Web of trust

Een manier om met certificaten te werken is met behulp van een zogenaamde **Web of trust**. Hiermee geef je handmatig aan wie je vertrouwt en je wisselt handmatig certificaten uit met PGP.
PGP staat voor **Pretty Good Privacy** en het is een programma om door middel van digitale certificaten asymmetrische versleuteling te realiseren. De identiteit van de certificaathouder wordt vastgesteld met een handtekening.
Er zijn commerciële programma's maar er is nog steeds een open source variant beschikbaar onder de naam **OpenPGP**.
Het PGP-certificaat kan gebruikt worden voor e-mail versleuteling of het ondertekenen van e-mails. Zender en ontvanger ondertekenen elkaars certificaat.

In dit practicum gaan we met OpenPGP certificaten uitwisselen.

- Eerst moeten er twee programma's geïnstalleerd worden.
- Vervolgens gaan we certificaten uitwisselen en ondertekenen.
- Tenslotte wisselen we een geheim bericht uit dat versleuteld is.

De software

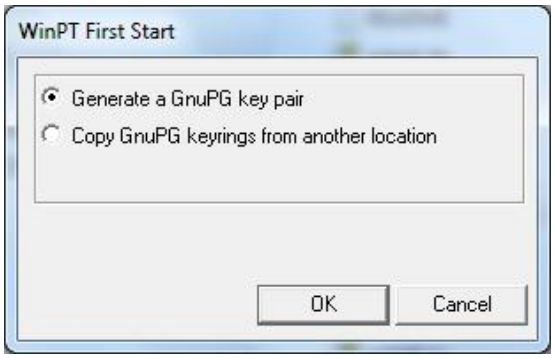
Allereerst hebben we de Windows versie van **GnuPG** nodig voor de OpenPGP functionaliteit. Download de laatste versie van GnuPG vanaf http://gnupg.org/download/ of vraag om de zip bij je docent.
Installeer GnuPG met de standaard opties en kies als taal nl-.

Daarnaast hebben we **WinPT** nodig wat je kunt downloaden vanaf http://wald.intevation.org/frs/?group_id=14. Installeer WinPT in c:\WinPT.

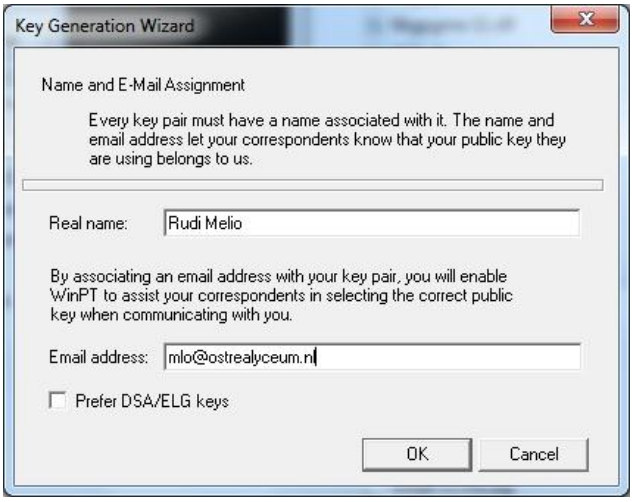
Het stappenplan

1 Start WinPT.exe.

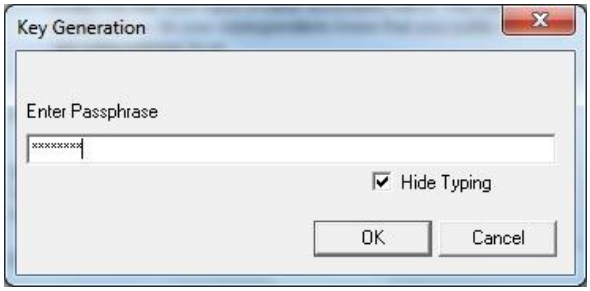
We zijn nog niet in het bezit van een sleutelpaar en we kiezen dan ook voor **Generate a GnuPG key pair** en klik op OK.



2 In de **Key Generation Wizard** geef je je naam en je e-mailadres op en klik je op OK.

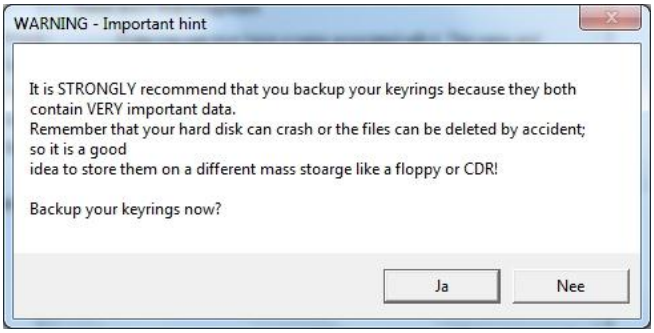


3 In het **Key Generation** scherm geef je bij **Enter Paraphrase** een wachtwoord op en klik je op OK.



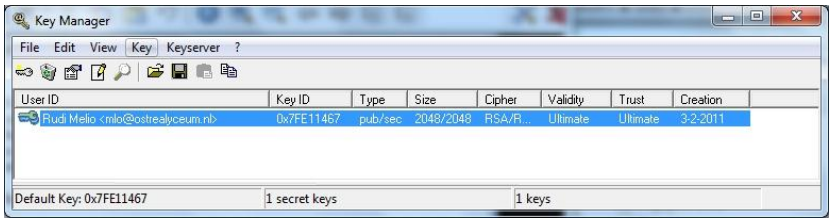
4 Geef nogmaals je wachtwoord op. Vervolgens wordt het wachtwoord versleuteld en er komt een melding dat de sleutels gegenereerd zijn.

5 In het volgende venster wordt er gevraagd of je een back-up wil maken. Als het enkel voor testdoeleinden is, hoef je geen back-up te maken maar als het een echte sleutel moet worden, is het aan te bevelen een back-up te maken.

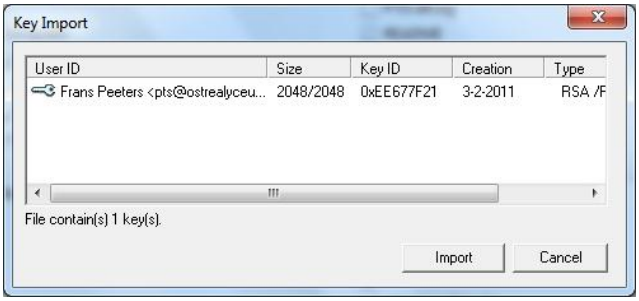


6 Nu heb je rechtsonder op je Windows menubalk een icoontje met een sleutel. Klik met de rechtermuisknop op het sleuteltje en open het WinPT menu. Klik daarna op **Key Manager**.

7 Selecteer in het **Key Manager** scherm je eigen sleutelpaarcertificaat en klik op **Key** en daarna op **Export …** Sla het bestand op.

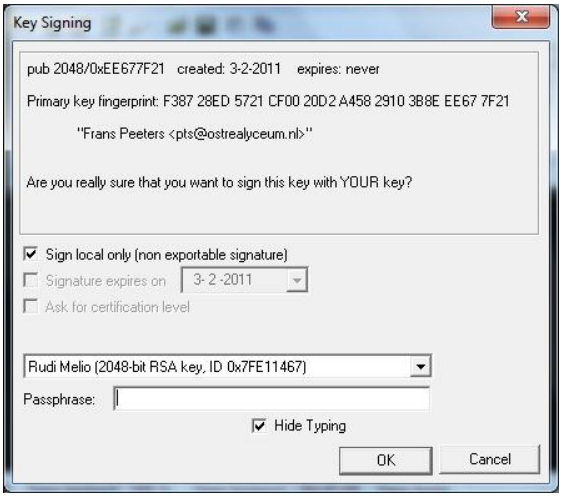


8 Wissel nu met elkaar je certificaat uit. Dat kan bijvoorbeeld met een usb-stick of per e-mail. Als je het certificaat van de ander ontvangt, moet dat geïmporteerd worden. In de **Key Manager** ga je naar **Key – Import …**
Blader naar het certificaat, importeer het certificaat, neem de statistiek gegevens voor kennisgeving aan en klik op OK.



9 Terug in het **Key Manager** menu zien we nu ook het geïmporteerde certificaat. In de kolom **Validity** kun je zien dat we de identiteit nog niet hebben vastgesteld en het certificaat dus nog niet hebben ondertekend. In de kolom **Trust** kun je zien dat we deze identiteit nog niet kunnen vertrouwen.

10 We gaan nu het certificaat ondertekenen. Klik rechts op het certificaat en kies **Sign…** Vink de optie **Sign local only (non exportable signature)** aan en geef het wachtwoord van je private sleutel zodat het certificaat ondertekend kan worden en klik vervolgens op OK. Er verschijnt een scherm dat bevestigt dat het certificaat ondertekend is. Klik op OK.



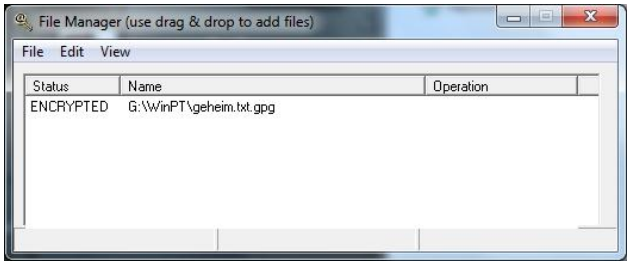
11 Voor ons **Web of trust** moeten we nog aangeven in hoeverre we de certificaathouder vertrouwen. Dubbelklik op het certificaat om het **Key Properties** venster aan te roepen. In het venster **Change** selecteer je een niveau en klik je op OK. Sluit alle openstaande vensters.

12 Maak nu een bestand met Kladblok of Word met een geheime boodschap en sla dat op. Klik op het sleuteltje in de taakbalk en kies **File Manager**. Het **File Manager** menu verschijnt. Sleep nu het bestand vanuit je verkenner in het venster van de **File Manager**.

13 We willen het bestand versleutelen met de publieke sleutel van de andere partij en we willen het ondertekenen met onze eigen sleutel zodat de ander weet dat het authentiek is. Selecteer het bestand en kies **File – Sign & Encrypt ...**

14 Het **File Encrypt** menu verschijnt. Selecteer onder **User ID** het certificaat met de publieke sleutel van de ontvanger en vink **Select Key for signing** aan en selecteer daaronder jouw eigen sleutel. Klik op OK. Vervolgens verschijnt het **Signing venster** waar je nog een keer je wachtwoord moet invullen. Vul het wachtwoord in en klik op OK.

15 Terug in het **File Manager** venster zien we dat het bestand de status ENCRYPTED heeft gekregen. Er is nu een extra bestand aangemaakt in dezelfde map met dezelfde naam maar met de extensie **.gpg**. Open het gpg bestand en je zult zien dat het versleuteld is.



16 Wissel nu de versleutelde bestanden uit. Sleep het ontvangen versleutelde bestand met de verkenner in het **File Manager** venster en kies **File – Decrypt**. Ontsleutel het bestand met je wachtwoord en klik op OK.

17 Het **Decrypt Verify** venster verschijnt en je kunt zien dat het bestand ondertekend was, dat de digitale handtekening gecontroleerd is in ons **Web of trust** en dat de handtekening goed is bevonden.

18 Sluit alle openstaande vensters en open het ontsleutelde bericht.