INTEREST

Datenschutz PRAXIS

Datenschutz – rechtssicher, vollständig, dauerhaft.

Ausgabe Juli 2005 | 9 € zzgl. MwSt.

Kryptographie

So erzeugen Sie E-Mails mit noch mehr als sieben Siegeln

Das Sicherheitsniveau unverschlüsselter E-Mails entspricht dem einer mit Bleistift geschrieben Postkarte. Jeder kann sie lesen und verändern. Durch Verschlüsselung wird die E-Mail in einen virtuellen Umschlag gesteckt. Durch die digitale Signatur lassen sich dann Veränderungen erkennen. So sollte im Zeitalter von SPAM mit gefälschten Absenderadressen zumindest eine Signatur unabdingbar sein. Wir zeigen Ihnen, wie Sie kinderleicht sichere E-Mails erstellen.

Zwei Verfahren zur E-Mail-Verschlüsselung haben sich durchgesetzt: OpenPGP und S/Mime. Beide Verfahren sind bezüglich der Qualität der Verschlüsselung, und damit bezüglich der Sicherheit, absolut gleichwertig. S/Mime ist in gängige E-Mail-Programme wie MS Outlook (Express), Mozilla Thunderbird und Netscape Mail von Haus aus eingebaut. OpenPGP gibt es in zwei wesentlichen Implementierungen, als kommerzielles PGP von PGP Corporation und als freies Gnu Privacy Guard (GnuPG) von Werner Koch.

Voraussetzung für den Austausch verschlüsselter E-Mails ist die Verwendung des gleichen Standards bei beiden Kommunikationspartnern. Einzige Ausnahme ist das neue PGP 9. Es kann auch mit S/Mime-Mails umgehen. Ansonsten gilt, dass eine im OpenPGP-Format verschlüsselte E-Mail nicht mit einem S/Mime-Programm entschlüsselt werden kann.

So funktioniert Verschlüsselung

Seriöse E-Mail-Verschlüsselung basiert auf asymmetrischer Verschlüsselung. Das Besondere hierbei ist, dass jeder Teilnehmer ein Schlüsselpaar bestehend aus dem öffentlichen und dem privaten Schlüssel benötigt. Dieses Schlüsselpaar wird von der

Fortsetzung auf Seite 6

Inhalt

ISSN-Nr. 1614-6867

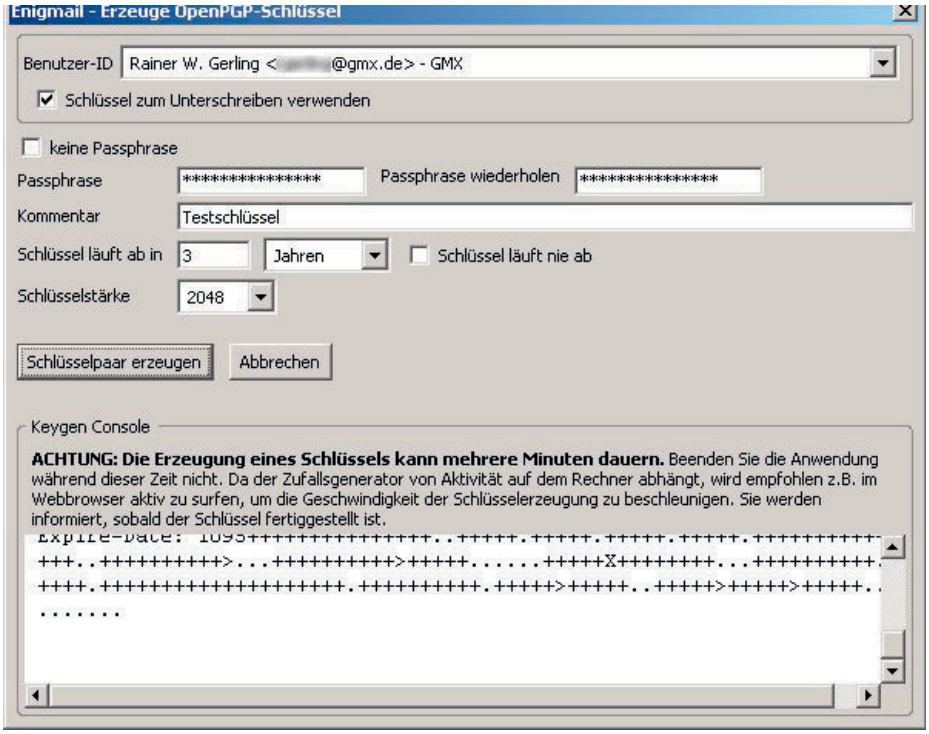

Abbildung 1: Der Schlüsselerzeugungsdialog in Enigmail.

Fortsetzung von Seite 1

Software aus Zufallszahlen generiert. Der Benutzer gibt dabei ein Passwort an, das den Zugriff auf den privaten Schlüssel schützt. Bei der Verwendung des privaten Schlüssels muss dieses Passwort immer eingegeben werden. Der öffentliche Schlüssel wird an alle Kommunikationspartner verteilt, der private Schlüssel ist geheim zu halten.

Zum Verschlüsseln wird der öffentliche Schlüssel des Empfängers benötigt, zum Signieren der eigene private Schlüssel. Hat man vom Empfänger keinen öffentlichen Schlüssel, kann man auch keine E-Mail an ihn verschlüsseln (Ausnahme: s. Notlösung).

Diese technischen Voraussetzungen müssen erfüllt sein

Traditionell benötigt man neben dem E-Mail-Programm ein Verschlüsselungsprogramm sowie ein so genanntes Plugin für das E-Mail-Programm. Dieses Plugin stellt die Verbindung zwischen dem E-Mail-Programm und der Verschlüsselungssoftware her. Für alle gängigen E-Mail-Programme gibt es Plugins. Nur das kommerzielle PGP unterstützte zu keinem Zeitpunkt Netscape Mail. Eine schöne und einfach zu bedienende Lösung ist Mozilla Thunderbird mit dem Plugin Enigmail und der freien Software GnuPG.

Die Schlüsselerzeugung

Zuerst muss ein Schlüsselpaar erzeugt werden. Dazu wird im Thunderbird unter Enigmail die OpenPGP-Schlüsselverwaltung aufgerufen. Über den Menüpunkt „Erzeugen“ – „Neues Schlüsselpaar“ erscheint ein Fenster wie in Abbildung 1. Die Benutzer-ID ist bereits aus der E-Mail-Konfiguration eingetragen. Das Passwort für den privaten Schlüssel wird zweimal eingegeben und die Gültigkeitsdauer auf drei Jahre reduziert. Nach einem Klick auf „Schlüsselpaar erzeugen“ kommt noch eine Sicherheitsabfrage, und dann wird der Schlüssel erzeugt.

Die Frage, ob ein Widerrufszertifikat erzeugt werden soll, wird mit Ja beantwortet. Dabei wird eine Datei „xxxxxxx@gmx.de (0x5146BBB5) rev.asc“ erzeugt, die das Widerrufszertifikat enthält. Bei der Erzeugung müssen Sie erstmals das Passwort für den privaten Schlüssel eingeben. Mit dieser Datei kann das Schlüsselpaar für ungültig erklärt werden, falls es keinen Zugang zum privaten Schlüssel mehr gibt. Diese Datei gehört auf eine CD-ROM gebrannt, die dann gut weggeschlossen werden muss.

So werden Schlüssel „unterschrieben“

In der Schlüsselverwaltung (Abb. 2) können Schlüssel importiert, auf

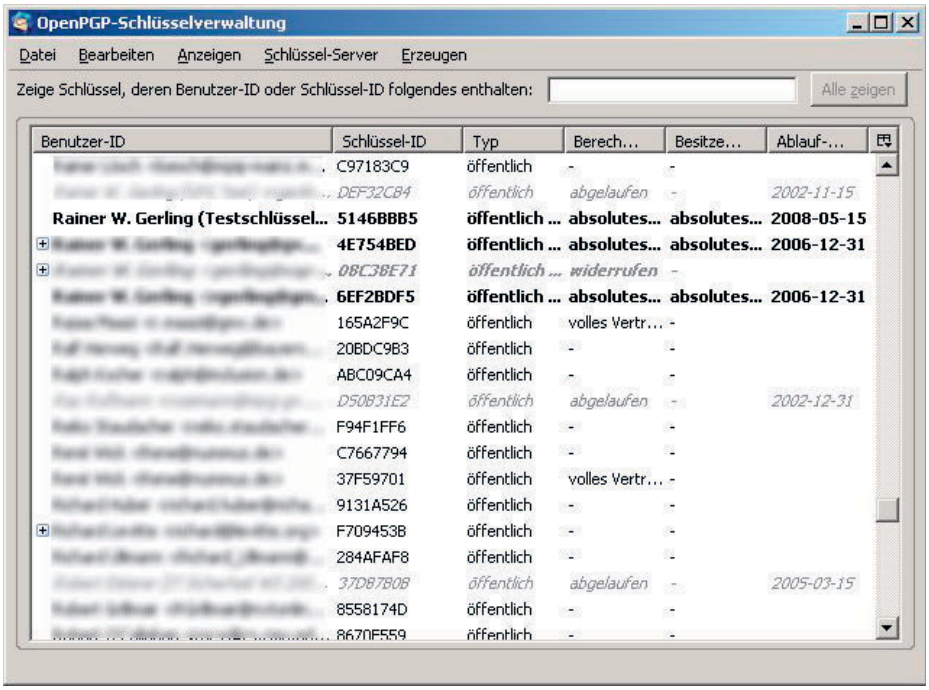

Abbildung 2: Die Schlüsselverwaltung in Enigmail.

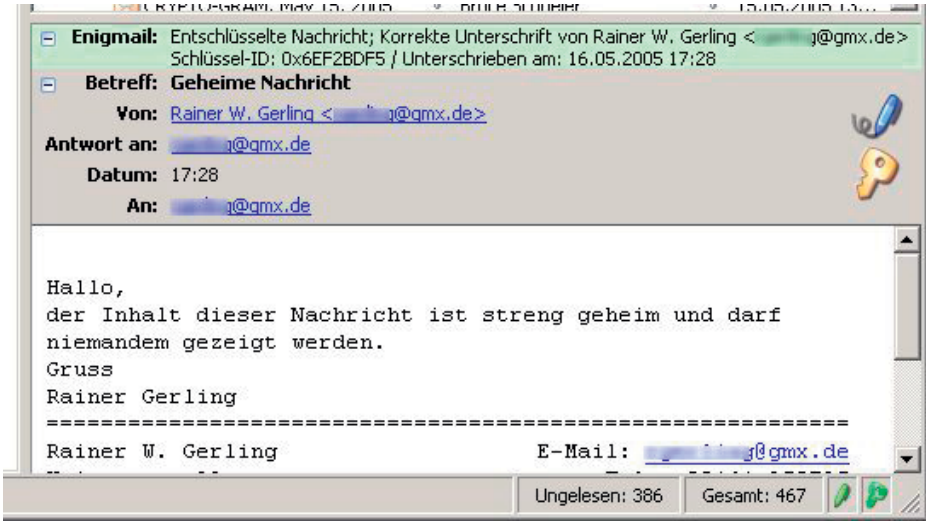

Abbildung 3: In Mozilla Thunderbird werden das Entschlüsseln und die geprüfte Signatur klar symbolisiert.

Schlüsselservern nach Schlüsseln gesucht werden u. dgl. mehr. Nur Schlüssel, die in der Schlüsselverwaltung vorhanden sind, können zur E-Mail-Verschlüsselung benutzt werden.

Ein wichtiger Akt ist das Gültigmachen von Schlüsseln. Dazu kontaktiert man den Besitzer des Schlüssels, überprüft den Fingerabdruck des Schlüssels (ist über „Schlüsseleigenschaften“ im Kontext-Menü abrufbar) und unterschreibt den Schlüssel dann.

Je nach Belieben können einzelne E-Mails dann verschlüsselt oder unverschlüsselt versendet werden

Auf Schlüsselservern kann über den Namen bzw. über die E-Mail-Adresse nach Schlüsseln gesucht werden. Wird ein Schlüssel per E-Mail zugeschickt, so kann er über die Zwischenablage importiert werden. Sobald einige öffentliche Schlüssel eingesammelt sind, können Sie mit der E-Mail-Verschlüsselung beginnen. Dazu wird beim Verfassen der E-Mail ausgewählt, ob verschlüsselt und/oder unterschrieben werden soll.

Die empfangenen E-Mails werden automatisch entschlüsselt. Wie in der Abbildung 3 ersichtlich, wird angezeigt, ob die E-Mail verschlüsselt war und ob die Signatur auch wirklich in Ordnung ist.

Probleme gibt es, wenn einer der Empfänger nicht entschlüsseln kann

Signierte E-Mails können auch von Personen gelesen werden, die nichts über Verschlüsselung wissen. Deshalb macht es Sinn, grundsätzlich alle E-Mails zu signieren. Signierte Dateianhänge können aber nur von Empfängern verarbeitet werden, die auch die entsprechende Verschlüsselungssoftware haben. Eine E-Mail gleichzeitig an zwei Empfänger zu schicken, einmal verschlüsselt, einmal unverschlüsselt, funktioniert nicht.

Prof. Dr. Rainer W. Gerling

Software zum Verschlüsseln

PGP Corporation:
http://www.pgp.com

GnuPG:
http://www.gnupg.org

GPGrelay:
http://sites.inka.de/tesla/gpgrelay.html

AXcrypt:
http://axcrypt.sourceforge.net

Utimaco:
http://www.utimaco.com/content_products/sg_pc.html

TugZip:
http://www.tugzip.de

Thunderbird:
http://www.thunderbird-mail.de

Notlösung für dringende Fälle

Wer ganz dringend einen verschlüsselten Text oder eine verschlüsselte Datei verschicken muss, kann sich behelfen. Viele Programme können eine Datei mit einem Passwort verschlüsseln. Das fängt bei Pack-Programmen für ZIP- oder RAR-Dateien an und hört bei Spezialprogrammen wie z.B. AXcrypt oder Utimaco Private Crypto auf. Eine solchermaßen verschlüsselte Datei kann wie jede andere Datei als E-Mail-Anhang verschickt werden. Insbesondere bei ZIP-Dateien kann man für das Entschlüsseln darauf vertrauen, dass der Empfänger die entsprechende Software hat. So kann Windows XP ohne Zusatzsoftware verschlüsselte ZIP-Dateien entschlüsseln. Nachteil der ZIP-Daten: die Verschlüsselung gilt nicht als besonders sicher.

Eine schlechte Idee ist es, selbstextrahierende verschlüsselte Dateien zu erzeugen, da ausführbare Dateien aus Sicherheitsgründen auf vielen Mail-Servern geblockt werden. Ansonsten liefern sie das Entschlüsselungsprogramm für ein Betriebssystem (in der Regel Windows) gleich mit. Das Passwort der verschlüsselten Datei sollte auch nicht in den Text der E-Mail geschrieben werden. Hier bietet sich ein kurzes Telefonat zum Durchgeben des Passworts an.

Fazit: Als Notlösung ist diese Methode durchaus geeignet. Für regelmäßige verschlüsselte Kommunikation sollte aber S/Mime oder PGP benutzt werden.