

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

2 TECHNISCHE UND PLANERISCHE VORAUSSETZUNGEN. 4 2.1 IPSEC-EINSTELLUNGEN. 4 3 ERSTELLUNG UND EXPORT DER ZERTIFIKATE. 6 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 4 KONFIGURATION DER DIGITALISIERUNGSBOX 15 4.1 DYNDNS-KONFIGURATION. 15 4.2 AKTIVIERUNG VON IPSEC. 17 4.4 KONFIGURATION DER NE (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 WINDOWS-10-CLIENTS. 27 5.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT). 27 5.2 KONFIGURATION DER VINDOWS-10-CLIENTS. 27 5.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT). 27 5.2 KONFIGURATION DER WINDOWS-10-CLIENTS. 27 5.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT). 30 <td< th=""><th>1</th><th>EINLEITUNG</th><th>3</th></td<>	1	EINLEITUNG	3
2.1 IPSEC-EINSTELLUNGEN. 4 3 ERSTELLUNG UND EXPORT DER ZERTIFIKATE. 6 3.1 HINWEISE ZUM THEMA ERSTELLUNG CA-SIGNIERTER BENUTZERZERTIFIKATE. 6 3.2 ERSTELLUNG DES AUF DER DIGITALISIERUNGSBOX ZU VERWENDENDEN PRIVATEN SCHLÜSSELS7 7 3.3 ERSTELLUNG DES AUF DER DIGITALISIERUNGSBOX ZU VERWENDENDEN BENUTZERZERTIFIKATS7 7 3.4 EXPORT DES AUSSTELLERZERTIFIKATES (CA-ZERTIFIKATES). 12 3.5 EXPORT DES BENUTZERZERTIFIKATES SOWIE DES PRIVATEN SCHLÜSSELS. 13 4 KONFIGURATION DER DIGITALISIERUNGSBOX 15 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 INDOWS-10-CLIENTS. 27 5.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT). 27 5.2 KONFIGURATION DER IPSEC-VERBINDUNG AUF DER DIGITALISIERUNGSBOX 2	2	TECHNISCHE UND PLANERISCHE VORAUSSETZUNGEN	4
3 ERSTELLUNG UND EXPORT DER ZERTIFIKATE. 6 3.1 HINWEISE ZUM THEMA ERSTELLUNG CA-SIGNIERTER BENUTZERZERTIFIKATE. 6 3.2 ERSTELLUNG DES AUF DER DIGITALISIERUNGSBOX ZU VERWENDENDEN PRIVATEN SCHLÜSSELS7 3.3 ERSTELLUNG DES AUF DER DIGITALISIERUNGSBOX ZU VERWENDENDEN BENUTZERZERTIFIKATS7 3.4 EXPORT DES AUSSTELLERZERTIFIKATES (CA-ZERTIFIKATES). 12 3.5 EXPORT DES BENUTZERZERTIFIKATES SOWIE DES PRIVATEN SCHLÜSSELS. 13 4 KONFIGURATION DER DIGITALISIERUNGSBOX 15 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. 20 4.5 KONFIGURATION DER IPSEC-VERBINDUNG AUF DER DIGITALISIERUNGSBOX 2. 24 5 KONFIGURATION DES WINDOWS-10-CLIENTS. 27 5.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT) 27 5.2 KONFIGURATION DER IPSEC-VERBINDUNG. 30 5.3 AUFBAU DER IPSEC-VERBINDUNG. <th></th> <th>2.1 IPSEC-EINSTELLUNGEN</th> <th>4</th>		2.1 IPSEC-EINSTELLUNGEN	4
3.1 HINWEISE ZUM THEMA ERSTELLUNG CA-SIGNIERTER BENUTZERZERTIFIKATE	3	ERSTELLUNG UND EXPORT DER ZERTIFIKATE	6
4 KONFIGURATION DER DIGITALISIERUNGSBOX. 15 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 5 KONFIGURATION DES WINDOWS-10-CLIENTS. 27 5.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT). 27 5.2 KONFIGURATION DER IPSEC-VERBINDUNG. 30 5.3 AUFBAU DER IPSEC-VERBINDUNG. 31 6 ANHANG. 33 6.1 ERSTELLUNG DER VPN-VERBINDUNG ÜBER WINDOWS 10 POWERSHELL. 33 6.2 SPLIT-TUNNELING AKTIVIEREN. 34		 3.1 Hinweise zum Thema Erstellung CA-signierter Benutzerzertifikate 3.2 Erstellung des auf der Digitalisierungsbox zu verwendenden Privaten Schlüssels 3.3 Erstellung des auf der Digitalisierungsbox zu verwendenden Benutzerzertifikats 3.4 Export des Ausstellerzertifikates (CA-Zertifikates)	6 7 7 12 13
4.1 DYNDNS-KONFIGURATION154.2 AKTIVIERUNG VON IPSEC174.3 IMPORT DER ZERTIFIKATE174.4 KONFIGURATION DER IKE (PHASE 1) UND IPSEC (PHASE 2) PROPOSALS204.4.1 IKE (Phase 1) Proposal204.4.2 IPSec (Phase 2) Proposal224.5 KONFIGURATION DER IPSEC-VERBINDUNG AUF DER DIGITALISIERUNGSBOX 2245 KONFIGURATION DES WINDOWS-10-CLIENTS275.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT)275.2 KONFIGURATION DER IPSEC-VERBINDUNG305.3 AUFBAU DER IPSEC-VERBINDUNG316 ANHANG336.1 ERSTELLUNG DER VPN-VERBINDUNG ÜBER WINDOWS 10 POWERSHELL336.2 SPLIT-TUNNELING AKTIVIEREN34	4	KONFIGURATION DER DIGITALISIERUNGSBOX	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. 20 4.5 KONFIGURATION DER IPSEC-VERBINDUNG AUF DER DIGITALISIERUNGSBOX 2. 24 5 KONFIGURATION DES WINDOWS-10-CLIENTS. 27 5.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT). 27 5.2 KONFIGURATION DER IPSEC-VERBINDUNG. 30 5.3 AUFBAU DER IPSEC-VERBINDUNG. 31 6 ANHANG. 33 6.1 ERSTELLUNG DER VPN-VERBINDUNG ÜBER WINDOWS 10 POWERSHELL. 33 6.2 SPLIT-TUNNELING AKTIVIEREN. 34		4.1 DYNDNS-KONFIGURATION	15
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 5 KONFIGURATION DES WINDOWS-10-CLIENTS. 27 5.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT). 27 5.2 KONFIGURATION DER IPSEC-VERBINDUNG. 30 5.3 AUFBAU DER IPSEC-VERBINDUNG. 31 6 ANHANG. 33 6.1 ERSTELLUNG DER VPN-VERBINDUNG ÜBER WINDOWS 10 POWERSHELL. 33 6.2 SPLIT-TUNNELING AKTIVIEREN. 34		4.2 Aktivierung von IPSec	17
4.4 KONFIGURATION DER IKE (PHASE 1) UND IPSEC (PHASE 2) PROPOSALS		4.3 Import der Zertifikate	17
4.4.1 IKE (Phase 1) Proposal		4.4 KONFIGURATION DER IKE (PHASE 1) UND IPSEC (PHASE 2) PROPOSALS	20
4.4.2 IPSec (Phase 2) Proposal		4.4.1 IKE (Phase 1) Proposal	20
4.5 KONFIGURATION DER IPSEC-VERBINDUNG AUF DER DIGITALISIERUNGSBOX 2		4.4.2 IPSec (Phase 2) Proposal	22
5 KONFIGURATION DES WINDOWS-10-CLIENTS. 27 5.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT). 27 5.2 KONFIGURATION DER IPSEC-VERBINDUNG. 30 5.3 AUFBAU DER IPSEC-VERBINDUNG. 31 6 ANHANG. 33 6.1 ERSTELLUNG DER VPN-VERBINDUNG ÜBER WINDOWS 10 POWERSHELL. 33 6.2 SPLIT-TUNNELING AKTIVIEREN. 34		4.5 KONFIGURATION DER IPSEC-VERBINDUNG AUF DER DIGITALISIERUNGSBOX 2	24
5.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT) 27 5.2 KONFIGURATION DER IPSEC-VERBINDUNG. 30 5.3 AUFBAU DER IPSEC-VERBINDUNG. 31 6 ANHANG. 33 6.1 ERSTELLUNG DER VPN-VERBINDUNG ÜBER WINDOWS 10 POWERSHELL. 33 6.2 SPLIT-TUNNELING AKTIVIEREN. 34	5	KONFIGURATION DES WINDOWS-10-CLIENTS	27
5.2 Konfiguration der IPSec-Verbindung. 30 5.3 Aufbau der IPSec-Verbindung. 31 6 ANHANG. 33 6.1 Erstellung der VPN-Verbindung über Windows 10 PowerShell. 33 6.2 Split-Tunneling aktivieren. 34		5.1 IMPORT DES AUSSTELLERZERTIFIKATS (CA-ZERTIFIKAT)	27
5.3 Aufbau der IPSec-Verbindung		5.2 Konfiguration der IPSec-Verbindung	30
6 ANHANG		5.3 Aufbau der IPSec-Verbindung	31
6.1 Erstellung der VPN-Verbindung über Windows 10 PowerShell	6	ANHANG	33
6.2 Split-Tunneling aktivieren		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 <u>Kapitel 3</u>.
- 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:

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

IPSec (Phase 2) Proposal:

Verschlüsselungsalgorithmus	AES256-CBC
Integritätsalgorithmus	SHA1-HMAC
Diffie-Hellmann-Gruppe (PFS)	MODP1024 (2)

bintec elmeg GmbH Nürnberg



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 <u>Kapitel 6</u> beschrieben.

Für die IPSec-Verbindung gelten folgende Vorgaben:

IPSec-Verbindung:

IKE Version	IKEv2
Authentifizierungsmethode	Öffentlicher Schlüssel mit EAP MS-CHAPv2
Lokale ID der Digitalisierungsbox	vpnqabintec.dyndns.ddnss.de
IPSec Gateway IP-Adresse / Hostname der Digitalisierungsbox	vpnqabintec.dyndns.ddnss.de
Lokales Netzwerk	192.168.2.0/24
IPSec-Client IP-Adress-Pool (IPSec-Clients wird dynamisch aus diesem IP-Adress-Pool eine IP-Adresse zugewiesen)	192.168.10.100 - 110
Benutzer 1 (Benutzername/Passwort)	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 <u>X - Certificate and Key management</u> 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-Zertifikats wird hier an dieser Stelle nicht behandelt. Lesen Sie hierzu z. B. die <u>XCA - Step by Step guides</u>. 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*:

X Certificate and Key management — — X						
Private Schlüssel Zertifikatsanträge Zertifikate Vorlagen	Rücknahmelisten					
Interner Name Typ	Länge Br 400.6 bit					
VPN Gateway - Privater Schlüssel RSA	2048 bit					
	Import					
	Import PFX (PKCS#12)					
	Detail <u>s</u> anzeigen					
	Löschen					
٢	>					
Datenbank: C:/Users/tschlech/Documents/QA-Bintec-Test-CA.xdb Suchen						

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			?	×
rstelle x509 Zertifikat			(a) Carried	- - 7/41
Herkunft Inhaber Erweiterungen Schlüsselverw	vendung Netscape Erweit	ert		
Zertifikatsantrag				
Diesen Zertifikatsantrag unterschreiben				~
🗹 Erweiterungen aus dem Zertifikatsantrag kopieren		Request anzeigen		
Inhaberinformation "subject" des Zertifikatsantrags än	Idern			
Erstelle ein Selbst signiertes Zertifikat mit der Serien nu Erstelle ein Selbst signiertes Zertifikat zum Unterschreiben	ummer 1 QA Bintec Test CA			•
Signatur algorithmus	SHA 256			•
Vorlage für das neue Zertifikat				
HTTP5_server				•
	Erweiterungen übernehmen	Subject übernehmen	Alles übernehm	en
		с	K Car	ncel

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:



Ì	X Certificate and Key	management			?	×
E	rstelle x509 Z	ertifikat				- Zine
	Herkunft Inhaber	Erweiterungen Schlüsselverwendung) Netscape Erweit	ert		
	Distinguished name					
	Interner Name	VPN Gateway	organizationName	bintec elmeg GmbH		
	countryName	DE] organizationalUnitName	QA		
	stateOrProvinceName	Bavaria	commonName	vpnqabintec.dyndns.ddnss.d	de	
	localityName	Nuremberg	emailAddress			
	Тур	,	Inhalt Hostname	muss auflösba	Hinzufügen Löschen	!
	Privater Schlüssel					_
	VPN Gateway - Private	er Schlüssel (RSA:2048 bit)	 auch verwendete 	Schlüssel Erstelle einen ner	uen Schlüss	el
				ОК	Can	cel

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 manag	jement						?	×
Erstelle x509 Zertifi	kat						A	4 9 7 7 4 11
Herkunft Inhaber Erwe	iterungen	Schlüsselverwendung	Netscape	Erwe	itert			
-X509v3 Basic Constraints						Key identifie	r	
Typ End Instanz				•		Subject I	Key Identifie	r
Pfadlänge					🗹 Critical	Authorit	y Key Identif	ier
Gültigkeit Nicht vor dem Nicht nach dem X509v3 Subject Alternative Nam	13.09. 13.09.	2022 11:18 GMT V 2023 11:18 GMT V	Zeitspanne 365 Mitternac	ht 🗌] Ortszeit	Tage ▼ □ Undefinierte	Übernehma es Ablaufdatu Bearbeil	en jim
X509v3 Issuer Alternative Name	. [Bearbeil	ten
VE0042 CBL Distribution Points							Bearbeil	ton .
Authority Information Access	0	CSP 🔻					Bearbeil	ten
						ОК	Car	ncel

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



Herkunft Inhaber Erweiterungen Schlüsselverwend	ung Netscape Erweitert
X509v3 Key Usage	X509v3 Extended Key Usage Critical TLS Web Client Authentication Code Signing E-mail Protection Time Stamping Microsoft Individual Code Signing Microsoft Commercial Code Signing Microsoft Commercial Code Signing Microsoft Server Gated Crypto Microsoft Encrypted File System Netscape Server Gated Crypto Microsoft EFS File Recovery IPSec End System IPSec Tunnel IPSec User IP security end entity Microsoft Smartcardlogin OCSP Signing EAP over IPP EAP over Lan Signing KDC Response

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):*

🎻 X Certificate and Key management		?	×
Zertifikatsexport			August - Tine
Name QA Bintec Test CA Dateiname C:/Users/tschlech/Documents,	/QA_Bintec_Test_RootCA.crt]
PEM Textformat mit Kopf- und Fußzeilen		Exportformat PEM (*.crt) OK C	Tancel
bintec elmeg GmbH Nürnberg	Seite 12 von 34	23.09.2	22



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**.



🭼 X Certificate and Key management	? ×
Zertifikatsexport	A Community Day
Name VPN Gateway	
Dateiname C:/Users/tschlech/Documents/VPN_Gateway.p12	
Das Zertifikat und der zugehörige private Schlüssel als verschlüsselte PKCS#12 Datei	Exportformat PKCS #12 (*.p12)
	OK Cancel

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.

🥜 X Certificate and Key management	? ×
Passwort	
Bitte geben Sie das Passwort zur Verschlüsselung d	er PKCS#12 Datei an
Passwort Passwort wiederholen	
	DK Cancel

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** (<u>https://ddnss.de/login.php</u>). 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=xxxxx&pwd=xxxxx&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:

Systemverwaltung	~					Sprache 🕜 Ausloggen
Netzwerk	~	Home Telefonie WLAN	N Internet & Netzwerk			
Erweiterte WLAN Einstellungen	~	INTERNET & NETZWERK > LOKALE	E DIENSTE > DYNDNS > DYNAMISC	HES DNS		
Lokale Dienste						
DNS						
DynDNS		Liste der eir	ngerichteten	Dynamic DNS-Kon	iten	
UPnP		Dynamic DNS stellt dem Inter	metnutzer eine Methode zur Verfü	igung, seine(n) Domänennamen mit		
Routing	~	Computern oder Servern zu ve	erbinden. Dynamic DNS stellt sich	ner, dass sich der Domänenname		
VPN	~	Adresse ändert.				
Firewall	~					
Physikalische Schnittstellen	~	Dieses Leistungsmerkmar wir DNS-Verbindung können Sie ti	trotz einer dynamischen IP-Adress	se lokal eine eigene Webseite, einen		
VolP	~					
Nummerierung	~					
Endgeräte	~					
Endgeräte Anrufkontrolle	č	Anbieter	Kontoname	Domainname	Aktiviert	Einstellen
Endgeräte Anrufkontrolle Anwendungen	~ ~ ~	Anbieter Es wurden keine Dynamic DN	Kontoname NS-Konten erstellt.	Domainname	Aktiviert	Einstellen
Endgeräte Anrufkontrolle Anwendungen Wartung	* * *	Anbieter Es wurden keine Dynamic DN	Kontoname NS-Konten erstellt.	Domainname	Aktiviert	Einstellen
Endgeräte Anrufkontrolle Anwendungen Wartung Monitoring	* * * *	Anbieter Es wurden keine Dynamic DN	Kontoname NS-Konten erstellt.	Domainname	Aktiviert	Einstellen
Endgeräte Anrufkontrolle Anwendungen Wartung Monitoring	* * * *	Anbieter Es wurden keine Dynamic DN	Kontoname YS-Konten erstellt.	Domainname	Aktiviert	Einstallen
Endgeräte Anrufkontrolle Anwendungen Wartung Monitoring	* * * *	Anbieter Es wurden keine Dynamic DN NEU	Kontoname VS-Konten erstellt.	Domainame	Aktiviert	Einstellen
Endgeräte Anrufkontrolle Anwendungen Wartung Monitoring	> > > >	Arbieter Es wurden keine Dynamic DN NEU	Kontoname VS-Konten erstellt.	Domainame	Aktiviert	Einstellen
Endgeräte Anrufkontrolle Anwendungen Wartung Monitoring	> > > >	Aebieter Es wurden keine Dynamic DN	Kontoname VS-Konten erstellt.	Domainame	Aktiviert	Einstellen
Endgeräte Anrufkontrolle Anwendungen Wartung Monitoring	* * *	Aebieter Es wurden keine Dynamic DN	Kontoname VS-Konten erstellt.	Domainname	Aktiviert	Einstellen
Endgeräte Anrufkontrolle Anwendungen Wartung Monitoring	* * *	Aebieter Es wurden keine Dynamic DN NEU	Kontename NS-Konten erstellt.	Domainame	Aktiviert	Einstallen
Endgeräte Anrufkontrolle Anrwendungen Wartung Monitoring	* * * *	Anbieter Es wurden keine Dynamic DN NEU	Kontename NS-Konten erstellt.	Domainame	Aktiviert	Einstellen
Endgesite Anrufkontrolle Annendungen Wartung Monitoring	* * *	Anbieter Es wurden keine Dynamic DN NEU	Kontoname VS-Konten erstellt.	Domainame	Aktiviert	Einstellen
Endgesite Anrufkontrolle Annendungen Westung Monitoring	* * *	Arbierer Es wurden keine Dynamic DN NEU	Kontoname VS-Konten erstellt.	Domainame	Aktiviert	Einstellen

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», «lpaddr», «ipaddró». 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 belspielsweise so zusammen:			
 inttps://ur//unstimestancestermanestarestermanestarestarestarestarestarestarestarestar			
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?t			
Erwartete Antwort des Servers: Domainname:			
Kontoname: Passwort:			
Passwortbestätigung:			
Dynamic DNS-Interface: PPPOE - VLAN 7 - WANOE V Aktivieren:			
	SPI	EICHERN	ABBRECHEN

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

Home Telefonie WLAN	Internet & Netzwerk			Sprache	2 Ausloggen
INTERNET & NETZWERK > LOKALE DIEN	STE > DYNDNS > DYNAMISCHES DNS				
Liste der eing Dynamic DNS stellt dem Internetru Computern oder Servern zu verblin automätisch der IP-Adresse anpas Adresse ändert.	Ierichteten Dyna Itzer eine Methode zur Verfügung, seine Iden. Dynamic DNS stellt sicher, dass sich st, Indem sich Ihr DNS-Eintrag ändert, wa	mic DNS-Konte n) Domänenname mit 1 der Domänenname nnn immer sich ihre IP-	en		
Dieses Leistungsmerkmal wird dur DNS-Verbindung können Sie trotz e E-Mail-Server, einen FTP-Server un	ch einen externen Dienstleister bereitge: einer dynamischen IP-Adresse lokal eine d anderes mehr betreiben.	stellt. Mit einer Dynamic eigene Webselte, einen			
Dynamic DNS einschalten					
Anbieter	Kontoname	Domainname	Aktiviert	Einstellen	
Update URL			\checkmark	/ 1	
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:

Systemverwaltung	~	Sprache	Ausloggen
Netzwerk		Home Telefonie WLAN Internet & Netzwerk	
Erweiterte WLAN Einstellungen		INTERNET & NETZWERX > VPN > IPSEC > GLOBALE IPSEC-EINSTELLUNGEN	
Lokale Dienste			
Routing		IPSEC-VERBINDUNGEN IPSEC IKE PROPOSALS IPSEC ESP PROPOSALS IPSEC POOLS GLOBALE IPSEC-EINSTELLUNGEN	
VPN			
IPSec		Globale IPSec-Finstellungen	
Firewall		IPSec bletet eine sichere Datenübertragung über optentiell unsichere Netze wie dem Internet an und ermöglicht die Einrichtung eines Virtual Private Networks (VPN).	
Physikalische			
Schnittstellen		IPSec aktivieren	
VoIP		Aktiviert	
Nummerierung			
Endgeräte			
Anrufkontrolle			✓ Mehr anzeigen
Anwendungen			-
Wartung			
Monitoring	~		
			ок

4.3 Import der Zertifikate

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

Systemverwaltung				Sprache	0	Ausloggen
Systeminformation	en	Home Telefonie WLAN Internet & Netzwerk				
Administrativer Zugriff		HOME > SYSTEMVERWALTUNG > ZERTIFIKATE > ZERTIFIKATSLISTE				
Globale Einstellungen						
Kennziffern		Zertifikatsliste				
Zertifikate		Zortimitatonoto				
Netzwerk	~	Beschreibung Typ	Status			
Erweiterte WLAN Einstellungen	~					
Lokale Dienste	~					
Routing	~					
VPN	~					
Firewall	~					
Physikalische Schnittstellen	~					
VolP	~					
Nummerierung	~					
Endgeräte	~					
Anrufkontrolle	~					
Anwendungen	~					
Wartung	~					
Monitoring	~					
				ок	CERTIFI	CATE IMPORT

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**:

bintec elmeg GmbH Nürnberg	Seite 17 von 34	23.09.22
bintec eineg Ginbh Numberg	Selle 17 VOII 34	23.09.22

Nome Yeard WLAN Weard WLAN Hotees & SYSTEMMERNALLUNG > ZERIFIKATEL > ZERIFIKATELESE Zertifikatsimpport Beschreibung Rocc Ca Zertifikat X:50% bodiert (unverschlüsselt, PEMFformatiert) ~ Zertifikat X:50% bodiert (unverschlüsse	Digitalisierungsbox 2 Release 16.40.2.12.00		bi	ntec elm	leg
HOME > SYSTEMVERWALTUNG > ZERTIFIKATE > ZERTIFIKATE.SLISTE Zertifikatsimport Root-CA Kennwort für geschütztes Zertifikat Deteiname Bowse QA. Biner, Tert, PootCA.ort	Home Telefonie WLAN Internet & Netzwerk			Sprache 👔 /	Ausloggen
	HOME > SYSTEMVERWALTUNG > ZERTIFIKATE > ZERTIFIKATSLISTE Zertifikatsimport Beschreibung Root-CA Kennwort für geschütztes Zertifikat	Zertifikatstyp Zertifikat X.509-kodiert (unverschlüsselt, PEM-formatiert) Zertifikat kann ein Benutzer-oder CA-Zertifikat sein Datelname Browse QA_Bintec_Test_RootCA.crt	Für IPSec verwenden		

Die Zertifikatsübersicht sieht nun wie folgt aus:

Home	Telefonie	WLAN Internet & Netzwerk		Sprache	0	Ausloggen		
HOME > SYSTEMVERWALTUNG > ZERTIFIKATE > ZERTIFIKATSLISTE								
Zer	tifikats	liste						
	Beschreibung	Тур	Status					
1:	Root-CA	CA-Zertifikat X.509 File	Verfügbar	<u>*</u>	/	Î		
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		Q			

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

Digitalisierungsbox 2 Release 16.40.2.12.00		bintec elmeg
Home Telefonie WLAN Internet & Netzwerk		Sprache 🕢 Ausloggen
HOME > SYSTEMVERWALTUNG > ZERTIFIKATE > ZERTIFIKATSLISTE Zertifikatsimport Beschreibung VPN-Gateway Kennwort für geschütztes Zertifikat	Zertifikatstyp Zertifikat und Schlüssel PKCS#12-verpackt v DateIname Browse VPN_Cateway.p12	Für IPSec verwenden

Die Zertifikatsübersicht sieht nun wie folgt aus:

Home	Telefonie WL	AN Internet & Netzwerk		Sprache	Ø	Ausloggen
HOME >	SYSTEMVERWALTUNG	> ZERTIFIKATE > ZERTIFIKATSLISTE				
Zer	tifikatsli	iste				
	Beschreibung	Тур	Status			
1:	Root-CA	CA-Zertifikat X.509 File	Verfügbar	±	/	Î
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		Q	
2:	VPN-Gateway	Zertifikat, Schlüssel PKCS#12 File	Nicht unterstützte Verschlüsselung	t	/	î
2.2		Zertifikat X.509			Q	
2.3		CA-Zertifikat X.509			Q	

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:

Systemverwaltung	~							Sprache	0	iusloggen
Netzwerk		Home Telefon	nie WLAN	Internet	& Netzwerk					
Erweiterte WLAN Einstellungen		INTERNET & NETZWEI	RK > VPN >	IPSEC > I	PSEC IKE PROPOSALS					
Lokale Dienste										
Routing					IPSEC-VERBINDUNGEN IPSEC IKE PROPOSALS	IPSEC ESP PROPOSALS IPSEC POO	LS GLOBALE IPSEC-EINS	TELLUNGEN		
VPN										
IPSec		IPSec.L	KF Pr	onos	sals					
Firewall	~	11 0001		opot	baio					
Physikalische Schnittstellen		Beschreibung	Gruppenindex	Priorität	Verschlüsselungsalgorithmen	Pseudozufallsfunktionen	Integritätsalgorithmen	Diffie-Hellman-Gruppen		
VoIP						prfsha256-prfsha384-		ecp256-ecp384-ecp521- ecp256bp-ecp384bp-ecp512bp-		
Nummerierung		default	0	1	aes128-aes192-aes256-aes128ctr-aes192ctr- aes256ctr	prfsha512-prfaesxcbc- prfaescmac	sha2_256-sha2_384- sha2_512-aesxcbc	modp2048-modp3072- modp4096-modp6144-		
Endgeräte						procontao		modp8192		
Anrufkontrolle					aae128ccm16.aae102ccm16.aae256ccm16.			ecp256-ecp384-ecp521-		
Anwendungen		default	0	2	aes128ccm12-aes192ccm12-aes256ccm12-	1926cm17-ees256ccm170 prfsha384- 1922cm17-ees256ccm12 prfsha312.prfsha384- 1922gcm17-ees256gcm16 prfaescmac 1922gcm17-ees256gcm12 prfaescmac				
Wartung					aes128gcm10-aes192gcm10-aes250gcm10- aes128gcm12-aes192gcm12-aes256gcm12					
Monitoring	~									
		& SCU02	1	1	aes256	prfsha256	sha256	modp1536	/	Î
		Swyx SCU03 (IKEv2 only)	2	1	aes256gcm12-aes256gcm16	prfsha256		ecp521	/	i i
										NEU

Klicken Sie auf **NEU** und konfigurieren Sie das Proposal gemäß der in <u>Kapitel 2.1</u> beschriebenen IPSec-Einstellungen:

Home Telefonie WLAN Internet & Net	zwerk			
INTERNET & NETZWERK > VPN > IPSEC > IPSEC I	KE PROPOSALS			
IPSEC	C-VERBINDUNGEN IPSEC IKE PROPOSALS	IPSEC ESP PROPOSALS IPSEC POOLS	GLOBALE IPSEC-EINSTELLUNGEN	
IPSec IKE Proposa	l			
Beschreibung	Gruppenindex		Prioritätsindex	
IKE-WIN10	3 🗸			
Verschlüsselungsalgorithmen benötigen einen ser Integritätsalgorithmus	paraten			
Ja				
Verschlüsselungsa	lgorithmen			
3DES-EDE-CBC AES	3128-CBC AES192-CBC	AES256-CBC	AES128-CTR	AES192-CTR
AES256-CTR				
Integritätsalgorithn	nen			
				OK ABBRECHEN

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

bintec elmeg GmbH Nürnberg	Seite 20 von 34	23.09.22
0 0		

Digitalisierungsbox 2

Release 16.4	0.2.12.00		bir	itec elmeg
Home Telefonie WLA	N Internet & Netzwerk			Sprache 😢 Ausloggen
Integritätsa	lgorithmen			
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
Pseudozufa	allsfunktionen	(PRF)		
MD5-PRF	SHA1-PRF	AES-XCBC-PRF	AES-CMAC-PRF SHA2_256-PRF	SHA2_384-PRF
SHA2_512-PRF				
Diffie-Hellm	an-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 Telefor	ie WLAN	Internet	& Netzwerk			Sprache		Ausioggen		
INTERNET & NETZWE	INTERNET & NETZWERK > VPN > IPSEC > IPSEC IKE PROPOSALS									
			IPSEC-VERBINDUNGEN IPSEC IKE PROPOSALS	IPSEC ESP PROPOSALS IPSEC POOL	S GLOBALE IPSEC-EINS	TELLUNGEN				
IPSec I	KE Pr	opos	sals							
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		i i		
Swyx SCU03 (IKEv2 only)	2	1	aes256gcm12-aes256gcm16	prfsha256		ecp521	/	Î		
IKE-Win10	3	1	aes256	prfsha256	sha256	modp1024	/	Î		



0

4.4.2 IPSec (Phase 2) Proposal

Wechseln Sie hierzu in das Menü IPSec ESP Proposals:

Systemverwaltung								Spr	ache	0	Ausloggen
Netzwerk		Home Telefonie	WLAN	Internet & N	letzwerk						
Erweiterte WLAN Einstellungen		INTERNET & NETZWERK	> VPN > IPS	EC > IPSE	C ESP PROPOSALS						
Lokale Dienste							_				
Routing			IPSEC-VERBINDUNGEN IPSEC IKE PROPOSALS IPSEC ESP PROPOSALS IPSEC POOLS GLOBALE IPSEC-EINSTELLUNGEN								
VPN											
IPSec		IPSec ES	SP Pro	ppos	als						
Firewall		11 0000 24		poo							
Physikalische Schnittstellen		Beschreibung	Gruppenindex	Priorität	Verschlüsselungsalgorithmen		Integritätsalgorithmen	Diffie-Hellman-Gruppen (PFS)			
VoIP							sha2 256-sha2 384-	ecp256-ecp384-ecp521-ecp256bp ecp384bp-ecp512bp-modp2048-			
Nummerierung		default	0	1	aes128-aes192-aes256-aes128ctr-aes192	ctr-aes256ctr	sha2_512-aesxcbc	modp3072-modp4096-modp6144- modp8192			
Endgeräte								ecp256-ecp384-ecp521-ecp256bp			
Anrufkontrolle		default	0	2	aes192ccm16-aes192ccm16-aes256ccm1 aes192ccm12-aes256ccm12-aes128gcm1	16-aes128ccm12- 16-aes192gcm16-		ecp384bp-ecp512bp-modp2048- modp3072-modp4096-modp6144-			
Anwendungen					aes256gcm16-aes128gcm12-aes192gcm1	12-aes256gcm12	modp8192				
wartung Monitoring	* *	IPSec (ESP) SCU01 & SCU02	1	1	aes256		sha1	modp1536		/	Î
		IPSec (ESP) SCU03 (IKEv2 only)	2	1	aes256gcm12-aes256gcm16			ecp521		1	
									_		NEU

Klicken Sie auf **NEU** und konfigurieren Sie das Proposal gemäß der in <u>Kapitel 2.1</u> beschriebenen IPSec-Einstellungen:

Home Telefonie WLAN Internet & Netzwerk			
INTERNET & NETZWERK > VPN > IPSEC > IPSEC ESP PROPOSALS			
IPSEC-VERBINDUNGEN	IPSEC IKE PROPOSALS	IPSEC POOLS GLOBALE IPSEC-EINSTELLUNGEN	
IPSec ESP Proposal			
Beschreibung	Gruppenindex	Prioritätsindex	
IPSec-Win10	3 🗸		
Verschlüsselungsalgorithmen benötigen einen separaten Integritätsalgorithmus Ja			
Verschlüsselungsalgorith	men		
3DES-EDE-CBC AES128-CBC	AES192-CBC	AES256-CBC AES128-CTR	AES192-CTR
AES256-CTR			
Integritätsalgorithmen			
			OK ABBRECHEN

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

Digitalisierungsbo Release 16.40.2.12		bint	ec	eln	neg				
Integritätsalgoriti	hmen								
MD5-HMAC	MD5_128-HMAC	SHA1-HMAC		SHA1_160-HMAC	\bigcirc	AES-XCBC	\bigcirc	AES-CM4	AC
AES_128-GMAC	AES_192-GMAC	AES_256-GMAC	\bigcirc	SHA2_256_128 HMAC	\bigcirc	SHA2_384_192 HMAC	\bigcirc	SHA2_51	2_256 HMAC
Diffie-Hellman-G	ruppen (PFS)								
MODP1024 (2)	MODP1536 (5)	MODP2048 (14)	\bigcirc	MODP3072 (15)	\bigcirc	MODP4096 (16)	\bigcirc	MODP61	44 (17)
MODP8192 (18)	ECP192 (25)	ECP224 (26)		ECP256 (19)		ECP384 (20)		ECP521 ((21)
ECP224BP (27)	ECP256BP (28)	ECP384BP (29)	\bigcirc	ECP512BP (30)	\bigcirc	CURVE25519 (31)	\bigcirc	CURVE44	48 (32)
								ок	ABBRECHEN

ļ

Die IPSec ESP Proposals Übersicht sieht nun wie folgt aus.

							Sprache	?	Auslo	ggen
Home Telefonie	WLAN	Internet & N	etzwerk							
INTERNET & NETZWERK > VPN > IPSEC > IPSEC ESP PROPOSALS										
		IPS	EC-VERBINDUNGEN IPSEC IKE PROPOSALS	PSEC ESP PROPOSALS	IPSEC POOLS GLOBALE	IPSEC-EINSTELLUNGEN				
IPSec E	SP Pro	pos	als							
Beschreibung	Gruppenindex	Priorität	Verschlüsselungsalgorithmen		Integritätsalgorithmen	Diffie-Hellman-Gruppen (PFS)				
default	0	1	aes128-aes192-aes256-aes128ctr-aes192ctr-aes	s256ctr	sha2_256-sha2_384- sha2_512-aesxcbc	ecp256-ecp384-ecp521-ecp2 ecp384bp-ecp512bp-modp20 modp3072-modp4096-modp6 modp8192	56bp- 48- 5144-			
default	0	2	aes128ccm16-aes192ccm16-aes256ccm16-aes aes192ccm12-aes256ccm12-aes128gcm16-aes aes256gcm16-aes128gcm12-aes192gcm12-aes	128ccm12- 192gcm16- 256gcm12		ecp256-ecp384-ecp521-ecp2 ecp384bp-ecp512bp-modp20 modp3072-modp4096-modp6 modp8192	56bp- 48- 5144-			
IPSec (ESP) SCU01 & SCU02	1	1	aes256		sha1	modp1536		1		Î
IPSec (ESP) SCU03 (IKEv2 only)	2	1	aes256gcm12-aes256gcm16			ecp521			•	Î
IPSec-Win10	3	1	aes256		sha1	modp1024		1		Î



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:

Systemverwaltung	~		Sprache	0	Ausloggen
Netzwerk		Home Telefonie WLAN Internet & Netzwerk		Ŭ	
Erweiterte WLAN Einstellungen		INTERNET & NETZWERK > VPN > IPSEC > IPSEC-VERBINDUNGEN			
Lokale Dienste					
Routing		IPSEC-VERBINDUNGEN IPSEC IKE PROPOSALS IPSEC ESP PROPOSALS IPSEC POOLS GLOBALE IPSEC-EINSTELLUNGEN			
VPN					
IPSec		IPSec-Verbindungen			
Firewall	~				
Physikalische Schnittstellen		Beschreibung Szenario Authentifizierungsmethode Status Aktion			
VoIP					
Nummerierung					
Endgeräte					
Anrufkontrolle					
Anwendungen					
Wartung					
Monitoring	~				
					NEU

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	
IPSec-Szenario	Authentifizierungsmethode 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 <u>Kapitel 2.1</u> definierten Einstellungen:

Digitalisierungst Release 16.40.2.	oox 2 12.00			bintec	elı	neg	
Home Telefonie WLAN Inte	ernet & Netzwerk				Sprac	ne 💔	Ausloggen
INTERNET & NETZWERK > VPN > IPSEC	> IPSEC-VERBINDUNGEN						
	IPSEC-VERBINDUNGEN	IPSEC IKE PROPOSALS	IPSEC ESP PROPOSALS	IPSEC POOLS	GLOBALE IPSEC-EINSTELLUNGEN		
VPN-IPSec							
Administrativer Status		IPSec-Szenario			Authentifizierungsmethode		
Aktiviert		IPSec-Fernzugangsserver			Lokal: Offentliche Schlusser (X.509-Zertifikate) Entfernt: EAP MS-CHAPv2		
Beschreibung		Internet Key Exchang	e Version				
Win10-VPN-Clients		IKEV2					
Lokaler Endpunkt							
Beliebig 💙							
Lokale ID							
vpnqabintec.dyndns.ddnss.de							
Benutzername/Passwort							
Benutzername	Pas	swort	7				
khmustermann	•••	•••••		Î			
						ок	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 Neu Y IP-Startadresse 192.168.100.100 Selektoren für den Datenverkehr	IP-Poolname IPSec-Pool IP-Endadresse 192.168.100.110		
Beschreibung LAN HINZUFÜGEN	Lokales Subnetz 192.168.2.0/24	i i	1
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:

vigitalisieru lelease 16.4	Ingsbox 2 40.2.12.00				_	bi	nte	c el	me
-lome Telefonie WL.	AN Internet & Netzwerk						Spi	ache 💡	Ausloge
TERNET & NETZWERK > VPN	> IPSEC > IPSEC-VERBINDUNGEN								
	IPSEC-VERBINDUNGEN	IPSEC IKE PROPOSALS	IPSEC ESP PROPOSALS	IPSEC POOLS	GLOBALE IP	SEC-EINSTELLUNGEN			
PSec-Verb	indungen								
Beschreibung Win10-VPN-Clients	Szenario Fernzugangsserver	Authentifizierungsmetho	el (X.509-Zertifikate)		Status	Aktion	î		Q
Win10-VPN-Clients	Fernzugangsserver	Öffentliche Schlüss	el (X.509-Zertifikate)		0	~ ~	Ĩ	1	Q

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:



X

Dateiname: C:\Users\tschlech\Documents\QA_Bintec_Test_RootCA.crt Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichwerden: Privater Informationsaustausch - PKCS #12 (.PFX,.P12)	CA.crt Durchsucher
Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichwerden: Privater Informationsaustausch - PKCS #12 (.PFX,.P12)	olgenden Formaten gespeicher
Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeich werden: Privater Informationsaustausch - PKCS #12 (.PFX,.P12)	olgenden Formaten gespeicher
Privater Informationsaustausch - PKCS #12 (.PFX,.P12)	
	.P12)
Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)	CS #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:

Zertif	katspeicher		
Z	ertifikatspeicher sind Systembere	eiche, in denen Zertihikate gespei	chert werden.
M S	indows kann automatisch einen Jeicherort für die Zertifikate ang	Zertifikatspeicher auswählen, od jeben.	er Sie können einen
	O Zertifikatspeicher automatis	sch auswählen (auf dem Zertifikal	typ basierend)
I	Alle Zertifikate in folgenden	n Speicher speichern	
	Zertifikatspeicher:		
	Vertrauenswürdige Stamm	nzertifizierungsstellen	Durchsuchen

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

bintec elmeg GmbH Nürnberg	Seite 28 von 34	23.09.22



X

÷	Ş	Zertifikatimport-Assistent	

Fertigstellen des Assistenten

Das Zertifikat wird importiert, nachdem Sie auf "Fertig stellen" geklickt haben.

Inhalt Dateiname	Zertifikat C:\Users\tschlech\Document:	s\QA_Bintec_T
Dateiname	C:\Users\tschlech\Document:	s\QA_Bintec_T
<		3
	Fastin staller	Abbasab

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

certim - Lertifikate - Lokaler Computer/Vertrauenswür	rdige stammzertifizierungsstellen\Zertifika	tej				_	ц ;
atei Aktion Ansicht ? • 🔿 📷 🔏 🗈 🗙 🕅 🗟 🗖 ன							
Zertifikate - Lokaler Computer	Ausgestellt für	Ausgestellt von	Ablaufdatum	Reabsichtigte Zwec	Anzeigename	Status	Zertifikatı
🧾 Eigene Zertifikate	GlobalSian Poot CA	GlobalSign Boot CA	20.01.2020	Clientsuthentifizier	GlobalSign Root CA	ototay	Lerenkee
📔 Vertrauenswürdige Stammzertifizierungsstellen	Contraction Contraction	Giobalsign Root CA	20.01.2020	Clientautrentifizier	Giobalsign Root CA		
🚞 Zertifikate	Co Daddy Class 2 Certification	Co Daddy Class 2 Certification Ad	29.00.2034	Clientauthentifizier	Go Daddy Class 2 C		
🦰 Organisationsvertrauen	Go Daddy Root Certificate Auth	Go Daddy Root Certificate Author	01.01.2038	Clientautnentifizier	Go Daddy Koot Cer		
📔 Zwischenzertifizierungsstellen	GIE Cyber Irust Global Root	GTE CyberTrust Global Root	14.08.2018	Clientauthentifizier	DigiCert Global Root		
📔 Vertrauenswürdige Herausgeber	Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	08.12.2043	Clientauthentifizier	Hotspot 2.0 Trust R		
🛅 Nicht vertrauenswürdige Zertifikate	LaIISRG Root X1	ISRG Root X1	04.06.2035	Clientauthentifizier	ISRG Root X1		
📋 Drittanbieter-Stammzertifizierungsstellen	Microsoft Authenticode(tm) Ro	Microsoft Authenticode(tm) Root	01.01.2000	Sichere E-Mail, Cod	Microsoft Authenti		
🛅 Vertrauenswürdige Personen	Microsoft ECC Product Root Ce	Microsoft ECC Product Root Certi	27.02.2043	<alle></alle>	Microsoft ECC Prod		
📋 Clientauthentifizierungsaussteller	Microsoft ECC TS Root Certifica	Microsoft ECC TS Root Certificate	27.02.2043	<alle></alle>	Microsoft ECC TS R		
📋 Stammelemente der Vorabversion	🔄 Microsoft Root Authority	Microsoft Root Authority	31.12.2020	<alle></alle>	Microsoft Root Aut		
🛅 Stämme testen	🔤 Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	10.05.2021	<alle></alle>	Microsoft Root Cert		
eSIM Certification Authorities	🔤 Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	24.06.2035	<alle></alle>	Microsoft Root Cert		
Homegroup Machine Certificates	🛛 🔄 Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	23.03.2036	<alle></alle>	Microsoft Root Cert		
📋 Local NonRemovable Certificates	🔄 🔄 NO LIABILITY ACCEPTED, (c)97	NO LIABILITY ACCEPTED, (c)97 Ve	08.01.2004	Zeitstempel	VeriSign Time Stam		
🛅 Remotedesktop	🔄 QuoVadis Root CA 2	QuoVadis Root CA 2	24.11.2031	Clientauthentifizier	QuoVadis Root CA 2		
📋 Zertifikatregistrierungsanforderungen	🔄 QuoVadis Root CA 2 G3	QuoVadis Root CA 2 G3	12.01.2042	Clientauthentifizier	QuoVadis Root CA		
📋 Smartcard vertrauenswürdige Stämme	🔄 QuoVadis Root CA 3	QuoVadis Root CA 3	24.11.2031	Clientauthentifizier	QuoVadis Root CA 3		
🗎 SPC	QuoVadis Root Certification Au	QuoVadis Root Certification Auth	17.03.2021	Clientauthentifizier	QuoVadis Root Cert		
📔 Vertrauenswürdige Geräte	SecureTrust CA	SecureTrust CA	31.12.2029	Clientauthentifizier	Trustwave		CA
📔 Windows Live ID Token Issuer	Security Communication Root	Security Communication RootCA1	30.09.2023	Clientauthentifizier	SECOM Trust Syste		
	SSL.com EV Root Certification	SSL.com EV Root Certification Aut	30.05.2042	Clientauthentifizier	SSL.com EV Root C		
	Starfield Class 2 Certification A	Starfield Class 2 Certification Auth	29.06.2034	Clientauthentifizier	Starfield Class 2 Cer		
	Starfield Boot Certificate Autho	Starfield Boot Certificate Authorit	01 01 2038	Clientauthentifizier	Starfield Boot Certif		
	StartCom Certification Authority	StartCom Certification Authority	17.09.2036	Clientauthentifizier	StartCom Certificati		
	SuizeSian Cold CA _ G2	Suircean Celd CA _ G2	25 10 2026	Clientauthentifizier	SeriesSign		
	Suissign Cold CA - 02	Suissaigh Obla CA - Oz	25.10.2030	Clientautientitzien	Suissaign Suissaign		
	Cartania Cartania Makila Da	Swisssign Silver CA - Gz	23.10.2030	Cirentautrenunzier	swisssign silver oz		
	Symantec Enterprise Mobile Ro	Symantec Enterprise Mobile Root	15.03.2032	Codesignatur	<keine></keine>		
	Lateldat-MADC02-CA	teldat-MADC02-CA	10.05.2026	KAIIE2	skeine>		
	testca.qa.pintec.net	testca.qa.bintec.net	13.09.2032	<alle></alle>	<keine></keine>		
	I nawte Premium Server CA	I nawte Premium Server CA	01.01.2021	Codesignatur, serv	thawte		
	La Ithawte Primary Root CA	thawte Primary Root CA	17.07.2036	Clientauthentifizier	thawte		
	Thawte Primary Root CA - G3	thawte Primary Root CA - G3	02.12.2037	Clientauthentifizier	thawte Primary Roo		
	Thawte Timestamping CA	Thawte Timestamping CA	01.01.2021	Zeitstempel	Thawte Timestamp		
	T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2	02.10.2033	Clientauthentifizier	T-TeleSec GlobalRo		
	🔄 T-TeleSec GlobalRoot Class 3	T-TeleSec GlobalRoot Class 3	02.10.2033	Clientauthentifizier	T-TeleSec Global R		
	USERTrust ECC Certification Aut	USERTrust ECC Certification Auth	19.01.2038	Clientauthentifizier	Sectigo ECC		
	USERTrust RSA Certification Aut	USERTrust RSA Certification Auth	19.01.2038	Clientauthentifizier	Sectigo		
	UTN-USERFirst-Object	UTN-USERFirst-Object	09.07.2019	Verschlüsselndes D	Sectigo (UTN Object)		
	🛛 🔄 VeriSign Class 3 Public Primary	VeriSign Class 3 Public Primary Ce	17.07.2036	Clientauthentifizier	VeriSign		
	VeriSign Universal Root Certific	VeriSign Universal Root Certificati	02.12.2037	Clientauthentifizier	VeriSign Universal R		
	-				-		



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:

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

bintec elmeg GmbH Nürnberg

Digitalisierungsbox 2 Release 16.40.2.12.00			bintec elmeg
VPN-Ve	rbindung hinzufügen		
VPN-Anbieto	er		
Windows (integriert) \sim		
Verbindungs	name		
IKEv2-Pub	ic-Key_with_EAP-MS-Chapv2		
Servername	oder IP-Adresse		
vpnqabint	ec.dyndns.ddnss.de		
VPN-Typ			
IKEv2	×		
Anmeldeinfo	ormationstyp		
Benutzerna	ame und Kennwort $$		
Benutzernan	ne (optional)		
khmustern	nann		
Kennwort (o	ptional)		
••••••	ି		
🗸 Anmeld	einformationen 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**:



bintec elmeg GmbH Nürnberg



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

Windows-Sicherheit				
Anmelden				
khmustermann				
Kennwort				
Der Benutzername bzw. das Kennwort ist falsch.				
ОК	Abbrechen			

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.ddnss.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 Power	Shell	- 🗆	\times
PS C:\WINDOWS\system32 EncryptionLevel Requin PS C:\WINDOWS\system32	2> Add-VpnConnection -Name "IKEv2-EAP-MS-Chapv2_AES256GCM" -ServerAddress vpnqabintec.dyndns.ddnss.de -TunnelTyp red -RememberCredential 2> Set-VpnConnectionIPsecConfiguration -ConnectionName "IKEv2-EAP-MS-Chapv2_AES256GCM" -AuthenticationTransformC	e "Ikev2 Constants	GC
MAES256 -CipherTransfo -Force	ormConstants GCNAES256 -EncryptionMethod GCNAES256 -IntegrityCheckMethod SHA256 -PfsGroup ECP256 -DHGroup ECP256		ru
AuthenticationTransfor	rmConstants : GCMAES256		
CipherTransformConstar	nts : GCMAES256		
DHGroup	: ECP256		
IntegrityCheckMethod	: 5HA250		
Prsuroup EncryptionMethod	: ELY 239 : GCMAE5256		
PS C:\WINDOWS\system32	2> Get-VpnConnection		
Name	: IKEv2-EAP-MS-Chapv2_AES256GCM		
ServerAddress	: vpnqabintec.dyndns.ddnss.de		
AllUserConnection	: False		
Guid TurnelTurne	: {L66401D2-762D-409A-93E1-34091ECE34E2}		
TunnerType AuthenticationMathod	: 1KeVZ		
Encryption evel	· Leaps · Custom		
L2tpIPsecAuth			
UseWinlogonCredential	: False		
EapConfigXmlStream	: #document		
ConnectionStatus	: Disconnected		
RememberCredential	: True		
Spirclunneling	- False		
TdleDisconnectSeconds	- 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 .