GnuPG

Verschlüsselte Kommunikation

Beni Buess

Swiss Privacy Foundation

SWISS PRIVACY FOUNDATION

SWISS PRIVACY FOUNDATION

Inhaltsverzeichnis

SWISS PRIVACY FOUNDATION

Inhaltsverzeichnis

SWISS PRIVACY FOUNDATION

Inhaltsverzeichnis

SWISS PRIVACY FOUNDATION

Inhaltsverzeichnis

SWISS PRIVACY FOUNDATION

Übersicht

SWISS PRIVACY FOUNDATION

Mails im Klartext

Emails sind auf den Mailservern im Klartext einsehbar!

Merke:

Daran ändert sich auch nichts, wenn die Kommunikation mit dem Mailserver mit SSL verschlüsselt wird.

SWISS PRIVACY FOUNDATION

Mails im Klartext

Emails sind auf den Mailservern im Klartext einsehbar!

Merke:

Daran ändert sich auch nichts, wenn die Kommunikation mit dem Mailserver mit SSL verschlüsselt wird.

SWISS PRIVACY FOUNDATION

Nichts zu verbergen?

- Wir entscheiden selber, wer unsere Nachrichten lesen kann.
- Durch die Signatur kann der Absender verifiziert werden.

?

Aus welchem Grund wollt ihr verschlüsseln?

SWISS PRIVACY FOUNDATION

Nichts zu verbergen?

- Wir entscheiden selber, wer unsere Nachrichten lesen kann.
- Durch die Signatur kann der Absender verifiziert werden.

?

Aus welchem Grund wollt ihr verschlüsseln?

SWISS PRIVACY FOUNDATION

Nichts zu verbergen?

- Wir entscheiden selber, wer unsere Nachrichten lesen kann.
- Durch die Signatur kann der Absender verifiziert werden.

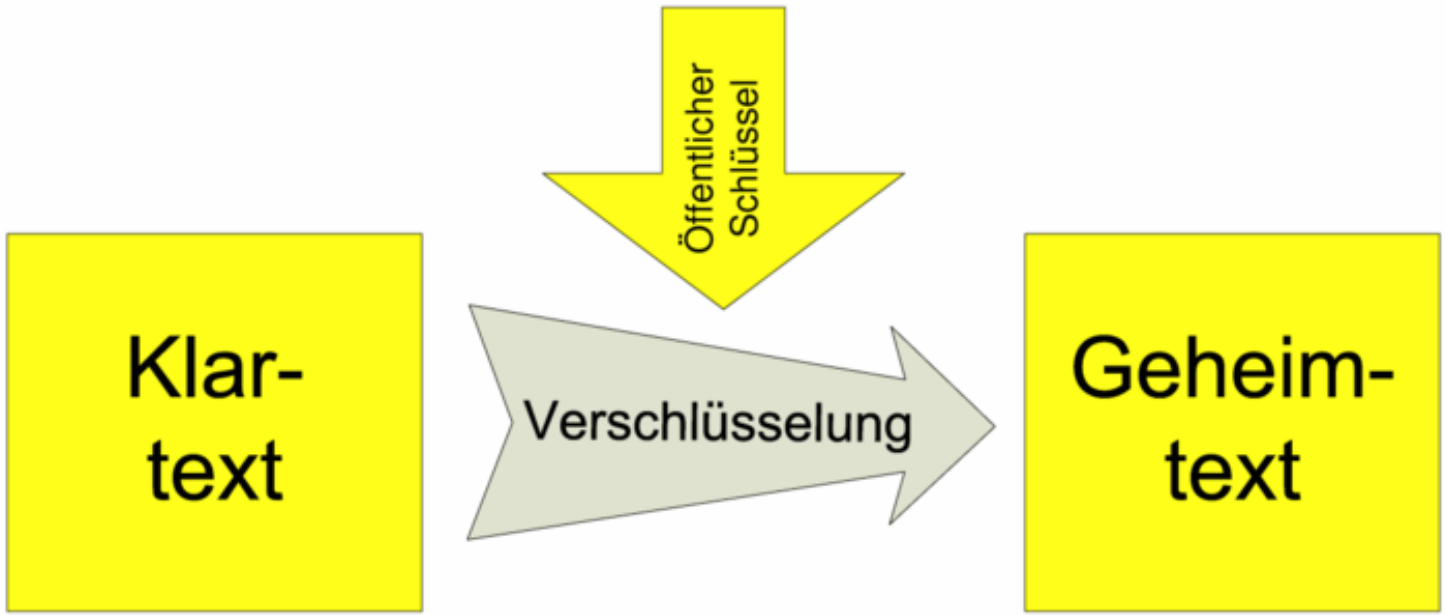
?

Aus welchem Grund wollt ihr verschlüsseln?

SWISS PRIVACY FOUNDATION

Übersicht

Asymmetrische Verschlüsselung



GnuPG

- Asymmetrische Verschlüsselung (Public-/Private-Key)
- Erweiterungen für alle gängigen Mailclients
- Erweiterungen für Texteditoren

SWISS PRIVACY FOUNDATION

Übersicht

SWISS PRIVACY FOUNDATION

GnuPG installieren Linux

Kommandozeile:

sudo apt-get install gnupg

SWISS PRIVACY FOUNDATION

GnuPG installieren OSX

macgpg

Unter `http://macgpg.sourceforge.net/de/#files` die passende Version von *GNU Privacy Guard* auswählen.

- Doppelklick auf GnuPG1.*.dmg
- GPL akzeptieren
- Doppelklick auf GnuPG for Mac OS X 1.*.mpkg

Merke:

Lass die MacGPG Seite offen. Du brauchst sie wieder.

Merke:

Unter `http://www.web-blog.net/comments/P171_0_1_0/` gibts eine gute Anleitung.

SWISS PRIVACY FOUNDATION

GnuPG installieren OSX

macgpg

Unter `http://macgpg.sourceforge.net/de/#files` die passende Version von *GNU Privacy Guard* auswählen.

- Doppelklick auf GnuPG1.*.dmg
- GPL akzeptieren
- Doppelklick auf GnuPG for Mac OS X 1.*.mpkg

Merke:

Lass die MacGPG Seite offen. Du brauchst sie wieder.

Merke:

Unter `http://www.web-blog.net/comments/P171_0_1_0/` gibts eine gute Anleitung.

SWISS PRIVACY FOUNDATION

GnuPG installieren OSX

macgpg

Unter `http://macgpg.sourceforge.net/de/#files` die passende Version von *GNU Privacy Guard* auswählen.

- Doppelklick auf GnuPG1.*.dmg
- GPL akzeptieren
- Doppelklick auf GnuPG for Mac OS X 1.*.mpkg

Merke:

Lass die MacGPG Seite offen. Du brauchst sie wieder.

Merke:

Unter `http://www.web-blog.net/comments/P171_0_1_0/` gibts eine gute Anleitung.

SWISS PRIVACY FOUNDATION

GnuPG installieren OSX

macgpg

Unter `http://macgpg.sourceforge.net/de/#files` die passende Version von *GNU Privacy Guard* auswählen.

- Doppelklick auf GnuPG1.*.dmg
- GPL akzeptieren
- Doppelklick auf GnuPG for Mac OS X 1.*.mpkg

Merke:

Lass die MacGPG Seite offen. Du brauchst sie wieder.

Merke:

Unter `http://www.web-blog.net/comments/P171_0_1_0/` gibts eine gute Anleitung.

SWISS PRIVACY FOUNDATION

GnuPG installieren Windows

GnuPT

Auf `http://www.gnupt.de` gibts eine Windowsversion zum download.

- `http://downloads.gnupt.de/gnupt.zip` downloaden und entpacken

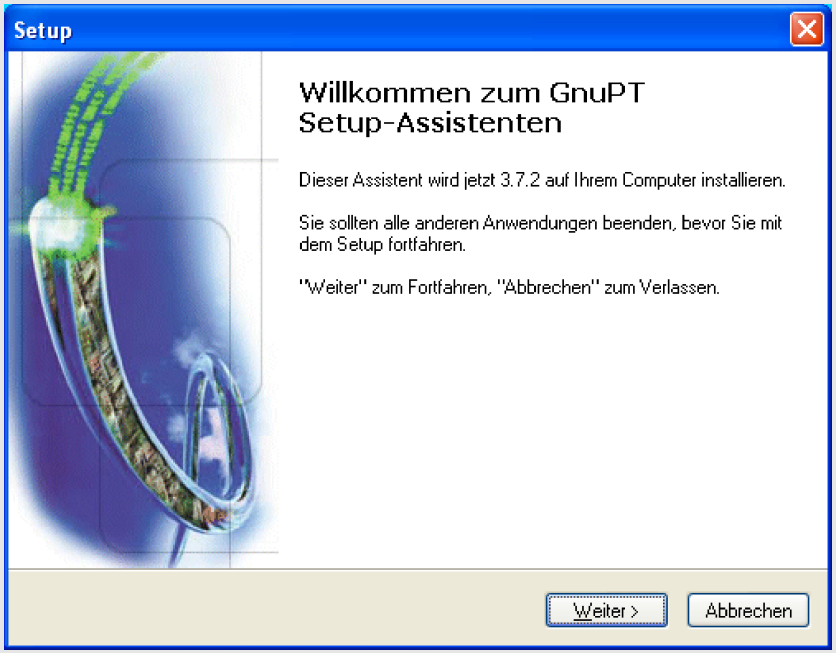
SWISS PRIVACY FOUNDATION

GnuPG installieren Windows

GnuPT

Auf `http://www.gnupt.de` gibts eine Windowsversion zum download.

- GnuPT Installer starten



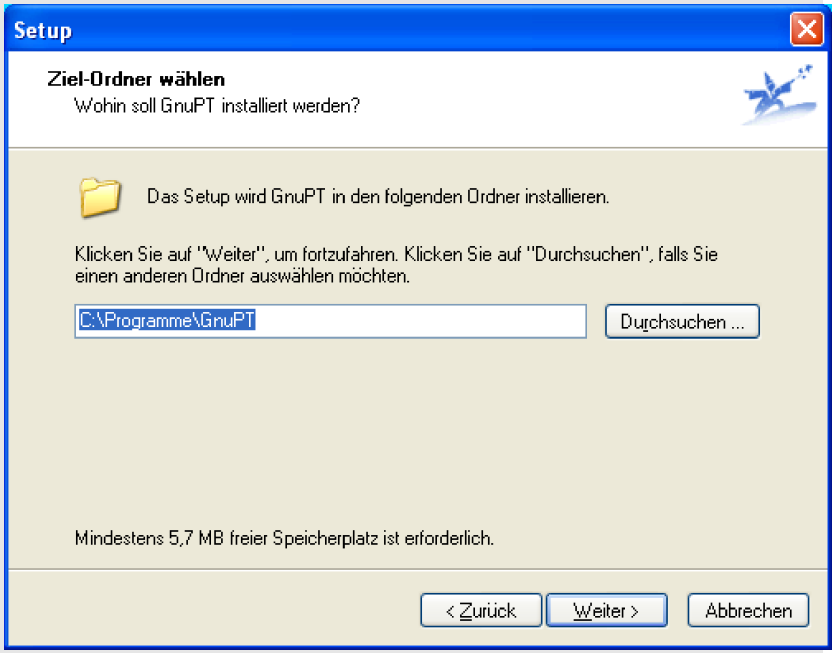
SWISS PRIVACY FOUNDATION

GnuPG installieren Windows

GnuPT

Auf `http://www.gnupt.de` gibts eine Windowsversion zum download.

- Zielordner auswählen



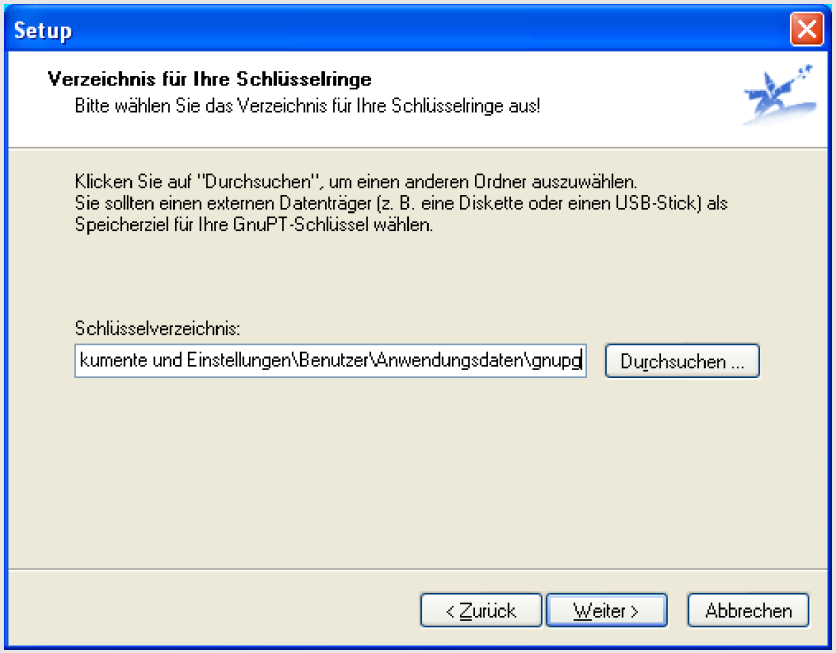
SWISS PRIVACY FOUNDATION

GnuPG installieren Windows

GnuPT

Auf `http://www.gnupt.de` gibts eine Windowsversion zum download.

- Schlüsselordner wählen



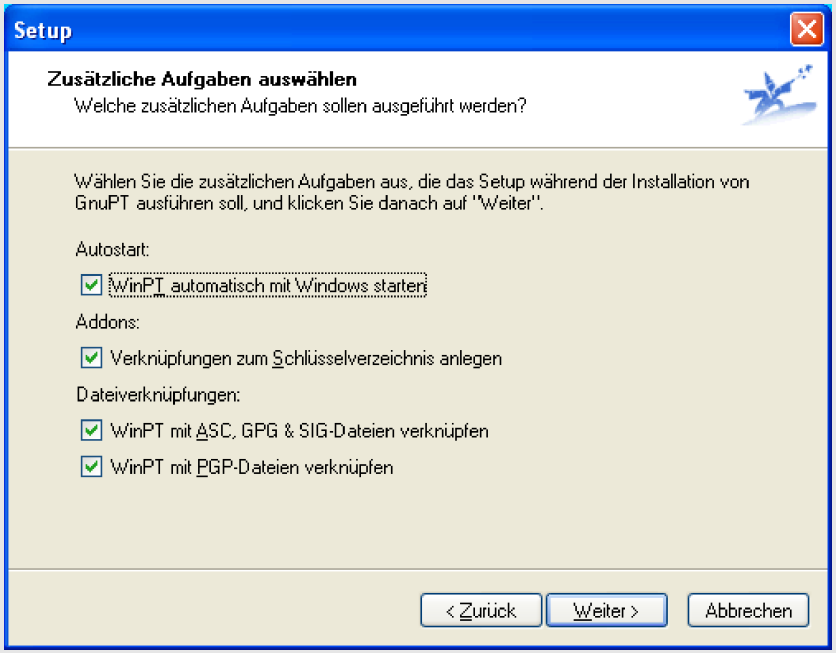
SWISS PRIVACY FOUNDATION

GnuPG installieren Windows

GnuPT

Auf `http://www.gnupt.de` gibts eine Windowsversion zum download.

- zusätzliche Aufgaben



SWISS PRIVACY FOUNDATION

Schlüssel generieren

Passphrase wichtig!!!

SWISS PRIVACY FOUNDATION

Schlüssel generieren Linux

Kommandozeile:

gpg –gen-key

Merke:

default generiert einen DSA Schlüssel zum Signieren mit 1024 Bit sowie einen ElGamal Schlüssel für die Verschlüsselung mit 2048 Bit Schlüsselstärke.

SWISS PRIVACY FOUNDATION

Schlüssel generieren Linux

gpg –gen-key

Please select what kind of key you want: default
What keysize do you want? 2048
Key is valid for? 0
Is this correct (y/n)? y

Merke:

Ob der richtige Name angeben wird für die User-ID liegt im eigenen Ermessen. Hat jemand gute Gründe dafür oder dagegen?

SWISS PRIVACY FOUNDATION

Schlüssel generieren OSX

Kommandozeile:

gpg –gen-key

Merke:

default generiert einen DSA Schlüssel zum Signieren mit 1024 Bit sowie einen ElGamal für die Verschlüsselung Schlüssel mit 2048 Bit Schlüsselstärke.

SWISS PRIVACY FOUNDATION

Schlüssel generieren OSX

gpg –gen-key

Please select what kind of key you want: default
What keysize do you want? 2048
Key is valid for? 0
Is this correct (y/n)? y

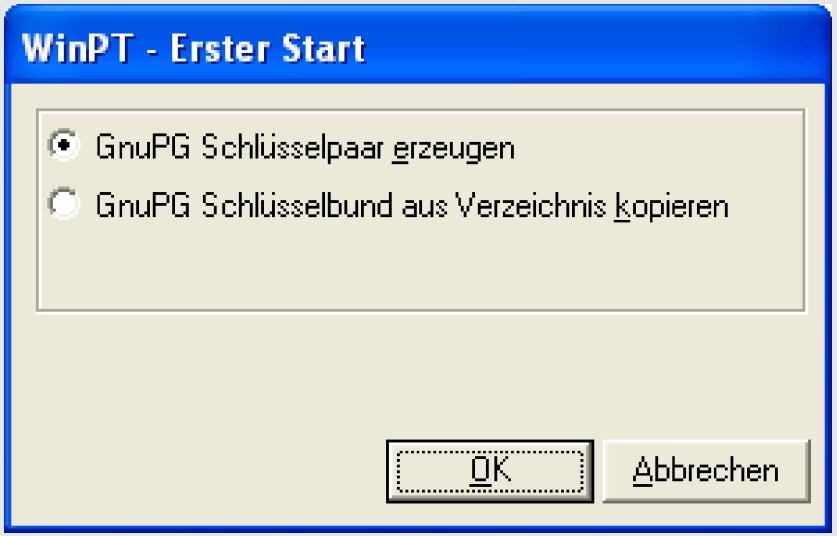
Merke:

Ob der richtige Name angeben wird für die User-ID liegt im eigenen Ermessen.
Hat jemand gute Gründe dafür oder dagegen?

SWISS PRIVACY FOUNDATION

Schlüssel generieren Windows

- Klick auf "Windows Privacy Tray"



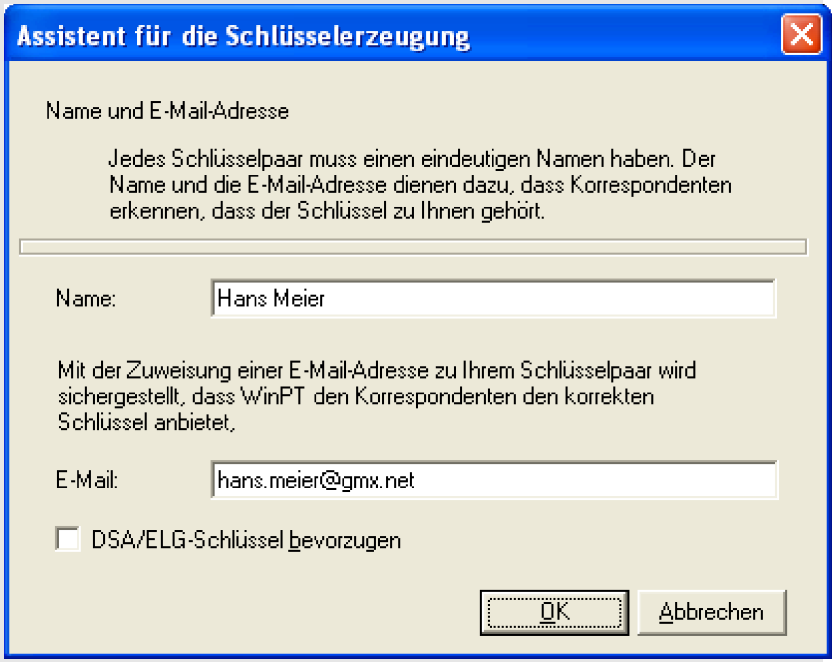
Merke:

Per default wird ein RSA/RSA 2048Bit Schlüsselpaar erzeugt.

SWISS PRIVACY FOUNDATION

Schlüssel generieren Windows

- GnuPG Schlüsselpaar erzeugen



Merke:

Per default wird ein RSA/RSA 2048Bit Schlüsselpaar erzeugt.

SWISS PRIVACY FOUNDATION

Schlüssel verwalten Linux

Seahorse

eignet sich für die Schlüsselverwaltung unter Gnome.

Kommandozeile:

sudo apt-get install seahorse

SWISS PRIVACY FOUNDATION

Schlüssel verwalten OSX

GPGPreferences

Von der MacGPG Seite GPGPreferences herunterladen und installieren.
Damit können die Einstellungen von GnuPG mit einem GUI kontrolliert werden.

GPGKeys

Von der MacGPG Seite GPGKeys (GPG Schlüsselbund) herunterladen und installieren.
GPGKeys ist ein GUI zur Schlüsselverwaltung.

SWISS PRIVACY FOUNDATION

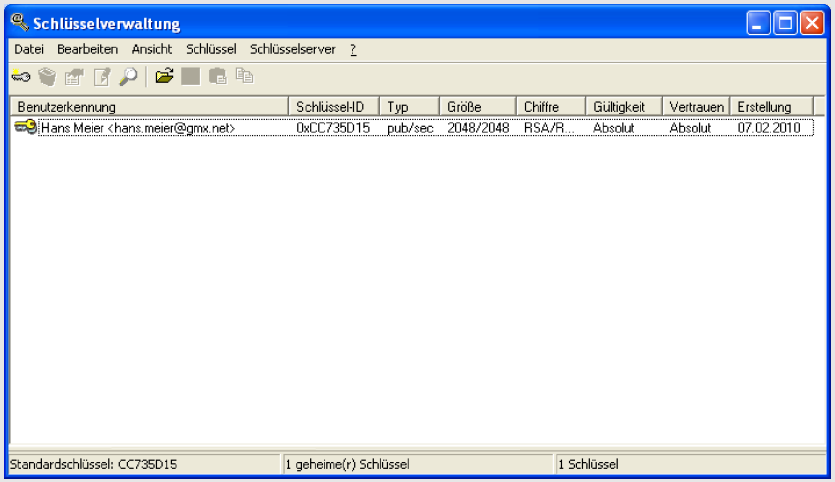
Schlüssel verwalten Windows

- Klick auf "Windows Privacy Tray"

SWISS PRIVACY FOUNDATION

Schlüssel verwalten Windows

- Schlüsselverwaltung



SWISS PRIVACY FOUNDATION

Schlüssel verteilen

Damit uns andere verschlüsselte Nachrichten schicken können, brauchen sie unseren öffentlichen Schlüssel.
Wir können diesen auf elektronischem Weg verteilen.

SWISS PRIVACY FOUNDATION

web of trust

Merke:

Es ist fraglich, ob die Keyserver verwendet werden sollten. Argumente?

Keyserver

Auf Keyservern werden öffentliche Schlüssel gespeichert. Diese können von den Benutzern signiert und diese Signaturen auf den Keyservern gespeichert werden. Ich kann dann vertrauen, wem vertraut, dem ich vertraue.

Merke:

Dieses Netzwerk der Signaturen nennt sich das web of trust.
http://wikipedia.de/Web_of_Trust

SWISS PRIVACY FOUNDATION

web of trust

Merke:

Es ist fraglich, ob die Keyserver verwendet werden sollten. Argumente?

Keyserver

Auf Keyservern werden öffentliche Schlüssel gespeichert. Diese können von den Benutzern signiert und diese Signaturen auf den Keyservern gespeichert werden. Ich kann dann vertrauen, wem vertraut, dem ich vertraue.

Merke:

Dieses Netzwerk der Signaturen nennt sich das web of trust.
http://wikipedia.de/Web_of_Trust

SWISS PRIVACY FOUNDATION

web of trust

Merke:

Es ist fraglich, ob die Keyserver verwendet werden sollten. Argumente?

Keyserver

Auf Keyservern werden öffentliche Schlüssel gespeichert. Diese können von den Benutzern signiert und diese Signaturen auf den Keyservern gespeichert werden. Ich kann dann vertrauen, wem vertraut, dem ich vertraue.

Merke:

Dieses Netzwerk der Signaturen nennt sich das web of trust.
http://wikipedia.de/Web_of_Trust

SWISS PRIVACY FOUNDATION

web of trust

Merke:

Es ist fraglich, ob die Keyserver verwendet werden sollten. Argumente?

Keyserver

Auf Keyservern werden öffentliche Schlüssel gespeichert. Diese können von den Benutzern signiert und diese Signaturen auf den Keyservern gespeichert werden. Ich kann dann vertrauen, wem vertraut, dem ich vertraue.

Merke:

Dieses Netzwerk der Signaturen nennt sich das web of trust.
http://wikipedia.de/Web_of_Trust

SWISS PRIVACY FOUNDATION

Schlüssel exportieren

mit Seahorse

Mit Seahorse kann der öffentliche Schlüssel exportiert werden. Unter eigene Schlüssel Rechtsklick auf den eigenen Schlüssel - Export

SWISS PRIVACY FOUNDATION

Schlüssel exportieren

mit GPGKeys

- öffentlichen Schlüssel markieren
- Ablage - Exportieren - Schlüssel
- Haken vor ASCII-Hülle

SWISS PRIVACY FOUNDATION

Schlüssel exportieren

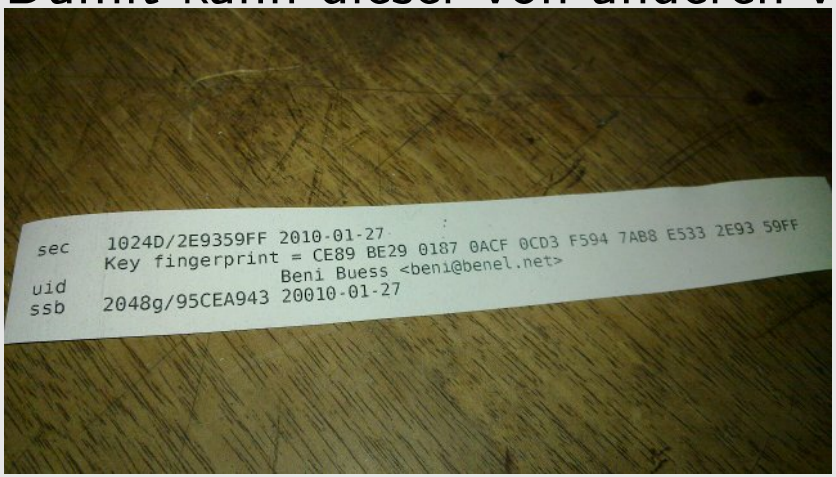
mit WinPT

- Schlüssel auswählen
  Menu Schlüssel - Exportieren
- Speicherort auswählen

SWISS PRIVACY FOUNDATION

Schlüsselstreifen

Schlüsselstreifen sind geeignet um den Fingerprint des öffentlichen Schlüssels zu verteilen.
Damit kann dieser von anderen verifiziert werden.



Kommandozeile:

gpg –list-secret-keys –fingerprint

SWISS PRIVACY FOUNDATION

Schlüssel importieren

mit Seahorse

Via Menu Datei - Import kann eine *.asc Schlüsseldatei importiert werden.
Alternativ kann man den Schlüsselblock aus einer Webseite kopiert und via Menu Bearbeiten - Einfügen importieren.

SWISS PRIVACY FOUNDATION

Schlüssel importieren

mit GPGKeys

Via Menu Ablage - Importieren kann eine *.asc Schlüsseldatei importiert werden.

SWISS PRIVACY FOUNDATION

Schlüssel importieren

mit WinPT

Via Menu Datei - Importieren kann eine *.asc Schlüsseldatei importiert werden.
Alternativ kann eine *.asc Datei auch direkt geöffnet werden.

SWISS PRIVACY FOUNDATION

Schlüssel signieren

Fingerprint überprüfen

Gehört der Fingerprint wirklich dieser Person? Und ist sie es wirklich?
Zur Kontrolle bieten sich Ausweis und Schlüsselstreifen an.

Achtung!

Achtet darauf, die signierten Schlüssel nicht auf Keyserver hochzuladen.
Jeder soll selbst entscheiden, wo seine Keys landen.

SWISS PRIVACY FOUNDATION

Schlüssel signieren

Fingerprint überprüfen

Gehört der Fingerprint wirklich dieser Person? Und ist sie es wirklich?
Zur Kontrolle bieten sich Ausweis und Schlüsselstreifen an.

mit Seahorse

Schlüssel aus der Liste andere Schlüssel öffnen und im Reiter "Vertrauen"den Schlüssel signieren.

SWISS PRIVACY FOUNDATION

Schlüssel signieren

Fingerprint überprüfen

Gehört der Fingerprint wirklich dieser Person? Und ist sie es wirklich?
Zur Kontrolle bieten sich Ausweis und Schlüsselstreifen an.

mit GPGKeys

Betreffenden Schlüssel markieren
Menu Schlüssel - Signieren
Terminal öffnet sich

SWISS PRIVACY FOUNDATION

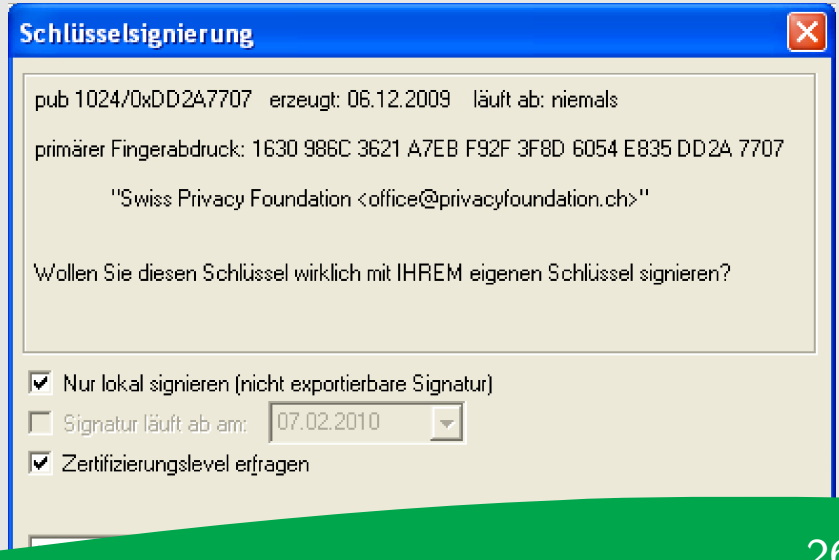
Schlüssel signieren

Fingerprint überprüfen

Gehört der Fingerprint wirklich dieser Person? Und ist sie es wirklich?
Zur Kontrolle bieten sich Ausweis und Schlüsselstreifen an.

mit WinPT

- Rechte Maustaste auf importierten Schlüssel - Signieren
- Zertifizierungslevel erfragen



SWISS PRIVACY FOUNDATION

Übersicht

SWISS PRIVACY FOUNDATION

Thunderbird & Enigmail

Enigmail ist eine Erweiterung für Thunderbird.

Merke:

*Enigmail 1.0 läuft nur mit Thunderbird 3.**

SWISS PRIVACY FOUNDATION

Enigmail installieren

Kommandozeile:

sudo apt-get install enigmail enigmail-locale-de

Download von
`http://enigmail.mozdev.org/download/index.php`
In Thunderbird unter Tools - Addons das Plugin auswählen.

SWISS PRIVACY FOUNDATION

Enigmail installieren

Kommandozeile:

sudo apt-get install enigmail enigmail-locale-de

Download von
`http://enigmail.mozdev.org/download/index.php`
In Thunderbird unter Tools - Addons das Plugin auswählen.

SWISS PRIVACY FOUNDATION

Enigmail Einstellungen

Im neuen Menu OpenPGP unter Einstellungen:

- Eigenen Schlüssel zur Empfängerliste hinzufügen.
- ...

SWISS PRIVACY FOUNDATION

Mail signieren & verschlüsseln

Im Fenster zum Erfassen neuer Nachrichten erscheint ein OpenPGP Button.
Da lässt sich auswählen, ob das Mail signiert und/oder verschlüsselt werden soll.

SWISS PRIVACY FOUNDATION

Mail entschlüsseln

Wenn eine verschlüsselte Nachricht geöffnet werden soll, wird die Passphrase abgefragt.
Hier kann kontrolliert werden, ob die Passphrase für einige Minuten gecacht werden soll.

SWISS PRIVACY FOUNDATION

Apple Mail & GPGMail

Achtung!

Apple Mail vor der Installation beenden!

GPGMail

GPGMail ist eine Erweiterung für Apple Mail.
Projektwebseite: `http://www.sente.ch/software/GPGMail/`
Download von
`http://sourceforge.net/projects/gpgmail/files/`

SWISS PRIVACY FOUNDATION

GPGMail Einstellungen

Nach der Installation von GPGMail kann Apple Mail wieder gestartet werden.
In den Apple Mail Einstellungen befindet sich nun ein Reiter "PGP".

Einstellungen

- Unter Schlüssel:
  - Standartschlüssel auswählen
  - immer das Kennwort abfragen
- Unter Verfassen:
  - Symbole beim Verfassen der Email anzeigen
  - Generell mit meinem öffentlichen Schlüssel verschlüsseln
  - Schlüssel, die nicht verwendet werden können, herausfiltern

SWISS PRIVACY FOUNDATION

Mail signieren & verschlüsseln

Beim Erstellen einer neuen Nachricht können nun Checkboxen zum Signieren resp. Verschlüsseln gesetzt werden.
Unter Signieren den eigenen Schlüssel wählen
Unter Verschlüsseln den öffentlichen Schlüssel des Empfängers wählen

Merke:

Bei bekannten Empfänger wird der richtige Schlüssel automatisch gewählt.

SWISS PRIVACY FOUNDATION

Mails entschlüsseln

Keine Doku gefunden. Keine Gelegenheit zum Testen bis anhin.
Wird wohl ohne Probleme funktionieren.
Bitte Hinweise melden.

SWISS PRIVACY FOUNDATION

Firegpg

Firegpg ist eine Extension für Firefox. Damit können verschlüsselte Mails (und anderer direkt im Browserfenster entschlüsselt werden.

SWISS PRIVACY FOUNDATION

gEdit

Kommandozeile:

sudo apt-get install seahorse-plugins

gEdit ist eine auf GTK basierender Editor.
Um gEdit zum Ver- und Entschlüsseln zu verwenden, muss ein Plugin aktiviert werden:
Bearbeiten - Einstellungen - Plugins - Text-Verschlüsselung
Neue Menupunkte unter Bearbeiten (Verschlüsseln, Entschlüsseln, Signieren)

SWISS PRIVACY FOUNDATION

Danke fürs Mitmachen!

Slides

Die Slides werden unter `https://privacyfoundation.ch` zum Download angeboten.

Lizenz

`http://creativecommons.org/licenses/by-nc-sa/2.5/ch/`

Kontakt

Anregungen werden gerne per Mail entgegen genommen.
Die Adresse kann dem Public-Key des Autors entnommen werden.
`http://benel.net/pubkey.html`