LU06x - gpg4usb

Diese Anleitung ist in der Überarbeitung da gpg4usb nicht mehr weiterentwickelt wird, verwenden Sie gpg4Win und versuchen Sie die Aufgabe damit.

GnuPG und PGP

PGP ist das Akronym für **P**retty **G**ood **P**rivacy, einem kommerziellen Programm zum Verschlüsseln und Signieren von Daten. Das Programm verschlüsselt die Daten mit einem symmetrischen Verfahren. Der dabei verwendete Schlüssel wird mittels Public Key-Verfahren (asymmetrisch) verschlüsselt. Dies wird als hybride Verschlüsselung bezeichnet.

GnuPG oder GPG steht für **G**NU **P**rivacy **G**uard. Im Gegensatz zu PGP verwendet GnuPG nur patentfreie Algorithmen zur Verschlüsselung und wird als OpenSource-Software vertrieben. Die Arbeitsweise und Funktionen von GnuPG sind vergleichbar mit PGP.

gpg4usb

gpg4usb ist ein einfaches, portables Programm, um Informationen zu verschlüsseln und entschlüsseln. Sie können das Programm herunterladen, entpacken und direkt loslegen. Eine Installation ist nicht notwendig.

Wir wollen das Verschlüsseln und Signieren mit gpg4usb direkt ausprobieren. Suchen Sie sich dazu einen Partner, mit dem Sie die Daten austauschen können. Dieser Austausch kann per E-Mail oder über einen USB-Stick erfolgen.

Vorgehen

1. Schlüsselpaar erzeugen.
2. Eigenen Public-Key exportieren.
3. Public-Key des Partners importieren.
4. Datei verschlüsseln.
5. Datei entschlüsseln.
6. Datei signieren.
7. Signatur prüfen.

Schlüsselpaar erzeugen

Bevor Sie Dateien verschlüsseln können, müssen Sie ein persönliches Schlüsselpaar

- Private Key: Geheim, nur Ihnen bekannt.
- Public Key: Öffentlich

anlegen.

Die Sicherheit des Verfahrens hängt stark von Ihrem Passwort ab. Verwenden Sie daher für den Schlüssel ein starkes Passwort oder noch besser einen kurzen Satz.

https://www.gpg4usb.org/docu_keygen.html

Eigenen Public-Key exportieren

Ihr Partner benötigt Ihren Public-Key zum Verschlüsseln und Verifizieren Ihren Signatur. Exportieren Sie dazu Ihren Public-Key in eine Datei und geben diese an Ihren Partner.

https://www.gpg4usb.org/docu_export_key.html

Public-Key des Partners importieren.

Nachdem Sie den Public-Key Ihres Partners erhalten haben, importieren Sie diesen.

https://www.gpg4usb.org/docu_import_key.html

Text verschlüsseln

Schreiben Sie einen beliebigen Text direkt in gpg4usb und verschlüsseln Sie diesen mit dem Public-Key Ihres Partners. Geben Sie die verschlüsselte Datei an Ihren Partner weiter.

https://www.gpg4usb.org/docu_encrypt.html

Datei entschlüsseln

Laden Sie die verschlüsselte Datei Ihres Partners und entschlüsseln Sie den Text.

https://www.gpg4usb.org/docu_decrypt.html

Text signieren

Schreiben Sie einen beliebigen Text direkt in gpg4usb und signieren Sie diesen mit Ihrem Private-Key. Geben Sie die signierte Datei an Ihren Partner weiter.

https://www.gpg4usb.org/docu_sign.html

Signatur prüfen

Laden Sie die signierte Datei und prüfen Sie die Unterschrift.

https://www.gpg4usb.org/docu_verify.html

---

m114-A0G