Clientbasierte Mailverschlüsselung

Service zur Erzeugung und Speicherung eines Schlüsselpaares

Zur Unterstützung des Schutzes eigener und fremder personenbezogener Daten stellt TU.it die Infrastruktur für den Bezug von E-Mail-Zertifikaten für eine clientbasierte Mailsignatur und –verschlüsselung zur Verfügung.
Auch für vertrauliche Daten, welche zum Beispiel unter eine Geheimhaltungsvereinbarung fallen können, wird eine Mailverschlüsselung empfohlen.

Die **digitale Signatur*** von E-Mails dient dem Empfänger zur Verifizierung des Senders und Sicherstellung, dass der Inhalt während der Übertragung nicht verändert wurde.
S/MIME (Secure / Multipurpose Internet Mail Extensions) gilt als Standard für die Verschlüsselung und das Signieren von MIME-gekapselten E-Mails.

Für die Nutzung von S/MIME-Zertifikaten zur Verschlüsselung und Signierung wird aufgrund des verwendeten Public-Key-Verschlüsselungsverfahrens ein **Schlüsselpaar aus *öffentlichem* und *privatem* Schlüssel** benötigt.

TU Wien Mitarbeiter_innen und TU-Studierende können über ein Webportal ein solches Schlüsselpaar anfordern, welches von DigiCert signiert wird. IT Solutions stellt somit ein Service zur Verfügung, welches die benötigten Schlüssel erzeugt und im Browser abspeichert.

Der für die **Verschlüsselung** notwendige öffentliche Schlüssel des Empfängers wird TU-intern durch die automatische Integration der Benutzerzertifikate in das upTUdate-Adressbuch bereitgestellt. (Vor dem Versand einer verschlüsselten E-Mail an TU-Externe, muss man zuvor eine signierte E-Mail des Empfängers erhalten haben).

Für die **Entschlüsselung** einer E-Mail bedarf es auf Empängerseite des privaten Schlüssels des Empfängers. Dieses Zertifikat muss auf dem Computer installiert sein, auf dem die verschlüsselte Nachricht gelesen werden soll.
Mit dem öffentlichen Zertifikat des Senders wird vom Empfänger schließlich die Unversehrtheit der E-Mail geprüft.

Für TU-Externe werden kostenlose S/MIME-Zertifikate von einigen Unternehmen angeboten, wie zum Beispiel Comodo Free Secure Email Certificate und Secorio S/MIME mit einer jeweiligen Gültigkeit von 1 Jahr.

Abbildung: Signatur / Ver- und Entschlüsselung (CC-BY-SA: www.reddoxx.com)

Abbildung: Signatur (CC-BY-SA: www.reddoxx.com)

*) *Die digitale Signatur ist nicht zu verwechseln mit der Signatur, die man als Visitenkarte am Ende einer E-Mail einträgt.*
