

Q-100.178 - TLS (Transport Layer Security)

Q-100.178 - TLS (Transport Layer Security)

aus Tobit KB importiert - vom 26.01.2007 - [Beitrag bei Tobit](#)

Problem

Was ist TLS und wie wird es unter David eingerichtet?

Antwort

Sie haben die Möglichkeit, eMails über sichere TLS-Verbindungen zu versenden und zu empfangen. TLS (Transport Layer Security) ermöglicht Ihnen eine verschlüsselte Übertragung von Daten, und verhindert so unautorisierten Zugriff auf die übertragenen Informationen.

Voraussetzung für die Nutzung von TLS ist ein entsprechendes "Zertifikat", das der eindeutigen Identifikation dient. Um eine Übertragung von Nachrichten über eine sichere Verbindung zu gewährleisten, muss sowohl der Absender als auch der Empfänger über ein Zertifikat verfügen, das ihn eindeutig identifiziert.

Ein solches Zertifikat wird üblicherweise bei einer sogenannten "Certification Authority" (wie z.B. VeriSign oder Thawte) beantragt, die bei eventuellen Zweifeln auch die Echtheit von Zertifikaten überprüft und gegebenenfalls bestätigt.

Sie können aber auch "selbstsignierte Zertifikate" verwenden. Ein solches Zertifikat wird vollständig selbst erzeugt und bietet daher keine zusätzliche Kontrollmöglichkeit. Bei der Erstellung eines Zertifikats werden auch die für die TSL-Übertragung notwendigen Code-Schlüssel erzeugt. Zu einem Zertifikat gehören jeweils zwei dieser Schlüssel.

Der "Public Key" dient zum Verschlüsseln von Nachrichten, die an Ihre eigene Adresse gesendet werden sollen. Daher ist dieser Schlüssel all denjenigen Personen zur Verfügung zu stellen, die Ihnen TLS-Nachrichten schicken wollen. Der "Private Key" dient zum Entschlüsseln von Nachrichten, die mit Ihrem Public Key verschlüsselt wurden. Geben Sie aus diesem Grund Ihren Private Key niemals heraus und bewahren Sie ihn an einem sicheren Ort auf.

Beim TLS-Verfahren findet (z.B. im Gegensatz zu PGP) keinerlei Verschlüsselung auf den Workstations statt. Daher ist auch keine Installation zusätzlicher Komponenten auf den Arbeitsstationen im Netz erforderlich. Die Ver- bzw. Entschlüsselung der Nachrichten wird vom David Server direkt beim Versand oder Empfang durchgeführt.

Das bedeutet, dass Sendeaufträge vom Anwender unverschlüsselt an den Server übergeben werden, der dann die verschlüsselte Übertragung übernimmt. Empfangene TLS-Nachrichten erreichen den Server verschlüsselt, werden anschließend direkt von diesem entschlüsselt und als Klartext im Tobit Archive System (TAS) abgelegt. Die Benutzer haben also an ihren Arbeitsplätzen jederzeit direkten Zugriff auf die unverschlüsselten Informationen.

Wenn Sie die TLS-Funktionen von David nutzen möchten, um einen verschlüsselten Nachrichtenversand und -empfang zu realisieren, so stehen Ihnen dazu zwei spezielle Menüpunkte in der Systemkonfiguration des David PostMan zur Verfügung:

- Aktivieren Sie die Funktion "TLS Empfang erlauben" um den Empfang von TLS-Nachrichten zu ermöglichen.
- Über die Auswahlliste "TLS bei Versand verwenden" können Sie bestimmen, ob bzw. in welcher Weise TLS beim Versand eingesetzt werden soll.

Im Verzeichnis »DAVID\UTIL\WINDOWS\TLSCERT« auf dem David Server finden Sie ein Programm mit dem Namen »TLSCERT.EXE«, mit dem Sie ein TLS-Zertifikat erstellen bzw. beantragen können. In der Hilfe zu diesem Programm (Taste F1) erfahren Sie ebenfalls, wie Sie das Zertifikat unter David PostMan verwenden.