

OpenPGP

Jan Tobias Mühlberg

[<muehlber@fh-brandenburg.de>](mailto:muehlber@fh-brandenburg.de)

Brandenburg an der Havel, den 23. November 2004

Gliederung

1. Die Entwicklung von OpenPGP
2. Funktionsweise:
 - Verwendete Algorithmen
 - Schlüsselerzeugung und -verwaltung
 - „Web-of-Trust“
3. Kompatibilität
4. Verfügbare Implementierungen und Links

Entwicklung von OpenPGP

- PGP steht für „Pretty Good Privacy“ und wurde 1991 von Phil Zimmermann, damals noch MIT-Student, „erfunden“
- Zimmermann wollte eine praktikable, einfach bedienbare Krypto-Infrastruktur schaffen, die an die anarchische Struktur des Internets anlehnt

Entwicklung von OpenPGP

- PGP erlaubt die Sicherstellung von Authentizität, Integrität und Vertraulichkeit von Daten – der Fokus liegt auf dem Schutz von E-Mail-Kommunikation
- PGP war Freeware mit offenem Quellcode und fand sehr schnell Verbreitung

Entwicklung von OpenPGP

- 1994 gründete Zimmermann die PGP Inc., die wurde 1997 von Network Associates Inc. aufgekauft
- NAI vertreibt bis heute PGP-Software
- die erste Standardisierung erfolgte 1996 mit RFC1991

Entwicklung von OpenPGP

- 1998 wurde die bis heute gültige Überarbeitung dieses Standards unter dem Titel „RFC2440: OpenPGP Message Format“ veröffentlicht
- RFC2440 ist abwärtskompatibel zu RFC1991

Algorithmen

- Publik-Key Chiffren
 - DSA (FIPS 186)
 - ElGamal (IEEE, 1985)
 - RSA (optional)

Algorithmen

- Symmetrische Chiffren
 - CAST5 (RFC 2144)
 - IDEA (patentiert, optional)
 - Blowfish (optional)
 - AES (optional)

Algorithmen

- Hash Algorithmen
 - SHA-1 (FIPS 180-1)
 - MD5 (optional)
- Komprimierung
 - ZLIB (RFC 1950)
 - ZIP (RFC 1951)

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

Schlüsselerzeugung

- 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

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

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 durch andere Teilnehmer, oder auch durch Trustcenter bzw. CAs geschehen, die mit ihrer Signatur für die Authentizität des Schlüsselmaterials bürgen

Web-of-Trust

- Unterschriften sind in verschiedenen Vertrau-
enklassen möglich:
 - kein kein Vertrauen
 - unbestimmtes Vertrauen
 - teilweises Vertrauen
 - vollständiges/ uneingeschränktes Vertrauen

Web-of-Trust

- 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

Kompatibilität

- PGP ist inkompatibel mit S/MIME (unterschiedliche Verfahren und Protokolle)
- PGP bietet einen größeren Funktionsumfang als S/MIME
- Web-of-Trust vs. Baum-Hierarchie
- leider muß für die Nutzung von PGP meist zusätzliche Software installiert werden

Software und Links

- verschiedene kommerzielle Implementierungen,
u.a. von NAI: <http://www.nai.com/>
- eine freie Implementierung,
GnuPG: <http://www.gnupg.org/>
- Dokumentation zu GnuPG:
<http://www.gnupg.org/gph/de/manual/>

Software und Links

- Kompatibilität zwischen S/MIME und OpenPGP bietet gpgsm:
<http://www.gnupg.org/aegypten/>
- DFN-Keyserver:
<http://www.pca.dfn.de/pgpkserver/>
- Plugins für diverse Mailsoftware finden sich meist auf den Webseiten des betreffenden Programms