Lars Wittmaack, Bernhard Esslinger, Ludger Schmidt, Benjamin Strenge, Arno Wacker

Vertrauensvolle E-Mail-Kommunikation

Technische Grundlagen der E-Mail(-Verschlüsselung)

Der „elektronische Brief“ bzw. die elektronische Mail (E-Mail) ist seit über 30 Jahren im privaten wie beruflichen Umfeld im Einsatz. Behörden, Steuerbüros, Krankenhäuser, Finanzinstitute und viele weitere Gruppen versenden und empfangen E-Mails, um Informationen auszutauschen. Innerhalb kurzer Zeit findet eine E-Mail ihren Weg vom Sender in Deutschland zum Empfänger in beispielsweise den USA. Wie funktioniert das? Und was hat es mit E-Mail-Verschlüsselung auf sich? Dieser Artikel betrachtet die grundlegende technische Funktionsweise der E-Mail sowie Hintergründe und Funktionsweise der Verschlüsselung mit S/MIME und PGP.

E-Mail ist – trotz neuer Kommunikationsformen (wie Instant Messaging und Soziale Netzwerke) – noch immer das häufigste Kommunikationsmedium im Internet[1]. Als elektronisches Äquivalent des postalischen Briefes hat sie Einzug in alle Lebensbereiche gehalten: E-Mail-Adresse des Empfängers eingeben, Text der Nachricht tippen und auf „Senden“ klicken – fertig. Was sich leicht anhört, musste technisch jedoch erst so weit gebracht werden.

Eine solche einfache, konsistente und weltweit interoperable Nutzung der E-Mail setzt voraus, dass technisch die „gleiche Sprache“ gesprochen wird. Andernfalls lassen sich Informationen nicht automatisiert verarbeiten. Es galt daher, Standards zu schaffen für Formate, die Informationen strukturieren, und Protokolle, um die strukturierten Informationen zwischen Systemen zu übertragen. Durchgesetzt haben sich die Standards der Internet Engineering Task Force (IETF).[2] Ihre Mission lautet „*to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet*“[3].

Die IETF verwaltet Standards in Form sogenannter Requests for Comments (RFCs). Grundlage der heutigen E-Mail-Kommunikation sind korrespondierende, über die Jahre geschaffene und kontinuierlich überarbeitete RFCs. Wesentlich für E-Mail sind:

- Formate
  - RFC 5322 Internet Message Format
  - RFC 2045 Multipurpose Internet Mail Extensions (MIME)
- Protokolle
  - RFC 5321 Simple Mail Transfer Protocol (SMTP)
  - RFC 3501 Internet Message Access Protocol (IMAP)
  - RFC 1939 Post Office Protocol – Version 3 (POP3)
- Sicherheitserweiterungen
  - RFC 5751 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2
  - RFC 4880 OpenPGP Message Format
  - RFC 3156 MIME Security with OpenPGP (PGP/MIME)

Während die Formate in der Regel vom Anwender kaum wahrzunehmen sind, dürften die drei Protokolle vielen Anwendern unter den Abkürzungen SMTP, IMAP und POP3 bereits ein Begriff sein. Bei der Konfiguration einer neuen privaten E-Mail-Adresse sind zu diesen Protokollen Einstellungen vorzunehmen (z.B. die IP-Adresse des Mail-Providers).

Sicherheitserweiterungen spezifizieren die Einbindung kryptographischer Dienste (wie verschlüsselte Nachrichten) in das S/MIME-Format. Für den Einsatz kryptographischer Dienste werden darüber hinaus Standards und Protokolle zu Verschlüsselungsalgorithmen und Schlüsselaustauschverfahren benötigt. Möglichkeiten zur Integration solcher Sicherheitsstandards in eine konsistente, benutzerfreundliche Lösung werden im Folgeartikel „xxxx“ (Seite xxx) beschrieben. In diesem Artikel widmen wir uns den technischen Grundlagen der E-Mail und deren Verschlüsselung anhand der Standards und entlang von 6 Fragen:

Wie sieht eine E-Mail technisch aus?

RFC 5322 (Internet Message Format) ist die grundlegende Spezifikation der Struktur einer textbasierten E-Mail. Sie beinhaltet noch nicht die Übertragung anderer Formate, wie Bilder oder Audio; diese sind in weiteren RFC-Erweiterungen spezifiziert. Zur Darstellung des Konzeptes der E-Mail und deren Übertragung soll uns eine Text-basierte E-Mail genügen.

Zur Veranschaulichung werden wir ein (erfundenes) E-Mail-Beispiel verwenden: Robert Sender (mit der E-Mail-Adresse robert.sender@gosec.de) sendet seinem amerikanischen Anwalt, Bob Receiver (mit der E-Mail-Adresse bob.receiver@attorney.com) eine E-Mail, in der er sich nach dem Stand von Verträgen erkundigt. Robert verfasst dazu die Abbildung 1 dargestellte E-Mail.

Bei der E-Mail wird – äquivalent zur realen Post – zwischen Umschlag (envelope) und Inhalt (contents) unterschieden. Nachdem Robert auf “Senden” geklickt hat, wird der Inhalt der E-Mail durch die E-Mail-Software in das Internet Message Format (RFC 5322) überführt. Dieser RFC spezifiziert dabei ausschließlich den Inhalt.

[1] http://newsroom.gmx.net/2015/03/23/studie-e-mail-nutzung-nimmt-weiter-zu/ Laut 1&1 wuchs gegenüber 2014 das echte, um Spam bereinigte Mail-Aufkommen 2015 in Deutschland um mehr als 6 % auf insgesamt 537 Milliarden. http://www.worldbank.org/en/publication/wdr2016 Laut dem aktuellen World Development Report 2016 der Weltbank ("DIGITAL DIVIDENDS") werden pro Tag 207 Mrd. E-Mails gesendet, 8,8 Mrd. YouTube-Videos angesehen und 4,2 Mrd. Google-Suchanfragen gestellt.

[2] Frühere Konkurrenzentwürfe von ITU-T oder ISO/IEC sind bedeutungslos.

[3] The Internet Engineering Task Force (IETF®): http://ietf.org/

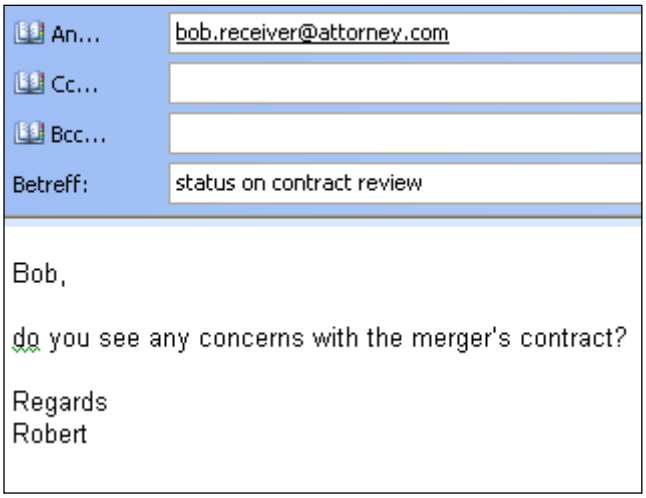

Abbildung 1: Verfasste E-Mail im E-Mail-Programm des Senders

Der Umschlag wird aus den Mailadressen erstellt und enthält alle Informationen, die für die Übertragung und Zustellung der E-Mail notwendig sind. Umschlag und Übertragung werden im Simple Mail Transfer Protocol (RFC 5321) spezifiziert. Informationen aus dem Inhalt können dabei für den Umschlag verwendet werden, müssen aber nicht.

Der Inhalt ist vom Umschlag getrennt und strukturiert die zu übertragenden Daten. Der Inhalt ist als Zeichenfolge spezifiziert und entspricht damit, grob gesprochen, einem Text mit mehreren Zeilen. Er muss jedoch einer definierten Syntax folgen. Er MUSS mit einem Header beginnen und KANN einen Body haben. Der Header entspricht einer festgelegten Struktur mit Datenfeldern (fields), wobei die Datenfelder in beliebiger Reihenfolge erstellt werden können. Bedeutung, Inhalte und Verarbeitung der definierten Datenfelder sind im RFC vermerkt. Es müssen minimal diese zwei Datenfelder verwendet werden:

Datenfeld	=	Feldtitel	Inhalt
orig-date	=	"Date:"	date-time
from	=	"From:"	mailbox-list

Das Internet Message Format wird durch die Multi Purpose Internet Mail Extensions (MIME) (RFC 2045-2049) ergänzt. Die MIME-Standards heben die Einschränkung des RFC 5322 in Bezug auf die Übertragung von Nicht-Text-Inhalten auf, indem zusätzliche Strukturen und Informationen über den Typ der übermittelten Daten (Content-Type-Feld, Internet Media Type) und der Zeichenkodierung (Content-Transfer-Encoding) spezifiziert werden.

Der Body folgt keiner festen Struktur. Er ist eine freie Sequenz von Zeichen. Header und Body werden durch eine Leerzeile voneinander getrennt. Im Falle unseres Beispiels sieht die technische Darstellung der E-Mail folgendermaßen aus:

```
-----------------------------------
Message-ID: <56DC363A.6050603@gosec.de>
Date: Sun, 06 Mar 2016 14:52:58 +0100
From: Robert Sender <rob-
ert.sender@gosec.de>
User-Agent: Mozilla/5.0 (Windows; U;
Windows NT 5.1; de; rv:1.9.2.13)
Gecko/20101207 Thunderbird/3.1.7
MIME-Version: 1.0
To: bob.receiver@attorney.com
Subject: status on contract review
Content-Type: text/plain; charset=UTF-8;
format=flowed
Content-Transfer-Encoding: 8bit

Bob,

do you see any concerns with the mer-
ger’s contract?

Regards
Robert
-----------------------------------
```

Gut zu erkennen ist die Trennung von Header und Body mit der Leerzeile vor „Bob,“.

Abbildung 2 zeigt die Darstellung der E-Mail beim Empfänger.

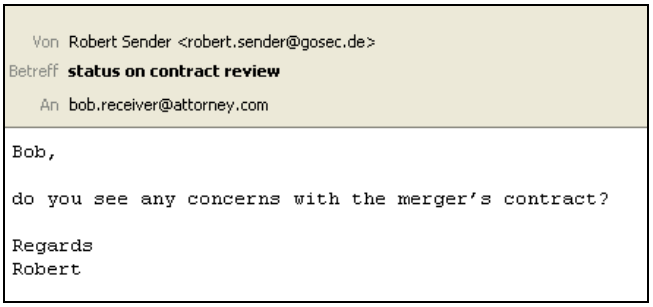

Abbildung 2: Empfangene E-Mail im E-Mail-Programm

Die technische Darstellung wird vom E-Mail-Programm des Empfängers aufbereitet und angezeigt. Dabei werden üblicherweise einige Informationen ausgelassen, die für Nutzer von geringem Interesse sind (beispielsweise Informationen des Felds „User Agent“).

Wie ist die E-Mail zum Empfänger gekommen?

Die empfangene E-Mail sieht technisch folgendermaßen aus:

```
-----------------------------------
Return-Path: <robert.sender@gosec.de>
Received: from mout.gosec.de
([218.107.12.17]) by mx-ha.attorney.com
(attorney006) with
 ESMTPS (Nemesis) id 0Lms1s-1ZvnFh42Vo-
00h3Bt for <bob.receiver@attorney.com>;
 Sun, 06 Mar 2016 14:53:09 +0100
```

```
Received: from [192.168.178.26]
([74.3.96.134]) by smtp.gosec.de
(mrgosec102) with
 ESMTPSA (Nemesis) id 0LzsGF-1Zr9D42Rdb-
01543r for <bob.receiver@attorney.com>;
 Sun, 06 Mar 2016 14:53:09 +0100
Message-ID: <56DC363A.6050603@web.de>
Date: Sun, 06 Mar 2016 14:52:58 +0100
From: Robert Sender <rob-
ert.sender@gosec.de>
User-Agent: Mozilla/5.0 (Windows; U;
Windows NT 5.1; de; rv:1.9.2.13)
Gecko/20101207 Thunderbird/3.1.7
MIME-Version: 1.0
To: bob.receiver@attorney.com
Subject: status on contract review
Content-Type: text/plain; charset=UTF-8;
format=flowed
Content-Transfer-Encoding: 8bit
Envelope-To: <bob.receiver@attorney.com>

Bob,

do you see any concerns with the mer-
ger's contract?

Regards
Robert
-----------------------------------
```

Offensichtlich sind dem Header im Inhalt der E-Mail weitere Felder hinzugefügt worden. Unsere Aufmerksamkeit richtet sich dabei auf die zwei Received-Zeilen:

```
Received: from mout.gosec.de
([218.107.12.17]) by mx-ha.attorney.com
(attorney006) with
 ESMTPS (Nemesis) id 0Lms1s-1ZvnFh42Vo-
00h3Bt for <bob.receiver@attorney.com>;
 Sun, 06 Mar 2016 14:53:09 +0100

Received: from [192.168.178.26]
([74.3.96.134]) by smtp.gosec.de
(mrgosec102) with
 ESMTPSA (Nemesis) id 0LzsGF-1Zr9D42Rdb-
01543r for <bob.receiver@attorney.com>;
 Sun, 06 Mar 2016 14:53:09 +0100
```

Das Datenfeld „Received“ wird im Internet Message Format mit folgender Spezifikation aufgeführt:

```
Datenfeld =  Feldtitel      Inhalt
-------------------------------------------------------------------
Received =  "Received:"  *received-token ";" date-time
```

Dieses Feld ist im RFC 5321 (Simple Mail Transfer Protocol) spezifiziert. Wir haben es also mit einem Feld mit Bezug zur Übertragung der Mail zu tun.

Gemäß dem SMTP-Standard handelt es sich um „Trace Informationen“. Jeder SMTP-Server (d.h. ein nach diesem Standard implementierter Mail-Server) MUSS nach Empfang einer E-Mail diese Informationen in dessen Header schreiben. Diese Informationen muss er vorne anhängen und es ist laut Standard untersagt, vorherige „Trace Information“ oder deren Reihenfolge zu ändern oder zu löschen.

Wenn man davon ausgeht, dass alle SMTP-Server standard-konform implementiert sind, beschreibt dies den Weg, den die E-Mail über das Internet genommen hat, z.B. über wie viele und welche Systeme die E-Mail transportiert wurde.

Aus den Informationen ist ersichtlich, dass die E-Mail über zwei SMTP-Server transportiert wurde:

1. Der SMTP-Server mit dem Namen smtp.gosec.de (mrgosec102) hat zum Zeitpunkt *Sun, 06 Mar 2016 14:53:09 +0100* die E-Mail vom System mit der IP-Adresse 192.168.178.26 bzw. 74.3.96.134 erhalten. Die Nachricht mit der Nachrichtenidentifikation 0LzsGF-1Zr9D42Rdb-01543r wurde für bob.receiver@attorney.com avisiert.

2. Der SMTP-Server mit dem Namen mx-ha.attorney.com (attorney006) hat zum Zeitpunkt *Sun, 06 Mar 2016 14:53:09 +0100* die E-Mail von mout.gosec.de mit der IP-Adresse 218.107.12.17 erhalten. Die Nachricht mit der Nachrichtenidentifikation 0Lms1s-1ZvnFh42Vo-00h3Bt wurde für bob.receiver@attorney.com avisiert.

Das letzte System hat die E-Mail offensichtlich für das Postfach „bob.receiver@attorney.com” bereitgestellt. Es sind keine weiteren Trace-Informationen vorhanden, da die E-Mail nicht durch SMTP weitertransportiert wurde, sondern vom E-Mail-Programm mit dem POP3-Protokoll vom Postfach abgeholt wurde. In RFC 1939 (POP3) sind keine Trace-Informationen vorgegeben (genauso wenig wie in RFC 3501 für IMAP). Beide schreiben nichts in den Header. Abbildung 3 visualisiert die Übertragungsverbindungen einer E-Mail.

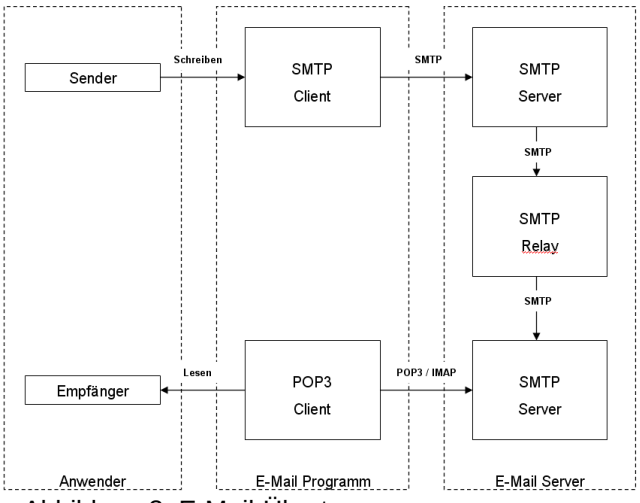

Abbildung 3: E-Mail-Übertragung

Ein Anwender nutzt ein E-Mail-Programm zum Versenden und Empfangen von E-Mails. Das Programm kann als dedizierte Anwendung (wie Thunderbird oder

Outlook) auf einem Gerät (PC, Smartphone o.ä.) oder als Webmail-Anwendung implementiert sein. Eine Webmail-Anwendung kann je nach Implementierung des Anbieters als Anwenderschnittstelle zu einem webbasierten E-Mail-Programm oder zu dem E-Mail-Postfach-Server ausgelegt sein. In E-Mail-Programmen wird mittels der Protokolle POP3 oder IMAP auf Nachrichten im Postfach-Server zugegriffen. Eine versendete E-Mail wird je nach Notwendigkeit über mehrere SMTP-Relays geleitet, bis sie bei dem SMTP-Server angekommen ist, der das Postfach des Empfängers verwaltet. Dazu wird das Protokoll SMTP eingesetzt.

Wie funktioniert die Übertragung via SMTP?

SMTP und das Internet Message Format sind eng miteinander verknüpft, der wesentliche Unterschied besteht darin, dass SMTP „lediglich" die mit dem Internet Message Format formatierte Nachricht von einem System zum anderen System überträgt. Um das tun zu können, wird im SMTP spezifiziert, wie zwei Systeme miteinander „sprechen", damit eine Nachricht zum Empfänger übermittelt wird. Technisch wird eine Sequenz von Befehlen ausgeführt, die dazu dient, Ursprung, Ziel und die Nachricht selbst festzulegen.
Die Übertragung sieht beispielsweise wie folgt aus, wobei S für den empfangenden SMTP-Server und C für den sendenden SMTP-Client steht:

```
S: 220 smtp.gosec.de Simple Mail Trans-
fer Service Ready
C: EHLO 192.168.178.26
S: 250- smtp.gosec.de greets
192.168.178.26
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
C: MAIL FROM:<robert.sender@gosec.de >
S: 250 OK
C: RCPT TO:<bob.receiver@attorney.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with
<CRLF>.<CRLF>
C: Message-ID:
<56DC363A.6050603@gosec.de>
C: Date: Sun, 06 Mar 2016 14:52:58 +0100
C: From: Robert Sender <rob-
ert.sender@gosec.de>
C: User-Agent: Mozilla/5.0 (Windows; U;
Windows NT 5.1; de; rv:1.9.2.13)
Gecko/20101207 Thunderbird/3.1.7
C: MIME-Version: 1.0
C: To: bob.receiver@attorney.com
C: Subject: status on contract review
C: Content-Type: text/plain; char-
set=UTF-8; format=flowed
C: Content-Transfer-Encoding: 8bit
C:
C: Bob,
C:
C: do you see any concerns with the mer-
ger's contract?
C:
C: Regards
C: Robert
C: .
S: 250 OK
C: QUIT
S: 221 smtp.gosec.de Service closing
transmission channel
```

Die SMTP-„Kommunikation" ist recht gut zu lesen und die Weitergabe von Informationen des Umschlag lässt sich gut erkennen („MAIL FROM:" bzw. „RCPT TO:"). Nachdem der SMTP-Server diese Daten jeweils akzeptiert hat („250 OK") übermittelt der SMTP-Client den Wunsch, die Nachricht zu übermitteln („DATA"). Der SMTP-Server signalisiert seine Bereitschaft und gibt die Zeichenfolge vor, die das Ende der Nachricht kennzeichnen soll („354 Start mail input; end with <CRLF>.<CRLF>"). Im Folgenden überträgt der Client Zeile für Zeile die E-Mail aus dem technischen Format und beendet sie mit der erwarteten Endzeichenfolge. Nachdem der Server bestätigt hat, dass aus dessen Sicht alles in Ordnung ist („250 OK"), schließt der Client die Übertragung ab („QUIT"). Die E-Mail im technischen Format wird nun vom SMTP-Mail-Server zugestellt oder weitergeleitet. Bevor er dies tut, ergänzt er den E-Mail-Header mit den entsprechenden Trace-Informationen.

Wozu Kryptographie und E-Mail Verschlüsselung?

Betrachtet man Abbildung 3 erneut und bedenkt, dass – wie vorausgehend aufgezeigt – sowohl die E-Mail als auch ihre Übertragung in Form lesbaren Textes erfolgt, so wird klar, dass die RFCs zu den Formaten und Protokollen weder Authentizität noch Integrität noch Vertraulichkeit gewährleisten. Vortäuschen, Abhören und Verändern von E-Mails ist an verschiedenen Stellen möglich. Besonders der Betreiber eines SMTP-Servers bzw. -Relays hat dazu einfache Möglichkeiten.
Kryptographie bietet Methoden und Verfahren, um mehr Sicherheit in Bezug auf Authentizität, Integrität und Vertraulichkeit zu erlangen. So wird Verschlüsselung, wie durch den Transport Layer Security (TLS), eingesetzt, um das SMTP-Protokoll für einen Teil der Wegstrecke in einer verschlüsselten Verbindung zu kapseln. Diese bietet allerdings nur Schutz vor Abhörung bei der technischen Übertragung der E-Mails. Bösartige Administratoren bei einem E-Mail-Dienst-Betreiber oder Angreifer, die E-Mail-Übertragungswege auf darunterliegenden technischen Ebenen auf ihren SMTP-Server umleiten (z.B. über DNS-Manipulationen), können diesen Schutz unbemerkt und in großem Maßstab umgehen. Der Inhalt einer E-Mail ist bei jedem transportierenden SMTP-Server einseh- und veränderbar. Mittels E-Mail-Verschlüsselung schon beim Absender kann dieses Risiko deutlich reduziert werden (vgl. Abbildung 4).
Eine E-Mail wird durch das sendende E-Mail-Programm schon vor der Übertragung an den ersten

SMTP-Server verschlüsselt. Anschließend wird die verschlüsselte E-Mail (ggf. zusätzlich mit Transportverschlüsselung) wie gehabt mittels SMTP übertragen, bis sie beim Empfänger ankommt. Dort muss sie vom E-Mail-Programm des Empfängers entschlüsselt werden, bevor er sie lesen kann. Eine Entschlüsselung setzt voraus, dass dieses den korrespondieren Schlüssel besitzt. Dieser muss in einer geeigneten, sicheren Form vorab ausgetauscht werden.

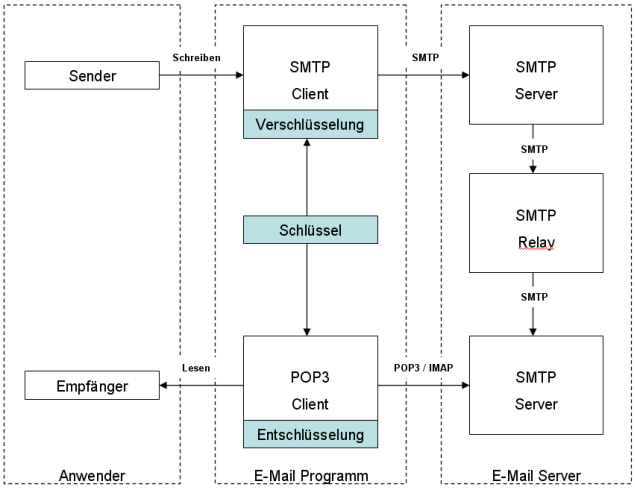

Abbildung 4: E-Mail-Übertragung mit Ende-zu-Ende-Verschlüsselung

Die Kryptographie bietet auch für diese Herausforderung geeignete Lösungen an. Es existieren Verfahren und Methoden, die es erlauben, Authentizität, Integrität und Vertraulichkeit für die Schlüssel und deren Austausch zu gewährleisten. Dazu gehört die „asymmetrische Kryptographie“. Mittels mathematischer Verfahren wird dabei für jeden Anwender (Sender und Empfänger) ein extra Schlüsselpaar generiert. Ein Schlüsselpaar besteht aus je zwei zusammengehörigen Schlüsseln: Ein „öffentlicher“ Schlüssel und ein „privater“ Schlüssel. Diese beiden Schlüssel sind genau aufeinander abgestimmt, jedoch kann man aus keinem den jeweils anderen rekonstruieren. Daten können nun wechselseitig mit einem Schlüssel ver- und mit dem anderen entschlüsselt werden. Diese wechselseitige Verwendung ermöglicht es, Integrität und Vertraulichkeit zu gewährleisten. Es setzt allerdings voraus, dass einer der beiden Schlüssel dem Sender bekannt ist (öffentlicher Schlüssel), während der andere ausschließlich dem Empfänger bekannt sein darf (privater Schlüssel). Der Sender verschlüsselt eine Nachricht an den Empfänger mit dem öffentlichen Schlüssel des Empfängers. Durch die mathematische Bedingung der beiden Schlüssel kann nur der Empfänger die Nachricht entschlüsseln. Die Nachricht ist somit vertraulich. Der Sender kann zudem seinen eigenen privaten Schlüssel verwenden, um seine Nachricht zu „signieren“. Dazu generiert er eine Art Fingerabdruck der Nachricht (Hashwert) und verschlüsselt diesen mit seinem privaten Schlüssel. Der private Schlüssel bleibt dabei weiterhin geheim. Der verschlüsselte Hashwert erlaubt dem Empfänger, die empfangene Nachricht auf eine mögliche Verfälschung hin zu prüfen (Integrität) und festzustellen, ob tatsächlich der korrespondierende öffentliche Schlüssel des erwarteten Senders verwendet wurde (Quellensicherheit bzw. Authentizität).
Hinzu kommt dann eine Infrastruktur für die Schlüssel. Eine Public-Key-Infrastruktur (PKI) ist hierarchisch organisiert und erstellt für die öffentlichen Schlüssel von Certificate Authority (CA) und User jeweils Zertifikate. Über diese digitalen „Zertifikate“ wird der öffentliche Schlüssel an einen Anwender (genauer an seine E-Mail-Adresse) „gebunden“. Alternative Schlüsselinfrastrukturen bietet das Web-of-Trust.
Der öffentliche Schlüssel darf tatsächlich öffentlich sein. Werden ergänzend sichere Schlüsselmedien für den privaten Schlüssel (wie z.B. eine Smartcard), kann die Sicherheit einer E-Mail bis hin zur Sicherstellung der technischen Authentizität einer Nachricht realisiert werden. Dies bedeutet, dass der Absender der E-Mail mit sehr hoher Wahrscheinlichkeit die im öffentlichen Zertifikat hinterlegte natürliche Person ist. Ohne diese Komponenten kann man sich diesbezüglich nicht sicher sein.

Wie sieht eine Ende-zu-Ende-verschlüsselte E-Mail technisch aus?

Erste Voraussetzung für eine Ende-zu-Ende-(E2E)-Verschlüsselung ist, dass die E-Mail-Programme der Anwender die benötigte kryptographische Funktionalität besitzen, sprich ver- und entschlüsseln bzw. signieren und prüfen können. Es gibt bereits viele E-Mail-Programme bzw. Programmerweiterungen, die dies ermöglichen, allerdings sind sie nicht zwangsläufig interoperabel. Es existieren zwei maßgebliche Formate zur E-Mail-Verschlüsselung: RFC 4880 für OpenPGP und RFC 5751 für S/MIME.

Das OpenPGP Message Format beschreibt Nachrichtenformate, die von OpenPGP-Anwendungen verwendet werden, um Ver- bzw. Entschlüsselung sowie Signaturen und Schlüsselmanagement bereitzustellen. OpenPGP ist damit erstmal unabhängig von der E-Mail (als Übertragungsmedium oder Format). S/MIME dagegen ist eine spezifische Erweiterung des Internet Message Protocols basierend auf dessen Multipurpose Internet Mail Extensions.

Eine OpenPGP-Nachricht entspricht einer zusammengefügten Kette definierter Inhalte:

- Einem Header, der den Datentyp der PGP-Nachricht angibt (für signierte, verschlüsselte oder komprimierte Nachrichten ist dies „BEGIN PGP MESSAGE“).
- Einem Armor Header, der Informationen zur Decodierung und zur Verwendung der Nachricht transportiert (z.B. Version oder eingesetzte Hashverfahren).
- Einer Leerzeile.
- Den codierten Daten.
- Einer Prüfsumme.
- Einer Fußzeile, die mit dem Header korrespondiert.

Eine verschlüsselte PGP-Nachricht sieht dann folgendermaßen aus:

```
-----BEGIN PGP MESSAGE-----
Version: OpenPrivacy 0.99

yD-
gBO22WxBHv7O8X7O/jygAEzol56iUKiXmV+XmpCt
mpqQUKiQrFqclFqUDBovzS
vBSFjNSiVHsuAA==
=njUN
-----END PGP MESSAGE-----
```

Die Übertragung dieser OpenPGP-Nachricht mittels des Internet Message Protocols würde originär als Inhalt versendet werden und sähe in der technischen Darstellung folgendermaßen aus:

```
---------------------------------------------------------------------
Message-ID: <56DC363A.6050603@gosec.de>
Date: Sun, 06 Mar 2016 14:52:58 +0100
From: Robert Sender <rob-
ert.sender@gosec.de>
User-Agent: Mozilla/5.0 (Windows; U;
Windows NT 5.1; de; rv:1.9.2.13)
Gecko/20101207 Thunderbird/3.1.7
MIME-Version: 1.0
To: bob.receiver@attorney.com
Subject: status on contract review
Content-Type: text/plain; charset=UTF-8;
format=flowed
Content-Transfer-Encoding: 8bit

-----BEGIN PGP MESSAGE-----
Version: 2.6.2

iQCVAwUB-
MJrRF2N9oWBghPDJAQE9UQQAtl7LuRVndBjrk4Eq
YBIb3h5QXIX/LC//
jJV5bNvkZIGPIcEmI5iFd9boEgvpirHtIREEqLQR
kYNoBActFBZmh9GC3C041WGq
uM-
brbxc+nIs1TIKlA08rVi9ig/2Yh7LFrK5Ein57U/
W72vgSxLhe/zhdfolT9Brn
HOxEa44b+EI=
=ndaj
-----END PGP MESSAGE------
---------------------------------------------------------------------
```

Es ist offensichtlich, dass der Header des Inhaltes nicht verschlüsselt ist (und auch nicht signiert wird). Dies ist bei aktuellen S/MIME-Nachrichten nicht anders.[4] Sie zeichnen sich allerdings dadurch aus, dass ein spezieller Content-Type „application/pkcs7-mime“ definiert ist. Eine S/MIME-verschlüsselte E-Mail sähe damit in der technischen Darstellung wie folgt aus.

```
---------------------------------------------------------------------
Message-ID: <56DC363A.6050603@gosec.de>
Date: Sun, 06 Mar 2016 14:52:58 +0100
From: Robert Sender <rob-
ert.sender@gosec.de>
User-Agent: Mozilla/5.0 (Windows; U;
Windows NT 5.1; de; rv:1.9.2.13)
Gecko/20101207 Thunderbird/3.1.7
MIME-Version: 1.0
To: bob.receiver@attorney.com
Subject: status on contract review
Content-Type: application/pkcs7-mime;
name="smime.p7m"; smime-type=enveloped-
data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; file-
name="smime.p7m"
Content-Description: S/MIME Encrypted
Message

Q09NT0RPIENBIExpbWl0ZWQxQTA/BgNVBAMTOENP
TU9ETyBTSEEtMjU2IENsaWVudCBBdXRoZW50aWNh
dGlvbiBhbmQgU2VjdXJlIEVtYWlsIENBAhEAm9mg
el/sMlhyrdfWN00s0DANBgkqSIb3DQEHA6CAMIAC
gIADCBsTCB-
MA1UEBhMCR0IxGzAZBgNVBAgTEkdyZWF0ZXIgTWF
uY2hlc3RlcjEQMA4GA1UEBxMHU2FsZDEaMBgGA1U
EChMvR/I6Z0w2BWgpSqghlQABuJ5MEey6SsGUrEk
NUMYr9eiWvW8ySovYYKa5Ftg
xgAAAAAAAAAAAA=
---------------------------------------------------------------------
```

Mit dem RFC 3156 wurde das OpenPGP-Format in MIME integriert, d.h. es wurde ebenfalls eine dedizierte Erweiterung spezifiziert und damit letztendlich die Programm-gesteuerte Auswertung erleichtert.
Laut RFC 3156 werden OpenPGP verschlüsselte Daten mit dem Content-Type "multipart/encrypted" beschrieben. Dieser muss einen Parameter "protocol" mit dem Wert "application/pgp-encrypted" haben. Der „multipart/encrypted” MIME-Inhalt muss aus zwei Teilen bestehen. Der erste mit Content-Type "application/pgp-encrypted" beinhaltet Kontrollinformationen. Um mit RFC 3156 konform zu sein, muss dieser Teil den Wert "Version: 1" enthalten. Nachdem das OpenPGP-Format (RFC 4880) alle weiteren Informationen beinhaltet, werden hier keine weiteren Angaben benötigt. Der zweite Teil muss die tatsächlichen verschlüsselten Daten beinhalten und mit dem Content-Type "application/octet-stream" beschrieben sein. Eine solche Nachricht sähe daher in der technischen Darstellung wie folgt aus:

```
---------------------------------------------------------------------
Message-ID: <56DC363A.6050603@gosec.de>
Date: Sun, 06 Mar 2016 14:52:58 +0100
From: Robert Sender <rob-
ert.sender@gosec.de>
User-Agent: Mozilla/5.0 (Windows; U;
Windows NT 5.1; de; rv:1.9.2.13)
Gecko/20101207 Thunderbird/3.1.7
MIME-Version: 1.0
To: bob.receiver@attorney.com
Subject: status on contract review
Content-Type: multipart/encrypted;
boundary=foo; protocol="application/pgp-
encrypted"

--foo
Content-Type: application/pgp-encrypted
```

[4] Genaugenommen gilt dies nur für die aktuellen Implementierungen, denn nach S/MIME v3.2 würde es gehen. Damit kann im Body eine vollständige Nachricht nach RFC 5322 enthalten sein, also inkl. aller Header. E-Mail-Clients sollten in solchen Fällen dann nur die „inneren“ Header anzeigen und die äußeren, im Klartext vorhandene, ignorieren. Leider wird das derzeit von keinem uns bekannten E-Mail-Programm unterstützt.

```
Version: 1

--foo
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: 2.6.2

hIwDY32hYGCE8MkBA/wOu7d45aUxF4Q0RKJprD3v
5Z9K1YcRJ2fve87lMlDlx4Oj
eW4GDdBfLbJE7VUpp13N19GL8e/AqbyyjHH4aS0Y
oTk10QQ9nnRvjY8nZL3MPXSZ
g9VGQxFeGqzykzmykU6A26MSMexR4ApeeON6xzZW
fo+0yOqAq6lb46wsvldZ96YA
AABH78hyX7YX4uT1tNCWEIIBoqqvCeIMpp7UQ2Iz
BrXg6GtukS8NxbukLeamqVW3
1yt21DYOjuLzcMNe/JNsD9vDVCvOOG3OCi8=
=zzaA
-----END PGP MESSAGE-----

--foo--
```

Warum nicht über verschiedene Verfahren hinweg vertrauensvoll kommunizieren?

Derzeit ist also bei allen drei Varianten verschlüsselter Kommunikation die Header-Informationen unverschlüsselt (das ist nicht zwingend so, aber leider heutige Realität). Zudem zeigt sich auch ohne, dass wir auf weitere Details bei einer Implementierung (wie Algorithmen, Codierungen etc.) eingegangen sind, dass S/MIME und OpenPGP nicht einfach interoperabel sind. Selbst wenn ein E-Mail-Programm beide Verfahren bzw. Formate unterstützt, werden diese in der Regel komplett separat gehandhabt (für eine Mail werden Schlüssel und Verfahren entweder aus PGP oder aus S/MIME genutzt). Eine automatische „Übersetzerfunktion“ von S/MIME zu OpenPGP und vice versa wäre machbar und könnte das Leben der Anwender einfacher machen und die Nutzung verschlüsselter Kommunikation zwischen unterschiedlichen Verfahren fördern.

Sicherheitstechnisch betrachtet ist es wünschenswert, dass E-Mails per se vertraulich sind. Allerdings fehlen den heutigen Implementierungen dazu aus Benutzersicht noch viele Teile, um kryptographische Verfahren interoperabel zwischen mehreren E-Mail Programmen einfach und synchronisiert zu verwenden.

Der Artikel „xxxx“ in diesem Heft auf Seite xxx beleuchtet diese Thematik genauer und gibt einen Ausblick, wie diese Probleme zukünftig gelöst werden könnten.

Fortschritte hierzu erfordern sowohl die Weiterentwicklung der Standards (RFCs) als auch deren Durchsetzung. Das könnten sowohl koordinierte Open-Source-Projekte leisten, aber wohl eher noch eine koordinierte Vorgehensweise der großen kommerziellen Anbieter Google, Facebook, Apple und Microsoft, von denen gerade in letzter Zeit einige Sicherheitsfeatures sehr pragmatisch durchgesetzt wurden (Facebook gegen Cross-Site-Scripting, Apple Mail, Google CA-Checking und Hash-Update).

Literaturangaben:

IETF; RFC 2045 Multipurpose Internet Mail Extensions;
https://tools.ietf.org/html/rfc2045

IETF; RFC 3501 Internet Message Access Protocol;
https://tools.ietf.org/html/rfc3501

IETF; RFC 3516 MIME Security with OpenPGP;
https://tools.ietf.org/html/rfc3156

IETF; RFC 4880 OpenPGP Message Format;
https://tools.ietf.org/html/rfc4880

IETF; RFC 5321 Simple Mail Transfer Protocol;
https://tools.ietf.org/html/rfc5321

IETF; RFC 5322 Internet Message Format;
https://tools.ietf.org/html/rfc5322

IETF; RFC 5751 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2;
https://tools.ietf.org/html/rfc5751