**HTW** Chur
Hochschule für Technik und Wirtschaft

Fachhochschule Ostschweiz
University of Applied Sciences

# Verschlüsselung mit GnuPG (GNU Privacy Project)


Autor: Luca Costa, HTW Chur, luca.costa@tet.htwchur.ch
Dozent: Bruno Wenk, HTW Chur, bruno.wenk@fh-htwchur.ch

# Inhaltsverzeichnis

# 1 Verschlüsselung mit GnuPG

## 1.1 Software installieren

Auf der Homepage von GnuPP [1] findet man nützliche Informationen für die Installation der Software. Im Prinzip gibt es zwei Möglichkeiten: man kann die einzelne Software manuell installieren oder man kann einen fix-fertigen Installer mit allen benötigten Programme herunterladen und installieren. Ich habe die zweite Variante gewählt, da sie schneller ist. Das Software Packet heisst „Gpg4win“ und ist auf der Homepage von Gpg4win [2] zu finden. Der Installer ist ca. 10 MB gross.


**Abbildung 1: Installation von Gpg4win**

Die letze stabile Version ist 1.1.3 und wurde am 17. September 2007 veröffentlicht. In der Zwischenzeit haben die Entwickler von Gpg4win auch eine BETA-Version programmiert, aber sie ist nur für Testzwecken geeignet.

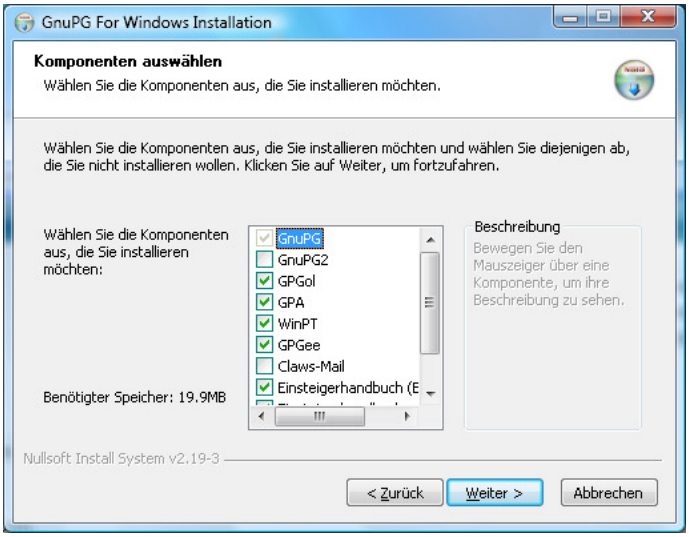



**Abbildung 2: Gpg4win-Komponenten auswählen**

Bei der Installation kann man die benötigten Pakete auswählen. Die Standard-Installation beinhaltet den Verschlüsselungsalgorithmus und die dazu benötigte Software um Nachrichten zu verschlüsseln, entschlüsseln und Dateien digital signieren.

## 1.2 Schlüsselpaar erzeugen

Mit dem Programm WinPT kann man die Schlüsselpaar erzeugen. Beim ersten Dialog muss man die Option „GnuPG Schlüsselpaar erzeugen“ auswählen“.


**Abbildung 3: WinPT Erster Start**

Danach muss man den Namen und die E-Mail-Adresse eingeben.

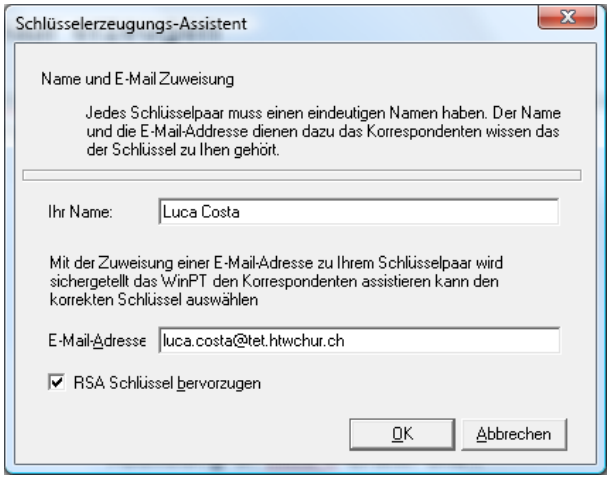



**Abbildung 4: Schlüsselerzeugungs-Assistent**

Um die Schlüssel zu erzeugen muss man noch ein Passwort eingeben. Es soll mindestens 8 Zeichen lang sein und sollte Ziffern und Buchstaben enthalten, somit ist die Sicherheit höher.

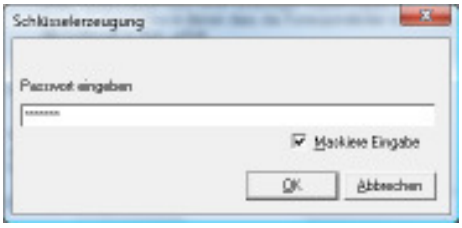
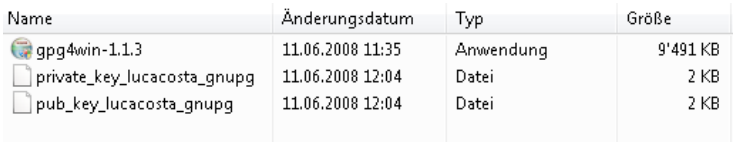



**Abbildung 5: Passwort eingeben**

Wenn alles erfolgreich war hat man jetzt zwei Schlüssel, einer ist öffentlich, also für alle sichtbar, und der andere ist privat. Empfehlenswert ist eine Backup-Kopie diesen Schlüssel auf ein externes Medium zu speichern.



| Name | Änderungsdatum | Typ | Größe |
|---|---|---|---|
| gpg4win-1.1.3 | 11.06.2008 11:35 | Anwendung | 9'491 KB |
| private_key_lucacosta_gnupg | 11.06.2008 12:04 | Datei | 2 KB |
| pub_key_lucacosta_gnupg | 11.06.2008 12:04 | Datei | 2 KB |

**Abbildung 6: Backup privater und öffentlicher Schlüssel**

Der Inhalt meiner öffentlichen Schlüssel sieht folgenermassen aus:

```
pub 1024D/5A2D0037 11.06.2008 Luca Costa <luca.costa@tet.htwchur.ch>
Primary key fingerprint:  3271 FE44 E636 EE24 ED7A 3828 E938 10B8 5A2D 0037

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.7 (MingW32) - WinPT 1.2.0

mQGiBEhPoxcRBACFmHsQfih8RHk5gF2BZtfw5pIu6ISE4Wubc+s+HmZIWNw61b5o
Hd/J5E2WqAwZSc2ICLfcpbb4VRsPKEKJp7pbEHKylxEJNRdXC13cxeKB/GR+KIH2
Vsa49GR41Dxazyu2SQYuLipwKBxCigm2b9e1aNJldaUegUhG+vTuLwGbDwCg5zAS
FhWNzKw+8LVoQgRT0+cAT0cD/jkW/eSCMLbyJvnCQqs8QMC1lfeIPOEDS7gL4His
g/VSrLPGWp1OmmLLJsVqb1X1u4Z2+G4urJkjSdIkYE0m+b/tvuoHDx10JGGuA8WY
UkBgySaYWp7aYlCMF29NuxZWXYaGQsfdQHg6AF5LTlxNM7gAYEzY7AUUYRvguP7o
NiAZA/0SJbTWV+QksZmWdurDcxW4FSE3SxZJYyq9xHhxfvcUFDzElnp5SMEvwEKh
e1zPSxHodgj2h8AN1wtfBb35g8UzlVyUsux1HLePzXtYwHomA40PI1wTOzNybdKa
+OdCM0MN+dxBLkd1Yxy+C3C26MxM0CFp3h0/k64CoD7UGQN2W7QmTHVjYSBDb3N0
YSA8bHVjYS5jb3N0YUB0ZXQuaHR3Y2h1ci5jaD6IYAQTEQIAIAUCSE+jFwIbAwYL
CQgHAwIEFQIIAwQWAgMBAh4BAheAAAoJEOk4ELhaLQA34d4AnRhCP5OLgrr9QhQX
ttLHm0KI1BIdAJwNbRv747b8w6NTOGwV/NdoIVrhXrkBDQRIT6MXAQgAt+jjksxN
Vgzf/gKrHCAnFjWMLwnyELxu2/3mtHRZOIweZMrhOTsaxFSgjO5CJo/wux1k23Ud
STD6shI8T0qJGakzjd1uZ1kFe7Jl0uyrYI1ai9hE849cCTaDo7B1DC2n2amzZa+j
gyOh0QQUIlRWVYkJdEL65yDisoomsqvWH928o00uVPqel/l2lCAQY3ji7nCw8nsW
eE7s0WFCQvsvdhBxRBMdeH0aEPy/zo2yxLEIZpxM8TmSPT+1Fh42Ks6ynxwbHJzh
is+J27jdzow2iyUDrslmw1jggpOrmqLV2UW6T3OfKaxkm31U4KbLXHmNP4Shyudc
VlonjaBGoLR8jwARAQABiQFoBBgRAgAJBQJIT6MXAhsuASkJEOk4ELhaLQA3wF0g
BBkBAgAGBQJIT6MXAAoJEHkheON8y9Z6Jc8H/0gvtkivtPLQtNOcEJIYBdnZV1Zp
jwF9IdrS1T3jZi/SWzpzzpjrME9eRsEyOfJY9puKYEGjpQNhRGjXU9ketcmLCMMR
HyEg4vcaVm0+xsxb2nrL4kqzi6DA1znd8ozc55uGeDG5UAOn9E2jYNa7Oj2t5MR2
SiYsBewamKZQqZ37MmTbNaH4LEq2himKQBH7wK8QPQKlUqQveSeNL99UTuKThpQM
+6GkDXCFk3fnqy5DWNRydg7CYuLivL3Titv9mvtW/jiQOEmCNEnxR2L03x/6GwF7
nEDjwTgQUScwnIMTfIpNYkmdkNOmt9LtFX2TGIs3BupUus5bsCa7Q8jvVcBNpwCg
w+U3aauRaQj5rsW65ECOuB7xS94AnisJSOmkgCvGC+Tvy1kZ+cSo+1fZ
=RHGs
-----END PGP PUBLIC KEY BLOCK-----
```

## 1.3 Öffentlicher Schlüssel importieren

Der Prozess, um einen Schlüssel zu importieren, ist sehr einfach. Man muss auf „Schlüssel -> importieren“ klicken. Danach muss man den Schlüssel in einem TXT-File abspeichern, um ihn zu importieren. Das Programm findet dann den Schlüssel in der TXT-Datei automatisch.

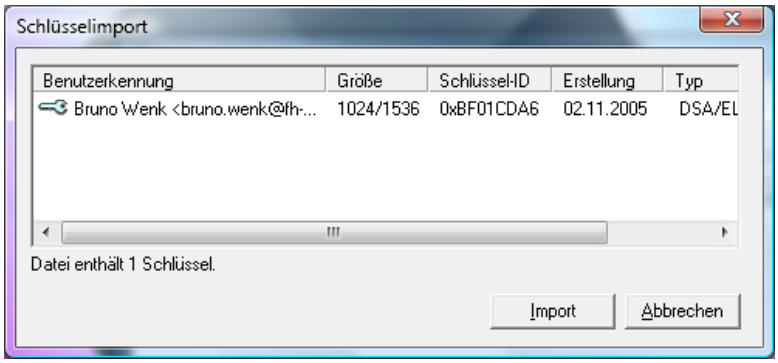



**Abbildung 7: Schlüssel importieren**

Das Resultat sieht folgendermassen aus:

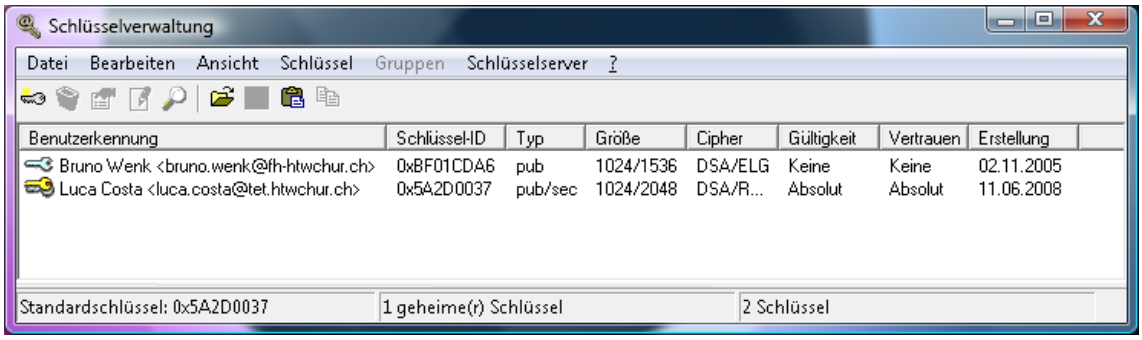



**Abbildung 8: Schlüsselverwaltung**

## 1.4 Verschlüsselte Nachricht entschlüsseln

Um eine Nachricht zu entschlüsseln muss man das Software „GPA“ brauchen. Unter „Dateien“ kann man eine Datei wählen, um diese mit dem privaten Schlüssel zu entschlüsseln. Es gibt einen zusätzlichen Sicherheitsmechanismus: man muss ein Passwort eingeben.

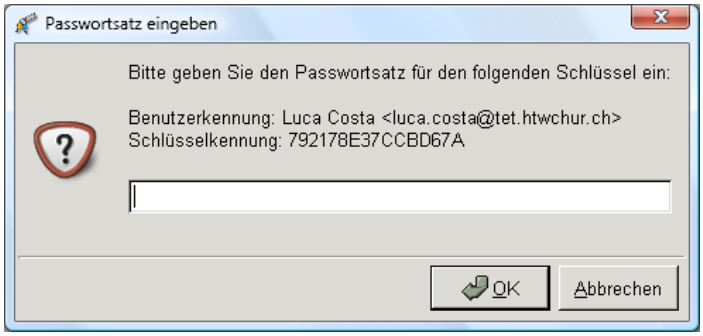



**Abbildung 9: Passwortsatz eingeben, um zu entschlüsseln**

Wenn alles erfolgreich war sieht man die Nachricht im Klartext.

## 1.5 Verschlüsselte Nachricht senden

Um eine Nachricht zu verschlüsseln muss man das Programm „WinPT“ brauchen. Man muss mit dem Rechtsklick auf die Tray-Icon (Unten rechts) klicken und dann „Zwischenablage -> Verschlüsseln“ wählen. Dann kann man den öffentlichen Schlüssel (Empfänger) heraussuchen und danach muss man auf „OK“ klicken, somit wird die Nachricht verschlüsselt.

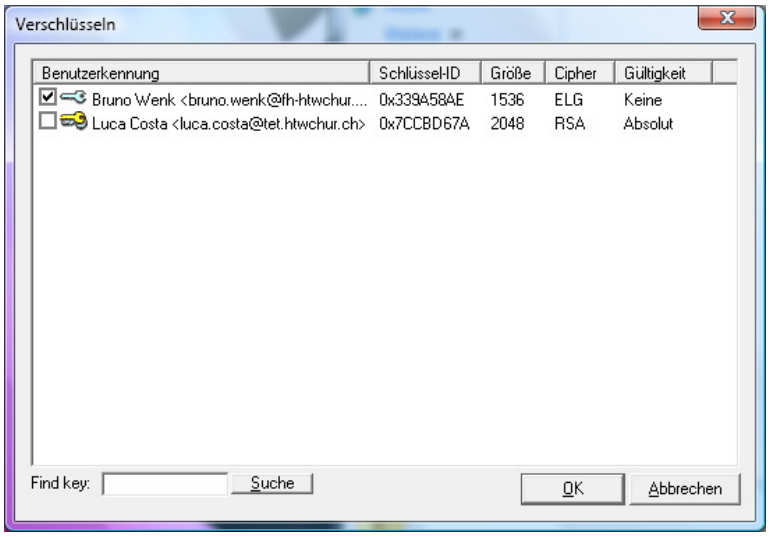



**Abbildung 10: Nachricht verschlüsseln**

Ich habe folgende Nachricht verschlüsselt:

```
Hat es mit der Entschlüsselung funktioniert? Danke :-)
```

Verschlüsselt sieht folgendermassen aus:

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (MingW32) - WinPT 1.2.0

hQGOA3WDdJEzmliuEAX9Hy+b/pbMmYqWxUfMcbmH88fy5oLKNhznoO/bQMZ3ABhw
Orsqt2ztE+spR5L7NmRzg6FJqQc6uQDuUzhUaeqV6dv/G4crw7KpvUaYhxFfUUH1
/kbOJb7uljsCOxAQ05WXrtsvdp+ji/16NVEvXPmt6w7KwSnbgmYV/ZY7FCs+8IY4
gpwYfvaJjcoEycZFOnchvOxkWi1lJ+rKSTqfC5cKSlB9qdJcSPqKysmO3fDAzfpm
zmlvsO3hOIohk+vOeZ8GBgDnDibLVMsPOEcyb2TjkCJUTPDuB8p6bKQ3M8itXy9K
FI/GxyEnk1ERpsnwlPgWPvnYkposacpgb2NKosLswjj77AWdoJD1+UifWrTTyfca
rvL7RakFkh/b6FHQK7MPY6j+0HcSpiR4jU8ylGSytsjtzqYhyik8Spux+fctRxZq
ifB+apqKpgnG7W2HHxf8ntyNPPkPbKff9/yNrc2rmZS812Z7UZxa/Mjus+Q5zNJb
9BIIZzGgLyEDB28yypntgZ7ScQG2NQYpH+9NFsBRYYZA8wOh9QIy447Q/MEoHImp
yY7LX0xZIJPY8bWwNVebsrZWIVu/P/J9wXsYGEbKnB4ubihndnzi63AenEIUsX2O
KhuXwtbAYd3kP2AlmwLVkJEuiQRrfD9xRrV/nxhFTyYcDT5e
=SoVr
-----END PGP MESSAGE-----
```

## 1.6 Dokument digital signieren

Es gibt verschiedene Möglichkeiten um einen Dokument zu signieren, ich werde hier die Methode mit dem Programm „GPGee“ kurz beschreiben. Der erste Schritt ist das Dokument zu wählen und mit dem Rechtsklick darauf zu klicken. Dann muss man die Option „GPGee -> Sign“ oder „GPGee -> Sign & Encrypt“ (Signieren und Verschlüsseln) wählen.

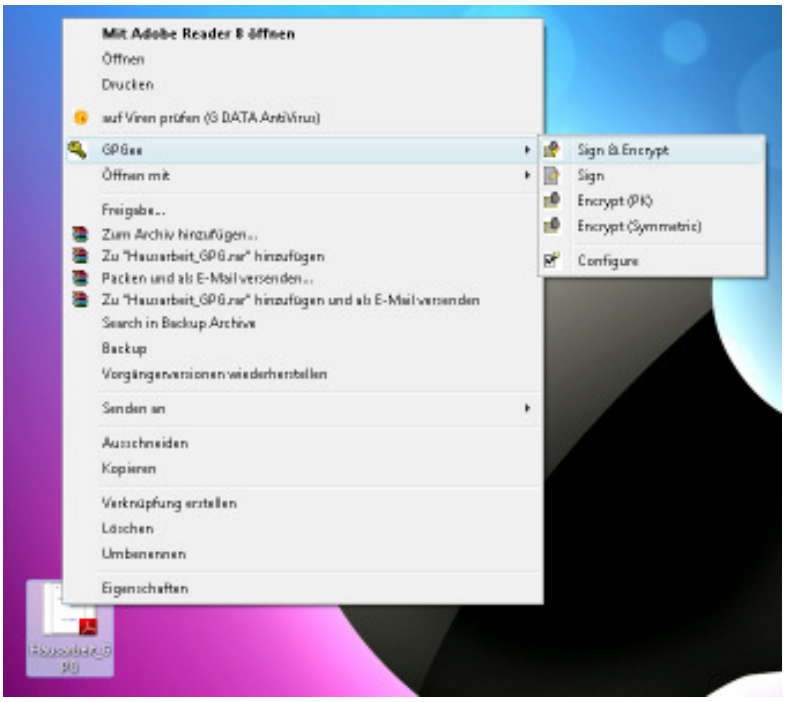



**Abbildung 11: Mit GPGee signieren**

Als nächstes muss man den öffentlichen Schlüssel (Empfänger) wählen und auf „Ok“ klicken. Somit entsteht ein digital signiertes Dokument.

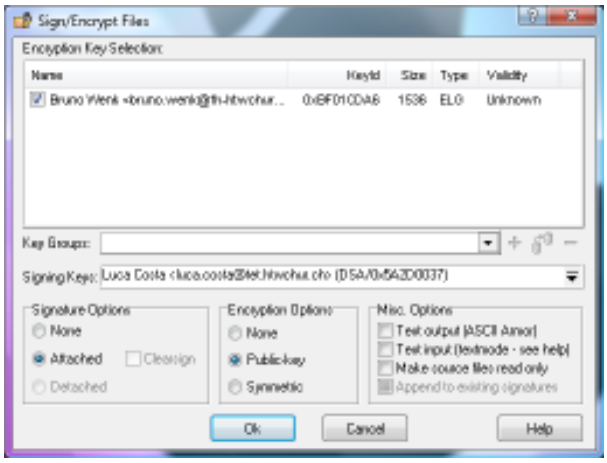



**Abbildung 12: Signieren und Verschlüsseln**

# 2 Quellenverzeichnis

## 2.1 Quellen aus dem Internet

[1] Software für GnuPP (GNU Privacy Project)
[http://www.gnupp.de/software.html], 2008

[2] Software-Packet Gpg4Win
[http://www.gpg4win.org/download.html], 2008

# 3 Anhang

## 3.1 Abbildungen