say **Yes** to IT-Security

SAY**TRUST** VPSC Zero Trust Network Access

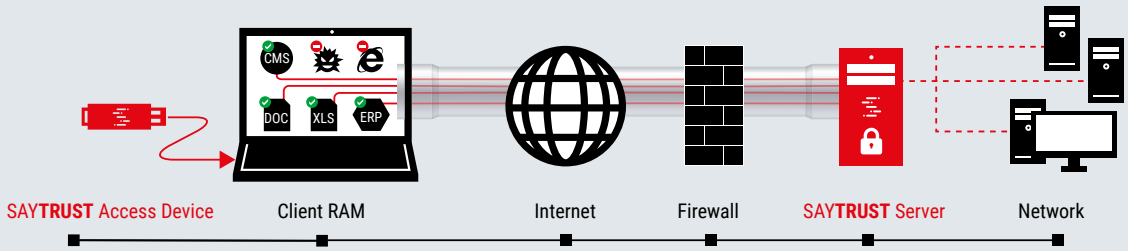
Personenschutz durch Überwachung der IT und Kommunikation nach innen und außen

SAYTEC

Personen des Öffentlichen Lebens sind Personen mit einem besonderen Bekanntheitsgrad.
Politisch aktive Personen, Schauspieler und bekannte Unternehmer gehören zu Person des öffentlichen Lebens, denen das Recht auf Privatsphäre verwehrt wird. Sie sind oft Opfer von Cyberattacken. Spionage und Erpressungen sind das Ziel.

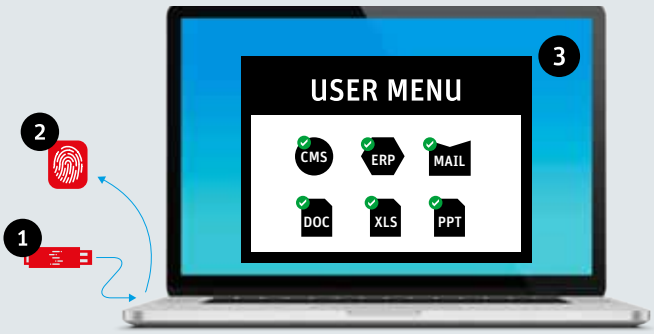
Da von diesen Personen ein öffentliches Interesse ausgeht, sind Privatsphäre und das Recht am eigenen Bild deutlich eingeschränkt. Auch sind Informationen, die diese Personen haben oder vertrauliche Daten interessant für Hacker. Sie können erpresst werden oder Ihre Entscheidungen können gezielt manipuliert werden. Entscheidungen, die weitreichende Auswirkungen haben.

Auf Grund der hohen Bekanntheit und Medienpräsenz dieser Personen, gelten Sie als besonders schutzbedürftig. Um den Schutz dieser Personen bestmöglich zu gewährleisten, werden Ihre IT-Systeme und Kommunikationsleitungen geschützt und überwacht. Durch sayTRUST VPSC Technologie können Personen des Öffentlichen Lebens hoch sicher von überall arbeiten und kommunizieren.



Besonderheiten

- Keine virtuelle Netzwerkkarte notwendig
- Keine separate Software-Installation erforderlich
- Prüfung bereits am Client - vor dem Tunnel
- Verbindung auf der Applikationsebene
- Keine Netzwerk-Netzwerkkopplung
- Kein Zugriff von außen möglich
- Keine Spuren auf Client & Verbindungsstrecke



Vorteile der SAY**TRUST** VPSC Technologie gegenüber VPN

Leichte Handhabung für Anwender

- Verbindungsaufbau von jedem beliebigen PC aus möglich
- Passwortmanager für Single Sign On (SSO)
- Automatische Aktualisierung aller Systeme

Hohe Sicherheit

- 8-stufige Sicherheit (Biometrie, PIN, mehrfach Authentifizierung, Zertifikat, personifizierte PFS, keine Backdoors, keine Herausgabe der Verschlüsselungs-Keys)
- der Kommunikationsaufbau erfolgt aus dem verschlüsselten Hauptspeicher des Endgerätes
- keine Datenreste auf Endgerät und der Verbindungsstrecke
- Verbindung auf Applikationsebene: d.h. das Endgerät erhält keine IP-Adresse vom Remotenetzwerk und hat keinerlei Informationen über den schützenden Netzwerk
- Client-PC wird nie Mitglied vom Netzwerk
- Tunnelaufbau für Applikationen aus dem verschlüsselten Arbeitsspeicher des Clients. Nicht autorisierte Anwendungen können daher keine Verbindung aufbauen
- für die Kommunikation wird im Prozessspeicher in Abhängigkeit des Client-Zertifikats nach Diffie-Hellman ein neuer, bis dahin unbekannter - dem Client + Server nicht bekannter Schlüssel generiert

Publish Applikationsplattform für Microsoft-Anwendungen ohne Citrix

Deutlich reduzierter Admin-Aufwand gegenüber traditionellen VPN Lösungen

- keine Installation einer virtuellen Netzwerkkarte auf dem Endgerät
- keine Softwareinstallation, Überwachung, Wartung und Pflege erforderlich

Perfekte Netztrennung und Isolierung von zu schützenden Anwendungen und Applikationen

- z.B. Trennung von Techniknetz vom Verwaltungsnetz
- externe Dienstleister erhalten nur zugewiesene Nutzungsrechte auf z.B. einzelne Applikationen oder Anwendungen

Geringere Betriebskosten

Sie wünschen mehr Information? Beratung unter **089 578 361 400**