Wie erstelle ich meinen eigenen PGP-Schlüssel?

Wichtigste Voraussetzung: Erstellen Sie Ihren PGP-Key nur auf einem vertrauenswürdigen Rechner mit aktuellem Anti-Malware-Programm. Beachten Sie dazu unsere Tipps auf dem Marktplatz IT-Sicherheit:
http://www.it-sicherheit.de/ratgeber/it_sicherheitstipps/basisschutz_fuer_ihren_pc/

Besuchen Sie zunächst die Seite http://www.gpg4win.de/ und laden sich dort das Paket Gpg4win 2.2.1 (oder höher) herunter. Achten Sie darauf, die Adresse richtig einzugeben und laden Sie Dateien nur von vertrauenswürdigen Webseiten herunter.
Gpg4win (Gnu Privacy Guard for Windows) ist eine OpenSource-Lösung zur Verwendung der PGP-Verschlüsselung. Es ist daher kostenlos erhältlich. Führen Sie die Datei aus. Das Paket enthält folgende Komponenten, die Sie wahlweise installieren können:

GnuPG
ist das Kernstück von Gpg4win – die eigentliche Verschlüsselungs-Software – und daher absolut notwendig.

Kleopatra
Die zentrale Zertifikatsverwaltung von Gpg4win, die für eine einheitliche Benutzerführung bei allen kryptografischen Operationen sorgt. Installation empfohlen.

GNU Privacy Assistent (GPA)
ist ein alternatives Programm zum Verwalten von Zertifikaten neben Kleopatra und nicht notwendig, wenn Sie Kleopatra installieren

GnuPG für Outlook (GpgOL)
ist eine Erweiterung für Microsoft Outlook 2003 und 2007, die verwendet wird, um Nachrichten zu signieren bzw. zu verschlüsseln. Empfehlenswert, wenn Sie diese Outlook-Versionen verwenden.

GPG Explorer Extension (GpgEX)
ist eine Erweiterung für den Windows-Explorer, mit der man Dateien über das Kontextmenü signieren bzw. verschlüsseln kann. Empfehlenswert, wenn Sie Dateien auf Ihrer Festplatte verschlüsseln wollen.

Claws Mail
ist ein vollständiges E-Mail-Programm mit sehr guter Unterstützung für GnuPG. Nicht zwingend notwendig, wenn Sie einen anderen E-Mail-Client verwenden, der ebenfalls

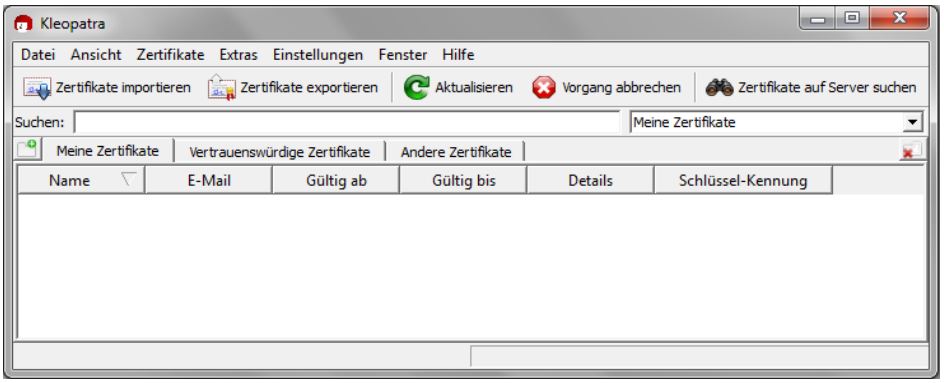
OpenPGP unterstützt. Beispiele hierfür sind Thunderbird, Outlook (nur 32bit-Versionen) oder Eudora.

Gpg4win-Kompendium
ist eine ausführliche Anleitung für Gpg4win mit Hintergrundinformationen und empfehlenswert.

Danach können Sie den gewünschten Installationspfad auswählen, Verknüpfungen und Startmenü-Ordner bestimmen und Gpg4win installieren. Gegebenenfalls müssen Sie Windows nach der Installation neu starten, was Sie auch umgehend tun sollten.

Nun, da Sie alle notwendigen Programme installiert haben, können Sie ein Schlüsselpaar erzeugen – also einen geheimen und einen öffentlichen Schlüssel. Das Schlüsselpaar ist ihre Eintrittskarte zur PGP-Verschlüsselung.

Öffnen Sie dazu das Programm Kleopatra, das Sie gerade installiert haben sollten. Normalerweise sollte sich eine Verknüpfung im Startmenü im Ordner „Gpg4win“ befinden, sofern sie nicht bei der Installation einen anderen Ort angegeben haben.



Das Hauptfenster ist zunächst noch leer. Um ein neues Schlüsselpaar zu erzeugen, klicken Sie auf Datei -> Neues Zertifikat.

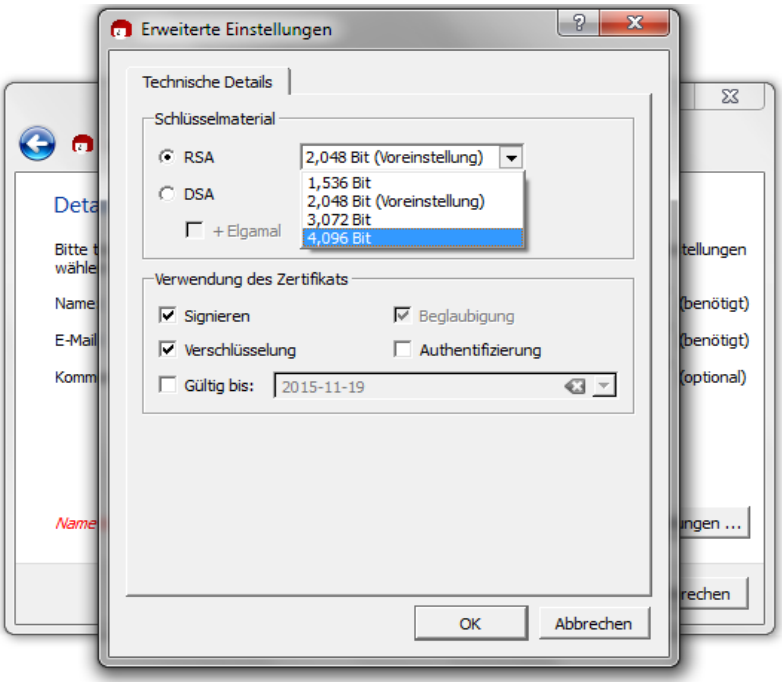
Im nun erscheinenden Fenster wählen Sie „Persönliches OpenPGP-Schlüsselpaar erzeugen“ aus.

Nun geben Sie Ihre E-Mail-Adresse und Ihren Namen ein. Bitte achten Sie darauf, dass Name und E-Mail-Adresse auch wirklich richtig sind und zueinander passen.
Das Feld „Kommentar“ können Sie leer lassen.

Um sicher zu gehen, dass sie auch den besten Schutz haben, klicken Sie auf das Feld „Erweiterte Einstellungen“. Dort sollte als Schlüsselmaterial „RSA“ ausgewählt sein. Bitte

E-Mail: information@internet-sicherheit.de
Internet: www.internet-sicherheit.de

ändern Sie die Einstellung der Schlüssellänge auf 4.096 Bit, um einen größtmöglichen Schutz zu gewährleisten.



Klicken Sie nun auf Okay und im anderen Fenster auf Weiter.

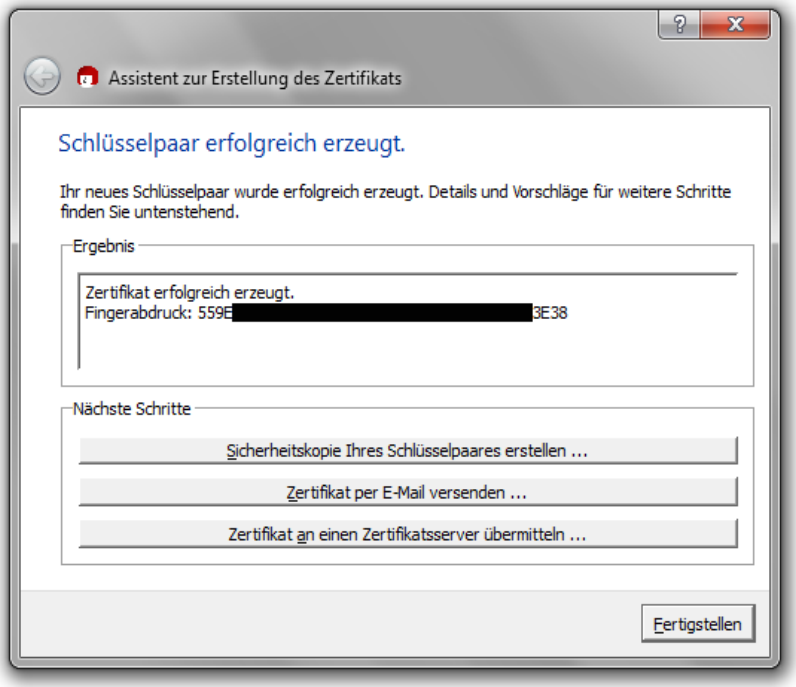
Nun können Sie Ihre Angaben noch einmal kontrollieren. Wenn Sie etwas ändern wollen, klicken Sie auf zurück. Ist alles in Ordnung, klicken Sie auf „Schlüssel erzeugen“.

Nun folgt der wichtigste Teil: Die Eingabe der Passphrase.
Dies ist Ihr Passwort, mit dem Sie zukünftig auf verschlüsselte Inhalte zugreifen können. Natürlich sollte dieses Passwort sehr sicher sein, und Sie müssen es sich sehr gut merken können. Wie Sie ein sicheres Passwort erstellen, erfahren Sie in unserer Checkliste auf: http://www.it-sicherheit.de/ratgeber/checklisten_it_sicherheit/checkliste/checkliste-verwende-ich-sichere-passwoerter/
Wenn Sie ein sicheres Passwort gewählt haben, müssen Sie dies zweimal eingeben und dann auf „OK“ klicken.

Ihr Schlüssel wird nun generiert. Dies kann je nach Rechner einige Minuten dauern. Um den Vorgang zu beschleunigen, können Sie beliebige Zahlen, Buchstaben oder Wörter eingeben. Keine Sorge, nichts davon wird öffentlich gemacht oder findet sich im Schlüssel wieder. Die Mausbewegungen und der zeitliche Abstand zwischen Ihrem Tastendrücken wird genutzt, um Zufallswerte zu erzeugen, die Ihren Schlüssel sicher machen und die Generierung unterstützen.

E-Mail: information@internet-sicherheit.de
Internet: www.internet-sicherheit.de

Nachdem Ihr Schlüssel erfolgreich erzeugt wurde, erscheint ein Dialogfenster. Diesen Fingerabdruck sollten Sie sich notieren. Sie können ihn auch jederzeit in Kleopatra abrufen. Mit dem Fingerabdruck kann jeder Schlüssel einwandfrei identifiziert werden. Wenn Zweifel bestehen, ob ein Schlüssel auch zur richtigen Person gehört, kann der richtige Fingerabdruck diese sofort ausräumen. Genau wie bei Menschen.



Sie haben nun drei Möglichkeiten:

1. Eine Sicherheitskopie Ihres Schlüssels erstellen.
   Klicken Sie dazu auf entsprechende Schaltfläche. Eine Datei, die Ihren vollständigen Schlüssel erhält, kann nun an einem beliebigen Ort abgelegt werden. WICHTIG: Achten Sie darauf, dass der Speicherort vor fremden Zugriffen geschützt ist! Das kann ein Rechner sein, der nicht mit dem Internet verbunden ist, oder ein externes Speichmedium wie z.B. ein USB-Stick oder eine DVD. In jedem Fall sollte die Sicherheitskopie nur in einem verschlüsselten Ordner abgelegt werden.

2. Zertifikat per E-Mail versenden
   Hiermit können Ihren öffentlichen Schlüssel als Anhang einer E-Mail versenden, etwa damit ein Freund seine Gültigkeit bestätigen kann.

E-Mail: information@internet-sicherheit.de
Internet: www.internet-sicherheit.de

3. Zertifikat zu Zertifikatserver senden
   Damit können Sie Ihren öffentlichen Schlüssel auf einem Keyserver veröffentlichen, damit andere PGP-Nutzer Ihnen verschlüsselte E-Mails senden können. Dazu später mehr.

Damit ist die Schlüsselerstellung vorerst abgeschlossen. Ihr neuer Schlüssel sollte nun im Hauptfenster von Kleopatra angezeigt werden. Bei einem Doppelklick auf Ihren Schlüssel können Sie nun alle Details Ihres Schlüssels sehen und ggf. Änderungen vornehmen. Nun sollten Sie Ihren öffentlichen Schlüssel auch veröffentlichen, damit andere Nutzer Ihnen verschlüsselte E-Mails senden können. Beachten Sie jedoch, dass ein einmal veröffentlichter Schlüssel nicht mehr zurückgezogen werden kann! Sie können Ihren Schlüssel jedoch zu jeder Zeit widerrufen und somit als ungültig erklären, etwa dann, wenn Sie einen neuen Schlüssel verwenden wollen und den alten nicht mehr benötigen. Zur Veröffentlichung folgen Sie am besten den Anweisungen von Kleopatra nach dem Punkt „Zertifikat zu Zertifikatserver senden“. Sie können Ihren Schlüssel auch an anderen vertrauensvollen Stellen veröffentlichen, wie natürlich der PGP-Zertifizierungsinstanz des Instituts für Internet-Sicherheit (http://www.internet-sicherheit.de/pgpzi/), aber auch bei anderen Anbietern, wie z.B. Heise (http://www.heise.de/security/dienste/Krypto-Kampagne-2111.html).

Sobald Sie Ihren eigenen Schlüssel nun erstellt und veröffentlicht haben, können Sie auch schon fast loslegen. Die meisten E-Mail-Clients unterstützen die PGP-Verschlüsselung mittels Plugins. Bei Thunderbird heißt das notwendige Plugin „Enigmail“ und kann bequem direkt über den Menüpunkt Add-ons gefunden und installiert werden.
Das Plugin für Outlook heißt GpgOL und kann bei der Installation von Gpg4win direkt mit installiert werden (s.o.).
Für Hilfe bei der Installation und Benutzung der Plugins stehen Ihnen im Internet zahlreiche Anleitungen zur Verfügung, etwa die Anleitung zur Installation von Enigmail bei Thunderbird des if(is). https://www.internet-sicherheit.de/pgpzi/

E-Mail: information@internet-sicherheit.de
Internet: www.internet-sicherheit.de