GPG4win: Verschlüsseln unter Windows

Ihr Schlüssel zur Sicherheit

Die Verschlüsselungstechnologie GPG4win soll für jedermann kostenlos die Sicherheit im E-Mail-Verkehr, bei E-Commerce und E-Government ermöglichen. Wir erklären Installation und Bedienung und geben Ihnen wertvolle Tipps – damit Sie Ihre Schlüssel nicht verlieren ...

Vor einigen Jahren wurde das GNU Privacy Projekt (GNU PP) vorgestellt. Es wurde durch das Bundesministerium für Wirtschaft und Arbeit gefördert. Das Projekt schlief damals ein. Ein neues Projekt, das in die Fußstapfen von GnuPP tritt, ist GPG4win.

Die Installation ist nur mit Administrator-Rechten möglich

GPG4win stellt für den Windows-Benutzer ein Komplettpaket zusammen, das dank grafischer Oberfläche einfach installiert werden kann. Dabei benötigen Sie allerdings Administrator-Rechte, da die Software im Programm-Verzeichnis installiert wird. Außerdem schreibt das Installationsprogramm in den Zweig HKEY_LOCAL_MACHINE der Registry, was nur dem Administrator erlaubt ist. Dann kann jeder Nutzer die Software anwenden.

Beim ersten Start müssen Sie die Schlüssel generieren

Beim ersten Start stellt das Programm fest, dass der Anwender noch kein Schlüsselpaar besitzt, und fordert ihn auf, entweder einen Schlüssel zu generieren oder ein bereits vorhandenes Schlüsselpaar zu installieren. Im Fall der Schlüsselgenerierung führt ein Assistent durch den Prozess.

Linktipps

http://www.gpg4win.de

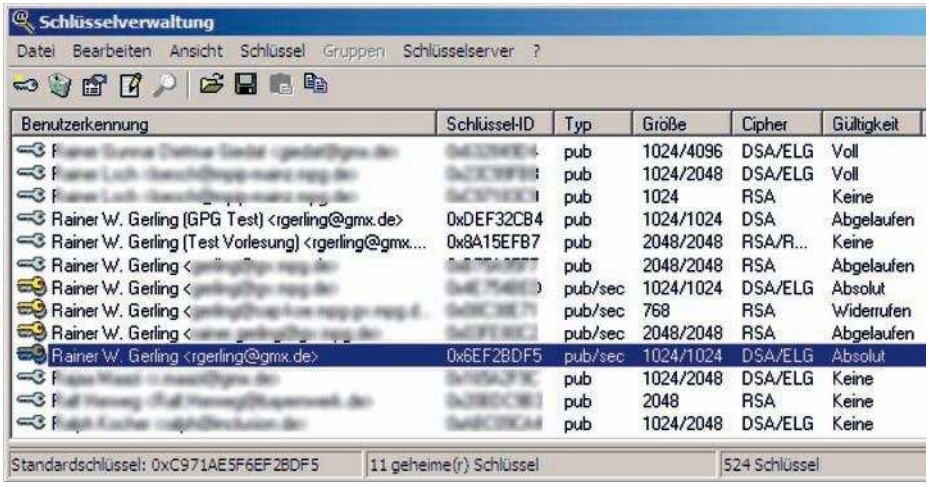
http://www.gnupg.de

Wenn Sie den Eindruck haben, dass Ihr Rechner hängt, wenn das Fenster „Schlüsselerzeugung – Fortschrittsdialog“ angezeigt wird, so müssen Sie den Mauszeiger heftig bewegen. Aus den Mauszeiger-Positionen werden nämlich Zufallszahlen generiert, die zur Schlüsselerzeugung benötigt werden.

Ist das Passwort verloren, lassen sich die Daten nicht mehr entschlüsseln

Der anschließenden Aufforderung, ein Backup des Schlüssels zu erstellen, sollten Sie nachkommen. Bewahren Sie die Sicherungskopie zusammen mit dem notierten Passwort des Schlüssels an einem sicheren Ort auf. Wenn Sie das Passwort des Schlüssels vergessen, können die verschlüsselten Dateien nicht mehr entschlüsselt werden.

Es ist auch sinnvoll, für alle Fälle ein Widerrufszertifikat für den eigenen privaten Schlüssel zu erzeugen.



Die Oberfläche zur Schlüsselverwaltung aus der Komponente WinPT.

Die Komponenten der Software

Die Software besteht aus folgenden Komponenten:

GnuPG: GNU Privacy Guard, die eigentliche Verschlüsselungssoftware. Diese Komponente ist unverzichtbar. Sie wird nur in der englischsprachigen Version installiert. Mit diesem Tool kommen Sie nur selten in Berührung.

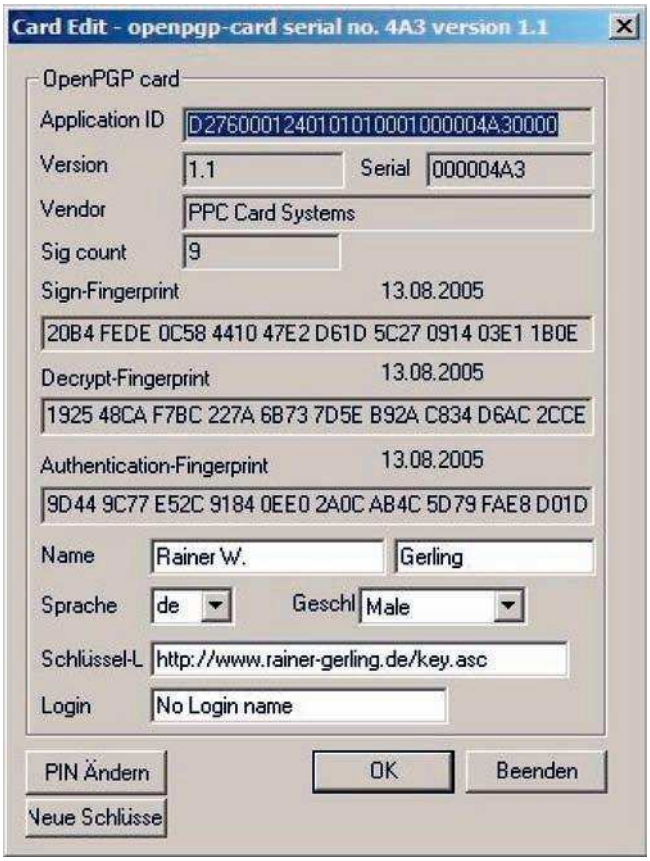
Mit dem GnuPG gibt es schon länger eine OpenPGP-Implementierung, die kostenfrei eingesetzt werden kann. Wesentlicher Entwickler und Vater der Software ist Werner Koch. GnuPG steht unter der GPL und ist kompatibel zur kommerziellen OpenPGP-Version der Firma PGP Corporation.

WinPT: Der Windows Privacy Tray des Informatikstudenten Timo Schulz ist die Komponente zum Starten der Schlüsselmanagement-Oberfläche und zum Ausführen von Verschlüsselungsoperationen für das aktuelle Fenster und die Zwischenablage. Über dieses Programm werden auch die Hotkeys verwaltet. Die Oberfläche der Software ist in Deutsch.

GPA: Der GNU Privacy Assistant ist eine alternative Software zu WinPT. Sie benötigen immer nur eines der beiden Tools. Da die Oberfläche vom GPA aufgrund seiner Herkunft Linux nachempfunden ist, ist die Bedienung gewöhnungsbedürftig.

Es empfiehlt sich, auf den GPA zu verzichten und nur WinPT zu installieren.

GPGol: ist das GnuPG Plugin für Outlook. Damit können Sie E-Mails



Da GnuPG in der aktuellen Version OpenPGP-Chipkarten unterstützt, können die privaten Schlüssel in einer Chipkarte gespeichert werden. WinPT bietet die Oberfläche zum Verwalten der Chipkarten.

ver- und entschlüsseln. Es funktioniert jedoch wegen interner Besonderheiten von Outlook nur ab Outlook 2003 Service Pack 2. Ältere Versionen von Outlook werden nicht unterstützt.

Werner Koch hat sich des ursprünglich von G-Data veröffentlichten Plugins angenommen und es von Grund auf neu geschrieben. Abweichend von der Beschreibung im Handbuch (GPG-4win für Durchblicker, Seite 45) werden auch Attachments verschlüsselt.

GPGee: integriert sich in den Windows Explorer und erstellt dort ein Menü zum Ver-/Entschlüsseln von Verzeichnissen und Dateien.

Sylpheed-Claws: Ein E-Mail-Programm, das in dem Paket eigentlich nichts verloren hat. Die Voreinstellung sieht vor, es nicht zu installieren – also ändern Sie die Voreinstellung nicht!

Handbücher: GPG-4win für Einsteiger und GPGwin für Durchblicker sind zwei deutschsprachige Handbücher, die den Umgang mit GPG4win und allgemeine Grundlagen der Verschlüsselung erklären. Sie basieren auf den Handbüchern des GnuPP.

Leider beschreiben sie nur die Verwendung von GPA und rudimentär von GP-Gee und gehen auf WinPT nicht näher ein. Die Handbücher enthalten die netten Illustrationen der GnuPP-Ausgabe.

Die Light-Version lohnt sich nicht

GPG4win light ist eine abgespeckte Ausgabe von GPG4win. Leider fehlen gerade wichtige Komponenten. Zugunsten von GPA und Sylpheed-Claws wurde auf die Handbücher verzichtet.

Also sparen Sie sich die Mühe, die Light-Version zu installieren!

Fazit: Ein wichtiger Schritt ist getan, das Ziel ist aber noch nicht erreicht

GPG4win ist die längst überfällige Fortsetzung von GnuPP. Es wäre sinnvoll, den GPA und das E-Mail-Programm Sylpheed-Claws wegzulassen und dafür das Outlook Express Plugin GPGOE aufzunehmen.

Darüber hinaus bedürfen die Handbücher der Überarbeitung und müssen zumindest um eine Beschreibung von WinPT ergänzt werden.

Prof. Dr. Rainer W. Gerling