sayTEC
SOLUTIONS

The solution for solutions.

Whitepaper

sayTRUST® Access

Encryption Processes

March 2014

Produktfilm sayTRUST

If it is about a connection of mobile users to a corporate network „Virtual Private Network", – in short VPN – is the common term. But one is inevitably and automatically always reminded of the associated effort and the multitude of problems associated with installation and operation of the VPN. In the following we would like to point out an overview of the unique, highly secure encryption method of sayTRUST Access.

The Encryption Method

The sayTRUST communication encryption between client and server is based on SSL with X509 certificates and TLS 1.2 using implementation of OpenSSL in the latest version (status as of 19th February 2014: 1.0.01f). On all platforms and for all versions we rely on our own translated encryption software library. Users' data are SSL encrypted only after successful X509 CA server and client certificate authentication, and all data is transmitted via a secure connection. This CA validation procedure for the verification of client and server certificate does not require CA certificates of public or external certification centers but only the CA certificate of the respective sayTRUST installation. The certificates and the keys of the certificates are generated solely on the sayTRUST server by making use of random numbers (under Linux: only /dev/random and no /dev/urandom). The users' data are transferred encrypted over AES symmetrical encryption procedure with 256 bits key length; the key created for the purpose is negociated via Perfect Forward Secrecy (PFS/FS) with Diffie-Hellman algorithm. The safest version of SHA with 256 Bits or 384 Bits ensures the safe transportation (Hashing) of the employed X509 certificates and the users' data. The asymmetric encryption and the signing is performed by OpenSSL with X509 certificates based on an RSA algorithm with a key length of 2048 bits. Inter alia, the generated Cipher-String of OpenSSL, checked by the client and the server, is the following: „DHE-RSA-AES256-GCM-SHA384". Users` data are encrypted via SSL safeguarding as described and unaltered transmitted. All attacks that are currently known as e.g. man-in-the-middle attacks can therefore be fended off adequately.

The users' authentification is carried out on the server side without password by using the X509 client certificate serial of the respective X509. On the client side the client certificate is by default only saved with password protection.

The certificate deployment for Windows systems is solved by manual download of the client software with certificate and a manual installation on the client.

The certificate deployment for mobile devices (smartphones, tablets) is realised as follows: the respective client can purchase the software sayTRUST in the respective software distribution system of the vendor or it can copy the software manually to the device and install the software on the device. Included here is a X509 CA certificate of

sayTEC GmbH, operating via secure connection with sayTEC certificate distribution systems (see above CA verification). Via this interface the client requests its X509 CA certificate for its sayTRUST installation, the certificate has been deposited before from the operator oft the sayTRUST installation. As this does not provide secret information, the client is not required to identify itself by means of a client certificate. The client can now establish a secure connection to the respective sayTRUST installation (see above CA verification). In this context no client certificate is neccessary, as the server first identifies itself to the client by means of CA verification of the server certificate and in a following step the client identifies itself to the server by means of its access data. By specifying its user name and password the client can retrieve its certificate.

The central certificate distribution system of sayTEC Solutions GmbH can be replaced with an own server of the customer and a CA certificate of the customer. Thus the customer needs his own client software and updates must be realized independently.

sayTRUST Access

For sayTRUST Access the administrative part of the connection initiation is done on the server side. In this context the administrator generates an own certificate for the respective user, this certificate is copied to the intended sayTRUST USB Access Client. For simple access it absolutely suffices to generate a group with the desired rights on the sayTRUST Access server and to add the client.

As soon as the client is installed on a sayTRUST USB Access Client (USB Stick) and has been surrendered to the respective user, it is ready to use. The user only has to authenticate himself in compliance with the companies corporate security policies by means of the sayTRUST Access and USB Access client. Optionally USB Access Clients with biometrical authentication can be obtained for sayTRUST Access. The user can then only access data for which he has the authorization. All other accesses are completely blocked – following the sayTRUST Access Server settings or are not masked before tunneling.

Furthermore it is also possible to tunnel only certain applications due to their program names. This means, only packages of those applications are send to the sayTRUST server. network data of other programs is either discarded or is proceeded past the tunnel and is completely normaly forwarded to the internet.

sayTRUST Access allows the tunnelling of TCP- and/or UDP based applications, that are installed on the respective Client PC or present on the sayTRUST USB Access Client (USB stick) in the form of a portable version.

Hence sayTRUST Access is neither restricted to a browser nor it relies on a proxy program.

The connection to the corporate network requires no installation on the respective client device!

The administration of the client certificates is completly on the server side. Allowances cancelled are automatically put on a exception list, so that the connection is rejected in case that the „old" client tries to connect anyway.

However, even if a user succeeds in manipulating a sayTRUST Access Client, all data directed to the network through the tunnel are evaluated again on server side and rejected without valid standard rule. Manipulations on the client side are thus not only infinitely more difficult than for SSL-VPNs but also utterly ineffective.

The sayTRUST configuration is encrypted at various levels and thus not changeable by the user. Configuration possibilities for the sayTRUST access clients are e.g. the user's limitation by the server or even the user's complete deactivation. In doing so, certain settings as e.g. complexity of the passwords can be enforced. Even changes of security policies do not require exchanging the sayTRUST Access Client.