Seminar Spezielle Wirtschaftsinformatik

Lehrstuhl für Wirtschaftsinformatik und Informationssysteme

Generalthema: Systemsicherheit

Sicherer E-Mail Verkehr

Vergleich von PGP und S/MIME

Referent: Patric Majcherek

E-Mail: patric@majcherek.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

DES - Digital Encryption Standard; Symmetrischer Verschlüsselungsalgorithmus mit einer Schlüssellänge von 56 Bit.

DSA - Digital Signature Algorithm; Ein von der NSA entwickelter, sehr sicherer Algorithmus zum Signieren von Daten. DSA verwendet den Hash-Algorithmus SHA1.

FSF - Free Software Foundation, 1985 von Richard Stallman gegründete gemeinnützige Stiftung, die die Distribution von Emacs und dann auch für andere GNU-Software übernahm.

GNU - GNU's Not Unix, von Richard Stallman 1984 gestartetes Projekt, eine freie, vollständige Unix-artige Betriebsumgebung zu schaffen.

GPL - GNU General Public License, von der FSF herausgegebene Lizenz, ursprünglich für das GNU-Projekt geschaffen, heute die am häufigsten verwendete Lizenz für freie Software.

HTML - HyperText Markup Language; die Auszeichnungssprache für Webseiten

HTTP - HyperText Transfer Protocol; das Übertragungsprotokoll für Webseiten

IAB - Internet Architecture Board, offenes Gremium für die Weiterentwicklung der Internet- Protokolle, 1983 als Internet Activities Board gegründet, 1992 in der ISOC aufgegangen und in AB umbenannt.

IDEA - International Data Encryption Standard. Symmetrischer Verschlüsselungsalgorithmus mit 128 Bit Schlüssellänge.

IEC - International Electrotechnical Commission, Standardisierungsgremium mit Sitz in Genf

IETF - Internet Engineering Task Force; das offene Gremium im Rahmen der ISOC, in dem die technischen Fragen der Internetinfrastruktur verhandelt werden.

ISO - International Organization for Standardization, (von gr. isos, gleich), internationale Vereinigung der Standardisierungsgremien von über 140 Ländern; verabschiedet internationale Standards in allen technischen Bereichen (außer in Elektrik und Elektronik, für die die IEC zuständig ist), darunter technische (z.B. MP3 oder Telefonkarten), klassifikatorische (z.B. Ländercodes wie .de, .nl, .jp.) und Verfahrensstandards (z.B. Qualitätsmanagement nach ISO 9000).

ISOC - Internet Society, 1992 gegründete NGO für die Pflege und Weiterentwicklung der Internetinfrastruktur; beherbergt die für die Internetstandards zuständigen Gremien IETF und IAB.

LAN - Local Area Network - lokales Computer- Netz; Mitte der 80er-Jahre entstanden parallel zum Weitverkehrsnetz.

MIME - Multimedia Internet Mail Extensions; eine Erweiterung des E-Mail-Standards, die das Anhängen von Binärinformationen (Bilder, Klänge, Programme) erlaubt. Spezifiziert in RFC 1437.

MIT - Massachusetts Institute of Technology, führende US-amerikanische Universität und Hochburg der Technologieentwicklung

NSA - National Security Agency; Amerikanischer Geheimdienst, der sich vorrangig mit Kryptographie und dem weltweiten gezielten Abhören der elektronischen Kommunikation beschäftigt.

OpenPGP - Protokoll, das den Austausch von verschlüsselten Daten, Signaturen und Schlüsseln regelt. Spezifiziert in RFC 2440.

OSI - (1) Open Systems Interconnection; ein ab 1982 von der ISO entwickelter verbindungsorientierter Internetzwerkstandard, der an die Stelle von TCP/IP treten sollte, heute jedoch weitgehend in Vergessenheit geraten ist. (2) Open Source Initiative, im Februar 1998 von Eric Raymond, Bruce Perens u.a. mit dem Ziel gegründete Vereinigung, freie Software unter Vermeidung des Begriffs "frei" neu zu definieren und OSD-konforme Lizenzen zu zertifizieren.

PGP - Pretty Good Privacy; ein asymmetrisches (Public/Private Key) Verschlüsselungsverfahren für E-Mails und andere Dateien, 1991 von Philip Zimmerman freigegeben.

RFC - Request for Comments; die Dokumente, in denen die Internet-Gemeinde ihre technischen Standards dokumentiert; technisch ist "internet" gleichbedeutend mit "RFC-Konform". Alle RFC sind unter http://www.rfceditor.org/

RSA - Verschlüsselungssystem nach dem Public-Private-Key-Verfahren, entwickelt von Ron Rivest, Adi Shamir und Len Adelman, die ihr System mit den Anfangsbuchstaben ihrer Namen als RSA bezeichneten. s. http://www.rsa.com/

S/MIME - Secure Multimedia Internet Mail Extensions; eine Erweiterung des MIME Standards für sicheren E-Mail Transport

TCP/IP - Transmission Control Protocol / Internet Protocol, technische Grundlage des Internet.

UNIX - ursprünglich UNICS, Uniplexed Information and Computing Service; ab 1969 von Ken Thompson auf den Ruinen von MULTICS errichtetes modulares und portierbares Betriebssystem; heute als Oberbegriff für alle Unix-artigen Betriebssysteme wie GNU/Linux oder BSD verwendet.

URL - Uniform Resource Locator, universelles Adressierungsformat für Dienste im Internet (z.B. http://www.majcherek.de).

WWW - World-Wide Web; von Tim Berners- Lee ab 1989 entwickeltes Hypertext-Protokoll, besteht aus HTTP und HTML.

Einleitung

1.1 Allgemeines

„Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich."[1]

„Der Einsatz kryptographischer Verfahren ist von außerordentlicher Bedeutung für eine effiziente technische Kriminalprävention. Dies gilt sowohl für die Gewährleistung der Authentizität und Integrität des Datenverkehrs wie auch für den Schutz der Vertraulichkeit."[2]

Im Zeitalter des Computers und der weltweiten Vernetzung spielen elektronische Daten eine wichtige Rolle. Heutzutage ist es einfach und effektiv möglich in die Privatsphäre von Dritten einzudringen, also Zugang zu deren vertraulichen Informationen zu erlangen. Nicht nur Privatleute, auch Firmen, Politiker und Behörden kommunizieren zunehmend per E-Mail. Das Mailaufkommen hat sich exponentiell auf 10 Milliarden E-Mails am Tag[3] erhöht. Persönliche Informationen, Firmengeheimnisse, Kundendaten, Forschungsergebnisse, Patienteninformationen, Umsatzzahlen, Daten zur Abwicklung von Geschäftsvorgängen und viele andere sensible Informationen werden vermehrt über das Internet versendet. Den Weg, den diese Daten zu einer Zieladresse nehmen, kann man im Regelfall weder vorhersagen noch vorherbestimmen. Alle Daten, die unverschlüsselt verschickt werden, sind quasi öffentlich. Vergleichbar wäre der Versand unverschlüsselter E-Mail Kommunikation mit dem Versenden von Postkarten. Das Problem ist jedoch vielen nicht in diesem Ausmaß bekannt, was unter anderem an falschen Analogien liegt. So wird die E-Mail als „elektronischer Brief" bezeichnet, obwohl es besser „elektronische Postkarte" heißen müsste. In vielen Programmen und auf vielen Webseiten hat sich der Briefumschlag als Symbol für das Verschicken von E-Mails durchgesetzt. Genau dieser Umschlag, der Sicherheit suggeriert, fehlt bei unverschlüsselter Internet-Kommunikation. Daher verwundert es nicht, dass E-Mails

---

[1] ([Grun02] Artikel 10, Absatz 1)

[2] [Bund99]

[3] Vgl. ([Frey02] S. 250)

auf ihrem Weg durch das Internet mitgelesen, gelöscht, verändert oder gespeichert werden können.

1.2 Warum Kryptographie?

Kryptographie[4] gewährleistet

- Vertraulichkeit,
- Integrität und
- Authentizität

der Daten und der Kommunikation.

Der Inhalt, der in einer unverschlüsselten E-Mail verschickt wird, sollte nicht vertraulicher sein als der, den man auch per Postkarte abgeschickt hätte. Die Administratoren des eigenen Mailservers, sowie die des Empfängers, können ohne weiteres den Mailverkehr abfangen, abhören, löschen oder verändern. Auf dem Weg zum Ziel durchlaufen E-Mails teilweise eine Menge an Stationen. Jeder, der Zugriff auf eine dieser Zwischenstationen hat, sowie jeder Cracker[5], kann mühelos oben genannte Angriffe durchführen. Weiterhin ist nicht auszuschließen, dass der Datenverkehr automatisiert gefiltert und gespeichert wird. Staatliche oder private Organisationen dringen so in die Privatsphäre ein.[6] Bewiesen gilt im allgemeinen der in die Milliarden gehende Verlust durch Wirtschaftsspionage. Der Bericht „Wirtschaftsspionage und deren Auswirkungen auf den internationalen Handel“ (COMINT impact on international trade)[7] von Duncan Campbell setzt sich mit vielen detaillierten Quellenangaben auseinander. Campbell kommt zu der Schlussfolgerung, dass es

---

[4] Wissenschaft von der Verschlüsselung

[5] Eine Person, die vorsätzlich, unbefugterweise und oft mit bösartiger Absicht in fremde Rechnersysteme eindringt. Ein Cracker steht im deutlichen Gegensatz zu „Hacker“, womit ein gutmeinender Computer-Freak gemeint ist (RFC 1983)

[6] Vgl. [Heise02a]

[7] [Camp01]

höchstwahrscheinlich der Fall ist, dass Europa seit 1992 bis heute signifikante Verluste an Arbeitsplätzen und finanzieller Natur erlitten hat, die auf das Ergebnis der US-Politik der „Einebnung des Spielfeldes“ zurückzuführen sind.

Verschlüsselt übertragene Daten kann ein Angreifer, selbst wenn er physikalischen Zugriff darauf hat, nicht sinnvoll lesen. Die Nicht-Authentifizierung von E-Mails ist ein weiteres Sicherheitsproblem. Ein Angreifer könnte nicht nur den Mail-Inhalt verändern, er könnte auch die Absenderadresse fälschen, was gerade bei offizieller oder geschäftlicher Korrespondenz, dem Austausch von Dokumenten und dem Abwickeln von Geschäftsvorgängen über das Internet, fatal wäre. Der Absender muss eindeutig zu identifizieren sein und die Integrität der Daten muss überprüft werden können. Die einzige Möglichkeit um Vertraulichkeit, Integrität und Authentizität von elektronischen Dokumenten zu gewährleisten ist die Benutzung wirkungsvoller kryptographischer Verfahren. Hierbei wird die E-Mail in eine Art elektronischen Briefumschlag gesteckt, der wiederum nur vom Empfänger geöffnet werden kann. Durch eine digitale Unterschrift wird darüber hinaus eine eindeutige Zuordnung zum Urheber möglich. Manipulationen können auf diese Weise festgestellt werden.

2 Konzepte

Es gibt mehrere kryptographische Verfahren: symmetrische Verschlüsselung, asymmetrische Verschlüsselung, hybride Verfahren und Einweg-Hashing. PGP und S/MIME unterstützen alle genannten Verfahren. Im Folgenden wird nun etwas näher auf die einzelnen Techniken eingegangen.

2.1 Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird zum Ver- und Entschlüsseln immer derselbe Schlüssel[8] benutzt. Die Korrespondenzpartner müssen sich vor der Übertragung der verschlüsselten Nachricht auf einen Schlüssel einigen. Dieser sollte zuvor über einen abhörsicheren Kanal[9] übertragen worden sein. Der nun über einen unsichereren Kanal[10] verschickte Geheimtext kann zwar abgefangen werden, die Integrität und Vertraulichkeit bleiben jedoch erhalten. Für je zwei Parteien wird ein eigener Schlüssel benötigt. Die Anzahl der insgesamt benutzten Schlüssel beträgt bei n Personen, die miteinander kommunizieren wollen, insgesamt

$$(1) \qquad S = \frac{n*(n-1)}{2}$$

Schlüssel.

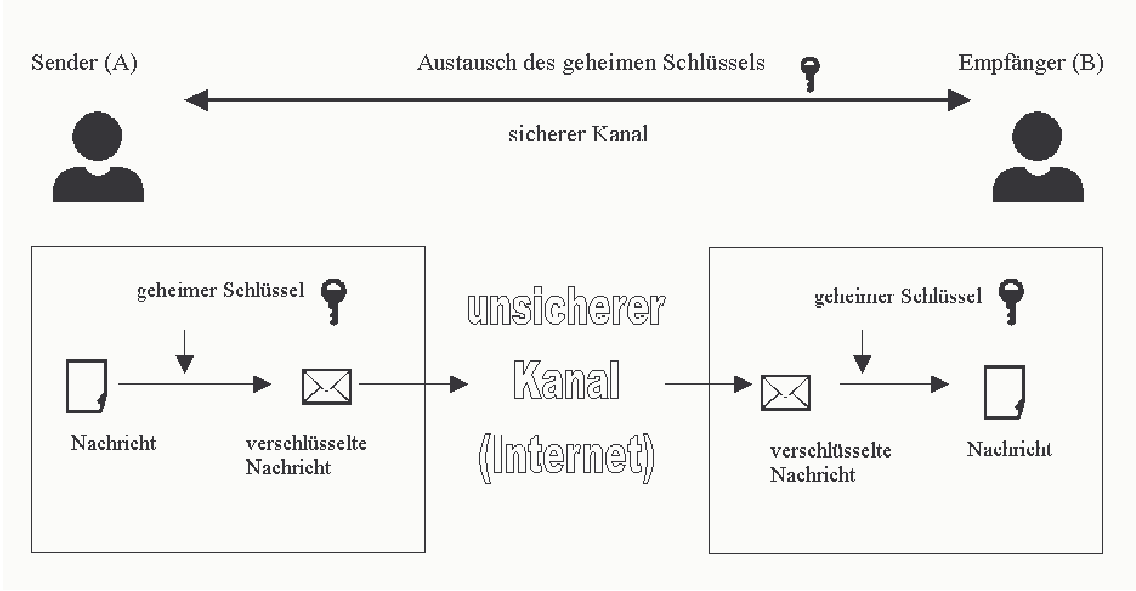

Abbildung (1): Symmetrische Verschlüsselung

[8] Datensequenz, die benutzt wird, um mit einer Verschlüsselungssoftware aus dem Klartext Geheimtext zu erzeugen (Verschlüsselung) und um aus dem Geheimtext den Klartext wieder herzustellen (Entschlüsselung). Auch zum Signieren und Überprüfen einer digitalen Signatur wird ein Schlüssel benötigt.

[9] Z.B. persönlich oder über eine vorhandene verschlüsselte Verbindung

[10] Hier das Internet

2.2 Asymmetrische Verschlüsselung

Um die Hauptprobleme der symmetrischen Verschlüsselung, viele Schlüssel sowie Austausch dieser nur über sichere Kanäle, zu umgehen, kann die asymmetrische Verschlüsselung, auch public key Verfahren genannt, angewendet werden. Der Sinn von Verschlüsselungsverfahren mit öffentlichem Schlüssel besteht darin das Sicherheitsrisiko beim gegenseitigen Schlüsselaustausch zu vermeiden. Jeder Empfänger von Nachrichten hat ein Schlüsselpaar mit einem öffentlichen und einem geheimen Schlüssel. Zum Verschlüsseln einer Nachricht wird der öffentliche Schlüssel des Empfängers benutzt. Nur der Inhaber des geheimen Schlüssels, also der rechtmäßige Empfänger, kann die Nachricht wieder entschlüsseln. Sender und Empfänger brauchen sich also nicht auf einen Schlüssel zu einigen. Der Absender muss nur eine Kopie des öffentlichen Schlüssels des Empfängers besitzen. Dieser öffentliche Schlüssel kann von jedem benutzt werden, der mit dem Empfänger kommunizieren will. Insgesamt sind somit nur

$$S = n \tag{2}$$

Schlüsselpaare bei n miteinander kommunizierenden Personen nötig.

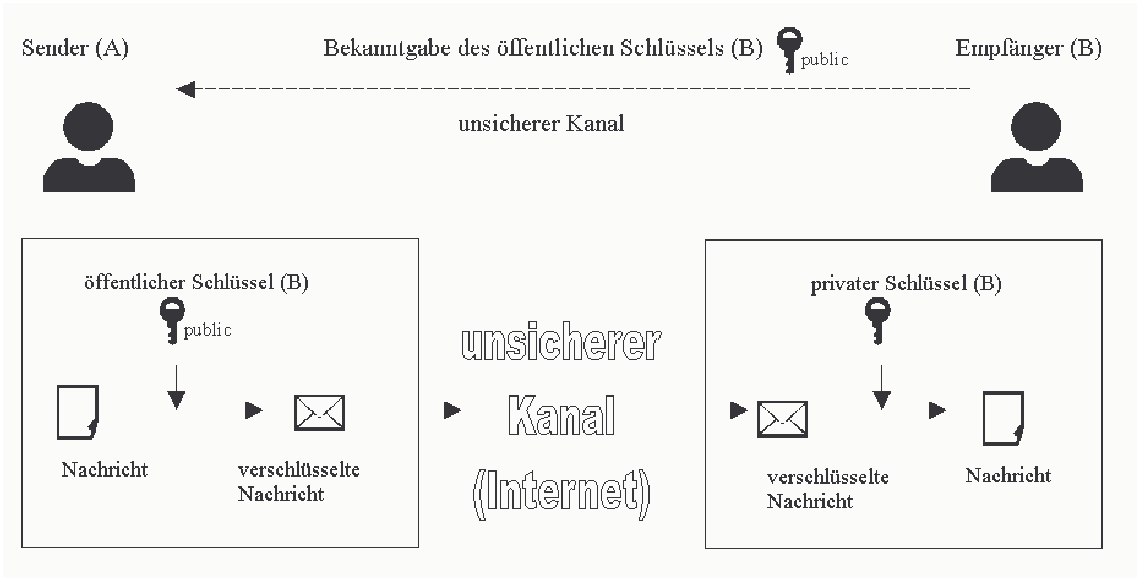

Abbildung (2): Asymmetrische Verschlüsselung

2.3 Hybride Verschlüsselungsverfahren

Vom Sicherheitsstandpunkt aus kann pauschal weder die symmetrische noch die asymmetrische Verschlüsselung bevorzugt werden. Ver- und Entschlüsselung sind bei einem asymmetrischen Verfahren aufwändiger als bei entsprechenden symmetrischen Systemen. Die Verwendung von public key Verfahren wird jedoch als geeignetes Mittel für den sicheren Austausch von symmetrischen Schlüsseln verwendet. Die Idee, die dahinter steckt, verbirgt sich in hybriden Verschlüsselungssystemen.

Eine hybride Verschlüsselung benutzt sowohl eine symmetrische Verschlüsselung als auch ein asymmetrisches Verfahren. Ein symmetrischer Sitzungsschlüssel, welcher von einem Zufallsgenerator erzeugt wird, verschlüsselt die eigentliche Nachricht. Dieser Sitzungsschlüssel wird dann mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Das schnelle symmetrische Verfahren wird somit auf die Nachricht, das langsamere asymmetrische Verfahren nur auf den Sitzungsschlüssel angewendet.

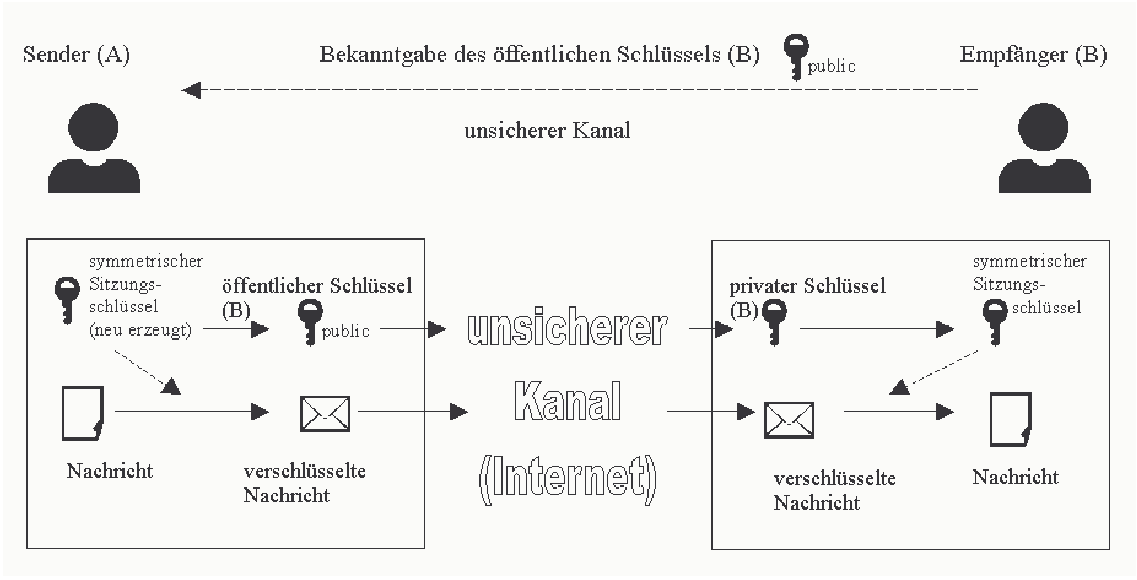

Abbildung (3): Hybride Verschlüsselung

2.4 Digitale Unterschriften

Eine digitale Unterschrift[11] eines Dokumentes kann zur Authentifikation des Senders mittels des asymmetrischen Verfahrens auf zwei Arten herangezogen werden. Bei der digitalen Signatur ohne Appendix wird eine Nachricht mit dem geheimen Schlüssel verschlüsselt. Durch Entschlüsseln dieser Nachricht mit dem öffentlichen Schlüssel kann nun überprüft werden, ob der zugehörige geheime Schlüssel verwendet wurde. Bei der Authentifikation mit Appendix wird eine Hash-Funktion[12] (*h*) auf das Dokument (m) angewendet.

$$(3) \qquad m' = h(m).$$

m´ wird nun mit dem geheimen Schlüssel verschlüsselt und kann vom Empfänger mit *h*(*m*) verglichen werden. Der Nachweis der Zusammengehörigkeit des öffentlichen Schlüssels mit einer gewünschten Identität bleibt jedoch aus.

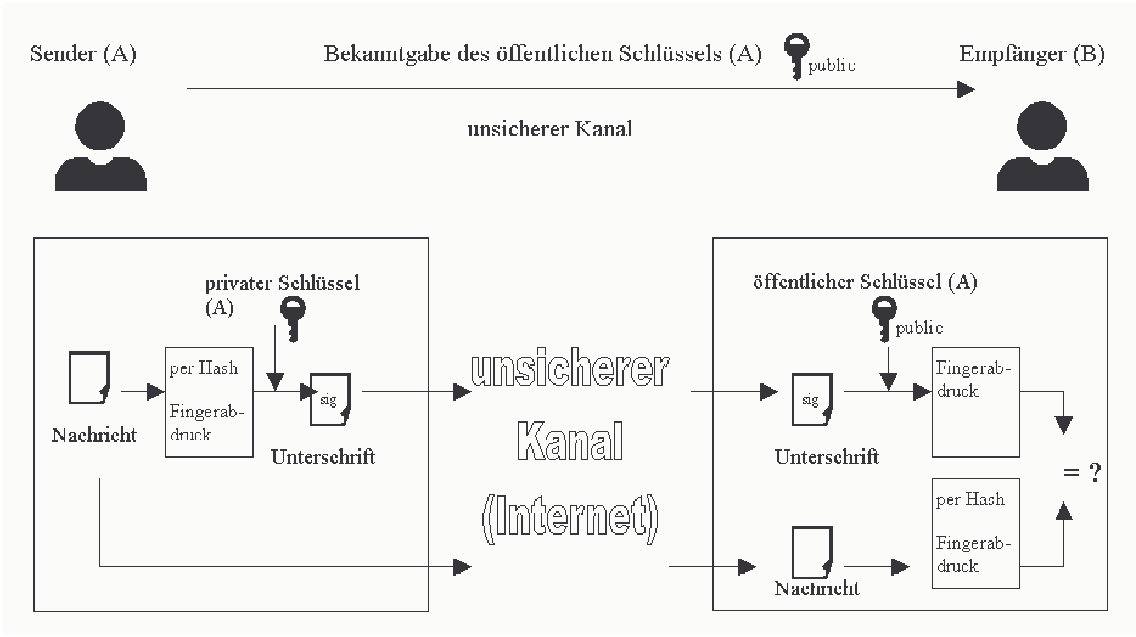

Abbildung (4): Digitale Signatur

[11] Auch digitale Signatur genannt

[12] Auch kryptographische Prüfsumme oder Message Digest genannt. Eine Hashfunktion ist eine Funktion, die aus einer Datei eine eindeutige Prüfsumme errechnet

3 Vorstellung der de-facto Standards

3.1 PGP, OpenPGP und GnuPG

Philip Zimmermann[13] ist der Erfinder von Pretty Good Privacy (PGP), eine von ihm in den USA entwickelte, weit verbreitete Verschlüsselungssoftware.[14] Im Juni 1991 stellte Zimmermann sein PGP erstmals der Öffentlichkeit zur Verfügung. Der damalige Student am US-amerikanischen Massachusetts Institute of Technology (MIT) wollte mit PGP eine sichere, einfach zu bedienende und praktikable Software schaffen, welche er dann als Freeware[15] freigab und den Quelltext offen legte. PGP fand sehr schnell Anklang in der Internet-Gemeinde. Die am Anfang kommandozeilenorientierten Versionen wurden im Laufe der Jahre durch graphische Versionen und Plug-Ins für Mail-Clients ersetzt. Philip Zimmermann gründete das Unternehmen PGP Inc., welches er 1997 an Network Associates (NAI)[16] verkaufte. Der Erfolg von PGP sorgte dafür, dass das zugrundeliegende Protokoll in den Internet-Standards, den sogenannten Request for Comments, mit Nummer RFC 1991[17] aufgenommen wurde. Dieses RFC erschien im August 1996 und definiert das PGP Message Format. In der Internet Engineering Task Force[18] bildete sich im Oktober 1997 eine Arbeitsgruppe, die eine Spezifikation für einen offenen Verschlüsselungsstandard, den OpenPGP-Standard, niederschrieb. Im November 1998 wurde das Dokument RFC 2440 mit dem OpenPGP als IETF-Standard verabschiedet. OpenPGP ist abwärtskompatibel zu alten PGP Versionen und bietet eine breitere Palette an Verschlüsselungsalgorithmen und -funktionen. Das Dokument der Arbeitsgruppe wird von vielen als Referenz für andere

---

[13] http://www.philzimmermann.com

[14] Teilweise werden im Folgenden mit PGP bzw. OpenPGP die eigentlichen Algorithmen bezeichnet

[15] Der Begriff „Freeware“ hat keine klar anerkannte Definition. Gemeinhin wird ein Softwarepaket als „Freeware“ bezeichnet, wenn die Weiterverbreitung, nicht jedoch Veränderung erlaubt ist. Der Quellcode ist nicht verfügbar. Diese Pakete sind keine freie Software im Gegensatz zu „freie Software“. Das „Free“ deutet hier nur „frei“ im Sinne von „Freibier“, nicht „Freiheit“ an (vgl. Definition der Free Software Foundation, Inc.).

[16] http://www.nai.com/

[17] Vgl. [Ietf96]

[18] Vgl. [Ietf02]

Implementierungen von OpenPGP verwendet[19]. Im Februar 2001 wechselte Philip Zimmermann von NAI nach Hush Communications[20]. Ein wichtiger Grund für diesen Wechsel war die Schwierigkeit bei der Offenlegung des PGP-Quellcodes. Das Management von NAI hat Ende 2000 die Veröffentlichung des Quelltextes ab Version 7 unterbunden. Ein wichtiges Element für Sicherheitssoftware, der Quellcode, war nun nicht mehr einsehbar. Zimmermann gab allen PGP Nutzern sein Ehrenwort und versicherte, dass es keine Hintertüren in der Software gebe. Wie aber schon der Sicherheitsexperte Bruce Schneier[21] in seinem monatlich erscheinenden Crypto-Gram richtig beschreibt, sieht auch er einen offen gelegten Quelltext als notwendig an.

> „As a cryptography and computer security expert, I have never understood the current fuss about the open source software movement. In the cryptography world, we consider open source necessary for good security; we have for decades. Public security is always more secure than proprietary security. It's true for cryptographic algorithms, security protocols, and security source code. For us, open source isn't just a business model; it's smart engineering practice."[22]

Das „Open" in OpenPGP steht laut IETF zwar für „offener Standard", die daraus resultierende Software muss jedoch nicht zwingend Open Source[23] bzw. freie Software[24] sein. Das von PGP verwendete RSA-Verfahren hat zudem den Nachteil, patentiert zu sein. 1998 lief das Patent auf das Diffie-Hellmann-Verfahren aus, sodass es von da an in PGP benutzt werden konnte. Letztendlich trugen auch Inkompatibilitäten zwischen PGP 6.0 und älteren Versionen zum Entstehen des GNU Privacy Guard (GnuPG)[25] bei. Eine Gruppe um Werner Koch hat dazu den OpenPGP Standard neu implementiert. GnuPG ist ein reines Kommandozeilentool und das eigentliche

---

[19] Auf http://www.cryptoex.com/ bietet z.B. die Glück & Kanja Software AG eine Public Key Infrastruktur (PKI) auf OpenPGP Basis an

[20] http://www.hush.com

[21] http://www.counterpane.com/schneier.html

[22] [Schn99]

[23] Der Ausdruck „Open Source" wird von manchen Leuten gebraucht, um mehr oder weniger das selbe auszudrücken wie „freie Software"

[24] Vgl. [Gnuo02]

[25] http://www.gnupg.org

Verschlüsselungsprogramm. Es kann sowohl mit alten als auch mit neuen PGP-Versionen kommunizieren. GnuPG steht unter der GPL Lizenz, so wird sicher gestellt, dass der Quelltext überprüfbar bleibt und eine dezentrale Evaluierung durch zahlreiche Stellen und Nutzer realisierbar ist. Die Weiterentwicklung[26] wird vom deutschen Bundesministerium für Wirtschaft und Technologie (BMWi)[27] gefördert. Als erstes freies Softwareprojekt überhaupt erhielt GnuPG somit Bundesmittel zur Verfügung gestellt. Ziel des BMWi ist es, dass die Verbreitung vorangetrieben, eine komfortable Benutzerschnittstelle sowie die Portabilität auf anderen Plattformen geschaffen werden. GnuPG entspricht der im RFC2440 festgelegten OpenPGP-Spezifikation. Als Frontends seien hier für GNU/Linux Kmail[28] und Mutt[29], für Windows GnuPP[30] mit Plug-Ins[31] für MS-Outlook, PostMe, Pegasus und Mozilla/Netscape genannt. Aus allen anderen E-Mail-Programmen kann mit Hilfe des Taskleistentools Windows Privacy Tray (WinPT), was zum GnuPP gehört, verschlüsselt werden. Im Folgenden wird PGP oft als Synonym für OpenPGP und GnuPG benutzt.

Folgende drei RFCs sind für PGP und OpenPGP von Bedeutung:

- 1991 PGP Message Exchange Formats (Status: INFORMATIONAL)
- 2440 OpenPGP Message Format (Status: PROPOSED STANDARD)
- 3156 MIME Security with OpenPGP (Status: PROPOSED STANDARD)

[26] http://www.gnupg.de/presse.html

[27] Vgl. [Bmwi02]

[28] http://kmail.kde.org/

[29] http://www.mutt.org/

[30] http://www.gnupp.de

[31] http://www.gnupp.de/download.html

3.2 S/MIME

Die Secure/Multipurpose Internet Mail Extensions (S/MIME) wurden durch ein Konsortium von Herstellern rund um RSA Security[32] entwickelt. S/MIME ist kein separates Programm, sondern eine Erweiterung der Multimedia Internet Mail Extension die wiederum eine Erweiterung des E-Mail-Standards ist. MIME erlaubt das Anhängen von Binärinformationen (Bilder, Klänge, Programme) an E-Mails. Programme müssen die Funktionalität von S/MIME daher direkt unterstützen. Trotz gleicher Algorithmen (wie RSA, Triple-DES und MD5) ist es nicht kompatibel zu PGP oder GnuPG. Nennenswerte Verbreitung fand S/MIME erst in Version 2, die im Wesentlichen auf RFC 2311 und RFC 2312 sowie PKCS (Public Key Cryptography Standards) RFC 2314 (PKCS#10) und RFC 2315 (PKCS#7) basiert. Die RFCs sind hier jedoch „Category: Informational“ und daher rein informativ. Die IETF hat S/MIME Version 2 nicht zum Standard erhoben. S/MIME Version 3 wurde im Juli 1999 von der IETF verabschiedet. Diese Version setzt auf RFC 2630, RFC 2631, RFC 2632 und RFC 2633 auf. Ein für E-Mails weit verbreiteter Standard zum Nachrichten-Austauschformat ist MIME, basierend auf RFC 822. S/MIME nutzt diese MIME Struktur der Mails und baut darauf mit kryptographischen Elementen auf. So kann der Text oder der Dateianhang verschlüsselt werden.

Für S/MIME sind folgende drei RFCs von Bedeutung:

- 2632 S/MIME Version 3 Certificate Handling (Status: PROPOSED STANDARD)
- 2633 S/MIME Version 3 Message Specification (Status: PROPOSED STANDARD)
- 2634 Enhanced Security Services for S/MIME (Status: PROPOSED STANDARD)

[32] Vgl. [Smim02]

4 Unterschiede zwischen PGP (GnuPG) und S/MIME

4.1 Sicherheit

Beide Protokolle erfüllen heutige Sicherheitsanforderungen anhand von identischen Algorithmen gleichermaßen. S/MIME und PGP können als „Schale“ angesehen werden, die kryptographischen Elemente übernehmen dann RSA, DES, DSA, IDEA oder Elgamal. Die bisher gefundenen Schwachstellen waren jeweils auf Implementierungsfehler der Hersteller zurückzuführen.

Der große Vorteil von freier Software, der offene Quelltext, ist jedoch nur bei GnuPG gegeben. Viele Entwickler und Hobbyprogrammierer durchsuchen den Quelltext tagtäglich nach Sicherheitslücken. Jeder, der Ahnung von Programmierung hat, kann sich den Code selber anschauen und verändern. Auf diese Weise lassen sich Sicherheitslücken schneller finden und werden meist innerhalb von wenigen Stunden behoben. Hintertüren in Programmen sind so praktisch auszuschließen.

4.2 Konzept des Vertrauens

Ein elementarer Unterschied zwischen PGP und S/MIME ist das Konzept des Vertrauens unter den Benutzern.

4.2.1 PGP und das Web-of-Trust

Bei PGP wird das sogenannte Web-of-Trust, ein „Netzwerk gegenseitigen Vertrauens“ angewendet. Dieses dient dazu, die Gültigkeit eines Schlüssels einer Person auch dann anzuerkennen, wenn der ihr zugehörige Schlüssel nicht selber überprüft wurde (s.u.). Bei dem Web-of-Trust unterschreiben die Benutzer ihre Schlüssel, nach Überprüfung

der Echtheit, gegenseitig. Jeder Nutzer von PGP hat die volle Kontrolle darüber, wem er wie weit vertraut. Hierzu kann man verschiede Stufen des Vertrauens einstellen.

Unbekannt

Es ist nichts über die Fähigkeit des Eigentümers bekannt. Alle Schlüssel, die einem nicht gehören, fallen zunächst unter diese Vertrauensstufe.

Kein Vertrauen

Der Eigentümer ist dafür bekannt andere Schlüssel nicht korrekt zu unterschreiben.

Teilweises Vertrauen

Der Eigentümer versteht die Implikationen des Unterschreibens von Schlüsseln und authentisiert Schlüssel richtig, bevor er sie unterschreibt.

Volles Vertrauen

Der Eigentümer hat ein ausgezeichnetes Verständnis hinsichtlich des Unterschreibens von Schlüsseln, seine Unterschrift auf einem Schlüssel zählt so viel wie die eigene.

Zu erkennen ist, dass nicht das Vertrauen in die andere Person, sondern das Vertrauen in deren Fähigkeit, Schlüssel sorgfältig zu authentifizieren und richtig zu signieren, entscheidend ist.

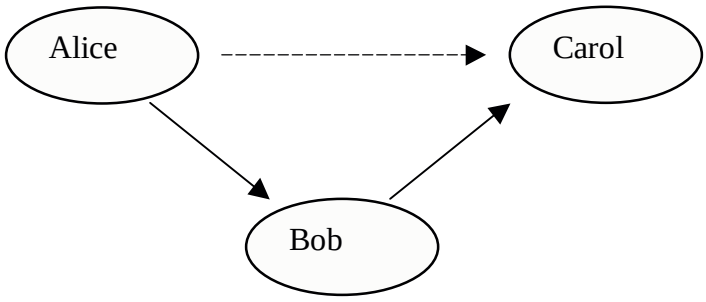

Abbildung (5): Web-of-Trust

In Abbildung 5 vertraut Alice Bob. Bob wiederum vertraut Carol und daher vertraut auch Alice implizit Carol. Dieses Vertrauensverhältnis kann noch feiner aufgestellt werden. Vertraut man einer Person nur teilweise, so müssen mindestens zwei

unabhängige Unterschriften die Echtheit bestätigen. Auch eine Pfadbeschränkung lässt sich optional verwirklichen. Der Pfad der unterschriebenen Schlüssel zwischen dem eigenen und dem zu authentisierenden darf eine bestimmt Länge nicht überschreiten.

Sollten Nachrichten mit einem engen und beständigen Personenkreis ausgetauscht werden, so bietet sich der direkte Schlüsselaustausch an. Hierzu wird der öffentliche Schlüssel, im Idealfall nach der Eigenbeglaubigung[33], weitergereicht und kann vom Empfänger mit Hilfe eines Fingerabdrucks überprüft werden. Der Fingerabdruck ist eine eindeutige Prüfsumme (Hash) des öffentlichen Schlüssels. Die Prüfsumme ist wesentlich kürzer als der Schlüssel selbst und wird zum Überprüfen bzw. Verifizieren eines öffentlichen Schlüssels heran gezogen. Der öffentliche Schlüssel kann auf mehrere Arten veröffentlicht werden.

Folgende Methoden haben sich bewährt:

- persönliche Übergabe des Schlüssels an den Korrespondenzpartner
- Übermittlung per E-Mail
- Publizieren des Schlüssels im WWW
- Weitergabe per Key-Server, die öffentliche Schlüssel sammeln und publizieren.

Der Fingerabdruck kann dem Empfänger des öffentlichen Schlüssels auch auf mehrere Arten übermittelt werden. Ein Key-fingerprint lautet z.B.: DED0 9C2E B936 1CC5 3FA0 15F3 4021 7753 F030 290C[34] und kann daher

- persönlich auf einem Zettel oder einer Visitenkarte,
- am Telefon, nach Erkennung der Stimme oder
- über einen vorhandenen sicheren Kanal

übermittelt werden.

---

[33] Auch Selbstunterzeichnung genannt. Indem der Benutzer seinen öffentlichen Schlüssel sowie die Benutzer-ID selbst mit seinem geheimen Schlüssel unterzeichnet, lassen sich Verfälschungen daran sehr leicht feststellen. Er bestätigt die Authentizität des Schlüssels.

[34] GnuPG Fingerprint von mir (Patric Majcherek)

Es ist jedoch auch eine Möglichkeit denkbar, mit der die Schlüsselprüfung ausgehebelt werden kann. A schiebt B einen falschen öffentlichen Schlüssel unter. Dieser untergeschobene Schlüssel, der vorgibt von C zu stammen, ist in Wirklichkeit aber von A ausgetauscht worden. Wenn ein solcher gefälschter Schlüssel signiert wird, hat das „Netz des Vertrauens“ ein Loch. Es ist also stets für alle Nutzer des Web-of-Trust wichtig, sich zu vergewissern, ob ein öffentlicher Schlüssel wirklich zu der Person gehört, der er zu gehören vorgibt. Eine praktikable Lösung bietet nur eine „übergeordnete” Instanz, der alle Benutzer vertrauen können. Zertifizierungsstellen für PGP sind z.B. das TC TrustCenter[35] sowie viele Universitäten. Das Web-of-Trust ist für PGP also nicht die einzige Möglichkeit um ein „Konzept des Vertrauens“ zu bilden.

PGP verschlüsselt und signiert nicht nur E-Mails, sondern auch digitale Daten und arbeitet unabhängig von den jeweiligen Formaten (E-Mail, Textdateien, Bilddaten, Sourcecode, Datenbanken, komplette Festplatten usw.). PGP verwendet dazu hauptsächlich ein hybrides Verfahren mit öffentlichem Schlüssel. Zum Verschlüsseln kann PGP aber ebenso ausschließlich symmetrische Verfahren einsetzen.

4.2.2 S/MIME und Certificate Chains

Die strenge Hierarchie von X.509 Zertifikaten ist das Grundgerüst des S/MIME Konzepts. X.509 Zertifikate werden bei SSL, S/MIME und IPSec eingesetzt.

[35] http://www.trustcenter.de/

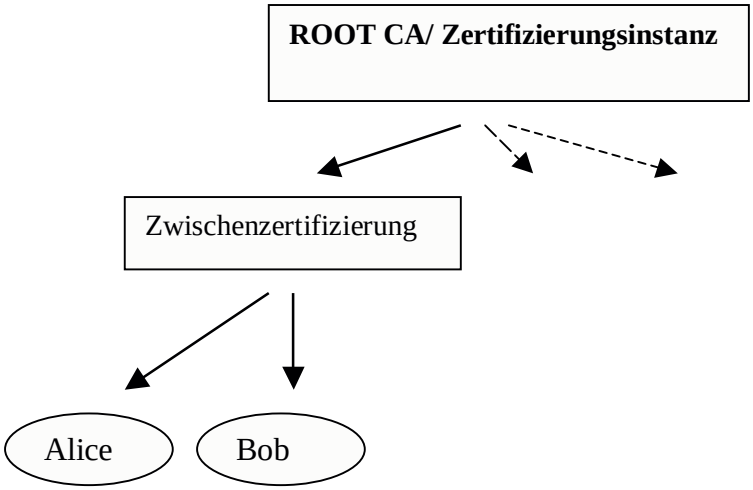

Abbildung (6): Certificate Chain

An höchster Stelle befindet sich die Root CA (Haupt–Zertifizierungsinstanz), die Certificate Authority. Sie stellt die höchste Stelle der PKI (Public Key Infrastructure) dar. Digitale Zertifikate X.509 oder die Digitale Signatur X.509 garantieren, dass ein öffentlicher Schlüssel eindeutig einem bestimmten Benutzer zugewiesen werden kann. Eine Certification Authority (CA) ist eine „Trusted Third Party“ (vertrauenswürdige Einheit), die Digitale Zertifikate herausgibt und verwaltet. Diese CA garantiert, dass ein öffentlicher Schlüssel einem einzigen, identifizierten Benutzer gehört. Die Herausgabe der Zertifikate kann offline und online geschehen. Online bietet z.B. das TC TrustCenter ein sogenanntes Class 1 Zertifikat an, dass kostenlos eine „einfache Sicherheitsstufe“ darstellt. Bei der Beantragung eines Class 1 oder Express-Zertifikates[36] wird lediglich die Richtigkeit der angegebenen E-Mail-Adresse überprüft. Bei TC TrustCenter Class 1 Zertifikaten werden äußerst geringe Anforderungen an den Nachweis der Identität gestellt. Vornehmlich dient es hier zum Ausprobieren von verschlüsseltem Mailverkehr mit Hilfe von X.509 Zertifikaten. Offline müssen Benutzer physisch bei der CA anwesend sein. Hier sei z.B. das Trustcenter Verisign[37] mit seinem Class 3 Zertifikat genannt. Wenn ein solches Center bestimmte Anforderungen erfüllt, sind die mit den Zertifikaten erstellten Unterschriften nach deutschem Gesetz rechtsgültig. TeleSec (Telekom) und Signtrust (Deutsche Post) sind zwei weitere

[36] Von TC TrustCenter so benannt

[37] http://www.verisign.com/

Anbieter der sogenannten „qualifizierenden Signatur“, für die eine Sicherheitsvermutung nach dem im März 2001 überarbeiteten Signaturgesetz gilt.

Solange einer höheren Instanz vertraut wird, sind automatisch alle davon abhängigen Zertifikate als vertrauenswürdig eingestuft.

Microsoft geht mit Windows XP einen neuen Weg. Hier wird dem Benutzer die Entscheidung über die Vertrauenswürdigkeit von CAs vollständig aus der Hand genommen. In der Dokumentation heißt es dazu:

> „New root certificates are no longer available with Microsoft Internet Explorer. Any new roots accepted by Microsoft are available to Windows XP clients through Windows Update. When a user visits a secure Web site (that is, by using HTTPS), reads a secure e-mail (that is, S/MIME), or downloads an ActiveX control that uses a new root certificate, the Windows XP certificate chain verification software checks the appropriate Windows Update location and downloads the necessary root certificate. To the user, the experience is seamless. The user does not see any security dialog boxes or warnings. The download happens automatically, behind the scenes.“ [38]

Betrachtet die Firma Microsoft nun eine CA als vertrauenswürdig, so ist auch der Nutzer von Windows XP gezwungen, diese als vertraut einzuschätzen. Die Sicherheit hängt hier von dem Urteil Microsofts, sowie von der Funktionalität und Unverwundbarkeit der „Windows Update location“ ab.[39]

---

[38] [Micr02]

[39] Difficile est saturam non scribere – frei übersetzt: es ist schwierig darüber (über Microsoft) keine Satire zu schreiben

4.3 Widerruf

Als Widerruf bezeichnet man eine Art Rückruf des öffentlichen Schlüssels. Ein Widerruf kann zu jedem Zeitpunkt vollzogen werden, ist jedoch meist nur in folgenden Situationen sinnvoll:

- der private Schlüssel ist verloren gegangen
- der private Schlüssel wurde wahrscheinlich von Dritten kopiert
- das Mantra[40] wurde vergessen

PGP und S/MIME bestreiten unterschiedliche Wege im Umgang mit widerrufenen Schlüsseln. Bei PGP kann eine Widerrufurkunde für den erzeugten Schlüssel erstellt werden. Mit einer Widerrufurkunde können andere in Kenntnis gesetzt werden, dass der dazugehörige öffentliche Schlüssel nicht mehr gültig ist. Der öffentliche Schlüssel sollte nicht mehr benutzt werden, was nicht heißt, dass das nicht möglich wäre. Unterschriebene Dokumente können weiterhin mit dem Schlüssel überprüft werden. So bleibt gewährleistet, dass Abmachungen und Verträge dadurch nicht ihre Gültigkeit verlieren. Eine Widerrufurkunde sollte aus Eigeninteresse sicher aufbewahrt werden.

PGP speichert widerrufene Schlüssel mit den gültigen Schlüsseln auf dem gleichen Keyserver. Der Widerruf wird als eine besondere Signatur an den Schlüssel gehängt.

S/MIME verwendet Certificate Revocation Lists (CRLs)[41], die alle gesperrten Schlüssel in einer Liste beinhalten. Die Nutzer laden sich die Liste (oder ein Listenupdate) von speziellen CRL-Servern. Die Liste der CRLs wächst ständig und sollte regelmäßig heruntergeladen und gespeichert werden.

---

[40] Passwort-Satz. Der geheime Schlüssel ist bei PGP noch einmal selbst mit einem Mantra geschützt. Ohne das Mantra kann man den geheimen Schlüssel weder zum Entschlüsseln noch zum Signieren verwenden.

[41] S/MIME bietet auch ein zu den CRLs inkompatibles Online Certificate Status Protocol (OCSP) an. Dieses funktioniert nach dem Prinzip der Widerrufurkunden von PGP, ist allerdings vom Verbreitungsgrad noch hinter den CRLs.

5 Gebrauch in der Praxis

Es ist nicht möglich eindeutige, unabhängige Zahlen über den Gebrauch der PGP und S/MIME Derivate zu finden.

PGP Version 7 wird per Plug-Ins unterstützt für Outlook, Outlook Express, Lotus Notes, Eudora, Pegasus Mail 3.0, Netscape Messanger und Claris E-Mailer (Mac).

GnuPG auf GNU/Linux mit x86, alpha, mips, sparc64, m68k oder powerpc CPUs, FreeBSD mit x86 CPU, OpenBSD, NetBSD Windows 95/98/NT/2000/ME mit x86 CPU. Nicht ausführlich getestet auch auf: AIX v4.3, BSDI v4.0.1, HPUX v9.x, v10.x und v11.0 mit HPPA CPU, IRIX v6.3 mit MIPS R10000 CPU, MP-RAS v3.02, OSF1 V4.0 mit Alpha CPU, OS/2 Version 2. SCO UnixWare/7.1.0. SunOS, Solaris auf Sparc und x86, USL Unixware v1.1.2.[42]

S/MIME wird von den Programmen Microsoft Outlook, Outlook Express, Lotus Domino/Notes, Noell GroupWise und Netscape Communicator bis 4.78 direkt unterstützt.

Network Associates hat bekannt gegeben, dass es die PGP-Produktreihe nicht mehr weiterentwickelt. Laut NAI hat sich kein adäquater Käufer für die rennomierte Verschlüsselungslösung gefunden.[43]

GnuPG kann mit Hilfe des Projekts GnuPP[44] unter Windows und GNU/Linux grafisch benutzt werden. WinPT ist ein Taskleistenwerkzeug. Über die Zwischenablage können E-Mails ver- und entschlüsselt werden. Die kryptographischen Algorithmen und Signaturerstellungen werden vom GNU Privacy Guard bereitgestellt. Dadurch ist es möglich GnuPG mit jedem Mailprogramm zu verwenden. Über die Zwischenablage

---

[42] Vgl. [Gnup02]

[43] Vgl. [Heise02b]

[44] http://www.gnupp.de

werden Schlüssel exportiert und importiert. Das relativ neu auf dem Markt befindliche Verschlüsselungssystem GnuPP findet ständig weitere Verbreitung. GnuPP ist ein vom Bundesministeriums für Wirtschaft und Technologie (BMWi) gefördertes Projekt. Die Projektleitung erfolgt seit März 2001 durch die G-N-U GmbH[45].

5.1 Beispiel einer S/MIME Zertifikat Installation

Zertifikate sind von Trustcenter wie z.B. AddTrust, BeTRUSTED (Price Waterhouse Coopers), BT TrustWise, Deutsche Telekom, VISA International oder XCERT International, Inc. zu erwerben. Im Folgenden Beispiel wird ein S/MIME Zertifikat bei der TC TrustCenter AG beantragt. Vier Klassifizierungen stehen zur Auswahl:

- Class 0 - keine Prüfung, wird umgehend ausgestellt
- Class 1 - nur Prüfung der im Zertifikat genannten E-Mail-Adresse
- Class 2 - Prüfung der E-Mail-Adresse und Prüfung von Dokumenten (HRA)
- Class 3 - Prüfung der E-Mail-Adresse, Prüfung von Dokumenten und persönliche Identitätsfeststellung (entweder Besuch bei TC TrustCenter oder Post-Ident-Verfahren bei einer beliebigen Postfiliale innerhalb Deutschlands).

Technische Unterschiede bezüglich der Sicherheit und Verschlüsselungsstärke gibt es nicht. Das Vertrauen in ein Zertifikat mit zunehmender Zertifikatsstufe ist jedoch höher. Das Class 1 Zertifikat ist kostenlos und wird in diesem Beispiel verwendet.

Als System wird der Netscape Communicator 4.78 Messenger unter GNU/Linux benutzt.

Auf der TC TrustCenter Homepage beantragt man ein S/MIME Class 1 Zertifikat. Nachdem Name und E-Mail Adresse verlangt worden sind, wird um ein Passwort gebeten. Dieses Passwort schützt die lokale Zertifikats-Datenbank, bleibt dem Trustcenter verborgen und wird nur von dem jeweiligen Browser verwaltet. Das

[45] http://www.g-n-u.de

Passwort ist vergleichbar mit dem Mantra unter PGP. Ein weiteres, sogenanntes Notfall-Passwort, dient zur eventuellen telefonischen Sperrung des Zertifikates und wird der TC TrustCenter AG übermittelt und von ihr verwaltet. Bei der Schlüssellänge wurden die Optionen zwischen 512, 1024 und 2048 Bit angeboten. Die optionalen Schlüssellängen sind vom verwendeten Browser abhängig. Je nachdem welche CSP (Cryprographic Service Provider) im Browser vorhanden sind, werden unterschiedliche Schlüssellängen angezeigt. Für Privatanwender reichen 1024 Bit, auf die ich mich jedoch zukunftsorientiert nicht beschränkt habe und so 2048 Bit auswählte. Die TC TrustCenter relevanten Daten werden nun über den Browser abgeschickt. Wenige Sekunden später erreicht einen eine E-Mail des Trustcenters mit der Bitte um Bestätigung. Diese dient der Überprüfung der angegebenen E-Mail Adresse. Sind Betreffzeile und Inhalt richtig ausgefüllt und die E-Mail abgeschickt, so sendet das TC TrustCenter eine weitere Mail mit einem Link zur Installation des Zertifikats im Browser. Auf der dort vorliegenden Seite sind die persönlichen Daten noch einmal abzugleichen und die Installation ist dann per Button zu starten. Das Zertifikat installiert sich nach der Eingabe des Passworts eigenständig.

Das Verteilen des eigenen öffentlichen Schlüssels erfolgt in jeder signierten Mail automatisch. Netscape integriert den Schlüssel in signierte Mails, falls die entsprechenden Optionen im Mailprogramm aktiviert sind. Standardmäßig ist dieses voreingestellt.

Um nun eine E-Mail zu verschlüsseln, wird der öffentliche Schlüssel des Empfängers benötigt. Hierzu muss z.B. eine signierte Mail von dem Kommunikationspartner empfangen worden sein. Ist der Schlüssel vorhanden, gestalten sich die Signierung und Verschlüsselung wie folgt:

Nachdem eine Mail wie gewohnt angelegt wurde, muss anschließend auf die unterste Registerkarte, über dem "Betreff"-Feld, geklickt werden. Nun können die Optionen für Verschlüsselung und Signierung auswählt werden.

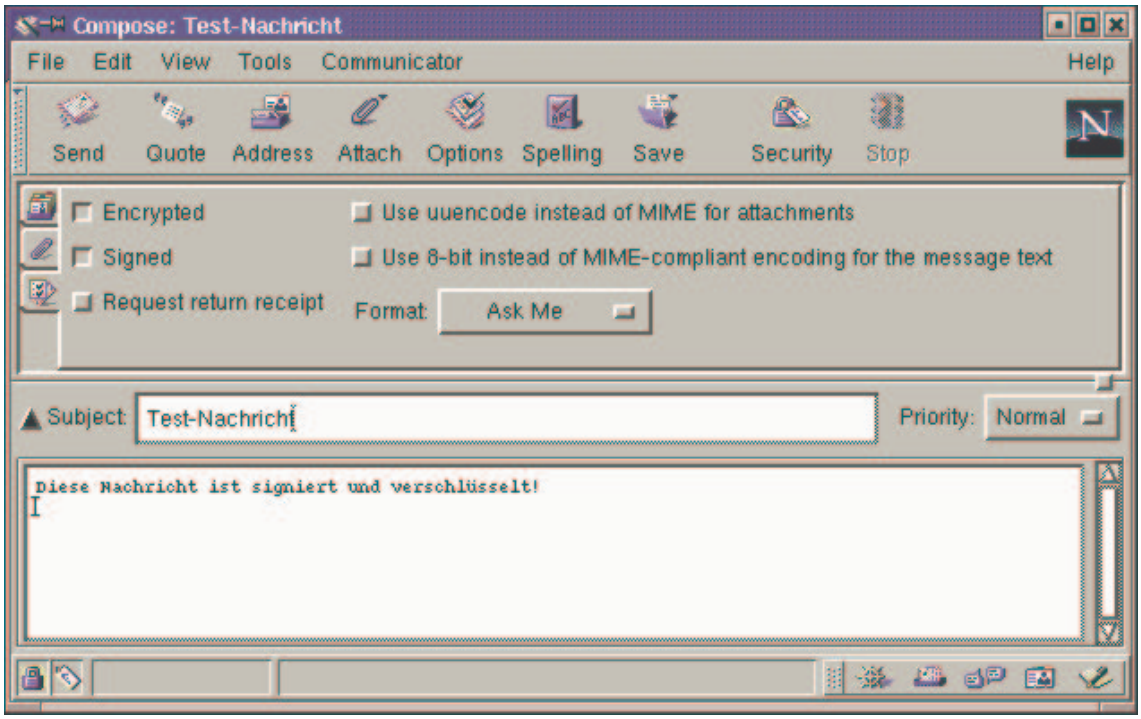

Abbildung (7): Nachricht erstellen

Eine verschlüsselte E-Mail, egal ob empfangen oder versendet, ist am Icon „Encrypted“, in der rechten Ecke der jeweiligen Mail, zu erkennen.

Das S/MIME Zertifikat Passwort muss einmal in jeder Sitzung richtig eingegeben werden. Ab diesem Zeitpunkt werden alle verschlüsselten E-Mails im Klartext angezeigt.

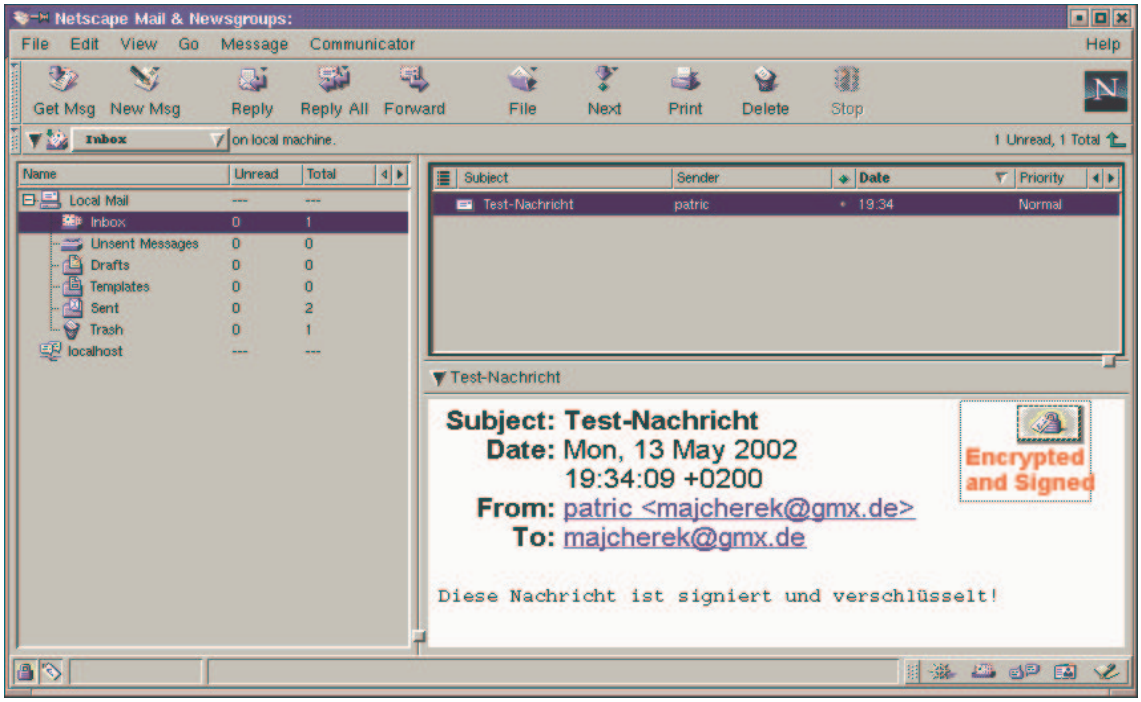

Abbildung (8): Nachricht lesen

Weitere Einstellungen zur Sicherheit und Sicherheitsmerkmale zur jeweiligen E-Mail lassen sich öffnen , indem auf das Schloss in der linken unteren Ecke geklickt wird.

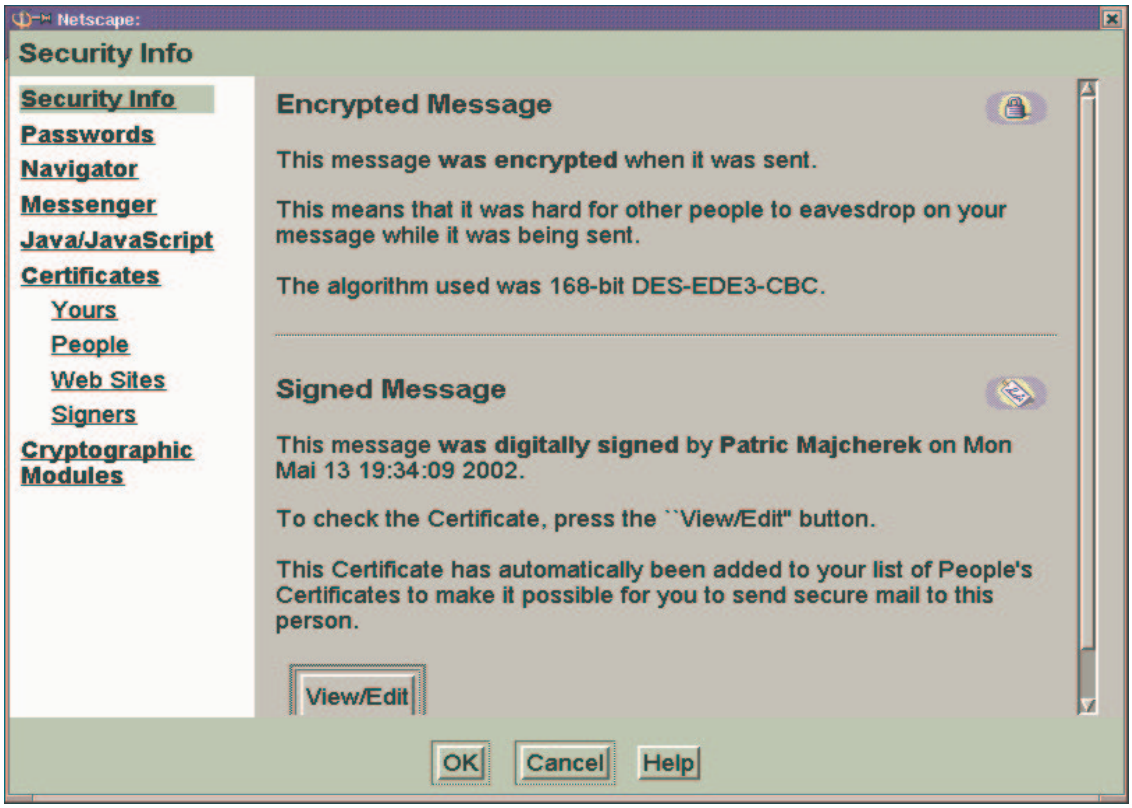

Abbildung (9): Security Info

Die Möglichkeit der S/MIME Verschlüsselung ist im Netscape Communicator bis Version 4.78 sowie im Internet Explorer implementiert. Eine S/MIME Mozilla Version ist in Bearbeitung.

5.2 Erfahrungen einer Zertifizierungsinstanz

Um mehr Informationen über den Gebrauch von PGP und S/MIME in der Praxis zu erfahren, sprach ich mit Dietmar Paulke, verantwortlich für den technischen Support der TC TrustCenter AG in Hamburg. Die folgenden Erläuterungen beziehen sich auf das Gespräch zwischen Herrn Paulke und mir.

Dank seiner langjährigen Erfahrung im Bereich der Sicherheit im E-Mail Verkehr konnte er zu vielen Punkten Stellung nehmen. Angaben über Benutzerzahlen der PGP oder S/MIME Protokolle hielt auch Herr Paulke für sehr schwer ermittelbar. Dies läge vor allem an der spärlichen Registrierung der PGP Benutzer bei diversen Trustcentern. Um sicher Daten zu verschicken, benötigen PGP Nutzer keinen, von einem Trustcenter signierten, öffentlichen Schlüssel. Oft tauschen die Nutzer von PGP den Schlüssel und ihren Fingerprint nur „unter sich“ aus. Eine Erhebung über die Benutzerzahlen ist so faktisch unmöglich. TC TrustCenter stellt Geschäftskunden-Zertifikate sowohl für X.509, als auch für PGP aus. Privatkunden-Zertifikate werden seit dem 17.05.2002 nicht mehr angeboten. Dies betrifft X.509 und PGP. Für private Anwender gibt es die kostenlosen Class 1-Zertifikate; X.509 über das Express Zertifikat und PGP über einen Link von der Homepage aus.

In vielen Sicherheitsbereichen, so Paulke, werden weder S/MIME noch PGP eingesetzt. Oft sind professionelle, proprietäre Lösungen aus unterschiedlichsten Gründen bevorzugt worden. Zwischen S/MIME und PGP scheinen Privatanwender zur Zeit in Richtung S/MIME zu tendieren. Vor allem der hohe Verbreitungsgrad des Microsoft Internet Explorers mit eingebundenem S/MIME Support ist Ursache für diesen Trend. Gegenläufig sind hier einige wenige auf Sicherheit bedachte Firmen, die sich nicht für S/MIME entschieden haben. Das Missvertrauen in proprietärer, nicht offen gelegter

Software, ist der Hauptgrund für diese Firmen. Die Krypto-Exportbeschränkung der USA, eine zu späte hohe Verschlüsselung auf dem Markt ausserhalb der Vereinigten Staaten von Amerika, verstärken das Misstrauen in den Sourcecode des S/MIME Protokolls. GnuPG und PGP sind dann die Erste Wahl.

6 Alternativen

An Bedeutung verloren hat heute Privacy Enhanced Mail (PEM). Als erster Standard für verschlüsselte und digital unterschriebene E-Mails wurde er geboren, hatte jedoch grundsätzliche Designfehler. PEM kann ausschließlich 7-Bit ASCII Text und Dateianhänge nur in das eigene Format bringen. Das damalige DES Verfahren ist für heutige Verhältnisse zu schwach ausgelegt.

MIME Object Security Services (MOSS) sollte die Nachteile von PEM beheben. MOSS hat sich jedoch nicht durchsetzen können und ist heutzutage nahezu bedeutungslos.

Was bleibt, sind die schon über Jahre teils wissenschaftlich getesteten Algorithmen, die in PGP/ OpenPGP/ GnuPG und S/MIME verwendet werden. Um eine flächendeckende Verbreitung zu fördern, wären einfach zu bedienende Programme dringend notwendig. Das GnuPP zielt in die richtige Richtung. S/MIME ist in ihrer eingeschränkten Umgebung schon recht komfortabel. Der Freemailer web.de versucht S/MIME noch bequemer zu gestalten. Web.de Freemail bietet eine für den Anwender angenehm nutzbare Verschlüsselung und Signatur auf Basis des Verfahrens S/MIME 2.0. Leider hat das Sicherheitsmodell von web.de eine ernsthafte Sicherheitslücke. Der Provider ist dabei im Besitz der privaten Schlüssel seiner Kunden. Dies soll zwar einem komfortablen mobilen Nutzen der Verschlüsselung dienen, widerspricht jedoch allen Regeln der Sicherheitslehre.

In dieser Seminararbeit wurde vor allem auf E-Mail-Programme mit Ver- und Entschlüsselung und dazugehörige Plug-Ins eingegangen. Es gibt jedoch noch drei weitere Möglichkeiten den E-Mail Verkehr zu sichern.

VPN-Lösungen[46] (Virtual Private Network), bei denen beispielsweise die Verbindung zwischen zwei Netzwerken oder zwei Rechnern über das Internet verschlüsselt wird, sind eine weitere Möglichkeit sichere E-Mail Kommunikation zu betreiben. Hier ist keine Installation für den Endbenutzer notwendig. Der größte Nachteil dieser Lösungen ist die fehlende „Ende-zu-Ende-Sicherheit“. So ist der Weg von der Verschlüsselungshardware (meist ein Firmenrechner am Eingang des LAN) zu dem Endbenutzer im internen Netzwerk unverschlüsselt. Diese Lösung eignet sich besonders gut für Firmen, die ihre Mails vorwiegend über das Internet zwischen zwei Firmenstandorten austauschen wollen.

Weiterhin bieten auch Proxy-Lösungen[47] Ver- und Entschlüsselung der ein- bzw. ausgehenden Mails auf dem Mailserver. Auch hier arbeitet die Verschlüsselung unabhängig vom E-Mail-Programm. Die Einrichtung bei den Endnutzern und auf dem Mailserver ist jedoch relativ aufwendig. Wie bei den VPN-Lösungen wird auch hier keine Ende-zu-Ende-Sicherheit geboten.

Zuletzt setzen noch sogenannte Winsock-Lösungen[48] direkt auf der Winsock, d.h. unterhalb der Anwendungsebene, auf. Auch diese Lösung ist vom E-Mail-Programm unabhängig. Ein großer Nachteil ist jedoch, dass Winsock-Lösungen ausschließlich unter Windows arbeiten.

7 Kritische Würdigung

Die Entscheidung für PGP, ein PGP Derivat oder S/MIME hängt von vielen Faktoren ab. Verschlüsselung von E-Mails ist mit beiden[49] Verfahren möglich. Sollen jedoch auch weitere Daten wie Textdateien, Bilddaten, Sourcecode, Datenbanken, oder komplette Festplatten verschlüsselt werden, so lässt sich dieses nur mit PGP vollziehen. Eine professionelle PKI finden wir bei S/MIME, da für die Generierung der Zertifikate

[46] Vgl. [Boeh02]

[47] Vgl. [Sack01]

[48] Vgl. [Reil00]

[49] Inkl. der PGP Derivate

eine zentrale Instanz vorausgesetzt wird. Viele TrustCenter leben von diesem Ansatz indem sie Zertifikate verkaufen und beglaubigen. Die Zertifizierung von PGP-Schlüsseln beruht auf dem Web-of-Trust Ansatz ohne zentrale oberste Instanz. Hierarchische Strukturen lassen sich jedoch auch mit PGP nachbilden, [50] die Grundstruktur besteht jedoch aus einem Netzwerk von Leuten, die sich kennen und vertrauen. PGP bietet stark eingeschränkten Import von MIME Zertifikaten an.[51] Kompatibilität ist zwischen beiden Internetstandards im Großen und Ganzen jedoch nicht vorgesehen. Für S/MIME bieten vielen Firmen professionellen Support. Auch für GnuPG lassen sich solche Firmen, wie z.B. die G-N-U GmbH (für GNU Nutzer Unterstützung) finden. Der administrative Aufwand ist für das Web-of-Trust höher, bietet aber auch mehr Optionen[52]. Ein Vertrauen zu S/MIME aufzubauen, fällt angesichts der neuen Strategie von Microsoft (siehe Kapitel 4.2.2) und des nicht vorhandenen Sourcecode sehr schwer.

Der größte Vorteil von GnuPG gegenüber proprietärer Software ist daher die Sicherheit, die in der Lizenz, unter der GnuPG fällt, begründet ist. Experten vom Bundesamt für Sicherheit in der Informationstechnik, des Bundesministeriums für Wirtschaft und Technologie sowie des Bundesministeriums des Innern über das Bundeswirtschafts- und Forschungsministerium bis zum Chaos Computer Club (CCC) sind der einhelligen Überzeugung, dass Quelloffenheit einer Software essenzielle Voraussetzung für ihre Sicherheit ist.[53] Bei proprietärer Software muss sich der Anwender auf das Wort des Anbieters verlassen, was grundsätzlich als suspekt angesehen werden sollte. Überprüfbarkeit durch Experten des Vertrauens, somit Quelloffenheit, ist eine Voraussetzung für Vertrauensbildung. Ein Allheilmittel oder der Schlüssel zur Sicherheit ist freie Software jedoch nicht. Nachträglich quelloffen gelegte Programme sind aufgrund der Komplexität oft schwer zu überschauen. Kaum jemand hat den Quelltext der PGP Version 5.0, die seit Anfang 1998 quelloffen gelegt wurde, durchgelesen. Selbst die Gefahr, in Teams etwas zu übersehen, ist nicht unbegründet. Erst über ein Jahr nach Offenlegung des Quelltextes, also im Mai 1999, wurde eine

---

[50] Auch hier kann jeder eine Art „Root CA“ bestimmt werden; Dieser wird voll vertraut; Von ihr wird allen Teilnehmern den jeweiligen öffentlichen Schlüssel signiert.

[51] RFC 3156 MIME Security with OpenPGP

[52] Vgl. Kap. 3.2.1

[53] Vgl. [Gras02]

Sicherheitslücke gefunden und behoben. Nur permanente, mitlaufende Überprüfung durch Nutzer, Gruppen und Behörden bieten die Gewähr, dass weder nachlässig noch gezielt Sicherheitsprobleme eingebaut werden. GnuPG wurde von Anfang an offen entwickelt.

8 Literaturverzeichnis

[Bmwi02] Startseite „Sicherheit im Internet”;
Bundesministerium für Wirtschaft und Technologie (BMWI);
http://www.sicherheit-im-internet.de/; 04.05.2002.

[Boeh02] Boehmer, Wolfgang; VPN, Virtual Private Networks;
1. Auflage; Hanser Fachbuchverlag; 2002.

[Bund99] Eckpunkte der deutschen Kryptopolitik;
verabschiedet vom deutschen Bundeskabinett am 2. Juni 1999.

[Camp01] COMINT Impact on International Trade;
Duncan Campbell;
http://www.heise.de/tp/deutsch/special/ech/7752/1.html; 29.04.2002.

[Frey02] Freyermuth, Gundolf S.; Telefonie 3.0; c´t 8/2002; S. 244-250.

[Gnuo02] The Free Software Definition;
Free Software Foundation, Inc.;
http://www.gnu.org/philosophy/free-sw.html; 04.05.2002.

[Gnup02] The GNU Privacy Guard;
Free Software Foundation, Inc.;
http://www.gnupg.org/backend.html; 04.05.2002.

[Gras02] Grassmuck, Volker; Freie Software;
Zwischen Privat- und Gemeineigentum;
1. Auflage; Bundeszentrale für politische Bildung; 2002.

[Grun02] Grundgesetz der Bundesrepublik Deutschland.

[Heise02a] Lauschposten in Bad Aibling bleibt bestehen;
Florian Rötzer;
http://www.heise.de/tp/deutsch/html/result.xhtml?url=/tp/deutsch/special/ech/9937/1.html; 29.04.2002.

[Heise02b] Kein Käufer für PGP;
http://heise.de/newsticker/data/pab-04.03.02-000/; 29.04.2002.

[Ietf02] The Internet Engineering Task Force;
Organized activity of the Internet Society http://www.isoc.org;
http://www.ietf.org/; 29.04.2002.

[Ietf96] PGP Message Exchange Formats;
The Internet Engineering Task Force;
http://www.ietf.org/rfc/rfc1991.txt?number=1991; 29.04.2002.

[Micr02] Microsoft Root Certificate Program;
Microsoft;
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/rootcert.asp; 29.04.2002.

[Reil00] Reilly, Douglas J.; Inside Server-Based Applications;
1. Auflage; Microsoft Press Corp.; 2000.

[Sack01] Sackett, George C.; CISCO Router Handbuch;
1. Auflage; Franzis; 2001.

[Schn99] Crypto-Gram Newsletter vom 15.09.1999;
Bruce Schneier;
http://www.counterpane.com/crypto-gram-9909.html#OpenSourceandSecurity; 29.04.2002.

[Smim02] S/MIME Central;
RSA Security;
http://www.rsasecurity.com/standards/smime/; 04.05.2002.