPN** eingesehen werden.

VPN SICCT Unicast Adresse (optional)

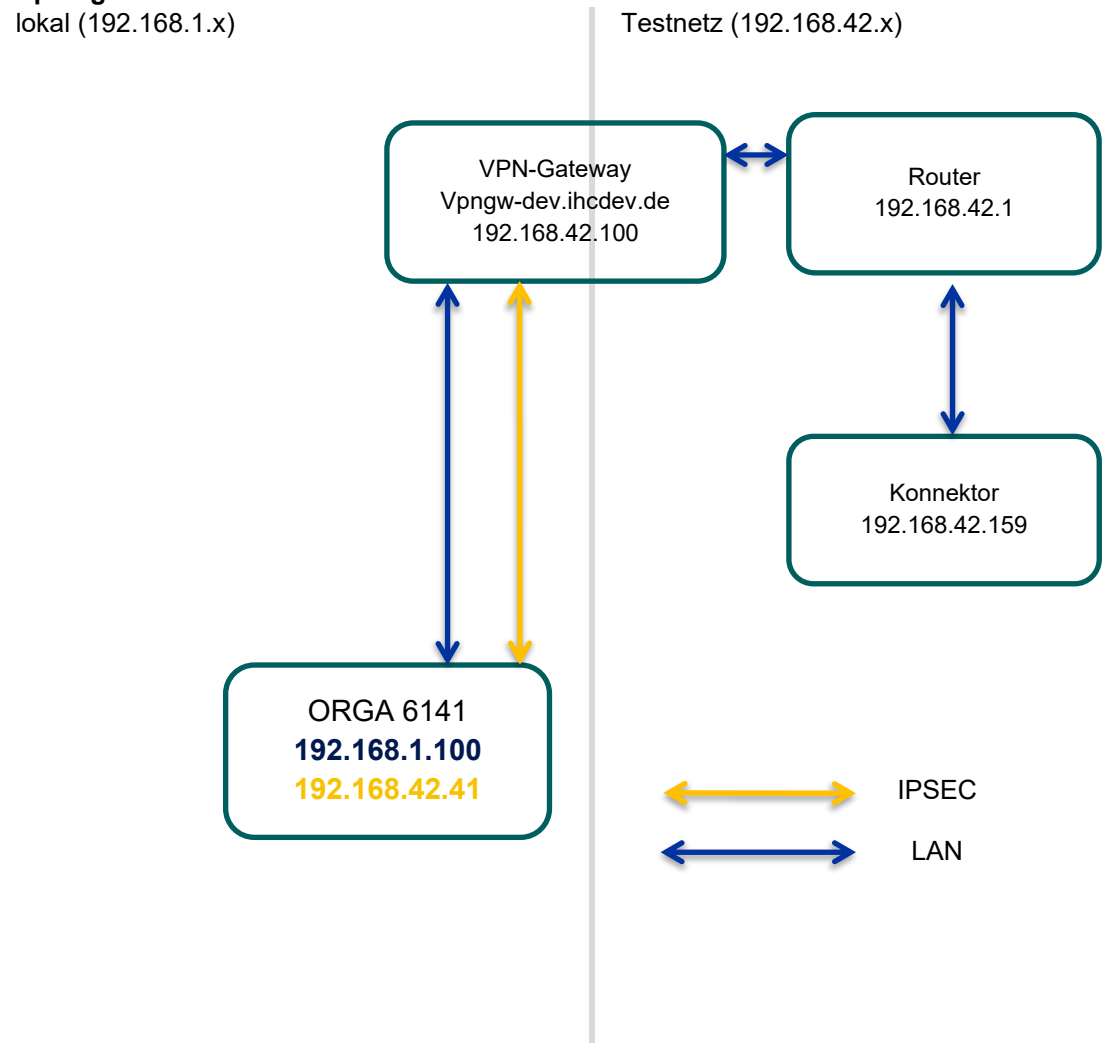
Das Kartenterminal verfügt über einen zusätzlichen UNICAST Announcement Parameter (IP-Adresse), mit dem die Zieladresse des SICCT Service-Announcement konfiguriert werden kann. Im Normalfall berechnet das Terminal diese Zieladresse aus dem vom Terminal zugewiesenen Netzsegment.

Im VPN-Umfeld kann es vorkommen, dass dieses Service Announcement zielgerichtet z.B. an einen Konnektor erfolgen soll. Für diesen Fall geben Sie die entsprechende Zieladresse hier ein.

Konfigurationen im Testumfeld

Nachfolgend wird die im Testumfeld verwendete Topologie sowie die verwendeten Konfigurationen für das VPN-Gateway, als auch für das Kartenterminal, beschrieben.

Topologie



VPN-Gateway

Auf dem VPN-Gateway wird eine StrongSwan v5.9.9 Instanz eingesetzt. Konfiguriert wird hierbei eine Authentifizierung des Servers per Zertifikat. Beim Client (Kartenterminal) wird die Authentifizierung per User / Passwort nach eap-mschapv2, PSK, sowie in einer Verbindung mit einem Public-Key bzw. EAP-TLS konfiguriert. Die IP-Adressen im VPN-Netz werden per DHCP den Clients zugewiesen.

```
root@ipsec-gw:cat swanctl.conf
connections {

   rw_pub {
      local_addrs = vpngw-dev.ihcdev.de
      pools = dhcp

      local {
         auth = pubkey
         certs = vpngw_ipsec_cert.pem
      }
      remote {
         auth = pubkey
      }
      children {
         net {
                hostaccess = yes
            local_ts  = 192.168.42.0/24

            updown = /usr/local/libexec/ipsec/_updown iptables
         }
      }
      version = 2
      fragmentation = yes
      encap = yes
   }

  rw_eap {
      local_addrs = vpngw-dev.ihcdev.de
      pools = dhcp

      local {
         auth = pubkey
         certs = vpngw_ipsec_cert.pem
      }
      remote {
        auth = eap-mschapv2
                id = %any
      }
      children {
         net {
            local_ts  = 192.168.42.0/24

            updown = /usr/local/libexec/ipsec/_updown iptables
         }
      }
      version = 2
      fragmentation = yes
      encap = yes
   }
```

```
rw_psk {
      local_addrs = vpngw-dev.ihcdev.de
      pools = dhcp

      local {
         auth = pubkey
         certs = vpngw_ipsec_cert.pem
      }
      remote {
        auth = psk
                id = %any
      }
      children {
         net {
            local_ts  = 192.168.42.0/24

            updown = /usr/local/libexec/ipsec/_updown iptables
         }
      }
      version = 2
      fragmentation = yes
      encap = yes
   }
}

include /usr/local/etc/swanctl/swanctl.secrets
```

Kartenterminal

Das Kartenterminal erstellt bei Systemstart, falls keine alternative Konfiguration eingespielt wurde, aus den bereits konfigurierten Daten eine entsprechende interne Standardkonfiguration.

```
$ cat swanctl.conf
# swanctl.conf - StrongSwan IPsec configuration file
connections {
  ike2 {
    version = 2
    local_addrs = %any
    remote_addrs = vpngw-dev.ihcdev.de
    vips = 0.0.0.0
    dpd_delay = 15s
    proposals = aes256-prfsha256-prfsha384-sha256-sha384-modp2048-modp3072-modp4096-ecp256-ecp384-
ecp256bp-ecp384bp, default
    local {
      auth = pubkey
      certs = vpn_credentional_cert
      id = 01400000003144@orga6141.online
    }
    remote {
      auth = pubkey
      id = %any
      cacerts = vpn_credentional_cacert
    }
    children {
      home {
        local_ts = dynamic
        remote_ts = 0.0.0.0/0
        mode = tunnel
        updown = /sbin/vpn_tunnel_updown.sh
        start_action=start
        dpd_action=start
        esp_proposals = aes256-sha256-sha384-modp2048-modp3072-modp4096-ecp256-ecp384-ecp256bp-ecp384bp,
default
      }
    }
  }
}
include /tmp/swanctl/swanctl.secrets
```

Erstellung und Umwandlung eines PKCS#12-Containers

Der PKCS#12-Container beinhaltet den privaten Schlüssel, das X.509-Zertifikat für den Client und ein oder mehrere CA-Zertifikate für den Server. Es wird empfohlen ein sicheres Passwort für den Zugriff auf den Container zu verwenden. Außerdem müssen die Wertepaare „net_vpn_pkcs12“ & net_vpn_pkcs12_passwd“ in einem Request gesendet werden. Der PKCS#12-Container kann beispielhaft mit openssl aus dem vorhanden, privaten Schlüssel, dem Client- und dem bzw. den CA-Zertifikaten des Servers erzeugt werden:

```
$ openssl pkcs12 -export -out 01400000003144.pfx-passout pass:${passwd} -inkey ${client_key} -in
${client_cert} -chain -CAfile ${server_ca_cert}
```

Zur Umwandlung wird im Beispiel das Kommandozeilen Programm base64 benutzt.

```
$ xxd 01400000003144.pfx
00000000: 3082 075b 0201 0330 8207 2106 092a 8648  0..[...0..!..*.H
00000010: 86f7 0d01 0701 a082 0712 0482 070e 3082  ..............0.
00000020: 070a 3082 05af 0609 2a86 4886 f70d 0107  ..0.....*.H.....
00000030: 06a0 8205 a030 8205 9c02 0100 3082 0595  .....0......0...
00000040: 0609 2a86 4886 f70d 0107 0130 1c06 0a2a  ..*.H......0...*
00000050: 8648 86f7 0d01 0c01 0630 0e04 0889 5bc4  .H.......0....[.
00000060: 00b4 c527 ec02 0208 0080 8205 68a7 d07c  ...'........h..|
00000070: e8cc ffb1 f72e e8a6 8277 ddf3 7129 a8ca  .........w..q)..
00000080: c4c0 8337 559a d2d2 af91 1ce4 fe6e b6da  ...7U........n..
00000090: 9153 c783 4d9a fc77 40af 9ad8 4914 c298  .S..M..w@...I...
000000a0: 4a99 bec4 9ffb 2886 27fc 6712 f7eb 2aaf  J.....(.'.g...*.
000000b0: 5011 3f82 0934 d699 303b 8a56 d568 8a2c  P.?..4..0;.V.h.,
000000c0: 5111 8fd5 475b ddae 8554 38ff b17f 03e0  Q...G[...T8.....
000000d0: 7e3a 976c 5d0d 6e1e e2c7 b98b 3e19 de7a  ~:.l].n.....>..z
000000e0: 3411 9965 13b6 d14f d5b4 e8e5 6c93 e8cc  4..e...O....l...
000000f0: e19a ed8d cdcf d292 2db4 c133 cc16 9e38  ........-..3...8
00000100: d0a0 2cef 7b47 7e7b 9b57 734d 2047 09b6  ..,.{G~{.WsM G..
00000110: ae6d fda7 928e df16 aa46 d5db 0f9c 89a6  .m.......F......
00000120: 795c 0be8 59c6 40d8 c066 6477 bcff 20d2  y\..Y.@..fdw.. .
00000130: 0997 a962 cd7e 266f 42e9 c8d9 a9cb 89df  ...b.~&oB.......
00000140: 5c85 c55a 5565 4670 379d 5643 7afa a55f  \..ZUeFp7.VCz.._
00000150: c915 d221 ee05 86d4 18dd 5fc1 fb2d 631d  ...!......_..-c.
00000160: 56d2 41cc 6678 6404 567c 9185 ba43 225f  V.A.fxd.V|...C"_
00000170: 7c67 b11e b944 c5b5 b2e6 6382 7e5c 7a65  |g...D....c.~\ze
00000180: 117b 7a0e c434 5db2 689c b66b f30e d810  .{z..4].h..k....
00000190: 0c47 c1db 28b4 0e4c aa9a 34b0 9f2d 0614  .G..(..L..4..-..
000001a0: 5ba9 abcb 4491 a318 1f77 3298 9b64 6d4e  [...D....w2..dmN
000001b0: 1a6f 7d97 e4b2 3718 db53 1469 1607 dc27  .o}...7..S.i...'
000001c0: abba 56ab 8e45 19ad 136e 3d02 2cf2 7b63  ..V..E...n=.,.{c
000001d0: bab9 3533 16da 4167 b580 98b5 20a8 30a8  ..53..Ag.... .0.
000001e0: 5e38 1746 9752 ec25 cd05 6403 1964 105d  ^8.F.R.%..d..d.]
000001f0: 958e 05f7 9237 e6d6 e7a4 22b2 ac00 81ef  .....7....".....
00000200: 1d83 1825 2c8b ff8b 4122 7cf6 6199 7bfc  ...%,...A"|.a.{.
00000210: 9deb 79c8 5a18 00af 340d 20c5 a7fc 6178  ..y.Z...4. ...ax
00000220: 3121 f693 6125 10ee 4325 b821 2aed 6f4f  1!..a%..C%.!*.oO
00000230: c6cf 6678 9b1d 1e35 0b6a 62b6 1f31 ea7d  ..fx...5.jb..1.}
00000240: 99c0 614a 48be ee33 bbaf 1ba1 6d16 386c  ..aJH..3....m.8l
00000250: f6ba 7cca 4833 9966 dfca b267 9e67 8b0d  ..|.H3.f...g.g..
00000260: d904 8655 4fce 50bb 2d1e a093 97c5 48f5  ...UO.P.-.....H.
00000270: dd8f 4bc7 7f30 be52 0dea ab87 d95f 85fb  ..K..0.R....._..
00000280: 2cc6 1c51 fc7f 3f03 725c 1ea9 9316 0afa  ,..Q..?.r\......
00000290: 7110 fc32 8f60 d3dd b4e5 2bf2 2f17 e2e3  q..2.`....+./...
000002a0: a041 8e83 ee56 3946 deef b0b9 b92f f6fd  .A...V9F...../..
000002b0: f6cc 20a8 f2a6 2357 5a1b 7d5d 4308 fac3  .. ...#WZ.}]C...
000002c0: 6e12 20af 98ee 6080 317b 4700 4170 c120  n. ...`.1{G.Ap.
000002d0: 7d55 288d b141 9f0b dcfb 7e24 14af b507  }U(..A....~$....
000002e0: 2b9a 3b6d be3d 8f58 c0f8 4de7 a108 2839  +.;m.=.X..M...(9
```

```
000002f0: 7c27 91e4 39e5 8a03 77c5 848f 1b2d 1bb3  |'..9...w....-..
00000300: d1b1 476a ce06 aa27 89ca 01dc b0e3 f47f  ..Gj...'........
00000310: 4901 79c4 ab41 6b55 27fd 67a8 845e 7fe6  I.y..AkU'.g..^..
00000320: 6497 378e 8617 cff7 b2a1 bad5 48c1 c997  d.7.........H...
00000330: c76d f92c 4f9c 899d 2ef7 03ad 018d 681e  .m.,O.........h.
00000340: 7e00 fd77 ef46 a120 ecef 1212 5723 43af  ~..w.F. ....W#C.
00000350: 22ac 118b 0182 c4d6 8719 0ff7 75c7 85f9  ".........u...
00000360: f415 bcfc 4aef 50df 63ae cea4 2f35 d12d  ....J.P.c.../5.-
00000370: 22e5 ce25 5540 268d 4fc0 6290 772e f8fb  "..%U@&.O.b.w...
00000380: 33b9 1b49 f60a e43e 5f32 865c b64d dbbb  3..I...>_2.\.M..
00000390: 87ed 12aa e2a5 88e5 fa84 0890 9fc5 4868  ..............Hh
000003a0: 006b 2596 b847 cdd9 2d04 f091 f109 aa3e  .k%..G..-......>
000003b0: a723 ffd9 7aad 966a a61d 7499 6b23 cb2e  .#..z..j..t.k#..
000003c0: ca61 2553 66d1 dce3 c389 4045 9a23 e6cd  .a%Sf.....@E.#..
000003d0: 978d 7a87 9419 e743 c19a b934 8471 1d0b  ..z....C...4.q..
000003e0: 10f5 9ec1 d622 0a5a 79ac 1657 03fb d22e  .....".Zy..W....
000003f0: 9a23 3682 5d53 264a 41ae 8772 7738 67e2  .#6.]S&JA..rw8g.
00000400: 57f5 e2bd 065d f00a ef2c e2c5 1490 7151  W....]...,....qQ
00000410: 515a e4c5 d406 97bf 55de a765 412d 90fe  QZ......U..eA-..
00000420: 08c0 a949 b458 9b72 2a55 8273 3417 f0cd  ...I.X.r*U.s4...
00000430: abde 6a33 5df8 105a 104c 1a46 d563 2e6d  ..j3]..Z.L.F.c.m
00000440: 7540 e7dd 9fd9 72a0 e867 829c 7d26 bb78  u@....r..g..}&.x
00000450: 9703 1bdb 6319 cca4 ddd1 164f 3534 bc41  ....c......O54.A
00000460: 796c 6ea2 4aee 11b8 e0da bb14 2fb4 dd49  yln.J......./..I
00000470: 7dce a83e fa22 d888 8d98 c2c0 2c48 94bf  }..>."......,H..
00000480: c9db dd45 3156 811f 411b f6c7 4a05 e108  ...E1V..A...J...
00000490: 6105 96ad 94c1 ea4a 838b 6b8d 7597 4291  a......J..k.u.B.
000004a0: ebad 86ae a5d9 4247 8192 d248 1354 a0c3  ......BG...H.T..
000004b0: 90a1 21b1 72b3 fa57 1f31 d59b d9ba 04a7  ..!.r..W.1......
000004c0: 3d82 ee3f 3601 a4d0 799a 014b 09b4 a0e0  =..?6...y..K....
000004d0: 177a 2e15 67ad 258e b774 3630 dd19 e661  .z..g.%..t60...a
000004e0: 9bc0 397e fa8b e76a b0ef 86a3 bb4a 2083  ..9~...j.....J .
000004f0: ad00 3d4b 246b e790 3756 1187 0e9d f477  ..=K$k..7V.....w
00000500: 47a3 4356 7655 0ddf bf42 ef9e 45a0 8d91  G.CVvU...B..E...
00000510: 8d92 7e54 4d3f 516d 06fa 951c 2d87 081f  ..~TM?Qm....-...
00000520: 7384 2ce8 9bcb 4c8f e797 9b09 f25a 1748  s.,...L......Z.H
00000530: 819a 2429 c058 3fe2 d22f 972b 8e4b 9dd3  ..$).X?../.+.K..
00000540: 8102 b02d 2ab6 d15d 82d1 266a d634 794a  ...-*..]..&j.4yJ
00000550: c578 0a4a a738 636d 88e1 8223 50b3 6f6f  .x.J.8cm...#P.oo
00000560: 3ec4 a407 6463 63b3 cc50 2e91 43ad ff3f  >...dcc..P..C..?
00000570: 4c2b 7e45 8e9f c8b1 213e 834e a8da 1208  L+~E....!>.N....
00000580: edd5 2478 398c b4e4 c37e ee60 31c9 f2d8  ..$x9....~.`1...
00000590: 652c 918a 8777 721e c357 0586 c401 3bea  e,...wr..W....;.
000005a0: 64cf dc74 9dac 4c34 2702 51ed e479 a02b  d..t..L4'.Q..y.+
000005b0: 5afa 270b 8e2f c0f6 ad38 47be 5dce 0904  Z.'../...8G.]...
000005c0: df49 b1e6 a64d 3756 f989 8366 371d 8e1e  .I...M7V...f7...
000005d0: d032 9385 b430 8201 5306 092a 8648 86f7  .2...0..S..*.H..
000005e0: 0d01 0701 a082 0144 0482 0140 3082 013c  .......D...@0..<
000005f0: 3082 0138 060b 2a86 4886 f70d 010c 0a01  0..8..*.H.......
00000600: 02a0 81b4 3081 b130 1c06 0a2a 8648 86f7  ....0..0...*.H..
00000610: 0d01 0c01 0330 0e04 08a9 76e9 4734 71db  .....0....v.G4q.
00000620: ae02 0208 0004 8190 0a93 9edf f2b0 379b  ..............7.
00000630: de62 2fa2 d828 ab80 1ce2 cfa2 bcbc 06c3  .b/..(..........
00000640: ec22 48e4 227e 42a0 a63a a3dd fc94 21fd  ."H."~B..:....!.
00000650: 5c57 41ee f82b d035 72b1 551a 2713 ec9c  \WA..+.5r.U.'...
00000660: ade8 4cd8 7b18 eeb6 e217 48ec aa09 2d6a  ..L.{.....H...-j
00000670: 34f8 c3b2 baaa 515b ee07 80e0 056f 91fd  4.....Q[.....o..
00000680: 9997 acb3 adf0 9ab8 9208 87c3 e50b ec39  ..............9
00000690: 5842 3061 024b 72ae 7ecd 5b9e 984b 81a2  XB0a.Kr.~.[..K..
000006a0: d148 a155 196f 3842 f59b c37e 6a3f e219  .H.U.o8B...~j?..
000006b0: 96a3 2199 ac11 d00e 3172 3023 0609 2a86  ..!.....1r0#..*.
000006c0: 4886 f70d 0109 1531 1604 1405 60ab 6af9  H......1....`.j.
000006d0: b3c8 2c0b cfda bb88 8f8e e658 616b d830  ..,........Xak.0
000006e0: 4b06 092a 8648 86f7 0d01 0914 313e 1e3c  K..*.H......1>.<
000006f0: 0030 0031 0034 0030 0030 0030 0030 0030  .0.1.4.0.0.0.0.0
00000700: 0030 0030 0033 0031 0034 0034 0040 006f  .0.0.3.1.4.4.@.o
00000710: 0072 0067 0061 0036 0031 0034 0031 002e  .r.g.a.6.1.4.1..
00000720: 006f 006e 006c 0069 006e 0065 3031 3021  .o.n.l.i.n.e010!
```

```
00000730: 3009 0605 2b0e 0302 1a05 0004 1439 7ab7  0...+........9z.
00000740: 0b37 644c 584d 9393 e02b 01fb 1654 005b  .7dLXM...+...T.[
00000750: 6204 0872 5a74 8dfd d4de 2202 0208 00    b..rZt...."....
```

$ cat 01400000003144.pfx | base64 -w 0


```
MIIHWwIBAzCCByEGCSqGSIb3DQEHAaCCBxIEggcOMIIHCjCCBa8GCSqGSIb3DQEHBqCCBaAwggWcAgEAMIIFlQYJKoZIhvcNAQcBMBwGCi
qGSIb3DQEMAQYwDgQIiVvEALTFJ+wCAggAgIIFaKfQfOjM/7H3Luimgnfd83EpqMrEwIM3VZrS0q+RHOT+brbakVPHg02a/HdAr5rYSRTC
mEqZvsSf+yiGJ/xnEvfrKq9QET+CCTTWmTA7ilbVaIosURGP1Udb3a6FVDj/sX8D4H46l2xdDW4e4se5iz4Z3no0EZllE7bRT9W06OVsk+
jM4Zrtjc3P0pIttMEzzBaeONCgLO97R357m1dzTSBHCbaubf2nko7fFqpG1dsPnImmeVwL6FnGQNjAZmR3vP8g0gmXqWLNfiZvQunI2anL
id9chcVaVWVGcDedVkN6+qVfyRXSIe4FhtQY3V/B+y1jHVbSQcxmeGQEVnyRhbpDIl98Z7EeuUTFtbLmY4J+XHplEXt6DsQ0XbJonLZr8w
7YEAxHwdsotA5Mqpo0sJ8tBhRbqavLRJGjGB93MpibZG1OGm99l+SyNxjbUxRpFgfcJ6u6VquORRmtE249Aizye2O6uTUzFtpBZ7WAmLUg
qDCoXjgXRpdS7CXNBWQDGWQQXZWOBfeSN+bW56QisqwAge8dgxglLIv/i0EifPZhmXv8net5yFoYAK80DSDFp/xheDEh9pNhJRDuQyW4IS
rtb0/Gz2Z4mx0eNQtqYrYfMep9mcBhSki+7jO7rxuhbRY4bPa6fMpIM5lm38qyZ55niw3ZBIZVT85Quy0eoJOXxUj13Y9Lx38wvlIN6quH
2V+F+yzGHFH8fz8DclweqZMWCvpxEPwyj2DT3bTlK/IvF+LjoEGOg+5WOUbe77C5uS/2/fbMIKjypiNXWht9XUMI+sNuEiCvmO5ggDF7Rw
BBcMEgfVUojbFBnwvc+34kFK+1ByuaO22+PY9YwPhN56EIKDl8J5HkOeWKA3fFhI8bLRuz0bFHas4GqieJygHcsOP0f0kBecSrQWtVJ/1n
qIRef+ZklzeOhhfP97KhutVIwcmXx235LE+ciZ0u9wOtAY1oHn4A/XfvRqEg7O8SElcjQ68irBGLAYLE1ocZD/d1x4X59BW8/ErvUN9jrs
6kLzXRLSLliVVQCaNT8BikHcu+PszuRtJ9grkPl8yhly2Tdu7h+0SquKliOX6hAiQn8VIaABrJZa4R83ZLQTwkfEJqj6nI//Zeq2WaqYd
dJlrI8suymElU2bR3OPDiUBFmiPmzZeNeoeUGedDwZq5NIRxHQsQ9Z7B1iIKWnmsFlcD+9IumiM2gl1TJkpBrodydzhn4lf14r0GXfAK7y
zixRSQcVFRWuTF1AaXv1Xep2VBLZD+CMCpSbRYm3IqVYJzNBfwzaveajNd+BBaEEwaRtVjLm11QOfdn9lyoOhngpx9Jrt4lwMb22MZzKTd
0RZPNTS8QXlsbqJK7hG44Nq7FC+03Ul9zqg++iLYiI2YwsAsSJS/ydvdRTFWgR9BG/bHSgXhCGEFlq2UwepKg4trjXWXQpHrrYaupdlCR4
GS0kgTVKDDkKEhsXKz+lcfMdWb2boEpz2C7j82AaTQeZoBSwm0oOAXei4VZ60ljrd0NjDdGeZhm8A5fvqL52qw74aju0ogg60APUska+eQ
N1YRhw6d9HdHo0NWdlUN379C755FoI2RjZJ+VE0/UW0G+pUcLYcIH3OELOiby0yP55ebCfJaF0iBmiQpwFg/4tIvlyuOS53TgQKwLSq20V
2C0SZq1jR5SsV4CkqnOGNtiOGCI1Czb28+xKQHZGNjs8xQLpFDrf8/TCt+RY6fyLEhPoNOqNoSCO3VJHg5jLTkw37uYDHJ8thlLJGKh3dy
HsNXBYbEATvqZM/cdJ2sTDQnAlHt5HmgK1r6JwuOL8D2rThHvl3OCQTfSbHmpk03VvmJg2Y3HY4e0DKThbQwggFTBgkqhkiG9w0BBwGggg
FEBIIBQDCCATwwggE4BgsqhkiG9w0BDAoBAqCBtDCBsTAcBgoqhkiG9w0BDAEDMA4ECKl26Uc0cduuAgIIAASBkAqTnt/ysDeb3mIvotgo
q4Ac4s+ivLwGw+wiSOQifkKgpjqj3fyUIf1cV0Hu+CvQNXKxVRonE+ycrehM2HsY7rbiF0jsqgktajT4w7K6qlFb7geA4AVvkf2Zl6yzrf
CauJIIh8PlC+w5WEIwYQJLcq5+zVuemEuBotFIoVUZbzhC9ZvDfmo/4hmWoyGZrBHQDjFyMCMGCSqGSIb3DQEJFTEWBBQFYKtq+bPILAvP
2ruIj47mWGFr2DBLBgkqhkiG9w0BCRQxPh48ADAAMQA0ADAAMAAwADAAMAAwADAAMwAxADQANABAAG8AcgBnAGEANgAxADQAMQAuAG8Abg
BsAGkAbgBlMDEwITAJBgUrDgMCGgUABBQ5ercLN2RMWE2Tk+ArAfsWVABbYgQIclp0jf3U3iICAggA
```

Quellenverweise

[i] IPSec – Wikipedia
[ii] WireGuard
[iii] StrongSwan – Ipsec VPN for Linux, Android, FreeBSD, Mac OS X, Windows
[3] Bedienungsanleitung ORGA 6141 online
[4] Dokumentation Remote Management Interface - ORGA 6141 online