



E-Mail-Verschlüsselung für Behörden und Unternehmen – Volksverschlüsselung und Ideen zum Schlüsselaustausch

Ulrich Waldmann

Fraunhofer-Institut für Sichere Informationstechnologie

Zusammenfassung

Die Ende-zu-Ende-Verschlüsselung gilt als ein wirksames Mittel gegen die anlasslose Massenüberwachung. Doch das Verschlüsseln von E-Mails ist noch immer nicht selbstverständlich, vor allem deswegen, weil die Anwendungen wenig benutzungsfreundlich sind. Die „Volksverschlüsselung“ ist eine Initiative des Fraunhofer SIT, das kostenlos eine Client-Software ausgibt, die den Nutzer durch den gesamten Prozess von Identitätsnachweis, Schlüsselgenerierung, Zertifizierung und Integration der Schlüssel in die Anwendungen führt. Die Software und Infrastruktur der Volksverschlüsselung kann zukünftig auch Lösungen für Unternehmen und Behörden bieten. Zudem entwickelt das BMBF-geförderten Forschungsprojekt „VVV - Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln“ ein Verfahren zum Auffinden authentischer Schlüsselverzeichnisse auf Basis von E-Mail-Adressen, so dass die E-Mail-Anwendungen die Schlüssel der gewünschten Kommunikationspartner leicht ermitteln können.

Kurz-Vita



Ulrich Waldmann hat an der Technischen Universität Darmstadt Informatik studiert und ist zertifizierter IT-Grundschutzexperte (TÜV). Seit 2002 ist er als wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie in der Abteilung „Cloud Computing, Identity and Privacy“ insbesondere in Projekten zu SmartCards, Cloud-Sicherheit und Selbstschutz tätig. Zusammen mit Annika Selzer leitet er öffentlich geförderte Forschungsprojekte wie „VeriMetrix“ (2014-2016), in welchem Datenschutzkennzahlen für das Cloud-Umfeld entwickelt wurden, und „VVV - Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln“ (2016-2018), ein Projekt, das die DNSSEC-gestützte Veröffentlichung von Schlüsseln realisiert. Er ist Teammitglied der „Volksverschlüsselung“, einer Initiative des Fraunhofer SIT zur Generierung und Zertifizierung von Schlüsseln, insbesondere für die private E-Mail-Kommunikation

Kontakt

Ulrich Waldmann, Fraunhofer SIT
Cloud Computing, Identity & Privacy (CIP)
Rheinstr. 75, 64295 Darmstadt
Tel.: 06151-869-222
E-Mail: ulrich.waldmann@sit.fraunhofer.de
Webseite: www.sit.fraunhofer.de