E-Mail-Zertifikat für die THM-Adresse

19.3.2018

von Prof. Dr. Thomas Sauerbier

Mit einem E-Mail-Zertifikat kann man seine E-Mails signieren und verschlüsselte E-Mails mit Personen austauschen, die ebenfalls ein entsprechendes Zertifikat besitzen.

Diese Ausführungen beziehen sich auf Zertifikate nach dem S/MIME-Verfahren, das von den meisten gängigen E-Mail-Programmen unterstützt wird (z.B. Thunderbird und Outlook). Nicht verfügbar ist dieser Standard meist auf einfacheren Programmen für Smartphones sowie beim Zugang über Web-Interfaces per Browser.

Ein S/MIME-Zertifikat können alle Hochschul-Angehörigen – also auch alle immatrikulierten Studierenden – für ihre THM-E-Mail-Adresse kostenlos beantragen. Die THM stellt jedoch keine Zertifikate für E-Mail-Adressen anderer Provider (z.B. T-Online oder Gmail) aus.

Nachfolgend eine Kurz-Anleitung, wie man das S/MIME-Zertifikat an der THM bekommt und auf seinem Rechner installiert. Die Ausführungen beziehen sich dabei auf Firefox als Browser und Thunderbird als E-Mail-Programm.

- Mit dem Browser (Firefox wird empfohlen) geht man auf die entsprechende Seite von ITS (Abteilung IT-Services der THM):

  https://www.thm.de/its/services/netzdienste/zertifikate.html

  (alternativ „https://www.thm.de/its“ aufrufen und von dort über „Services“, „Netzdienste“ und „Zertifikate“ gehen)

  Dort geht man auf „Zertifikate für E-Mail-Verschlüsselung“ und folgt den dortigen Anweisungen. Dabei ist ein Web-Formular auszufüllen. Anschließend wird dazu ein Antragsformular (PDF) erzeugt, das auszudrucken und zu unterschreiben ist.

- Mit dem unterschriebenen Antrag geht man in Friedberg zu Herrn Frädrich (Raum A4.122). Dort muss man zur Überprüfung, ob es sich wirklich um die zur E-Mail-Adresse passende Person handelt, seinen Personal-Ausweis vorlegen.

- Nach kurzer Zeit erhält man eine E-Mail mit weiteren Hinweisen und Links zu Seiten, von denen aus man Zertifikate auf den eigenen Rechner lädt. Wichtig: Es muss derselbe Rechner sein, von dem aus man den Online-Antrag gestellt hat!

- Nach dem Importieren der Wurzel-Zertifikate sowie des eigenen Zertifikats ist dieses in Firefox vorhanden. Um es im E-Mail-Programm zu nutzen, muss es von Firefox aus als Datei mit der Endung „p12“ exportiert werden. Dazu wird „Extras | Einstellungen“ aufgerufen. Unter „Datenschutz & Sicherheit“ drückt man ganz unten auf den Button „Zertifikate anzeigen“. Unter „Ihre Zertifikate“ sieht man sein eigenes Zertifikat, das man anklicken und mit „Sichern...“ exportieren kann. Wichtig: Diese Datei enthält den persönlichen Schlüssel und ist deshalb unbedingt mit einem sicheren Passwort zu schützen!

- Anschließend wird das Zertifikat aus dieser Datei in Thunderbird importiert. Dazu wird dort „Extras | Einstellungen...“ aufgerufen. Unter „Erweitert | Zertifikate“ klickt man auf „Zertifikate verwalten“. Unter „Ihre Zertifikate“ kann man sein Zertifikat aus der zuvor erzeugten p12-Datei importieren.

- Um das Zertifikat für das Konto der THM-Adresse zu nutzen, ist bei den dortigen Konto-Einstellungen unter „S/MIME-Sicherheit“ das gerade importierte Zertifikat auszuwählen. Mit einem Häkchen bei „Nachricht digital unterschreiben (als Standard)“ wird ab sofort

jede Nachricht automatisch mit einer Signatur versehen. Diese ist auch für solche Empfänger sichtbar, die selbst kein Zertifikat besitzen.

- Sofern man das Zertifikat auch auf anderen Rechnern nutzen will, ist die p12-Datei auch dort in das E-Mail-Programm zu importieren.

Damit ist das Zertifikat nutzbar. Aus Gründen der Sicherheit sollte man jetzt noch unbedingt Folgendes machen:

- Jeder, der Zugang zum E-Mail-Programm mit dem importierten Zertifikat hat, kann jetzt grundsätzlich mit der Signatur des Besitzers unterschreiben sowie an diesen gerichtete verschlüsselte E-Mails lesen. Um Missbrauch zu verhindern, sollte deshalb der Zugriff auf das Zertifikat im E-Mail-Programm mittels Master-Passwort geschützt werden. Dieses kann bei Thunderbird – wenn dies bisher noch nicht geschehen ist – unter „Extras | Einstellungen“ und dann „Sicherheit | Passwörter“ eingerichtet werden.
- Im Browser ist das Zertifikat nicht notwendig. Es ist deshalb sinnvoll, es dort nach dem Erzeugen der p12-Datei wieder zu löschen, da sonst Nutzer des Browsers ebenfalls die Möglichkeit haben, das Zertifikat zu exportieren und anderweitig (missbräuchlich) zu verwenden. Alternativ ist auch der Browser über ein Master-Passwort zu schützen.
- Um das Zertifikat auch bei Datenverlust auf dem Rechner zu erhalten, sollte eine Sicherheits-Kopie der p12-Datei auf einem getrennten Datenträger sicher verwahrt werden.

Hier noch einige grundsätzliche Hinweise zum praktischen Gebrauch des Zertifikats:

- Nachdem das Master-Passwort für das E-Mail-Programm aktiviert wurde, wird es von diesem automatisch abgefragt, sobald ein Zugriff auf das Zertifikat erfolgt. Das ist beim Versenden signierter E-Mails oder beim Empfangen verschlüsselter E-Mails der Fall. Zusätzlich erfolgt die Abfrage auch dann, wenn der aktuelle Stand einer gerade in Bearbeitung befindlichen E-Mail automatisch unter „Entwürfe“ gespeichert wird. Die Abfrage erfolgt nach dem Aufruf von Thunderbird aber nur beim ersten Mal (bis zum Beenden des Programms).
- Will man eine verschlüsselte E-Mail an jemanden verschicken, muss auch dieser ein S/MIME-Zertifikat besitzen. Um dieses zu nutzen, muss man nur irgendwann eine signierte E-Mail dieser Person empfangen haben (das kann auch vor dem Erstellen des eigenen Zertifikats erfolgt sein). Dann speichert Thunderbird automatisch das Zertifikat dieser Person und stellt es bei einem späteren Versenden an diese Adresse bereit. Zur Verschlüsselung ist bei Thunderbird im Editor-Fenster unter „S/MIME“ nur das Häkchen bei „Nachricht verschlüsseln“ zu setzen.
- Ob man immer die Möglichkeit zur Verschlüsselung nutzen sollte, muss jeder selbst abwägen. Nachteilig ist auf jeden Fall, dass der Empfänger solche Nachrichten nicht von überall aus (evtl. Web-Interface, Smartphone usw.) lesen kann: Er sieht dann nur den Absender und den Betreff, nicht aber den Inhalt oder Anhänge.
- Es ist zu beachten, dass die Verschlüsselung empfangener E-Mails auch über das erste Öffnen und Lesen hinaus wirkt. Wenn man also z.B. eine mehrere Jahre alte verschlüsselte E-Mail nochmals lesen möchte, benötigt man dafür sein (damaliges!) Zertifikat. Zertifikate sollten also auch dann verfügbar gehalten werden, wenn sie abgelaufen sind. Nicht betroffen davon sind aber Anhänge, die man als Datei abgespeichert hat.