


## Zertifikatsbasierte Virtual Private Networks



## Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>2</b>
<b>2</b>	<b>Grundlagen</b>	<b>2</b>
<b>3</b>	<b>Bestandteile eines zertifikatsbasierten VPN</b>	<b>3</b>
<b>4</b>	<b>Anforderungen an ein sicheres, zertifikatsbasiertes VPN</b>	<b>4</b>
<b>5</b>	<b>Konkrete Beispiele für den Einsatz eines zertifikatesbasierten VPN</b>	<b>6</b>
<b>6</b>	<b>Kostenvergleich mit anderen Lösungen</b>	<b>8</b>
<b>7</b>	<b>Das STRUST VPN Security Package</b>	<b>10</b>
<b>8</b>	<b>Kontakt</b>	<b>12</b>

## 1 Einleitung

In der heutigen Zeit spielen Mobilität, der dezentrale Zugriff auf Informationen und Schnelligkeit im Geschäftsleben eine entscheidende Rolle. Außendienstmitarbeiter benötigen überall Zugriff auf aktuelle Kunden- und Produktinformationen. Viele Unternehmen bieten Ihren Mitarbeitern heute zudem Heimarbeitsplätze an. Auch hier müssen die Mitarbeiter Zugang zu den gleichen Systemen haben wie im Unternehmen. Ein weiteres Beispiel für die notwendige Vernetzung im Unternehmen ist die Anbindung von Filialen an die IT-Infrastruktur der Zentrale.

Viele Unternehmen setzen hierzu auch heute noch auf herkömmliche Systeme wie teure Standleitungen und Remote Access Services (RAS) mit Einwahlknoten. Ihnen ist meist das enorme Sparpotenzial eines internetbasierten Virtual Private Network (VPN) nicht bewusst. Durch Zertifikate abgesichert, bietet ein VPN mindestens den gleichen Sicherheitsstandard bei deutlich niedrigeren Kosten. Die folgenden Seiten vermitteln Ihnen einen Überblick und erklären, auf was man bei der Einführung unbedingt achten sollte.

## 2 Grundlagen

### Was ist ein zertifikatsbasiertes VPN?

Ein Virtual Private Network (VPN) verbindet zwei Rechner oder Netzwerke miteinander, in dem es das Internet zur günstigen Übertragung nutzt. Durch die Verschlüsselung der Daten wird ein eigenes „privates“ Netz innerhalb des Internets aufgebaut. Die Übertragung erfolgt wie in einem abgeschlossenen „Tunnel“, d.h. die Daten können von Unberechtigten nicht gelesen werden. Ein zertifikatsbasiertes VPN benutzt Personenzertifikate, auch Clientzertifikate genannt, zur Anmeldung und eindeutigen Authentifizierung am VPN und am Unternehmensnetzwerk. Durch die eingesetzten Zertifikate wird die Ende-zu-Ende-Absicherung der Datenübertragung von Rechner zu Rechner gewährleistet.

### Wie wird die Sicherheit in einem zertifikatsbasierten VPN gewährleistet?

Die Nutzer sowie die VPN-Gateways werden mit einem Zertifikat ausgestattet, das sie eindeutig identifiziert. Nur mit Hilfe eines gültigen Zertifikats können sie sich am VPN und am Unternehmensnetzwerk anmelden. Die Ende-zu-Ende-Sicherheit wird gewährleistet.

Die Datenübertragung innerhalb des VPN erfolgt verschlüsselt. Wir empfehlen, hierzu das am weitesten verbreitete Internet-Verschlüsselungs-Protokoll IPSec (IP Security Protocol) zu verwenden. Dieses verschlüsselt nach der derzeit als nicht knackbar geltenden 3-DES-Methode dreifach mit drei verschiedenen 56-Bit-Schlüsseln.

### Wo liegen die Vorteile gegenüber dem RAS-System bzw. der Standleitung?

In den 90er Jahren wurden zahlreiche Remote Access Services (RAS) Einwahlknoten installiert. Ein solches System erlaubt es Nutzern, sich über ein analoges Modem oder eine ISDN-Verbindung von außerhalb in ein Netzwerk einzuwählen und eine zeitweilige Verbindung aufzubauen. Die Administration dieser komplexen Lösung ist jedoch sehr aufwändig, die Wartung entsprechend teuer. Zudem fallen hohe, entfernungsabhängige Verbindungsgebühren an. Die Einwahl in ein VPN erfolgt hingegen über das Internet und ist daher viel günstiger. Durch den Einsatz von Zertifikaten ist eine VPN-Lösung zudem sehr sicher.

### **3 Bestandteile eines zertifikatsbasierten VPN**

Zum Aufbau eines sicheren VPN werden folgende Komponenten benötigt:

#### Hardware

- **VPN-Gateway, auch VPN-Router genannt**
- **VPN-Konzentrator bzw. VPN-Switch**

#### Software

- **Management-Software für VPN-Gateway**
- **Stateful Firewall für VPN-Switches**  
Diese verfolgt den Zustand der VPN-Verbindungen mit und kann die übermittelten Datenpakete daher im Kontext beurteilen. So verhindert sie das Eindringen von Viren, etc.
- **VPN-Client-Software**  
Software zur Herstellung der VPN-Verbindung für die Laptops bzw. PC der Nutzer
- **Personal Firewall für Clients**  
Firewall-Software für die Laptops bzw. PC der Nutzer

#### Zertifikate

- **Personenzertifikate**  
Zur höheren Sicherheit können diese softwarebasierten Zertifikate auch auf einer Smart Card oder einem speziellen USB-Stick gespeichert werden.
- **Administrations-Tool zur Ausgabe und Verwaltung der Zertifikate**

#### 4 Anforderungen an ein sicheres, zertifikatsbasiertes VPN

Grundsätzlich wird im VPN eine Ende-zu-Ende-Beziehung betrachtet, d.h. die Daten werden durchgängig während der gesamten Übertragung verschlüsselt. Sie ist gemäß der Abbildung 1 aufgebaut.

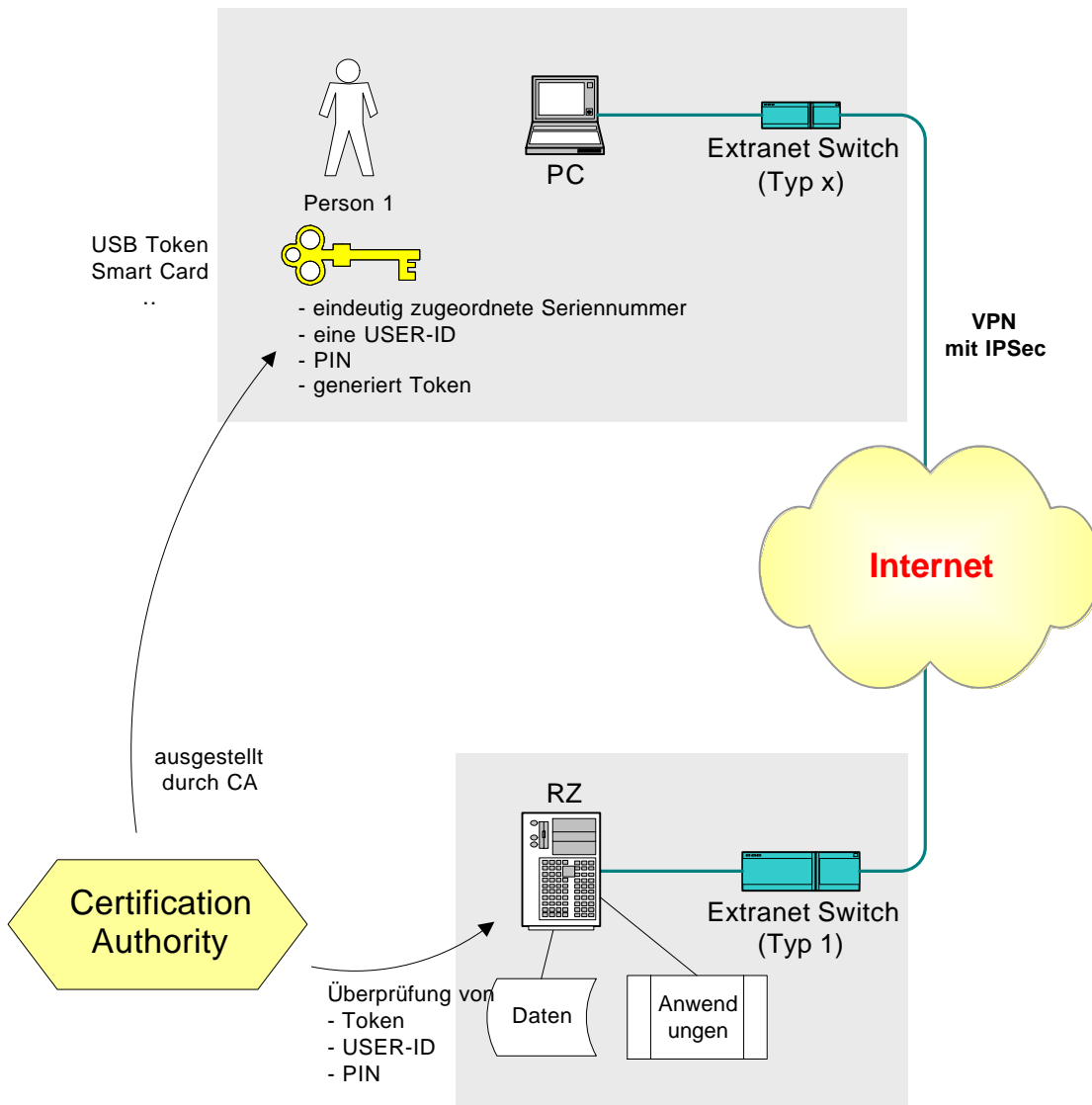


Abbildung 1: Ende-zu-Ende-Beziehung im VPN

Folgende Anforderungen müssen erfüllt sein:

### **Authentifizierung**

Der Nutzer sowie die technischen Bestandteile eines VPN müssen eindeutig identifiziert und ihre Zugangsberechtigung zu VPN und Unternehmensnetzwerk bewiesen werden können.

### **Vertraulichkeit**

Die Internetkommunikation und -transaktion sensibler Inhalte, wie z.B. die Bilanzdaten müssen vertraulich ablaufen.

### **Datenintegrität**

Die Kommunikation muss vor dem unbefugten Eingriff Dritter während der Übertragung über das Internet geschützt werden.

Für ein günstiges und sicheres VPN im Internet sollte daher Folgendes beachtet werden:

**A1:** Nutzung der kostengünstigsten Verbindungsmöglichkeit

- mit der höchstmöglichen Bandbreite
- möglichst als „Flat Rate“
- und der höchsten Verfügbarkeit

**A2:** sichere Datenübertragungsstrecke vom Anwender bis zur Applikation mit

**A3:** verschlüsselter Information auf der Datenübertragungsstrecke und

**A4:** Authentifizierung des Anwenders mittels Zertifikat an seinem PC und

**A5:** Authentifizierung an den VPN- Endpunkten zur Vermeidung eines Man-in-the-middle-Angriffs.

**A6:** Umsetzung der Quality of Service Anforderungen im VPN  
(d.h. Bandbreitensicherung, Jitter, usw.)

## 5 Konkrete Beispiele für den Einsatz eines zertifikatesbasierten VPN

### Fall 1: Heimarbeitsplätze (Home Office) oder mobiler Arbeitsplatz

Diese modernen, oft genutzten Arbeitsformen setzen am Heimarbeitsplatz des Mitarbeiters oder am Laptop des Außendienstmitarbeiters lediglich einen Zugang zum Internet über ein 56 Kbit/s Modem, eine ISDN- oder xDSL-Verbindung voraus. Nach erfolgreicher Authentifizierung mit einem Personenzertifikat wird vom Client, d.h. dem Rechner des Endanwenders, bis zum Extranet Switch, d.h. dem VPN-Gateway, in der Zentrale ein sicherer Tunnel aufgebaut. Dieser Tunnel ist logisch wie eine Punkt-zu-Punkt-Verbindung zu sehen. So ist es möglich, weltweit den Mitarbeitern kostengünstig einen sicheren Zugang zu Ihrer Zentrale anzubieten.

Ist das Personenzertifikat hingegen manipuliert (gefälscht, abgelaufen oder gesperrt) wird nicht nur der Zugang zum Endgerät, sondern auch zum Unternehmensnetzwerk (LAN) verweigert.

Diesen Fall verdeutlicht die nachfolgende Abbildung 2.

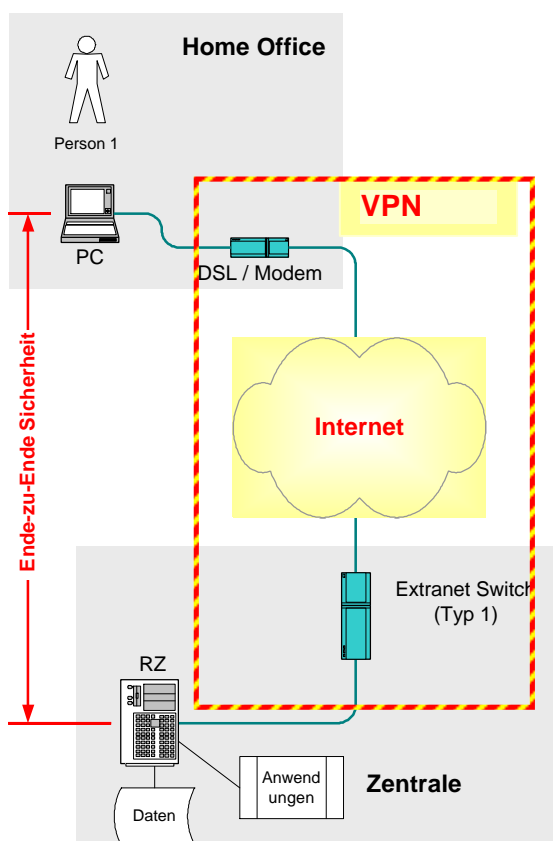


Abbildung 2: Anbindung eines Heim- bzw. mobilen Arbeitsplatzes

## Fall 2: Anbindung von Außenstellen und Filialen

Mit nur kleinen Anpassungen des Szenarios aus dem Fall 1 lässt sich die Außenstellen-Anbindung darstellen. Der wesentliche Unterschied besteht darin, dass im Außenstellennetz nicht ein Nutzer sondern ein ganzes Netzwerk mit unterschiedlichen Nutzern betrachtet werden muss. Das bedeutet, der Zugang zum Internet erfolgt hier für ein Netzwerk und nicht für einen einzelnen Client, bzw. Rechner.

Weiterhin sind drei unterschiedliche Sicherheitsbetrachtungen durchzuführen:

- die Sicherheit des VPN-Tunnels selbst (Schutz vor Man-in-the-middle-Attacken)
- die eindeutige Authentifizierung des Mitarbeiters am Endgerät (PC oder Laptop) im Außenstellen-Netzwerk
- die Ende-zu-Ende-Absicherung zur Vermeidung interner Sicherheitslücken

Damit erfolgt eine Authentisierung des VPN-Tunnels und eine Authentisierung des Mitarbeiters im Netzwerk selbst. Die Abbildung 3 zeigt diesen Fall.

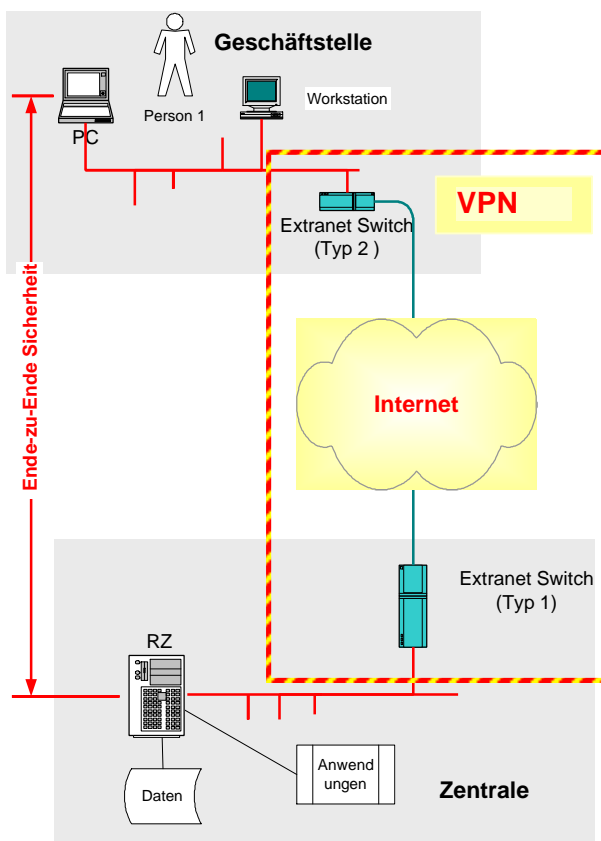


Abbildung 3: Anbindung einer Geschäftsstelle

## 6 Kostenvergleich mit anderen Lösungen

### Remote Access Service (RAS)

Für eine RAS-Lösung werden so gut wie keine separaten Hardware- und Softwarekomponenten benötigt. Vom Investitionsansatz gesehen, ist diese Alternative daher die günstigste Lösung. Wenn allerdings alle entstehenden Kosten, d.h. Investitions- und Betriebskosten, in Betracht gezogen werden, ändert sich dieses Bild dramatisch. Das folgende Beispiel vergleicht die Gesamtkosten für die Anbindung von Heimarbeitsplätzen ans Unternehmen.

Die Prämissen sind:

#### Alternative RAS

- 150 Home Arbeitsplätze, davon 50 mit analogem Modem und 100 mit ISDN
- Zentrale mit 30 analogen und 60 ISDN gleichzeitig zu betreibenden Kanälen (ist bereits eine Einschränkung bei 150 Usern)
- Einwählzeit 2 Stunden pro Tag bei 20 Tagen / Monat

#### Alternative zertifikatsbasiertes VPN

Grundsätzlicher Einsatz von DSL bei 150 Home Arbeitsplätze mit „Flat Rate“ und Zertifikaten auf USB-Token.

Die nachfolgende Tabelle 1 zeigt den Kostenvergleich von RAS und zertifikatsbasiertem VPN auf Basis der oben genannten Prämissen. Hierbei wird deutlich, dass selbst bei unfairen Basisprämissen, wie z.B. 2 Stunden Verbindungszeit pro Tag, bei RAS gegen DSL mit Flat Rate eine deutliche Kostensenkung im ersten Jahr und in den Folgejahren erzielt werden kann.

	RAS		VPN	
	1. Jahr	Folgejahre	1. Jahr	Folgejahre
Grundgebühren	21.931,20 €	21.931,20 €	81.492,00 €	81.492,00 €
Verbindungsgebühren	318.715,20 €	318.715,20 €		
Zertifikate			6.525,00 €	6.525,00 €
RAS Hardware (Router)	18.246,76 €	180,66 €		
VPN-Hardware (Switch/Router/Firewall..)			86.572,50 €	7.941,50 €
	<b>358.893,16 €</b>	<b>340.827,06 €</b>	<b>174.589,50 €</b>	<b>95.958,50 €</b>
Differenz im 1. Jahr und Differenz in den Folgejahren	<b>184.303,66 €</b>	<b>244.868,56 €</b>		

**Insgesamt nach 5 Jahren 1.163.777,91 €**

Tabelle 1: Kostenvergleich RAS- und VPN-Lösung

Wenn die für das VPN eingeführten Zertifikate auch für andere Anwendungen genutzt werden, ergeben sich weitere Optimierungsmöglichkeiten und damit Einsparungen.

## Secure-ID versus Zertifikate

Eine Secure-ID ist ein Hardware-Token, das simultan mit dem Server einen Passcode errechnet, der für eine gewisse Zeitspanne gültig ist. Dieser wird bei der Anmeldung an der RAS- oder VPN-Lösung zur Authentifizierung eingesetzt. Im Folgenden werden die Kosten für die Authentifizierungs-Komponenten Zertifikate und Secure-ID verglichen.

Die Leistungsmerkmale auf den Clients für beide Lösungen sind:

- **VPN-Security Package**
  - Personal Firewall auf jedem Endgerät zzgl. Virens scanner
  - das Zertifikat liegt auf einem USB-Token oder Smart Card
  - zusätzliche Bildschirmschonerfunktion und Festplattenverschlüsselung
- **RSA Secure-ID**
  - alle 60 Sekunden erfolgt eine Passcode-Änderung
  - Basis ist ein Hardware-Token

Die folgenden Tabelle zeigt die preislichen Unterschiede, wobei bei der Secure-ID-Lösung lediglich die Standardkonfiguration ohne zusätzliche Features betrachtet worden ist. Im Preisvergleich wurde das Zertifikat sowie der Zertifikatsträger bzw. der Secure-ID-Hardware-Token und der Server zzgl. Codierungssystematik berücksichtigt.

	Zertifikate	Secure-ID
<b>Investitionskosten</b>	15.514,50 €	52.098 €
<b>Folgekosten/Jahr</b>	6.844,50 €	14.830 €

Tabelle 2: Kostenvergleich Zertifikate und Secure-ID

Auch hierbei ist zu berücksichtigen, dass die Zertifikate im Gegensatz zu der Secure-ID auch für viele weitere Anwendungen, wie z.B. E-Mail-Verschlüsselung oder Single-Sign-On, genutzt werden können. In diesem Fall verteilen sich die Investitionskosten für die Zertifikate entsprechend.

## 7 Das **STRUST** VPN Security Package

Zur einfachen Handhabung bieten wir Ihnen eine Komplettlösung für ein sicheres, zertifikatsbasiertes VPN an. Das **STRUST** VPN Security Package erfüllt alle Voraussetzungen aus den bereits oben aufgeführten Forderungen:

- Es baut durch Verschlüsselung ein über die ganze Übertragungsstrecke gesichertes VPN im Internet auf.
- Zugangsvoraussetzung ist die jeweilige Authentifizierung an den beiden Endpunkten eines VPN.
- Es nutzt das Internet als kostengünstigste Verbindungsform.

### Bestandteile

Grundsätzlich wird das Paket mit Soft- und Hardware-Komponenten verschiedener namhafter Hersteller nach den individuellen Wünschen des Kunden zusammengestellt. Hierdurch kann die VPN-Lösung optimal in ein vorhandenes, kundenspezifisches Netzwerk eingebaut werden. Das reibungslose Zusammenspiel der angebotenen Komponenten mit den ebenfalls im Paket enthaltenen Zertifikaten wurde bereits nachgewiesen. Das Besondere am **STRUST** VPN Security Package ist, dass das Komplettangebot die Installation vor Ort einschließt.

### Hardware:

- VPN-Gateways
- VPN-Konzentrator

### Software:

- Management-Software für VPN-Gateway
- Stateful Firewall für VPN-Switches
- VPN-Client-Software
- Personal Firewall zur Sicherung des VPN-Clients

### Zertifikate:

- Softwarebasierte Personenzertifikate, auf Wunsch auf Chipkarte oder speziellem USB-Token
- Administrationstool zur einfachen Verwaltung der Zertifikate

## Ihre Vorteile im Überblick

Profitieren Sie mit dem **STRUST** VPN Security Package von allen Vorteilen zertifikatsbasierter VPN wie z.B.:

- den günstigen Verbindungskosten durch die Nutzung des Internets
- der durchgängigen Ende-zu-Ende-Absicherung
- der einfachen Authentifizierung durch Zertifikate
- den weiteren Einsatzmöglichkeiten der für das VPN ausgegebenen Zertifikate ohne Mehrkosten für
  - **digitale Signatur**
  - **verschlüsselte E-Mail-Kommunikation**
  - **Web Access** - Legitimation für einen geschützten Bereich eines Online-Portals
  - **Secure Log-On** - Zugriffssperrung des Computers bzw. Laptops (Boot-Schutz)
  - **Festplattenverschlüsselung**
  - **Single-Sign-On** - einmalige Anmeldung verschafft Zugriff auf alle Daten und Anwendungen
  - u.v.m.

Das Komplettangebot bietet Ihnen zudem folgende Pluspunkte:

- Das Paket kann aus verschiedenen Komponenten führender Hersteller individuell zusammengestellt werden
- Alle Komponenten wurden im Vorfeld auf Ihre Kompatibilität getestet
- Auf Wunsch erhalten Sie die gesamte Projektsteuerung und Systemintegration aus einer Hand
- In Arbeitskreisen mit unseren Partnern werden die Lösungen permanent weiterentwickelt

## **8 Kontakt**

Gerne beraten wir Sie persönlich zu der Einführung eines zertifikatsbasierten VPN in Ihrem Unternehmen. Aber auch für weitere Lösungen, die Zertifikate benötigen, sind wir ein kompetenter Ansprechpartner. Sie erreichen uns

telefonisch über die kostenlose Servicenummer

**08 00 / 4 78 78 78**  
**(08 00 / 4 STRUST)**

per E-Mail an

**info@s-trust.de**

oder besuchen Sie uns im Internet unter

[www.s-trust.de](http://www.s-trust.de)