SecurITy made in Germany

sayTEC

Whitepaper

sayTRUST® Access

Sichere Kommunikation für Daten, Anwendungen und abgesicherte Arbeitsumgebung mit sayTRUST Access

VERSION 1.0
2019/05

Common Criteria EAL 4+
(findet gerade statt)

2018 STEVIE GOLD WINNER GERMAN STEVIE AWARDS

SOFTSHELL VENDOR REPORT 2018 SOFTSHELL

INNOVATIV DURCH FORSCHUNG

qualityaustria SYSTEMZERTIFIZIERT ISO 9001:2015 NR.21628/22

Die zunehmende Digitalisierung durchzieht unseren Alltag. Sie bietet neue Möglichkeiten für die Gesellschaft, weist aber auch Risiken auf. Durch die Vernetzung nahezu aller Lebensbereiche erhalten wir stetig mehr Zugang zu digitalen Infrastrukturen, Dienstleistungen und Datenquellen, mit denen wir ständig interagieren. Sie erleichtern in vielen Bereichen unser Leben, z.B. bei der medizinischen Versorgung und verbessern die Nutzung erneuerbarer Energien. Damit nehmen jedoch der Datenbedarf und der Datentransfer rasant zu.

Für viele Firmen sind Daten der wesentliche Teil ihres Unternehmenswertes. Jederzeit können durch technisches Versagen, Anwenderfehler, Angriffe oder Manipulationen gespeicherte Daten verloren gehen, komplette Serversysteme zusammenbrechen oder unbrauchbar gemacht werden. Der Erhalt des Betriebes und dessen Präsenz am Markt sind davon abhängig. Aus diesem Grund müssen Netzwerke, Daten und Anwendungen gegen mögliche Angriffe geschützt werden. Doch viele Betriebe begegnen der drohenden Gefahr nicht mit der notwendigen Ernsthaftigkeit, obwohl in Deutschland die Absicherung von Daten gesetzlich vorgeschrieben ist.

Schlagzeilen über verheerende Cyberangriffe nehmen immer mehr zu. Eine Betriebsunterbrechung kann ein mittelständisches Unternehmen mehrere hunderttausend Euro am Tag kosten. Untersuchungen zeigen, dass bis zu 70 Prozent der Unternehmen nach einem Störfall oder Angriff ihre Daten nicht wiederherstellen konnten. Dabei zeigt sich, dass viele der Angriffe oder Betriebsunterbrechungen vermeidbar wären. Daher ist eine konsistente Datenschutz- und Erhaltungsstrategie unerlässlich.

Anwender, die im Home-Office an unterschiedlichen Standorten oder mobil arbeiten, müssen auf Firmendaten zugreifen können. Dazu benötigen Sie einen Fernzugriff, der nicht nur eine schnelle und stabile, sondern auch eine sichere Verbindung bereitstellen soll. Ein Großteil der Unternehmen setzt dazu eine der vielen VPN -Lösung (Virtual Private Network) ein. Anwender beklagen beim Einsatz solcher Lösungen häufig eine Reihe von Problemen. Software, die sich auf den Clients schlecht oder gar nicht integrieren lässt, umständliche Hardware oder auch quälende langsame Verbindungen sind nur einige der Herausforderungen. Sie koppeln den mobilen Arbeitsplatz mit dem zu schützenden Unternehmens-netzwerk. Die LAN-LAN Kopplung eines Clients aus einer unsicheren Umgebung in ein geschütztes Netzwerk verursacht jedoch während der Installation und auch später im Betrieb viele Schwierigkeiten.

Neue Technologien – neue Lösungen

Während bei herkömmlichen Lösungen immer ein Kompromiss eingegangen wird, hat sich die sayTEC AG bei der Entwicklung des sayTRUST® Secure Access den von Kunden herangetragenen Anforderungen angenommen. Herausgekommen ist eine neue verschlüsselte Kommunikationstechnologie als Werkzeug, das hohe Sicherheit und einfache Bedienung miteinander vereint: „VPSC (Virtual Protected Secure Communication)“.

Die Lösung besteht aus einem Server und einer Client Komponente in Form eines USB Sticks, einer SD Karte oder einer App. Der Server kann als Appliance oder als Software (auch virtualisiert) zum Einsatz kommen. Mit dieser Technologie ermöglicht SayTRUST® Secure Access eine abgesicherte Arbeitsumgebung, eine sichere, flexible und anwenderfreundliche Kommunikation ohne LAN-LAN-Kopplung. Somit ist ein sicherer Zugang auch ohne Installation von Software (Plug and Play) von jedem beliebigen PC aus möglich.

Im Gegensatz zu VPN Technologien setzen die Sicherheitsmechanismen bereits vor dem Kommunikationstunnel ein. Dies geschieht durch den koordinierten Einsatz mehrerer ineinandergreifender Sicherheitsstufen (Defense in Depth). So werden Daten und Netzwerk in höchstem Grad geschützt. Das vielschichtige Abwehrsystem minimiert die Risiken und die Möglichkeiten eines Eindringens exponentiell im Vergleich zu VPN-Lösungen. Sollte es einem Hacker dennoch gelingen, eine der Sicherheitsbarrieren zu überwinden (siehe Abbildung 1), so wird der Zugriff durch die weiteren Sicherheitsstufen unterbunden. Nur wenn sämtliche ineinandergreifende und voneinander abhängige Sicherheitsstufen durchlaufen werden, wird die sichere Kommunikation aufgebaut.

Hierbei sind die Sicherheitsstufen in drei Sicherheitsblöcke unterteilt:

Sicherheitsblock 1: Sicherheit durch eindeutige persönliche Identifizierung
Sicherheitsblock 2: Verbindungssicherheit durch Defense in Depth
Sicherheitsblock 3: Commitment-Sicherheit

Abbildung 1

Die Verbindungssicherheit (VPSC)

Bevor der sayTRUST® Access Client auf einem PC oder einem Notebook aktiviert wird, wird zunächst die Identität des Benutzers mehrstufig überprüft:

1. Der VPSC Kommunikations-Client überprüft anhand des durch die Certificate Authority (CA) des sayTRUST® Servers erstellten 2048 Bit Anwenderzertifikats mögliche Zugriffe auf lokale, mobile oder remote Anwendungen und Ressourcen im Prozessspeicher. So werden nur erlaubte Anwendungen getunnelt. Nicht erlaubte Anwendungen werden blockiert. Bevor jedoch eine Kommunikation mit den zu schützenden Ressourcen (Anwendungen, Server, Netzwerk, ...) zustande kommen kann, wird in Abhängigkeit des Anwenderzertifikats ein

2. personifizierter, client- und serverseitiger Perfect Forward Secrecy Schlüssel (PPFS) für die Kommunikation zwischen dem sayTRUST® Client und sayTRUST® Access Server ausgehandelt. Der in Abhängigkeit des Anwenderzertifikats neu generierte, bis zu diesem Zeitpunkt weder dem Client noch dem Server bekannte Schlüssel wird dann für die Kommunikation verwendet.

3. Dabei wird der Socket der Anwendung direkt vom Arbeitsspeicher des Clientrechners gestartet und die Verbindung zum geschützten Netzwerk/Ressource getunnelt.

Virtual Private Secure Communication (VPSC)

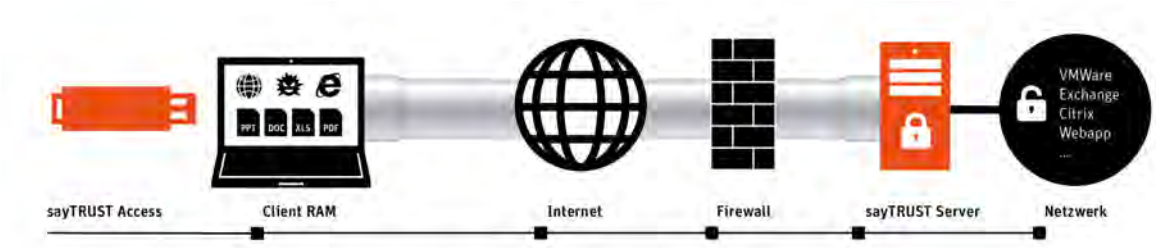


Abbildung 2

Der Client-PC kann sich in einer unsicheren Umgebung befinden und stellt das schwächste Glied in der Kommunikationskette dar. Im Gegensatz zu herkömmlichen VPN Technologien wird bei der VPSC Technologie der Client-PC nicht ein Mitglied des geschützten Netzwerks. Die durch sayTRUST® Access aufgebaute VPSC-Verbindung erfolgt auf der Anwendungsebene. Informationen des geschützten Netzwerkes werden nicht auf dem Client-Rechner vorgehalten und sind damit weder auf dem Client-Rechner noch auf der Verbindungsstrecke sichtbar. Wird die Verbindung beendet, verbleiben auf dem Client-Rechner keinerlei Informationen zurück.

Einfache, schnelle und flexible Installation und Nutzung

sayTRUST® Secure Access ist sehr sehr einfach zu bedienen (siehe Abbildung 3):

- Nach Einstecken des USB-Access Clients (1) erfolgt zunächst die persönliche Identifikation (2).
- Nach erfolgreicher Identifikation startet das sayTRUST® Menü (3).
- Benutzer- und netzwerkspezifische Informationen werden im Arbeitsspeicher erstellt und verwaltet. Nach Beendigung der Kommunikation werden diese gelöscht, es verbleiben keine Spuren auf dem PC.

Abbildung 3

Die Kommunikation via sayTRUST®

- erfordert keine Softwareinstallation auf dem Client-PC,
- keine Installation und Konfiguration von virtuellen Netzwerkkarte
- Plug und Play verwendbar

ist flexibel nutzbar für Anwendungen,

- die remote und lokal installiert sind,
- die sich in Anwendungsfarmen befinden und/oder
- mobil auf dem sayTRUST® USB-Access Client eingerichtet sind.

Das Anwendermenü ist einfach, intuitiv in der Bedienung. Der Komfort für den Anwender wird deutlich erhöht durch

- Passwortmanager für Single Sign On (SSO)
- Dokumentenlenkung
- File transfer und File Synchronization
- Encryption Tool
- Frontend für virtuelle und veröffentlichte Anwendungen
- Integration für VoIP Telefonie und Vieles mehr

Die Defense in Depth-Sicherheit beginnt vor dem Client-Rechner mit der eindeutigen Identifizierung und Bereitstellung der Ressourcen entsprechend den Benutzer- bzw. Gruppenberechtigungen. Mehrere ineinandergreifende Sicherheitsstufen für die Kommunikation steuern aus dem Prozessspeicher des Clientrechners heraus gezielt eine sichere Kommunikation.

Verschlüsselungsverfahren

Die Verschlüsselung der sayTRUST® Kommunikation zwischen Client und Server basiert auf SSL mit X.509 Zertifikaten und TLS 1.3 unter der Verwendung der Implementierung von OpenSSL in der aktuellen Version. Auf allen Plattformen und Versionen setzen wir auf die eigene Übersetzung dieser Verschlüsselungssoftware-Bibliothek.

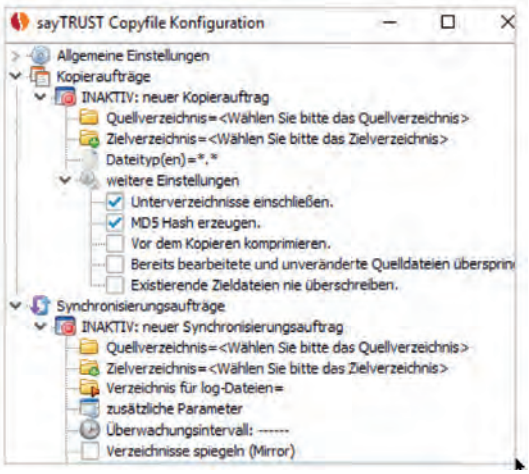
Die Bedingung für die SSL verschlüsselte und gesicherte Übertragung der Nutzerdaten ist eine positive X.509 CA Server- und Client-Zertifikats-Authentifizierung. Die Überprüfung der Client- und Server-Zertifikates lässt keine CA-Zertifikate öffentlicher oder externer Zertifizierungsstellen zu, sondern ausschließlich CA-Zertifikat der jeweiligen sayTRUST® Installation. Die Zertifikate und deren Schlüssel werden somit ausschließlich auf dem sayTRUST® Server unter Verwendung von Zufallszahlen (Unter Linux: Nur /dev/random und kein /dev/urandom) generiert. Die Nutzerdaten werden über das symmetrische Verschlüsselungsverfahren AES mit 256 Bit Schlüssellänge verschlüsselt und übertragen. Der hierfür eingesetzte Schlüssel wird über Perfect Forward Secrecy (PFS/FS) mittels des Diffie-Hellman Algorithmus ausgehandelt.

Die Transportsicherung (Hashing) der hierfür eingesetzten X.509 Zertifikate sowie der Nutzerdaten gewährleistet SHA in der sicheren Version mit 256 oder 384 Bits. Die asymmetrische Verschlüsselung sowie die Signierung werden von OpenSSL mittels X.509 Zertifikaten durchgeführt, die auf dem Algorithmus RSA mit der Schlüssellänge von 2048 Bits basieren.

Die Nutzerdaten werden verschlüsselt und unverfälscht übertragen. Sämtliche derzeit bekannten Angriffe wie auch Man-in-the-Middle-Attacken werden somit abgewehrt. Die Authentifizierung der Anwender wird auf Serverseite passwortlos über das X.509 Clientzertifikats-Serial des jeweiligen X.509 Clientzertifikates vorgenommen. Auf Clientseite wird das Clientzertifikat standardmäßig nur mit einem Passwortschutz abgelegt. Die Zertifikatsverteilung für Windows-Systeme wird durch ein manuelles Herunterladen der Kommunikationssoftware mit dem entsprechenden Zertifikat oder über das sayTRUST® Verteilungs-software durchgeführt und kann unmittelbar auf dem Client ausfügeführt werden.

Die Zertifikatsverteilung für mobile Geräte (Smartphones, Tablets) ist wie folgt umgesetzt:

Der betreffende Client kann das Zertifikat über das Softwareverteilungssystem beziehen oder manuell herunterladen. Hier ist ein X.509 CA Zertifikat der sayTEC AG enthalten, das eine sichere Verbindung auf sayTEC Zertifikatsverteilungssysteme sicherstellt (siehe CA Überprüfung weiter oben). Der Client fordert über diese Verbindung für seine sayTRUST® Installation das X.509 CA Zertifikat an, welches hier vorher vom Betreiber der sayTRUST® Installation hinterlegt worden ist. Da dies keine geheime Information darstellt, muss sich der Client nicht durch ein Clientzertifikat ausweisen. Nun kann der Client eine sichere Verbindung zur betreffenden sayTRUST® Installation herstellen (siehe CA Überprüfung weiter oben). Auch hier ist kein Clientzertifikat nötig, da sich der Server gegenüber dem Client zunächst durch die CA-Überprüfung des Server-Zertifikates ausweist und der Client sich in einem nächsten Schritt über seine Zugangsdaten gegenüber dem Server identifiziert. Unter Angabe seines Benutzernamens und Passwortes kann der Client sein Zertifikat abrufen.



sayTRUST® Access Anwendermenü und Erweiterungen

Einfache Bedienung

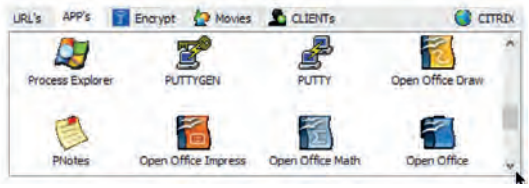
Das Anwendermenü dient zur Vereinfachung der Arbeitsumgebung und Bedienung. Unabhängig vom Clientrechner erhält der Anwender eine eigene Arbeitsumgebung. Inhalte und Darstellung können zentral durch den Administrator oder individuell durch den An-wender gestaltet und verwaltet werden.

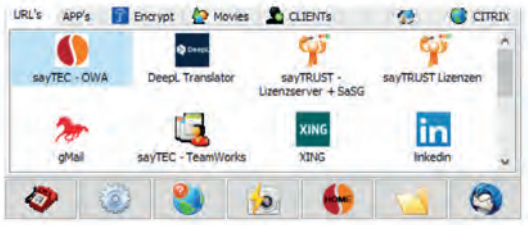
Passwortmanager für SSO

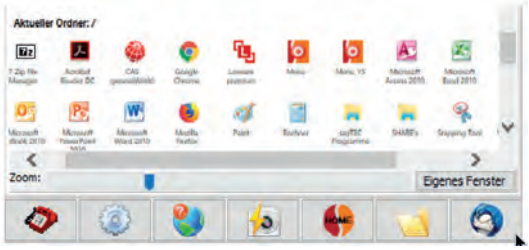
Der Passwortmanager ermöglicht eine weitere Vereinfachung in der Bedienung. Anwender müssen sich nur einmal anmelden, um Dienste zu nutzen. Alle Passwörter werden in der Passwort-Datenbank verwaltet und je nach Berechtigung in die jeweiligen Bereiche eingefügt.

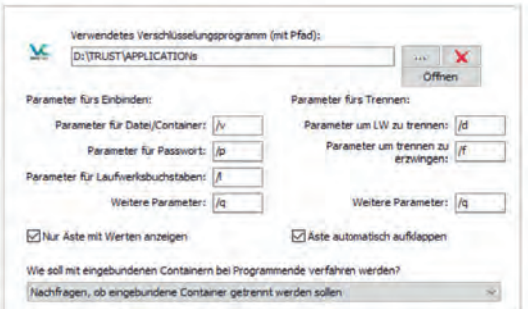
Secure-Shares-Copyfile für File Transfer und Syncronisation

Kopieren und Synchronisieren großer Dateien und Verzeichnisse mit dem sayTRUST® Secure-Share-Verzeichnis. Das Programm startet Kopieraufträge reentrant, so dass der Kopiervorgang auch nach einem Verbindungsabbruch wieder an der letzten Stelle aufgenommen werden kann. Dabei prüft der Kopiervorgang, ob die Datei bereits an dem Zielort identisch









vorhanden ist, und kopiert ausschließlich Dateien, die neu sind oder geändert wurden. Um sicherzustellen, dass der Kopiervorgang erfolgreich war, kann auch ein MD5 Hash-File erzeugt werden.

Portable Apps

Stellen auf dem USB Acces Client mobile Anwendungen bereit wie Mail-, Telefonclient oder Office Anwendungen zur online- und offline-Nutzung.

Website

Speichert und verwaltet häufig verwendete Internetadressen und ermöglicht die Nutzung durch den auf dem sayTRUST® Access installierten oder auf dem Gastrechner installierten Webbrowser.

Microsoft und/oder Citrix Anwendungsfarmen

Stellt und verwaltet Citrix und Microsoft Anwendungsfarmen und ermöglicht die mobile Nutzung auch ohne einen vorinstallierte Receiver.

sayTRUST® Encyption Tool

Das Encryption Tool stellt eine einfache Benutzeroberfläche zur Verwaltung und Einbindung verschlüsselter Container zur Verfügung.

sayTRUST® Access Komponenten

sayTRUST® Access Server	VPST Appliance Varianten		
Ausführung/ Funktionsumfang	sayTRUST® Access VPST Appliance **Basic**	sayTRUST® Access VPST Appliance **Professional**	sayTRUST® Access VPST Appliance **Enterprise**
Darstellung			
Betriebssystem	VPST Server **Basic**	VPST Server **Professional**	VPST Server **Enterprise**
Remote VPST-Lizenzen im Lieferumfang	5	5	5
Max. Anzahl VPST-Verbindungen	25	250	unbegrenzt
Anzahl enthaltener Lizensen	5	5	5
Upgradefähig	nein	ja	ja
Mobile Device Optionen	nein	nein	ja
Hochverfügbarkeitsoption (HA)	nein	nein	optional
VoIP-Optionen	nein	nein	ja

sayTRUST® Access Server	VPSC Appliance Varianten		
Ausführung/ Funktionsumfang	sayTRUST® Access VPSC Appliance **Basic**	sayTRUST® Access VPSC Appliance **Professional**	sayTRUST® Access VPSC Appliance **Enterprise**
Darstellung			
Betriebssystem	VPSC Server **Basic**	VPSC Server **Professional**	VPSC Server **Enterprise**
Remote VPST-Lizenzen im Lieferumfang	5	5	5
Max. Anzahl VPST-Verbindungen	25	250	unbegrenzt
Anzahl enthaltener Lizensen	4	8	4 x Glasfaser, 12 x Kupfer
Upgradefähig	nein	ja	ja
Mobile Device Optionen	nein	nein	ja
Hochverfügbarkeitsoption (HA)	nein	nein	ja
VoIP-Optionen	nein	nein	ja

sayTRUST® Access Client	Varianten			
Ausführung/ Funktionsumfang	Software Client	USB-Client	Biometric USB Client	Biometric Microprocessor USB Client
Darstellung				
Sicherheitsstufen für Personifizierung	2	2	3	3
Sicherheitsstufen für Remote-Access	3	3	3	3
Authentifizierungschip	-	-	-	x
Biometrie	-	-	x	x
Passwort für Biometrie	-	-	x	x
Hardwareverschlüsselung	-	-	x	x
Hardwareverschlüsselungstiefe	-	-	AES 256	AES 256
Anwenderzertifikat	x	x	x	x
PIN für Anwenderzertifikat	x	x	x	x
Kopierschutz für Zertifikat	x	x	x	x
sayTRUST® Anwendermenü	x	x	x	x

sayTRUST® Access biometrischer USB-Client mit mikroprozessorbasierter Verifikation

- Biometrisch sicherer Mikrochip
- Fest integrierte AES (256-Bit) auf dem Mikrochip
- Die Plattform arbeitet unabhängig
- Benötigt keine Installationssoftware
- Hinterlässt keine Spuren auf dem Computer
- Speicherunabhängige Mikrochips für die biometrische Verifikation
- Sichert bequem sämtliche sensiblen Daten, ob persönlich oder geschäftlich
- Mehrstufige Authentifizierung, unabhängig von der PC-Plattform
- Integrierte sichere PIN-Eingabe für verschiedene Funktionen (optional)
- Der Fingerabdruck wird nur auf dem Gerät, nicht aber auf dem Server gespeichert
- Erst nach erfolgreicher biometrischer Fingererkennung ist die USB-Flash-Disk-Einheit im Betriebssystem sichtbar und ein AES (256-Bit) verschlüsselter Flash-Speicher ist verfügbar