sayTEC SOLUTIONS

Die Lösung für Lösungen.

Whitepaper

sayTRUST® Access

Verschlüsselungsverfahren

März 2014

Produktfilm sayTRUST

Wenn es um die Anbindung mobiler Anwender an ein Firmennetzwerk geht, ist das „Virtual Private Network“ – kurz VPN – der gängige Begriff. Doch unweigerlich denkt man dabei in der Regel automatisch an den verbundenen Aufwand und die Vielzahl von Problemen, die bei der Installation und dem Betrieb eines VPN auftreten können.

Im Folgenden wollen wir Ihnen einen kleinen Überblick über das einzigartige und hochsichere Verschlüsselungsverfahren von sayTRUST Access geben.

Das Verschlüsselungsverfahren

Die Verschlüsselung der sayTRUST Kommunikation zwischen Client und Server basiert auf SSL mit X509 Zertifikaten und TLS 1.2 unter der Verwendung der Implementation von OpenSSL in der aktuellsten Version (Stand 19.02.2014: 1.0.01f). Auf allen Plattformen und Versionen setzen wir auf die eigene Übersetzung dieser Verschlüsselungssoftware-Bibliothek.

Nutzerdaten werden erst nach einer erfolgreichen X509 CA Server- und Clientzertifikatsauthentifizierung über SSL verschlüsselt und gesichert übertragen. In dieser CA-Überprüfung des Client- und Server-Zertifikates werden keine CA-Zertifikate öffentlicher oder externer Zertifizierungsstellen berücksichtigt, sondern lediglich das CA-Zertifikat der jeweiligen sayTRUST Installation. Die Zertifikate und deren Schlüssel werden ausschließlich auf dem sayTRUST Server unter Verwendung von guten Zufallszahlen (Unter Linux: Nur /dev/random und kein /dev/urandom) generiert. Die Nutzdaten werden über das symmetrische Verschlüsselungsverfahren AES mit 256 Bit Schlüssellänge verschlüsselt übertragen; der hierfür eingesetzte Schüssel wird über Perfect Forward Secrecy (PFS/FS) mittels des Diffie-Hellman Algorithmus ausgehandelt. Die Transportsicherung (Hashing) der hierfür eingesetzten X509 Zertifikate sowie der Nutzdaten stellt SHA in der sicheren Version mit 256 Bits oder 384 Bit sicher. Die asymmetrische Verschlüsselung sowie die Signierung wird von OpenSSL mittels X509 Zertifikaten durchgeführt, die auf dem Algorithmus RSA mit der Schlüssellänge von 2048 Bits basiert. Der sich unter anderem hieraus ergebende Cipher-String von OpenSSL, der vom Client als auch Server überprüft worden ist, ist der Folgende: „DHE-RSA-AES256-GCM-SHA384“. Über diese beschriebene SSL Sicherung werden die Nutzdaten verschlüsselt und unverfälscht übertragen. Alle derzeit bekannten Angriffe wie auch Man-in-the-middle-Attacken werden hiermit sicher abgewendet.

Die Authentifizierung der Anwender wird auf Serverseite passwortlos über das X509 Clientzertifikats-Serial des jeweiligen X509 Clientzertifikats vorgenommen. Auf Clientseite wird das Clientzertifikat standardmäßig nur mit einem Passwortschutz abgelegt.

Die Zertifikatsverteilung für Windows-Systeme wird durch ein manuelles Herunterladen der Clientsoftware mit Zertifikat sowie manuelle Installation auf dem Client gelöst.

Die Zertifikatsverteilung für mobile Geräte (Smartphones, Tablets) ist folgendermaßen umgesetzt: Der betreffende Client kann die Software sayTRUST im jeweiligen Softwareverteilungssystem des Herstellers beziehen oder die Software manuell auf das Gerät kopieren und installieren. Hier ist ein X509 CA Zertifikat der sayTEC GmbH enthalten, das eine sichere Verbindung auf sayTEC Zertifikatsverteiltungssysteme sicherstellen kann (siehe CA Überprüfung weiter oben). Der Client fordert über diese Verbindung für seine sayTRUST Installation das X509 CA Zertifikat an, welches hier

vorher vom Betreiber der sayTRUST Installation hinterlegt worden ist. Da dies keine geheime Information darstellt, muss sich hier 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 dem Client gegenüber durch die CA-Überprüfung des Server-Zertifikats zunächst ausweist und der Client in einem nächsten Schritt über seine Zugangsdaten dem Server. Unter Angabe seines Benutzernamens und Passwortes kann der Client sein Zertifikat abrufen.

Das zentrale Zertifikatsverteilungssystem der sayTEC Solutions GmbH kann durch einen eigenen Server des Kunden und ein CA Zertifikat des Kunden ersetzt werden. Dadurch ist eine eigene Clientsoftware notwendig und Updates müssen eigenverantwortlich umgesetzt werden.

sayTRUST Access

Bei sayTRUST Access erfolgt der administrative Teil für die Einrichtung des Verbindungsaufbaus auf dem Server. Vom Administrator wird dabei für den jeweiligen Anwender ein eigenes Zertifikat erstellt und auf den für den Anwender vorgesehenen sayTRUST USB Access Client kopiert. Für einfache Zugriffe ist es dabei völlig ausreichend, eine Gruppe mit den gewünschten Rechten auf dem sayTRUST Access Server anzulegen und einen Client hinzuzufügen.

Sobald der Client auf einem sayTRUST USB Access Client (USB Stick) installiert ist und dem jeweiligen Anwender ausgehändigt wurde, ist dieser auch schon einsatzbereit. Dazu muss sich der Anwender lediglich entsprechend den Unternehmensrichtlinien über den sayTRUST USB Access Client authentisieren. Optional sind für den sayTRUST Access auch USB Access Clients mit biometrischer Authentisierung erhältlich.

Der Benutzer kann dann ausschließlich auf die für ihn freigegebenen Ressourcen zugreifen. Alle anderen Zugriffe werden - entsprechend den Einstellungen am sayTRUST Access Server-- komplett gesperrt oder nicht getunnelt.

Weiterhin besteht die Möglichkeit, nur bestimmte Anwendungen auf Grund ihres Programmnamens zu tunneln. Das bedeutet, nur Pakete dieser Anwendungen werden zum sayTRUST Server geschickt. Netzwerkdaten anderer Programme werden entweder verworfen oder am Tunnel vorbei ganz normal ins Internet geleitet.

Mit sayTRUST Access können TCP- bzw. UDP-basierende Anwendungen getunnelt werden, die auf dem jeweiligen Client-PC installiert, oder auf dem sayTRUST USB Access Client (USB Stick) in Form einer portablen Version vorhanden sind.

sayTRUST Access ist also weder auf den Browser beschränkt, noch auf Proxy-Programme angewiesen.

Für die Verbindung in das Firmennetzwerk ist keinerlei Installation am jeweiligen Client-Rechner erforderlich!

Die Verwaltung der Client-Zertifikate erfolgt vollständig serverseitig. Gelöschte Client-Zertifikate werden automatisch auf eine Sperrliste gesetzt, damit die Verbindung zurückgewiesen wird, falls sich der "alte" Client dennoch verbinden möchte.

Selbst wenn es einem Anwender gelingen sollte, einen sayTRUST Access Client zu manipulieren, werden alle Daten, die über den Tunnel in das Firmennetzwerk geleitet

werden, serverseitig nochmals ausgewertet und ohne vorhandenen, gültigen Regelsatz verworfen.

Clientseitige Manipulationen sind somit nicht nur ungleich schwieriger als bei SSL-VPNs sondern auch absolut wirkungslos!

Die Konfiguration des sayTRUST Clients ist in mehreren Ebenen verschlüsselt und somit nicht durch den User änderbar. Möglichkeiten der Konfiguration des sayTRUST Access Clients sind z.B. die Einschränkung für den Benutzer durch den Server, oder auch die komplette Abschaltung. Bestimmte Einstellungen, wie z.B. die Komplexität der Passwörter, können dabei erzwungen werden. Selbst Veränderungen der Sicherheits-Policies erfordern nicht den Austausch des sayTRUST Access Clients.