

E-Mails: Verschlüsselt und unterschrieben

Über die Sicherheit von E-Mail war bereits im gleichnamigen Artikel etwas zu lesen. Die folgende Abhandlung befasst sich ebenfalls mit diesem Thema. Es wird allerdings etwas spezieller auf die Möglichkeit eingegangen, die elektronische Konversation via E-Mail abzusichern. Dabei stehen die Punkte Vertraulichkeit, Authentizität und Integrität im Mittelpunkt. Diese Punkte sollen in Bezug auf E-Mail sicherstellen, dass:

- die Informationen nur vom Adressaten gelesen werden können,
- E-Mails wirklich vom angegebenen Absender stammen und
- der Inhalt der Nachricht durch Dritte nicht verändert wurde.

Die Realisierung dieser drei Punkte leistet das nachfolgend beschriebene Programm:

PGP (Pretty Good Privacy) ist ein Freeware-Verschlüsselungsprogramm, das u. a. das Signieren und Verschlüsseln von E-Mails erlaubt. Das Programm wurde 1991 von Philip R. Zimmermann entwickelt und hat inzwischen eine sehr große Verbreitung erlangt. Zu finden ist es auf der CD „Zugang zum Internet“ des RZ oder im Internet unter der Adresse <http://www.pgpi.com/>.

```
Date: Thu, 05 Aug 1999 11:38:30 +0200
To: winks@rz.hu-berlin.de
From: Jens-Uwe Winks <Winks@rz.hu-berlin.de>
Subject: PGP

-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.0.2i

hQEMAx493pEwH6MJAQf+KHZmIxsv7Kmad1TGgntm6pbouAi5CRzMX/frjpfD7JwX
[....]
0zEKrvb51KCEmlCV8XPiJl07o6IBY4t5XwNIIYk8le2kFV8V0jfwNwF+asD3UsF9
krk=
=R9PP
-----END PGP MESSAGE-----
```

Abb. 1: Beispiel für eine verschlüsselte Mail

Das Programm arbeitet mit einem Schlüsselpaar, bestehend aus einem geheimen und einem öffentlichen Schlüssel (Secret und Public Key), die bei der Installation (unter Windows) generiert werden. Mit diesen werden die drei oben genannten Punkte wie folgt realisiert:

Vertraulichkeit

Mit dem öffentlichen Schlüssel des Empfängers können E-Mails verschlüsselt werden. Nur der Empfänger ist in der Lage, mit seinem geheimen Schlüssel den Text wieder in eine lesbare Form zu bringen.

Authentizität und Integrität

Mit seinem geheimen Schlüssel kann der Verfasser einer E-Mail eine Signatur erzeugen. Darunter kann man sich eine mehrere Zeilen umfassende Zeichenfolge vorstellen, die an die E-Mail gehängt wird (siehe Abb. 2). Der Empfänger kann mit dem öffentlichen Schlüssel des Absenders überprüfen, ob die Signatur zum Text gehört. Nur dann ist sichergestellt, dass die E-Mail tatsächlich vom angegebenen Absender stammt und der Inhalt nicht verändert wurde.

Der Secret Key sollte, wie der Name schon sagt, geheim sein und auch bleiben, da nur mit diesem das Entschlüsseln und Signieren bewerkstelligt werden kann. Bei der Generation des Schlüsselpaars wird die Eingabe einer Passphrase verlangt, die den geheimen Schlüssel vor Missbrauch schützt. Sie sollte möglichst aus einem Satz bestehen, der auch geheim gehalten werden muss.

Der öffentliche Schlüssel kann – damit er anderen zugänglich ist – auf einem Public Key Server hinterlegt werden (z. B. <http://keys.pgp.com:11371/>). Weiterhin gibt es Web-Interfaces, die das Hinterlegen und die Suche nach Schlüsseln gestatten, wie z. B. <http://math-www.uni-paderborn.de/pgp/>.

PGP gibt es in verschiedenen Versionen für verschiedene Plattformen. Bei der Arbeit mit PGP unter Unix muss auf die kommandozeilenorientierte Version zurückgegriffen werden. Die Auswahl der gewünschten Funktion (z. B. das Generieren eines Schlüsselpaars) erfolgt über Optionen, die beim Aufruf übergeben werden. Einige Mailtools im Unix bieten aber auch eine direkte Unterstützung für PGP an. So kann beispielsweise im Mailprogramm elm das Signieren und Verschlüsseln über entsprechende Menüpunkte erfolgen.

```
Date: Thu, 05 Aug 1999 12:01:44 +0200
To: winks@rz.hu-berlin.de
From: Jens-Uwe Winks <Winks@rz.hu-berlin.de>
Subject: PGP

-----BEGIN PGP SIGNED MESSAGE-----

Das ist eine Mail mit Signatur.
-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 6.0.2i

iQEVAwUBN6lS+B493pEwH6MJAQFwocgf/de5VC3EUMURE87Ag1Hb/G2n7Enu2HLlm
[....]
HB2OC9/qoDDdmmg41Sd2vEwh2nr8z1EIt2mFLbBXhv6/QTQU+dLwXQ==
=9hhQ
-----END PGP SIGNATURE-----
```

Abb. 2: Beispiel für eine signierte Mail

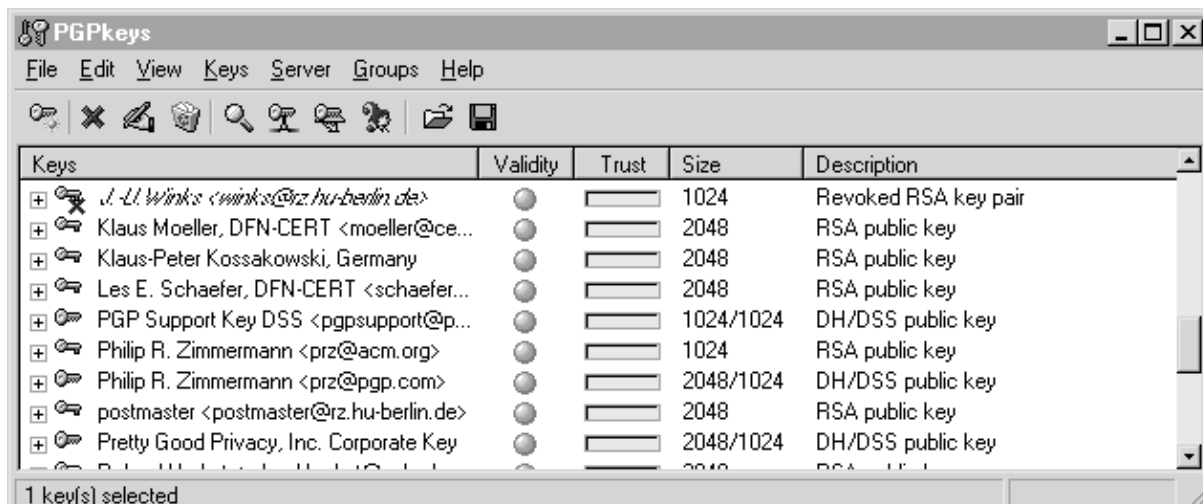


Abb. 3: Windows PGP-Interface

Für Windows gibt es eine graphische Oberfläche (siehe Abb. 3), die das Verwalten fremder Public Keys und die Arbeit mit PGP ermöglicht. Des weiteren beinhaltet diese Version auch Plugins für Eudora und Microsoft Outlook, die PGP in diese Mailoberflächen integrieren. Damit werden das Ver- und Entschlüsseln und das Signieren sehr einfach. In die Oberfläche des Mailtools werden Buttons und Menüs für die PGP-Funktionen integriert. Über die Einstellungen im Mailtool kann festgelegt werden, ob ausgehende Mails standardmäßig signiert und/oder verschlüsselt werden sollen bzw. ob das Entschlüsseln von Mails und Verifizieren von Signaturen automatisch erfolgen soll.

Beispiele:

Auszug aus der Menüleiste von Eudora (mit PGP-Plugin) beim Erstellen einer neuen Mail:

- v.l.n.r.:
- Benutzung von PGP/MIME aktivieren
 - abgehende Mail verschlüsseln
 - abgehende Mail signieren
 - Mail abschicken



Abb. 4: PGP-Buttons aus der Eudora-Menüleiste

Header einer entschlüsselten Mail in Eudora:

```
*** PGP Signature Status: good
*** Signer: daniel b. <b@hu-berlin.de>
*** Signed: 23.07.99 15:07:23
*** Verified: 26.07.99 13:56:39
*** BEGIN PGP DECRYPTED/VERIFIED
MESSAGE ***
```

Abschließend sei noch auf die sehr ausführlichen Dokumentationen hingewiesen, die bei der Installation eingespielt werden können bzw. auf den öffentlichen Workstations des RZ unter /usr/local/lib/pgp verfügbar sind.

Jens-Uwe Winks
winks@rz.hu-berlin.de