



CHERRY eHealth Terminal ST-1506

Konfiguration VPN Client

KNOWLEDGE BASE

Inhaltsverzeichnis

Inhaltsverzeichnis	2
1 „VPN Client“ des ST-1506.....	3
2 Funktionsbeschreibung.....	3
3 Konfiguration VPN Client.....	3
3.1 Allgemeine Konfiguration.....	3
3.2 Konfiguration TLS Authentifizierung	5
3.3 Konfiguration MSCHAPv2 Authentifizierung	5
4 Beispielkonfigurationen nach strongSwan	6
4.1 VPN-Client ST-1506.....	6
4.2 VPN-Gateway.....	8
5 Kontakt.....	10

1 „VPN Client“ des ST-1506

Das Cherry eHealth Terminal ST-1506 unterstützt seit der Firmwareversion 3.0.0 den Aufbau von VPN-Netzwerkverbindung bzw. VPN-Tunnel nach IPSec/IKEv2 (<https://de.wikipedia.org/wiki/IPsec>).

Dieses Dokument dient als Leitfaden für die Konfiguration des ST-1506 und des VPN-Gateway.

2 Funktionsbeschreibung

Der **VPN Client** im ST-1506 unterstützt zwei verschiedene Authentifizierungsmethoden, entweder EAP-MSCHAPv2, Authentisierung mit Benutzername und Passwort, oder EAP-TLS, Authentisierung mit Client Zertifikat und Private Key. Die Konfiguration des VPN-Clients findet über die Remote Schnittstelle des ST-1506 statt und wird in Kapitel 3 beschrieben.

Wird der VPN-Client im ST-1506 aktiviert, so wird sofort eine Verbindung zum VPN-Gateway aufgebaut und jeglicher Netzwerkverkehr, wie zum Beispiel die Konnektor Verbindung oder die Remote Schnittstelle über den VPN Kanal geroutet und somit sind diese Schnittstellen nicht mehr aus dem lokalen Netzwerk erreichbar.

3 Konfiguration VPN Client

Im Folgenden wird die Konfiguration des VPN-Clients anhand des Browserinterface des ST-1506 beschrieben.

3.1 Allgemeine Konfiguration

Unter der Allgemeinen Konfiguration können folgende Elemente konfiguriert werden:

Konfiguration: Auswahl der zu verwendenden Authentisierung oder deaktivieren des VPN-Clients (Zustände: Aus, TLS, MSCHAPv2)

Server IP Adresse: IP-Adresse des VPN-Gateways

CA Zertifikat: CA-Zertifikat des VPN-Gateways in base64-Konvertierung. Dieses Zertifikat muss self signed sein, da keine Chain unterstützt wird.

Beispiel:

```
-----BEGIN CERTIFICATE-----
MIICQjCCACgAwIBAgIEKA/juTAKBgqhkJOPQQDAjBIMQswCQYDVQQGEwJBVDE
PMA0GA1UECAwGVmlbm5hMSgwJgYDVQQDDDB9TVDE1MDYtSVBTRUMtU0VDU
...
/055iMDMoDbUbdW/qzUnhceJWzHCoDye8i4uMa9cNU2Deh2yxmBnyNYbqLMA==
-----END CERTIFICATE-----
```

- CRL URI's:** optional kann eine oder mehrere CRL's verwendet werden.
(Format: https://address.com/filename, http://address.com/filename, ...
Die verwendeten Adressen müssen korrekt und erreichbar sein für MSCHAP
(Setting "revocation=ifuri")
- DPD delay:** Intervall in Sekunden in dem Dead Peer Detection (DPD) Pakete gesendet werden (default 20 Sekunden).
- DPD timeout:** Timeout Wert in Sekunden nachdem die VPN-Verbindung beendet wird, wenn keine Antwort auf die DPD-Pakete erfolgt (default 85 Sekunden)

VPN

Allgemein

Konfiguration: ☒ **Aus** ☐ **TLS** ☐ **MSCHAPv2**

Server IP Adresse:

CA Zertifikat:

CRL URI's:

DPD delay:

DPD timeout:

Speichern der geänderten Einstellungen: **SPEICHERN**

Durch Betätigen des Speicher Buttons werden die vorgenommenen Einstellungen gespeichert und das Netzwerkinterface wird neu gestartet.

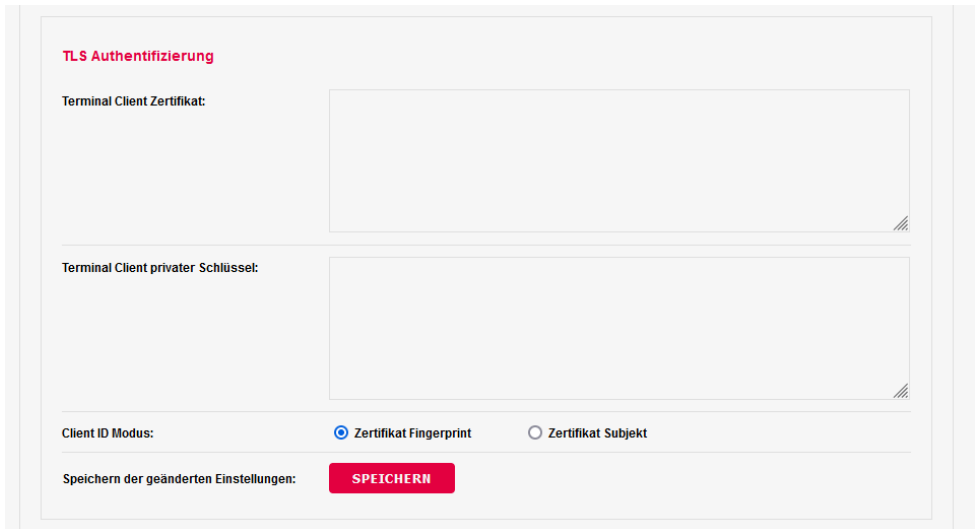
ACHTUNG:

Nach dem Aktivieren des VPN-Clients durch Auswahl einer Authentisierungsmethode wird sofort eine Verbindung zum VPN-Gateway aufgebaut und jeglicher Netzwerkverkehr, wie zum Beispiel die Konnektor Verbindung oder die Remote Schnittstelle über den VPN Kanal geroutet. Somit sind diese Schnittstellen nicht mehr aus dem lokalen Netzwerk erreichbar.

3.2 Konfiguration TLS Authentifizierung

Unter TLS Authentifizierung können die folgenden Elemente dieses Modus konfiguriert werden:

- Terminal Client Zertifikat:** selbsterstelltes Client Zertifikat in base64 Konvertierung.
- Terminal Client privater Schlüssel:** Private Key des Client Zertifikates in base64 Konvertierung.
- Client ID Modus:** Auswahl der zu verwendenden Client ID. Bei TLS werden die Optionen Zertifikat Fingerprint oder Zertifikat Subjekt angeboten.



The screenshot shows a web-based configuration interface for TLS authentication. At the top, the title "TLS Authentifizierung" is displayed in red. Below it, there are two large text input fields. The first is labeled "Terminal Client Zertifikat:" and the second is labeled "Terminal Client privater Schlüssel:". At the bottom of the form, there is a section for "Client ID Modus:" with two radio button options: "Zertifikat Fingerprint" (which is selected) and "Zertifikat Subjekt". Below this, there is a label "Speichern der geänderten Einstellungen:" followed by a red button with the text "SPEICHERN".

Durch Betätigen des Speicher Buttons werden die vorgenommenen Einstellungen gespeichert.

3.3 Konfiguration MSCHAPv2 Authentifizierung

Unter MSCHAPv2 Authentifizierung können die folgenden Elemente dieses Modus konfiguriert werden:

- Benutzername:** Benutzername welcher für die Authentisierung verwendet werden soll.
- Passwort:** Passwort welches für die Authentisierung verwendet werden soll.
- Client ID Modus:** Auswahl der zu verwendenden Client ID. Bei MSCHAPv2 werden die Optionen lokale IP Adresse, Seriennummer/Gerät oder Text angeboten.

Client ID Text: Bei Auswahl des Client ID Modus „Text“ kann hier eine selbst definierte Client ID vergeben werden. Als default Wert ist hier die ID hinterlegt, welche bei der Auswahl des Modus „Seriennummer/Gerät“ verwendet wird.

MSCHAPv2 Authentifizierung

Benutzername:

Passwort:

Client ID Modus: ☒ lokale IP Adresse ☐ Seriennummer/Gerät ☐ Text

Client ID Text:

Speichern der geänderten Einstellungen: **SPEICHERN**

Durch Betätigen des Speicher Buttons werden die vorgenommenen Einstellungen gespeichert.

4 Beispielkonfigurationen nach strongSwan

4.1 VPN-Client ST-1506

Nachfolgend ist eine äquivalente swanctl.conf Konfiguration des ST-1506 dargestellt:
(Authentifizierung über Username/Passwort bei EAP-Mschap, bzw Client Zertifikat bei EAP-TLS)

```
connections {
    connect_with_xeap_tls {
        local_addrs = 0.0.0.0
        remote_addrs = 10.2.0.64 # setable Server address
        dpd_delay=30 # setable
        dpd_timeout=150 # setable

        unique=replace
        send_cert=always

        vips=0.0.0.0

        local {
            auth = eap-tls
            certs = /usr/share/keys/ipsec/ipsec-peer.rsa4k.pem # Client Zertifikat
            id = "CN=ST1506-IPSEC-RSA4K-PEER-DEBUG, ST=Vienna, C=AT"
        }
        remote {
```

```

    auth = eap-tls
}
children {
    xtunnel {
        local_ts = 0.0.0.0-169.253.255.255, 169.255.0.0-254.255.255.255 # restricted from FW v4.0.0,
0.0.0.0 v3.0.0
        remote_ts = 0.0.0.0/0
        start_action=start
        dpd_action=start
        close_action=trap
        esp_proposals = aes256gcm64-sha256-sha384-sha512, aes256-sha256-sha384-sha512
        rekey_time = 24h
    }
}
# ike2
version = 2
send_certreq = yes
proposals = aes256gcm64-sha256-sha384-sha512-ecp384-ecp521-ecp384bp-ecp512bp-modp4096,
aes256-sha256-sha384-sha512-ecp384-ecp521-ecp384bp-ecp512bp-modp4096
rekey_time = 8h
}

connect_with_xeap_mschapv2 {
    local_addrs = 0.0.0.0
    remote_addrs = 10.2.0.64 # setable
    dpd_delay=30 # setable
    dpd_timeout=150 # setable

    unique=replace
    send_cert=never

    # ike2
    version = 2
    send_certreq = yes
    proposals = aes256gcm64-sha256-sha384-sha512-ecp384-ecp521-ecp384bp-ecp512bp-modp4096,
aes256-sha256-sha384-sha512-ecp384-ecp521-ecp384bp-ecp512bp-modp4096
    rekey_time = 8h

    vips=0.0.0.0

    local {
        auth = eap-mschapv2
        eap_id = theobroma # setable
        id = A12345678.ST1506.Cherry # setable from FW v4.0.0, otherwise empty !
    }
    remote {
        auth = pubkey
        revocation=ifuri
    }
}

```

```

children {
  xtunnel_chap {
    local_ts = 0.0.0.0-169.253.255.255, 169.255.0.0-254.255.255.255 # restricted from FW v4.0.0,
0.0.0.0 otherwise
    remote_ts = 0.0.0.0/0
    start_action=start
    dpd_action=start
    close_action=trap
    esp_proposals = aes256gcm64-sha256-sha384-sha512,aes256-sha256-sha384-sha512
    rekey_time = 24h
  }
}
}
}
}

```

Zur Information wird im Folgenden die cipher selection dargestellt, die der Strongswan Server beim Verbindungsaufbau sieht:

#11[CFG] received proposals:

IKE:AES_GCM_8_256/PRF_HMAC_SHA2_256/PRF_HMAC_SHA2_384/PRF_HMAC_SHA2_512/ECP_384/
ECP_521/ECP_384_BP/ECP_512_BP/MODP_4096,

IKE:AES_CBC_256/HMAC_SHA2_256_128/HMAC_SHA2_384_192/HMAC_SHA2_512_256/PRF_HMAC_S
HA2_256/PRF_HMAC_SHA2_384/PRF_HMAC_SHA2_512/ECP_384/ECP_521/ECP_384_BP/ECP_512_B
P/MODP_4096

10[CFG] received supported signature hash algorithms: sha256 sha384 sha512 identity

4.2 VPN-Gateway

Nachfolgend ist eine Ipsec.conf Konfiguration eines VPN Server (strongSwan 5.9.1) dargestellt:

```

# basic cipher setup
conn cipher-setup
# enforce IKEv2
keyexchange=ikev2
keyingtries=%forever
lifetime=12h
ikelifetime=24h
# configure dead peer detection (DPD)
dpddelay=45
dpdtimeout=80
dpdaction=restart

```

```

# basic network setup
conn network-setup
left=%defaulttroute
leftid=%any
leftsourceip=172.16.0.0/24
# allow connection from anyone
right=%any

```



```
# ASSIGN the peer an ip address within the given range
# ! do not use Link local address range here !
rightsourcelp=172.18.0.0/24
```

```
conn authenticate-with-eap-tls
# use basic cipher and network configuration
also=cipher-setup
also=network-setup
auto=add
# authenticate using eap-tls
rightauth=eap-tls
leftauth=eap-tls
authby=pubkey
leftcert=/etc/ipsec.d/certs/ipsec-site.secp384r1.pem
leftid="CN=ST1506-IPSEC-SECP384R1-SITE-DEBUG, ST=Vienna, C=AT"
rightid=%any
#or rightid="CN=*,ST=Vienna,C=AT"
```

```
conn authenticate-with-eap-mschapv2
# use basic cipher and network configuration
also=cipher-setup
also=network-setup
auto=add
## authenticate using eap-mschap
rightauth=eap-mschapv2
leftauth=pubkey
leftcert=/etc/ipsec.d/certs/ipsec-site-revoked-1.secp384r1.pem
leftid="CN=ST1506-IPSEC-SECP384R1-SITE-DEBUG, ST=Vienna, C=AT"
rightid=%any
#oder rightid="*.ST1506.Cherry" # v4.0.0: client id modus: Seriennummer
eap_identity=%identity
```

5 Kontakt

Bitte halten Sie bei Anfragen an den Technischen Support folgende Informationen bereit:

- Artikel- und Serien-Nr. des CHERRY eHealth-Kartenterminals
- Firmware-Version des CHERRY eHealth-Kartenterminals
- Name und Version verwendeter Software
- Bezeichnung und Hersteller Ihres Systems (Konnektor, Verwaltungssoftware)
- Betriebssystem und ggf. installierte Version eines Service Packs

Cherry Digital Health GmbH
Einsteinstraße 174
81677 München

Internet: www.cherry.de

Telefon: +49 (0) 9643 2061-100*

*zum Ortstarif aus dem deutschen Festnetz, abweichende Preise für Anrufe aus Mobilfunknetzen möglich