

Gpg4win 3.0 unterstützt ECC und Anhänge in Outlook

Gpg4win, die Freie E-Mail- und Datei-Verschlüsselungslösung für Windows, ist am 20. September nach knapp 2-jähriger Entwicklungszeit in Version 3.0 erschienen. Das Installationspaket kann auf <https://gpg4win.de> heruntergeladen werden. Nutzer können den Preis selbst bestimmen.

Outlook-Plugin mit MIME-Unterstützung

Gpg4win bringt ein überarbeitetes Plugin für Outlook ab Version 2010 mit, welches nun eine vollständige Unterstützung für MIME-E-Mails bietet.

Neue Kryptoverfahren mit elliptischen Kurven

Gpg4win hat das neue Kryptobackend GnuPG 2.2 integriert. Dadurch werden erstmals Kryptoverfahren mit elliptischen Kurven (ECC) für OpenPGP angeboten. Die Voreinstellung für neue Schlüssel ist noch RSA, weil alle Kommunikationspartner zunächst Software brauchen, die damit kompatibel ist.

Updatebenachrichtigung und leichtes Schlüsselfinden

Gpg4win prüft nun in der Standardeinstellung, ob neue Gpg4win-Versionen verfügbar sind. Somit können sich Nutzer zeitnah für eine Aktualisierung entscheiden. Weiterhin gibt die neue Version einen Ausblick darauf, wie sich das Finden öffentlichen Schlüssel der Kommunikationspartner in der Zukunft leichter wird: Sofern der Mailprovider des Empfängers das neue Web-Key-Directory-Verfahren anbietet, wird der richtige öffentliche Schlüssel automatisch heruntergeladen.

Beauftragungen durch das BSI

Viele der Verbesserungen in Gpg4win 3.0 wurden in den letzten 2 Jahren im Rahmen von drei Beauftragungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) umgesetzt. Federführend in der Umsetzung waren die deutschen Unternehmen Intevation und g10Code. Details zu den Aufträgen unter <https://wiki.gnupg.org/Gpg4win>.

Was ist Gpg4win?

Gpg4win (GNU Privacy Guard for Windows) ist ein Kryptografie-Paket für Windows. Das Software-Produkt ist Freie Software und wurde 2005 vom BSI erstmals in Auftrag gegeben. Mit Gpg4win lassen sich E-Mails und Dateien ver- und entschlüsseln, sowie ihre Integrität (Unverändertheit) und Herkunft (Authentizität) mittels digitaler Signaturen absichern. Die Software unterstützt die beiden relevanten kryptografischen Standards OpenPGP und S/MIME.

Gpg4win ist die offizielle GnuPG-Distribution für Windows und wird von den GnuPG-Entwicklern gepflegt und weiterentwickelt. Professioneller Support und Entwicklungsdienstleistungen zu Gpg4win werden u. a. durch die deutschen Unternehmen Intevation und g10Code angeboten.

Gpg4win 3.0: Die wichtigsten Neuerungen

- x Unterstützung von Elliptic Curve Cryptography (ECC) durch GnuPG 2.2.
- x Das Outlook-Plugin GpgOL wurde komplett überarbeitet (ab Outlook 2010):
 - o Vollständige Unterstützung für OpenPGP/MIME.
 - o Neues Benutzerinterface zur Ver- und Entschlüsselung, neue Anzeige des Crypto-Status im Mailfenster.
 - o Automatische Entschlüsselung von E-Mails (ohne störendes Popup).
 - o Unterstützung zum Senden und Empfangen von HTML Mails.
- x Vereinfachte Krypto-Nutzererfahrung durch automatischen Abruf von fehlenden öffentlichen OpenPGP-Schlüsseln (aus dem „Web Key Directory“ der Mailprovider). Neuer Standard mit GnuPG 2.2. Details siehe <https://wiki.gnupg.org/WKD>.
- x Verbesserte Zertifikats- und Schlüsselverwaltung mit Kleopatra:
 - o Dateiverschlüsselung mit dem Explorer-Plugin GpgEX optimiert (Reduzierung der nötigen Klicks auf ein Minimum).
 - o Kleopatra erkennt nun automatisch, um welchen Dateityp es sich handelt und startet bei Doppelklick die entsprechende Aktion (z.B. Entschlüsseln).
 - o Symmetrische Verschlüsselung (nur mit Passwort) nun auch über Kleopatra möglich.
 - o Neue Benutzeroberfläche zum Verwalten von Smartcards.
 - o Portierung auf KDE Frameworks 5 (deutliche Reduzierung der KDE-Abhängigkeiten, von 68 auf 18 Pakete).
 - o Verwendung des neuen KDE-Icon-Themes „Breeze“.
- x Verschiedenes
 - o Neue Benachrichtigung für verfügbare Gpg4win-Updates.
 - o Vereinfachter Gpg4win-Installationsprozess. Installation nun auch möglich für normale Nutzer ohne Administrator-Rechte.
 - o Pinentry erlaubt, die eingegebene Passphrase anzuzeigen.
 - o Voreingestellter OpenPGP-Schlüsselservers.
 - o Die Deutsche Fassung des Gpg4win-Kompendiums wurde vollständig für Version 3.0 überarbeitet.

Mehr Details auf der Gpg4win-Website, u.a. unter [Änderungshistorie](#), [Screenshots](#) und [Version 3](#).

Ansprechpartner:

Emanuel Schütze

Intevation GmbH | Neuer Graben 17 | 49074 Osnabrück

E-Mail: emanuel.schuetze@intevation.de | Telefon: 0541 335083-746