



Antwort der Landesregierung auf eine Kleine Anfrage zur schriftlichen Beantwortung

Abgeordneter Jan Wagner (DIE LINKE)

Ende-zu-Ende-Verschlüsselung bei DE-Mail

Kleine Anfrage - **KA 6/8931**

Vorbemerkung des Fragestellenden:

In ihrer Antwort auf meine Kleine Anfrage „Umsetzung der Beschlussrealisierung zur vertraulichen Kommunikation“, Drs. 6/4299, behauptet die Landesregierung: „Seit dem 20. April 2015 ist von den DE-Mail-Diensteanbietern die Möglichkeit zur Nutzung der Ende-zu-Ende-Verschlüsselung bei DE-Mail stark vereinfacht worden und Bestandteil der DE-Mail-Nutzung.“ Mir vorliegenden Medienberichten zufolge erfolgte seitens der zu diesem Zeitpunkt akkreditierten DE-Mail-Anbieter lediglich die Meldung, für DE-Mails die Möglichkeit einer PGP-Verschlüsselung zu nutzen.

Antwort der Landesregierung erstellt vom Ministerium der Finanzen

Vorbemerkung:

In der Antwort auf die Kleine Anfrage „Umsetzung der Beschlussrealisierung zur vertraulichen Kommunikation“, Drs. 6/4299, wurden die Informationen der DE-Mail-Dienstleister zum Angebot einer Ende-zu-Ende-Verschlüsselung genutzt. Eine klare Vorgabe durch den Gesetzgeber besteht derzeit noch nicht. Seit diesem Zeitpunkt stellen akkreditierte DE-Mail-Anbieter die Möglichkeit bereit über eine PGP-Verschlüsselung diese Sicherheitsanforderung umzusetzen. Das zugehörige Verfahren muss vom Bundesamt für Sicherheit in der Informationstechnik (BSI) noch geprüft werden.

1. Inwiefern ist nach Auffassung der Landesregierung Ende-zu-Ende-Verschlüsselung „Bestandteil“ der DE-Mail-Nutzung geworden?

Akkreditierte DE-Mail-Anbieter haben zur Realisierung des Angebots das Browser-Plug-in [Mailvelope](#) in die Web-Oberfläche integriert. Speziell für De-Mail haben die Mailvelope-Entwickler ein Client-API entwickelt, dass die Funktionen des Plug-ins erweitert. Damit lassen sich auch Anhänge PGP-verschlüsseln. Alternativ bieten andere Anbieter ein Plug-in für das E-Mail-Programm Outlook an. Francotyp-Postalia bietet beispielsweise eine Erweiterung für Exchange-Outlook-Umgebungen an.

Damit können De-Mail-Kunden der Deutschen Telekom, von United Internet (1&1, GMX und Web.de) sowie von Francotyp-Postalia untereinander PGP-gesicherte Mails austauschen, sofern sie im Frontend die Sicherheitsstufe „hoch“ aktiviert haben.

2. Wo wurde dieser Bestandteil technisch spezifiziert?

Mailvelope nutzt die [quelloffene JavaScript-Implementierung OpenPGP.js](#), die die Schlüsselerstellung und Speicherung im lokalen Browser-Store ermöglicht. Die Exchange-Erweiterung basiert auf der Open-Source-Software Gpg4win.

3. Ist die Aufnahme der Ende-zu-Ende-Verschlüsselung als Bestandteil der DE-Mail mit den Vorgaben des DE-Mail-Gesetzes des Bundes, insbesondere im Hinblick auf § 5, Abs. 3, Satz 2 vereinbar?

Die Bundesregierung beabsichtigt, bis Ende 2016 einen fortführenden Bericht zu erforderlichen Weiterentwicklungen bei De-Mail vorzulegen, in den die dann vorliegenden drei Jahre Erfahrungen mit De-Mail-Diensten im Markt sowie die erforderlichen Änderungen aus den Arbeiten zur Digitalen Agenda und zur eIDAS-VO einfließen können.

Laut Vorgaben des DE-Mail-Gesetzes § 5, Abs. 3 bleibt der Einsatz einer durchgängigen Verschlüsselung zwischen Sender und Empfänger (Ende-zu-Ende-Verschlüsselung) hiervon unberührt.