

Sicherheitseigenschaften neuerer Systeme zur E-Mail-Kommunikation zwischen Bürgern und Behörden

Jörn Freiheit

Hochschule für Technik und Wirtschaft Berlin
Wilhelminenhofstr. 75A, 12459 Berlin
Joern.Freiheit@HTW-Berlin.de

Abstract: Bei der Kommunikation mit Behörden und der Justiz wird nach wie vor der herkömmliche Brief bevorzugt, obwohl sowohl für Privatpersonen als auch für Unternehmen die Briefpost fast vollständig durch E-Mails abgelöst worden ist. Preis und Geschwindigkeit der E-Mail sind dem herkömmlichen Brief deutlich überlegen, doch datenschutzrechtliche Aspekte haben bis heute verhindert, dass mit Behörden rechtsverbindlich per E-Mail kommuniziert werden kann. Hier soll mit Neuentwicklungen wie dem e-Postbrief, De-Mail oder dem Elektronischen Gerichts- und Verwaltungspostfach (EGVP) Abhilfe geschaffen werden. Die Aspekte Vertraulichkeit, Integrität und Authentizität in diesen Neuentwicklungen und die Praktikabilität für die elektronische Kommunikation zwischen Bürgern und Behörden werden in diesem Papier diskutiert.

1 Einleitung

Für die sichere und einfache elektronische Kommunikation zwischen Bürgern, Behörden und Unternehmen wurden in den vergangenen Jahren neue Produkte entwickelt und zur Verfügung gestellt. Dazu gehören De-Mail, der e-Postbrief und das Elektronische Gerichts- und Verwaltungspostfach (EGVP). Allen diesen Systemen ist jedoch gemein, dass ihre Einführung mit hohen Anlaufschwierigkeiten verbunden ist. So wurde die Einführung von De-Mail auf Ende 2011 verschoben, da der Akkreditierungsprozess der privaten De-Mail-Provider aufwändiger als vermutet ist. Darüber hinaus kritisieren Datenschützer, dass eine durchgehende Verschlüsselung einer De-Mail vom Absender bis zum Empfänger nicht verbindlich ist [Le11, Sch11]. Über den e-Postbrief hat im August 2011 das Landgericht Bonn geurteilt, dass die Aussage der Deutschen Post, „der E-Postbrief ist so sicher und verbindlich wie der Brief“, unwahr ist. Darüber hinaus wurde durch das Landgericht Bonn auch die Werbebehauptung der Deutschen Post: „der E-Postbrief überträgt die Vorteile des klassischen Briefs in das Internet und bietet damit auch in der elektronischen Welt eine verbindliche, vertrauliche und verlässliche Schriftkommunikation“ verboten¹³. Das elektronische Gerichts- und Verwaltungspostfach wird als Eigenentwicklung der Justiz derzeit ausschließlich innerhalb der Justiz zur Kommunikation zwischen Gerichten, Staatsanwaltschaften, Anwälten und Notaren verwendet und ist von den genannten drei Verfahren bereits das „dienstälteste“. Es wird,

¹³ Landgericht Bonn, Urteil vom 30. Juni 2011 – 14 O 17/11

im Gegensatz zu den beiden anderen Verfahren, von der Justiz kostenfrei zur Verfügung gestellt. In einigen Verfahren (Handelsregistersachen, Mahnsachen) ist das EGVP per Gesetz als ausschließlicher Kommunikationsweg mit der Justiz vorgeschrieben. Papiereingänge werden in diesen Sachen nicht akzeptiert. In Verfahren, in denen die Übermittlung per EGVP freiwillig erfolgt, wird es jedoch nur von einer sehr überschaubaren Anzahl von Rechtsanwälten genutzt.

In diesem Papier sollen diese Kommunikationsinfrastrukturen bezüglich ihrer *Sicherheitseigenschaften* diskutiert werden. Dazu wird zunächst in Abschnitt 2 allgemein erläutert, welche Anforderungen an eine sichere E-Mail-Kommunikation zwischen Bürgern, Behörden und Unternehmen gestellt werden müssen. Abschnitt 3 beschreibt etablierte technische Möglichkeiten der sicheren E-Mail-Kommunikation und diskutiert deren Praktikabilität. In Abschnitt 4 werden die Systeme De-Mail, e-Postbrief und EGVP näher beschrieben und unter den in Abschnitt 2 identifizierten Sicherheitsanforderungen bewertet.

2 Allgemeine Anforderungen an die sichere E-Mail-Kommunikation

In diesem Abschnitt werden die unterschiedlichen Anforderungen beschrieben, die eine *sichere* E-Mail-Kommunikation nach heutigem Stand der Wissenschaft erfüllen muss. Eine E-Mail-Kommunikation ist sicher, wenn sie vertraulich ist, die Kommunikationspartner eindeutig identifizierbar sind und die Integrität der übermittelten Daten beziehungsweise Dokumente garantiert wird. Dies bedeutet grob zusammengefasst, dass Daten, die per E-Mail versendet werden, nicht von Unbefugten gelesen (Vertraulichkeit) und nicht geändert (Integrität) werden können und dass die Daten tatsächlich von dem vorgegebenen Autor beziehungsweise Absender stammen (Authentizität). Neben diesen drei Anforderungen können weitere Anforderungen an eine sichere E-Mail-Kommunikation gestellt werden, wie zum Beispiel dass ein E-Mail-Dienst stets verfügbar sein muss oder Fehlermeldungen bei Unzustellbarkeit versendet werden. Auf diese weiteren, technischen Anforderungen, wird in diesem Papier jedoch nicht eingegangen.

2.1 Vertraulichkeit

„Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.“ [BSI]

Hierbei ist zu betonen, dass die Vertraulichkeit verletzt ist, wenn Unbefugten die Daten in einer lesbaren Form zugänglich sind, das heißt wenn die Daten durch Unbefugte auswertbar und weiterverwendbar sind. Die Vertraulichkeit ist umgekehrt nicht verletzt, wenn Unbefugte Zugang zu den Daten erhalten, diese aber, zum Beispiel durch Verschlüsselung (siehe Abschnitt 3.1), nicht lesbar und weiterverwendbar sind. Neben dieser Anforderung an die Lesbarkeit und Weiterverwendbarkeit von Daten ist klarzustellen, wer als *unbefugt* im Sinne der Vertraulichkeit gilt. Eine sehr restriktive Eingrenzung dieses Begriffes, zum Beispiel die Festlegung, dass die einzig Befugten bei der

sicheren E-Mail-Kommunikation ausschließlich Absender und Empfänger sind, führt in der Praxis häufig zu Vertraulichkeitsverletzungen, die rein theoretischer Natur sind (siehe Abschnitte 4.1 und 4.2).

2.2 Integrität

Integrität bezeichnet laut Glossar des Bundesamtes für Sicherheit in der Informationstechnik (BSI) die Sicherstellung der Korrektheit, das heißt Unversehrtheit von Daten. Der Verlust der Integrität kann bedeuten, „dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.“ [BSI]. Werden also Daten per E-Mail versendet, so muss zur Wahrung der Integrität sichergestellt werden, dass diese genauso beim Empfänger angekommen, wie sie der Absender versendet hat. Die Sicherstellung der Integrität ist eine zentrale Anforderung für den sicheren Versand elektronischer Daten in der Justiz.

Es sei an dieser Stelle betont, dass es genügt, wenn die Integrität einer Nachricht beziehungsweise ihre Verletzung nachträglich festgestellt werden kann. Das bedeutet, dass der Schutz der Integrität nicht zwingend erfordert, dass es keine Möglichkeit gibt, die Integrität zu verletzen. Vielmehr muss sichergestellt werden, dass die Verletzung der Integrität im Zweifel nachgewiesen werden kann (siehe Abschnitt 2.2). Werkzeuge zum Schutz der Integrität ermöglichen somit das sichere Erkennen der Wahrung beziehungsweise der Verletzung der Integrität.

2.3 Authentizität

„Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden.“ [BSI]

Eine E-Mail-Kommunikation ist demnach dann authentisch, wenn der Absender auch tatsächlich die Person ist, die er vorgibt zu sein. Die Verletzung der Authentizität wird insbesondere bei den als *Phishing* bekannten Attacken praktiziert (siehe auch Kapitel 1.3.2 bei [Eck09]). Tatsächlich ist der Nachweis über die Identität des Absenders bei der elektronischen Kommunikation schwierig zu führen. Dies liegt unter anderem auch daran, dass die Anforderungen an die Authentizität im Falle der elektronischen Kommunikation häufig strenger sind, als man dies beispielsweise von der herkömmlichen Briefkommunikation kennt, bei der man zunächst von der Korrektheit der vorgegebenen Identität des Absenders ausgeht, wenn der Brief handschriftlich unterzeichnet wurde. In Anlehnung an die handschriftliche Unterschrift wurde die elektronische Signatur entwickelt, die einen Nachweis der Authentizität ermöglicht (siehe Abschnitt 3.2).

3 Technische Möglichkeiten für eine sichere E-Mail-Kommunikation

Um die Anforderungen an die sichere E-Mail-Kommunikation zu erfüllen, wurden technische Verfahren entwickelt, die im Folgenden diskutiert werden. Dabei wird insbesondere darauf eingegangen, welche der Anforderungen Integrität, Vertraulichkeit und Authentizität durch die jeweiligen technischen Verfahren gewährleistet werden und welche Besonderheiten in der praktischen Anwendung der jeweiligen Verfahren zu berücksichtigen sind.

3.1 Verschlüsselung

Mit der sogenannten *Verschlüsselung* werden die Daten und/oder Nachrichten mithilfe kryptografischer Verfahren in eine Folge von Zeichen überführt, die ohne Bedeutung und ohne Rückschlussmöglichkeit auf den tatsächlichen Inhalt ist. Das Entschlüsseln dieser Folge von Zeichen kann ohne einen Schlüssel nicht erfolgen. Die Qualität der Verschlüsselung hängt davon ab, wie leicht beziehungsweise schwer es mithilfe gegenwärtiger technischer Hilfsmittel möglich ist, den zur Entschlüsselung benötigten Schlüssel unberechtigterweise herauszufinden. Sichere Verfahren benötigen zur Schlüsselermittlung selbst bei Verwendung aller heute verfügbaren Rechnerkapazitäten viele Jahre. Einen Überblick über die jeweils als gegenwärtig sicher eingestuften kryptografischen Verfahren zur Verschlüsselung gibt die Bundesnetzagentur in einem jährlich aktualisierten Katalog heraus [BNA].

3.1.1 Ablauf

Zur Verschlüsselung ist ein Paar von Schlüsseln notwendig. Der eine Schlüssel wird zum Ver- und der andere Schlüssel zum Entschlüsseln verwendet. Es wird zwischen *symmetrischen* und *asymmetrischen* Verfahren unterschieden. Bei den symmetrischen Verfahren sind die Schlüssel zum Ver- und Entschlüsseln gleich (oder lassen sich leicht voneinander ableiten). Bei den asymmetrischen Verfahren werden unterschiedliche Schlüssel zum Ver- und Entschlüsseln verwendet. Asymmetrische Verfahren werden zum Verschlüsseln von E-Mails verwendet. Das asymmetrische Ver- und Entschlüsseln zwischen zwei Kommunikationspartnern A und B läuft dabei grob wie folgt ab:

1. A und B erzeugen jeweils ein Schlüsselpaar $(S_A^{\text{Ö}}, S_A^{\text{P}})$ und $(S_B^{\text{Ö}}, S_B^{\text{P}})$. Dabei sind $S_A^{\text{Ö}}$ und $S_B^{\text{Ö}}$ die *öffentlichen* Schlüssel von A und B und S_A^{P} und S_B^{P} die *privaten* Schlüssel von A und B.
2. A schickt seinen öffentlichen Schlüssel $S_A^{\text{Ö}}$ an B und B schickt seinen öffentlichen Schlüssel $S_B^{\text{Ö}}$ an A.
3. A verschlüsselt die für B vorgesehene E-Mail E_K (E-Mail als Klartext) mithilfe des öffentlichen Schlüssels $S_B^{\text{Ö}}$ von B. Es entsteht eine verschlüsselte E-Mail $E_V = \text{verschlüsselt}(E_K, S_B^{\text{Ö}})$. Diese verschlüsselte E-Mail E_V wird von A an B versendet.
4. B empfängt die E-Mail E_V und entschlüsselt diese mithilfe seines privaten Schlüssels S_B^{P} . Durch das Entschlüsseln erhält B die ursprüngliche E-Mail wieder im Klartext $E_K = \text{entschlüsselt}(E_V, S_B^{\text{P}})$.

5. Will B nun A antworten, so verwendet er zum Verschlüsseln den öffentlichen Schlüssel S_A^O von A und A entschlüsselt die von B erhaltene verschlüsselte E-Mail mithilfe seines privaten Schlüssels S_A^P .

3.1.2 Schlüsselaustausch

Generell muss also zum Verschlüsseln einer E-Mail der öffentliche Schlüssel des Empfängers bekannt sein. Dieser muss in den Besitz des Absenders gelangen. Dies stellt in der Praxis oft eine hohe Hürde dar, da entweder der Empfänger gar keinen öffentlichen Schlüssel besitzt oder aber dieser nur aufwändig (zum Beispiel durch Suche auf Zertifikatsservern oder auf der persönlichen Webseite des Empfängers) zu beschaffen ist. Ein weiterer praktischer Nachteil der Verschlüsselung besteht darin, dass die E-Mail nur vom Empfänger selbst (mithilfe seines privaten Schlüssels) entschlüsselt werden kann. Dies ist insbesondere in größeren Organisationen, in denen der Zugriff auf E-Mail-Konten oft delegiert wird, problematisch. Das Senden verschlüsselter E-Mails an mehrere Empfänger ist nicht möglich (und auch nicht sinnvoll), da das Verschlüsseln stets für genau einen Empfänger (die Person, die den passenden privaten Schlüssel besitzt) geschieht. Darüber hinaus ist die Verwaltung sowohl des eigenen privaten Schlüssels als auch der fremden öffentlichen Schlüssel aufwändig. Einerseits wäre ein Verlust (oder das Bekanntwerden) des eigenen privaten Schlüssels fatal, andererseits führt eine redundante Speicherung des privaten Schlüssels an mehreren Sicherungsspeicherorten zu einem erhöhten Risiko. Das Entziehen des öffentlichen Schlüssels, das durch den Verlust des privaten Schlüssels notwendig wird, ist kompliziert und wird bei Risikobetrachtungen häufig vernachlässigt.

3.1.3 Werkzeuge

Das Bundesamt für Sicherheit in der Informationstechnik stellt ein kostenloses Werkzeug zur Verschlüsselung von E-Mails bereit. Dieses Werkzeug Gpg4win kann in E-Mail-Programme, wie zum Beispiel Microsoft Outlook eingebunden werden. Gpg4win basiert auf dem ebenfalls frei erhältlichen Werkzeug GnuPG.

Sowohl De-Mail, der e-Postbrief als auch das EGVP verwenden Verschlüsselungen zum E-Mail-Austausch. Es unterscheiden sich diese Verfahren jedoch darin, ob standardmäßig eine durchgehende Verschlüsselung vom Absender bis zum Empfänger erfolgt. Dies ist nur beim EGVP der Fall (siehe Abschnitt 4).

3.1.4 Bewertung

Verschlüsselungsverfahren wahren die Integrität und die Vertraulichkeit der übersandten Daten. Die Authentizität jedoch ist nur mittelbar gewahrt. Zwar werden bei der Erstellung der Schlüsselpaare vertrauenswürdige Zertifikatsstellen (je nach Zertifikat wird eine Hierarchiekette des Vertrauens oder ein Netz des Vertrauens verwendet) eingebunden, die dabei gemachten Angaben über beispielsweise den Namen des Nutzers werden jedoch nicht geprüft.

Für einen allgemeinen Einsatz in der Verwaltung und Justiz sind die Verschlüsselungsverfahren aufgrund der genannten praktischen Nachteile nicht geeignet.

3.2 Elektronische Signatur

Bereits seit 1997 gibt es gesetzliche Rahmenbedingungen für den Einsatz elektronischer Signaturen in Deutschland. Von besonderer Bedeutung ist dabei die *qualifizierte elektronische Signatur*, die die höchsten Sicherheitsanforderungen an eine elektronische Signatur stellt. Die qualifizierte elektronische Signatur ist eine mit einem privaten Schlüssel verschlüsselte Datei, die Informationen über ein, dieser qualifizierten elektronischen Signatur zugeordnetem Dokument enthält. Die qualifizierte elektronische Signatur kann nur mit dem öffentlichen Schlüssel entschlüsselt werden, der zu dem zur Verschlüsselung der Signatur verwendeten privaten Schlüssel gehört. Das Schlüsselpaar aus privatem und öffentlichem Schlüssel wurde dabei von einer Zertifizierungsstelle erzeugt, bei der die Identität des Schlüsselpaarinhabers hinterlegt ist. Mit der qualifizierten elektronischen Signatur ist somit die Authentizität sichergestellt. Sie kann auch jederzeit bei den Trustcentern, die die Signatur ausgestellt haben, nachgeprüft werden.

Die in der qualifizierten elektronischen Signatur enthaltenen Informationen über das signierte Dokument sichern darüber hinaus die Integrität des Dokumentes. Dies wird dadurch sichergestellt, dass ein sogenannter Hashwert für das Dokument erstellt wird. Hashwertberechnungen werden verwendet, um große Datenmengen, zum Beispiel elektronische Dokumente oder elektronische Akten, auf einen kleinen, eindeutigen Wert abzubilden. Dieser Hashwert liefert mithilfe kryptografischer Verfahren eine eindeutige Prüfsumme für dieses Dokument. Wird das Dokument geändert, so ändert sich auch die Prüfsumme (der Hashwert).

Das Verfahren zur qualifizierten elektronischen Signatur besteht aus drei Teilschritten:

1. dem Ausstellen einer Signaturkarte,
2. dem Signieren einer Datei oder eines Dokumentes sowie
3. dem Prüfen der Signatur.

3.2.1 Das Ausstellen der Signaturkarte

Um qualifiziert elektronisch signieren zu können, ist eine Signaturkarte erforderlich. Diese wird von einem Trustcenter ausgestellt. Das Trustcenter prüft die Identität der die Signaturkarte beantragenden natürlichen Person. Dies kann beispielsweise über das Post-Ident-Verfahren erfolgen. Nach Prüfung der Identität des Antragstellers generiert das Trustcenter ein Schlüsselpaar¹⁴, das aus einem öffentlichen und einem privaten Schlüssel besteht. Das Trustcenter speichert die zu diesem Schlüsselpaar zugehörige

¹⁴ Auf Basis von Zufallszahlengeneratoren (siehe Bundesnetzagentur, Übersicht über geeignete Algorithmen, Mai 2011, online abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011_2_AlgoKatpdf.pdf?__blob=publicationFile)

Identität. Der öffentliche Schlüssel wird durch das Trustcenter in einem öffentlichen Verzeichnis zum Abruf bereitgestellt.¹⁵

3.2.2 Das Signieren einer Datei

Das Signieren einer Datei erfolgt in zwei Schritten. Zunächst wird der Hashwert dieser Datei mithilfe eines Verfahrens zur Hashwertberechnung¹⁶ gebildet. Für jede Datei ist dieser Hashwert eindeutig. Eine Änderung an der Datei bewirkt auch einen neuen Hashwert. Das Verfahren der Hashwertberechnung ist eine Funktion der Signaturanwendungskomponente¹⁷ (Soft- und Hardware zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen).

In einem zweiten Schritt wird der Hashwert mithilfe kryptographischer Verfahren (den sogenannten Signaturverfahren)¹⁸ mit dem privaten Schlüssel, der auf der Signaturkarte gespeichert ist, verbunden. Dazu ist die Eingabe einer PIN am Kartenlesegerät notwendig, um die Authentizität des Signierenden zu sichern. Die Kombination aus Hashwert und privatem Schlüssel ist die qualifizierte elektronische Signatur. Die Signaturverfahren sind ebenfalls Funktionen der Signaturanwendungskomponente.

Im Ergebnis liegen nach dem Signieren einer Datei demnach zwei Dateien vor; die signierte Datei und die Signatur, die den Hashwert der signierten Datei und den persönlichen Schlüssel des Signierenden enthält.

Zum Anbringen einer qualifizierten elektronischen Signatur sind nach § 2 SigG eine den Anforderungen des Signaturgesetzes entsprechende sichere Signaturerstellungseinheit (Signaturkarte und Kartenleser) sowie eine Signaturanwendungskomponente (die Software) erforderlich. Für die Software muss entweder eine Prüfung und Bestätigung nach Signaturgesetz erfolgt sein oder die Bundesnetzagentur hat eine entsprechende Herstellererklärung des Softwareanbieters veröffentlicht.¹⁹

¹⁵ Tatsächlich werden nicht nur der öffentliche Schlüssel, sondern gleichzeitig auch noch die Identität desjenigen bereitgestellt, der den zu dem öffentlichen Schlüssel korrespondierenden privaten Schlüssel besitzt. Diese Kombination aus öffentlichem Schlüssel und Identitätsinformationen wird „Zertifikat“ genannt. „Qualifizierte Zertifikate“ sind nach § 2 SigG „elektronische Bescheinigungen, mit denen Signaturprüfchlüssel einer natürlichen Person zugeordnet werden und die Identität dieser Person bestätigt wird.“ Diese Zertifikate müssen die „Voraussetzungen des § 7 erfüllen und von Zertifizierungsdiensteanbietern ausgestellt werden, die mindestens die Anforderungen nach den §§ 4 bis 14 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen.“

¹⁶ In der von der Bundesnetzagentur am 20. Mai 2011 veröffentlichten Übersicht über geeignete Algorithmen zur elektronischen Signatur sind die Verfahren SHA-256, SHA-384, SHA-512 als bis 2017 geeignet (das heißt sicher) aufgeführt (SHA = secure hash algorithm, die Zahl gibt die Länge des Hashwertes in bit an)

¹⁷ Siehe § 2 Nr. 11 SigG

¹⁸ In der von der Bundesnetzagentur am 20. Mai 2011 veröffentlichten Übersicht über geeignete Algorithmen zur elektronischen Signatur sind RSA-Verfahren mit den Parametern 176 bit (Mindestwert) beziehungsweise 2048 bit (empfohlen), DSA-Verfahren mit den Parametern 2048 bit und 256 bit sowie DSA-Varianten mit dem Parameter q=250 bit als bis 2017 geeignet (das heißt sicher) aufgeführt.

¹⁹ Nach § 17 Absatz 4 SigG

3.2.3 Das Prüfen einer Signatur

Auch das Prüfen einer Signatur ist ein zweistufiges Verfahren. Zunächst wird von der zu prüfenden Datei ein Hashwert mit dem gleichen Verfahren gebildet, wie es bei der Erstellung der Signatur verwendet wurde. Danach wird die Signatur mithilfe des öffentlichen Schlüssels entschlüsselt. Dies gelingt nur, wenn der vorgebliche Signierende auch tatsächlich derjenige war, der die Signatur erstellt, das heißt wenn sein privater Schlüssel zum Signieren verwendet wurde. Nur dann ist es auch möglich mit dem dazugehörigen öffentlichen Schlüssel, die Signatur zu entschlüsseln. Nach dem Entschlüsseln der Signatur ist der beim Signieren erstellte Hashwert lesbar und kann mit dem im ersten Schritt gebildeten Hashwert verglichen werden. Sind beide Hashwerte gleich, so wurde die Datei seit dem Signieren nicht mehr verändert. Für das Prüfen von Signaturen stehen diverse auch kostenfreie Programme bereit.

3.2.4 Bewertung

Obwohl für das Verfahren der qualifizierten elektronischen Signatur seit bereits fast 15 Jahren eine rechtliche Grundlage existiert, hat es sich noch nicht durchgesetzt und wird aufgrund der aufwändigen praktischen Handhabung kritisiert [BLK11]. Dies hängt insbesondere damit zusammen, dass der Einsatz der qualifizierten elektronischen Signatur in Behörden nicht den herkömmlichen Büroabläufen angepasst ist. Die qualifizierte elektronische Signatur ist genau einer Person, nicht jedoch einer Behörde zugeordnet, was einerseits einen organisatorischen Mehraufwand in einer Behörde zulasten eines Einzelnen bedeutet und andererseits oft über das Ziel hinausgeht, wenn nämlich die absendende Person im Gegensatz zur absendenden Behörde unwichtig ist. Darüber hinaus ist bei der Archivierung von mit der qualifizierten elektronischen Signatur signierten Dokumenten zu beachten, dass Zertifikate ablaufen und ein spätes Prüfen der Signatur und der Integrität der damit assoziierten Dokumente einen zusätzlichen Organisationsaufwand (zum Beispiel durch Übersignieren) hervorruft.

So wurde beispielsweise in dem (allerdings nicht vom Bundesrat zugestimmten) Steuervereinfachungsgesetz 2011 vorgesehen, die Anforderungen an elektronische Rechnungen derart zu vereinfachen, dass eine qualifizierte elektronische Signatur unter einer solchen elektronischen Rechnung nicht mehr notwendig ist.

Generell gilt zu beachten, dass die Verwendung qualifizierter elektronischer Signaturen die mit diesen Verfahren versehenen Dateien *nicht* vor Änderungen schützen, sondern diese nur nachweisbar machen. Insbesondere bietet die qualifizierte elektronische Signatur keinen Schutz der Vertraulichkeit, da das signierte Dokument nicht verschlüsselt wird. Die Gewährleistung der Sicherheit der elektronischen Kommunikation unter abschließlichem Einsatz der qualifizierten elektronischen Signatur ist somit nicht gegeben.

Sowohl De-Mail, der e-Postbrief als auch das EGVP unterstützen den Einsatz qualifizierter elektronischer Signaturen. Bei De-Mail und dem e-Postbrief kommen qualifizierte elektronische Signaturen optional zum Einsatz, wenn der Absender einer E-Mail zusätzlich durch den Provider bestätigt wird und wenn eine Empfangsbestätigung (Einschreiben) erforderlich ist. Beim EGVP werden qualifizierte elektronische Signaturen

automatisch ausgestellt. Beim EGVP werden auch automatisch Empfangsbestätigungen übersandt.

4 Neuentwicklungen für die sichere E-Mail-Kommunikation

Aufgrund der beschriebenen Nachteile der bereits bekannten und in Abschnitt 3 beschriebenen technischen Möglichkeiten zur sicheren E-Mail-Kommunikation sind in den letzten Jahren Verfahren und Infrastrukturen entwickelt worden, die eine sichere E-Mail-Kommunikation zwischen Privatpersonen und Behörden ermöglichen sollen. Diese werden im Folgenden diskutiert.

4.1 De-Mail

De-Mail wurde am Bundesministerium des Innern entwickelt. Die oberste Aufsichtsbehörde des De-Mail-Systems ist das Bundesamt für Sicherheit in der Informationstechnik. Im Mai 2011 trat das De-Mail-Gesetz [DeMG] in Kraft. Das Gesetz sieht vor, einen „sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet“ sicherzustellen. Dazu werden private E-Mail-Provider zertifiziert und als De-Mail-Provider akkreditiert. Dieser aufwändige Zertifizierungs- und Akkreditierungsprozess hat offiziell zu einer Verzögerung des Starts von De-Mail geführt, der nunmehr für Ende 2011 geplant ist. Von Oktober 2009 bis März 2010 wurde De-Mail in einem Pilotprojekt in Friedrichshafen mit den E-Mail-Providern Deutsche Telekom, GMX, T-Systems und WEB.DE von Behörden, Bürgern und Unternehmen getestet.

De-Mail ist kein zentral betriebener Dienst. Vielmehr können sich beliebig viele private E-Mail-Provider als De-Mail-Dienstanbieter nach § 17 De-Mail-Gesetz vom Bundesamt für Sicherheit in der Informationstechnik zertifizieren und akkreditieren lassen. Dies bedeutet auch, dass kein zentrales Verzeichnis aller De-Mail-Nutzer existiert, sondern dass jeder De-Mail-Dienstanbieter seine eigenen De-Mail-Nutzer nach den Vorgaben von § 3 des De-Mail-Gesetzes verwaltet.

De-Mail steht allen Bürgern, Behörden und Unternehmen kostenpflichtig zur Verfügung. Datenschützer kritisieren De-Mail teilweise heftig [Le11, Sch11]. Ihre Kritik ist, dass eine Ende-zu-Ende-Verschlüsselung, das heißt die durchgehende Verschlüsselung vom Absender bis zum Empfänger einer Nachricht, in De-Mail nicht verpflichtend ist. Dem ist einerseits entgegenzuhalten, dass die Ende-zu-Ende-Verschlüsselung in De-Mail möglich ist, wenn Empfänger und Absender dem Speichern ihrer öffentlichen Schlüssel im De-Mail-System zugestimmt haben. Andererseits erfolgt das Ent- und erneute Verschlüsseln beim Provider automatisiert und in einem Zeitraum von „wenigen Millisekunden bis zu einer Sekunde“ [BSIb]. Es bleibt darüber hinaus offen, ob ein zertifizierter und akkreditierter De-Mail-Provider ein Unbefugter im Sinne der Definition der Vertraulichkeit ist. Es erscheint vielmehr gerechtfertigt, Nachrichten automatisiert auf Viren oder ähnliche Gefährdungen zu prüfen, solange sichergestellt wird, wie es im Zertifizierungs- und Akkreditierungsprozess geprüft wird, dass eine Kenntnis-

nahme, Speicherung und Änderung der Nachrichteninhalte durch Dritte ausgeschlossen ist.

Vielmehr ist die Sicherung der Integrität der übersandten Nachrichten und Daten insofern problematischer, als durch das automatisierte Ent- und Verschlüsseln der Nachricht, dem Prüfen auf Viren und dem dazu notwendigen temporärem Zwischenspeichern die Prüfsumme (der Hashwert) über die Daten bereits verändert werden könnte, obwohl die Inhaltsdaten nicht geändert wurden. Nach § 5 Absatz 3 De-Mail-Gesetz ist der De-Mail-Diensteanbieter jedoch verpflichtet, die Integrität der Daten sicherzustellen, auch dann, wenn eine Ende-zu-Ende-Verschlüsselung durch den Nutzer nicht verwendet wird. Es bleibt bis zur Einführung von De-Mail abzuwarten, ob die Sicherung der Integrität automatisiert prüfbar bleibt oder ob die Sicherung der Integrität aufgrund der technischen Umsetzung der rechtlichen Anforderungen zweifelsfrei angenommen werden kann.

Zur Registrierung beim De-Mail-System muss der zukünftige Nutzer sich eindeutig identifizieren. Der Provider, bei dem sich der Nutzer registriert, kann somit eindeutig ein Postfach einer Identität zuordnen. Dies gilt auch dann, wenn für die De-Mail-Adresse ein Pseudonym verwendet wird. Unter der Annahme, dass eine Anmeldung an das De-Mail-System nur mithilfe von Nutzernamen und Passwort als nicht sicher gilt, ist die Anmeldung an De-Mail über das gesicherte Verfahren nach § 4 De-Mail-Gesetz, das heißt die Verwendung von „zwei geeigneten und voneinander unabhängigen Sicherungsmitteln“, zu verlangen, um die Authentizität sicherzustellen.

Die Praktikabilität von De-Mail wird insbesondere durch Plug-Ins unterstützt, die eine Verwendung von De-Mail in herkömmlichen E-Mail-Programmen, wie zum Beispiel Microsoft Outlook, ermöglicht [Men].

4.2 e-Postbrief

Der e-Postbrief wird durch die Deutsche Post AG bereits seit Juli 2010 zur Verfügung gestellt. Der e-Postbriefdienst und somit auch die Verwaltung der e-Postbrief-Nutzer-Adressen werden zentral betrieben. Ein e-Postbrief kostet 0,55 Euro, mit Einschreiben 2,15 Euro. Die Deutsche Post hat angekündigt, als De-Mail-Provider zu agieren, sobald De-Mail eingeführt wird.

Die Kommunikation erfolgt verschlüsselt. Dabei wird TLS (Transport Security Layer) verwendet, ein Verschlüsselungsprotokoll zur Datenübertragung. Wie bei De-Mail wird auch hier die Nachricht beim Provider ent- und wieder verschlüsselt. Auch für den e-Postbrief eine Ende-zu-Ende-Verschlüsselung möglich.

Im Gegensatz zu De-Mail unterliegt der e-Postbrief jedoch nicht den gesetzlichen Anforderungen des De-Mail-Gesetzes. Bei dem e-Postbriefdienst handelt es sich um ein hybrides Verfahren. Das bedeutet, dass ein e-Postbrief, dessen Empfänger keine e-Postadresse besitzt, ausgedruckt und als herkömmlicher Papierbrief dem Empfänger zugestellt wird. Bei diesem Prozess ist die Vertraulichkeit nicht gewahrt. Die Deutsche Post unterliegt als Betreiber des e-Postbriefes auch keiner Akkreditierung und ist auch

nicht gesetzlich verpflichtet, die Integrität zu wahren. In einem Urteil des Landgerichtes Bonn vom August 2011 wurde entschieden, dass die Aussage der Deutschen Post, „der E-Postbrief ist so sicher und verbindlich wie der Brief“, unwahr ist [LGBö].

Die Registrierung bei e-Postbrief erfolgt über das Post-Ident-Verfahren. Für die Anmeldung gibt es, wie bei De-Mail, zwei Sicherheitsstufen. Die normale Anmeldung erfolgt durch Benutzername und Passwort. Bei der hohen Sicherheitsstufe wird zusätzlich die Eingabe einer mobilen TAN abgefragt. Die Authentizität ist somit bei dem e-Postbrief gewahrt.

Die Praktikabilität des e-Postbriefes wird dadurch erschwert, dass eine Integration des e-Postbriefes in herkömmliche E-Mail-Programme derzeit noch nicht möglich ist, so dass für das Empfangen und Versenden von e-Postbriefen stets die Webanwendung der Post AG in einem Browser geöffnet werden muss.

4.3 EGVP

Das Elektronische Gerichts- und Verzeichnispostfach (EGVP), das durch die Bundesländer und den Bund im Verbund für die Justiz entwickelt wurde, steht in der aktuellen Version 2.6 Gerichten, Staatsanwaltschaften, Notaren und Anwälten kostenfrei zur elektronischen Kommunikation zur Verfügung und wird gegenwärtig von rund 40 000 Nutzern verwendet. Für Handelsregistereinträge und in Mahnsachen ist die Verwendung des EGVP verbindlich. Monatlich werden über das EGVP rund 400 000 Nachrichten versendet.

Um das EGVP nutzen zu können, ist die Installation eines separaten Clients erforderlich. Eine Einbindung in etablierte E-Mail-Programme, wie zum Beispiel Microsoft Outlook oder Thunderbird ist nur mit einem kostenpflichtigen Plug-In, das am Markt erhältlich ist, möglich. Mithilfe der ab November 2011 erhältlichen EGVP-Version „Enterprise“ soll eine Einbindung des EGVP-Clients in Fachverfahren möglich werden, so dass keine separate Installation des EGVP-Clients mehr notwendig ist.

Zur Gewährleistung der Vertraulichkeit werden die Nachrichten im EGVP Ende-zu-Ende verschlüsselt. Als Übertragungsprotokoll der Kommunikation wird OSCI verwendet. Die Verwaltung der Nutzer und deren Schlüssel erfolgt mithilfe des Registrierungsdienstes S.A.F.E. (Secure Access to Federated e-Justice/e-Government), der in der aktuellen Version 1.4 ebenfalls kostenfrei angesprochen werden kann und in Zukunft nicht nur als Registrierungsdienst für das EGVP, sondern darüber hinaus auch für weitere Anwendungen, wie zum Beispiel das Zentrale Testamentsregister, verwendet wird. Die Integrität der Nachrichten kann mithilfe der qualifizierten elektronischen Signatur, die an jede Nachricht angefügt werden kann, überprüft werden.

Der Benutzerkreis des EGVP ist geschlossen. Es wird unterschieden zwischen Nutzern, die ein sogenanntes EGVP-Backend (zum Beispiel Gerichte) besitzen und solche mit einem EGVP-Bürgerclient (zum Beispiel Rechtsanwälte und Notare). Ein Versenden von Nachrichten ist nur zwischen Backends, zwischen Backends und Clients, nicht jedoch zwischen Clients möglich. Ein Registrieren bei EGVP kann ohne den Nachweis

der Identität erfolgen. Die Anmeldung erfolgt mit Softwarezertifikaten. Das EGVP ermöglicht als Signaturanwendungskomponente das Anbringen von Signaturen an Nachrichten. Die Authentizität ist beim EGVP somit nur gewährleistet, wenn die Nachricht qualifiziert elektronisch signiert wurde.

Auf dem IT-Gipfel 2012 wurde eine Zusammenarbeit von EGVP und De-Mail vereinbart [Bec11]. Dabei sollen die Nutzerkreise dieser Systeme gegenseitig geöffnet werden, so dass eine gegenseitige Adressierung und somit eine Kommunikation zwischen den Systemen ermöglicht wird.

5 Zusammenfassung und Ausblick

Die in diesem Papier diskutierten neuen Infrastrukturen für eine sichere E-Mail-Kommunikation erfüllen prinzipiell die Anforderungen an die Sicherheit. Das EGVP ist aufgrund der Ende-zu-Ende-Kommunikation im Zusammenspiel mit der qualifizierten elektronischen Signatur bezüglich der Wahrung der Integrität, Authentizität und der Vertraulichkeit am stärksten. Nachteile des EGVP liegen aufgrund der fehlenden Überprüfung der registrierten Identitäten und des einfachen Anmeldevorgangs am EGVP-Client, da die zusätzliche Anbringung einer qualifizierten elektronischen Signatur erforderlich ist, um die Authentizität zu sichern. Das EGVP steht grundsätzlich auch für die Kommunikation mit Verwaltungsbehörden zur Verfügung. Allerdings sind nach derzeitigem Stand nur wenige Verwaltungen oder öffentliche Einrichtungen (zum Beispiel IHKs) über das EGVP erreichbar.

Für die Kommunikation zwischen Bürger und Verwaltungen wurden die vorgestellten Infrastrukturen De-Mail und der e-Postbrief entwickelt. Diesen beiden fehlt eine verbindlich zu nutzende Ende-zu-Ende-Verschlüsselung. Bei beiden Verfahren ist diese jedoch optional verwendbar. Es ist jedoch fraglich, ob die maschinell und im Sekundenbruchteil durchgeführte Ent- und Verschlüsselung einen Bruch der Vertraulichkeit darstellt. Akkreditierte Diensteanbieter sind vielmehr verpflichtet, die Vertraulichkeit zu gewährleisten. Dasselbe gilt für die Sicherstellung der Integrität der übersendeten Nachrichten und Daten. Hierbei ist jedoch zu beachten, dass diesbezüglich nur sichergestellt werden muss, dass die Integrität der versendeten Nachrichten und Daten verletzt, das heißt dass sie während der Übertragung geändert wurden. Hierbei bleibt jedoch offen, wie sichergestellt werden soll, dass positive Fehler vermieden werden, das heißt eine geänderte Prüfsumme suggeriert eine Änderung der Daten ohne dass tatsächlich eine inhaltliche Änderung passierte. Im Gegenteil zum EGVP werden bei der Registrierung für De-Mail und e-Postbrief die Identitäten geprüft. De-Mail ist im Vergleich zum e-Postbrief insofern praktikabler, als dass für De-Mail bereits heute Integrationsmöglichkeiten in herkömmliche E-Mail-Programme verfügbar sind. Eine parallele Verwendung von Webanwendungen im Browser wird dadurch vermieden. Dies wird auch mit der entstehenden EGVP-Enterprise-Version möglich, wobei das EGVP dabei in Fachverfahren integriert wird.

Literaturverzeichnis

- [Bac11] Bachmann, R.: „E-Mail Plugin für De-Mail vorerst nur für Firmen“, 2011, Blog-Beitrag, online abrufbar unter <http://baetschman.ralfbachmann.de/2011/02/>
- [Bec11] Beck-Aktuell: „IT-Gipfel 2011: De-Mail soll Kommunikation mit Gerichten erleichtern“, 2011, online abrufbar unter <http://beck-aktuell.beck.de/news/it-gipfel-2011-de-mail-soll-kommunikation-mit-gerichten-erleichtern>
- [BLK11] Bericht der Bund-Länder-Kommission, Unterarbeitsgruppe: „Konsequenzen der Ausweitung des elektronischen Rechtsverkehrs in kontradiktorischen Verfahren“, 2011, S.6
- [BSI] Bundesamt für Sicherheit in der Informationstechnik. Glossar der IT-Grundschutz-Kataloge. Online abrufbar unter https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html
- [BSIb] Bundesamt für Sicherheit in der Informationstechnik, De-Mail verbessert die Sicherheit in der E-Mail-Kommunikation. BSI: Kritik an der Sicherheit der De-Mail ist unbegründet, 2010, online abrufbar unter https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2010/De_Mail_Sicherheit_E_Mail_230710.html
- [BNA] Bundesnetzagentur. Algorithmenkatalog. Online abrufbar unter http://www.bundesnetzagentur.de/cln_1912/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen_node.html
- [DeMG] De-Mail-Gesetz, 2011, online abrufbar unter <http://www.gesetze-im-internet.de/de-mail-g/index.html>
- [Eck09] Eckert, C.: IT-Sicherheit. Konzepte, Verfahren, Protokolle. 6. Auflage, Oldenbourg Verlag, München, 2009
- [Lap11] Lapp, T., EGVP funktioniert nicht mal innerhalb der Justiz, Beck-Blog, 2011. Online abrufbar unter <http://blog.beck.de/2011/09/06/egvp-funktioniert-nicht-mal-innerhalb-der-justiz>
- [Le11] Lechtenbörger, J., Zur Sicherheit von De-Mail, Datenschutz und Datensicherheit 4, 2011
- [LGBö] Landgericht Bonn, Urteil vom 30. Juni 2011 – 14 O 17/11
- [Men] Mentana-Claimsoft AG, Homepage des Unternehmens zu DeMail: <http://mentana-claimsoft.de/de-mail-fuer-unternehmen.html>
- [Sch11] Schaar, P.: De-Mail: Wer sicher gehen will, sollte verschlüsseln!, Mitteilung des Bundesbeauftragten für Datenschutz und Informationsfreiheit, 12/2011. Online abrufbar unter http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/12_InkrafttretenDEMailGesetz.html?nn=408908

