WORLDLINE

ORGA 6141 online
VPN Tutorial

Dokumentenkategorie

Tutorial zur Firmware 3.8.1

Herausgeber / Editor

Worldline Healthcare GmbH
Konrad-Zuse-Ring 1
24220 Flintbek
Internet: https://ingenico.de/healthcare
E-Mail: kontakt.ihc@ingenico.com

Copyrights

Versionsstand

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
0.7	22.12.2021	JBR	• Redaktionelle Korrekturen

Inhaltsverzeichnis

1. Motivation

Das stationäre eHealth-Kartenterminal ORGA 6141 online unterstützt seit der Firmwareversion 3.8.0 den Aufbau von VPN-Netzwerkverbindung bzw. VPN-Tunnel nach IPSec/IKEv2[i]. Dieses Tutorial dient als Leitfaden für die Erstellung und das Importieren der Konfiguration ins Kartenterminal sowie die Aktivierung der VPN-Netzwerkverbindung.

2. Systemvoraussetzung

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

1. VPN-Gateway
   - IPsec-Server (z.B. strongSwan[ii])
   - Öffentlich zugängliche IP-Adresse bzw. Domainnamen
   - Offene Netzwerk-Ports 500 und 4500
   - Unterstützung der Authentifizierungsmethoden EAP-MSCHAPv2 zur Authentifizierung der Clients mittels Benutzername-/Kennung, Passwort und Public-Key
   - Routing von Broadcast-Nachrichten

Die Konfiguration des VPN-Gateways wird in diesem Tutorial nicht näher beschrieben.

2. Kartenterminal
   - Benutzername-/Kennung und Passwort
   - CA-Zertifikat des VPN-Gateways
   - USB-Stick für dem Import der erstellten Konfiguration
   - Uhrzeit setzen via NTP

Wie die aktuell im Kartenterminal hinterlegten Zugangsdaten ausgelesen werden können, erfahren Sie im Kapital 7: Info zu Zugangsdaten

3. Erstellung der Konfigurationsdatei

Der Im- und Export von Konfigurationsparametern via USB-Stick ist im Kapitel 7.3.6 der Bedienungsanleitung[iii] beschrieben. Im Folgenden werden die Elemente bzgl. des VPN-Tunnels detaillierter dargestellt.

vpn_account_user	Benutzername-/kennung für die Authentifizierung des Kartenterminals am VPN-Gateways
vpn_gateway_addr	IP-Adresse oder Domainname des VPN-Gateways
ipsec_cacert	base64-kodiertes CA-Zertifikat des VPN-Gateways
ipsec_cert	base64-kodiertes Client-Zertifikat des Kartenterminals
ipsec_conf	alternativ, base64-kodierte Konfiguration des VPN-Clients im Kartenterminal

Für den Betrieb des VPN-Tunnels muss die Uhr 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.

ntp_addr IP-Adresse des bevorzugten NTP-Servers. Das kann z.B. einer im lokalen Netz oder z.B. von der Physikalisch-Technische Bundesanstalt in Braunschweig sein
ptbtime1.ptb.de = 192.53.103.108
ptbtime2.ptb.de = 192.53.103.104
ptbtime2.ptb.de = 192.53.103.103

mct_ntp_enabled Starten den NTP-Dienst bei jedem Neustart des Kartenterminals

Das CA-Zertifikat des VPN-Gateways muss für den Import, unabhängig vom Inhalt, base64-kodiert sein. Das kann mittels Kommandozeile schnell erledigt werden.

Beispiel für die base64-Konvertierung von ipsec_cert und ipsec_cacert:

root@ipsec-gw:~/tmp# cat cacert.pem
-----BEGIN CERTIFICATE-----
MIIFQDCCAyigAwIBAgIIOFuJaNtPARcwDQYJKoZIhvcNAQEMBQAwPjELMAkGA1UE
BhMCREUxFzAVBgNVBAoTDkIlQy1QbGF5Z3JvdW5kMRYwFAYDVQQDEw1JUFNFQyBS
b290IENBMB4XDTIxMDEwMTAwMDAwMFoXDTMxMTIzMTIzNTk1OVowPjELMAkGA1UE
BhMCREUxFzAVBgNVBAoTDkIlQy1QbGF5Z3JvdW5kMRYwFAYDVQQDEw1JUFNFQyBS
b290IENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA05OUjc8mv739
utReEg3HEo7GnNLe8U2Y6gD1UbnPW7IlxQD1weGE3Z6Al/3tVfeK52Ap0RNNL03d
Bt/pYwrKqIGORBWbIe62Cq9nABQ9WExMqeXOKQYwD80hA+IlkdaJCT/dK7yqjWNV
QoC2pT47Cxwp5uulea14JwdQz9nECDvGRgL2mIvmzXcf3bRSyptwgna0KPSU8RWI
gII4+V6zdLst1EjlNSSOc/hLo5elJYIxQZyWe7UNj5tmdTXD1lEVtUw5QGERyj9v
xH4jZGuJFh4BLpMZEYSpsBGyqeW/CzQLfUvhZsaktWGFNCAmPyu/STkG9AZhHRY9
E7ytqbDI5TdIYnqP4oFfMAnzs0jnjHGIT/xC7jDyzJX5RT0tW+d2PdFFoh16U1gM
c6Zx71XN9F2JH1Z/0LC+yoQ642Bu6wdUJctE2uvtVgcy7EkKLgE00z6E3SHKyHIP
bDB8yKFFUm+Bx+0rpiSl9g7B9FvIoerA7mLaFwN7q5N3evNTv2jaQPCF1s2w+Bdq
ZpWkROA5+XCP32GY0/ugntyRqnz99aHyUwoDuhQ9mjgUEbRRaycrgckeulkNVc2z
LtpQCkTRtG73SD4V1Iaa+ATeDb4MI2bFXuWuYELpm4xkuz5RW6oJxZ2fZPYqSHdK
swysJhZDdYqeH5tgnNXhwcSvPEMZRgkCAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB
/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFL+bfBCeHFkFOBgTU+0ZTI1qt2wZ
MA0GCSqGSIb3DQEBDAUAA4ICAQAagP1jimwhPjYQrVe9wpZ+TsPA7BNhKwqjmoBR
xUD7eBTQe5lhfxQEEcl/Y3Ft2NtmmiLryGcLyLZ6eeQl+FmrO5/kxxnjCL3/YBgt
BjNZGFHh3yku99enJj0T6yeTkw8XeOC0DPJAecZA/zmzmPhKQV8XjdWeLCPrrcBu
7xmooG9PxGnaXkRDpxQgozLdOUzBhfzRNU8GNn8/82zqy5grsr+CdyNIX4XyvlTn
odRVHLf9kXPmeHtCxaUcWDx3N35Wc5DRe6pVpc4D6DK/EV5xHYACfntfm9Rg100T
C32ELUS21LUhi8T+DIREJjce43SuBROkDtYgHvvlj8IFKWCHQ///k4F8nwSpIrKb
o52zp4fPPdT7hPQBK8rtWNuyZn+OZQMwrcwTMUFQTus1RPoN7+qe/m8eQJ0b1ubn
5Lkli9fxfhZsD1zL33UA3pn3PV4BL63x13ZFjlqBZMGKUkTsJ226UH5ytrRLtzSL
0rmm/pHZmZEOfqgCz8TCRxoFFqHM3bprba/E4wLKAvAjQ7ztxVkejqUd7GyIYx2b
CLIEMRs4XLHkqJ/HzBYBmd7gmOi2QXxhw9JQoveA9e9ZWNNnNK+6x7zINaisWsnz
kRzrukw9gwwmaiMFlUiICKdZ6GdYrL5joi8WnMJztEyM+xKRpkD9Hq/aavnDgGSn
N035xQ==
-----END CERTIFICATE-----

```
root@ipsec-gw:~/tmp#  base64 -w 0 cacert.pem
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZRRENDQXlpZ0F3SUJBZ0lJT0Z1SmFOdFBBUmN3RFFZSktvWklod
mNOQVFFTUJRQXdQakVMTUFrR0ExVUUKQmhNQ1JFVXhGekFWQmdOVkJBb1REa2xJUXkxUWJHRjVaM0p2ZFc1a01SW
XdGQVIEVlFRREV3MUpVRk5GUXlCUwpiMjkwSUVOQk1CNFhEVEl4TURFd01UQXdNREF3TUZvWERUTXhNVEl6TVRJek5
UazFPVm93UGpFTE1Ba0dBMVVFCkJoTUNSRVV4RnpBVkJnTlZCQW9URGtsSVF5MVFiR0Y1WjNKdmRXNWtNUll3RkFZRF
ZRUURFdzFKVUZORlF5QlMKYjI5MElFTkJNSUlDSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQWc4QU1JSUNDZ0tDQWdFQ
TA1T1VqYzhtdjczOEp1dFJlRWczSEVvN0duTkxlOFUyWTZnRDFVYm5QVzdJbHhRRDF3ZUdFM1o2QWwvM3RWZmVLNTJB
cDBSTk5MMDNkCkJ0L3BZd3JLcUlHT1JCV2JJZTYyQ3E5bkFCUTlXRXhNcWVYT0tRWXdEODBoQStJbGtkYUpDVC9kSzd5c
WpXTlYKUW9DMnBUNDdDeHdwNXV1bGVhMTRKd2RRejluRUNEdkdSZ0wybUl2bXpYY2YzYlJTeXB0d2duYTBLUFNVOFJX
SQpnSUk0K1Y2emRMc3QxRWpsTlNTT2MvaExvNWVJSllJeFFaeVdlN1VOajV0bWRUWEQxbEVWdFV3NVFHRVJ5ajl2CnhIN
GpaR3VKRmg0QkxwTVpFWVNwc0JHeXFlVy9DelFMZlV2aFpzYWt0V0dGTkNBbVB5dS9TVGtHOUFaaEhSWTkKRTd5dHFiR
Ek1VGRJWW5xUDRvRmZNQW56czBqbmpIR2xUL3hDN2pEeXpKWDVSVDB0VytkMlBkRkZvaDE2VTFnTQpjNlp4NzFYTjlGM
kpIMVovMExDK3lvUTY0MkJ1NndkVUpjdEUydXZ0VmdjeTdFa0tMZ0UwMHo2RTNTSEt5SElQCmJEQjh5S0ZGVW0rQngrMHJ
waVNsOWc3QjlGdklvZXJBN21MYUZ3TjdxNU4zZXZOVHYyamFRUENGMXMydytCZHEKWnBXa1JPQTUrWENQMzJHWTAvd
WdudHlScW56OTlhSHlVd29EdWhROW1qZ1VFYlJSYXljcmdja2V1bGtOVmMyegpMdHBRQ2tUUnRHNzNTRDRWMUlhYStBV
GVEYjRNSTJiRlh1V3VZRUxwbTR4a3V6NVJXNm9KeFoyZlpQWXFTSGRLCnN3eXNKaFpEZFlxZUg1dGduTlhod2NTdlBFTVp
SZ2tDQXdFQUFhTkNNRUF3RHdZRFZSMFRBUUgvQkFVd0F3RUlKL3pBT0JnTlZIUThCQWY4RUJBTUNBUVl3SFFZRFZSM
E9CQllFRkwrYmZCQ2VIRmtGT0JnVFUrMFpUSTFxdDJ3WgpNQTBHQ1NxR1NJYjNEUUVCREFVQUE0SUNBUUFhZ1Axamlt
d2hQallRclZlOXdwWitUc1BBN0JOaEt3cWptb0JSCnhVRDdlQlRRZTVsaGZ4UUVFY2wvWTNGdDJOdG1taUxyeUdjTHlMWjZlZ
VFsK0Ztck81L2t4eG5qQ0wzL1lCZ3QKQmpOWkdGSGgzeWt1OTllbkpqMFQ2eWVUa3c4WGVPQzBEUEpBZWNaQS96bXptU
GhLUVY4WGpkV2VMQ1BycmNCdQo3eG1vb0c5UHhHbmFYa1JEcHhRZ296TGRPVXpCaGZ6Uk5VOEdObjgvODJ6cXk1Z3Jz
citDZHlOSVg0WHl2bFRuCm9kUlZITGY5a1hQbWVIdEN4YVVjV0R4M04zNVdjNURSZTZwVnBjNEQ2REsvRVY1eEhZQUNmb
nRmbTlSZzEwMFQKQzMyRUxVUzlxTFVoaThUK0RJUkVKamNlNDNTdUJST2tEdFlnSHZ2SWo4SUZLV0NIUS8vL2s0Rjhud1
NwSXJLYgpvNTJ6cDRmUFBkVDdoUFFCSzhydFdOdXlabitPWlFNd3Jjd1RNVUZRVHVzMVJQb043K3FIL204ZVFKMGlxdWJu
CjVMa2xpOWZ4Zmhac0QxekwzM1VBM3BuM1BWNEJMNjN4MTNaRmpscUJaTUdLVWtUc0oyMjZVSDV5dHJSTHR6U0wKM
HJtbS9wSFptWkVPZnFnQ3o4VENSeG9GRnFITTNicHJiYS9FNHdMS0F2QWpRN3p0eFZrZWpxVWQ3R3lJWXgyYgpDTElFTV
JzNFhMSGtxSi9lekJZQm1kN2dtT2kyUVh4aHc5SlFvdmVBOWU5WldOTm5OSys2eDd6SU5haXNXc256CmtSenJ1a3c5Z3d3b
WFpTUZsVWlJQ0tkWjZHZFlyTDVqb2k4V25NSnp0RXlNK3hLUnBrRDllcS9hYXZuRGdHU24KTjAzNXhRPT0KLS0tLS1FTkQg
Q0VSVElGSUNBVEUtLS0tLQo=
```

Das base64 kodierte Zertifikat muss kopiert und in die nachfolgend beschriebene Konfigurationsdatei an entsprechender Stelle „ipsec_cacert“ bzw „ipsec_cert“ eingefügt werden.

Sollte im Speziellen die in Kapital 8 aufgeführte Standardkonfiguration des Kartenterminals mit dem entsprechenden VPN-Gateway nicht kompatibel sein, kann mittels ipsec_conf eine alternative Konfiguration ins Kartenterminal übertragen werden. Diese muss gemäß der im Kartenterminal integrierten VPN-Lösung strongSwan[iv] aufgebaut und analog zum ipsec_cacert konvertiert werden.

Wenn Sie eine alternative Konfiguration vorgeben möchten, ist dabei folgendes zu beachten:

- Im Abschnitt *local* (siehe Abschnitt Kartenterminal) muss bei EAP-MSCHAPv2 die eap_id mit %EAP_IDENTINY% konfiguriert sein, da dieser Wert beim Systemstart automatisch aus dem Benutzerdaten übernommen wird
- Im Abschnitt *children* muss updown = /sbin/vpn_tunnel_updown.sh gesetzt sein.
- Bei EAP-MSCHAPv2 werden die Secrets am Ende aus /tmp/swanctl/swanctl.secrets inkludiert.

Beispiel einer Import-Konfigurationsdatei:

```
root@ipsec-gw:~/tmp# cat vpn_testgateway_import.cfg
# set idle text
welcome_message=Ike2 eHealth KT(Test)

# setup network
dhcp_enabled=true
domain_name_server=192.168.221.1

# ntp ptbtime1.ptb.de
ntp_addr=192.53.103.108
mct_ntp_enabled=true
```

```
# set account config ORGA6141 : '123456'
vpn_account_user=ORGA6141

# set address of vpn gateway
vpn_gateway_addr=ipsec-gw.ihcdev.de

# remove existing ca-certs and alternative configs
ipsec_cacert=
ipsec_conf=

# stores the followering ca-certificat under the filename ‘test_ihcdev.cacert.pem’
import_filename=test_ihcdev.cacert.pem

# data of ca-certificate
# !! all data in one line !!
ipsec_cacert=
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZRRENDQXlpZ0F3SUJBZ0lJT0Z1SmFOdFBBUmN3RFFZSktvWklod
mNOQVFFTUJRQXdQakVMTUFrR0ExVUUKQmhNQ1JFVXhGekFWQmdOVkJBb1REa2xJUXkxUWJHRjVaM0p2ZFc1a01SW
XdGQVIEVlFRREV3MUpVRk5GUXlCUwpiMjkwSUVOQk1CNFhEVEl4TURFd01UQXdNREF3TUZvWERUTXhNVEl6TVRJek5
UazFPVm93UGpFTE1Ba0dBMVVFCkJoTUNSRVV4RnpBVkJnTlZCQW9URGtsSVF5MVFiR0Y1WjNKdmRXNWtNUll3RkFZRF
ZRUURFdzFKVUZORlF5QlMKYjI5MElFTkJNSUlDSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQWc4QU1JSUNDZ0tDQWdFQ
TA1T1VqYzhtdjczOQp1dFJlRWczSEVvN0duTkxlOFUyWTZnRDFVYm5QVzdJbHhRRDF3ZUdFM1o2QWwvM3RWZmVLNTJB
cDBSTk5MMDNkCkJ0L3BZd3JLcUlHT1JCV2JJZTYyQ3E5bkFCUTlXRXhNcWVYT0tRWXdEODBoQStJbGtkYUpDVC9kSzd5c
WpXTlYKUW9DMnBUNDdDeHdwNXV1bGVhMTRKd2RRejluRUNEdkdSZ0wybUl2bXpYY2YzYlJTeXB0d2duYTBLUFNVOFJX
SQpnSUk0K1Y2emRMc3QxRWpsTlNTT2MvaExvNWVJSllJeFFaeVdlN1VOajV0bWRUWEQxbEVWdFV3NVFHRVJ5ajl2CnhIN
GpaR3VKRmg0QkxwTVpFWVNwc0JHeXFlVy9DelFMZlV2aFpzYWt0V0dGTkNBbVB5dS9TVGtHOUFaaEhSWTkKRTd5dHFiR
Ek1VGRJWW5xUDRvRmZNQW56czBqbmpIR2xUL3hDN2pEeXpKWDVSVDB0VytkMlBkRkZvaDE2VTFnTQpjNlp4NzFYTjlGM
kpIMVovMExDK3lvUTY0MkJ1NndkVUpjdEUydXZ0VmdjeTdFa0tMZ0UwMHo2RTNTSEt5SElQCmJEQjh5S0ZGVW0rQngrMHJ
waVNsOWc3QjlGdklvZXJBN21MYUZ3TjdxNU4zZXZOVHYyamFRUENGMXMydytCZHEKWnBXa1JPQTUrWENQMzJHWTAvd
WdudHlScW56OTlhSHlVd29EdWhROW1qZ1VFYlJSYXljcmdja2V1bGtOVmMyegpMdHBRQ2tUUnRHNzNTRDRWMUlhYStBV
GVEYjRNSTJiRlh1V3VZRUxwbTR4a3V6NVJXNm9KeFoyZlpQWXFTSGRLCnN3eXNKaFpEZFlxZUg1dGduTlhod2NTdlBFTVp
SZ2tDQXdFQUFhTkNNRUF3RHdZRFZSMFRBUUgvQkFVd0F3RUIKL3pBT0JnTlZIUThCQWY4RUJBTUNBUVI3SFFZRFZSM
E9CQllFRkwrYmZCQ2VIRmtGT0JnVFUrMFpUSTFxdDJ3WgpNQTBHQ1NxR1NJYjNEUUVCREFVQUE0SUNBUUFhZ1Axamlt
d2hQallRclZlOXdwWitUc1BBN0JOaEt3cWptb0JSCnhVRDdlQlRRZTVsaGZ4UUVFY2wvWTNGdDJOdG1taUxyeUdjTHlMWjZlZ
VFsK0Ztck81L2t4eG5qQ0wzL1lCZ3QKQmpOWkdGSGgzeWt1OTllbkpqMFQ2eWVUa3c4WGVPQzBEUEpBZWNaQS96bXptU
GhLUVY4WGpkV2VMQ1BycmNCdQo3eG1vb0c5UHhHbmFYa1JEcHhRZ296TGRPVXpCaGZ6Uk5VOEdObjgvODJ6cXk1Z3Jz
citDZHlOSVg0WHl2bFRuCm9kUlZITGY5a1hQbWVIdEN4YVVjV0R4M04zNVdjNURSZTZwVnBjNEQ2REsvRVY1eEhZQUNmb
nRmbTlSZzEwMFQKQzMyRUxVUzIxTFVoaThUK0RJUkVKamNlNDNTdUJST2tEdFlnSHZ2SWo4SUZLV0NIUS8vL2s0Rjhud1
NwSXJLYgpvNTJ6cDRmUFBkVDdoUFFCSzhydFdOdXlabitPWlFNd3Jjd1RNVUZRVHVzMVJQb043K3FlL204ZVFKMGIxdWJu
CjVMa2xpOWZ4Zmhac0QxekwzM1VBM3BuM1BWNEJMNjN4MTNaRmpscUJaTUdLVWtUc0oyMjZVSDV5dHJSTHR6U0wKM
HJtbS9wSFptWkVPZnFnQ3o4VENSeG9GRnFITTNicHJiYS9FNHdMS0F2QWpRN3p0eFZrZWpxVWQ3R3lJWXgyYgpDTElFTV
JzNFhMSGtxSi9lekJZQm1kN2dtT2kyUVh4aHc5SlFvdmVBOWU5WldOTm5OSys2eDd6SU5haXNXc256CmtSenJ1a3c5Z3d3b
WFpTUZsVWlJQ0tkWjZHZFlyTDVqb2k4V25NSnp0RXlNK3hLUnBrRDlIcS9hYXZuRGdHU24KTjAzNXhRPT0KLS0tLS1FTkQg
Q0VSVElGSUNBVEUtLS0tLQo=
```

4. Erzeugung eines Certification-Signing-Request (CSR)

Soll die Authentifizierung mittels Public-Key erfolgen, muss für das Clientzertifikat entsprechend ein 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.

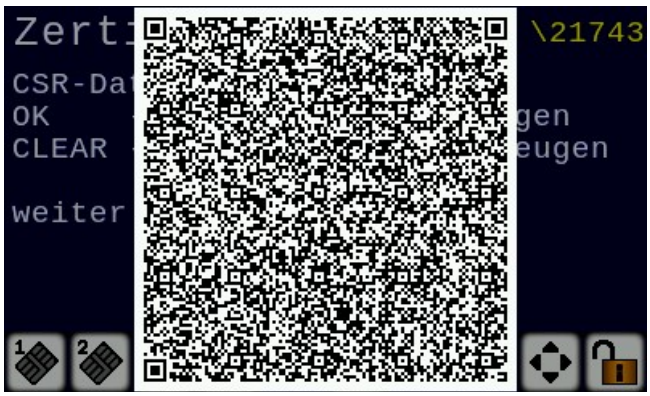
Mit Menüpunkt [21743] wird die Erzeugung eines CSR gestartet. Ist kein zuvor generierter Schlüssel vorhanden, wir automatisch ein **ECC-Schlüssel auf Basis der „brainpool256r1“-Kurve** generiert. Andernfalls erfolgt eine Auswahl

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	= SH
L	= Flintbek
O	= INGENICO HEALTHCARE GMBH
CN	= (Seriennummer des Kartenterminals)@orga6141.online

Zum Schluss wird der CSR per QR-Code angezeigt.



Der im QR-Code enthaltener CSR kann dann eingescannt und für die Erstellung eines Clientzertifikates durch die herausgebende Stelle des VPN-Betreibers benutzt werden. Das erstellte Clientzertifikat wird dann per USB-Stick ins Kartenterminal importiert.

CSR-Daten:

$ cat csr

-----BEGIN CERTIFICATE REQUEST-----
MIIBcjCCARgCAQAweTELMAkGA1UEBhMCREUxCzAJBgNVBAgMAlNIMREwDwYDVQQH
DAhGTElOVEJFSzEhMB8GA1UECgwYSU5HRU5JQ08gSEVBTFRIQ0FSRSBHTUJIMScw
JQYDVQQDDB4wMTQwMDAwMDAwMzE0NEBvcmdhNjE0MS5vbmxpbmUwWjAUBgcqhkjO
PQIBBgkrJAMDAggBAQcDQgAEUgmZju915TFI8CqvrIDupxNkmIA0ejHUA0E8Svuy
CLWoiJAIMRgeEUuDtTpNcAOuymfuROqA8JmScE/1zX5AEKA8MDoGCSqGSIb3DQEJ
DjEtMCswKQYDVR0RBCIwIIEeMDE0MDAwMDAwMDMxNDRAb3JnYTYxNDEub25saW5l
MAoGCCqGSM49BAMCA0gAMEUCID2UFOazk2fdfPKppn6HJlm1O43hT6xIkfREjWmO
2D/cAiEAiaIdkS6EZwe27YEA0YZ9CQ/FPOKiXga3CpNVDfKzuGk=
-----END CERTIFICATE REQUEST-----

```
$ openssl req -text -noout -in csr
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = DE, ST = SH, L = FLINTBEK, O = INGENICO HEALTHCARE GMBH, CN =
01400000003144@orga6141.online
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:52:09:99:8e:ef:75:e5:31:48:f0:2a:af:ac:80:
                    ee:a7:13:64:98:80:34:7a:31:d4:03:41:3c:4a:fb:
                    b2:08:b5:a8:88:90:08:31:18:1e:11:4b:83:b5:3a:
                    4d:70:03:ae:ca:67:ee:44:ea:80:f0:99:92:70:4f:
                    f5:cd:7e:40:10
                ASN1 OID: brainpoolP256r1
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                email:01400000003144@orga6141.online
    Signature Algorithm: ecdsa-with-SHA256
         30:45:02:20:3d:94:14:e6:b3:93:67:dd:7c:f2:a9:a6:7e:87:
         26:59:b5:3b:8d:e1:4f:ac:48:91:f4:44:8d:69:8e:d8:3f:dc:
         02:21:00:89:a2:1d:91:2e:84:67:07:b6:ed:81:00:d1:86:7d:
         09:0f:c5:3c:e2:a2:5e:06:b7:0a:93:55:0d:f2:b3:b8:69
```

Beispielaufruf zur Erstellung des Clientzertifikates:

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

Clientzertifikat:

```
$ openssl x509 -text -noout -in 01400000003144@orga6141.online-cert.pem
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            75:16:9a:20:aa:01:be:3c:ee:88:62:bd:54:93:df:8b:ab:c1:d7:fb
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = DE, O = Ingenico Healthcare GmbH, CN = IHC-CA01 TEST
        Validity
            Not Before: Aug 19 11:11:12 2021 GMT
            Not After : Aug 19 11:11:12 2022 GMT
        Subject: C = DE, ST = SH, L = FLINTBEK, O = INGENICO HEALTHCARE GMBH, CN =
01400000003144@orga6141.online
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:52:09:99:8e:ef:75:e5:31:48:f0:2a:af:ac:80:
                    ee:a7:13:64:98:80:34:7a:31:d4:03:41:3c:4a:fb:
                    b2:08:b5:a8:88:90:08:31:18:1e:11:4b:83:b5:3a:
                    4d:70:03:ae:ca:67:ee:44:ea:80:f0:99:92:70:4f:
                    f5:cd:7e:40:10
                ASN1 OID: brainpoolP256r1
    Signature Algorithm: ecdsa-with-SHA256
        30:64:02:30:1d:79:3c:6a:b9:87:fa:20:29:e4:f6:3d:37:4e:
        3d:44:5c:e0:cc:df:59:11:06:60:e0:bc:3f:bd:41:33:1f:eb:
        0e:99:76:23:50:86:ba:97:13:07:ed:b4:41:03:04:61:02:30:
        29:18:1b:18:79:8c:c8:e6:36:e3:6d:e0:20:3b:83:76:51:05:
        6d:40:70:0a:1f:b4:fd:e7:41:a3:4a:c7:74:3e:5b:4d:37:d7:
        13:b8:fa:b3:c2:71:43:84:20:fb:ab:b8
```

5. Import der Konfigurationsdatei

Nachdem die erstellte Konfigurationsdatei auf einen FAT32 formatierten USB-Stick ins Stammverzeichnis 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 ein Log auf dem USB-Stick angelegt. In diesem 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!

Der Import ist im Kapitel 7.3.6.1 der Bedienungsanleitung[v] beschrieben.

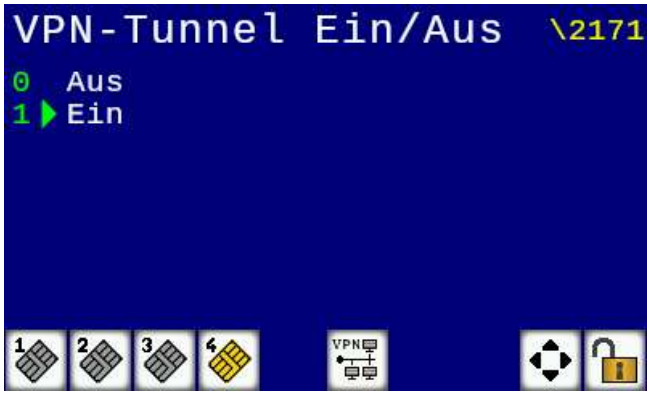
6. Aktivierung des VPN-Tunnel

Für die Aktivierung des VPN-Tunnels gehen Sie ins Menü [*IPSec VPN* \217].

Im Falle von EAP-MSCHAPv2 müssen nach dem Import zuerst die Zugangsdaten unter dem Menüpunkt 21742 vervollständigen werden.

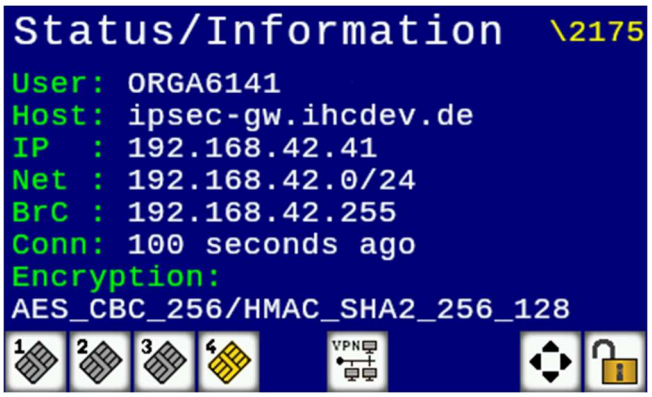
Drücken Sie die Taste ‚CLEAR' und ergänzen das Password.

Nun sollten alle benötigten Daten vorhanden sein und Sie können unter dem Menüpunkt [1] den VPN-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.

Der Status des VPN-Tunnels kann unter dem Menüpunkt [5] abgefragt werden.



Angezeigt werden im Betrieb:

- **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.** Ausgehandelten Verschlüsselungsmethoden

Im Falle eines Fehlers bzw. einer Störung werden

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

angezeigt.

7. Informationen zu Zugangsdaten

Unter dem Menüpunkt [217431] können Informationen bzgl. der aktuell verwendeten Zugangsdaten abgefragt werden.

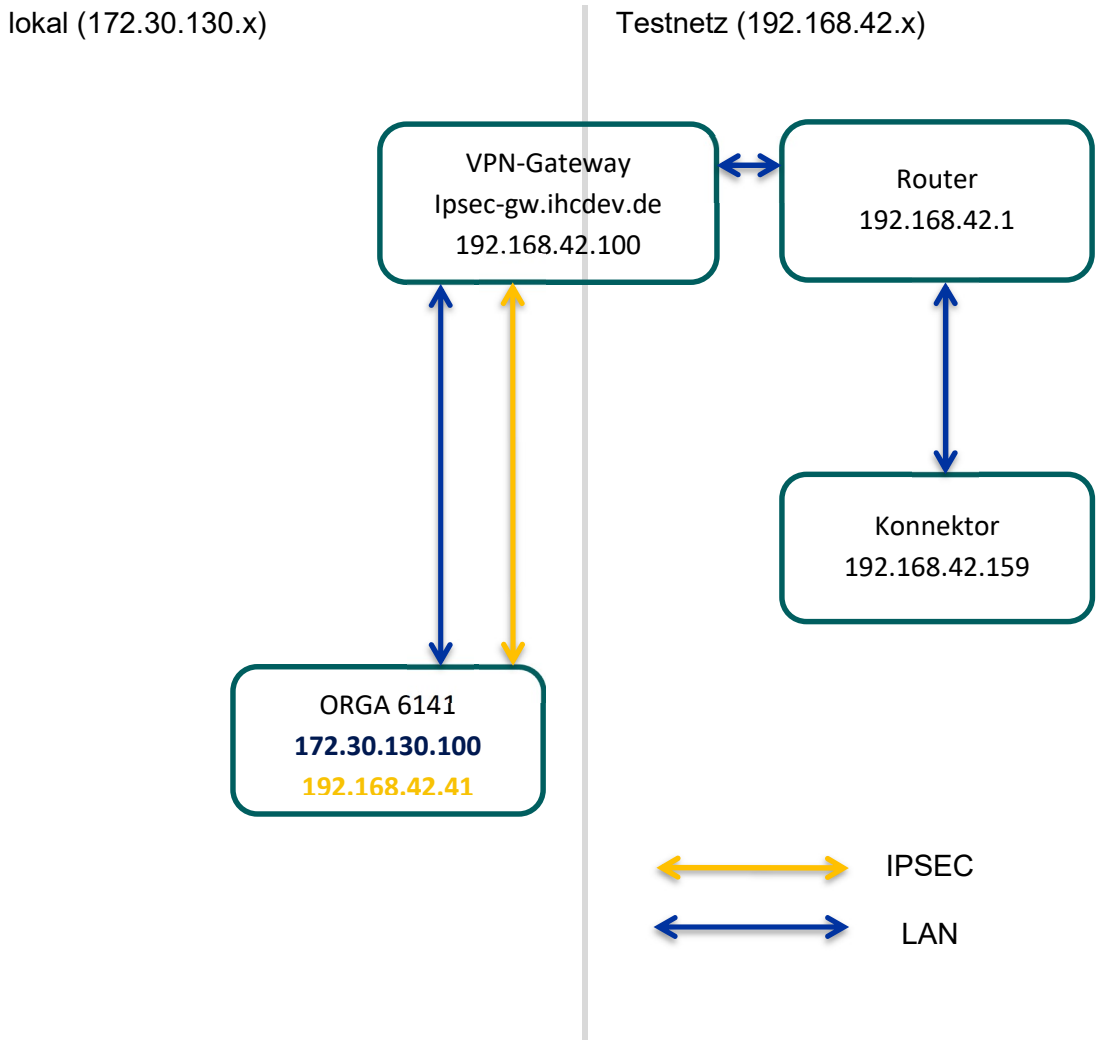
Angezeigt werden im Betrieb:

- **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

8. Konfigurationen im Testumfeld

Nachfolgend sind die Topologie sowie die verwendeten Konfigurationen für das VPN-Gateway als auch für das Kartenterminal, die in diesem Testumfeld benutzt wurden, beschrieben.

Topologie


lokal (172.30.130.x)
Testnetz (192.168.42.x)
VPN-Gateway
Ipsec-gw.ihcdev.de
192.168.42.100
Router
192.168.42.1
Konnektor
192.168.42.159
ORGA 6141
172.30.130.100
192.168.42.41
IPSEC
LAN

VPN-Gateway

Auf dem VPN-Gateway setzen wir zurzeit eine strongSwan v5.9.3 Instanz ein. Konfiguriert wird eine Authentifizierung des Servers hierbei per Zertifikat. Beim Client (Kartenterminal) wird die Authentifizierung per User/Passwort nach eap-mschapv2 sowie in einer Verbindung mit einem Public-Key konfiguriert. Die IP-Adressen im VPN-Netz werden per DHCP den Clients zugewiesen.

root@ipsec-gw:/usr/local/etc# cat swanclt.conf

```
connections {
  rw_pub {
    local_addrs = ipsecgw-dev.ihcdev.de
    pools = dhcp
    local {
      auth = pubkey
      certs = server-cert.pem
      id = ipsecgw-dev.ihcdev.de
    }
    remote {
      auth = pubkey
    }
    children {
      net {
        local_ts  = 192.168.42.0/24
        updown = /usr/local/libexec/ipsec/_updown iptables
      }
    }
    version = 2
    fragmentation = yes
    encap = yes
  }

  rw_eap {
    local_addrs = ipsecgw-dev.ihcdev.de
    pools = dhcp
    local {
      auth = pubkey
      certs = server-cert.pem
      id = ipsecgw-dev.ihcdev.de
    }
    remote {
      auth = eap-mschapv2
            eap_id = %any
    }
    children {
      net {
        local_ts  = 192.168.42.0/24
        updown = /usr/local/libexec/ipsec/_updown iptables
      }
    }
    version = 2
    fragmentation = yes
    encap = yes
  }
}
secrets {
   eap-orga6141-ths {
      id = ORGA6141-THS
            secret = 123456
   }
}
# end
```

Kartenterminal

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

```
> cat swanctl.conf
# swanctl.conf - strongSwan IPsec configuration file
connections {
  ike2 {
    version = 2
    local_addrs = %any
    remote_addrs = ipsec-gw.ihcdev.de
    vips = 0.0.0.0
    dpd_delay = 20s
    proposals = aes256-prfsha256-sha256-modp2048, default
    local {
      auth = eap-mschapv2
      eap_id = ORGA6141-THS
    }
    remote {
      auth = pubkey
      id = %any
      cacerts = test_ihcdev.cacert.pem
    }
    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-modp2048, default
      }
    }
  }
}
include /tmp/swanctl/swanctl.secrets


> cat /tmp/swanctl/swanctl.secrets
# swanctl.secrets - strongSwan IPsec secrets file
secrets {
  eap-ORGA6141-THS {
    id = ORGA6141-THS
    secret = 123456
  }
}
```

9. Quellenverweise

[i] IPsec – Wikipedia
[ii] strongSwan - IPsec VPN for Linux, Android, FreeBSD, Mac OS X, Windows
[iii] AGD ORGA 6141 online_V21.12.1.pdf
[iv] strongSwan - swanctl.conf
[v] AGD ORGA 6141 online_V21.12.1.pdf