Ende-zu-Ende-Verschlüsselung bei De-Mail

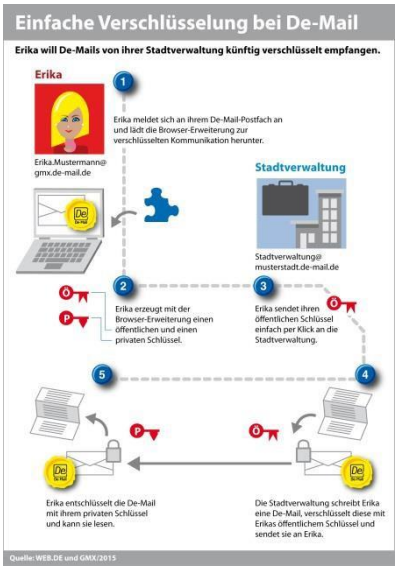
Warum Ende-zu-Ende-Verschlüsselung?

De-Mail bietet per se sichere digitale Kommunikation. Sicher bedeutet zum einen „technologisch sicher“, d.h. sämtliche Daten bleiben in Deutschland, der Transportweg ist verschlüsselt etc. Zum anderen ist De-Mail „rechtssicher“. Durch das De-Mail-Gesetz und der eindeutig identifizierten Kommunikationsteilnehmer weiß man stets, mit wem man kommuniziert und kann sicher sein, dies verbindlich und nachweisbar zu tun.

Neben diesen Aspekten der Sicherheit ist es wichtig, auch den Nachrichteninhalt selbst inklusive der Anhänge zu verschlüsseln, und damit eine „echte“ Ende-zu-Ende-Verschlüsselung zu bieten.

Wie funktioniert das bei De-Mail?

Um dies zu erreichen, kommt bei der Ende-zu-Ende-Verschlüsselung die Browser-Erweiterung „Mailvelope“ zum Einsatz. Bei Mailvelope handelt es sich um eine kostenlose OpenSource Browser-Erweiterung. Sie ermöglicht es, Nachrichten- Inhalte auf Basis von OpenPGP zu verschlüsseln und empfangene Nachrichten zu entschlüsseln. Dabei kümmert sich Mailvelope sowohl um das Ver- und Entschlüsseln selbst als auch um die Verwaltung der Schlüssel (Schlüssel erzeugen, importieren, exportieren).



Die Erweiterung wird einfach im Browser installiert und arbeitet fortan mit dem Web-Frontend von De-Mail nahtlos zusammen. Dabei finden alle sicherheitsrelevanten Aktionen und Operationen im lokalen Plugin statt und insb. nicht in der Web-Oberfläche von De-Mail.

Woher bekomme ich die Browser-Erweiterung?

Die Browser-Erweiterung kann direkt aus den Einstellungen des De-Mail-Postfachs heruntergeladen und installiert werden.

Nachdem die Erweiterung installiert ist, muss lediglich noch ein Schlüsselpaar erzeugt werden und schon kann es losgehen.

Was ist das Besondere an der Ende-zu-Ende-Verschlüsselung bei De-Mail?

Ende-zu-Ende-Verschlüsselung gibt es nicht nur bei De-Mail. Auch die klassischen E-Mail-Dienste von WEB.DE und GMX beherrschen mittlerweile Ende-zu-Ende. Daneben gibt es natürlich schon seit längerer Zeit frei verfügbare Erweiterungen und Werkzeuge, um beispielsweise per Thunderbird oder Outlook verschlüsselt zu kommunizieren.

Eine Schwachstelle der Ende-zu-Ende-Verschlüsselung war und ist der Knackpunkt des Schlüsselaustauschs. Woher weiß ich als Anwender, dass ich den „echten“ (öffentlichen) Schlüssel meines Kommunikationspartners habe und verwende? Beim Veröffentlichen bzw. Herunterladen von öffentlichen Keyservern fehlt es oftmals an Vertrauen und Sicherheit.

An diesem Punkt bietet De-Mail einen entscheidenden Vorteil – und damit auch ein Alleinstellungsmerkmal. Jeder De-Mail-Nutzer kann seinen öffentlichen Schlüssel im Öffentlichen Verzeichnisdienst (ÖVD) veröffentlichen. Von dort können umgekehrt dann die benötigten Schlüssel heruntergeladen werden. Da bei De-Mail alle Kommunikationsteilnehmer eindeutig persönlich identifiziert sind und sichergestellt wird, dass das Hochladen eines Schlüssels nur durch diese Person erfolgen kann, gibt es an dieser Stelle keinen Spielraum für Manipulation. In gleichem Maße wie ich bei De-Mail der Identität meines Kommunikationspartners vertrauen kann, kann ich auch der Echtheit seines Schlüssels vertrauen.

Wo erhalte ich Informationen zum Addin, insb. zur Einrichtung?

Die Installation und die Einrichtung sind einfach. Eine ausführliche Anleitung zur Installation, zum Einrichten und zur Verwendung finden Sie unter https://hilfe.web.de/demail/ende_zu_ende.html bzw. https://hilfe.gmx.net/demail/ende_zu_ende.html.

Sie haben noch keinen De-Mail-Account?

Dann wird’s aber Zeit! Einfach unter https://produkte.web.de/de-mail/ oder http://www.gmx.net/produkte/de-mail/ zu De-Mail anmelden. Sobald Sie freigeschaltet seid, können Sie auch von der Ende-zu-Ende-Verschlüsselung profitieren.