

## IPSec Anbindung eines Windows-10-Clients über IKEv2-Public-Key-Authentifizierung mit anschließender Benutzerauthentifizierung über EAP MS-CHAPv2

**Digitalisierungsbox 2 Release 16.40.2.12.00**

**Geräte** Digitalisierungsbox Premium 2/Smart 2

**Release** 16.40.2.12.00

**Datum** 23.09.22

## Inhaltsverzeichnis

<b>1 EINLEITUNG.....</b>	<b>3</b>
<b>2 TECHNISCHE UND PLANERISCHE VORAUSSETZUNGEN.....</b>	<b>4</b>
2.1 IPSEC-EINSTELLUNGEN.....	4
<b>3 ERSTELLUNG UND EXPORT DER ZERTIFIKATE.....</b>	<b>6</b>
3.1 HINWEISE ZUM THEMA ERSTELLUNG CA-SIGNIERTER BENUTZERZERTIFIKATE.....	6
3.2 ERSTELLUNG DES AUF DER DIGITALISIERUNGSBOX ZU VERWENDENDEN PRIVATEN SCHLÜSSELS.....	7
3.3 ERSTELLUNG DES AUF DER DIGITALISIERUNGSBOX ZU VERWENDENDEN BENUTZERZERTIFIKATS.....	7
3.4 EXPORT DES AUSSTELLERZERTIFIKATES (CA-ZERTIFIKATES).....	12
3.5 EXPORT DES BENUTZERZERTIFIKATES SOWIE DES PRIVATEN SCHLÜSSELS.....	13
<b>4 KONFIGURATION DER DIGITALISIERUNGSBOX.....</b>	<b>15</b>
4.1 DYNDNS-KONFIGURATION.....	15
4.2 AKTIVIERUNG VON IPSEC.....	17
4.3 IMPORT DER ZERTIFIKATE.....	17
4.4 KONFIGURATION DER IKE (PHASE 1) UND IPSEC (PHASE 2) PROPOSALS.....	20
4.4.1 IKE (Phase 1) Proposal.....	20
4.4.2 IPsec (Phase 2) Proposal.....	22
4.5 KONFIGURATION DER IPSEC-VERBINDUNG AUF DER DIGITALISIERUNGSBOX 2.....	24
<b>5 KONFIGURATION DES WINDOWS-10-CLIENTS.....</b>	<b>27</b>
5.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT).....	27
5.2 KONFIGURATION DER IPSEC-VERBINDUNG.....	30
5.3 AUFBAU DER IPSEC-VERBINDUNG.....	31
<b>6 ANHANG.....</b>	<b>33</b>
6.1 ERSTELLUNG DER VPN-VERBINDUNG ÜBER WINDOWS 10 POWERSHELL.....	33
6.2 SPLIT-TUNNELING AKTIVIEREN.....	34

## 1 Einleitung

Mit der Softwareversion 16.40.2.12.00 unterstützt die Digitalisierungsbox 2 die Authentifizierungsmethode *IKEv2 Öffentlicher Schlüssel mit EAP MS-CHAPv2*. Diese Authentifizierungsmethode kann verwendet werden, um einen Windows-10-Client über den Windows-eigenen IPSec-Client an die Digitalisierungsbox 2 per IPSec anzubinden. In diesem Anwendungsfall baut der Windows-10-Client die IPSec-Verbindung zur Digitalisierungsbox 2 auf. Die Digitalisierungsbox 2 ist somit aus Sicht des Windows-Clients der VPN-Fernzugangsserver.

Die gegenseitige Authentifizierung der beiden Verbindungspartner erfolgt bei der Methode *Öffentlicher Schlüssel mit EAP MS-CHAPv2* über zwei verschiedene Authentifizierungsmethoden:

- (1) Die Authentisierung der Digitalisierungsbox 2 gegenüber dem Windows-10-Client erfolgt über ein auf der Digitalisierungsbox installiertes Zertifikat. Dieses Zertifikat ist ein von einem Aussteller (CA – Certificate Authority) signiertes Zertifikat. Die Digitalisierungsbox 2 sendet das Zertifikat an den Windows-10-Client, und dieser überprüft daraufhin dessen Gültigkeit. Bei erfolgreicher Überprüfung sendet der Client eine Bestätigung an die Digitalisierungsbox.

**Hinweis:**

Der öffentliche Schlüssel ist neben den Angaben zur eindeutigen Identifikation des Eigentümers des Zertifikates, den Angaben zur Nutzung des Zertifikates und den Sicherheitsmerkmalen (z. B. Fingerprint) im Zertifikat enthalten.

- (2) Die Authentisierung des Windows-10-Clients gegenüber der Digitalisierungsbox erfolgt per EAP MS-CHAPv2. Nach Erhalt der Zertifikatsbestätigung fordert die Digitalisierungsbox den Client auf, sich per EAP MS-CHAP (Benutzername/Passwort) zu authentifizieren. Hierzu müssen auf der Digitalisierungsbox entsprechende Benutzerkonten konfiguriert sein. Erst nach erfolgreicher Benutzerauthentifizierung wird die IPSec-Verbindung aufgebaut.

**Hinweis:**

Die Digitalisierungsbox erlaubt die Konfiguration mehrerer Benutzerkonten pro IPSec-Verbindung. Mehrere Benutzer können somit die IPSec-Verbindung gemeinsam nutzen. Voraussetzung ist jedoch die Eindeutigkeit der Benutzerkonten.

**Wichtig:**

Die hier erläuterte Konfiguration kann als Vorlage für die Verwendung anderer IPSec-Clients dienen, vorausgesetzt diese unterstützen ebenfalls die Authentifizierungsmethode *Öffentlicher Schlüssel mit EAP MS-CHAPv2*. Die Verwendung des Windows-10-eigenen VPN-Clients dient hier als Beispiel zur Demonstration der Funktionsweise.

Die Erstellung der Zertifikate sowie die Konfiguration der Digitalisierungsbox sind für diesen Anwendungsfall allgemein gültig.

## 2 Technische und planerische Voraussetzungen

Folgende Voraussetzungen müssen für die Anbindung erfüllt sein:

- Der Internetzugang muss auf der Digitalisierungsbox konfiguriert sein.
- Die öffentliche IP-Adresse der Digitalisierungsbox muss entweder statisch oder der Hostname per DNS auflösbar sein. In unserem Anwendungsfall nutzen wir DynDNS, um den Hostnamen bei Änderung der IP-Adresse automatisch zu aktualisieren.
- Das Zertifikat des Ausstellers (CA-Zertifikat), das Benutzerzertifikat sowie der dazugehörige Private Schlüssel müssen vorhanden sein oder erstellt werden. Hierbei sind die Zertifikatsanforderungen, die Windows an die Nutzung des Zertifikats zur Authentifizierung an einem VPN-Fernzugangsserver stellt, unbedingt zu beachten. In unserem Anwendungsbeispiel erstellen wir die Zertifikate sowie Schlüssel selbst. Mehr hierzu im [Kapitel 3](#).
- Auf der Digitalisierungsbox müssen das Zertifikat des Ausstellers (CA-Zertifikat), das Benutzerzertifikat sowie der dazugehörige Private Schlüssel installiert werden.
- Auf dem Client muss das Ausstellerzertifikat (CA-Zertifikat) installiert werden, wenn die Zertifikate wie in unserem Anwendungsbeispiel selbst erzeugt wurden.
- Der Client muss Zugang zum Internet haben.
- Die IPSec-Verbindung muss sowohl auf der Digitalisierungsbox als auch auf dem Client konfiguriert werden.

### 2.1 IPSec-Einstellungen

In unserem Anwendungsbeispiel bestimmt der Windows-10-VPN-Client die verfügbaren IPSec-Einstellungen. Um die Kompatibilität mit dem Windows-10-Client zu gewährleisten, sind folgende IKE bzw. IPSec Proposals auf der Digitalisierungsbox erforderlich:

#### IKE (Phase 1) Proposal:

<b>IKE Version</b>	IKEv2
<b>Verschlüsselungsalgorithmus</b>	AES256-CBC
<b>Integritätsalgorithmus</b>	SHA2-256_128 HMAC
<b>Pseudozufallsfunktion</b>	SHA2-256-PRF
<b>Diffie-Hellmann-Gruppe</b>	MODP1024 (2)

#### IPSec (Phase 2) Proposal:

<b>Verschlüsselungsalgorithmus</b>	AES256-CBC
<b>Integritätsalgorithmus</b>	SHA1-HMAC
<b>Diffie-Hellmann-Gruppe (PFS)</b>	MODP1024 (2)

**Hinweis:**

MODP1024 (2) sowie SHA1-HMAC sind aus sicherheitstechnischer Sicht als schwach einzustufen. Man kann jedoch die vom Windows-10-Client verwendeten IPSec-Einstellungen über PowerShell-Kommandos anpassen. Auf diesem Weg sind auch sehr sichere IPSec-Einstellungen konfigurierbar, die dazu erforderlichen Befehle sind in [Kapitel 6](#) beschrieben.

Für die IPSec-Verbindung gelten folgende Vorgaben:

**IPSec-Verbindung:**

<b>IKE Version</b>	IKEv2
<b>Authentifizierungsmethode</b>	Öffentlicher Schlüssel mit EAP MS-CHAPv2
<b>Lokale ID der Digitalisierungsbox</b>	vpnqabintec.dyndns.ddnss.de
<b>IPSec Gateway IP-Adresse / Hostname der Digitalisierungsbox</b>	vpnqabintec.dyndns.ddnss.de
<b>Lokales Netzwerk</b>	192.168.2.0/24
<b>IPSec-Client IP-Adress-Pool (IPSec-Clients wird dynamisch aus diesem IP-Adress-Pool eine IP-Adresse zugewiesen)</b>	192.168.10.100 - 110
<b>Benutzer 1 (Benutzername/Passwort)</b>	khmustermann / Nai4weiS

## 3 Erstellung und Export der Zertifikate

Die größte Hürde bei der Nutzung der Authentifizierungsmethode *IKEv2 Öffentlicher Schlüssel mit EAP MS-CHAPv2* stellen die Zertifikate dar. In kleineren Installationen werden selten öffentliche Zertifikate beantragt, so dass die Zertifikate selbst erstellt werden müssen. Es gibt hierzu vielfältige Möglichkeiten. In Windows-Serverumgebungen kann dies z. B. über die Windows-Server-eigenen Tools erfolgen.

In unserem Beispiel benutzen wir das für Windows und MacOS frei erhältliche Zertifikatsverwaltungsprogramm **XCA**. Dieses Programm kann entweder über den Windows Store oder von der Entwicklerseite [X - Certificate and Key management](#) heruntergeladen werden. Hier findet sich auch eine umfangreiche Dokumentation zur Verwendung des Programms.

Im Folgenden sind die wichtigsten Schritte zur Erstellung des Benutzerzertifikates erläutert. Die Erstellung des CA-Zertifikates wird hier an dieser Stelle nicht behandelt. Lesen Sie hierzu z. B. die [XCA - Step by Step guides](#). Das Programm ist sehr übersichtlich gestaltet, so dass die Nutzung nach kurzer Einarbeitung kein Problem darstellt.

### 3.1 Hinweise zum Thema Erstellung CA-signierter Benutzerzertifikate

Einleitend ein paar Hinweise zu grundsätzlichen Punkten, die bei der Erstellung von CA-signierten Benutzerzertifikaten immer zu beachten sind:

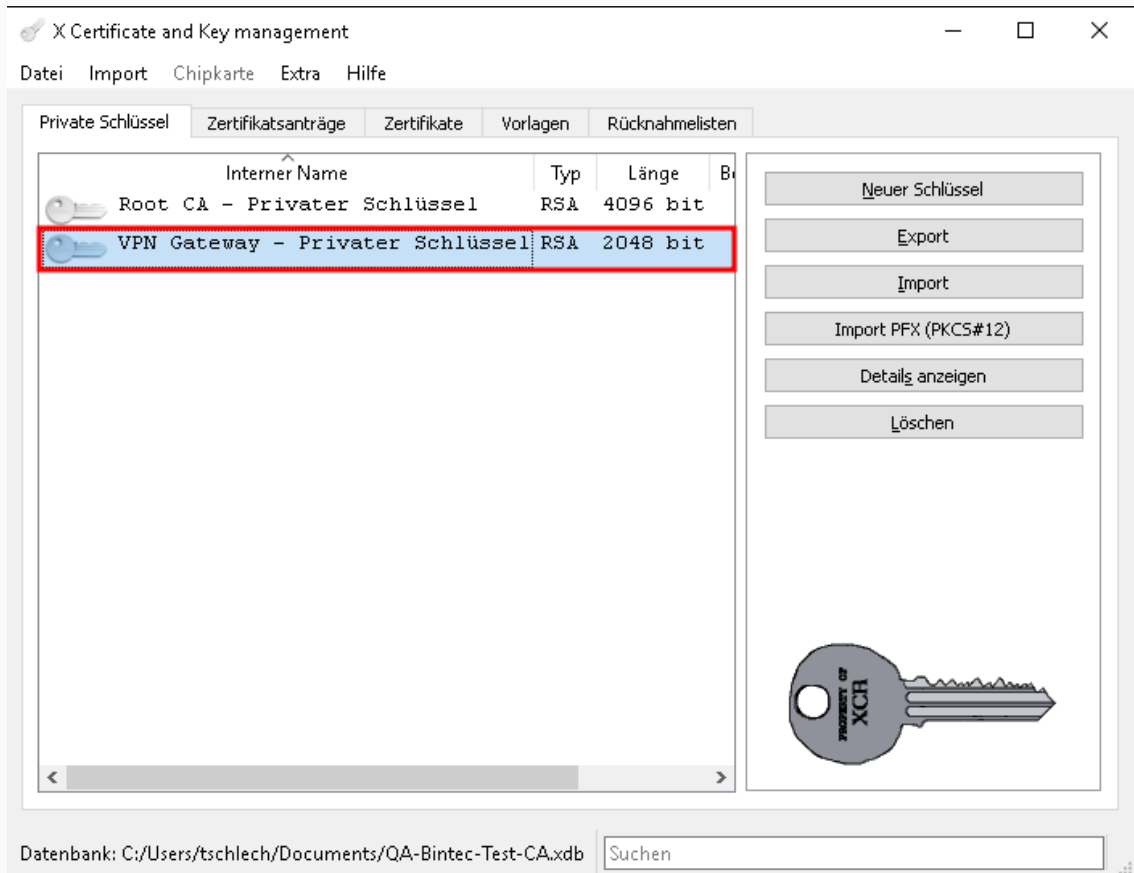
- **Schritt 1** ist immer die Erstellung des Privaten Schlüssels.
- **Schritt 2** ist die Erstellung des Benutzerzertifikates. Dies kann am einfachsten über eine Zertifikatsvorlage erfolgen. Das Programm bietet hier einige Vorlagen an. Hierbei sind folgende Punkte zu beachten:
  - a) Der zu signierende Private Schlüssel muss zugewiesen sein.
  - b) Die Angaben zur Identifikation des Zertifikatsinhabers sind zwingend anzugeben.
  - c) Optional können alternative Angaben zum Inhaber des Zertifikates (z. B. DNS Hostname, E-Mail Adresse oder IP-Adresse) hinzugefügt werden. Diese Angaben sind nicht zwingend erforderlich, werden jedoch häufig als ergänzende Identifikationsmerkmale angegeben.
  - d) Die Gültigkeitsdauer des Zertifikates muss angegeben werden. Hierbei darf die Gültigkeitsdauer des Benutzerzertifikates nie die Gültigkeitsdauer des CA-Zertifikates überschreiten. In der Regel ist die Gültigkeitsdauer des CA-Zertifikates deutlich länger als die Gültigkeitsdauer des Benutzerzertifikates. Das XCA-Programm gibt hier sinnvolle Werte vor.
  - e) Die Angaben zur Verwendung des Zertifikates (Schlüssels) müssen je nach Verwendungsfall individuell angepasst werden. Windows 10 ist hier sehr restriktiv.
- **Schritt 3** ist der Export der Zertifikate und Schlüssel, um diese anschließend auf den Geräten (Server, Notebooks, Gateways etc.) installieren zu können. Hier kommen je nach Inhalt verschiedene Exportformate zur Anwendung.

**Achtung:**

**Der private Schlüssel darf niemals unverschlüsselt über offene Kommunikationswege weitergegeben werden. Erstellung und Import des Privaten Schlüssels auf die Digitalisierungsbox sollten direkt nach Erstellung am gleichen Ort und bestenfalls vom Ersteller vorgenommen werden.**

## 3.2 Erstellung des auf der Digitalisierungsbox zu verwendenden Privaten Schlüssels

Als Erstes ist ein privater Schlüssel zu erzeugen. Als Schlüsseltyp verwenden wir RSA und wählen eine Schlüssellänge von 2048 Bit. Der Schlüsselnamen ist in unserem Beispiel *VPN Gateway – Privater Schlüssel*:



## 3.3 Erstellung des auf der Digitalisierungsbox zu verwendenden Benutzerzertifikats

Wechseln Sie hierzu in das Menü **Zertifikate** und öffnen Sie das Menü **Neues Zertifikat**. Im Menü **Herkunft** wählen Sie unter **Unterschreiben** die Option **Verwende dieses Zertifikat zum Unterschreiben** und das im Vorfeld erstellte Ausstellerzertifikat (CA-Zertifikat) aus. Als Zertifikatsvorlage wählen Sie *HTTPS\_Server* bzw. *TLS\_Server*:

X Certificate and Key management

### Erstelle x509 Zertifikat

Herkunft   Inhaber   Erweiterungen   Schlüsselverwendung   Netscape   Erweitert

Zertifikatsantrag

Diesen Zertifikatsantrag unterschreiben

Erweiterungen aus dem Zertifikatsantrag kopieren

Inhaberinformation "subject" des Zertifikatsantrags ändern

Request anzeigen

Unterschreiben

Erstelle ein Selbst signiertes Zertifikat mit der Seriennummer 1

Verwende dieses Zertifikat zum Unterschreiben

QA Bintec Test CA

Signatur algorithmus

SHA 256

Vorlage für das neue Zertifikat

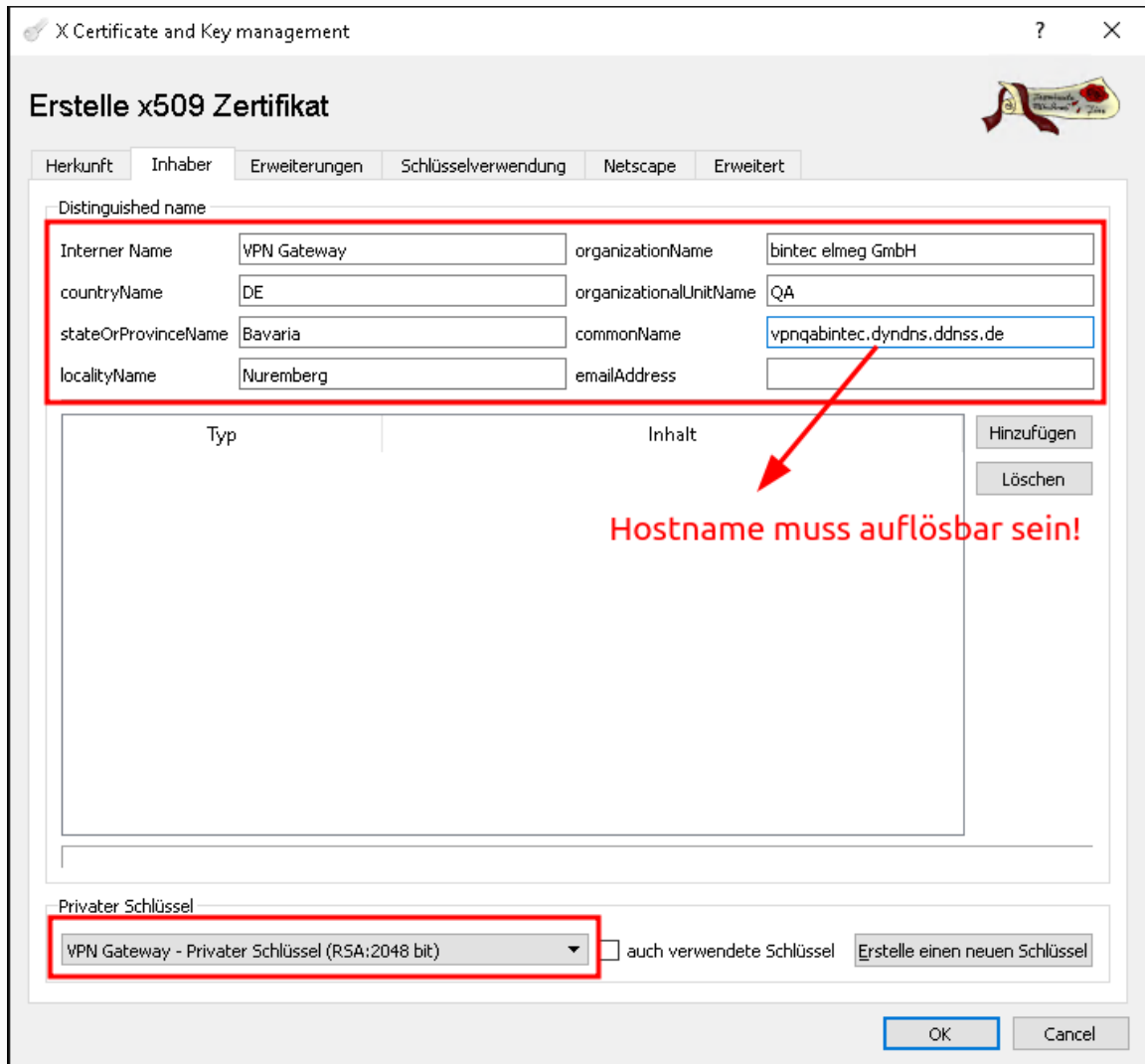
HTTPS\_server

Erweiterungen übernehmen   Subject übernehmen   Alles übernehmen

OK   Cancel

Wechseln Sie nun in das Menü **Inhaber**. Hier müssen Sie die Daten zur eindeutigen Identifikation des Zertifikatsinhabers eingeben und den zu signierenden privaten Schlüssel auswählen (siehe Menüpunkt **Privater Schlüssel**). In unserem Beispiel sieht das wie folgt aus:





X Certificate and Key management

### Erstelle x509 Zertifikat

Herkunft Inhaber Erweiterungen Schlüsselverwendung Netscape Erweitert

Distinguished name

Interner Name	VPN Gateway	organizationName	bintec elmeg GmbH
countryName	DE	organizationalUnitName	QA
stateOrProvinceName	Bavaria	commonName	vpnqabintec.dyndns.ddnss.de
localityName	Nuremberg	emailAddress	

Typ	Inhalt	Hinzufügen	Löschen
-----	--------	------------	---------

Privater Schlüssel

VPN Gateway - Privater Schlüssel (RSA:2048 bit)  auch verwendete Schlüssel

OK Cancel

**Wichtig:**

Der als **commonName** angegebene Hostname muss per DNS auflösbar sein. Ansonsten weist der Windows-10-Client das Zertifikat als ungültig zurück.

Wechseln Sie nun in das Menü **Erweiterungen**. In unserem Beispiel wurde dem Zertifikat der Hostname unserer Digitalisierungsbox als **X.509 Alternative Name** hinzugefügt. Dieser ist identisch mit dem **commonName**.

X Certificate and Key management

### Erstelle x509 Zertifikat

Herkunft Inhaber Erweiterungen Schlüsselverwendung Netscape Erweitert

X509v3 Basic Constraints

Typ

Pfadlänge   Critical

Key identifier

Subject Key Identifier

Authority Key Identifier

Gültigkeit

Nicht vor dem

Nicht nach dem

Zeitspanne

Tage

Mitternacht  Ortszeit  Undefiniertes Ablaufdatum

X509v3 Subject Alternative Name

X509v3 Issuer Alternative Name

X509v3 CRL Distribution Points

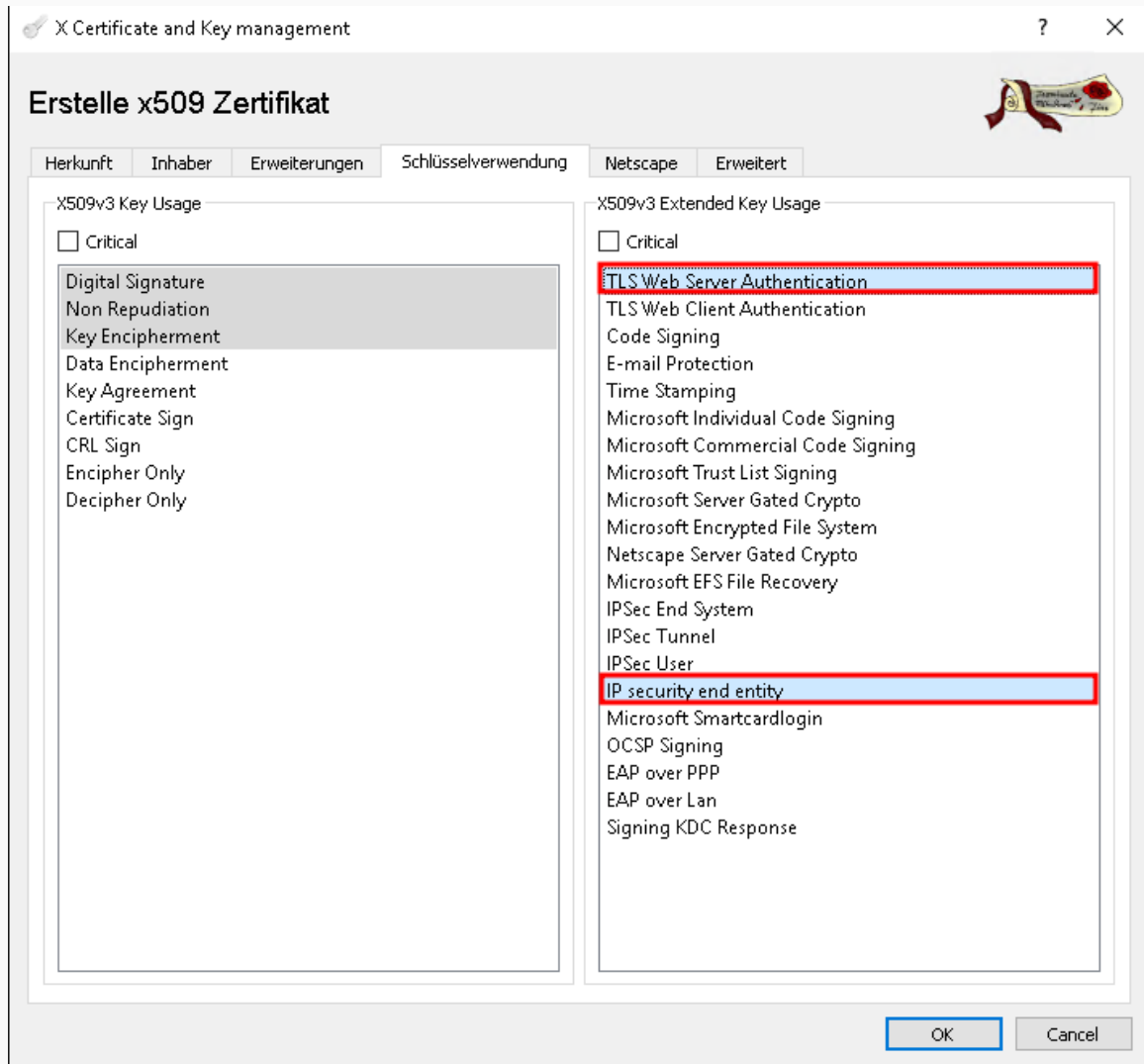
Authority Information Access

**Hinweis:**

In Menü Erweiterungen wird auch die Gültigkeitsdauer des Zertifikates festgelegt. In unserem Beispiel haben wir die vom XCA-Programm vorgeschlagene Gültigkeitsdauer von einem Jahr verwendet.

Wechseln Sie nun in das Menü **Schlüsselverwendung**. Hier sind zusätzlich zu den auf der linken Seite bereits gewählten Angaben zur **X509v3 Key Usage** die auf der rechten Seite markierten Angaben zur **X509v3 Extended Key Usage** hinzuzufügen. Diese sind in unserem Fall:

- *TLS Web Server Authentication*
- *IP security end entity*



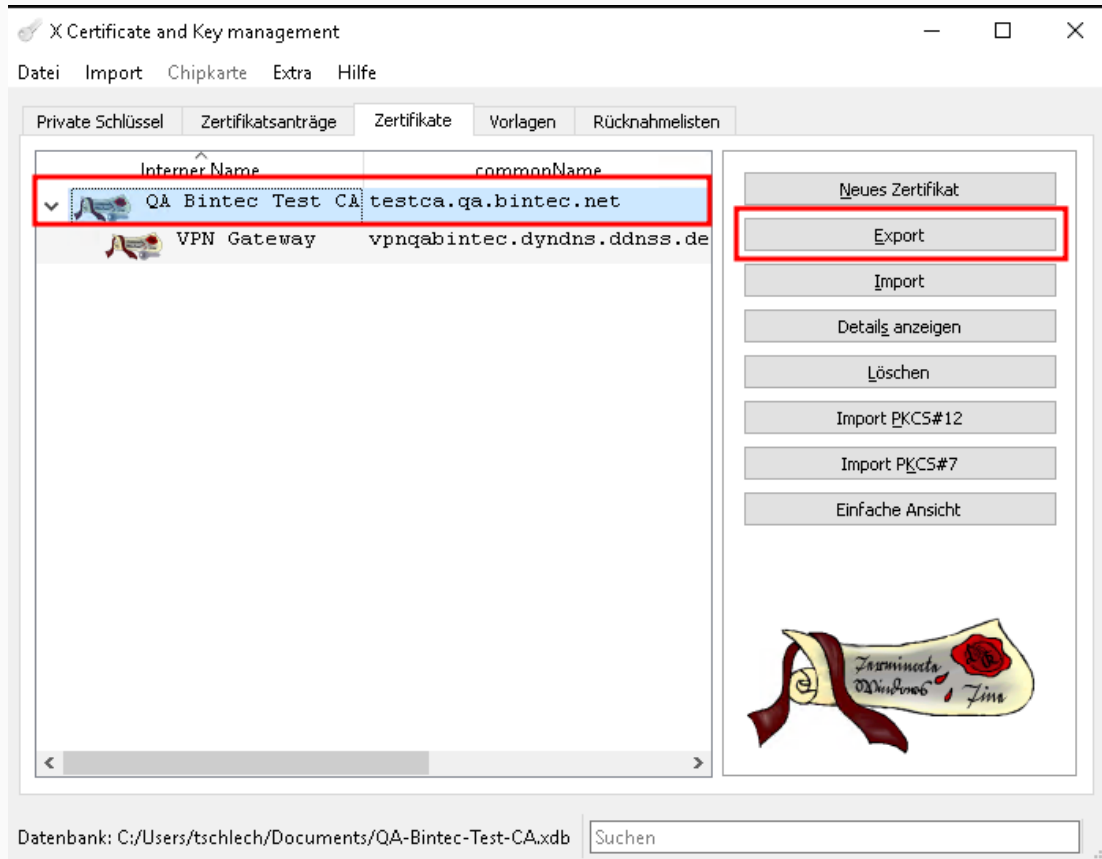
**Wichtig:**

Die beiden Extended Key Usage Angaben sind zwingend erforderlich. Anderenfalls weist der Windows-10-Client das Zertifikat als ungültig zurück.

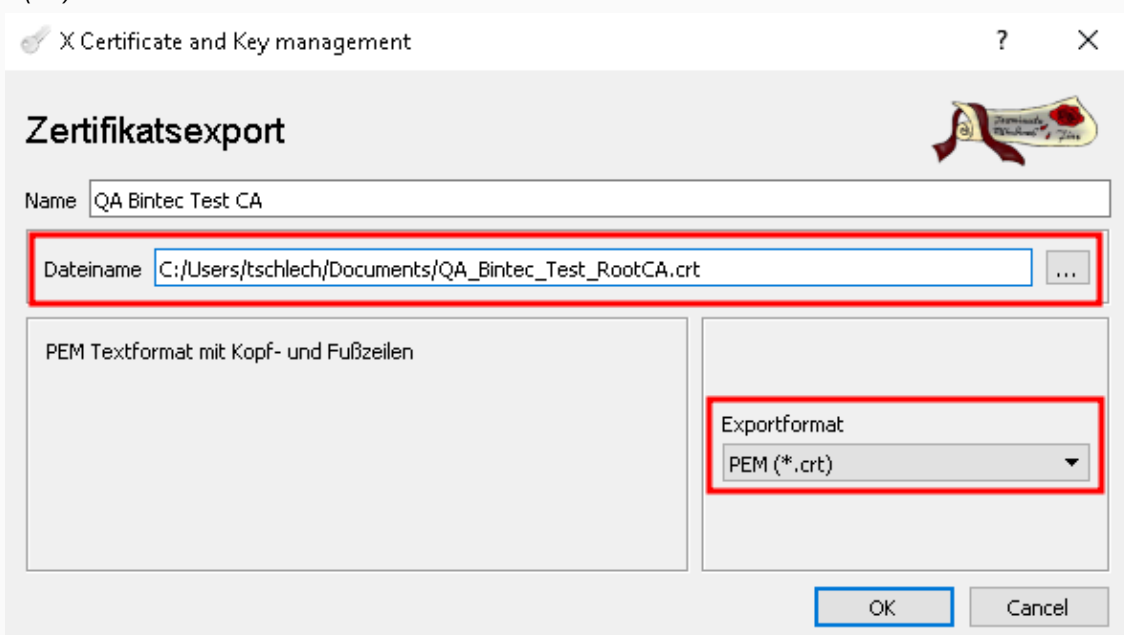
Abschließend bestätigen Sie alle Eingaben mit **OK**. Hiermit ist das CA-signierte Benutzerzertifikat erstellt.

### 3.4 Export des Ausstellerzertifikates (CA-Zertifikates)

Wechseln Sie hierzu in das Menü **Zertifikate**, markieren Sie das Ausstellerzertifikat (CA-Zertifikat) (in unserem Fall **QA Bintec Test CA**) und klicken Sie auf **Export**:

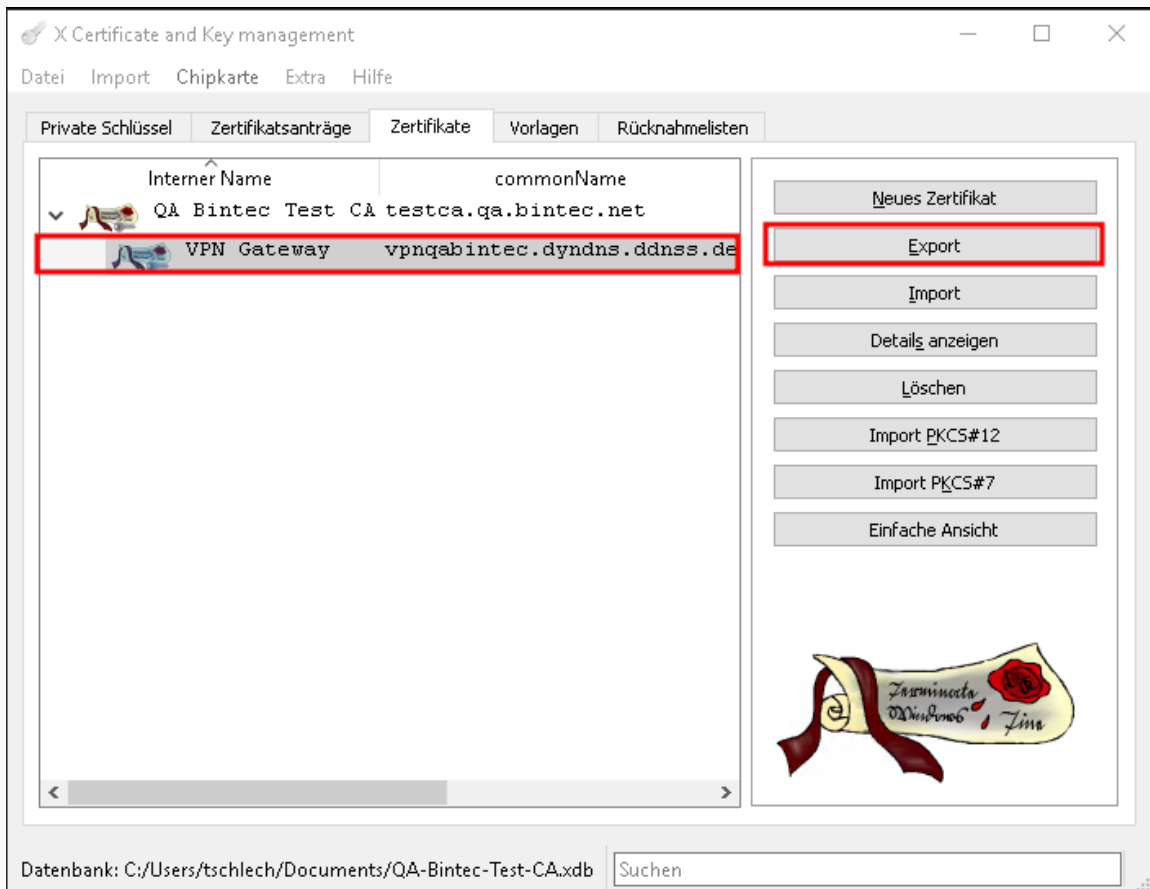


Legen Sie ein Verzeichnis fest, in dem die CA-Zertifikatsdatei gespeichert werden soll und wählen Sie als **Exportformat** **PEM (\*.crt)**:



### 3.5 Export des Benutzerzertifikates sowie des Privaten Schlüssels

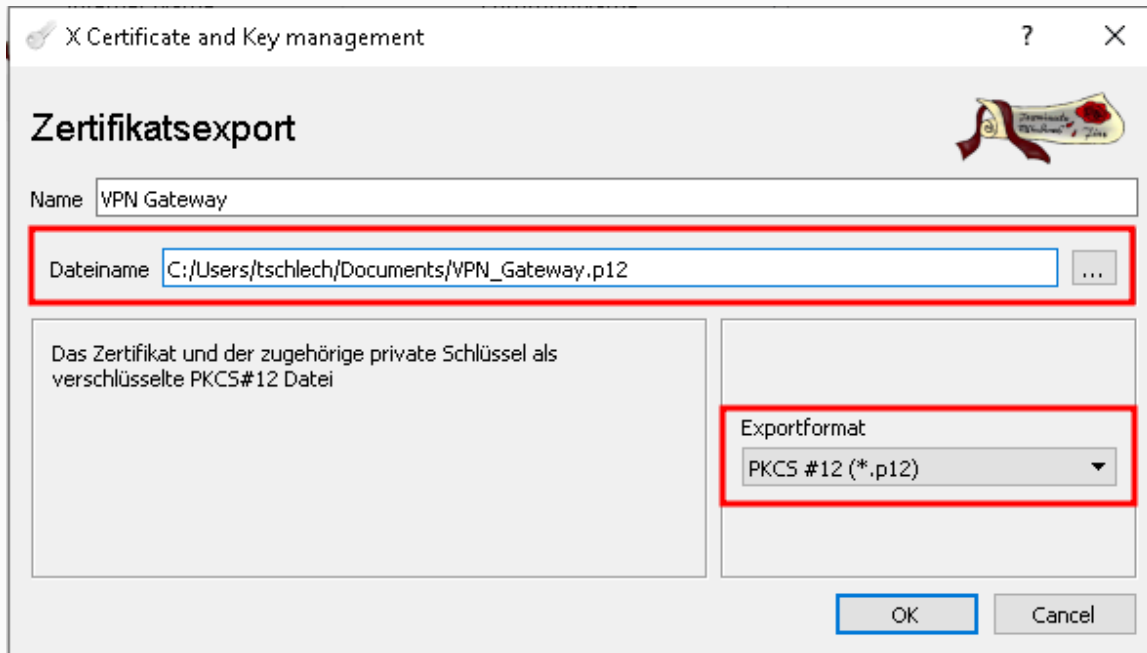
Wechseln Sie hierzu in das Menü **Zertifikate**, markieren Sie das Benutzerzertifikat (in unserem Fall VPN Gateway) und klicken Sie auf **Export**:



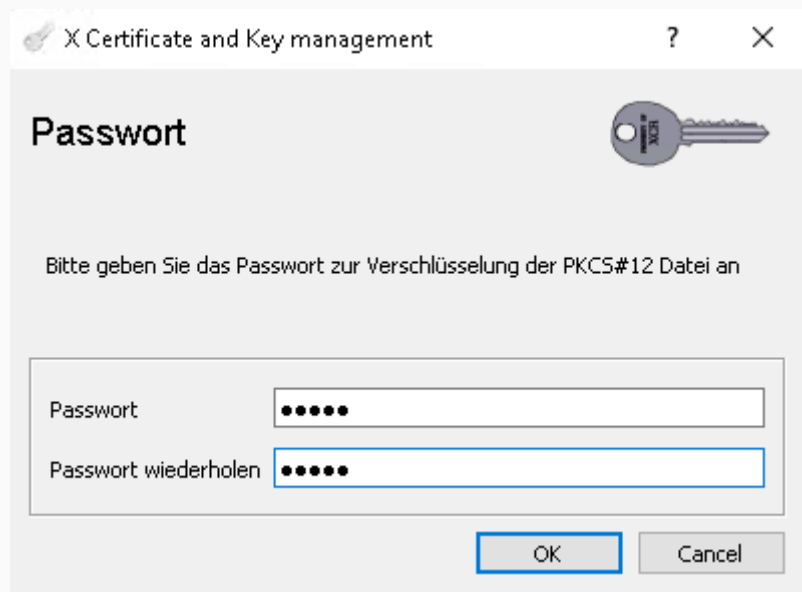
Legen Sie das Verzeichnis fest, in dem die Benutzerzertifikatsdatei gespeichert werden soll und wählen Sie als **Exportformat PKCS#12 (\*.p12)**.

**Hinweis:**

Das Exportformat **PKCS#12** erlaubt den Export des Benutzerzertifikats sowie des dazugehörigen Privaten Schlüssels in einer Datei. Wählen Sie deshalb unbedingt dieses Dateiformat. Bestätigen Sie die Eingaben mit **OK**.



Sie werden abschließend nach einem **Passwort** gefragt. Dieses Passwort wird genutzt, um den Inhalt der PKCS#12-Datei zu verschlüsseln. Dies ist von zentraler Bedeutung, da der enthaltene Private Schlüssel niemals offengelegt werden darf.



Hiermit ist der Export der Zertifikate abgeschlossen.

## 4 Konfiguration der Digitalisierungsbox

Bei der Konfiguration ist folgende Reihenfolge zu beachten:

- (1) DynDNS konfigurieren
- (2) Aktivierung von IPSec sofern nicht bereits aktiv
- (3) Import der Zertifikate und Schlüssel
- (4) Konfiguration der IKE (Phase 1) und IPSec (Phase 2) Proposals
- (5) Konfiguration der IPSec-Verbindung.

### 4.1 DynDNS-Konfiguration

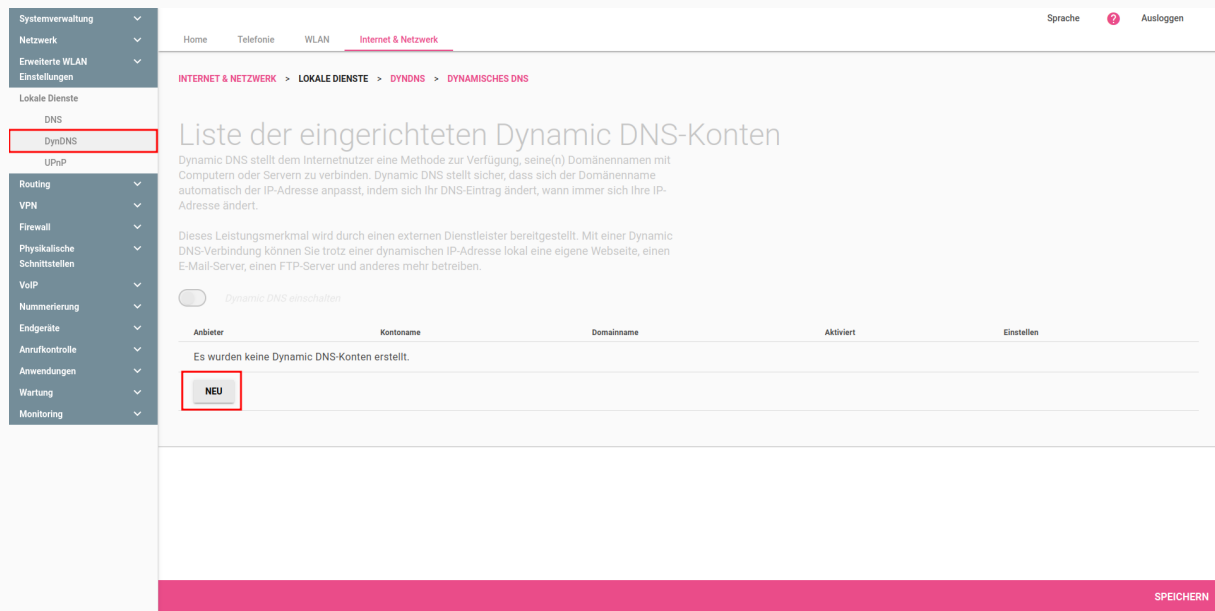
In unserem Anwendungsfall wird DynDNS genutzt, um den Hostnamen der Digitalisierungsbox bei Änderung der IP-Adresse automatisch zu aktualisieren. Zur Konfiguration wechseln Sie hierzu in das Menü **Internet & Netzwerk** und öffnen im Bereich **Mehr anzeigen** das Menü **Lokale Dienste** → **DynDNS**.

Wir verwenden hier den DynDNS-Provider **ddnss.de** (<https://ddnss.de/login.php>). Da dessen DynDNS-Anbieterprofil aktuell nicht von der Digitalisierungsbox 2 angeboten wird, muss es über die Konfiguration der **Update URL** zunächst erstellt werden. Für **ddnss.de** sieht die URL zum Update der IPv4/IPv6-Adresse wie folgt aus:

**<https://ddnss.de/upd.php?user=xxxxxx&pwd=xxxxxx&host=vpnqabintec.dyndns.ddnss.de&ip=<ipaddr>&ip6=<ipaddr6>>**

Die user-, pwd- und host-Angaben (rot gekennzeichnet) sind individuell und müssen an die eigenen Gegebenheiten angepasst werden.

Die folgenden Abbildungen zeigen die notwendigen Konfigurationsschritte:



Geben Sie die URL ein und wählen Sie den von Ihnen genutzten Internetzugang:

Home Telefonie WLAN **Internet & Netzwerk** Sprache ? Ausloggen

Folgende Platzhalter sind in der URL möglich: <domain>, <username>, <password>, <ipaddr>, <ipaddr6>. Für die Aktualisierung werden diese Platzhalter mit Ihren Werten für "Domainname", "Kontoname" und "Passwort" ersetzt. Die IP-Adresse wird hierbei automatisch ermittelt und ersetzt. Die URL setzt sich dann beispielsweise so zusammen:

- `https://url/?hostname=<domain>&username=<username>&password=<password>&myip=<ipaddr>&myip6=<ipaddr6>`
- `http://url/update?hostname=<domain>&username=<username>&myvalue=value`
- `http://<username>.url/?hostname=<domain>&myip=<ipaddr>`

Die "Erwartete Antwort des Servers" kann einen Text enthalten, welchen der Server zurückliefert wenn das Update erfolgreich war. Es muss hierbei nicht die komplette Antwort des Servers angegeben werden. Die Antwort des Servers wird nach dem angegebenen Text durchsucht. Sollte der Server bei Erfolg beispielsweise "Das Update war erfolgreich" liefern, so reicht es wenn "erfolgreich" eingetragen wird.

Hinweis: Systembedingt können in Ihrem Gerät nicht alle Sonderzeichen im Dynamic DNS-Passwort verwendet werden. Bitte beachten Sie, bei der Vergabe von Passwörtern über Ihren Dienstleister, folgende Sonderzeichen nicht zu verwenden: \* | { } ; ' ~ ^

Anbieter: Update URL

Server-Adresse: `https://ddnss.de/upd.php?l`

Erwartete Antwort des Servers:

Domainname:

Kontoname:

Passwort:

Passwortbestätigung:

Dynamic DNS-Interface: PPPoE → VLAN 7 → WAnGE

Aktivieren:

SPEICHERN ABBRECHEN

Schließen Sie die Konfiguration mit **SPEICHERN** ab. Anschließend sieht die DynDNS Konfiguration wie folgt aus:

Home Telefonie WLAN **Internet & Netzwerk** Sprache ? Ausloggen



INTERNET & NETZWERK > LOKALE DIENSTE > DYNDNS > DYNAMISCHES DNS

### Liste der eingerichteten Dynamic DNS-Konten

Dynamic DNS stellt dem Internetnutzer eine Methode zur Verfügung, seine(n) Domännennamen mit Computern oder Servern zu verbinden. Dynamic DNS stellt sicher, dass sich der Domännename automatisch der IP-Adresse anpasst, indem sich Ihr DNS-Eintrag ändert, wann immer sich Ihre IP-Adresse ändert.

Dieses Leistungsmerkmal wird durch einen externen Dienstleister bereitgestellt. Mit einer Dynamic DNS-Verbindung können Sie trotz einer dynamischen IP-Adresse lokal eine eigene Webseite, einen E-Mail-Server, einen FTP-Server und anderes mehr betreiben.

Dynamic DNS einschalten

Anbieter	Kontoname	Domainname	Aktiviert	Einstellen
Update URL	-	-	✓	 

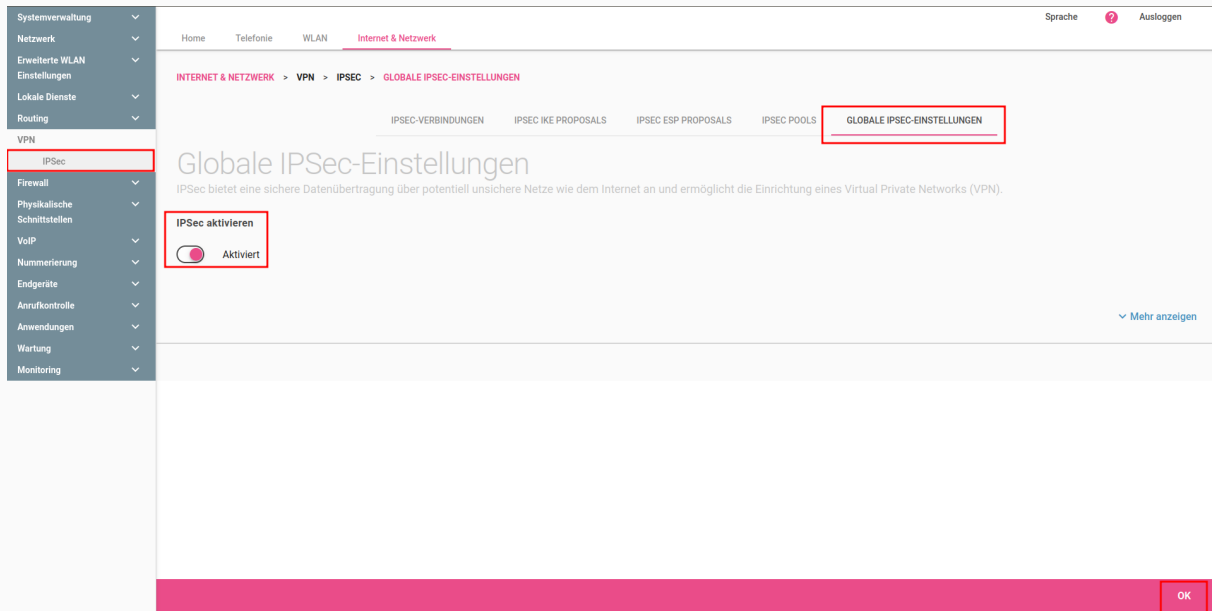
NEU

SPEICHERN



## 4.2 Aktivierung von IPSec

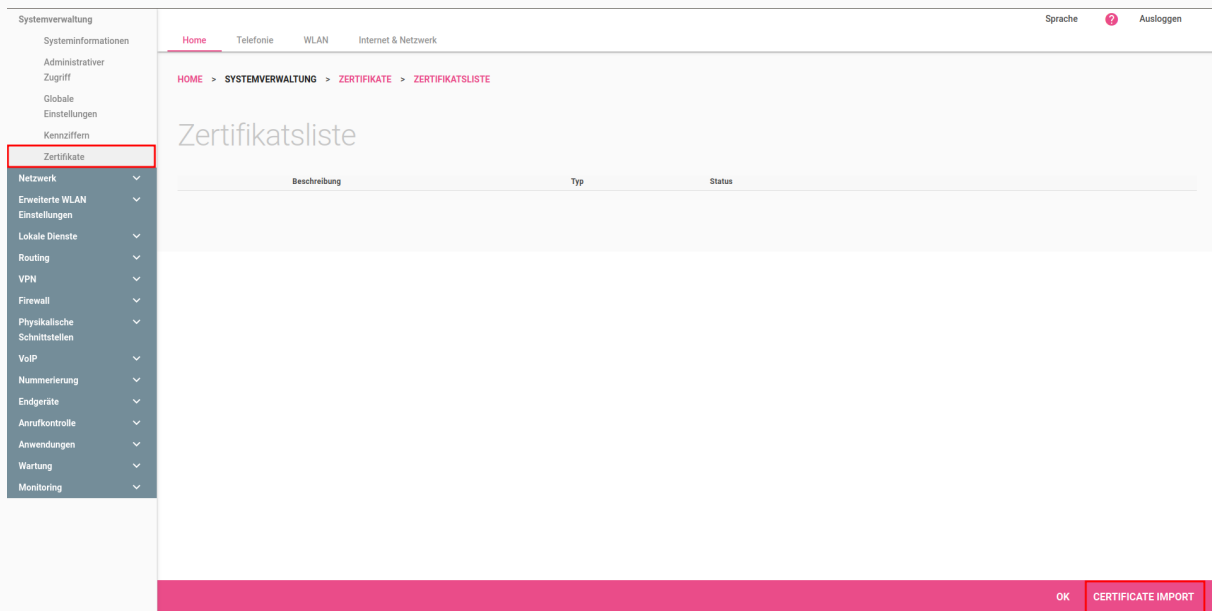
Wechseln Sie hierzu in das Menü **Internet & Netzwerk**, öffnen Sie im Bereich **Mehr anzeigen** das Menü **IPSec** und aktivieren Sie IPSec über die Option **IPSec aktivieren** im Menü **Globale IPSec-Einstellungen**:



The screenshot shows the 'Globale IPSec-Einstellungen' page. The breadcrumb path is 'INTERNET & NETZWERK > VPN > IPSEC > GLOBALE IPSEC-EINSTELLUNGEN'. The 'IPSec aktivieren' toggle is turned on, indicated by a red circle and the text 'Aktiviert'. The page title is 'Globale IPSec-Einstellungen' and the subtitle is 'IPSec bietet eine sichere Datenübertragung über potentiell unsichere Netze wie dem Internet an und ermöglicht die Einrichtung eines Virtual Private Networks (VPN)'. There is an 'OK' button at the bottom right.

## 4.3 Import der Zertifikate

Wechseln Sie hierzu in das Menü **Home** und öffnen Sie im Bereich **Mehr anzeigen** das Menü **Zertifikate**:



The screenshot shows the 'Zertifikatsliste' page. The breadcrumb path is 'HOME > SYSTEMVERWALTUNG > ZERTIFIKATE > ZERTIFIKATSLISTE'. The 'Zertifikate' menu item is highlighted in the left sidebar. The page title is 'Zertifikatsliste'. There is a table with columns 'Beschreibung', 'Typ', and 'Status'. There are 'OK' and 'CERTIFICATE IMPORT' buttons at the bottom right.

### Hinweis:

Achten Sie darauf, beim Import beider Zertifikate die Option **Für IPSec verwenden** zu aktivieren.

Als Erstes importieren wir das Ausstellerzertifikat (CA-Zertifikat) über **CERTIFICATE IMPORT**. Als Zertifikatstyp muss zum Import unseres CA-Zertifikats der **Zertifikatstyp Zertifikat X.509-kodiert (unverschlüsselt, PEM-formatiert)** gewählt werden. Der Dateiname ist in unserem Beispiel **QA\_Bintec\_Test\_RootCA.crt**. Bestätigen Sie die Eingaben mit **OK**:

Home Telefonie WLAN Internet & Netzwerk Sprache ? Ausloggen

HOME > SYSTEMVERWALTUNG > ZERTIFIKATE > ZERTIFIKATSLISTE

### Zertifikatsimport

**Beschreibung**  
Root-CA

**Zertifikatstyp**  
Zertifikat X.509-kodiert (unverschlüsselt, PEM-formatiert) ▼  
Zertifikat kann ein Benutzer- oder CA-Zertifikat sein

**Für IPSec verwenden**  
 Aktiviert

**Datenname**  
[Browse...] QA\_Bintec\_Test\_RootCA.crt

**Kennwort für geschütztes Zertifikat**





OK ABBRECHEN

Die Zertifikatsübersicht sieht nun wie folgt aus:

Home Telefonie WLAN Internet & Netzwerk Sprache ? Ausloggen

HOME > SYSTEMVERWALTUNG > ZERTIFIKATE > ZERTIFIKATSLISTE

### Zertifikatsliste

Beschreibung	Typ	Status	
1:	Root-CA	CA-Zertifikat X.509 File	Verfügbar   
1.1	CA-Zertifikat X.509	C = DE, ST = Bavaria, L = Nuremberg, O = bintec elmeg GmbH, OU = QA, CN = testca.qa.bintec.net C = DE, ST = Bavaria, L = Nuremberg, O = bintec elmeg GmbH, OU = QA, CN = testca.qa.bintec.net	

OK CERTIFICATE IMPORT

Im zweiten Schritt importieren wir das Benutzerzertifikat. Als **Zertifikatstyp** ist hier Zertifikat und Schlüssel PKCS#12-  
verpackt zu wählen. Zusätzlich ist hier zum Import das Kennwort anzugeben, das beim Export zur Verschlüsselung der  
PKCS#12-Datei genutzt wurde:

Home Telefonie WLAN Internet & Netzwerk Sprache ? Ausloggen

HOME > SYSTEMVERWALTUNG > ZERTIFIKATE > ZERTIFIKATSLISTE

### Zertifikatsimport

<b>Beschreibung</b> VPN-Gateway	<b>Zertifikatstyp</b> Zertifikat und Schlüssel PKCS#12-verpackt	<b>Für IPSec verwenden</b> <input checked="" type="checkbox"/> Aktiviert
<b>Kennwort für geschütztes Zertifikat</b> *****	<b>Datenname</b> Browse... VPN_Gateway.p12	










OK ABBRECHEN

Die Zertifikatsübersicht sieht nun wie folgt aus:

Home Telefonie WLAN Internet & Netzwerk Sprache ? Ausloggen

HOME > SYSTEMVERWALTUNG > ZERTIFIKATE > ZERTIFIKATSLISTE

### Zertifikatsliste

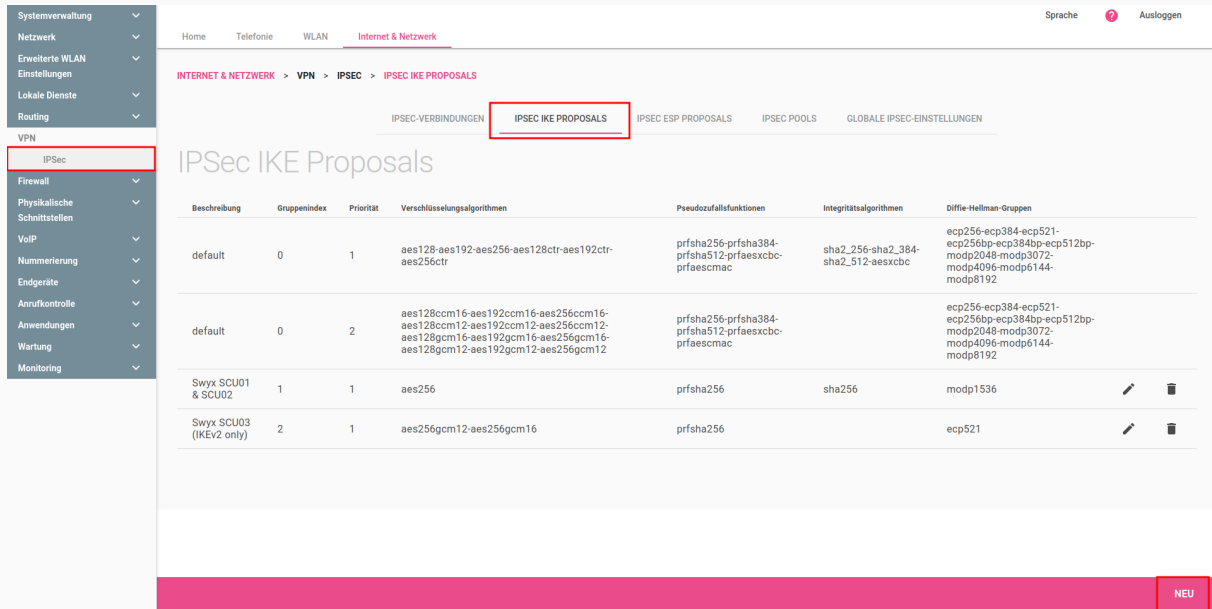
Beschreibung	Typ	Status	
1: Root-CA	CA-Zertifikat X.509 File	Verfügbar	  
1.1	CA-Zertifikat X.509	C = DE, ST = Bavaria, L = Nuremberg, O = bintec elmeg GmbH, OU = QA, CN = testca.qa.bintec.net C = DE, ST = Bavaria, L = Nuremberg, O = bintec elmeg GmbH, OU = QA, CN = testca.qa.bintec.net	
2: VPN-Gateway	Zertifikat, Schlüssel PKCS#12 File	Nicht unterstützte Verschlüsselung	  
2.2	Zertifikat X.509		
2.3	CA-Zertifikat X.509		

OK CERTIFICATE IMPORT

## 4.4 Konfiguration der IKE (Phase 1) und IPsec (Phase 2) Proposals

### 4.4.1 IKE (Phase 1) Proposal

Wechseln Sie in das Menü **Internet & Netzwerk** und öffnen Sie im Bereich **Mehr anzeigen** das Menü **IPsec** und wechseln Sie in das Menü **IPsec IKE Proposals**:

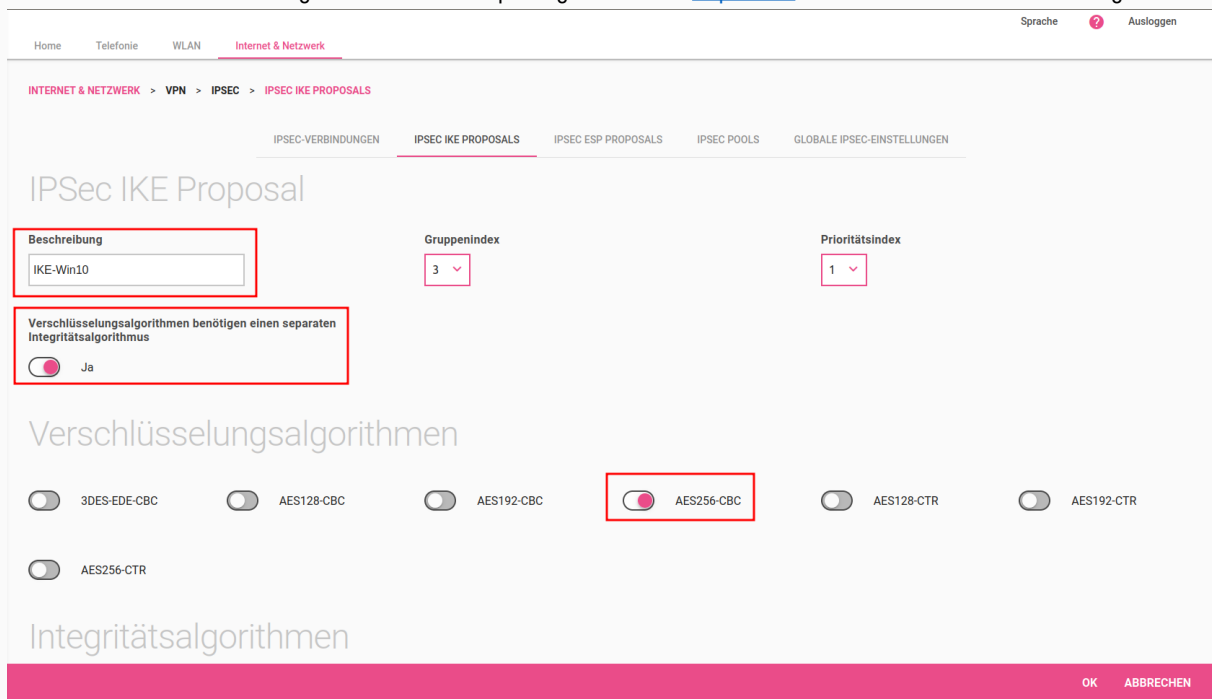


The screenshot shows the 'IPsec IKE Proposals' configuration page. On the left is a navigation menu with 'IPsec' highlighted. The main content area shows a table of existing proposals:

Beschreibung	Gruppenindex	Priorität	Verschlüsselungsalgorithmen	Pseudozufallsfunktionen	Integritätsalgorithmen	Diffie-Hellman-Gruppen
default	0	1	aes128-aes192-aes256-aes128ctr-aes192ctr-aes256ctr	prfsha256-prfsha384-prfsha512-prfaesxcbc-prfaescmac	sha2_256-sha2_384-sha2_512-aesxcbc	ecp256-ecp384-ecp521-ecp256bp-ecp384bp-ecp512bp-modp2048-modp3072-modp4096-modp6144-modp8192
default	0	2	aes128ccm16-aes192ccm16-aes256ccm16-aes128ccm12-aes192ccm12-aes256ccm12-aes128gcm16-aes192gcm16-aes256gcm16-aes128gcm12-aes192gcm12-aes256gcm12	prfsha256-prfsha384-prfsha512-prfaesxcbc-prfaescmac		ecp256-ecp384-ecp521-ecp256bp-ecp384bp-ecp512bp-modp2048-modp3072-modp4096-modp6144-modp8192
Swyx SCU01 & SCU02	1	1	aes256	prfsha256	sha256	modp1536
Swyx SCU03 (IKEv2 only)	2	1	aes256gcm12-aes192gcm16	prfsha256		ecp521

A red box highlights the 'IPsec IKE PROPOSALS' tab in the top navigation. At the bottom right, there is a red button labeled 'NEU'.

Klicken Sie auf **NEU** und konfigurieren Sie das Proposal gemäß der in [Kapitel 2.1](#) beschriebenen IPsec-Einstellungen:



The screenshot shows the configuration form for a new IPsec IKE Proposal. The 'Beschreibung' field is set to 'IKE-Win10'. The 'Gruppenindex' is set to 3 and the 'Prioritätsindex' is set to 1. A checkbox labeled 'Verschlüsselungsalgorithmen benötigen einen separaten Integritätsalgorithmus' is checked. Under 'Verschlüsselungsalgorithmen', the 'AES256-CBC' option is selected. The 'Integritätsalgorithmen' section is currently empty. At the bottom right, there are 'OK' and 'ABBRECHEN' buttons.

Scrollen Sie die Seite zur weiteren Konfiguration nach unten und bestätigen Sie die Eingaben mit **OK**.

Home Telefonie WLAN **Internet & Netzwerk** Sprache ? Ausloggen

### Integritätsalgorithmen

MD5-HMAC   
  MD5\_128-HMAC   
  SHA1-HMAC   
  SHA1\_160-HMAC   
  AES-XCBC   
  AES-CMAC  
 AES\_128-GMAC   
  AES\_192-GMAC   
  AES\_256-GMAC   
  SHA2\_256\_128 HMAC   
  SHA2\_384\_192 HMAC   
  SHA2\_512\_256 HMAC

### Pseudozufallsfunktionen (PRF)

MD5-PRF   
  SHA1-PRF   
  AES-XCBC-PRF   
  AES-CMAC-PRF   
  SHA2\_256-PRF   
  SHA2\_384-PRF  
 SHA2\_512-PRF

### Diffie-Hellman-Gruppen

MODP1024 (2)   
  MODP1536 (5)   
  MODP2048 (14)   
  MODP3072 (15)   
  MODP4096 (16)   
  MODP6144 (17)  
 MODP8192 (18)   
  ECP192 (25)   
  ECP224 (26)   
  ECP256 (19)   
  ECP384 (20)   
  ECP521 (21)

**OK**    **ABBRECHEN**

Die IPsec IKE Proposals Übersicht sieht nun wie folgt aus:

Home Telefonie WLAN **Internet & Netzwerk** Sprache ? Ausloggen

INTERNET & NETZWERK > VPN > IPSEC > IPSEC IKE PROPOSALS

IPSEC-VERBINDUNGEN    **IPSEC IKE PROPOSALS**    IPSEC ESP PROPOSALS    IPSEC POOLS    GLOBALE IPSEC-EINSTELLUNGEN

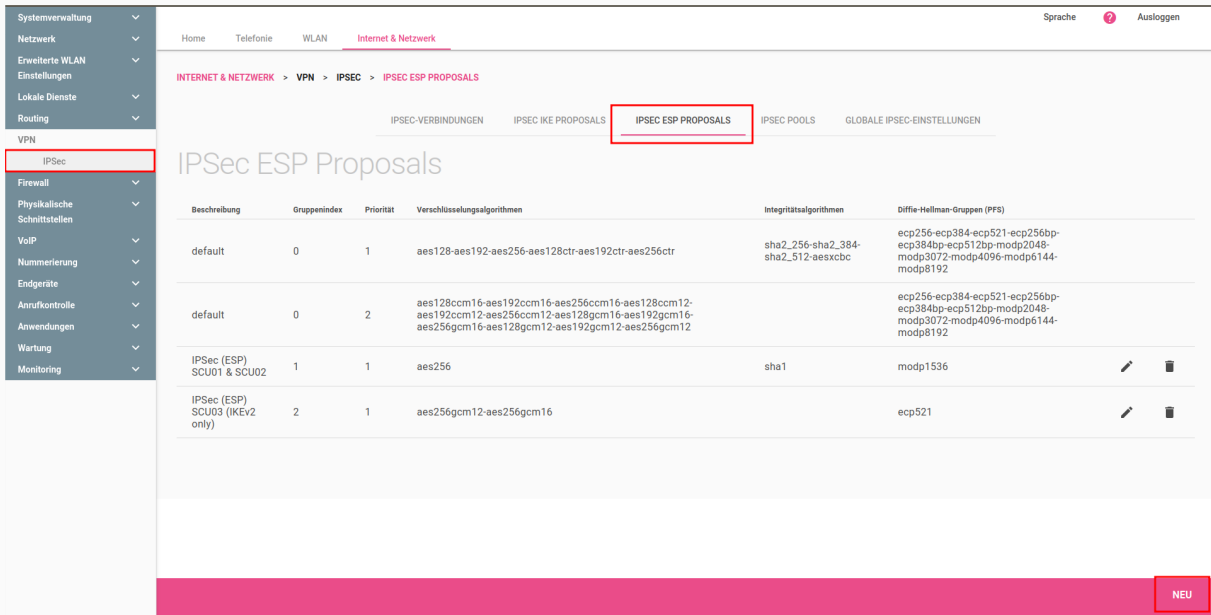
### IPsec IKE Proposals

Beschreibung	Gruppenindex	Priorität	Verschlüsselungsalgorithmen	Pseudozufallsfunktionen	Integritätsalgorithmen	Diffie-Hellman-Gruppen		
default	0	1	aes128-aes192-aes256-aes128ctr-aes192ctr-aes256ctr	prfsha256-prfsha384-prfsha512-prfaesxcbc-prfaescmac	sha2_256-sha2_384-sha2_512-aesxcbc	ecp256-ecp384-ecp521-ecp256bp-ecp384bp-ecp512bp-modp2048-modp3072-modp4096-modp6144-modp8192		
default	0	2	aes128ccm16-aes192ccm16-aes256ccm16-aes128ccm12-aes192ccm12-aes256ccm12-aes128gcm16-aes192gcm16-aes256gcm16-aes128gcm12-aes192gcm12-aes256gcm12	prfsha256-prfsha384-prfsha512-prfaesxcbc-prfaescmac		ecp256-ecp384-ecp521-ecp256bp-ecp384bp-ecp512bp-modp2048-modp3072-modp4096-modp6144-modp8192		
Swyx SCU01 & SCU02	1	1	aes256	prfsha256	sha256	modp1536		
Swyx SCU03 (IKEv2 only)	2	1	aes256gcm12-aes256gcm16	prfsha256		ecp521		
<b>IKE-Win10</b>	<b>3</b>	<b>1</b>	<b>aes256</b>	<b>prfsha256</b>	<b>sha256</b>	<b>modp1024</b>		





**NEU**

## 4.4.2 IPsec (Phase 2) Proposal

Wechseln Sie hierzu in das Menü **IPsec ESP Proposals**:

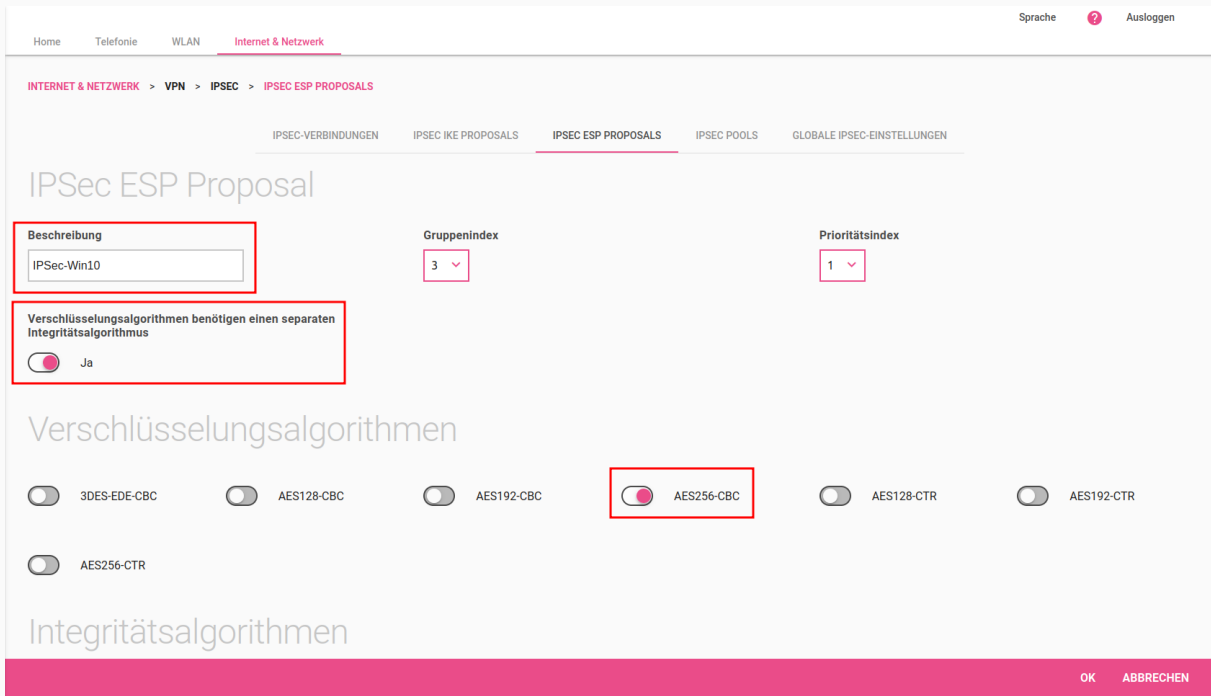


The screenshot shows the 'IPsec ESP Proposals' configuration page. The left sidebar contains a navigation menu with 'VPN' and 'IPsec' highlighted. The main content area displays a table of proposals:

Beschreibung	Gruppenindex	Priorität	Verschlüsselungsalgorithmen	Integritätsalgorithmen	Diffie-Hellman-Gruppen (PFS)	
default	0	1	aes128-aes192-aes256-aes128ctr-aes192ctr-aes256ctr	sha2_256-sha2_384-sha2_512-aesxcbc	ecp256-ecp384-ecp521-ecp256bp-ecp384bp-ecp512bp-modp2048-modp3072-modp4096-modp6144-modp8192	
default	0	2	aes128ccm16-aes192ccm16-aes256ccm16-aes128ccm12-aes192ccm12-aes256ccm12-aes128gcm16-aes192gcm16-aes256gcm16-aes128gcm12-aes192gcm12-aes256gcm12		ecp256-ecp384-ecp521-ecp256bp-ecp384bp-ecp512bp-modp2048-modp3072-modp4096-modp6144-modp8192	
IPsec (ESP) SCU01 & SCU02	1	1	aes256	sha1	modp1536	 
IPsec (ESP) SCU03 (IKEv2 only)	2	1	aes256gcm12-aes256gcm16		ecp521	 

A red box highlights the 'IPsec' menu item in the sidebar. Another red box highlights the 'IPSEC ESP PROPOSALS' tab in the top navigation. A red box at the bottom right contains the 'NEU' button.

Klicken Sie auf **NEU** und konfigurieren Sie das Proposal gemäß der in [Kapitel 2.1](#) beschriebenen IPsec-Einstellungen:



The screenshot shows the configuration form for a new IPsec ESP Proposal. The 'Beschreibung' field contains 'IPsec-Win10'. The 'Gruppenindex' is set to 3 and the 'Prioritätsindex' is set to 1. The checkbox 'Verschlüsselungsalgorithmen benötigen einen separaten Integritätsalgorithmus' is checked. Under 'Verschlüsselungsalgorithmen', the 'AES256-CBC' option is selected. The 'OK' and 'ABBRECHEN' buttons are visible at the bottom right.

Scrollen Sie die Seite zur weiteren Konfiguration nach unten und bestätigen Sie die Eingaben mit **OK**:

### Integritätsalgorithmen

- MD5-HMAC
- MD5\_128-HMAC
- SHA1-HMAC
- SHA1\_160-HMAC
- AES-XCBC
- AES-CMAC
- AES\_128-GMAC
- AES\_192-GMAC
- AES\_256-GMAC
- SHA2\_256\_128 HMAC
- SHA2\_384\_192 HMAC
- SHA2\_512\_256 HMAC

### Diffie-Hellman-Gruppen (PFS)

- MODP1024 (2)
- MODP1536 (5)
- MODP2048 (14)
- MODP3072 (15)
- MODP4096 (16)
- MODP6144 (17)
- MODP8192 (18)
- ECP192 (25)
- ECP224 (26)
- ECP256 (19)
- ECP384 (20)
- ECP521 (21)
- ECP224BP (27)
- ECP256BP (28)
- ECP384BP (29)
- ECP512BP (30)
- CURVE25519 (31)
- CURVE448 (32)

OK ABBRECHEN

Die **IPSec ESP Proposals** Übersicht sieht nun wie folgt aus.

Home Telefonie WLAN **Internet & Netzwerk**
Sprache ? Ausloggen

---

INTERNET & NETZWERK > VPN > IPSEC > IPSEC ESP PROPOSALS

IPSEC-VERBINDUNGEN
IPSEC IKE PROPOSALS
IPSEC ESP PROPOSALS
IPSEC POOLS
GLOBALE IPSEC-EINSTELLUNGEN

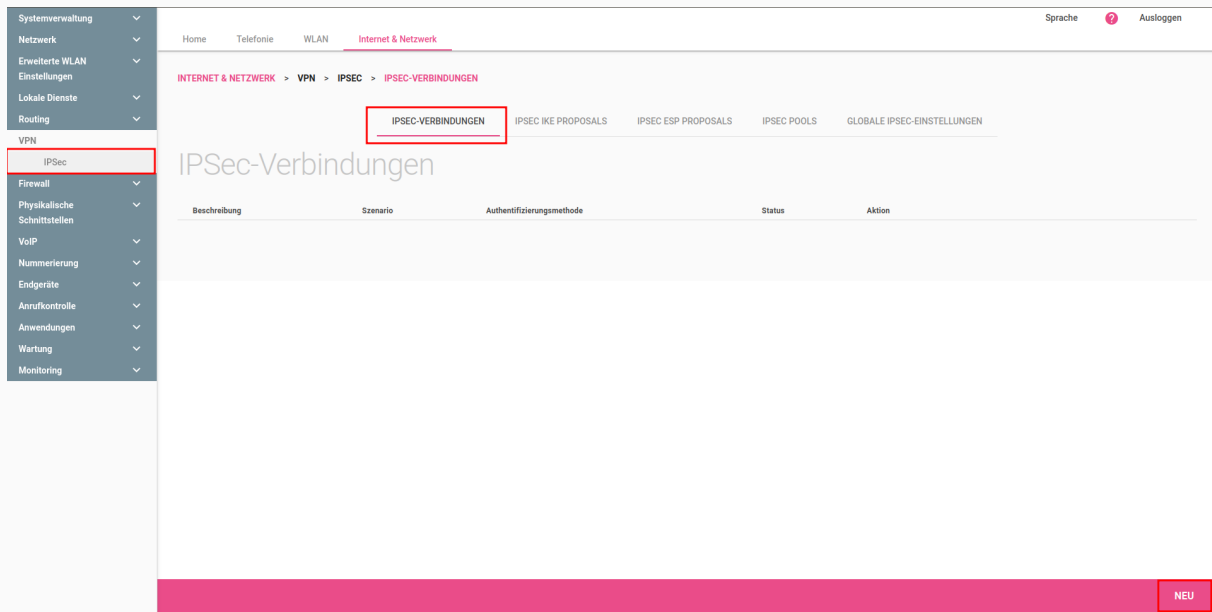
## IPSec ESP Proposals

Beschreibung	Gruppenindex	Priorität	Verschlüsselungsalgorithmen	Integritätsalgorithmen	Diffie-Hellman-Gruppen (PFS)	
default	0	1	aes128-aes192-aes256-aes128ctr-aes192ctr-aes256ctr	sha2_256-sha2_384-sha2_512-aesxcbc	ecp256-ecp384-ecp521-ecp256bp-ecp384bp-ecp512bp-modp2048-modp3072-modp4096-modp6144-modp8192	
default	0	2	aes128ccm16-aes192ccm16-aes256ccm16-aes128ccm12-aes192ccm12-aes256ccm12-aes128gcm16-aes192gcm16-aes256gcm16-aes128gcm12-aes192gcm12-aes256gcm12		ecp256-ecp384-ecp521-ecp256bp-ecp384bp-ecp512bp-modp2048-modp3072-modp4096-modp6144-modp8192	
IPSec (ESP) SCU01 & SCU02	1	1	aes256	sha1	modp1536	
IPSec (ESP) SCU03 (IKEV2 only)	2	1	aes256gcm12-aes256gcm16		ecp521	
IPSec-Win10	3	1	aes256	sha1	modp1024	

NEU

## 4.5 Konfiguration der IPSec-Verbindung auf der Digitalisierungsbox 2

Wechseln Sie in das Menü **IPSec-Verbindungen** und klicken Sie auf **NEU** zur Erstellung einer neuen IPSec-Verbindung:



The screenshot shows the web interface of the Digitalisierungsbox 2. On the left is a navigation menu with categories like Systemverwaltung, Netzwerk, and VPN. The 'VPN' category is expanded, and 'IPSec' is selected. The main content area shows the 'IPSec-Verbindungen' page with a breadcrumb trail: INTERNET & NETZWERK > VPN > IPSEC > IPSEC-VERBINDUNGEN. Below the breadcrumb are several sub-menus: IPSEC-VERBINDUNGEN (highlighted with a red box), IPSEC IKE PROPOSALS, IPSEC ESP PROPOSALS, IPSEC POOLS, and GLOBALE IPSEC-EINSTELLUNGEN. A table with columns 'Beschreibung', 'Szenario', 'Authentifizierungsmethode', 'Status', and 'Aktion' is visible but empty. At the bottom right of the page, there is a red button labeled 'NEU' (highlighted with a red box).

Für unser Anwendungsbeispiel wählen Sie das IPSec-Szenario *IPSec-Fernzugangsserver*, wählen die **Authentifizierungsmethode** *Öffentlicher Schlüssel mit EAP MS-CHAPv2* und bestätigen die Eingabe mit **Weiter**:

### VPN-IPSec

<b>IPSec-Szenario</b> IPSec-Fernzugangsserver ▾	<b>Authentifizierungsmethode</b> Öffentlicher Schlüssel mit EAP MS-CHAPv2 ▾
--	--

WEITER    ABBRECHEN

Im ersten Teil der Konfiguration des Menüs **IPSec-Verbindungen** werden die Authentifizierungsdaten konfiguriert. Verwenden Sie hier die für unser Beispiel die in [Kapitel 2.1](#) definierten Einstellungen:



Home Telefonie WLAN **Internet & Netzwerk** Sprache ? Ausloggen

INTERNET & NETZWERK > VPN > IPSEC > IPSEC-VERBINDUNGEN

IPSEC-VERBINDUNGEN IPSEC IKE PROPOSALS IPSEC ESP PROPOSALS IPSEC POOLS GLOBALE IPSEC-EINSTELLUNGEN

## VPN-IPSec

**Administrativer Status**  
Aktiviert

**IPSec-Szenario**  
IPSec-Fernzugangsserver

**Authentifizierungsmethode**  
Lokal: Öffentliche Schlüssel (X.509-Zertifikate)  
Entfernt: EAP MS-CHAPv2

**Beschreibung**  
Win10-VPN-Clients

**Internet Key Exchange Version**  
IKEv2

**Lokaler Endpunkt**  
Beliebig

**Lokale ID**  
vpnqabintec.dyndns.ddnss.de

**Benutzername/Passwort**

Benutzername	Passwort
khmustermann	*****

OK ABBRECHEN

Im nächsten Teil sind der **IP-Adress-Pool** und in der Tabelle **Selektoren für den Datenverkehr** das lokale IP-Netzwerk der Digitalisierungsbox sowie das zu verwendende **IPSec IKE Proposal/IPSec ESP Proposal** zu konfigurieren.

**IP-Adress-Pool**

IP-Adress-Pool: Neu

IP-Poolname: IPSec-Pool

IP-Startadresse: 192.168.100.100

IP-Endadresse: 192.168.100.110

**Selektoren für den Datenverkehr**

Beschreibung	Lokales Subnetz
LAN	192.168.2.0/24

HINZUFÜGEN

**IPSec IKE Proposal**  
3: IKE-Win10 (1)

**IPSec ESP Proposal**  
3: IPSec-Win10 (1)

[Mehr anzeigen](#)

OK ABBRECHEN

### Hinweis:

In der Tabelle **Benutzername/Passwort** können mehrere Benutzereinträge konfiguriert werden. Hierüber wird eine Mehrfachnutzung der IPSec-Verbindung möglich. Die konfigurierten Nutzer können somit die IPSec-Verbindung gleichzeitig nutzen.

Bestätigen Sie die Einstellungen mit **OK**. Danach sieht die Tabelle der konfigurierten IPSec-Verbindungen wie folgt aus:

Home Telefonie WLAN **Internet & Netzwerk** Sprache ? Ausloggen

INTERNET & NETZWERK > VPN > IPSEC > **IPSEC-VERBINDUNGEN**

IPSEC-VERBINDUNGEN IPSEC IKE PROPOSALS IPSEC ESP PROPOSALS IPSEC POOLS GLOBALE IPSEC-EINSTELLUNGEN

## IPSec-Verbindungen

Beschreibung	Szenario	Authentifizierungsmethode	Status	Aktion
Win10-VPN-Clients	Fernzugangsserver	Öffentliche Schlüssel (X.509-Zertifikate)		

NEU

Hiermit ist die Konfiguration auf Ihrer Digitalisierungsbox abgeschlossen.

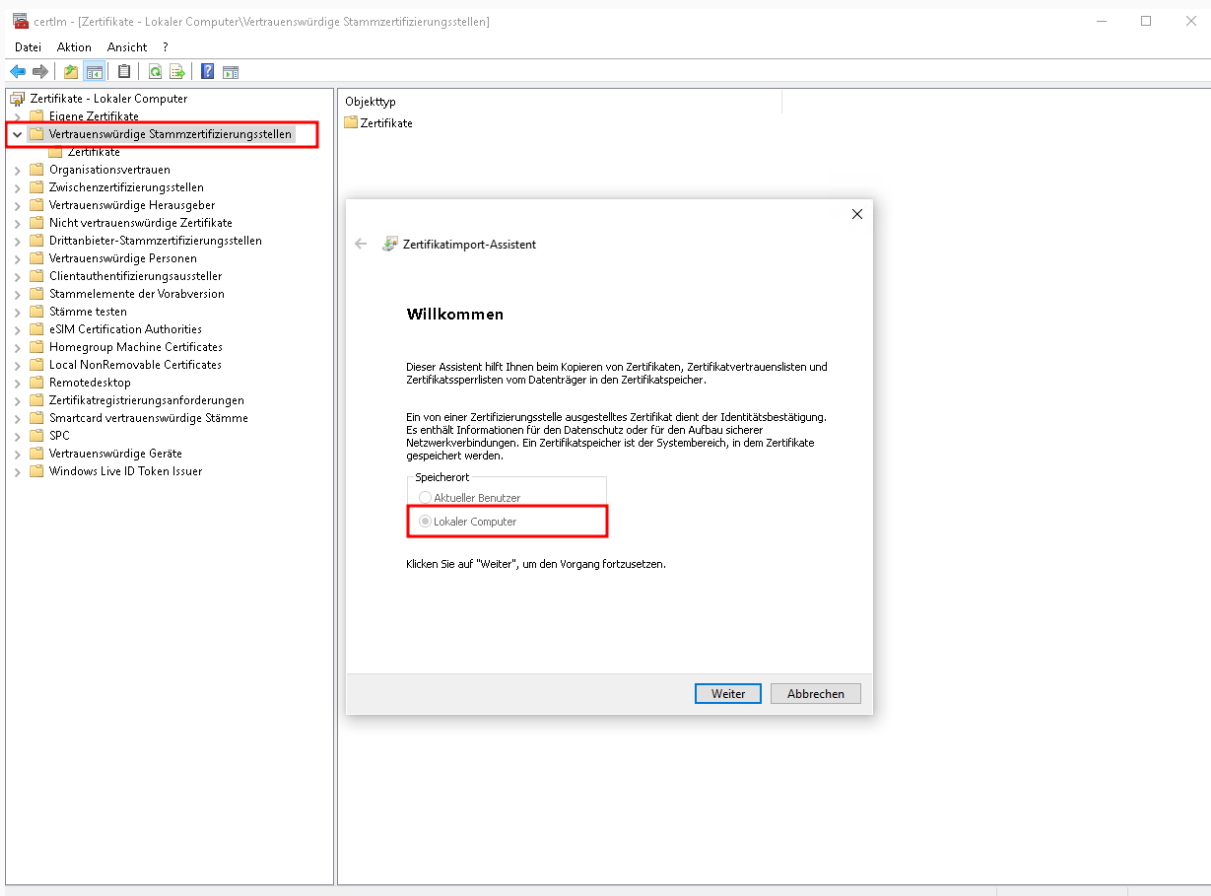
## 5 Konfiguration des Windows-10-Clients

Bei der Konfiguration ist folgende Reihenfolge zu beachten:

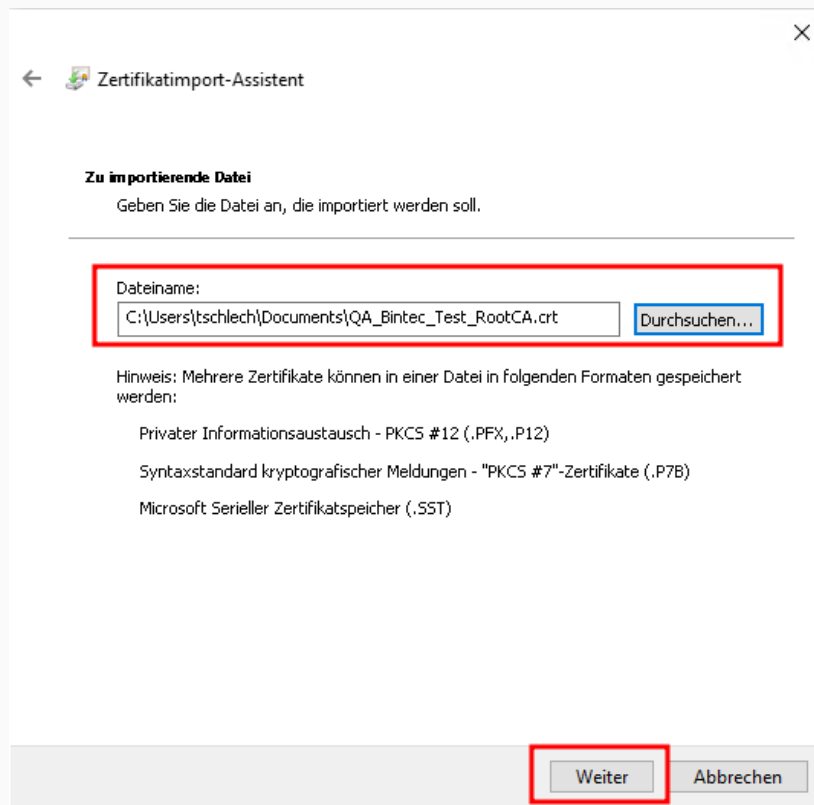
- (1) Import des Ausstellerzertifikats (CA-Zertifikat)
- (2) Konfiguration der IPSec-Verbindung.

### 5.1 Import des Ausstellerzertifikats (CA-Zertifikat)

Kopieren Sie hierzu das Ausstellerzertifikat (CA-Zertifikat) auf Ihren Windows-PC und öffnen Sie in der Systemsteuerung das Menü **Computerzertifikate verwalten (certlm)**. Wechseln Sie anschließend in den Bereich **Vertrauenswürdige Stammzertifizierungsstellen** und wählen Sie als Aktion **Import**. In dem sich öffnenden Fenster wählen Sie **Lokaler Computer** und klicken auf **Weiter**:



Anschließend wählen Sie die zu importierende Zertifikatsdatei (hier `QA_Bintec_Test_RootCA.crt`) und klicken auf **Weiter**:



← Zertifikatimport-Assistent

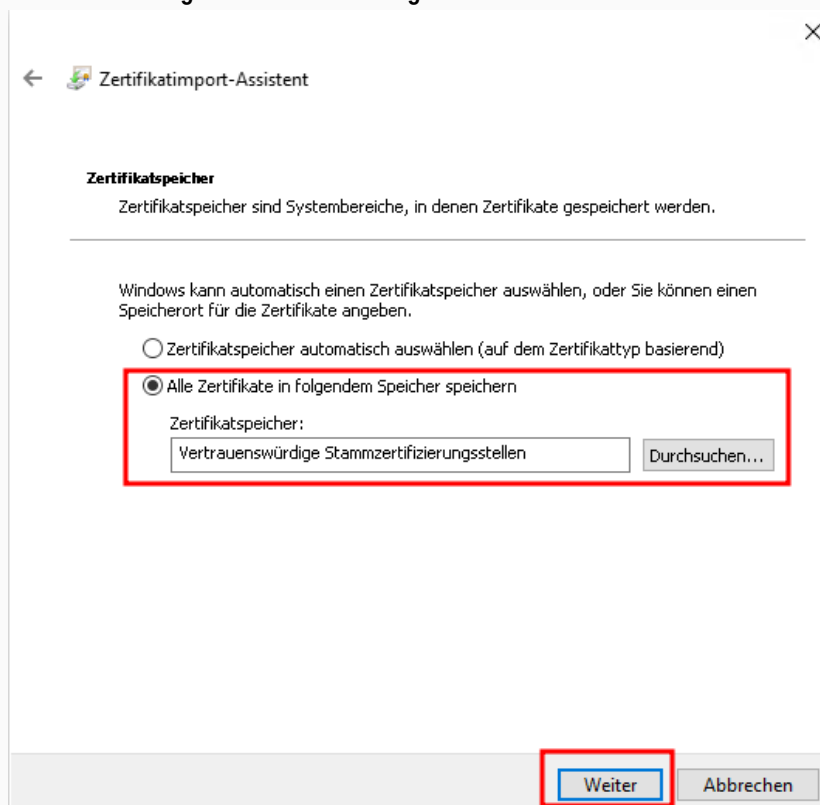
**Zu importierende Datei**  
Geben Sie die Datei an, die importiert werden soll.

Dateiname:  
C:\Users\tschlech\Documents\QA\_Bintec\_Test\_RootCA.crt

Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:

- Privater Informationsaustausch - PKCS #12 (.PFX, .P12)
- Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
- Microsoft Serieller Zertifikatspeicher (.SST)

Im nächsten Schritt wählen Sie bitte die Option **Alle Zertifikate in folgendem Speicher speichern** und als Zertifikatsspeicher **Vertrauenswürdige Stammzertifizierungsstellen** aus:



← Zertifikatimport-Assistent

**Zertifikatspeicher**  
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

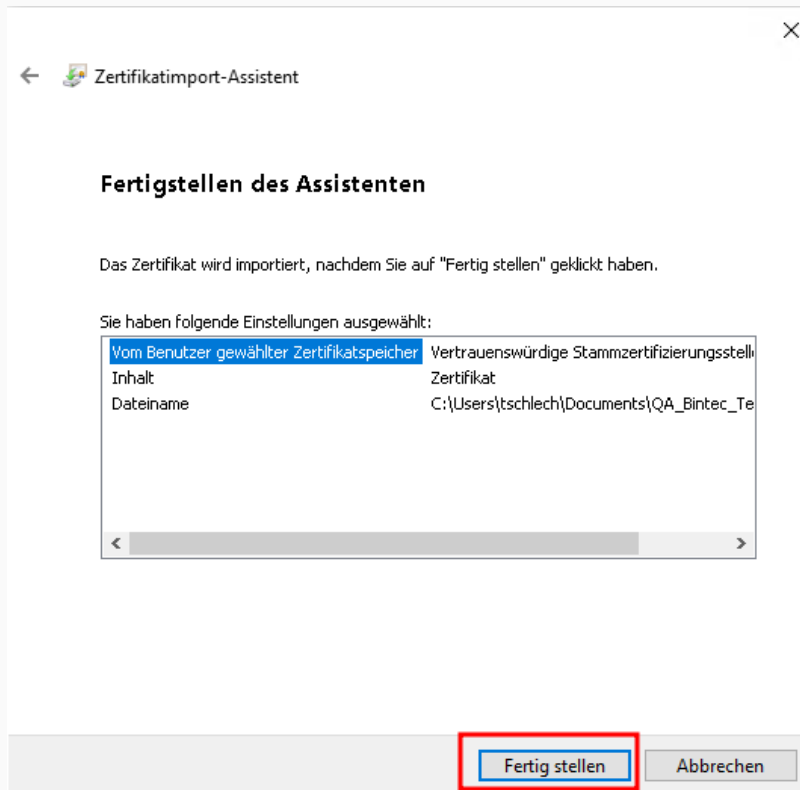
Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.

Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)

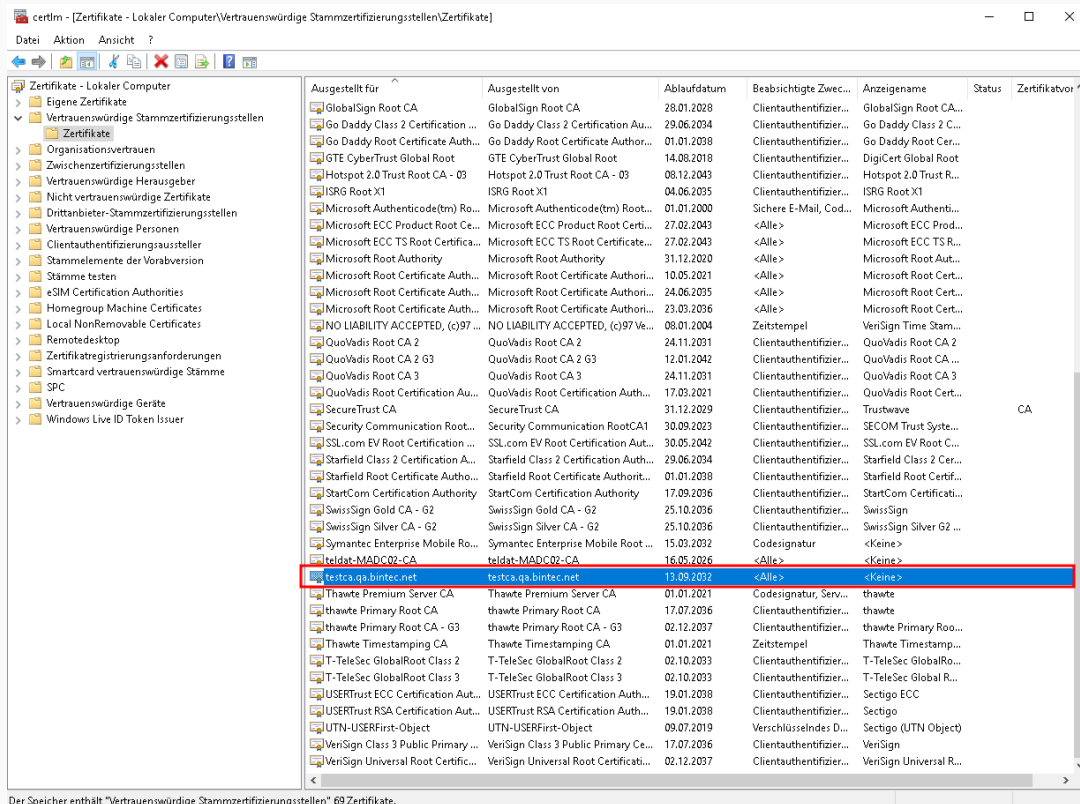
**Alle Zertifikate in folgendem Speicher speichern**

Zertifikatspeicher:  
Vertrauenswürdige Stammzertifizierungsstellen

Im letzten Schritt schließen Sie den Import mit einem Klick auf **Fertig stellen** ab:

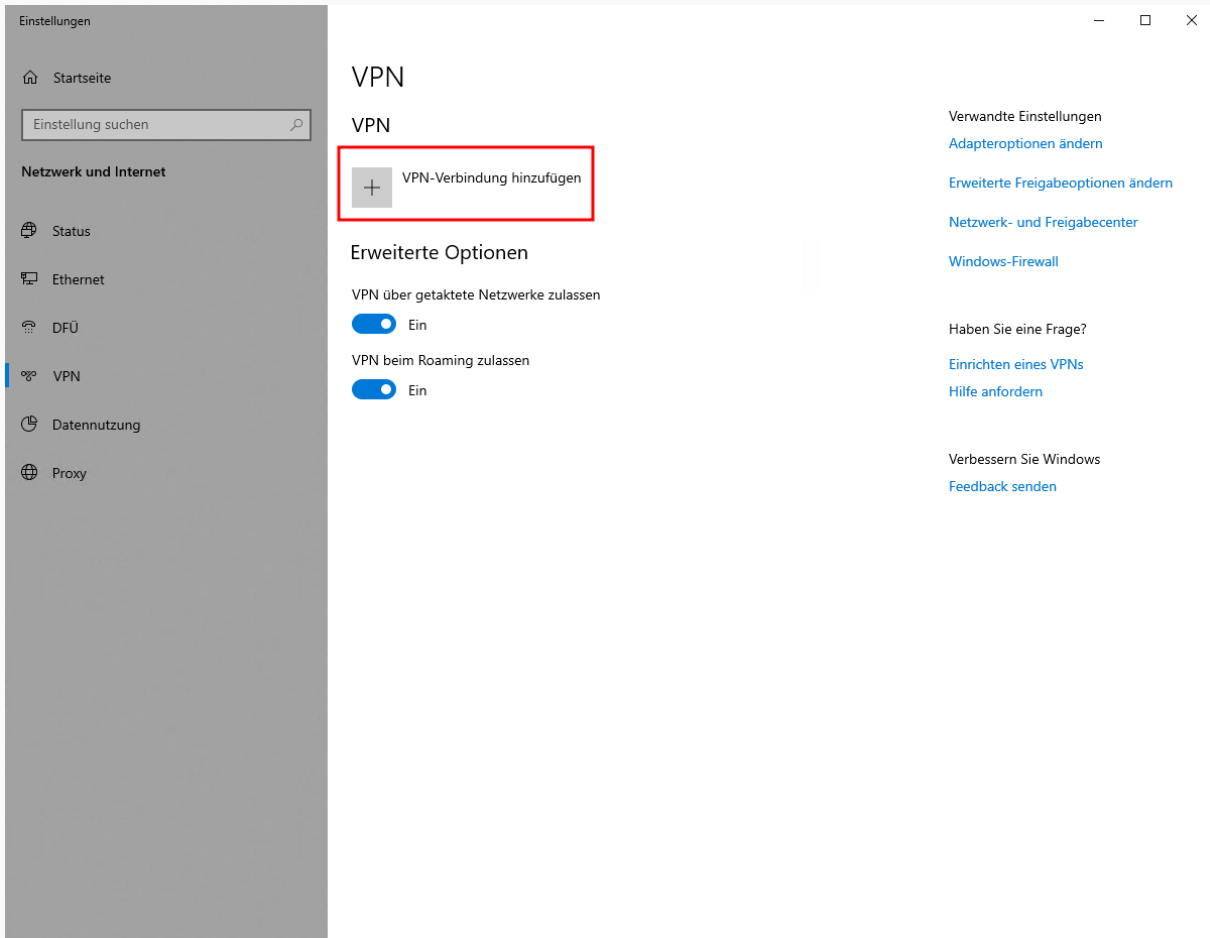


In der Liste der **Vertrauenswürdige Stammzertifizierungsstellen** ist nun unser importiertes Ausstellerzertifikat (CA-Zertifikat) enthalten:



## 5.2 Konfiguration der IPSec-Verbindung

Zur Konfiguration der IPSec-Verbindung auf dem Windows 10 PC öffnen Sie das Menü **VPN-Einstellungen**:



Öffnen Sie über **VPN-Verbindung hinzufügen** das Menü zur Erstellung der VPN-Verbindung und konfigurieren Sie die Verbindung wie folgt:

<b>VPN-Anbieter</b>	Windows (integriert)
<b>Servername</b>	Hostname der Digitalisierungsbox, in unserem Bsp. <i>vpngabintec.dyndns.ddnss.de</i> .
<b>VPN-Typ</b>	IKEv2
<b>Anmeldeinformationstyp</b>	Benutzernamen und Kennwort
<b>Benutzername</b>	Benutzernamen (khmustermann)
<b>Kennwort</b>	Kennwort (Nai4weiS)
<b>Anmeldeinformationen speichern</b>	ja

VPN-Verbindung hinzufügen

VPN-Anbieter  
Windows (integriert)

Verbindungsname  
IKEv2-Public-Key\_with\_EAP-MS-Chapv2

Servername oder IP-Adresse  
vpnqabintec.dyndns.ddnss.de

VPN-Typ  
IKEv2

Anmeldeinformationstyp  
Benutzername und Kennwort

Benutzername (optional)  
khmustermann

Kennwort (optional)  
••••••••

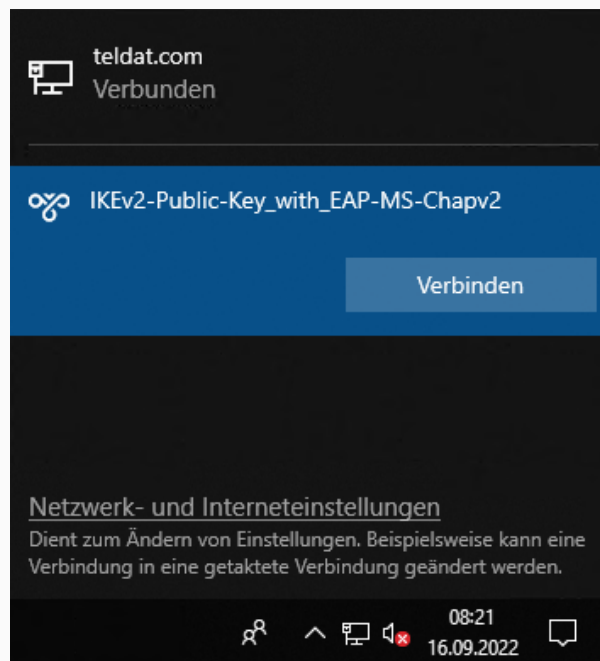
Anmeldeinformationen speichern

Speichern Abbrechen

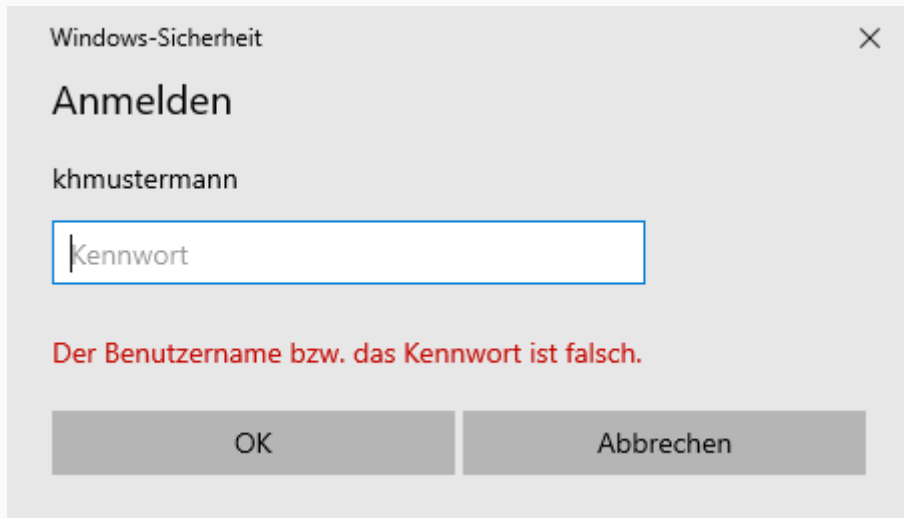
Schließen Sie die Konfiguration mit **Speichern** ab. Hiermit ist die Konfiguration der IPSec-Verbindung auf dem Windows-10-Client abgeschlossen.

### 5.3 Aufbau der IPSec-Verbindung

Hierzu klicken Sie bitte am unteren rechten Rand des Windows Bildschirms auf **Netzwerk Internetzugriff**, wählen die konfigurierte VPN-Verbindung aus und starten Sie den Verbindungsaufbau mittels **Verbinden**:



Bei erfolgreicher Authentifizierung der Digitalisierungsbox gegenüber dem Windows-Client wird für den konfigurierten Benutzer noch einmal das Kennwort abgefragt:



Nach erfolgter Benutzerauthentifizierung ist die VPN-Verbindung nutzbar und der Status wechselt auf *Verbunden*. Abgebaut werden kann die VPN-Verbindung durch **Trennen** (wie im folgenden Bild gezeigt):





## 6 Anhang

### 6.1 Erstellung der VPN-Verbindung über Windows 10 PowerShell

Wie im [Kapitel 2.1](#) bereits erwähnt gibt es die Möglichkeit, die VPN-Verbindung über die Windows PowerShell zu konfigurieren. Die PowerShell bietet die Möglichkeit, sehr viel sicherere IPSec-Einstellungen zu konfigurieren, als es über den Windows-Assistenten möglich ist.

In unserem Beispiel werden folgende IKE/IPSec Proposal Einstellungen verwendet:

#### IKE (Phase 1) Proposal:

IKE Version	IKEv2
Verschlüsselungsalgorithmus	AES256-GCM
Integritätsalgorithmus	SHA2-256_128 HMAC
Pseudozufallsfunktion	SHA2-256-PRF
Diffie-Hellmann-Gruppe	ECP256 (19)

#### IPSec (Phase 2) Proposal:

Verschlüsselungsalgorithmus	AES256-GCM
Integritätsalgorithmus	SHA2-256_128 HMAC
Diffie-Hellmann-Gruppe (PFS)	ECP256 (19)

Zur Konfiguration gehen Sie wie folgt vor:

Zum Start der PowerShell, geben Sie einfach im Startmenü **PowerShell** ein. Klicken Sie mit der rechten Maustaste auf den Eintrag und wählen Sie **Als Administrator ausführen** aus. Anschließend geben Sie folgende Kommandos ein:

#### Schritt 1. Kommando zum Hinzufügen der VPN-Verbindung

```
Add-VpnConnection -Name "IKEv2-EAP-MS-Chapv2_AES256GCM" -ServerAddress  
vpnqabintec.dyndns.ddns.de -TunnelType "Ikev2" -EncryptionLevel Required -  
RememberCredential
```

#### Schritt 2. Kommando zum Hinzufügen der VPN IPSec-Konfiguration

```
Set-VpnConnectionIPsecConfiguration -ConnectionName "IKEV2-EAP-MS-Chapv2_AES256GCM"  
-AuthenticationTransformConstants GCMAES256 -CipherTransformConstants GCMAES256 -  
EncryptionMethod GCMAES256 -IntegrityCheckMethod SHA256 -PfsGroup ECP256 -DHGroup  
ECP256 -PassThru -Force
```

Im Bild ist das beispielhaft gezeigt:

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Add-VpnConnection -Name "IKEv2-EAP-MS-Chapv2_AES256GCM" -ServerAddress vpnqabintec.dyndns.ddnss.de -TunnelType "Ikev2" -
EncryptionLevel Required -RememberCredential
PS C:\WINDOWS\system32> Set-VpnConnectionIPsecConfiguration -ConnectionName "IKEv2-EAP-MS-Chapv2_AES256GCM" -AuthenticationTransformConstants GC
MAES256 -CipherTransformConstants GCMAES256 -EncryptionMethod GCMAES256 -IntegrityCheckMethod SHA256 -PfsGroup ECP256 -DHGroup ECP256 -PassThru
-Force

AuthenticationTransformConstants : GCMAES256
CipherTransformConstants         : GCMAES256
DHGroup                          : ECP256
IntegrityCheckMethod             : SHA256
PfsGroup                         : ECP256
EncryptionMethod                 : GCMAES256

PS C:\WINDOWS\system32> Get-VpnConnection

Name                : IKEv2-EAP-MS-Chapv2_AES256GCM
ServerAddress       : vpnqabintec.dyndns.ddnss.de
AllUserConnection  : False
Guid                : {E66401D2-762D-409A-93E1-34091ECE34E2}
TunnelType         : Ikev2
AuthenticationMethod : {Eap}
EncryptionLevel    : Custom
L2tpIPsecAuth     :
UseWinlogonCredential : False
EapConfigXMLStream : #document
ConnectionStatus   : Disconnected
RememberCredential : True
SplitTunneling     : False
DnsSuffix          :
IdleDisconnectSeconds : 0
```

Mit `Get-VpnConnection` kann man sich die wichtigsten Einstellungen der erstellten VPN-Anbindung anzeigen.

#### Hinweis:

Die Anmeldedaten für die IPSec-Verbindung werden beim ersten Verbindungsaufbau abgefragt und müssen daher nicht in der Konfiguration hinterlegt werden.

## 6.2 Split-Tunneling aktivieren

In der gezeigten Beispielkonfiguration kommt es aus Sicht des Windows-Clients zu folgendem Problem: Sämtliche vom Client gesendete Daten werden über den Tunnel gesendet. Das hat zur Konsequenz, dass der Datenverkehr ins Zielnetz 192.168.2.0/24 funktioniert, der Internetdatenverkehr jedoch nicht, da die IPSec-Konfiguration (Zielnetz 192.168.2.0/24) dies nicht zulässt.

Die Lösung des Problems ist die Aktivierung der Funktion **Split Tunneling** für die VPN-Verbindung. Diese kann für unsere VPN-Verbindung `IKEv2-EAP-MS-Chapv2_AES256GCM` über folgendes PowerShell-Kommando aktiviert werden:

```
Set-VpnConnection -Name "IKEv2-EAP-MS-Chapv2_AES256GCM" -SplitTunneling $True
```

Damit der Datenverkehr ins Zielnetz 192.168.2.0/24 funktionieren kann, muss nun eine Route in unser Zielnetz 192.168.2.0/24 konfiguriert werden. Dies ist über das PowerShell Kommando **Add-VpnConnectionRoute** möglich. Für unser Beispiel sieht dies wie folgt aus:

```
Add-VpnConnectionRoute -ConnectionName "IKEv2-EAP-MS-Chapv2_AES256GCM" -
DestinationPrefix "192.168.2.0/24" -PassThru
```

Damit funktioniert nach Aufbau der VPN-Verbindung alles wie gewünscht: Der Internetdatenverkehr wird direkt über die Standardroute ins Internet und der zu verschlüsselnde Datenverkehr ins Zielnetz 192.168.2.0/24 über unsere VPN-Verbindung übertragen .