DATENSCHUTZPRAXIS

DIE VERTRAUENSWÜRDIGE VERTEILUNG VON VERSCHLÜSSELUNGSSCHLÜSSELN ALS HEMMSCHUH DER E-MAIL-VERSCHLÜSSELUNG – EIN LÖSUNGSANSATZ[1]

Stephan Blazy, Susan Gonscherowski,
Thomas Kunz, Annika Selzer, Ulrich Waldmann

1. Was ist das Problem?

Möchte der Sender einer E-Mail eine Information verschlüsselt an den E-Mail-Empfänger senden, so benötigt der Sender den öffentlichen Schlüssel des Empfängers in Form eines digitalen Zertifikats (im Folgenden: Zertifikat). Ein Zertifikat bescheinigt die Vertrauenswürdigkeit eines öffentlichen Schlüssels und enthält neben dem öffentlichen Schlüssel i. d. R. auch personenbezogene Daten, wie z. B. den Namen und die E-Mail-Adresse des Zertifikatinhabers.[2] Mit dem öffentlichen Schlüssel wird die Information verschlüsselt, d. h. in einen Geheimtext überführt, dann an den Empfänger versandt und mit Hilfe seines privaten Schlüssels wieder in den Klartext versetzt bzw. entschlüsselt. Die Sicherheit des Verfahrens hängt dabei auch vom verantwortungsvollen Umgang mit dem privaten Schlüssel ab, der - im Gegensatz zum öffentlichen Schlüssel - nur dem Zertifikatsinhaber bekannt sein darf.[3]

Problematisch ist, dass Personen, die über ein kryptographisches Schlüsselpaar verfügen, häufig Schwierigkeiten dabei haben, das Zertifikat ihres Kommunikationspartners aufzufinden. Somit fehlt Personen, die verschlüsselte E-Mails versenden möchten, die grundlegende Information, ohne die eine E-Mail-Verschlüsselung nicht möglich ist.

Um dieses grundlegende Problem der E-Mail-Verschlüsselung zu lösen, arbeitet seit 2016 ein Konsortium aus Industrie und Wissenschaft an dem Projekt „Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln“ (VVV).[4]

2. Wie kann das Problem gelöst werden?

Zertifikate können in so genannten Verzeichnisdiensten abgelegt werden, die eine Art „Telefonbuch“ für Verschlüsselungsschlüssel darstellen. Der Sender einer Information kann in einem solchen Verzeichnisdienst – z. B. durch die Eingabe der E-Mail-Adresse des Empfängers – nachschauen, ob sein gewünschter Kommunikationspartner sein Zertifikat in dem Verzeichnisdienst hinterlegt hat. Die Nutzung von Verzeichnisdiensten stellt Nutzer in der Praxis jedoch vor Probleme. Hinzu kommt, dass die beiden verbreitetsten Verfahren zur E-Mail-Verschlüsselung, S/MIME und OpenPGP, hinsichtlich der eingesetzten Schlüsselformate und Vertrauensmodelle nicht zueinander kompatibel sind. Beide Verfahren sind hinsichtlich der Schlüsselverteilung kompliziert und wenig benutzungsfreundlich.

So stellen S/MIME-Verzeichnisdienste i. d. R. „isolierte Insellösungen“ dar, d. h. sie sind nicht miteinander verbunden und jeder Nutzer kann in seinem E-Mail-Client nur einen einzigen Verzeichnisdienst einstellen. Ist in diesem Verzeichnisdienst das Zertifikat des gewünschten Kommunikationspartners nicht auffindbar, so wird das Zertifikat nicht automatisch in allen weiteren bekannten Verzeichnisdiensten gesucht. Dies ist in etwa vergleichbar mit der Reichweite gedruckter Telefonbücher für einzelne Städte im Gegensatz zu der Onlinevariante eines Telefonbuches, in dem Telefonnummern weltweit gesucht werden können.

Beim OpenPGP-Standard stellt sich wiederum das Problem, dass Verzeichnisdienste zwar untereinander synchronisiert werden, dieser Umstand jedoch u. a. dazu führt, dass ein Zertifikat nicht mehr manuell durch den Nutzer gelöscht werden oder korrigiert werden kann bzw. nicht (gut) überprüfbar ist, ob eine Veröffentlichung tatsächlich von dem Berechtigten selbst autorisiert wurde oder welches der veröffentlichten Zertifikate (noch) aktuell ist.

Diese wenig praktikablen Lösungen sollten durch ein für OpenPGP und S/MIME einheitliches und benutzerfreundliches Verfahren zum Auffinden von Zertifikaten abgelöst werden. Genau dies hat sich das Projekt VVV zum Ziel gesetzt.

3. Wie ist die Lösung technisch ausgestaltet?

VVV macht es möglich, von einer E-Mail-Adresse auf den Speicherort eines dazu gehörigen Zertifikats zu schließen. Jeder Nutzer veröffentlicht sein Zertifikat auf einem Schlüsselserver seines E-Mail-Anbieters. Die Adresse des Schlüsselservers wird auf dem DNS-Server der Mail-Domain in Form eines „Service Resource Records“ hinterlegt. Dieser Resource Record ist mittels DNS Security Extensions“ (DNSSEC) geschützt, konkret durch eine DNSSEC-Signatur des E-Mail-Anbieters, dessen Signaturschlüssel wiederum vom darüber liegenden Domain-Inhaber signiert wurde usw. bis hin zur Signatur der Root-Domain des DNS. Auf diese Weise entsteht eine eindeutige Vertrauenskette von signierten Schlüsseln der Domain-Inhaber auf Basis eindeutiger Instanzen (bestimmt durch die E-Mail-Domain) und einer einzigen Root-Domain. Die E-Mail-Anwendung überprüft die Authentizität der Resource Records durch die Validierung der DNSSEC-Signaturen. Der E-Mail-Anbieter hat die entscheidende Rolle inne, da er für die Zuordnung von den Schlüsseln zu den E-Mail-Adressen der Nutzer bürgt. Damit brauchen die Nutzer nur solchen Instanzen zu vertrauen, denen sie beim Gebrauch von E-Mail-Adressen ohnehin vertrauen: Den Betreibern der grundlegenden Internetdienste (DNS) und den E-Mail-Anbietern.

Die beiden wichtigsten Anwendungsfälle der Schlüsselverteilung sind das Veröffentlichen und das Abrufen von Schlüsseln. Nutzer veröffentlichen mit Hilfe des VVV-Verfahrens ihre eigenen Zertifikate. Sie werden mittels der VVV-Lösung für andere Nutzer automatisch abrufbar, so dass sich alle Nutzer die Schlüssel ihrer Kommunikationspartner leicht beschaffen können.

Veröffentlichung von Schlüsseln: Zur Veröffentlichung des Zertifikats weist der Nutzer gegenüber dem E-Mail-Anbieter nach, dass er auf das E-Mail-Postfach Zugriff hat. Die E-Mail-Anwendung vermittelt die Nutzer-Authentifizierung und sendet nach erfolgreicher Authentifizierung das ausgewählte Zertifikat zur Veröffentlichung an den E-Mail-Anbieter. Der Nutzer muss nun den Besitz des zugehörigen privaten Schlüssels nachweisen. Dazu verschlüsselt der E-Mail-Anbieter mit dem empfangenen öffentlichen Schlüssel einen Verifikationscode. Nach erfolgreicher Entschlüsselung sendet die Anwendung den Verifikationscode an den E-Mail-Anbieter zurück, der den Schlüssel auf einem seiner Schlüsselserver veröffentlicht. Der Nutzer kann ein veröffentlichtes Zertifikat jederzeit aktualisieren oder auch ersatzlos löschen.[5]

Abruf von Schlüsseln: Der Nutzer verfasst in seiner E-Mail-Anwendung eine E-Mail und hat die E-Mail-Verschlüsselung aktiviert. Sobald er eine vollständige E-Mail-Adresse in das Empfängerfeld eingetragen hat, sucht die Anwendung mit der E-Mail-Adresse nach dem entsprechenden Zertifikat des Empfängers. ▶

[1] Dieser Beitrag entstand im Rahmen des Projekts „Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln (VVV)“ (https://keys4all.de), das vom Bundesministerium für Bildung und Forschung unter dem Förderkennzeichen 16KIS0354K gefördert wird.

[2] Es ist jedoch grundsätzlich auch möglich, dass das Zertifikat neben dem öffentlichen Schlüssel lediglich pseudonymisierte Daten wie z. B. eine pseudonyme E-Mail-Adresse enthält. Dieser Fall steht jedoch nicht im Fokus dieser Ausarbeitung.

[3] Herfert/Selzer/Waldmann, Selbstdatenschutz in Zeiten massenhafter E-Mail-Überwachungen, in: BvD-News 01/2016, S. 57-59.

[4] Für nähere Details zu den in diesem Artikel beschriebenen Projektergebnissen vgl. Blazy/Gonscherowski/Selzer, Anforderungen des künftigen europäischen Datenschutzrechts an die vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln und Fischer/Kunz/Lorenz/Waldmann, Verfahren zur vertrauenswürdigen Verteilung von Verschlüsselungsschlüsseln, beides in: Eibl/Gaedke (Hrsg.): INFORMATIK 2017, Lecture Notes in Informatics (LNI), Bonn 2017. Beide Veröffentlichungen können über die Projekt-Webseite www.keys4all.de abgerufen werden.

[5] Das Löschen könnte aus verschiedenen Gründen vom Nutzer gewollt sein, beispielsweise weil der private Schlüssel kompromittiert wurde oder weil der Nutzer mit seiner E-Mail-Adresse nicht mehr in einem offen zugänglichen Verzeichnis stehen möchte. Das Löschen ist also nicht unbedingt mit einem Widerruf des Schlüssels gleichzusetzen.

DATENSCHUTZPRAXIS

Dazu ruft die Anwendung vom DNS-Server des E-Mail-Anbieters des Empfängers den entsprechenden Resource Record ab und überprüft die DNSSEC-Signaturen dieses Records. Konnten die Server-Adressen auf diese Weise verifiziert werden, so ruft die Anwendung anhand der E-Mail-Adressen auf den Schlüssel-Servern die Schlüssel der Empfänger ab. Schließlich wird die E-Mail für die Empfänger verschlüsselt und abgesendet.

4. Was muss die Lösung aus Sicht des Datenschutzes beachten?

Die im VVV-Projekt entwickelte Anwendung stellt dem Nutzer über eine Anwendung die Zertifikate der Kommunikationspartner zur Verfügung. Die im Zertifikat aufgeführten Daten wie Name, Vorname sowie weitere Angaben, etwa Anschrift oder E-Mail-Adresse – OpenPGP erlaubt gar das Einfügen von Gesichtsbildern – stellen personenbezogene Daten dar. Beabsichtigt der E-Mail-Anbieter nun im Rahmen einer Public-Key-Infrastruktur diese Zertifikate zu verwalten und zu verteilen, sind die einschlägigen datenschutzrechtlichen Regelungen zu beachten.

Über die o. g. Anwendung können Inhalte über die Anwendung in Verzeichnisse veröffentlicht und auch aus elektronischen Verzeichnissen abgerufen werden. Es handelt sich entsprechend um einen Telemediendienst, der es dem Nutzer ermöglicht ein Zertifikat in einem Verzeichnis eines E-Mail-Übertragungsdienstes bereitzustellen. E-Mail-Übertragungsdienste gehören zur Kategorie interpersoneller Kommunikationsdienste, wie sie in Art. 2 Abs. 5 im Entwurf der Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation definiert sind. Dieser Definition folgt auch der Entwurf der e-Privacy-VO.

Art. 15 e-Privacy-VO-E befasst sich mit der Regelung öffentlich zugänglicher Verzeichnisse. Die Hinterlegung des einem Endnutzer zugeordneten Zertifikats in ein providerseitiges Verzeichnis und die Möglichkeit der öffentlichen Abfrage dieser Information mit dem Zweck der Kontaktaufnahme fällt in den Anwendungsbereich des Verordnungsentwurfs. Dies hätte zu Folge, dass die E-Mail-Anbieter von dem Nutzer als Betroffenen gem. Art. 15 Abs. 1 e-Privacy-VO-E die ausdrückliche Einwilligung in die Aufnahme des Verzeichnisdienstes einzuholen verpflichtet sind. Neben der Aufnahme erstreckt sich die Einwilligung auch auf die Suchfunktionalitäten, über die der Nutzer im Vorhinein aufzuklären ist. Den Nutzern – unabhängig ob sie nun natürliche oder juristische Personen sind – wird darüber hinaus nach Art. 15 Abs. 4 e-Privacy-VO-E das Recht eingeräumt ihre Zertifikate kostenlos auf ihre Richtigkeit hin zu überprüfen und ggf. zu löschen. Zusätzlich sind eine Fülle von Vorgaben gem. DS-GVO einzuhalten. Hierzu zählen u. a.:

Rechtmäßigkeit der Verarbeitung: Die Zertifikate des Nutzers werden vom Anbieter gespeichert und bei entsprechenden Anfragen an die jeweiligen Kommunikationsteilnehmer übermittelt. Diese Verwaltung der Zertifikate beim Anbieter stellt eine Verarbeitung i. S. d. Art. 4 Nr. 2 DS-GVO dar und muss für eine rechtliche Legitimation einen Tatbestand des Art. 6 Abs. 1 UAbs. 1 DS-GVO erfüllen. Hat der Nutzer einen Account bei einem E-Mail-Anbieter, liegt als Rechtsgrundlage bereits ein Vertrag mit dem Anbieter i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO vor. Das Hochladen des eigenen Zertifikats mit einem vom E-Mail-Anbieter bereitgestellten Verfahren kann in diesem Fall als konkludente Vertragserweiterung angesehen werden, auf welche die Verarbeitung gestützt werden kann. Die Verarbeitung personenbezogener Daten Dritter, z. B. in Form eines signierten Schlüssels, ist jedoch nicht vertraglich erfasst.[6]

Datenminimierung: In den in Art. 5 DS-GVO normierten Grundsätzen der Datenverarbeitung ist in Art. 5 Abs. 1 lit. c DS-GVO die Datenminimierung festgeschrieben. Hiernach muss die Verarbeitung personenbezogener Daten dem Zweck angemessen, erheblich sowie auf das notwendige Maß begrenzt sein.

Datenrichtigkeit und Löschung: Gem. Art. 15 und 16 DS-GVO muss der E-Mail-Anbieter eine Überprüfung („Auskunftsrecht") und Berichtigung („Recht auf Berichtigung") personenbezogener Daten ermöglichen. Korrespondierend normiert Art. 17 Abs. 1 DS-GVO den Anspruch der betroffenen Person auf Löschung ihrer sämtlichen personenbezogenen Daten. Dieses „Recht auf Vergessenwerden" greift in den Fällen, in denen die Daten für die ursprüngliche Zweckerreichung nicht mehr notwendig sind, der Betroffene seine Einwilligung widerruft, die Befristung ausläuft, der Verarbeitung widersprochen wird bzw. diese mit der DS-GVO nicht vereinbar ist.

Informationspflichten: Zu den Informationspflichten eines E-Mail-Anbieters gehören hauptsächlich Aufklärung, Auskunft und Benachrichtigung der Nutzer. Die DS-GVO stellt auf eine umfassende Informiertheit des Betroffenen ab. Die Pflichten des Verantwortlichen gegenüber dem Betroffenen gelten unabhängig davon, ob die Erhebung direkt bei der Person oder an anderer Stelle stattfindet. Jedoch erweitert Art. 14 Abs. 1 und Abs. 2 litt. a-d DS-GVO in diesem Fall den Umfang der Informationspflichten.

Datensicherheit: Die E-Mail-Anbieter müssen auch für die Sicherheit der ihnen überantworteten personenbezogenen Zertifikatsinformationen Sorge tragen. Den Rahmen hierfür geben Art. 5 Abs. 1 lit f und Art. 32 DS-GVO vor.

Nachweis-/Rechenschaftspflichten und Haftung der E-Mail-Anbieter: Art. 82 Abs. 2 DS-GVO besagt: Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechenden Verarbeitung verursacht wurde.[7] In Art. 5 Abs. 2 DS-GVO legt der Gesetzgeber ausdrücklich fest, dass der Verantwortliche die Einhaltung der Bestimmungen aus Art. 5 Abs. 1 DS-GVO nachweisen können muss. Entsprechend dieser Gesetzeslage kann eine betroffene (natürliche) Person Schadenersatz verlangen, wenn der E-Mail-Anbieter nicht nachweisen kann, dass die Verarbeitungsgrundsätze der Verordnung eingehalten wurden. Zu den Nachweispflichten gegenüber der Aufsichtsbehörde zählen die Verfahrensnachweise bzw. Datenschutz-Folgenabschätzungen (Art. 35 DS-GVO) und Meldungen von Verletzungen des Schutzes personenbezogener Daten gem. Art. 33 DS-GVO. Mit Art. 24 DS-GVO erfolgt eine Umkehrung der Beweislast zu Gunsten des Betroffenen.

5. Wie ist der Stand der Umsetzung?

Das Projekt „Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln" (VVV) wird unter der Leitung von Fraunhofer SIT gemeinsam mit der Universität Kassel (provet), der Universität der Künste Berlin, mailbox.org und dem Unabhängigen Landeszentrum für Datenschutz (ULD) bearbeitet.

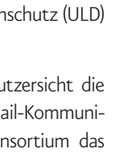
Da die E-Mail-Anwendung aus Nutzersicht die zentrale Komponente der E-Mail-Kommunikation ist, implementiert das Konsortium das VVV-Verfahren derzeit beispielhaft in Form einer Erweiterung (Plugin) der E-Mail-Anwendung Thunderbird und nutzt die DNS- und Schlüsselserver des E-Mail-Anbieter mailbox.org. Gemeinsam mit mailbox.org führt das Fraunhofer SIT die Implementierungsarbeiten durch und verantwortet darüber hinaus die IT-Sicherheit des VVV-Verfahrens. Die Projektgruppe provet der Universität Kassel und das Unabhängige Landeszentrum für Datenschutz begleiten das Projekt aus verfassungsrechtlicher sowie datenschutzrechtlicher Sicht. Die Universität der Künste bezieht unterschiedliche Nutzergruppen in allen Phasen des Entwicklungsprozesses mit ein, um Anforderungen für das Bedienkonzept des Plugins zu ermitteln.

Über die Autoren

Stephan Blazy
Universität Kassel (Provet)
▶ s.blazy@uni-kassel.de

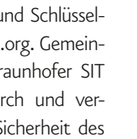
provet

Susan Gonscherowski
Unabhängiges Landeszentrum für Datenschutz
▶ sgonscherowski@datenschutzzentrum.de

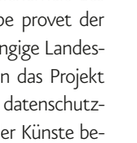


ULD

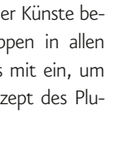
Thomas Kunz
Fraunhofer SIT, Darmstadt
▶ thomas.kunz@sit.fraunhofer.de



Annika Selzer
Fraunhofer SIT, Darmstadt
▶ annika.selzer@sit.fraunhofer.de



Ulrich Waldmann
Fraunhofer SIT, Darmstadt
▶ ulrich.waldmann@sit.fraunhofer.de



Fraunhofer SIT

[6] Mommers, BGH präzisiert Zulässigkeit von Deep-Links, in: DFN-Infobrief Recht 1/11, 2011.

[7] Die Haftung in der e-Privacy-VO-E ist in Art. 22 geregelt und verweist auf die Ausnahmetatbestände des Art. 82 DS-GVO.