Michael Herfert, Annika Selzer, Ulrich Waldmann

Laientaugliche Schlüsselgenerierung für die Ende-zu-Ende-Verschlüsselung

Schlüssel für alle durch die Volksverschlüsselung

Mehr als dreißig Jahre sind seit der Erfindung asymmetrischer Verschlüsselungsverfahren vergangen, und noch immer finden jene kryptographischen Verfahren längst nicht überall dort Anwendung, wo sie z. B. vor Massenüberwachung schützen könnten. Wichtige Ursachen dafür sind insbesondere Schwierigkeiten bei der Verbreitung von Verschlüsselungsschlüsseln sowie die fehlende Benutzerfreundlichkeit existierender Lösungen. Vor diesem Hintergrund stellt dieser Beitrag die Volksverschlüsselung vor, die eine laientaugliche und sichere Schlüsselgenerierung, Zertifizierung und automatische Integration der Schlüssel in die Anwendungen vorsieht.

Michael Herfert

Leiter der Abteilung Cloud Computing & Identity und Privacy am Fraunhofer SIT

E-Mail: michael.herfert@sit.fraunhofer.de

Annika Selzer

Wissenschaftliche Mitarbeiterin am Fraunhofer-Institut für sichere Informationstechnologie.

E-Mail: annika.selzer@sit.fraunhofer.de

Ulrich Waldmann

Wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie.

E-Mail: ulrich.waldmann@sit.fraunhofer.de

1 Hintergrund

1.1 Massenüberwachung

Spätestens seit Edward Snowden im Jahr 2013 Informationen über die weltweiten Überwachungspraktiken der „Five Eyes", also der Geheimdienste Australiens, Neuseelands, Kanadas, Großbritanniens und der USA veröffentlichte, wissen wir, dass große Teile der weltweiten Onlinekommunikation überwacht werden. Von der Überwachung betroffen sind u. a. E-Mails, Bilder und Videos, die über das Internet geteilt werden. Unter der Bevölkerung löste das Bekanntwerden dieser Überwachungspraktiken großes Unbehagen aus, so dass sich konsequenterweise viele Bürger fragen, wie sie sich vor Massenüberwachungen durch Geheimdienste schützen können [1].

Das Gefühl, sich unbeobachtet im Internet zu bewegen, bildet die Grundlage für eine selbstbestimmte und freie Nutzung und Kommunikation im Internet, wohingegen das Gefühl von Überwachung auf Dauer zu einem gehemmten und angepassten Verhalten führen kann. Diese fatalen Auswirkungen gilt es durch technische und organisatorische Maßnahmen aufzuhalten.

Vor allem technische Lösungen wie z. B. E-Mail-Verschlüsselung, sichere Instant-Messaging-Dienste sowie Anonymisierungsnetzwerke können den Bürgern die Freiheit und Selbstbestimmung im Internet wiedergeben [2]. Für eine wirklich geschützte E-Mail-Kommunikation sollte unbedingt das Konzept der Ende-zu-Ende-Verschlüsselung zur Anwendung kommen. Denn nur dieses stellt sicher, dass ausschließlich der gewünschte Empfänger die Nachricht im Klartext lesen kann, keinesfalls zwischengeschaltete Instanzen wie Router oder Mailserver. Dies impliziert, dass allein Sender und Empfänger über die Schlüssel verfügen, um die Nachricht zu entschlüsseln. Dritte dürfen die

Schlüssel weder besitzen noch die Möglichkeit haben, sie mit begrenztem Aufwand zu errechnen.

1.2 Mangelnde Verbreitung von Schlüsseln

Obwohl die Konzepte der Verschlüsselung lange bekannt sind, besitzen nur wenige Menschen kryptographische Schlüssel, die für eine verschlüsselte E-Mail-Kommunikation auf Basis von PGP/GnuPG oder S/MIME Voraussetzung sind. Gründe für den Mangel an Schlüsseln liegen zum einen in der mangelnden Benutzungsfreundlichkeit der Anwendungen, in denen kryptographische Schlüssel verwendet werden, zum anderen in der Komplexität der Public-Key-Infrastrukturen (PKIs), die notwendig sind, um Schlüssel eindeutig mit Personen zu verknüpfen und diese Informationen, z. B. mit Hilfe von digitalen Zertifikaten, allen Kommunikationspartnern zugänglich zu machen. Der einzelne Nutzer kann sich in der Regel nur bestehenden Infrastrukturen (z. B. eines großen Unternehmens oder einer anderen Organisation) anschließen, denen er selbst angehört. Vorhandene Schlüssel werden dann hauptsächlich für interne Anwendungen und Anmeldevorgänge eingesetzt, kaum für die Kommunikation mit externen Partnern, da die PKIs verschiedener Organisationen nicht per se vernetzt sind. Kleinere Unternehmen können sich meist keine eigene PKI leisten und Privatnutzer wissen in der Regel nicht, wie sie Schlüssel erzeugen und wo sie entsprechende Zertifikate beziehen können. Sie können die Sinnhaftigkeit und Seriosität von Zertifizierungsdiensten nur schwierig einschätzen und sind daher selten bereit, für Zertifikate Geld auszugeben.

1.3 Fehlende Laientauglichkeit

Die meisten potentiellen Nutzer wissen nicht, wie sie Schlüssel und Zertifikate generieren, verwalten und nutzen können [3]. Für die Verschlüsselung von E-Mails müssen sich Nutzer in der Regel zunächst darüber verständigen, welches Verfahren sie dafür verwenden möchten, da die beiden Standards S/MIME und PGP/GnuPG hinsichtlich Zertifikaten und Vertrauensmodellen nicht miteinander kompatibel sind.

So verwendet S/MIME X.509-Zertifikate von hierarchisch organisierten öffentlichen Zertifizierungsstellen („hierarchische PKI“). Die Nutzer müssen sich vorab ihre Zertifikate mitteilen oder ihre Anwendungen so konfigurieren, dass der richtige Verzeichnisdienst zum Auffinden der gewünschten Zertifikate eingetragen ist. Beides ist in der Praxis umständlich, und die Nutzer müssen ihre E-Mail-Anwendung entsprechend selbst konfigurieren.

Bei vorliegenden X.509-Zertifikaten haben die Kommunikationspartner zudem das Problem, eindeutig zu überprüfen, ob ein bestimmter Verschlüsselungsschlüssel wirklich zu dem gewünschten Kommunikationspartner gehört. Der Nutzer muss der Instanz, welche das Zertifikat erstellt hat, vertrauen, obwohl es per se nicht klar ist, wie und warum er der digitalen Signatur einer ihm wahrscheinlich unbekannten Zertifizierungsstelle vertrauen sollte. Zur Lösung dieses Problems werden zurzeit Wurzelzertifikate als Vertrauensanker verwendet, mit denen vollständige Zertifikatsketten geprüft werden können. Viele Anwendungen haben solche Wurzelzertifikate integriert. Die Auswahl dieser Vertrauensanker kontrolliert der Nutzer jedoch in der Regel nicht selbst, da dies sehr aufwändig ist und Wissen über die dahinter liegenden Konzepte voraussetzt.

Während S/MIME von den meisten Programmen unterstützt wird, muss für PGP/GnuPG zusätzliche Software (z. B. Enigmail für Mozilla Thunderbird) installiert werden. Die Nutzer müssen sich gegenseitig ihre Schlüssel signieren (*Web of Trust*). Sie können sich die Schlüssel gegenseitig mitteilen und auch auf Schlüsselservern veröffentlichen. Dabei verlieren sie allerdings die Kontrolle darüber, wer die veröffentlichten persönlichen Daten für welche Zwecke verwendet, wer den öffentlichen Schlüssel signiert und ob unter dem gleichen Namen evtl. weitere Schlüssel hochgeladen werden. Die authentische Herkunft von Signaturen ist oftmals fraglich [4]. Die Daten können zudem weder gelöscht noch nachhaltig gesperrt werden.

Untersuchungen zur Benutzbarkeit von E-Mail-Verschlüsselung zeigen, dass nur wenige Nutzer wissen, wie man die Schlüssel verwendet, ohne dabei Fehler zu begehen [3, 5]. Empfohlen wird, dass eine Sicherheitssoftware den Nutzer an den Schlüsselprozessen beteiligt, um das Bewusstsein für Sicherheit zu erhöhen und Rückmeldungen gibt, zugleich aber keine schwerwiegenden Nutzungsfehler zulässt. Sicherheit sollte so einfach wie möglich gestaltet sein, ohne beim Nutzer das Lesen von Tutorials vorauszusetzen.

Die Webmail-Anbieter GMX und Web.de bieten mit dem Browser-Plugin Mailvelope eine benutzungsfreundliche Lösung, um PGP-Schlüssel für den Schutz von Webmails zu erzeugen und zu nutzen. Die PGP-Schlüssel werden lokal im Browser verwaltet, stehen jedoch nicht per se beliebigen E-Mail-Anwendungen zur Verfügung. Die Nutzer müssen zudem über einen GMX oder Web.de-Mailaccount verfügen.[1]

2 Die Volksverschlüsselung

Aus den genannten Gründen ist bisher keinem nationalen oder privatwirtschaftlichen Projekt zur Propagierung von Verschlüsselung eine flächendeckende Schlüsselverteilung gelungen. Die Volksverschlüsselung (kurz: VV) ist eine Initiative des Fraunhofer SIT und verfolgt das Ziel, kostenlos alle Privatnutzer, die ihre E-Mail-Kommunikation verschlüsseln möchten, mit kryptographischen Schlüsseln zu versorgen. Die Volksverschlüsselung besteht aus zwei Teilen: Einer zentralen Infrastruktur (VV-Server) für die Identitätsprüfung der Nutzer und die Zertifizierung kryptographischer Schlüssel und einer Client-Software (VV-Software) zur lokalen Erzeugung und automatischen Integration der Schlüsseln in solche Anwendungen, die der Anwender ohnehin benutzt. Die Prozesse der Schlüsselgenerierung und Schlüsselverteilung sollen derart vereinfacht werden, dass selbst IT-Sicherheitslaien problemlos damit zurechtkommen und schließlich die Schlüssel wirklich für die Ende-zu-Ende-Verschlüsselung von E-Mails einsetzen.

Die Volksverschlüsselung nutzt Public-Key-Kryptografie in einer Weise, dass die folgenden Schritte für den Nutzer leicht ausführbar sind. Der Nutzer lädt sich die VV-Software herunter und führt sie aus. Die Software führt den Nutzer durch den gesamten Prozess.

- **Identitätsprüfung des Nutzers:** Die VV-Software fordert den Nutzer auf, seine Identität gegenüber dem VV-Server nachzuweisen. Der Nutzer kann wählen, ob er dazu die Online-Ausweisfunktion des neuen Personalausweises verwendet, seinen

1 Verschlüsselung mit OpenPGP für Webmail: www.mailvelope.com

Festnetz-Account bei der Deutschen Telekom oder einen Registrierungscode, den er bei einer persönlichen Vor-Ort-Identifikation[2] erhalten hat. Jedes dieser Verfahren liefert Namen und Vornamen des Nutzers, die im nächsten Schritt mit einer E-Mail-Adresse des Nutzers verknüpft werden, aus einer sicheren Quelle.

- **Verifikation der E-Mail-Adresse:** Die VV-Software stellt die auf dem PC gefundenen E-Mail-Accounts zur Auswahl. Der Nutzer wählt daraus eine Adresse oder gibt eine andere Adresse ein, für die das Zertifikat ausgestellt werden soll. Der Server sendet einen Verifikationscode an die ausgewählte Adresse. Der Nutzer bestätigt den Empfang der E-Mail über den Verifikationscode, den er in die VV-Software eingibt.
- **Schlüsselerzeugung durch den Nutzer**: Die VV-Software erzeugt automatisch das kryptographische Schlüsselpaar für die Verschlüsselung von E-Mails.[3] Der private Schlüssel verbleibt ausschließlich im privaten Kontrollbereich des Nutzers (in der Regel im geschützten Zertifikatsspeicher des Betriebssystems oder der Anwendungen).
- **Bindung des öffentlichen Schlüssels an die Identität des Nutzers**: Der Server zertifiziert den öffentlichen Schlüssel zusammen mit dem Namen, dem Vornamen und der E-Mail-Adresse und sendet das Zertifikat an die VV-Software.
- **Integration des Schlüsselpaares in die Anwendungsprogramme**: Die VV-Software konfiguriert auf Wunsch des Nutzers automatisch Mailtools und Browser, so dass das Schlüsselpaar anschließend unmittelbar genutzt werden kann.

Die persönliche Vor-Ort-Identifikation des Nutzers (vgl. den oben genannten Schritt 1) wird durch das Fraunhofer SIT angeboten, um auch Menschen, die weder die Online-Ausweisfunktion des Personalausweises nutzen noch einen Telekom-Account besitzen, die Identifikation zu ermöglichen. Auf Messen und weiteren Veranstaltungen kann sich jeder für die Volksverschlüsselung registrieren, der sich mit Personalausweis oder Reisepass ausweisen kann. Gegen Vorlage des Ausweisdokuments und nach Erfassung des Vor- und Nachnamens sowie der E-Mail-Adresse stellt das Fraunhofer SIT eine Karte mit einem 12stelligen Registrierungscode aus (Abb. 1). Mit dieser Kennung kann sich der zu Registrierende später an seinem PC mittels VV-Software gegenüber der Volksverschlüsselung authentisieren.

Die zentrale Infrastruktur stellt weitere Dienste zur Verfügung, die ebenfalls durch die VV-Software vermittelt werden. Dazu gehören auf Wunsch des Nutzers die Veröffentlichung der Zertifikate in einem Verzeichnisdienst (LDAP), damit andere Nutzer die öffentlichen Schlüssel finden können, und ein Validierungsdienst (OCSP), damit die Zertifikatsgültigkeit überprüft werden kann. Der Nutzer kann über die VV-Software Schlüssel exportieren und importieren und die Zertifikate verloren gegangener Schlüssel sperren lassen.

Bisher werden X.509-Zertifikate (für S/MIME) unterstützt. Fraunhofer SIT arbeitet an Erweiterungen, unter anderem für PGP/GnuPG, sowie an einer sicheren Übergabe der Schlüssel vom Desktop-Computer an Mobilgeräte. Da der Quellcode veröffentlicht wird, können sich auch unabhängige Experten von der korrekten Implementierung der Funktionen überzeugen. Durch

2 So geschehen am Fraunhofer-Stand auf der CeBIT 2016. Weitere Termine werden unter www.volksverschluesselung.de bekannt gegeben.

3 Außerdem werden jeweils ein Schlüsselpaar für Authentisierung und fortgeschrittene Signatur erzeugt, auf die im Folgenden jedoch nicht weiter eingegangen wird.

Abb. 1 | Beispiel eines Registrierungscodes

das offene Kommunikationsprotokoll ist die Volksverschlüsselung offen für alternative Clients und für die Anbindung weiterer kryptographischer Anwendungen und PKIs. Geplant ist die Erweiterung um die Identifizierung von neuen Nutzern mit bereits existierenden Schlüsseln.

3 Schlüsselverzeichnis

Die VV-Software ermöglicht es den Nutzern, ihre öffentlichen Schlüssel in Form eines digitalen Zertifikats für potenzielle Sender über einen Verzeichnisdienst abrufbar zu machen. Ein solcher Verzeichnisdienst birgt sowohl Chancen als auch Risiken, die im Folgenden diskutiert werden sollen.

3.1 Chancen & Risiken von Verzeichnisdiensten

Ein Sender, der eine verschlüsselte Nachricht an einen Empfänger schicken möchte, benötigt dessen öffentlichen Schlüssel. Um diesen zu ermitteln, stellt die Volksverschlüsselung einen Verzeichnisdienst zur Verfügung. Die VV-Software bietet jedem Nutzer an, dass sein Verschlüsselungsschlüssel in diesen Verzeichnisdienst eingestellt wird. Wenn der Nutzer zustimmt, haben Sender es leicht, ihm eine verschlüsselte Nachricht zu schicken, denn sie können den Schlüssel mit der E-Mail-Adresse des Empfängers als Suchkriterium abrufen. Wenn der Nutzer nicht zustimmt, muss er sich selber darum kümmern, dass potentielle Sender auf seinen Schlüssel zugreifen können. Der Verzeichnisdienst sorgt somit nicht nur für eine vereinfachte Nutzbarkeit der VV-Software sondern auch für eine schnelle und unkomplizierte Verbreitung verschlüsselter Kommunikation als eine wichtige Maßnahme zum Selbstdatenschutz.

Den Chancen von Verzeichnisdiensten stehen jedoch auch Risiken gegenüber, vgl. [6, 7], die sich aus dem Personenbezug der abrufbaren Daten ergeben und unter das Datenschutzrecht fallen. So können Verzeichnisdienste u. a. eine Profilbildung über das Nutzerverhalten ermöglichen: Schnell aufeinander folgende Anfragen von einer IP-Adresse können einem Client zugewie-

sen werden. Dadurch kann sich ein Verzeichnisdienst u. a. merken, welche Personen oder Gruppen von Menschen miteinander kommunizieren.[4] Darüber hinaus können Verzeichnisdienste durch gezielte Massenabfragen für geschäftliche Zwecke missbraucht werden, wie insbesondere für den E-Mail-Adresshandel.

Um diesen und weiteren Risiken vorzubeugen stellen die geltenden Datenschutzgesetze Anforderungen an die Verarbeitung personenbezogener Daten. U. a. ist für die Verarbeitung personenbezogener Daten eine gesetzliche Erlaubnisnorm oder die Einwilligung der Betroffen erforderlich. Darüber hinaus hat die Verarbeitung personenbezogener Daten zweckgebunden, auf das erforderliche Maß beschränkt und datensparsam zu erfolgen. Des Weiteren muss es Betroffenen ermöglicht werden, die über sie gespeicherten Daten einzusehen, berichtigen und löschen (bzw. sperren) zu lassen. Verantwortliche Stellen bzw. Auftragsdatenverarbeiter haben technische und organisatorische Schutzmaßnahmen zu treffen, wenn deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Die zu treffenden Maßnahmen sollten insbesondere den o. g. Risiken entgegenwirken.[5]

In Bezug auf den Verzeichnisdienst setzt die Volksverschlüsselung diese Anforderungen u. a. dadurch um, dass der öffentliche Schlüssel nur dann über den Verzeichnisdienst der Volksverschlüsselung veröffentlicht wird, wenn der jeweilige Betroffene zuvor wirksam in die Veröffentlichung eingewilligt hat. Die Volksverschlüsselung hat sich hierbei zum Ziel gesetzt, die Betroffenen ausführlich und allgemein verständlich aufzuklären und auf mögliche Risiken hinzuweisen. Die im Falle einer erteilten Einwilligung veröffentlichten Daten sind darüber hinaus auf das für die Funktion des Verzeichnisdiensts notwendige Maß beschränkt und werden nur auf Servern in Deutschland[6] gespeichert. Ändert der Betroffene nach einer einmal erteilten Einwilligung in die Veröffentlichung seine Meinung, kann er seine Einwilligung widerrufen. In diesem Fall wird der öffentliche Schlüssel aus dem Verzeichnisdienst gelöscht. Bereits in der Einwilligung zur Veröffentlichung wird der Betroffene darauf hingewiesen, dass die Volksverschlüsselung im Falle des Widerrufs nicht die Verpflichtung hat, etwaig auf anderen Servern gespeicherte Daten – z. B. von Suchmaschinen – zu löschen oder löschen zu lassen. Technische und organisatorische Maßnahmen werden getroffen, um u. a. gezielten Massenabfragen zu geschäftlichen Zwecken soweit möglich entgegenzuwirken. Dies wird u. a. dadurch realisiert, dass der Verzeichnisdienst nur bei Kenntnis der gesamten E-Mail-Adresse eine Antwort gibt, auf eine Anfrage maximal ein Ergebnis zurückgegeben wird und nach einer geringen Anzahl von Suchanfragen ein Timeout die Weitersuche verzögert.

3.2 Zusammenspiel mehrerer Verzeichnisdienste

Der Verzeichnisdienst der Volksverschlüsselung wird durch einen LDAP-Server implementiert. Das *Lightweight Directory Access Protocol* (LDAP) ist durch die RFCs 4510 bis 4519 definiert. Gängige Mailprogramme, darunter Microsoft Outlook und Thunderbird, beherrschen das Protokoll und sind in der Lage, lokal nicht bekannte Schlüssel automatisch aus dem Verzeichnisdienst abzurufen. Das ist eine recht komfortable Funktion, denn im Idealfall merkt der Nutzer davon nichts.

Schwieriger wird die Situation, wenn ein Nutzer schon einen Verzeichnisdienst konfiguriert hat, bevor er Kunde der Volksverschlüsselung wird, zum Beispiel weil er einem Unternehmen angehört, welches über eine eigene Public-Key-Infrastruktur mit einem eigenen Verzeichnisdienst verfügt. Die Mailtools können zwar mehrere Verzeichnisdienste verwalten, aber zu einer Zeit ist nur einer aktiv. Noch komplizierter wird es, wenn der Sender eine Nachricht an mehrere Empfänger schicken will und diese sich in verschiedenen Infrastrukturen befinden, die jeweils einen eigenen Verzeichnisdienst betreiben.

Am einfachsten wäre, wenn die Mailprogramme mehrere Verzeichnisdienste gleichzeitig benutzen könnten. Ob und wann dies der Fall sein wird, ist ungewiss. Aus einer pragmatischen Sicht ist eine Lösung wünschenswert, die sofort einsetzbar ist. Das LDAP-Protokoll bietet für diesen Zweck zwei Mechanismen, ein dritter Mechanismus kann protokollunabhängig benutzt werden:

- **Durch den Referal-Mechanismus** kann ein LDAP-Server, der eine Anfrage nicht beantworten will oder kann, eine Menge von *Universal Ressource Identifiers* (URIs) zurückliefern. Jeder davon verweist auf einen LDAP-Server, der die Anfrage möglicherweise beantworten kann. Es ist die Aufgabe des Clients, diesen Hinweisen zu folgen und dabei darauf zu achten, dass er sich nicht in einer Schleife (A verweist auf B und B verweist auf A) verfängt.
- **Durch den Continuation-Reference-Mechanismus** kann ein LDAP-Server, der schon Ergebnisse gefunden hat, auf weitere LDAP-Server hinweisen, welche die Ergebnisse erweitern könnten. Auch dieser Hinweis geschieht durch eine Menge von URIs.
- **Durch den Chaining-Mechanismus**, der nicht Bestandteil des LDAP-Protokolls ist, können einige Implementierungen von LDAP-Servern selbständig Anfragen bei anderen Servern stellen, wenn sie selbst die Anfrage nicht oder nur teilweise beantworten können. Für den Client ist das transparent.

Mechanismus 1 erlaubt den Clients sehr viel Kontrolle, hat aber den Nachteil, dass die korrekte Funktionsweise davon abhängig ist, dass alle Clients die gelieferten URIs korrekt auswerten. Mechanismus 2 kommt für die Volksverschlüsselung nicht in Frage, weil der Verzeichnisdienst so konfiguriert ist, dass er entweder exakt eine Antwort liefert oder gar keine.

Mechanismus 3 hat den Nachteil, dass der aufrufende Client nicht genau weiß, aus welcher Quelle seine Antwort stammt. Diese Transparenz ist jedoch zugleich der entscheidende Vorteil, denn sie führt dazu, dass sie Client-unabhängig funktioniert. Für die Akzeptanz ist es wichtig, dass sich alle beteiligten Server bezüglich der Qualität ihrer Daten auf einem Niveau befinden. Diese Forderung muss transitiv gelten, denn auch die angefragten Server könnten wiederum andere Server anfragen. Es ist Aufgabe der Server dafür zu sorgen, dass kein Kreisbezug entsteht, bzw. dass ein solcher entdeckt wird.

In der ersten Version der Volksverschlüsselung wird der Verzeichnisdienst keine der drei Mechanismen nutzen, sondern wie die meisten anderen Server nur seine eigenen Daten ausliefern. In späteren Versionen erscheint Mechanismus 3 geeignet, verschiedene Infrastrukturen zu verbinden. Durch Variationen der Anfrage oder indem man von der optionalen Möglichkeit Gebrauch

4 Profilbildungen jeder Art sind im Rahmen der Volksverschlüsselung durch die *Fraunhofer SIT Certificate Policy* ausdrücklich ausgeschlossen.

5 Für eine ausführliche Beschreibung der datenschutzrechtlichen Grundprinzipien vgl. u. a. [8, 9].

6 Diese Aussage ist beschränkt auf Verarbeitungsprozesse des VV-Verzeichnisdienstes. Sobald die öffentlichen Schlüssel über den Verzeichnisdienst abgerufen wurden, können Dritte diese auch außerhalb Deutschlands verarbeiten.

macht, dass sich ein Client authentifiziert, könnte der Verzeichnisdienst sogar individuell an einen Anfrager oder an Gruppen von Anfragern angepasst werden.

Wenn durch die Volksverschlüsselung und andere Initiativen Schlüssel und damit auch Verzeichnisdienste an Bedeutung gewinnen, ist hier sicherlich eine ganze Reihe von Variationen zu erwarten. Für die Zukunft wird es daher wichtig sein, dass sich Verzeichnisdienstanbieter auf die Möglichkeit der gegenseitigen Anfrage bzw. des Referenzierens einerseits sowie auf eine einheitlich starke Authentifizierung ihrer Nutzer andererseits verständigen. Letzteres ist notwendig, um den Anfragenden, der seine Anfrage z. B. bei dem Verzeichnisdienst der Volksverschlüsselung stellt und dessen Anfrage an andere Verzeichnisdienste weitergeleitet wird, bzgl. der von der Volksverschlüsselung erwarteten starken Authentisierung ihrer Nutzer nicht in einer falschen Gewissheit zu wiegen.

4 Ausblick

Langfristig wäre der Ersatz der Schlüsselserver und Zertifikatsverzeichnisse, die nicht leicht zu überschauende Insellösungen darstellen, durch ein einheitliches und benutzungsfreundliches Verfahren zum Auffinden und Prüfen öffentlicher Schlüssel wünschenswert. Dazu kann das Domain Name System (DNS) dienen, das mittels DNS Security Extensions (DNSSEC) die Herkunft von DNS-Daten und auch weiteren Daten kryptografisch absichern kann. Auf Grundlage von DNSSEC kann der Verwalter einer Domain mittels des so genannten DANE-Protokolls (DNS-Based Authentication of Named Entities) beispielsweise die zur Domain gehörenden E-Mail-Adressen an die öffentlichen Schlüssel der Nutzer binden, indem entsprechende Schlüsselinformationen auf den DNS-Servern abrufbar sind [10].

Die Volksverschlüsselung und andere Initiativen fördern den Selbstdatenschutz. Nutzer können damit im Sinne von Fernmeldegeheimnis und informationeller Selbstbestimmung die Vertraulichkeit ihrer Kommunikation besser schützen, bestenfalls ohne sich persönlich um das zugrunde liegende Vertrauensmodell kümmern zu müssen. Darüber hinaus sollte auch die Bundesregierung darauf hinwirken, dass die Ende-zu-Ende-Verschlüsselung in Zukunft so selbstverständlich und nutzerfreundlich sein wird, dass man sie als Bürger nicht einmal mehr bemerkt. Hierzu könnte eine stärkere Förderung der Entwicklung neuer Schutzmaßnahmen durch die Bundesregierung beitragen, um damit jedem Bürger zu ermöglichen, seine Daten wirksam zu schützen.

Literatur

[1] Michael Herfert / Michael Waidner: *Privatsphärenschutz und Vertraulichkeit im Internet*. Trend- und Strategiebericht des Fraunhofer SIT, 2013.

[2] Murat Karaboga / Philipp Masur / Tobias Matzner et. al.: *Selbstdatenschutz*, Whitepaper des „Forum Privatheit", 2014.

[3] Broderick Sheng / Hyland Koranda: *Why Johnny still can't encrypt: evaluating the usability of email encryption software*, CMU, Berkeley University, 2006.

[4] Jürgen Schmidt: *Lasst PGP sterben*, Heise Medien, 2015.

[5] Tygar Whitten: *Why Johnny can't encrypt: a usability evaluation of PGP 5.0*, CMU, Berkeley University, 1999.

[6] Arbeitskreis: Technische und organisatorische Datenschutzfragen: *Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten*, 2000.

[7] Landesbeauftragter für den Datenschutz Sachsen-Anhalt: *Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt* vom 01.04.1999-31.03.2001.

[8] Jürgen Kühling / Christian Seidel / Anastasios Sivridis: *Datenschutzrecht*, 2008.

[9] Marie-Theres Tinnefeld / Benedikt Buchner / Thomas Petri: *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, 2012.

[10] Carsten Strotmann: *Hilfestellung – Wie DNSSEC und DANE die Mail-Verschlüsselung erleichtern*, in: c´t 2015 Heft 8, S. 154-155.