

Q-103.165 - Serverbasierte Verschlüsselung (TLS) bei den eMail-Diensten

Q-103.165 - Serverbasierte Verschlüsselung (TLS) bei den eMail-Diensten

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

Problem

Es soll die Serverbasierte Verschlüsselung TLS bei den eMail-Diensten genutzt werden.

Antwort

David bietet die Möglichkeit, eMails über sichere TLS-Verbindungen zu versenden und zu empfangen. TLS (Transport Layer Security) ermöglicht 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 so genannten Certification Authority (wie z.B. VeriSign oder Thawte) beantragt, die bei eventuellen Zweifeln auch die Echtheit von Zertifikaten überprüft und ggf. bestätigt. Es ist jedoch auch möglich, selbstsignierte Zertifikate zu verwenden. Ein solches Zertifikat wird vollständig selbst erzeugt und bietet daher keine zusätzliche Kontrollmöglichkeit. Bei der Erstellung eines Zertifikats werden auch die für die TLS-Übertragung notwendigen Code-Schlüssel erzeugt.

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 David-TLS-Funktionen nutzen möchten, um einen verschlüsselten Nachrichtenversand und -empfang zu realisieren, so stehen Ihnen dazu zwei spezielle Menüpunkte in der David PostMan Systemkonfiguration unterhalb von »Erweitert« 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.

Für einzelne Nachrichten kann der verschlüsselte Versand auch direkt im David InfoCenter über den entsprechenden Schalter in den Nachrichten Optionen erzwungen werden. Der Versand findet in diesem Fall generell in verschlüsselter Form statt. Ein unverschlüsselter eMail-Versand ist bei dieser Einstellung nicht möglich. Sendeaufträge, die nicht als TLS-Nachricht übertragen werden können, werden nicht ausgeführt und erscheinen mit einer entsprechenden Fehlermeldung im Ausgangs-Archive des Absenders.

Im Verzeichnis »DAVID\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.

Hinweis:

Weitere Informationen zu dem Thema »Datensicherheit bei den eMail-Diensten« erhalten Sie im [KnowledgeBase Artikel 103.164](#).