OpenPGP

Jan Tobias Mühlberg
<muehlber@fh-brandenburg.de>

Brandenburg, den 9. Dezember 2003

OMNIS ENIM RES, QUAE DANDO NON DEFICIT,
DUM HABETUR ET NON DATUR, NONDUM HABETUR,
QUOMODUM HABENDA EST.

— St. Augustinus, 397 CE, „De doctrina christiana“

Gliederung

1. Entwicklung von OpenPGP
2. Funktionsweise
   - Schlüsselerzeugung und -verwaltung
   - „Web of Trust“
3. Implementierungen und Verwendbarkeit

Die Entwicklung von OpenPGP

- PGP steht für „Pretty Good Privacy“ und wurde 1991 von Phil Zimmermann, damals noch MIT-Student, „erfunden“.
- Zimmermall wollte eine praktikable, einfach bedienbare Krypto-Infrastruktur schaffen, die an die anarchische Struktur des Internets anlehnt.
- PGP war Freeware mit offenem Quellcode und fand sehr schnell Verbreitung.

Die Entwicklung von OpenPGP

- 1994 gründete Zimmermann die PGP Inc., die wurde 1997 von Network Associates Inc. aufgekauft. NAI vertreibt bis heute erfolgreich PGP-Software.
- Die erste Standardisierung erfolgte 1996 mit RFC1991.
- 1998 wurde die bis heute gültige Überarbeitung dieses Standards uter dem Titel „RFC2440: OpenPGP Message Format“ veröffentlicht.
- RFC2440 ist abwärtskompatibel zu RFC1991.

Die Funktionsweise von PGP - Schlüsselerzeugung

- Teilnehmer erzeugen sich selbst ein, üblicherweise jedoch zwei Schlüsselpaare, eines zum Signieren und eines zum Verschlüsseln von Nachrichten.
- Die beiden Schlüsselpaare werden zusammengefaßt gespeichert, der Benutzer bemerkt von der Teilung nichts.
- Nach der Erzeugung werden die Benutzerdaten (Name, E-Mail-Adresse) mittels einer Signatur an den Schlüssel gebunden.
- Der Schlüssel kann mehrere Sätze von Benutzerdaten enthalten, also auch für verschiedene E-Mail-Adressen gültig sein.

Die Funktionsweise von PGP - Schlüsselverwaltung

- PGP-Implementierungen verwenden meist zwei Schlüsselringe, einen für öffentliche und einen für geheime Schlüssel.
- Beiden Schlüsselringen können beliebig viele Schlüssel zugefügt werden.
- Geheime Schlüssel sind einzeln durch symmetrische Verschlüsselung geschützt.

Die Funktionsweise von PGP - Schlüsselaustausch

- Neben den Schlüsselringen gibt es auch ein internationales Netzwerk von **Keyservern**, auf denen öffentliche Schlüssel hinterlegt sind.

- Keyserver können bei Bedarf nach einem Schlüssel oder einer E-Mail-Adresse durchsucht werden.

Web of Trust

- OpenPGP-Schlüsselmaterial kann beliebig oft erneut signiert werden.
- Dies kann beispielsweise duch andere Teilnehmer, oder auch durch Trustcenter bzw. CAs geschehen, die mit ihrer Signatur für die Authentizität des Schlüsselmaterials bürgen.
- Unterschrieben wird immer der öffentliche Schlüssel.
- Das gegenseitige Unterschreiben von Schlüsseln führt zum Aufbau eines „Web of Trust“, in dem viele Teilnehmer gegenseitig für die Authentizität verwendeter Schlüssel bürgen.

Verfügbare Software und Links

- Verschiedene kommerzielle Implementierungen, u.a. von NAI: http://www.nai.com/
- Eine freie Implementierung, GnuPG: http://www.gnupg.org/
- Kompatibilität zwischen S/MIME und OpenPGP bietet gpgsm: http://www.gnupg.org/aegypten/
- DFN-Keyserver: http://www.pca.dfn.de/pgpkserv/
- Plugins für diverse Mailsoftware finden sich meist auf den Webseiten des betreffenden Programms.