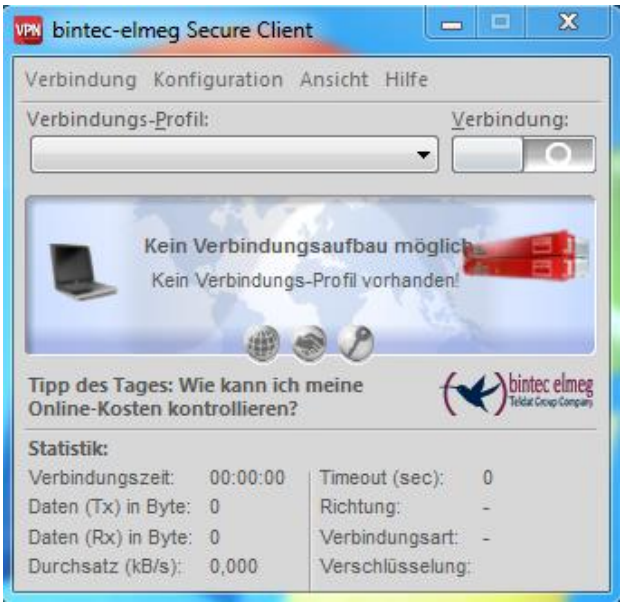
Installation des

bintec-elmeg Secure Client



In diesem Dokument finden Sie neben der Installationsbeschreibung eine kurze Produktbeschreibung. Zudem sind spezielle Installationsmöglichkeiten und die Lizenzierung beschrieben.

Weiterführende Beschreibungen zur Erstellung von Profilen und zur IPSec-Konfiguration finden Sie in den Beschreibung Secure Client Monitor und Secure Client Parameter.

Eine Übersicht bietet der Client-Navigator. In dieser PDF-Datei sind alle aktuell verfügbaren Dokumente zu Ihrem Client verzeichnet.

Vom Navigator aus können Sie alle relevanten Dokumente direkt auswählen und – falls sie noch nicht in Ihrem Navigationsverzeichnis gespeichert sind – von der bintec-Homepage herunterladen.

11. Oktober 2017

Inhalt

1. Produktbeschreibung

1.1. Bintec-elmeg Secure Client – universelle Lösung für sichere VPN-Lösungen

Der IPSec Client kann in beliebigen VPN-Umgebungen eingesetzt werden. Er kommuniziert auf der Basis des IPSec-Standards mit den Gateways verschiedenster Hersteller* und ist die Alternative zu der am Markt angebotenen, einheitlichen IPSec- Client-Technologie. Die Client-Software emuliert einen Ethernet LAN-Adapter. Der IPSec Client verfügt über zusätzliche Leistungsmerkmale, die dem Anwender den Einstieg in eine ganzheitliche Remote Access VPN-Lösung ermöglichen.

1.2. Der IPSec Client bietet

- Unterstützung aller gängigen Betriebssysteme

Einwahl über alle Übertragungsnetze

- Kompatibilität mit den VPN Gateways unterschiedlichster Hersteller
- Integrierte Personal Firewall für mehr Sicherheit
- Dialer-Schutz (keine Bedrohung durch 0190er- und 0900er-Dialer)
- Höhere Geschwindigkeit im ISDN (Kanalbündelung)
- Gebührenersparnis (Kosten- und Verbindungskontrolle)
- Bedienungskomfort (grafische Oberfläche)

1.3. Leistungsumfang

Der IPSec Client unterstützt alle gängigen Betriebssysteme 32 und 64 Bit (Windows 10, Windows 8.x, Windows 7, Windows Vista). Die Einwahl in das Firmennetz erfolgt unabhängig vom Mediatyp, d. h. neben ISDN, PSTN (analoges Fernsprechnetz), GSM, GPRS/UMTS und xDSL wird auch LAN-Technik wie im WLAN (am Firmengelände und Hotspot) oder lokalen Netzwerk (z. B. Filialnetz) unterstützt. Auf diese Weise kann mit ein und demselben Endgerät von unterschiedlichen Lokationen auf das Firmennetz zugegriffen werden:

- in der Filiale über WLAN
- in der Zentrale über LAN
- unterwegs an Hotspots und beim Kunden über WLAN bzw. GPRS
- im Home Office über xDSL oder ISDN

Weitere Informationen entnehmen Sie bitte unserer Webseite unter www.bintec-elmeg.com.

2. Installationsvoraussetzungen

Betriebssysteme	Windows (32 und 64 Bit): Windows 10, Windows 8.x, Windows 7, Windows Vista
Security Features	Unterstützung aller IPsec Standards nach RFC
Personal Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (Automatische Umschaltung der Firewall-Regeln bei Erkennung des angeschlossenen Netzwerkes anhand des IP-Adressbereiches oder eines FND-Servers*); FND-abhängige Aktion starten; Secure Hotspot Logon; Homezone; differenzierte Filterregeln bezüglich: Protokolle, Ports, Anwendungen und Adressen, Schutz des LAN-Adapters; IPv4 und IPv6 Unterstützung
VPN Bypass	Die VPN-Bypass-Funktion gestattet Anwendungen festzulegen, die trotz deaktiviertem Split Tunneling außerhalb der VPN-Konfiguration direkt ins Internet kommunizieren dürfen. Alternativ ist es möglich, Domänen bzw. Zieladressen zu bestimmen, zu denen die Datenkommunikation am VPN-Tunnel vorbei stattfinden soll.
Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC-konform; IPsec-Proposals können determiniert werden durch das IPsec - Gateway (IKEv1/IKEv2, IPsec Phase 2); Event log; Kommunikation nur im Tunnel; MTU Size Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPsec Tunnel Mode
Verschlüsselung (Encryption)	Symmetrische Verfahren: AES 128,192,256 Bits; Blowfish 128,448 Bits; Triple-DES 112,168 Bits; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 2048 Bits; Seamless Rekeying (PFS); Hash Algorithmen: SHA-256, SHA-384, SHA-512, MD5, DH Gruppe 1, 2, 5, 14-21, 25, 26
FIPS Inside	Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1747). Die FIPS Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden: • Diffie Hellman-Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 Bit) • Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit • Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit oder Triple DES

Authentisierungsverfahren	IKE (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP); PFS; PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): erweiterte Authentifikation gegenüber Switches und Access Points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): erweiterte Authentifikation gegenüber Switches und Access Points auf Basis von Zertifikaten (Layer 2); Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards und USB Tokens; Multi-Zertifikatskonfiguration; Pre-Shared Secrets; One-Time Passwords und Challenge Response Systeme (u.a. RSA SecurID Ready)
Starke Authentisierung - Standards	X.509 v.3 Standard; Entrust Ready PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); Smart Card Betriebssysteme: TCOS 1.2, 2.0 und 3.0; Smart Card ReaderInterfaces: PC/SC, CT-API; PKCS#12 Interface für Private Schlüssel in Soft Zertifikaten; CSP zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher; PIN-Richtlinie; administrative Vorgabe für die Eingabe beliebig komplexer PINs; Revocation: EPRL (End-entity Public-Key Certificate Revocation List, vorm. CRL), CARL (Certification Authority Revocation List, vorm. ARL), OCSP
Networking Features	LAN Emulation: Virtual Ethernet-Adapter mit NDIS-Interface, integrierter, vollständiger WLAN- (Wireless Local Area Netzwork) und WWAN-Support (Wireless Wide Area Network, Mobile Broadband ab Windows 7)
Netzwerkprotokoll	IP
Dialer	Internet Connector, Microsoft RAS Dialer (für ISP-Einwahl mittels Einwahl-Script) Connection Manager für internationale Einwahl via GoRemote (vorm. GRIC), UuNet, Infonet, MCI (auf Anfrage)
Seamless Roaming	Automatische Umschaltung des VPN-Tunnels auf ein anderes Internet-Übertragungsmedium (LAN/WLAN/3G/4G) ohne IP-Adresswechsel, so dass über den VPN-Tunnel kommunizierende Anwendungen nicht beeinflusst werden, bzw. die Anwendungs-Session nicht getrennt wird Voraussetzung: Secure Enterprise VPN Server
VPN Path Finder	VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist (Voraussetzung: VPN Path Finder Technology am VPN Gateway erforderlich)
IP Address Allocation	DHCP (Dynamic Host Control Protocol); DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server
Übertragungsmedien	Internet, LAN, WLAN, GSM (inkl. HSCSD), GPRS, UMTS, LTE, HSDPA, analoges Fernsprechnetz, ISDN

Line Management	DPD mit konfigurierbarem Zeitintervall; Short Hold Mode; WLAN-Roaming (Handover); Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert; Timeout (zeit- und gebührengesteuert); Budget Manager (Verwaltung von Verbindungszeit und/oder -volumen für GPRS/UMTS und WLAN, bei GPRS/UMTS getrennte Verwaltung für Roaming im Ausland)
APN von SIM Karte	Der APN (Access Point Name) definiert den Zugangspunkt eines Providers für eine mobile Datenverbindung. Die APN-Daten werden bei einem Providerwechsel automatisiert aus der jeweiligen SIM-Karte in die Client-Konfiguration übernommen
Datenkompression	IPCOMP (lzs), Deflate
Weitere Features	Automatische Mediatyp-Erkennung, UDP-Encapsulation; WISPr-Support (T-Mobile Hotspots); IPsec-Roaming bzw., WLAN-Roaming (Voraussetzung: Secure Enterprise VPN Server); Importfunktion der Dateiformate:*.ini, *.pcf, *.wgx und *.spd., Multi Zertifikatsunterstützung
Point-to-Point Protokolle	PPP over ISDN, PPP over GSM, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Internet Society RFCs und Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T),UDP encapsulation, IPCOMP
Client Monitor Intuitive, grafische Benutzeroberfläche	Mehrsprachig (Deutsch, Englisch, Spanisch, Französisch); Client Info Center; Konfiguration, Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files (farbige Darstellung, einfache Copy&Paste-Funktion); Test-Werkzeug für Internet-Verfügbarkeit; Trace-Werkzeug für Fehlerdiagnose; Ampelsymbol für Anzeige des Verbindungsstatus; Integrierte Anzeige von Mobile Connect Cards (PCMCIA, embedded); individuell gestaltbares Textfeld; Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre; Automatische Prüfung auf neue Version

3. Installationshinweise

Wenn Windows ein Anniversary-Update durchführt, empfiehlt sich den IPSec Client zu deinstallieren!

Bevor Sie die Software installieren, müssen zur vollen Funktionsfähigkeit die entsprechenden Installationsvoraussetzungen erfüllt sein:

Firewall deaktivieren

Antiviren-Programm deinstallieren

Anwendung des CC-Cleaners wird empfohlen / Registry bereinigen

3.1. Installation der Software

Die vorliegende Version und künftige Versionen des Clients werden von der Qualitätssicherung nur noch für die Windows-Betriebssysteme Windows 10, Windows 8.x, Windows XP und Windows Vista getestet. Für Windows NT sowie Windows 98 oder älter kann somit keine Gewähr mehr für die volle Funktionsfähigkeit der Client Software übernommen werden.

Sie können die Software in Form einer EXE-Datei als Download von der bintec elmeg-Internetseite unter www.bintec-elmeg.com beziehen. Die Installation erfolgt für die Betriebssysteme Windows 2000/XP und Vista im Wesentlichen gleich.

3.2. Installation und Lizenzierung

Der bintec Secure IPSec Client wird zunächst immer als Testversion installiert. Haben Sie eine Lizenz erworben, so können die Lizenzierungsdaten nach der Installation und einem Reboot im Monitor- Menü **Hilfe -> Lizenzinfo und Aktivierung** eingegeben werden. Spätestens in den letzten 10 Tagen vor Ablauf der 30-tägigen Gültigkeitsdauer der Testversion werden Sie im Client-Monitor daran erinnert, dass eine Lizenzierung vorgenommen werden muss, wenn die Client Software weiter verwendet werden soll. Bitte beachten Sie zur Lizenzierung die Beschreibung **Secure-Client-SW-Aktivierung**.

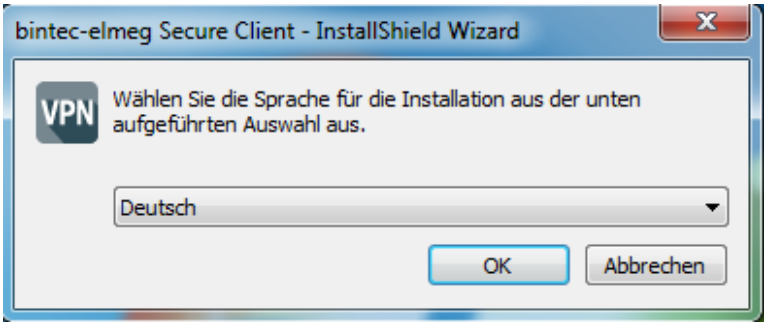
4. Standard-Installation

Die EXE-Datei, die Sie mit einem Download erhalten haben, kopieren Sie auf die Festplatte des PCs. Der Dateiname der EXE-Datei beinhaltet Versions- und Build-Nummer der Software, z. B.:

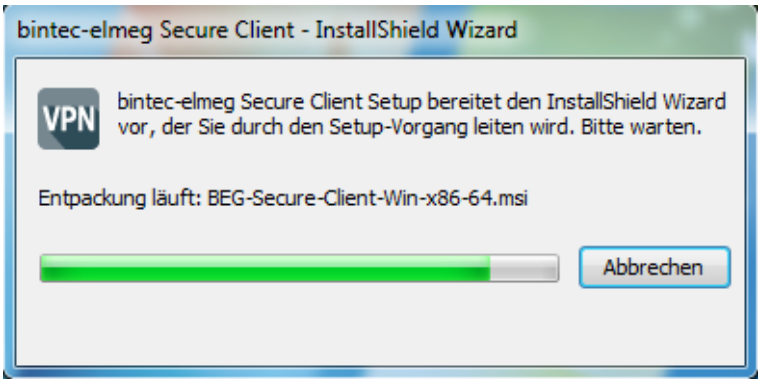
```
BEG_Secure-Clien_Windows-x86-64-304-31256.EXE
```

Wählen Sie im Windows-Hauptmenu **Start -> Einstellungen -> Systemsteuerung**. In der Windows-Systemsteuerung wählen Sie **Software** oder **Neue Programme hinzufügen**. Klicken Sie dann auf den Button zum Installieren von Festplatte. Im daraufhin erscheinenden Fenster klicken Sie auf **Durchsuchen**, um die EXE-Datei Ihrer Software im Verzeichnis <Disk1> zu suchen. Wenn sie angezeigt wird, klicken Sie auf **Fertigstellen**.

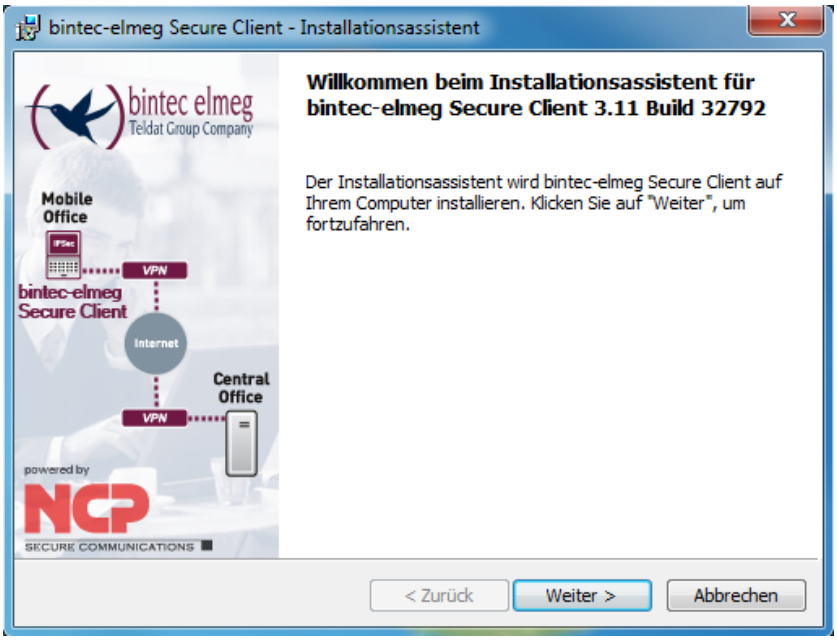
Im folgenden Fenster können Sie die Setup-Sprache auswählen. Klicken Sie danach auf **OK**.



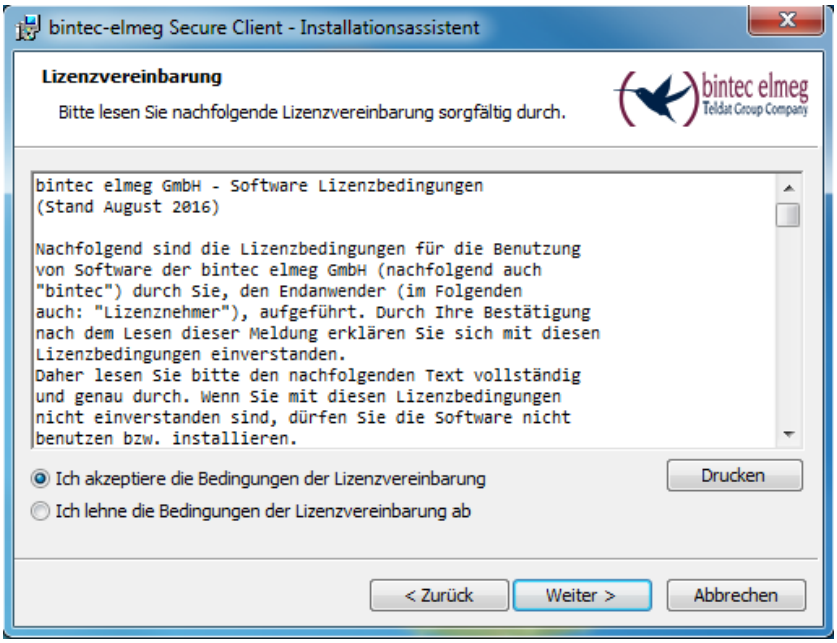
Anschließend bereitet das Setup-Programm den InstallShield-Assistenten vor, mit dessen Hilfe die Installation fortgesetzt wird.



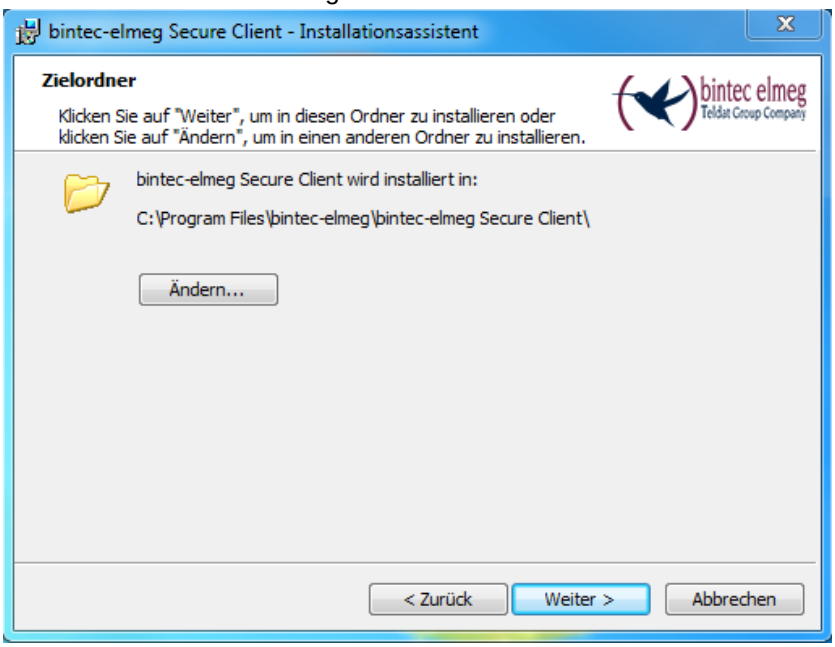
Lesen Sie bitte die Hinweise im Willkommen-Fenster des Setup-Programms bevor Sie auf **Weiter** klicken.



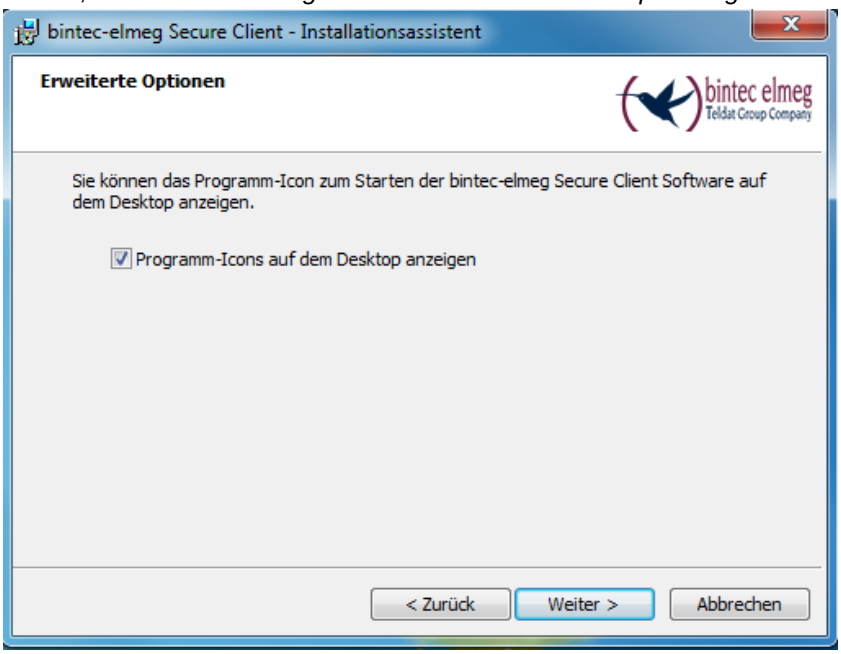
Anschließend werden die Lizenzbedingungen gezeigt. Aktivieren Sie *Ich akzeptiere die Bedienungen der Lizenzvereinbarung* und klicken Sie auf **Weiter**.



Belassen Sie die Einstellungen **Secure Client** und klicken Sie auf **Weiter**.

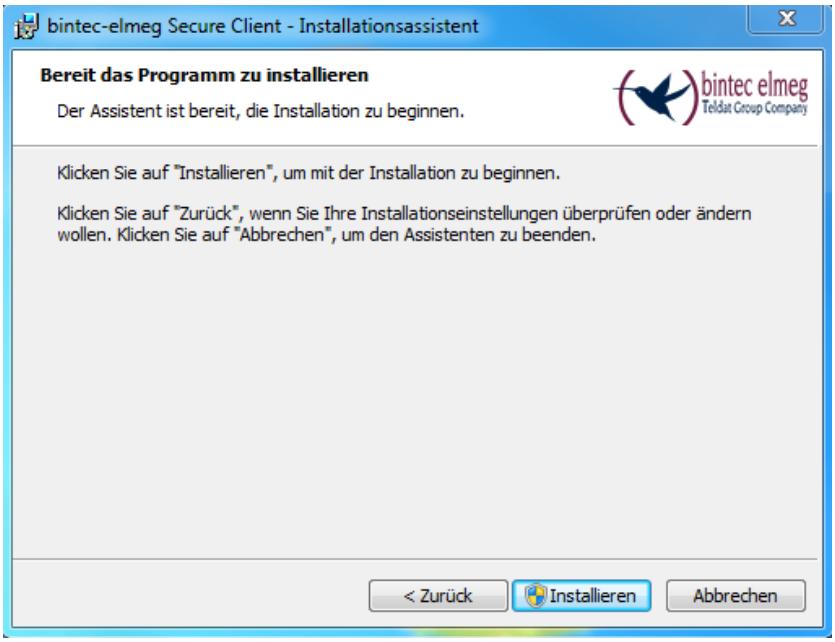


Wenn Sie für den bintec-elmeg Secure Client ein Icon auf dem Desktop Ihres PC anzeigen lassen wollen, aktivieren Sie *Programm-Icon auf dem Desktop anzeigen* und klicken Sie auf **Weiter**.

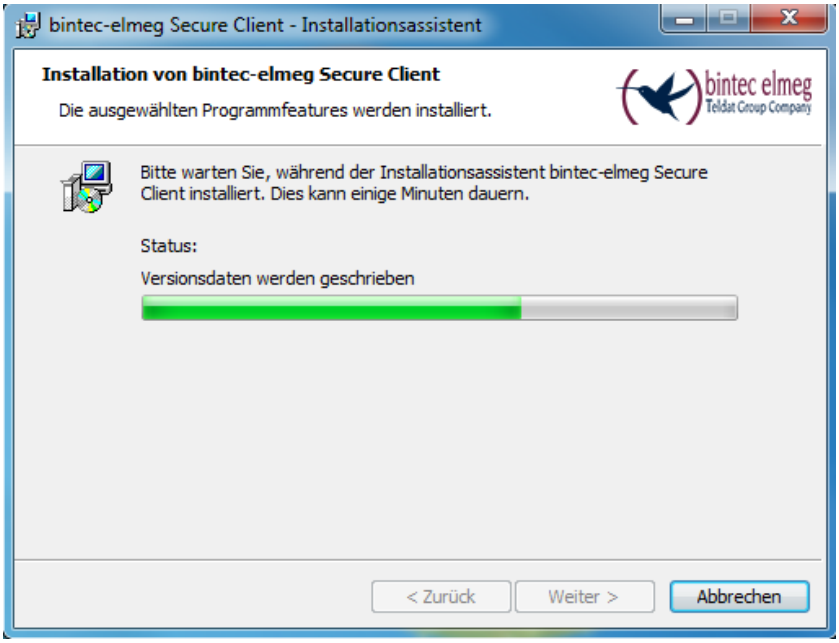


Die Vorbereitungen für die Installation sind abgeschlossen.

Klicken Sie auf **Installieren**.

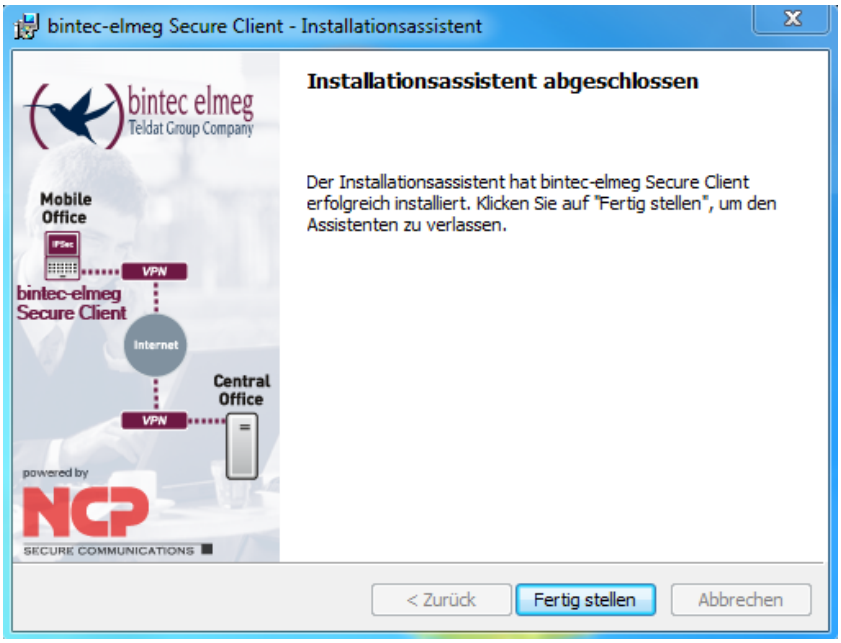


Der bintec-elmeg Secure Client wird installiert.

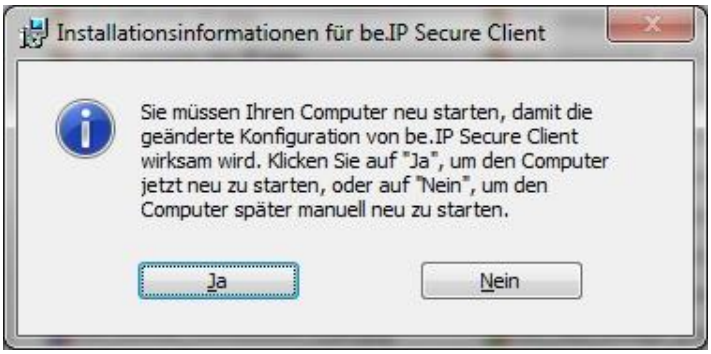


Damit ist die Installation der Client Software abgeschlossen.

Klicken Sie auf **Fertig stellen**.



Die neuen Einstellungen werden erst wirksam, wenn Sie den Computer neu starten. Klicken Sie auf **Ja**, um Ihren PC neu zu starten.



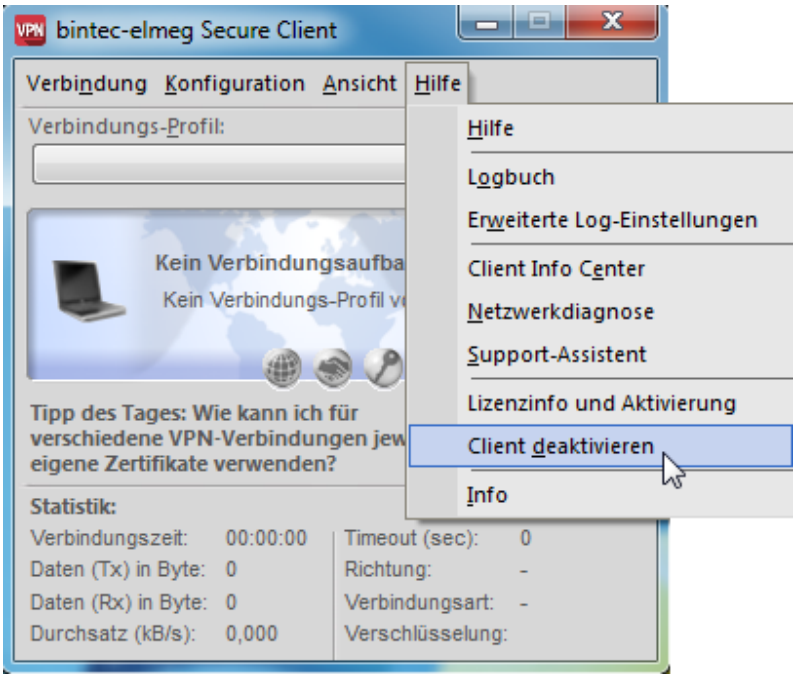
Nachdem Sie die Software installiert haben und zum Abschluss der Installation den PC neu gestartet haben, wird der Client Monitor automatisch nach dem Booten geladen.

5. Migration auf einen neuen Rechner

Falls Sie einen Rechner, auf dem ein aktivierter IPSec Client läuft, austauschen müssen empfiehlt es sich den IPSec Client vorher auf den alten Rechner zu deaktivieren.

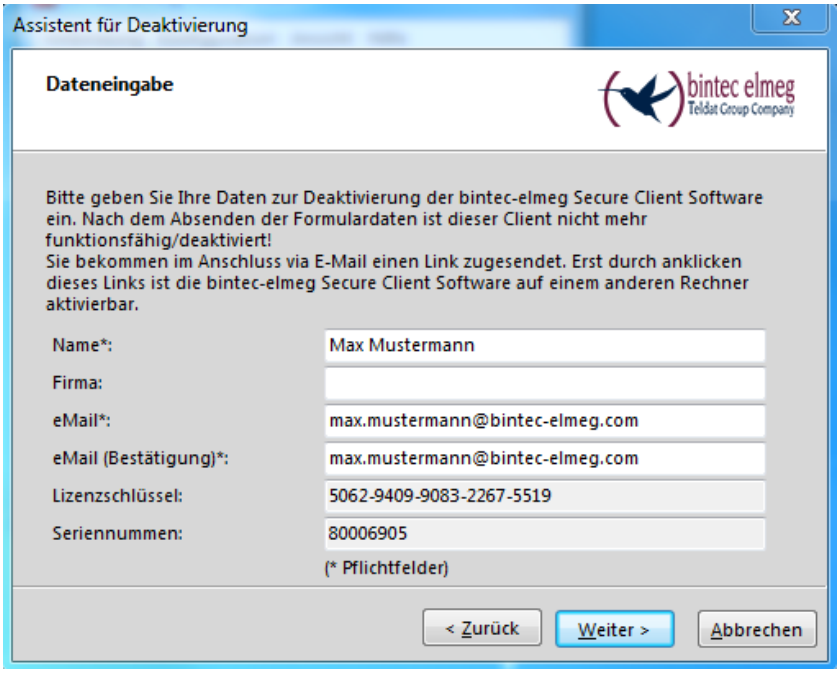
Dadurch wird der Aktivierungszähler in der Online-Aktivierungs-Datenbank zurückgesetzt und damit eine erneute Installation erlaubt.

Starten Sie den IPSec Client und gehen Sie in das Menü **Hilfe -> Client deaktivieren**.



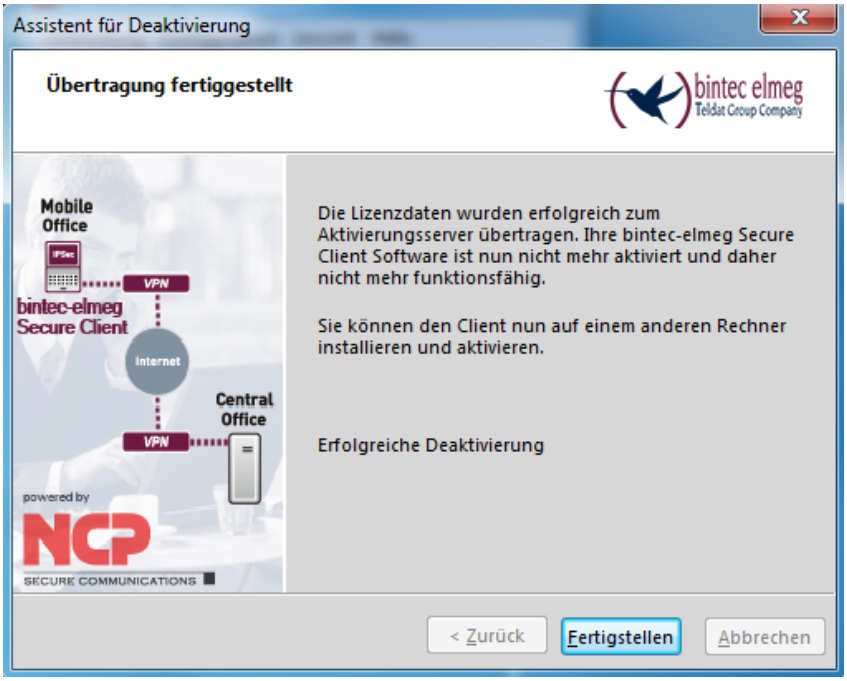
Auf der Startseite des Assistenten klicken Sie auf **Weiter**.

Geben Sie Ihren Namen und eine gültige E-Mail-Adresse ein. Lizenzschlüssel und die Seriennummer werden automatisch eingetragen. Klicken Sie auf **Weiter**.

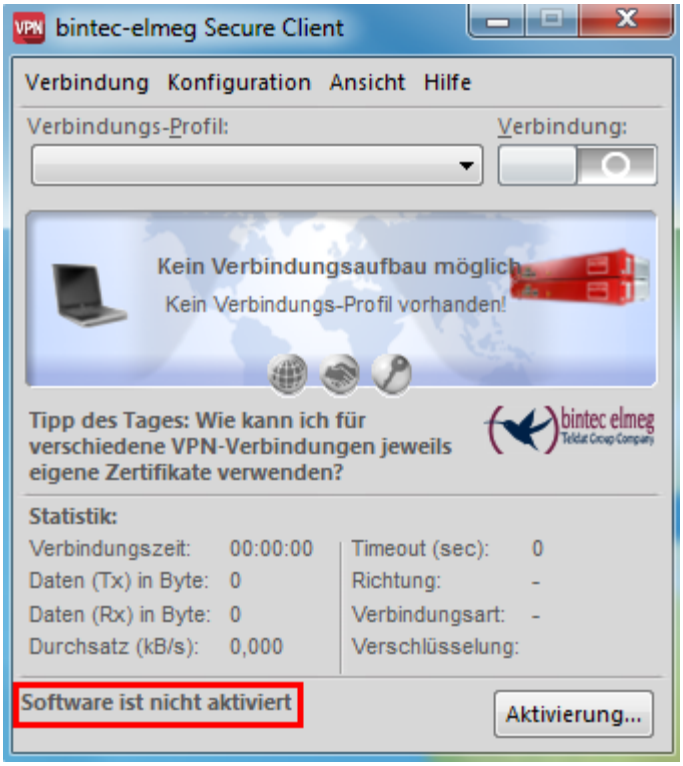


Daten werden zum Aktivierungsserver übertragen.

Nachdem die Deaktivierung durchgelaufen ist erhalten Sie eine Meldung durch das Programm, ob der Vorgang geklappt hat. Klicken Sie auf **Fertigstellen**.



Ob die Deaktivierung erfolgreich war sehen Sie auch im IPSec Client an der Meldung: **Software ist nicht aktiviert**.



Anschließend bekommen Sie eine E-Mail mit dem Bestätigungslink. Klicken Sie auf dem Link um den Vorgang abzuschließen.

Nachdem Sie den Link in der E-Mail bestätigt haben, erhalten Sie eine weitere Rückmeldung von Ihrem Browser.

Nun können Sie den IPSec Client auf den neuen Rechner installieren (wie im Kapitel **Standard Installation** beschrieben).

6. Update

Auf der Website von bintec elmeg GmbH werden Sie ständig über Updates zu Ihrem Produkt auf dem Laufenden gehalten.

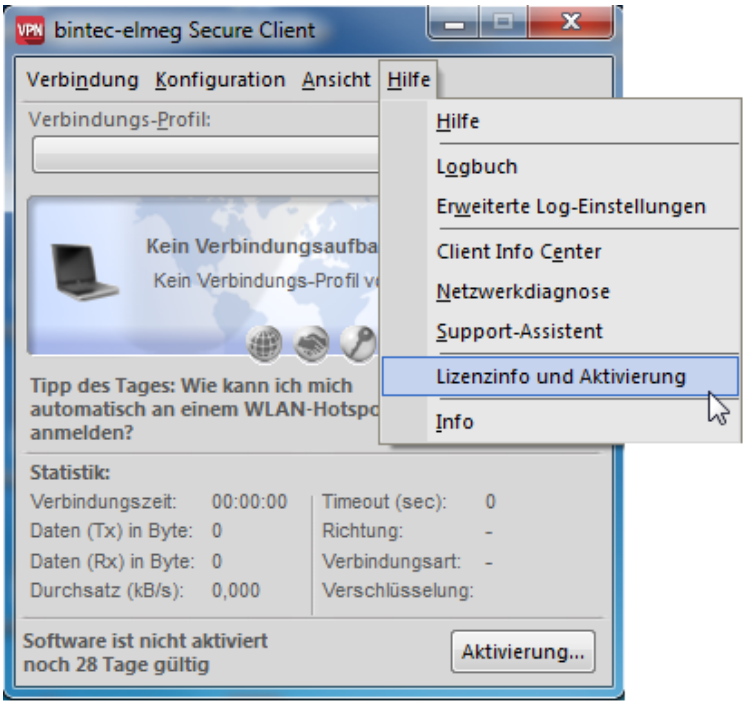
Das Software-Update ist immer dann kostenfrei, wenn es sich bei der neueren Version um ein Service Release handelt, das unter anderem Bugfixes, eine Erweiterung der Hardware-Unterstützung und Kompatibilitätserweiterungen enthalten kann. Diese Software können Sie jederzeit von der Website runterladen.

Wenn ein Update notwendig ist, gehen Sie bitte wie bei **Migration auf einen neuen Rechner** beschrieben vor.

7. Hinweise zur Online-Aktivierung

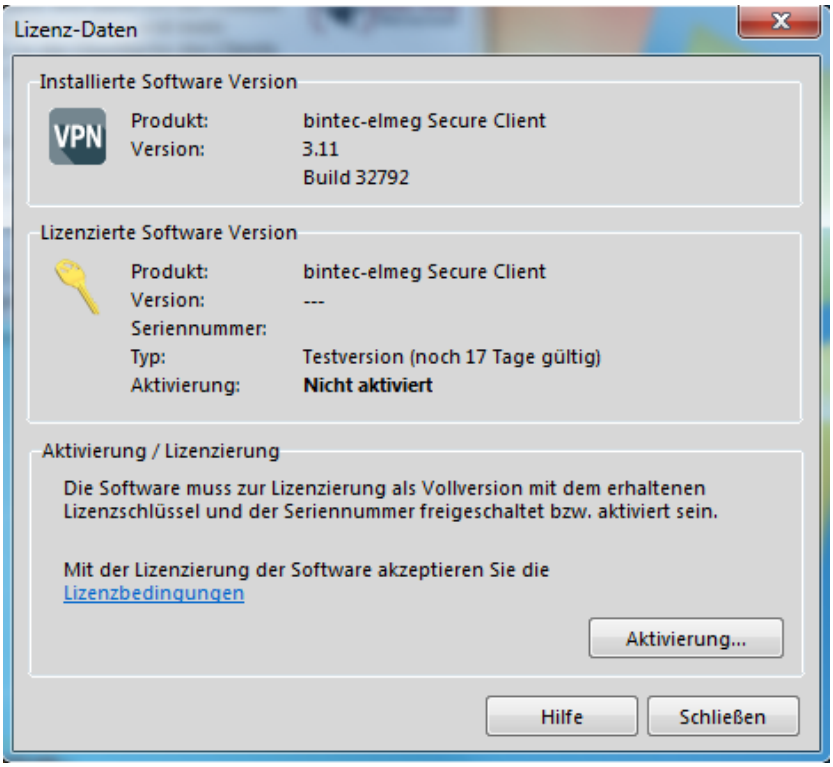
Bei der Online-Aktivierung werden die Lizenzdaten über eine Internetverbindung zum Aktivierungs-Server übertragen. Soll die Internetverbindung nicht über den IPSec Client hergestellt werden, so muss die Verbindung zunächst hergestellt werden.

Starten Sie den Aktivierungs-Assistenten über das Menü **Hilfe -> Lizenzinfo und Aktivierung**.



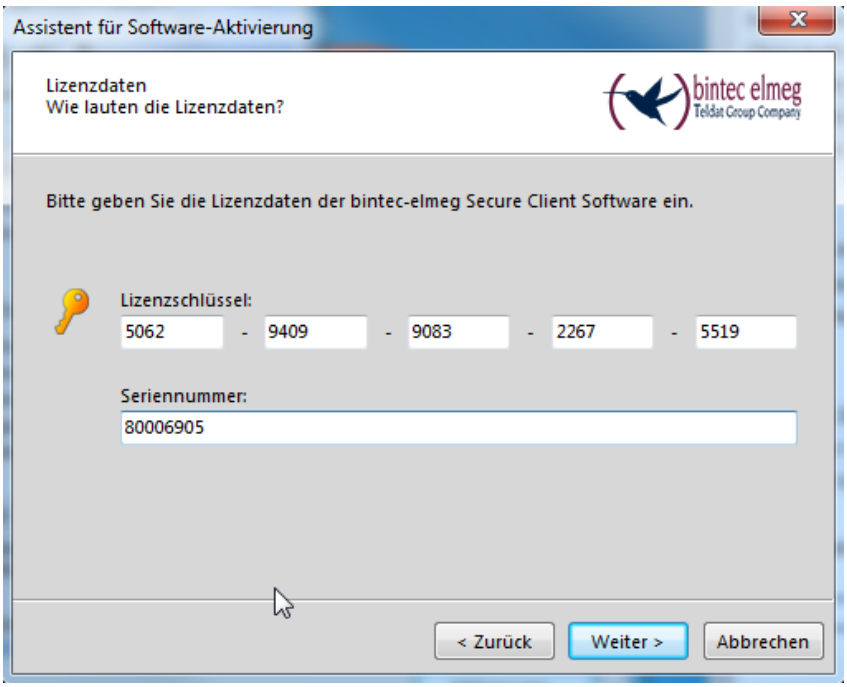
Wurde die Software lizenziert, so wird die Seriennummer angezeigt, darunter die Software-Version einschließlich der Build-Nummer, sowie die Versionsnummer der lizenzierten Version. Zum Beispiel kann eine höhere Software-Version mit älteren Seriennummer und Aktivierungsschlüssel, sprich für eine niedrigere Version, lizenziert worden sein.

Klicken Sie auf **Aktivierung…** um die Software zur Lizenzierung freizuschalten.

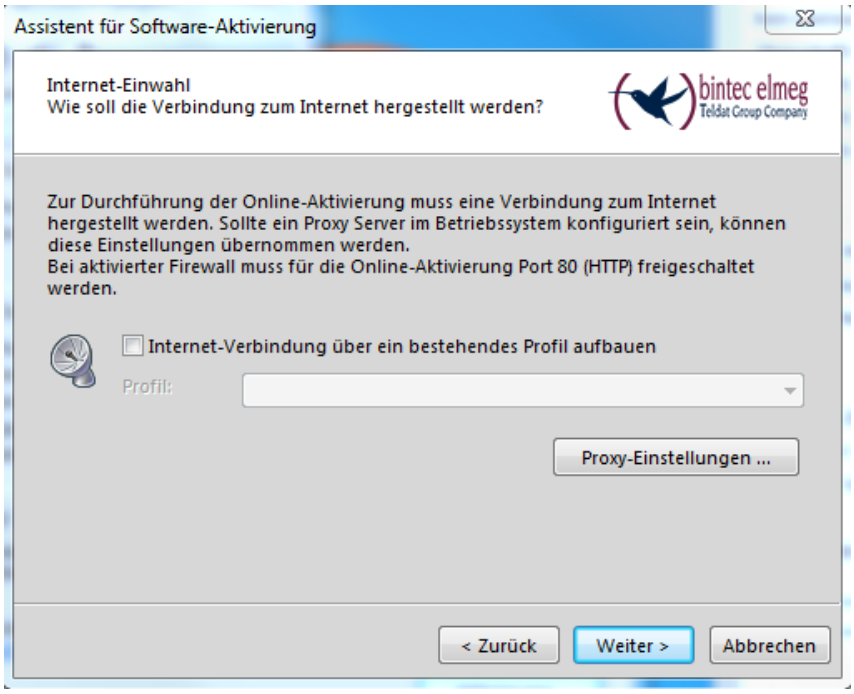


Wählen Sie in dem Assistenten für Software-Aktivierung die Aktivierungsart **Online-Aktivierung** aus. Klicken Sie auf **Weiter**.

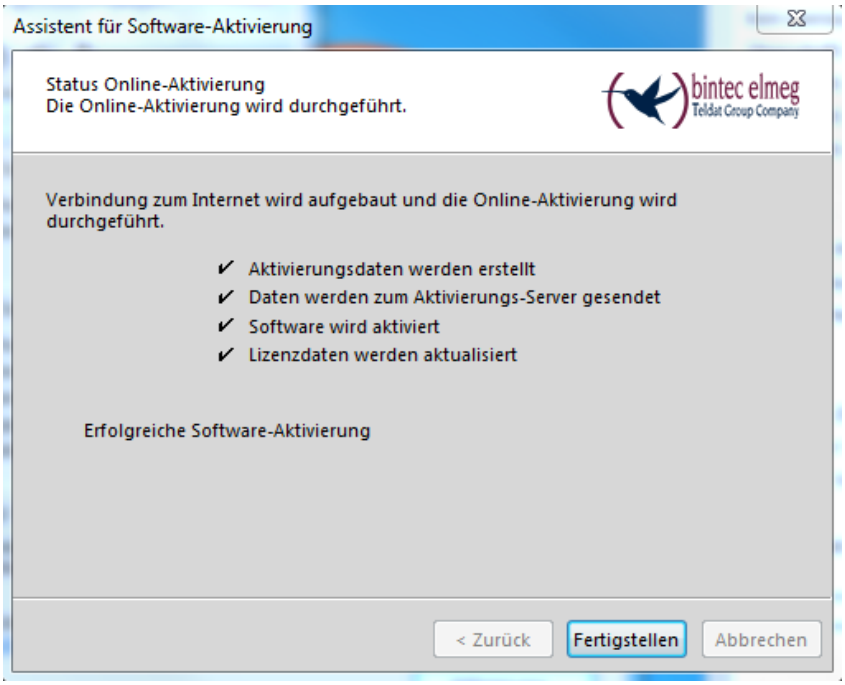
Nun geben Sie Ihre **Lizenzschlüssel** und die **Seriennummer** ein und bestätigen Sie mit **Weiter**.



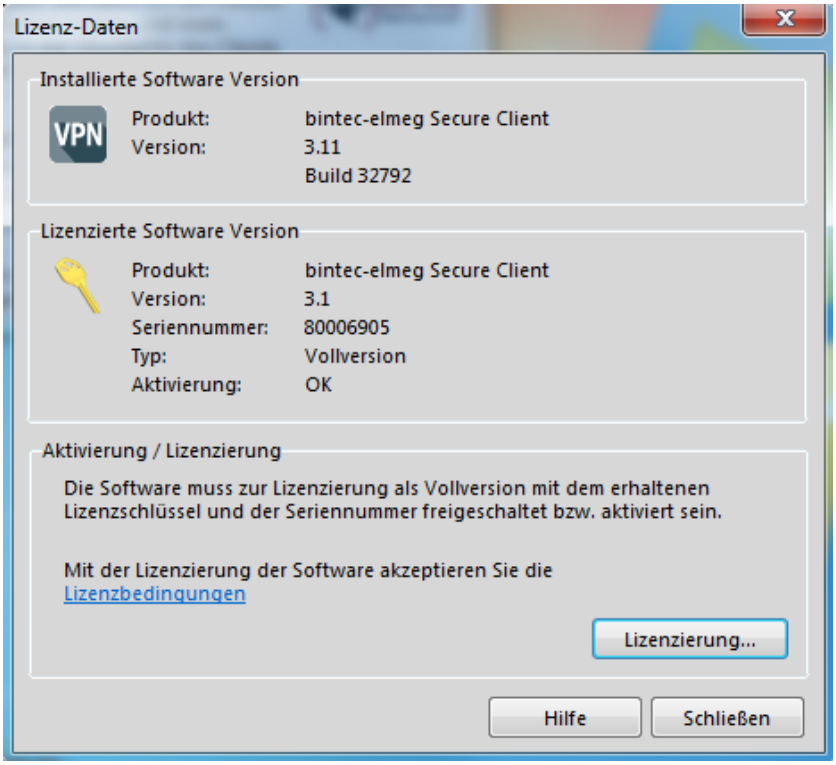
Für die Software-Aktivierung benötigen Sie eine aktive Internetverbindung. Klicken Sie auf **Weiter**.



Die Online-Aktivierung der Software wird durchgeführt. Wenn die Software erfolgreich aktiviert ist, klicken Sie auf **Fertigstellen**.



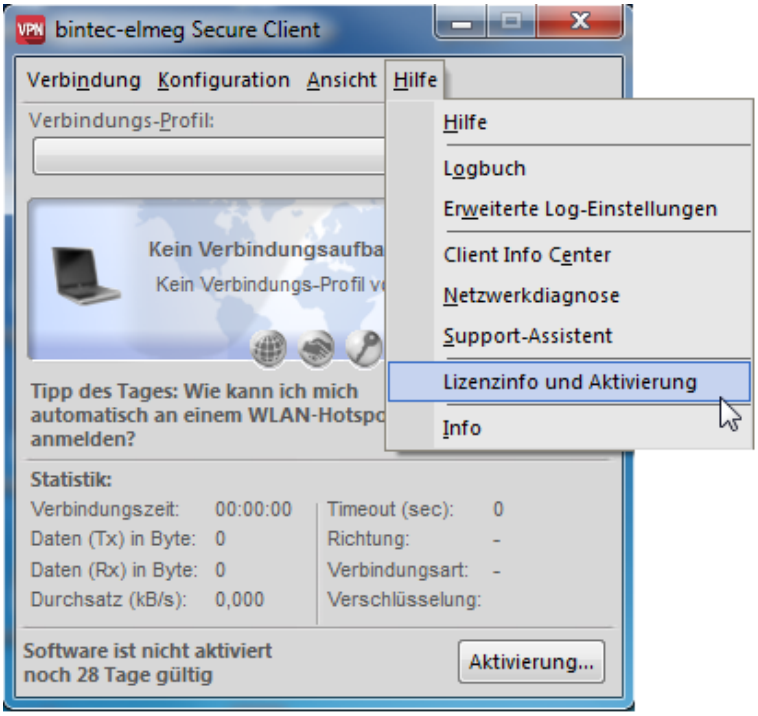
Die Software wurde erfolgreich aktiviert.



8. Hinweise zur Offline-Aktivierung

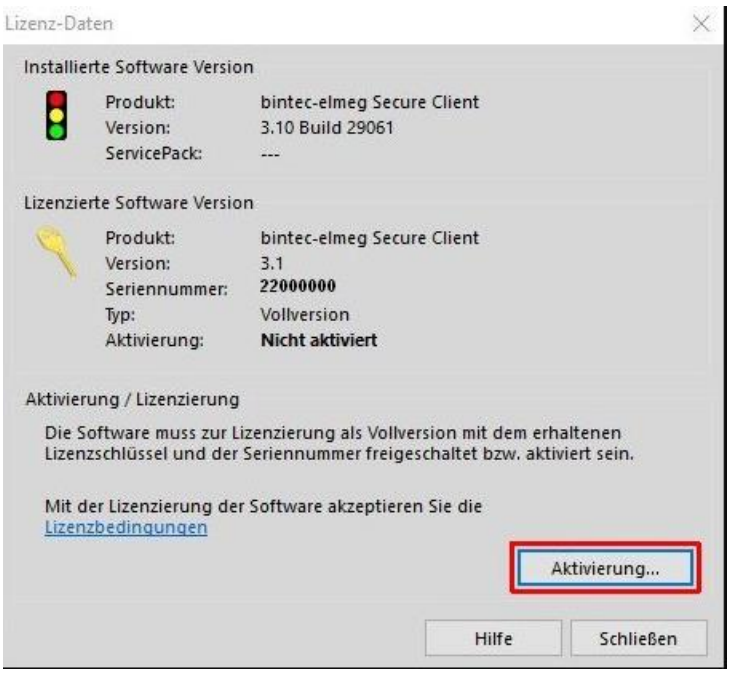
Wenn eine Online-Aktivierung nicht durchgeführt werden kann (z. B. bei eingeschränktem Netzwerkverkehr), können Sie den Client auch per Offline-Aktivierung freischalten.

Starten Sie den Assistenten über das Menü **Hilfe -> Lizenzinfo und Aktivierung.**

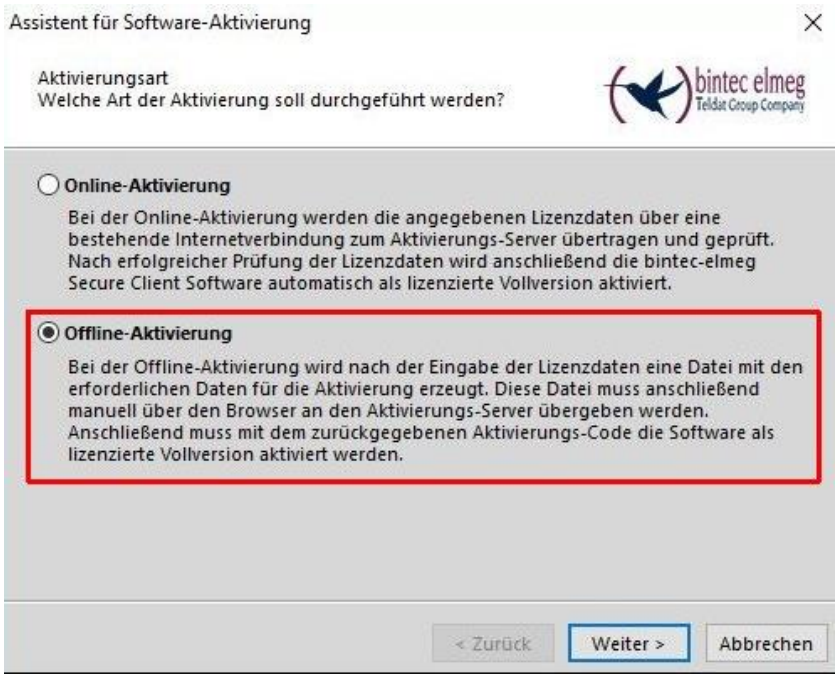


Wurde die Software lizenziert, so wird die Seriennummer angezeigt, darunter die Software-Version einschließlich der Build-Nummer, sowie die Versionsnummer der lizenzierten Version. Zum Beispiel kann eine höhere Software-Version mit älteren Seriennummer und Aktivierungsschlüssel, sprich für eine niedrigere Version, lizenziert worden sein.

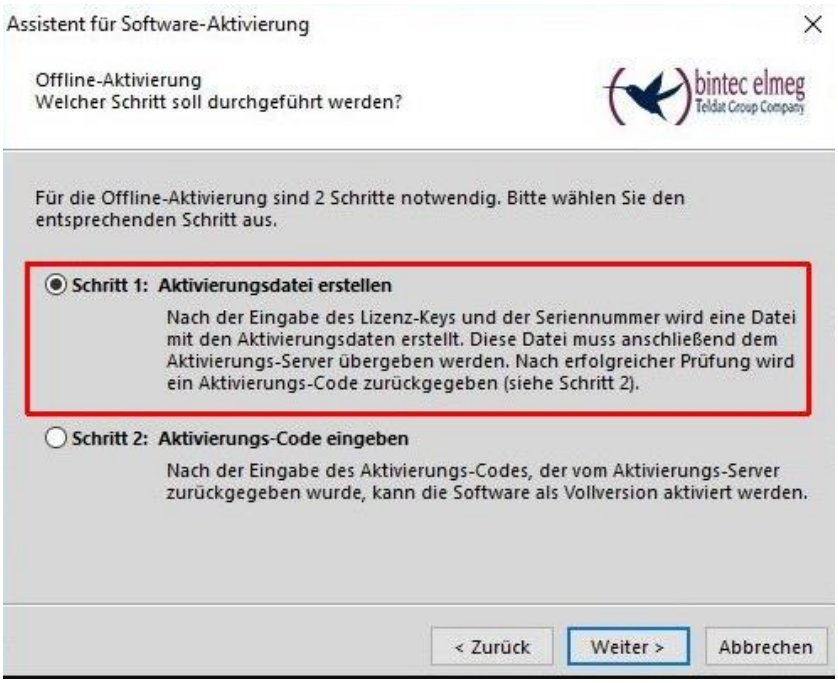
Klicken Sie auf **Aktivierung…** um die Software zur Lizenzierung freizuschalten.



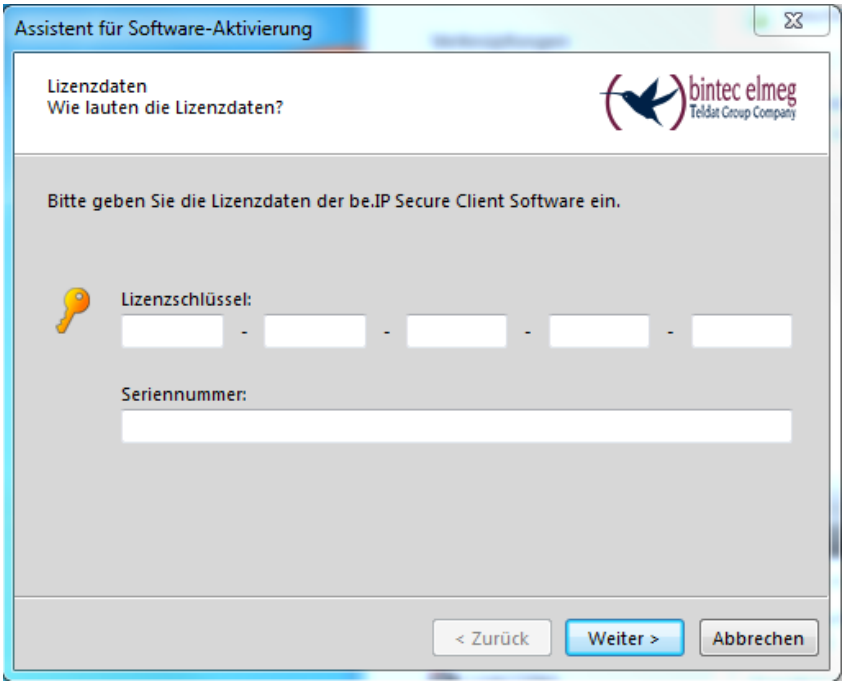
Wählen Sie in dem Assistenten für Software-Aktivierung die Aktivierungsart **Offline-Aktivierung** aus. Klicken Sie auf **Weiter**.



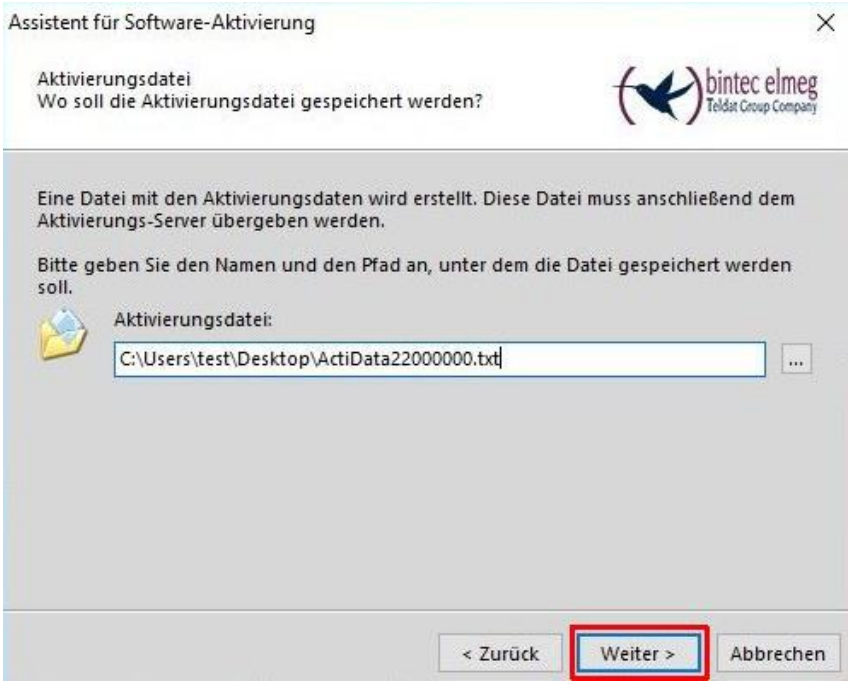
Im nächsten Schritt wählen Sie **Schritt 1: Aktivierungsdatei erstellen** aus. Klicken Sie auf **Weiter**.



Nun geben Sie Ihre **Lizenzschlüssel** und die **Seriennummer** ein und bestätigen Sie mit **Weiter**.



Es werden Ihnen vom System automatisch ein **Name** und ein **Ort** für die Aktivierungsdatei vorgeschlagen. Bestätigen Sie mit **Weiter**.

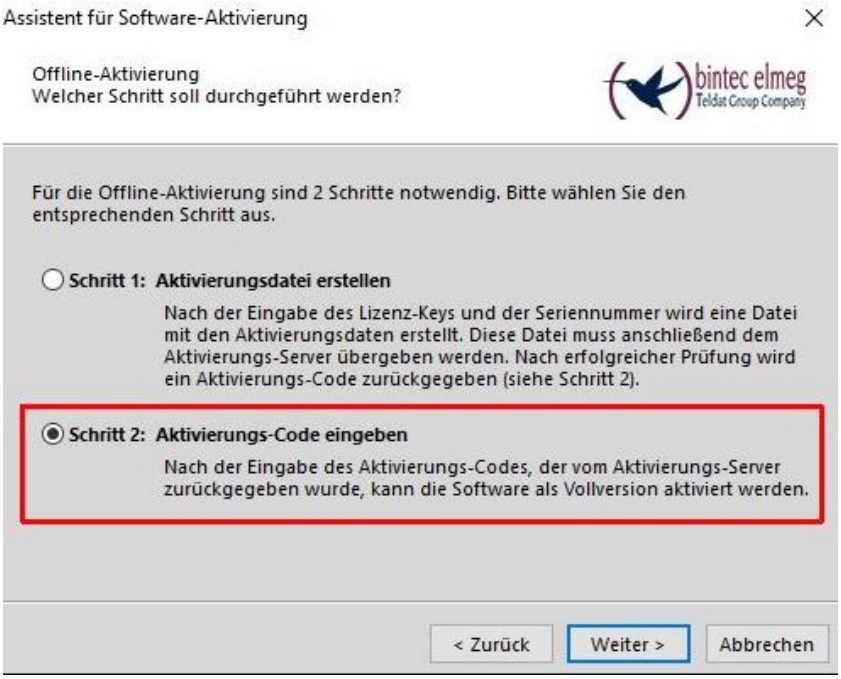


Nachdem die Aktivierungsdatei erstellt wurde, gehen Sie im Browser auf unsere Webseite zum Formular **Secure IPSec Client Software Aktivierung**. Wählen Sie dort entweder die eben erstellte Datei über den Button **Durchsuchen** aus oder kopieren Sie den Inhalt dieser Datei ins weiße Feld. Nachdem Sie damit fertig sind bestätigen Sie dies über den Button **Request Absenden.**

Sie bekommen daraufhin eine Rückmeldung, die den Aktivierungscode enthält.

Bitte notieren Sie sich den Aktivierungscode da dieser im weiteren Verlauf benötigt wird!

Gehen Sie wieder in den Aktivierungsassistenten. Wählen Sie **Schritt2: Aktivierungs-Code eingeben** aus.



Geben Sie Ihren **Aktivierungscode** ein und bestätigen Sie mit **Weiter**.

Sie sollten jetzt vom System eine Rückmeldung erhalten, dass die Aktivierung erfolgreich war.

Copyright

Marken

Haftung

Wie Sie uns erreichen:

Bintec elmeg GmbH
Südwestpark 94
D-90440 Nürnberg
Germany

Telefon: +49911-9673-0
Fax: +49911-688 0725
Internet: www.bintec elmeg.com