Echte privacy?

Ruud Uphoff

Er wordt wat afgezeurd over privacy! Maar tegelijkertijd gaan we gewoon door met onze e-mail onversleuteld over het internet te jagen. Wat zeg je? Je gebruikt een beveiligde verbinding naar je ISP? Laat je nu niets wijsmaken zeg! Het enig waartegen dat beveiligt is het meelezen van je buurman in de trein, als je aan open Wi-Fi hangt.

Als je mail verstuurt via TLS, dus over poort 465, dan gaat je bericht onleesbaar gecodeerd naar de smtp-server van je ISP. Maar die levert het vervolgens onversleuteld af bij de smtp-server van de ISP van de geadresseerde, waar het pontificaal leesbaar staat te wachten tot het wordt opgehaald met POP3. Ja, dat ophalen kan weer vercijferd gaan, maar in je mailbox staat het toch gewoon leesbaar.
Boze tongen beweren dat Microsoft in Windows 8 geen POP3 wil ondersteunen, omdat de mail dan te snel van de server verdwijnt. Nee, het moet echt alleen IMAP zijn, zodat belangrijke mail daar lekker blijft staan, voor de marketingmafia en de NSA. Niet? Welnu, ook de schijn vermijden zou ik Microsoft aanbevelen!

Het kan echt helemaal prive!

En dat ook nog eens heel simpel! Iedereen kan het, al heeft het een voordeel Thunderbird als mailprogramma te gebruiken. Er bestaat een freeware systeem van asymmetrische encryptie. Daarbij moet data worden gedecodeerd met een andere sleutel dan die waarmee ze werd gecodeerd. Data wordt gecodeerd met een publieke sleutel, zo genoemd omdat je die aan iedereen verstrekt die in staat moet zijn gecodeerde informatie naar jou te sturen. Decoderen kan echter alleen met jouw privésleutel, die je uiteraard als topgeheim behandelt. Daarnaast kun je een bericht digitaal waarmerken, zodat er geen twijfel over bestaat dat het van jou komt.


Phil Zimmerman

In 1991 kwam Phil Zimmerman met zijn programma Pretty Good Privacy (PGP), dat asymmetrische encryptie beschikbaar stelde aan het grote publiek.
Het werd niet massaal gebruikt omdat er nog nauwelijks sprake was van e-mail, maar oude rotten binnen HCC en CompUsers herinneren zich ongetwijfeld de discussie over het wel of niet toestaan van encryptie in het HCC-Fidonet.
PGP was volmaakte freeware, en ook toen de rechten overgingen in commerciële handen, bleef er een freewareversie bestaan. Tot PGP in 2010 werd verkocht aan Symantec, een bedrijf dat een naam heeft hoog te houden in het opkopen van programmatuur, om vervolgens de ondersteuning daarvan de nek om te draaien. Daarmee verdween ook de freeware versie van PGP, maar gelukkig hebben we die toch nog onder de naam GnuPG. De broncode was namelijk 'Open Source' en geen commercie kan die de nek omdraaien.

GnuPG installeren (indien nodig)

Gebruikers van de meeste Linux-distributies hebben het gemakkelijk. GnuPG met bijbehorende gebruikersomgeving 'Kleopatra' is al standaard, in elk geval in (K)Ubuntu en openSUSE. Voor Windows kun je 'Gpg4win' downloaden bij www.gpg4win.org en de installatie is zo simpel dat deze geen verdere uitleg nodig heeft. Accepteer de standaards.

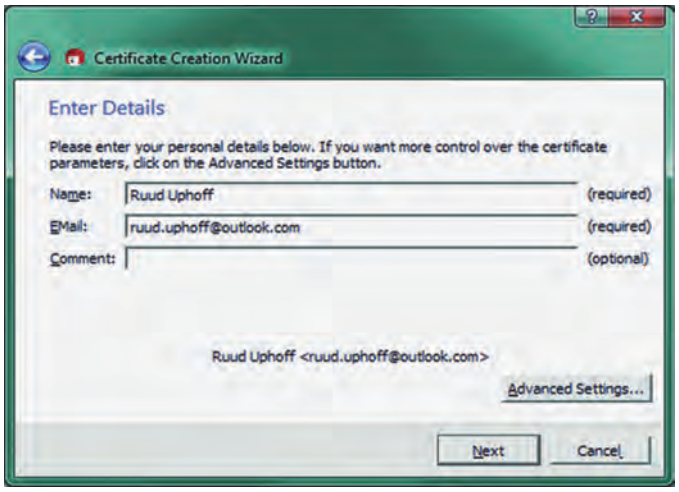
Beknopt overzicht
In het kort werkt het geheel als volgt: je maakt een persoonlijk sleutelpaar aan. Daarmee kun je om te beginnen een document elektronisch waarmerken. De ontvanger van het document ziet daardoor niet alleen dat het document met zekerheid van jou afkomstig is, maar beschikt nu ook over jouw publieke sleutel. Maakt hij nu zelf ook een sleutelpaar aan, dan kunnen jullie strikt geheim documenten uitwisselen.

Na installatie codeer je een bestand door erop te klikken met de rechter muisknop en onder Windows te kiezen voor *Sign & encrypt*. Onder Linuxdistributies zijn soortgelijke opties te vinden. Het decoderen van een ontvangen bestand is ook weer een kwestie van de rechter muisknop. Verderop meer details.
Het gecodeerde bestand wordt naar de geadresseerden gezonden; langs welke weg is niet relevant: kies maar!

Een sleutelpaar aanmaken.

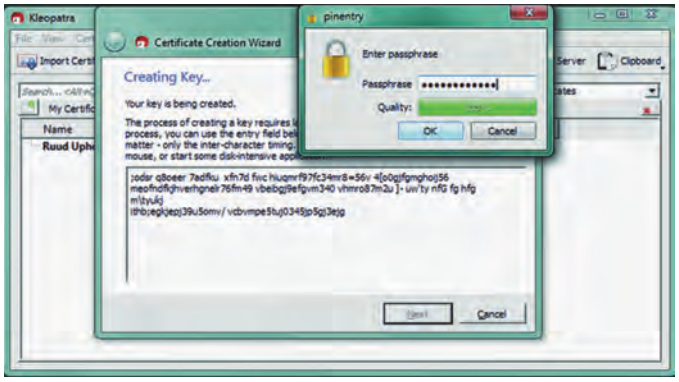
Het aanmaken van je eigen sleutelpaar is een vrij simpele kwestie. Start *Kleopatra*.
Kies *File ==> New Certificate*.
Er wordt gevraagd het type certificaat te kiezen.
Kies altijd voor *Create a personal OpenPGP key pair* (fig. 1).
Klik daarna op *Next*.

Figuur 1



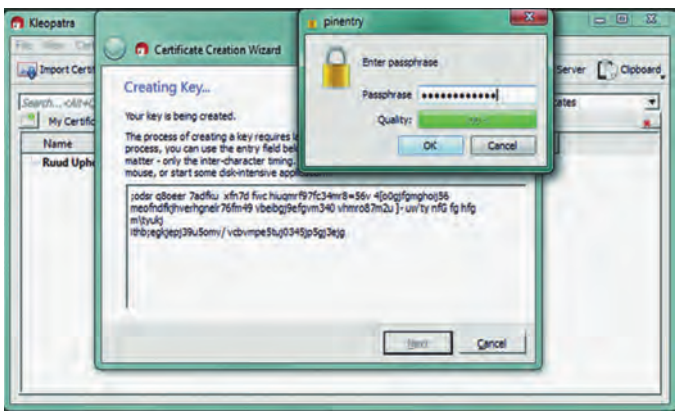
Figuur 2

Er wordt je nu gevraagd je naam en e-mailadres in te vullen (*Figuur 2)*. Bedenk dat anderen je onder die naam moeten kennen, dus gebruik geen mistig pseudoniem! Het sleutelpaar moet jouw identiteit kunnen bevestigen. De knop *Advanced settings* kun je gebruiken als je een strengere encryptie dan de standaard 2048 bits wilt, of een geldigheidsduur wilt instellen. Normaal is het sleutelpaar onbeperkt geldig. Heel belangrijk is de volgende stap, waarin je *figuur 3* te zien krijgt.



Figuur 3

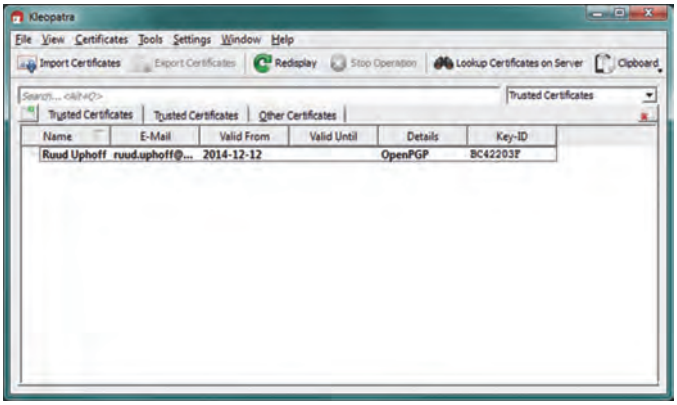
Vul nog geen *passphrase* in, maar schuif het venstertje waarin je dat moet doen even opzij, zoals de figuur toont! We moeten het namelijk eerst NSA en andere 'Big Brothers' zo moeilijk mogelijk maken. Dat doen we door in het grote vlak een bulk willekeurige tekens in te typen. Het best laat je je kat even over het toetsenbord lopen. Het moet willekeurige troep zijn. Vul pas daarna de *passphrase* in. Er is nu een afwijkende initialisering van de randomgenerator gebruikt waar NSA niet blij mee is.
Figuur 5 toont het resultaat. Vanaf nu kun je met de rechter muisknop op een document klikken en dat document vercijferen. Je moet dan een of meer geadresseerden selecteren in het scherm van Kleopatra dat dan verschijnt.



Figuur 4

Als je een publieke sleutel ontvangt.

Een publieke sleutel ontvang je als platte tekst, normaliter als *.asc-bestand. Je opent dan Kleopatra en klikt in *figuur 5* op *Import Certificates*. Blader naar het bestandje en je kunt deze persoon vercijferde documenten sturen.



Figuur 5

Enigmail. Integratie in Thunderbird.

Voor de zoveelste keer moet ik een lans breken voor het enige echte mailprogramma. Dat is met stip nog steeds Thunderbird! Er is over het ontwerp echt nagedacht. Het is zo flexibel dat ik onder Linux dezelfde datamap gebruik als onder Windows, want de hele database is puur platte tekst. De dataopslag van Thunderbird is volledig systeemonafhankelijk en een ander sterk punt zijn de uitbreidingen die je kunt installeren. Een van deze uitbreidingen heet *Enigmail*.

Klik in Thunderbird op *Extra* ==> *Add-ons* en ga naar tabblad *Add-ons verkrijgen*. Als je *Enigmail* in het zoekvakje typt, verschijnt ie meteen bovenaan. Je kunt nu gecodeerde berichten verzenden en ontvangen, waarbij Thunderbird gebruik maakt van GnuPG.
Na de installatie heeft de menubalk van Thunderbird een extra item *Enigmail* gekregen. Klik erop en kies Instellingen Wizard. Je moet een aantal vragen beantwoorden:

Scherm 1. Kies *Ja, ik wil dat de me op weg helpt*.
Scherm 2. Kies *Ik wil Enigmail alleen instellen voor de volgende identiteiten*: Zorg dat je alleen accounts selecteert waarvoor je een sleutelpaar hebt gemaakt of nog zult maken.
Scherm 3. Kies *Versleutel mijn bestanden niet standaard*.
Scherm 4: Kies *Onderteken mijn berichten niet standaard*. Als je standaard ondertekent, zijn er gegarandeerd mensen die je bericht wantrouwend bekijken omdat er een verdachte bijlage aan hangt. Met name als het bericht wordt gelezen met zoiets als Windows Live Mail.
Scherm 5. Kies *Ja*. Klik dan op de knop *Details*.... en zet voorlopig alle vinkjes uit. Anders ben je slachtoffer van purisme uit de wereld van de Linux-boys. Berichten verzenden en ontvangen in uitsluitend platte tekst is echt niet meer van deze tijd. Nadeel is dat je een bericht niet rechtstreeks vanuit Thunderbird gedecodeerd kunt opslaan.
Scherm 6. Kies je sleutelpaar of maak hier een nieuw paar aan. Een nieuw paar aanmaken doe je echter bij voorkeur met Kleopatra.
Scherm 7. Controleer of alles naar wens is.

Enigmail is nu prima bruikbaar.

Lees ook de (Nederlandstalige) help!