Maximilian Eibl, Martin Gaedke. (Hrsg.): INFORMATIK 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 773

Die Volksverschlüsselung: Förderung vertrauenswürdiger Ende-zu-Ende-Verschlüsselung durch benutzerfreundliches Schlüssel- und Zertifikatsmanagement

Dominik Spychalski[1] Levona Eckstein[1] Michael Herfer[1] Daniel Trick[1] Tatjana Rubinstein[2]

Abstract: Obwohl schon seit Jahren standardisierte sichere Verschlüsselungsverfahren existieren und diese auch von den meisten E-Mail-Anwendungen unterstützt werden, hat sich vertrauenswürdige Ende-zu-Ende-Verschlüsselung in der E-Mail-Kommunikation bis heute noch nicht flächendeckend etabliert. Als Ursachen für die geringe Nutzung werden u.a. die für viele Nutzer zu komplizierten und wenig benutzerfreundlichen Prozesse zur Schlüsselbeschaffung und zur Einrichtung der genutzten Anwendungen genannt. Dieser Beitrag beschreibt die Lösung der Volksverschlüsselung, die alle Prozesse zur Erzeugung und Zertifizierung von kryptografischen Schlüsseln sowie deren Integration in bestehende Anwendungen automatisiert durchführt und einfach zu bedienen ist.

Keywords: Ende-zu-Ende-Verschlüsselung; S/MIME; OpenPGP; Zertifizierung; Public Key Infrastructure; Gebrauchstauglichkeit

1 Einführung und Motivation

Nach einer Analyse der beiden größten deutschen E-Mail-Anbieter hat sich die Anzahl der jährlich versendeten E-Mails seit dem Jahr 2010 auf ungefähr 625,8 Milliarden verdoppelt. Ein ähnliches Wachstum wird für die nächsten Jahre erwartet[3]. Das Einsatzszenario der E-Mail als Kommunikationsmedium der Wahl reicht dabei von einer rein privaten Nutzung bis hin zur Übermittlung sensibler Informationen innerhalb eines geschäftlichen Kontextes. Dennoch verschlüsseln nach einer Umfrage des Digitalverbandes BITKOM nur etwa 15 % der Nutzer in Deutschland ihre E-Mails[Ve].

Wird eine E-Mail versendet, wird diese über eine unbestimmte Anzahl von Knotenpunkten (den Mailservern) im Internet geleitet, bis sie letztendlich dem gewünschten Empfänger zugestellt wird. Dritten, die nicht direkt an der Kommunikation beteiligt sind und Zugriff auf den Transportweg der E-Mail haben, ist es mit einfachen Mitteln möglich, sowohl den Inhalt

[1] Fraunhofer-Institut für Sichere Informationstechnologie, Cloud Computing and Identity & Privacy, Rheinstraße 75, 64295 Darmstadt, Deutschland, ⟨vorname⟩.⟨nachname⟩@sit.fraunhofer.de
[2] Fraunhofer-Institut für Sichere Informationstechnologie, Security Management, Schloss Birlinghoven, 53754 Sankt Augustin, Deutschland, tatjana.rubinstein@sit.fraunhofer.de
[3] https://newsroom.web.de/2017/02/13/2016-rekordjahr-fuer-e-mail/

doi:10.18420/in2017_76

als auch die Kommunikationsmetadaten der E-Mail einzusehen. Letztere ermöglichen eine Profilbildung der Kommunikationspartner. Durch transportweg-absichernde Mechanismen der Provider, wie zum Beispiel *SSL/TLS*, können diese Informationen unberechtigten Dritten gegenüber geschützt werden. Auf den Knotenpunkten selbst ist die E-Mail jedoch noch immer im Klartext einsehbar.

Die Vertraulichkeit der E-Mail und der damit einhergehende Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung der Kommunikationspartner kann nur durch Nutzung einer durchgängigen Ende-Zu-Ende-Verschlüsselung gewährleistet werden. Bei Einsatz der Ende-Zu-Ende-Verschlüsselung wird die zu versendende E-Mail noch vor dem Verlassen des Systems des Absenders mit kryptographischen Hilfsmitteln verschlüsselt und erst auf dem System des adressierten Empfängers entschlüsselt. Durch die Kombination der provider-seitigen und der nutzer-seitigen Schutzmechanismen der Transportwegsicherung und der Ende-Zu-Ende-Verschlüsselung kann somit nicht nur die Vertraulichkeit der E-Mail, sondern auch der Schutz vor Profilbildung gewährleistet werden.

Die zur Ende-zu-Ende-Verschlüsselung verwendeten kryptographischen Mechanismen und konzeptuellen Modelle, wie *S/MIME*[TR10] und *OpenPGP*[Fi07], sind nicht nur schon seit vielen Jahren etabliert und beweisbar sicher, sondern auch in fast allen gängigen E-Mail-Anwendungen nativ integriert oder zumindest über etablierte Plugins nutzbar. Egal ob S/MIME oder OpenPGP, der Einsatz setzt entsprechende Fachkenntnisse voraus, welche insbesondere nicht technikaffine Anwender davor abschrecken, Ende-zu-Ende-Verschlüsselung zu nutzen.

Hier setzt die vom Fraunhofer-Institut für Sichere Informationstechnologie entwickelte Lösung *Volksverschlüsselung* an, welche Gegenstand dieses Beitrags ist.

2 Projektziele

Um die Nutzung der Ende-zu-Ende-Verschlüsselung in den existierenden Anwendungen signifikant zu erhöhen, verfolgt die Initiative Volksverschlüsselung folgende Ziele:

Gebrauchstauglichkeit: Alle Prozesse der lokalen Schlüsselerzeugung, der Authentifikation des Nutzers, der Zertifizierung des öffentlichen Schlüsselmaterials sowie die Integration in den späteren Anwendungen sollen so weit wie möglich automatisiert durchgeführt werden, so dass eine maximale Laientauglichkeit erreicht wird.

Identifizierende Schlüssel: Ein Zertifikat der Volksverschlüsselung, welches die Zuordnung eines Schlüssels zu einer Person bescheinigt, ist immer an die reale Identität des Schlüsselinhabers und an eine E-Mail-Adresse gebunden. Es werden nur geprüfte Inhalte in das Zertifikat übernommen. Hierbei werden die vom BSI definierten Qualitätsanforderungen hinsichtlich der verwendeten Verschlüsselungsverfahren und der erzeugten Schlüssel berücksichtigt.

Offene Schnittstellen: Die Infrastruktur muss die Möglichkeit bieten, von beliebigen Applikationen genutzt zu werden, sofern die Schnittstellen eingehalten werden.

Verwendung von Verschlüsselungsstandards: Um die flächendeckende Ende-Zu-Ende-Verschlüsselung zu fördern, sollen die etablierten Modelle *S/MIME* und *OpenPGP* unterstützt werden.

Datenschutz und Datensparsamkeit: Es sollen nur die im Rahmen identifizierender Schlüssel unbedingt notwendigen Daten auf eine datenschutzfreundliche Art und Weise erhoben und persistiert werden.

Transparenz: Die Prozesse der lokalen Schlüsselerzeugung und -verwendung müssen transparent sein.

Keine Kosten für Privatnutzer: Die Schlüssel und Zertifikate sollen für Privatanwender dauerhaft kostenlos sein.

3 Verwandte Lösungen

Für den Bezug der für *S/MIME* benötigten Zertifikate hat ein Nutzer verschiedene Zertifizierungsstellen zur Auswahl, wobei sich die ausgestellten Zertifikate durch ihre Klasse in ihrer Qualität unterscheiden können: Bei Zertifikaten der Klasse 1 erfolgt lediglich eine Überprüfung der E-Mail-Adresse, Klasse 2 Zertifikate verifizieren zusätzlich die Identität des Beantragenden anhand externer Quellen, Zertifikate der Klasse 3 setzten das persönliche Ausweisen des Beantragenden voraus.

Deutsche und europäische X.509-Zertifizierungsstellen wie *D-Trust*, *T-Systems*, *SwissSign*, *GlobalSign* und *Comodo* bieten in der Regel nur kostenpflichtige Klasse 3 Zertifikate an. Der Anbieter *Comodo* bietet zusätzlich kostenlose Zertifikate der Klasse 1 an. Der Vorteil dieser Zertifizierungsinstanzen besteht darin, dass ihre Stammzertifikate bereits in den gängigen Betriebssystemen und Browsern integriert sind, wodurch sie ohne zusätzliche Konfiguration als vertrauenswürdig eingestuft werden. Ist ein Hersteller von der Vertrauenswürdigkeit einer Zertifizierungsinstanz nicht mehr vollends überzeugt, kann, wie in den Fällen der Zertifizierungsinstanzen *WoSign* und *StartCom*[4] geschehen, die Integration auch wieder rückgängig gemacht werden.

Die deutsche Firma *Virtual Solution* stellt mit *SecurePIM*[5] eine mobile E-Mail-App für Android und Apple iOS bereit, die einen einfachen E-Mail-Client bietet und direkt an die Schweizer Zertifizierungsstelle *SwissSign* zur Ausstellung von Klasse 1 Zertifikaten angebunden ist. Die Schlüsselgenerierung erfolgt lokal. Nach einer kostenlosen Testphase ist die Lösung jedoch kostenpflichtig.

[4] https://www.heise.de/security/meldung/Zertifizierungsstellen-WoSign-und-StartCom-verlieren-Apples-und-Mozillas-Vertrauen-3341294.html

[5] https://virtual-solution.com

In Bezug auf die vertrauenswürdige Beglaubigung von PGP-Schlüsseln können die Offline-Zertifizierungsstellen des *Heise Verlags*[6] oder des *Instituts für Internet-Sicherheit*[7] verwendet werden. Zur Zertifizierung ist immer ein persönlicher Kontakt erforderlich, da die Überprüfung der Identität auf Basis eines gültigen Ausweisdokumentes erfolgt. Die Bearbeitungszeit der Zertifizierungsanträge liegt zwischen 6 und 8 Wochen. Der Prozess des Signaturwiderrufs ist nicht spezifiziert.

Die deutschen Mail-Anbieter *Web.de* und *GMX*, beide Töchter der *United Internet AG*, unterstützen pgp-basierte Ende-Zu-Ende-Verschlüsselung in ihren Webmailern nativ. Voraussetzung dafür ist jedoch, dass der Nutzer die Open-Source-Browser-Erweiterung *Mailvelope* installiert hat. Durch das Plugin wird der Schlüssel auf dem lokalen Gerät des Nutzers erzeugt. Sein öffentlicher Teil wird später in einem internen Adressbuch veröffentlicht, was eine benutzerfreundliche ende-zu-ende-verschlüsselte Kommunikation der Nutzer direkt über das Frontend erlaubt. Eine Identitätsvalidierung oder ein Vertrauensmodell bietet der Ansatz jedoch nicht.

4 Vertrauensmodelle

Die beiden etablierten Ansätze *S/MIME* und *OpenPGP* verfolgen das gleiche Ziel, verwenden asymmetrische Kryptographie und setzen voraus, dass Sender und Empfänger ein system-spezifisch zertifiziertes kryptographisches Schlüsselpaar besitzen. In der Umsetzung unterscheiden sich beide Ansätze durch die jeweilig eingesetzten Vertrauensmodelle jedoch elementar: Während *S/MIME* auf den zentralisierten Ansatz einer hierarchischen Zertifizierungsstruktur aufbaut, verwendet *OpenPGP* das dezentrale Modell des *Web of Trust*[AR97]. Das zugrunde liegende Vertrauensmodell ist notwendig, um die Vertrauenswürdigkeit eines öffentlichen Schlüssels in Form eines Zertifikates zu bescheinigen. Ein Zertifikat ist eine Datenstruktur, welche mit kryptographischen Hilfsmitteln ein Objekt fest an ein Subjekt bindet.

Im zentralisierten *S/MIME*-Modell muss ein Nutzer auf die ordnungsgemäße Prüfung der Schlüsselzugehörigkeit durch die zentrale Instanz, die Zertifizierungsstelle (*Certification Authority, CA*), vertrauen. Nach erfolgreicher Prüfung stellt die Zertifizierungsstelle ein Zertifikat entsprechend der internationalen Norm X.509[ITR00] für den öffentlichen Teil des kryptographischen Schlüssels aus. Das X.509-Zertifikat stellt eine atomare Datenstruktur dar. Die Definition der Verifikations- und Betriebsprozesse sind über die veröffentlichten *Zertifizierungsrichtlinien* und die *Erklärung zum Zertifizierungsbetrieb* einsehbar. Die Qualität der durch die zentrale Instanz ausgestellten Zertifikate ist dadurch äquivalent. Um die Gültigkeit eines Zertifikats zu prüfen, müssen alle Zertifikate der Zertifizierungskette, bis hin zum Wurzelzertifikat, geprüft werden. Der Widerruf eines Zertifikates erfolgt

[6] https://www.heise.de/security/dienste/Was-ist-die-c-t-Krypto-Kampagne-473381.html

[7] https://www.internet-sicherheit.de/pgpzi/

analog der Ausstellung durch die Zertifizierungsstelle. Der Austausch eines Zertifikates kann persönlich initiiert oder mit Hilfe eines Verzeichnisdienstes erfolgen.

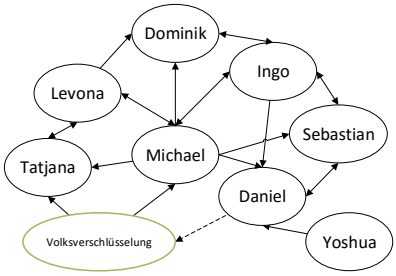

Abb. 1: *Web of Trust*: Nutzer bescheinigen gegenseitig die Authentizität eines Schlüssels mittels einer Signatur. Die *Volksverschlüsselung* stellt eine vertrauenswürdige externe Instanz dar.

Wie in Abbildung 1 schematisch illustriert, wird bei *OpenPGP* die an einen öffentlichen Schlüssel gebundene Identität (die so genannte *UID*) durch andere dem *Web of Trust* angehörige Nutzer in Form einer Signatur beglaubigt (dargestellt durch gerichtete Kanten). Dafür muss technisch nicht zwangsläufig eine explizite Identitätsprüfung erfolgen. Die ordnungsgemäße Überprüfung der Schlüsselzugehörigkeit liegt im Verantwortungsbereich des signierenden Nutzers, wodurch die Qualität von durch verschiedene Nutzer ausgestellte Signaturen nicht prinzipiell vergleichbar ist. Schwierig wird die verantwortungsbewusste Ausstellung einer Signatur vor allem dann, wenn man den Besitzer des öffentlichen Schlüssels nicht persönlich kennt oder der Schlüssel nicht im persönlichen Kontakt ausgetauscht wurde. Abhilfe schafft die Beglaubigung der Identität des Schlüsselinhabers durch eine vertrauenswürdige externe Instanz.

Die Datenstruktur eines PGP-Zertifikates, welches während der Erstellung des kryptographischen Schlüssels automatisch mit erzeugt wird, ist modular, wodurch es auf verschiedenen Schlüsselservern verteilt und später lokal rekonstruiert werden kann. Analog zu *S/MIME* kann das Zertifikat auch persönlich initiiert ausgetauscht werden.

Im PGP-Kontext gibt es zwei verschiedene Widerrufs-Mechanismen: Zum einen kann über die Publikation eines sich im Besitz des Nutzers befindlichen Widerrufs-Zertifikat der PGP-Schlüssel im Gesamten gesperrt werden, zum anderen kann über die Publikation einer auf eine explizite Signatur referenzierte Widerrufs-Signatur nur diese zurückgezogen werden.

Durch die konzeptuellen Unterschiede der Verfahren werden an die jeweilig eingesetzten Formate und Strukturen unterschiedliche Anforderungen gestellt. Das hat zur Folge, dass beide Ansätze nicht kompatibel zu einander sind, wodurch sich Sender und Empfänger zunächst auf eines der Verfahren einigen müssen, wenn sie ende-zu-ende-verschlüsselt miteinander kommunizieren möchten.

5 Architektur und Funktionsweise

Das Gesamtsystem *Volksverschlüsselung* unterteilt sich in eine Client- und eine Serverseite. Die Clientseite, die *Volksverschlüsselung-Software (VV-SW)*, dient der Unterstützung des beantragenden Nutzers und automatisiert alle notwendigen Schritte so weit wie möglich.

Das zu zertifizierende Schlüsselmaterial wird durch die Software lokal generiert. Im Falle der PGP-Zertifizierung kann es zusätzlich aus externen Anwendungen bezogen werden.

Serverseitig unterteilt sich die Infrastruktur der *Volksverschlüsselung*, wie in Abbildung 2 schematisch illustriert, in zwei verschiedene physisch getrennte Netze und mehrere verschiedene Komponenten. So ist das Netz der Zertifizierungsstelle (CA-Server), welches auch das für ihre kryptographischen Schlüssel verwendete und nach FIPS-140-2 Level 3 zertifizierte *Hardware-Sicherheitsmodul (HSM)* beinhaltet, strikt von dem öffentlich zugänglichen Netz der Registrierungsstelle (RA-Server) getrennt.

Die Kommunikation zwischen *VV-SW* und Server-Infrastruktur erfolgt über die REST-Schnittstelle des RA-Servers. Die Schnittstelle steht der Entwicklung eigener Client-Anwendungen durch Dritte offen gegenüber. Der RA-Server ist für die Durchführung der Authentifizierung sowie die Korrektheit aller eingehenden Zertifizierungsparameter verantwortlich. Abhängig des durch den beantragenden Nutzer gewählten Authentifizierungsverfahrens können weitere externe Dienste notwendig sein. So ist zum Beispiel der *eID-Service* eines externen Dienstleisters zur Nutzung der Online-Ausweisfunktion des deutschen Personalausweises angebunden.

Die erfolgreich validierten Zertifizierungsanfragen werden durch die entsprechende Zertifizierungsinstanz verarbeitet, welche die Zertifikate ausstellt. Die Bearbeitungszeit beträgt, Abhängig von dem aktuellen Anfrageaufkommen, nur wenige Minuten. Der Datenaustausch zwischen RA-Server und CA-Server erfolgt im *Polling Modus*. Das bedeutet, dass die Übertragung der Zertifizierungsanfragen und der ausgestellten Zertifikate stets durch den CA-Server initiiert wird. Ein Zugriff auf ihn von außerhalb ist technisch nicht möglich.

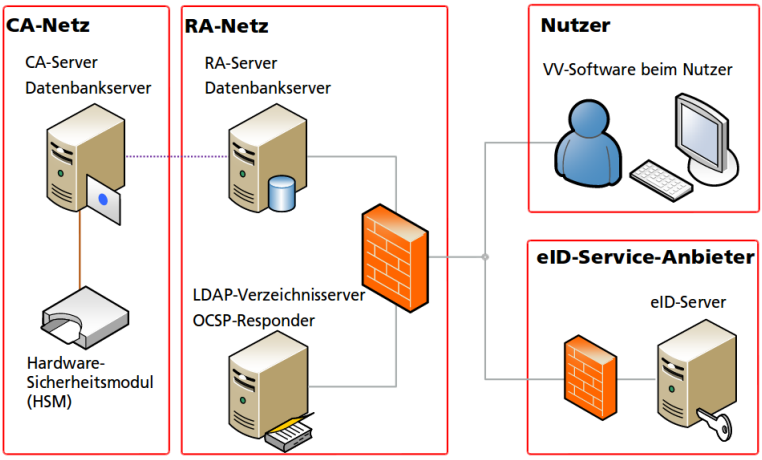

Abb. 2: Abstrakte Darstellung der Komponenten der *Volksverschlüsselung*.

Weitere Dienste der Volksverschlüsselung sind unter anderem das Adressbuch (der Verzeichnisdienst) sowie der *OCSP-Responder (Online Certificate Status Protocol, RFC*

6960), welcher nahezu Echtzeitinformationen über den Zustand eines X.509-Zertifikates der Volksverschlüsselung erlaubt. Zur Verteilung der Revokationsinformationen werden Zertifikats-Sperrlisten *(Certificate Revocation List, CRL)* erzeugt. Der Publikationsort dieser Listen ist innerhalb der Zertifikate fest kodiert, wodurch sie automatisch durch die vom Nutzer eingesetzten E-Mail-Anwendungen zu beziehen sind.

Der Verzeichnisdienst der Volksverschlüsselung basiert auf einem OpenLDAP-Server. In ihm werden die Verschlüsselungszertifikate sowie die E-Mail-Adresse und der Namen der Nutzer hinterlegt. Die Veröffentlichung ist optional und kann während des Zertifizierungsprozesses in der Client-Anwendung beantragt werden. Der Zugriff auf das Adressbuch erfolgt innerhalb eines anonymen Kontextes, wodurch es auch durch Nutzer anderer Zertifizierungsinstanzen verwendet werden kann. Aus Gründen des Datenschutzes sieht der Verzeichnisdienst vor, dass eine Suchanfrage nur auf Basis einer vollständigen E-Mail-Adresse erfolgen darf. Das Auslesen aller veröffentlichten Nutzerdaten ist nicht möglich.

Die zentrale Infrastruktur der Volksverschlüsselung wird in einem gemäß ISO 27001 zertifizierten Rechenzentrum der *Deutschen Telekom AG* in Deutschland betrieben. Die Entwicklung der Volksverschlüsselung und Zertifizierungsverantwortung liegt ausschließlich bei Fraunhofer SIT.

6 Das Zertifizierungsmodell

Durch die technischen und konzeptionellen Unterschiede der beiden Vertrauensmodelle *S/MIME* und *OpenPGP* ist eine gemeinsame technologie-übergreifende Nutzung von nur einer Zertifizierungsinstanz nicht möglich.

Das entworfene Modell sieht daher, wie in Abbildung 3 illustriert, den parallelen Betrieb zweier zentraler Zertifizierungshierarchien vor, welche organisatorisch jedoch als eine Komponente betrachtet werden. Der hierarchische Aufbau erlaubt, neben der Bündelung des Vertrauens in einem zentralen Wurzelknoten, auch eine organisatorische und funktionsbezogene Gruppierung der später ausgestellten X.509-Zertifikate bzw. PGP-Signaturen. Die Zertifizierungsinfrastruktur der Volksverschlüsselung umfasst folgende Zertifizierungsstellen (*CAs*):

- Eine *Root-CA* für jedes $Format \in \{X.509, PGP\}$, welche den jeweiligen Vertrauensanker der korrespondierenden Zertifizierungshierarchie darstellt (siehe Abbildung 3). Das Zertifikat ist selbst signiert und hat eine Laufzeit von 7 Jahren. Der Betrieb einer eigenen *Root-CA* war notwendig, um die in Abschnitt 2 definierten Projektziele zu erreichen. Die Stammzertifikate sind jedoch noch nicht auf den gängigen Plattformen integriert.
- Eine *Private-CA* für jedes $Format \in \{X.509, PGP\}$. Diese Zertifizierungsstelle stellt kostenlose X.509-Zertifikate bzw. PGP-Signaturen zur privaten Nutzung mit einer Laufzeit von 2 Jahren aus. Das CA-Zertifikat hat eine Laufzeit von 5 Jahren.

- Eine oder mehrere *Business-CA(s)* für jedes $Format \in \{X.509, PGP\}$. Diese Zertifizierungsstellen stellen, analog der *Private-CAs*, X.509-Zertifikate bzw. PGP-Signaturen für Endnutzer aus. Die ausgestellten Zertifikate sind nach den Lizenzbestimmungen der Volksverschlüsselung im Kontext einer geschäftlichen Nutzung verwendbar.
- Die *Internal-Service-CA* stellt eine Zertifizierungsstelle dar, welche ausschließlich X.509-Zertifikate für interne Komponenten zum Aufbau sicherer Kommunikationsverbindungen ausstellt.

Das Zertifikat einer Zertifizierungsstelle ist stets durch die übergeordnete Zertifizierungsstelle ausgestellt und signiert. Die Zertifikate der PGP-Zertifizierungsstellen sind zusätzlich durch sich selbst signiert, man spricht von einer *Selbstsignatur*. In Abbildung 3 sind diese *Selbstsignaturen* durch Kanten dargestellt, bei welchen Anfang und Ende der gleiche Knoten ist. Die zugrunde liegenden Algorithmen und Sicherheitsparameter entsprechen den aktuellen Empfehlungen des BSI[Ma08].

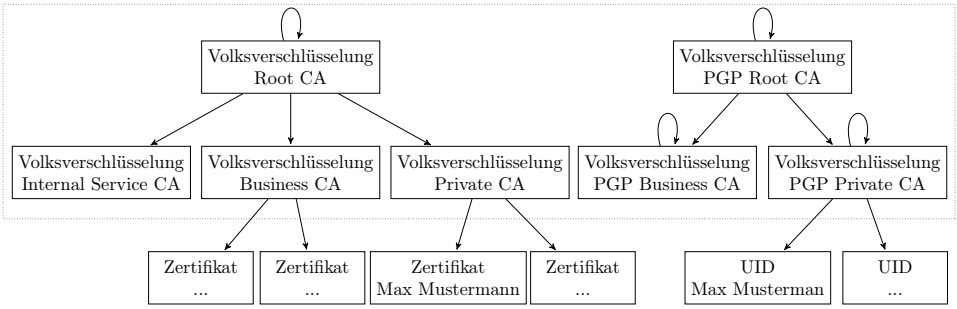

Abb. 3: Zertifizierungsarchitektur der Volksverschlüsselung: Paralleler Betrieb einer Zertifizierungsinstanz für hierarchische und einer PGP-CA für dezentrale Vertrauensmodelle. Signatur-Beziehungen werden durch Kanten Dargestellt: A $\rightarrow$ B $\equiv$ A signiert B.

6.1 Zertifizierungsparadigma

Der Prozess einer Zertifizierung ist im Kontext der Volksverschlüsselung standardisiert und generalisiert, so dass einzelne Module, wie zum Beispiel die Authentifizierung oder das Erzeugen der Zertifikate, austauschbar und erweiterbar sind. Ein Zustandswechsel innerhalb des Zertifizierungsprozesses erfolgt stets über definierte Schnittstellen und Formate, wodurch spezifische technische Gegebenheiten in der jeweiligen Implementierung abgebildet werden können.

Wie in Abbildung 4 schematisch illustriert, stellt die erfolgreiche Identifikation des Nutzers sowie die erfolgreiche Verifikation seiner E-Mail-Adresse eine Grundvoraussetzung für die Erstellung der X.509-Zertifikate bzw. PGP-Signaturen dar. Des Weiteren darf es zu jeder E-Mail-Adresse im Kontext der Volksverschlüsselung nur ein gültiges Zertifikat pro Zertifizierungsformat geben.

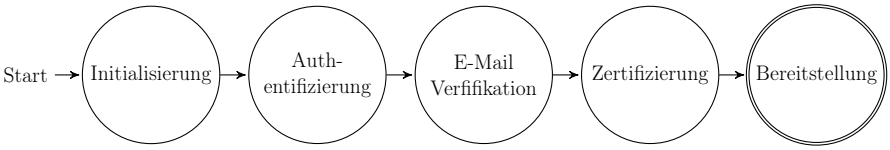

Abb. 4: Abstrakte Darstellung des Zertifizierungsprozesses der Volksverschlüsselung.

6.2 Zertifikatsqualität durch Identitätsprüfung

Ein elementarer Punkt der vertrauenswürdigen Ende-Zu-Ende-Verschlüsselung liegt vor allem in der Authentizität des zu verwendenden kryptographischen Schlüsselmaterials. Es muss sicher gestellt sein, dass der eingesetzte kryptographische Schlüssel auch wirklich von der angegebenen Person stammt.

Zertifikate der Volksverschlüsselung basieren stets auf einer starken Identitätsprüfung. Ein Zertifikatsempfänger kann somit sicher sein, dass die im Zertifikat kodierte Identität der realen Identität des Inhabers entspricht. Hierzu hat die Volksverschlüsselung aktuell folgende Verfahren angebunden:

Online-Ausweisfunktion des Personalausweises[Ma11, NK10]: Für das Auslesen von Name, Vorname(n) und ggf. Titel wurde ein technisches Zertifikat der *Vergabestelle für Berechtigungszertifikate* erworben.

Kundenkonto der Telekom: Festnetzkunden der Deutschen Telekom AG können sich mit dem dazu gehörigen Kundenkonto authentifizieren, da ihre Identität bei Vertragsabschluss ausreichend verifiziert wurde.

Registrierungscode: Für Personen, für welche die Nutzung der bisher genannten Methoden nicht in Frage kommt, wurde das Verfahren der *Vor-Ort-Registrierung* geschaffen. Nutzer können eine Registrierungscode-Karte (Abbildung 5) in einem persönlichen Kontakt mit Fraunhofer SIT gegen Vorlage eines gültigen Ausweisdokumentes[8] erhalten. Die Datenerhebung ist hierbei analog der des eID-Verfahrens. Nach Aktivierung ist der Registrierungscode 28 Tage gültig.

Abb. 5: Registrierungskarte der Volksverschlüsselung.

SmartCard der Fraunhofer-Gesellschaft: Mitarbeiter der Fraunhofer-Gesellschaft können sich auf Basis ihrer SmartCard auf einer nur aus dem internen Netzwerk adressierbaren Web-Schnittstelle Registrierungscodes beschaffen, welche zu denen der *Vor-Ort-Registrierung* äquivalent sind.

[8] Personalausweise, Reisepässe der EU-Mitgliedsstaaten

7 Realisierungs- und Betriebsdetails

Zur Umsetzung der Komponenten der Volksverschlüsselung wurden, unter Berücksichtigung der Sicherheitsanforderungen, verschiedene etablierte OpenSource-Technologien eingesetzt. Während des gesamten Entwicklungsprozesses lag der Fokus stets auf der Gebrauchstauglichkeit. Diese wurde durch eine Studie der *Universität der Künste Berlin*, eigene Nutzertests sowie studentische Arbeiten analysiert und immer weiter verbessert.

7.1 Volksverschlüsselung-Software

Die Client-Software der Volksverschlüsselung wurde zunächst für *Microsoft Windows* und auf Basis von *Microsoft.NET* (Version 4.5) entwickelt. Als Programmiersprache kommt hierbei *C#* zum Einsatz. Zur Darstellung der graphischen Benutzeroberfläche wird *WPF (Windows Presentation Foundation)* bzw. *XAML (Extensible Application Markup Language)* genutzt. Für die Umsetzung der kryptographischen Funktionen wurde mit *Bouncy Castle*[9] auf eine etablierte OpenSource-Bibliothek zurückgegriffen. Als lokale Verwaltungsdatenbank wird *SQLite*[10] eingesetzt. Alle vertraulichen Daten, wie etwa die privaten Schlüssel, sind kryptographisch über den Windows-Schlüsselspeicher abgesichert. Zwecks Konfiguration der Anwendungsprogramme ist die Client-Software mit einer Plugin-Schnittstelle ausgestattet, so dass mit geringem Aufwand weitere Anwendungsprogramme integriert werden können. Aktuell stehen Plugins für *Mozilla* (*Thunderbird*, *SeaMonkey* und *Firefox*), *Microsoft Outlook*, *Google Chrome* sowie *Windows Live-Mail* zur Verfügung. Zur Anbindung der Online-Ausweisfunktion des Personalausweises ist die vom *BSI* zertifizierte *Open eCard App*[11] in der Client-Software integriert.

Die Backup-Funktion des Clients ermöglicht das Verteilen der Schlüssel auf andere Plattformen. Über den Export eines *Konfigurations-Profiles* z.B. ist eine einfache Integration der Schlüssel auf Apple-Geräten möglich, während das *PKCS#12-Format*[Mo14] eine plattform-unabhängige Verteilung erlaubt. Über die eingebaute Auto-Update-Funktion wird die Software stets auf dem aktuellen Stand gehalten.

Die Software ist mit einem *Extended Validated Code Signing*-Zertifikat der Zertifizierungsstelle *GlobalSign* signiert, wodurch sie eindeutig und öffentlich verifizierbar ihrem ordnungsgemäßen Herausgeber zugeordnet ist und Manipulationsversuche durch Dritte festgestellt werden können. Ferner ist es möglich, die Anwendungen auf Basis des zur Einsicht veröffentlichten Quellcodes selbständig zu kompilieren. Die Veröffentlichung schafft Transparenz hinsichtlich der Erstellung und Weitergabe des kryptographischen Schlüsselmaterials.

[9] http://www.bouncycastle.org/
[10] https://www.sqlite.org/
[11] https://www.openecard.org

7.2 Registrierungsstelle

Die Registrierungsstelle der Volksverschlüsselung wurde auf Basis der Programmiersprache Java und des *Play Frameworks* entwickelt, welches den Aufbau stark skalierender, zustandsloser und robuster Web-Anwendungen erlaubt. Als Persistenzschicht wird eine MySQL-Datenbank eingesetzt. Die durch die Registrierungsstelle erhobenen personenbezogenen Daten sind aus Datenschutzgründen auf das zur Identifizierung des Schlüsselinhabers erforderliche Minimum beschränkt und werden stets mit einem individuellen Zufallswert und durch die kryptographische Hash-Funktion *SHA-256* verarbeitet gespeichert.

Geht eine Zertifizierungsanfrage ein, wird vor der Weitergabe an die Zertifizierungsstelle verifiziert, ob der dem Schlüssel zugrunde liegende kryptographische Algorithmus und die Größe des Sicherheitsparameter gültig sind und den aktuellen Empfehlungen des BSI[Ma08] entsprechen.

7.3 Zertifizierungsstelle

Zur Ausstellung der X.509-Zertifikate setzt die Volksverschlüsselung die *Enterprise JavaBeans Certification Authority (EJBCA)*[12] ein. *EJBCA* ist eine auf Java basierende OpenSource lizenzierte Zertifizierungsstelle, welche es erlaubt, skalierende und komplexe Zertifizierungsinfrastrukturen aufzubauen. Mitgelieferte Komponenten sind, neben der Zertifizierungsinstanz selbst, ein *OCSP-Responder* und eine Registrierungsstelle. Letztere konnte durch die speziellen Anforderungen der Volksverschlüsselung jedoch nicht verwendet werden.

Die im Rahmen der Volksverschlüsselung entwickelte PGP-Zertifizierungsstelle baut, analog zum Client, auf der etablierten Krypto-Bibliothek *BouncyCastle* auf. Das Referenzieren des *Hardware Sicherheitsmoduls* erfolgt per *CryptoServerProvider* der *Java Cryptography Extension (JCE)*. Die privaten Schlüssel der Zertifizierungsstelle werden innerhalb des *HSM* erzeugt und verlassen dieses auch während der Ausstellung einer Signatur nicht.

Zusätzlich zur Standardüberprüfung der Registrierungsstelle erfolgt die Verifikation der format-spezifischen Parameter des öffentlichen PGP-Schlüssels. Dazu gehören die verwendete PGP-Version und der strukturelle Aufbau der zu dem Schlüssel korrespondierenden UID[13]. Bei letzterer Überprüfung müssen der Inhalt sowie die Struktur der *UID* nach einem definierten Muster zu den aus dem gewählten Authentifizierungsverfahren bezogenen Nutzerinformationen passen.

[12] `https://www.ejbca.org/`

[13] *UID, User Identifier (RFC 4880 Abschnitt 5.11 und RFC 2822 Abschnitt 3.4):* Repräsentiert einen Namen (oder ein Pseudonym) des Schlüsselbesitzers vergleichbar mit dem *CommonName*-Attribut der X.509-Zertifikate.

7.4 Verzeichnisdienst

Aus Gründen des Datenschutzes ist die Suche eines Zertifikates auf dem Verzeichnisdienst nur auf Basis einer vollständigen E-Mail-Adresse möglich. Um diese Anforderung zu erfüllen, wurde der eingesetzte *OpenLDAP*-Server durch eine in der Programmiersprache *C* und unter Einsatz des integrierten *SLAPI Frameworks* entworfenen Erweiterung des Typs *preoperation* ergänzt. Erweiterungen dieses Typs werden in der *Overlay*-Schicht des Servers registriert und erlauben unter anderem das Verarbeiten eingehender Suchanfragen (Filter), noch bevor diese an das Backend des *OpenLDAP*-Servers zur Verarbeitung weiter gegeben werden.

Geht eine LDAP-Suchanfrage, egal welcher Komplexität, ein, wird zunächst nach dem ersten atomaren Filter basierend auf dem *mail*-Attribut gesucht. Ist ein solcher Filter gefunden, wird er unabhängig seines Typs (z.B. relationaler Vergleich oder Teilstring-Suche) zu einem Filter des Typs *equaly* transformiert. Filter des Typs *equaly* liefern genau dann ein Ergebnis, wenn der Filterwert genau dem Attributwert entspricht. Der Vergleich kann hierbei *case-sensitive* oder *case-insensitive* erfolgen. Wird kein Filter basierend auf dem *mail*-Attribut gefunden, wird ein neuer Filter erzeugt, welcher kein Suchergebnis liefert. Die Ergebnismenge einer Suchanfrage kann somit entweder eine Menge mit genau einem Eintrag oder die leere Menge sein.

8 Fazit und Ausblick

Die Volksverschlüsselung ist eine Initiative, welche das Ziel verfolgt, kryptographische Schlüssel benutzerfreundlich an Nutzer zu verteilen, so dass Ende-Zu-Ende-Verschlüsselung und der damit einhergehende Selbstdatenschutz gefördert und selbstverständlich wird. Um die Volksverschlüsselung perspektivisch noch mehr Nutzern zur Verfügung stellen zu können, wird sie kontinuierlich weiterentwickelt. Hierzu gehören zum einen die Entwicklung neuer Authentifizierungsverfahren, wie z.B. die Identifikation per *Internet-Video-Chat*. Des Weiteren ist auch das Portfolio der Konfigurations-Plugins der Client-Software zu erweitern, so dass zukünftig z.B. auch die zur Ende-Zu-Ende-Verschlüsselung in Webmailern notwendigen Browser-Erweiterungen nativ unterstützt werden.

Auch durch die unterschiedlichen möglichen Einsatzszenarien der Volksverschlüsselung, z.B. innerhalb eines kommerziellen Kontextes, ergeben sich neue Anforderungen, wodurch z.B. die Entwicklung erweiterter Backup- oder Schlüsselverteilungsmechanismen notwendig wird.

Um die technische Akzeptanz der Volksverschlüsselung weiter zu steigern, sind zukünftig auch die verschiedenen Möglichkeiten der *Cross-Zertifizierung* oder ihr Anschluss an die

TeleTrusT European Bridge CA (EBCA)[14] zu diskutieren. Zusätzlich strebt die Volksverschlüsselung auch jenseits einer formalen *Cross-Zertifizierung* die Kooperation mit anderen Zertifizierungsstellen an.

Literaturverzeichnis

[AR97] Abdul-Rahman, Alfarez: The PGP Trust Model. EDI-Forum: The Journal of Electronic Commerce, 10(3):27–31, 1997.

[Fi07] Finney, Hal; Donnerhacke, Lutz; Callas, Jon; Thayer, Rodney L.; Shaw, David: , OpenPGP Message Format. RFC 4880, November 2007.

[ITR00] ITU-T RECOMMENDATION, X: 509 I ISO/IEC 9594-8. Information Technology–Open Systems Interconnection–The Directory: Public-key and attribute certificate frameworks, 2000.

[Ma08] Margraf, Marian: Kryptographische Verfahren: Empfehlungen und Schlüssellangen. Technische Richtlinie TR-02102, Bundesamt für Sicherheit in der Informationstechnik, 2008.

[Ma11] Margraf, Marian: The New German ID Card. In: ISSE 2010 Securing Electronic Business Processes, S. 367–373. Springer, 2011.

[Mo14] Moriarty, Kathleen; Nystrom, Magnus; Parkinson, Sean; Rusch, Andreas; Scott, Michael: , PKCS #12: Personal Information Exchange Syntax v1.1. RFC 7292, Juli 2014.

[NK10] Noack, Torsten; Kubicek, Herbert: The Introduction of Online Authentication as Part of the New Electronic National Identity Card in Germany. Identity in the Information Society, 3(1):87–110, 2010.

[TR10] Turner, Sean; Ramsdell, Blake C.: , Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification. RFC 5751, Januar 2010.

[Ve] Verschlüsselung von E-Mails kommt nur langsam voran. `https://www.bitkom.org/Presse/Presseinformation/Verschluesselung-von-E-Mails-kommt-nur-langsam-voran.html`. Zugriff: 19.04.2017.

[14] `http://www.ebca.de/ebca`