TITEL

gpg_5_min – GnuPG in 5 minuten

INHOUDSOPGAVE

1..... **Inleiding**
1.1..... Wat is dit voor een tekst?
1.2..... Waarom zou ik GnuPG gebruiken?
1.3..... Dit lijkt me niks, kan het niet op een andere manier?
1.4..... OK, ik wil met GnuPG gaan werken. Wat nu?

2..... **Installatie**
2.1..... Hoe installeer ik PGP software?
2.2..... Genereer een PGP/GnuPG key
2.3..... Wat is een keypair eigenlijk?
2.4..... Hoe vertel ik mijn e-mailprogramma dat ie GnuPG moet gebruiken?

3..... **Keysigning**
3.1..... Publiceer het publieke deel van je keypair
3.2..... Wat moet ik doen zodat iemand anders mijn key kan signen?
3.3..... Hoe sign ik een key van iemand Anders?
3.4..... Ik heb deelgenomen aan een PGP Keysigning Party. Wat nu?
3.5..... Hoe werkt het Web of Trust? Wat heb ik eraan?
3.6..... Hoe kan ik meehelpen aan het Web of Trust?

4..... **Gebruik van GnuPG**
4.1..... Hoe kan ik nu veilig e-mailen?
4.2..... Maar ik kan GnuPG toch ook gebruiken voor het versleutelen van bestanden?

5..... **En verder?**
5.1..... Maar dit is niet alle informatie over GnuPG, wel? Noem eens wat externe links!
5.2..... Heb je misschien nog wat specifieke tips?

FAQ

Inleiding

1.1 Wat is dit voor een tekst?

Deze tekst gaat over GnuPG en andere PGP software. Het is een zeer minimale inleiding: de bedoeling is dat je zo snel mogelijk die software kunt gebruiken. Aan het eind staat een lijstje van meer uitgebreide documenten. Lees die als je meer over technische details, of over de achterliggende beveiligsaspecten wilt weten. En besef: GnuPG is slechts een instrument, echte veiligheid en zekerheid is alleen mogelijk als je weet wat je aan het doen bent. Het lezen van meer uitgebreide documentatie kan daar natuurlijk bij helpen.

Er wordt van je verondersteld dat je in staat bent software op je computer te installeren (je weet wat een "binary" is), en dat je om weet te gaan met e-mail. De meeste voorbeelden gaan ervan uit dat je het GnuPG programma op de commandline gebruikt. Voor MS Windows gebruikers ziet dat eruit als DOS. Echter: vrijwel alles wat voorgedaan wordt kan ook met grafische programma's gedaan worden. Hoe dat precies moet staat beschreven in de documentatie waar dit document naar zal verwijzen.

Deze tekst wordt bijgehouden en gepubliceerd op http://mdcc.cx/gnupg/. Werk aan de tekst is begonnen op de mailinglijst van LOSC Breda, in oktober 2003.

1.2 Waarom zou ik GnuPG gebruiken?

Als je GnuPG gebruikt, kun je met andere mensen (die ook GnuPG of een vergelijkbaar PGP programma gebruiken) veilig e-mailen. Jouw e-mail kan alleen door de geadresseerde gelezen worden; niemand kan je e-mailverkeer dus afluisteren. Verder is de geadresseerde er zeker van dat het bericht echt van jou afkomt. Voor e-mail van anderen naar jou geldt hetzelfde.

Normale e-mail garandeert je zoiets niet. Het is in het bijzonder erg eenvoudig mailtjes te sturen met vervalste afzender.

1.3 Dit lijkt me niks, kan het niet op een andere manier?

Er zijn alternatieven voor GnuPG die ongeveer dezelfde functionaliteit leveren.

Je hoeft geen GnuPG of andere PGP-implementatie te gebruiken: S/MIME via bijvoorbeeld *CAcert* levert ook autenticatie en vertrouwelijkheid. Sommigen zeggen dat dit systeem minder leertijd vergen. Anderzijds zou het kunnen dat deze manier van werken je meer afhankelijk maakt van 1 centrale

Dit document suggereert dat je je e-mailprogramma aanpast om PGP te gebruiken. Je kunt het PGP-werk echter ook buiten je e-mailprogramma laten doen. De *GNU Anubis* software maakt dat mogelijk. GNU Anubis kan handig zijn als het moeilijk is je e-mailsoftware aan te passen voor PGP. Een ander pakket dat ongeveer hetzelfde doet voor MS Windows is *GPGrelay* van Andreas John.

Uiteraard geldt: kies zelf uit welke manier jou het beste bevalt.

1.4 OK, ik wil met GnuPG gaan werken. Wat nu?

Je moet zes dingen doen:

1 Installeer GnuPG of andere vergelijkbare software (zie de *Installatie* sectie hierover)
2 Genereer een keypair voor jezelf (zie de *''Genereer een PGP/GnuPG key''* paragraaf daarover)
3 Maak het publieke deel van je key bekend (zie de paragraaf *''Publiceer het publieke deel van je keypair''*)
4 Zorg dat je e-mailprogramma met GnuPG kan omgaan (zie de vraag *''Hoe vertel ik mijn e-mailprogramma dat ie GnuPG moet gebruiken?''*)
5 Sign keys van de mensen waarmee je communiceert, vraag of die mensen jouw key willen signen, werk aan het Web of Trust (zie de *sectie over Keysigning*)
6 Ga veilig e-mailen (zie de vraag *''Hoe kan ik nu veilig e-mailen?''*)

Hieronder worden die dingen uitgelegd.

Installatie

2.1 Hoe installeer ik PGP software?

Als je het Debian of Ubuntu GNU/Linux besturingssysteem gebruikt, is het redelijk eenvoudig. Installeer het pakket "gnupg" met een pakketbeheerder zoals *synaptic*, of voer dit commando uit:

```
# aptitude update && aptitude install gnupg
```

Voor ander GNU/Linux distributies zul je dit op een andere manier moeten doen; voor Gentoo Linux ziet het er bijvoorbeeld uit als `emerge --sync && emerge gnupg`. (Deze commando's moet je als root uitvoeren; dat kun je zien omdat er een # voor staat. Commando's die

je onder je normale gebruikers-account uitvoert worden door een $ vooraf gegaan.)

Voor vrijwel alle andere GNU/Linux en BSD distributies zijn er gnupg packages beschikbaar. Ook op andere besturingsystemen (Mac OS X bijvoorbeeld) werkt GnuPG, zie http://www.gnupg.org/download/supported_systems.html.

Mensen die Microsoft Windows gebruiken, kunnen een .zip bestand met gnupg binary van ftp://ftp.gnupg.org/gcrypt/binary/ halen. Zie http://www.gnupg.org/download/ .

2.2 Genereer een PGP/GnuPG key

Er zijn verschillende smaken van keypairs. Sommige mensen gebruiken keys met subkeys. Hoe je zoiets maakt kun je lezen in de *handleiding voor PGP keys met subkeys* door Guus Sliepen e.a. Hier zullen we de traditionele en eenvoudigere manier laten zien. Zorg eerst dat de klok van je PC goed staat. GnuPG wil nogal eens lastig doen als er rare tijden of datums in je key staan. Genereer dan een keypair voor jezelf:

```
$ gpg --gen-key
```

of, onder Microsoft Windows:

```
c:> \pad\naar\gpg --gen-key
```

Er worden verschillende vragen gesteld. De standaard antwoorden zijn bijna altijd goed. Kies een veilige passphrase (op dezelfde manier waarop je een veilig password kiest). NB: tijdens het geven van je passphrase zal er niks op je scherm verschijnen; er zullen geen sterretjes weergegeven worden.

Genereer verder een revocation certificate:

```
$ gpg --gen-revoke jouwemailadres
```

Print de regels tussen

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

en

```
-----END PGP PUBLIC KEY BLOCK-----
```

op een briefje, en berg dat veilig op. Je hebt dit briefje nodig als onverhoopt iemand je keypair steelt. (Je kunt de regels ook in een bestand zetten, dat op een CD branden en de CD veilig opbergen.)

2.3 Wat is een keypair eigenlijk?

Het keypair dat met `gpg --gen-key` gegenereerd is, bestaat uit twee delen: een publiek en een geheim deel. Het publieke deel is in `~/.gnupg/pubring.gpg` gezet, het geheime deel in `~/.gnupg/secring.gpg`. Zorg dat andere mensen het geheime bestand nooit kunnen lezen. Zorg dus dat de computer waarop je zulke bestanden bewaart, *goed beveiligd* is.

2.4 Hoe vertel ik mijn e-mailprogramma dat ie GnuPG moet gebruiken?

Je e-mailprogramma moet verschillende dingen mogelijk maken:

- E-mail met jouw digitale handtekening eronder (ge-sign-de e-mail), versturen.
- Versleutelde (encrypted) e-mail versturen. De versleuteling moet alleen door de geadresseerde ontcijferd kunnen worden.
- Verifiëren of ontvangen en ge-sign-de e-mail echt door de afzender getekend is, en aangeven of de key van de afzender te vertrouwen is.
- E-mail die versleuteld is voor jou, kunnen ontcijferen.

Als je voor je e-mail mutt gebruikt op Debian GNU/Linux of Ubuntu, dan heb je geluk: het werkt gewoon; de functies voor het signen en encrypten van e-mail zitten onder de ‘‘p’’. Bij het openen van ondertekende e-mail wordt meteen aangegeven of de handtekening klopt, en of die door jou te vertrouwen is. Bij het openen van versleutelde e-mail, wordt meteen begonnen met ontcijfering.

Als je de *Mozilla* mailer of *Mozilla Thunderbird* gebruikt (onder GNU/Linux, Unix of Microsoft Windows), dan kun je enigmail gebruiken als lijmlaag tussen je e-mailprogramma en GnuPG. Zie de enigmail website op http://enigmail.mozdev.org/ voor informatie. Een Nederlandse handleiding voor mensen die Enigmail onder MS Windows gebruiken staat op deze *Enigmail handleiding van Tjaard de Vries*. (NB: Ik heb geen goede Nederlandstalige site met hulp voor GNU/Linux gebruikers van Enigmail kunnen vinden. Het zou mooi zijn als de *Enigmail Quick Start Guide* ook naar het *Nederlands vertaald* werd.)

Ook Gnome’s *Evolution* (voor GNU/Linux en andere Unix-achtigen) heeft goede support voor GnuPG.

Voor andere e-mailprogramma’s en besturingssystemen zul je zelf wat onderzoek moeten doen. Een goede start is http://gnupg.org/related_software/frontends.html#mua. Een prima handleiding voor MS Windows gebruikers staat op http://drcwww.uvt.nl/~robert/gnupg/gnupg-windows.txt.

Keysigning

3.1 Publiceer het publieke deel van je keypair

Upload het publieke deel van je key naar een keyserver:

```
$ gpg --keyserver=subkeys.pgp.net --send-key jouwkeyID
```

Je kunt achterhalen wat het key ID van jouw key is, door het commando

```
$ gpg --list-keys jouwemailadres
```

te geven. De eerste regel die je dan ziet, zal eruit zien als bijvoorbeeld

```
pub   1024D/969457F0 2000-01-28 [expires: 2035-01-22]
```

De code achter de / is je key ID. In dit geval zou je dus uitvoeren

```
$ gpg --keyserver=subkeys.pgp.net --send-key 969457F0
```

Je kunt ook een andere keyserver dan subkeys.pgp.net gebruiken; pgp.surfnet.nl bijvoorbeeld. Het maakt niet zoveel uit welke je gebruikt: de verschillende OpenPGP servers copiëren geregeld de data van elkaar.

Als je *echt* een *nog* andere keyserver wilt proberen, kun je de lijst van keyservers op http://www.gurski.org/~gurski/keys/keyservers raadplegen.

3.2 Wat moet ik doen zodat iemand anders mijn key kan signen?

De meest gangbare methode om je key gesigned te krijgen is om degene die je key wil signen in levende lijve te ontmoeten. Als die persoon niet helemaal absoluut zeker is dat je bent wie je zegt dat je bent, dan overtuig je die persoon daarvan, bijvoorbeeld door je paspoort of rijbewijs te laten zien. Verder geef je de fingerprint van je publieke key aan die persoon. Dat kun je doen door die op een briefje te printen, en dat briefje te geven. Zo'n briefje - ook wel een keyslip geheten - kun je maken door

```
$ gpg --fingerprint jouwemailadres | lpr
```

te doen. Op zo'n briefje staat dan iets als

```
pub  1024D/88C6EDF6 2002-11-04 Joost van Baal <j.e.vanbaal@example.com>
     Key fingerprint = 7177 F40B 051B 5793 8A0B  E219 5F76 E17A 88C6 EDF6
uid                            Joost van Baal <joostvb@example.com>
sub  1024g/450B4EE8 2002-11-04 [expires: 2035-05-01]
```

Je kunt ook het script *gpg-key2ps* gebruiken (als je Debian of Ubuntu gebruikt, te verkrijgen via het `signing-party` Debian pakket) om een A4 met keyslips te maken in PostScript formaat:

```
$ gpg-key2ps jouwemailadres > keyslips.ps
```

3.3 Hoe sign ik een key van iemand Anders?

Ontmoet Ander, en verifieer of die echt Ander is. Vraag haar om haar key fingerprint. Zorg dat je die op papier hebt, of sla de fingerprint die Ander je gaf op, op b.v. je laptop. Als de eerste regel van de keyslip van de Ander er uit ziet als

```
pub  1024D/88C6EDF6 2002-11-04 Joost van Baal <j.e.vanbaal@example.com>
```

dan is de ''keyid'' van de ander `88C6EDF6`. Ga naar huis. Als je geen reden hebt om aan te nemen dat Ander slecht met haar private key omgaat, dan kun je daarna haar key signen. Zie daarvoor de *volgende sectie*.

3.4 Ik heb deelgenomen aan een PGP Keysigning Party. Wat nu?

Als je deelgenomen hebt aan een PGP Keysigning Party, dan heb je nu waarschijnlijk een stapel briefjes met key fingerprints. Als het goed is heb je op de bijeenkomst geverifiëerd of die fingerprints echt van de personen zijn waarvan ze claimen te zijn. Je kunt dan nu die keys gaan signen.

Voor iedere keyslip voer je daarvoor het volgende uit. Download eerst de key:

```
$ gpg --keyserver=subkeys.pgp.net --recv-key keyidvanander
```

(Je kunt trouwens ook zonder een keyid te gebruiken naar de public key van de Ander zoeken door

```
$ gpg --keyserver=subkeys.pgp.net --search-key "Naam van de Ander"
```

te doen.)

Sign daarna de key:

```
$ gpg --sign-key keyidvanander
[...]
 [ unknown] (1). Iemand Anders <ander@example.com>
 [ unknown] (2)  Iemand Anders <i.m.anders@example.com>
Really sign all user IDs? (y/N)
```

Als alle user IDs van dezelfde naam voorzien zijn, kies dan "y".

```
Vingerafdruk van de primaire sleutel: 7177 F40B 051B 5793 8A0B  E219 5F76 E17A 88C6 E
 Iemand Anders <ander@example.com>
 Iemand Anders <i.m.anders@example.com>
Weet u zeker dat U deze sleutel wilt ondertekenen met Uw sleutel
 Joost van Baal <j.e.vanbaal@example.com> (88C6EDF6)
Really sign? (y/N)
```

Check nu of de fingerprint die gpg je toont echt dezelfde is als op de keyslip staat. Als dat zo is, kies dan "y". Geef daarna de passphrase van je eigen key. De key van Ander is dan gesigned met jouw key.

Daarna kun je de gesignde key uploaden op het OpenPGP keyserver netwerk door te doen

```
$ gpg --keyserver=subkeys.pgp.net --send-key keyidvanander
```

. En je kunt Ander een mailtje sturen, waarin je schrijft dat je haar key hebt ge-upload.

N.B.: er zijn mensen die liever niet hebben dat je jouw signature op hun key zelf upload. Als je netjes wilt zijn, doe je dat dus niet, maar mail je de gesignde key naar die mensen. De gesignde key kun je in een bestandje opslaan (dat je daarna kunt mailen), door uit te voeren:

```
$ gpg --export --armor keyidvanander >signedkey.asc
```

Zie verder overigens de opmerking over "caff" in de *sectie met externe links* voor nog een andere manier om te signen.

Waarschijnlijk zullen de andere deelnemers van de party jouw key gaan signen. Daarvoor hoef je in het algemeen verder niks te doen. Na een paar dagen kun je eventueel

```
$ gpg --recv-key jouwkeyid
```

doen, om de signatures van de anderen op jouw key te downloaden.

3.5 Hoe werkt het Web of Trust? Wat heb ik eraan?

PGP software wordt o.a. veel gebruikt door Vrije Software ontwikkelaars, die samenwerken met mensen die ze nooit in levende lijve ontmoet hebben. Om toch enigszins zeker te zijn over de identiteit van je collega in Nieuw Zeeland, is het handig om GnuPG te gebruiken. Stel nu dat Hans in Nederland samen wil werken met Anne in Nieuw Zeeland, voor een project. Het project heeft echter geen budget om vliegreizen naar Nieuw Zeeland te betalen. Nu is het zo dat Anne een nicht in Duitsland heeft: Gisela. Met kerstmis ontmoeten Anne en Gisela elkaar, ze sign-en elkaars GnuPG keys. Jij ontmoet Gisela op een conferentie, en daar is een keysigning party. Omdat je dit document gelezen hebt, doe je natuurlijk mee aan die party. Wanneer je nu een versleuteld en ondertekend mailtje van je collega Anne krijgt, zie je dat Gisela de key van Anne gesigned heeft. Omdat jij zeker weet dat de key van Gisela van Gisela is (jij hebt die immers gesigned), en omdat je het gevoel hebt dat Gisela wel verstand van zaken heeft wat betreft

keysigning (je hebt haar bezig gezien op de conferentie), kun je er wel vanuit gaan dat Gisela's signature op de key van Anne waarde heeft. Het is dus waarschijnlijk dat de key van Anne echt van Anne is.

(Het Web of Trust krijgt een lek als een key gecompromiteerd raakt zonder dat die revoked wordt! Stel dat Boef de geheime sleutel van Anne steelt (of Anne vergist zich in het gebruik van PGP, en geeft haar geheime sleutel aan Boef). Toen Gisela de key van Anne sign-de, kon zij niet nagaan hoe goed Anne met haar geheime sleutel omsprong. (Dit kan zelfs bijna nooit, in het algemeen.) Gisela kon alleen verifiëren dat Anne echt Anne is. Wanneer Boef de geheime sleutel van Anne te pakken heeft gekregen, kan het versleutelde en ondertekende mailtje dus van Boef komen, in plaats van van Anne!)

Omdat ook jij mogelijk de rol van Gisela kunt spelen voor anderen, is het fijn voor anderen als jij veel keys sign-t. Het is ook fijn voor anderen als je veel mensen de mogelijkheid geeft jouw key te sign-en. En, als je dit veel doet, dan heb je meer kans dat er voor jou een "Gisela" is als je die nodig hebt bij de communicatie met een "Anne".

3.6 Hoe kan ik meehelpen aan het Web of Trust?

Ik wil wel meehelpen. Maar waar zijn die conferentie's dan? Of zijn er ook andere manieren om mensen te ontmoeten die hun key gesigned willen hebben?

Lijsten van mensen die geïnteresseerd zijn in keysigning zijn o.a. te vinden op http://www.biglumber.com/x/web?va=1 en http://nm.debian.org/gpg.php . Je kunt jezelf daar ook opgeven.

Gebruik van GnuPG

4.1 Hoe kan ik nu veilig e-mailen?

Hoe je nu veilig kunt e-mailen, hangt nogal af van het e-mailprogramma dat je gebruikt. Voorlopig zul je de documentatie die je bij je e-mailprogramma kreeg moeten bekijken: dit hoofdstuk is nog niet geschreven. Ook het stukje over *Hoe vertel ik mijn e-mailprogramma dat ie GnuPG moet gebruiken?* kan je misschien op weg helpen. Uiteraard geldt: de auteur is blij met jouw bijdrage, en met relevante links.

4.2 Maar ik kan GnuPG toch ook gebruiken voor het versleutelen van bestanden?

GnuPG kan niet alleen voor e-mail gebruikt worden, maar ook voor het ondertekenen en versleutelen van bestanden. Dat doe je als volgt.

Versleutel en onderteken een bestand zodat alleen jij het nog kunt ontcijferen:

```
$ gpg -se bestand
```

Het is aan te raden om bestanden die je versleutelt, altijd *ook* te ondertekenen. Op die manier weet je zeker dat de inhoud van het bestand niet stiekem gewijzigd is.

Het versleutelde bestand zal opgeslaan zijn onder de naam bestand.gpg. Dat versleutelde bestand zal niet-ascii-karakters bevatten. Vaak is het handig als zo'n bestand zonder problemen in een terminal te openen is, en eenvoudig per e-mail te versturen is. Geef in dat geval de optie "-a" (ofwel "--armor") mee aan gpg. In dat geval ziet het versleutelde bestand eruit als:

```
 -----BEGIN PGP MESSAGE-----
 Version: GnuPG v1.4.9 (GNU/Linux)

 hQEOA46mUF8VzrWeEAQAns0J32CTYyk70sufV6Gymi9ai+9XCQQZr9/kjG6HEIzF
[...]
 ycr4f7pR41Sac9SYSOTfi/SMylZ+v5lbbD2gEzZxmmHNTHw3Dkv6opfoYw==
 =vOZ+
 -----END PGP MESSAGE-----
```

Zo'n bestand zal opgeslagen worden onder de naam bestand.asc.

Versleutel en onderteken een bestand zodat alleen Ander (of jij) het nog kunt ontcijferen:

```
 $ gpg -se -r Ander bestand
```

N.B.: dit is *alleen* zinvol als je zeker weet dat de sleutel van Ander echt alleen van Ander is! Zie de *sectie over Keysigning*.

Ontcijfer een bestand

```
 $ gpg bestand.gpg
```

Als het bestand ook ondertekend is, zal een melding over de geldigheid en betrouwbaarheid van de ondertekening gemeld worden.

Je kunt een bestand trouwens ook versleutelen voor meer dan 1 ontvanger:

```
 $ gpg -se -r Ander -r Nogeenander -r Ennogeen bestand
```

En verder?

5.1 Maar dit is niet alle informatie over GnuPG, wel? Noem eens wat externe links!

Dit is zeker niet alle informatie! En er zijn in dit stuk dingen over GnuPG niet behandeld, die toch wel belangrijk zijn. Het is dus zeker zinvol er meer over te lezen. Zoals eerder gezegd: GnuPG is slechts een instrument; echte veiligheid en zekerheid is alleen mogelijk als je weet wat je aan het doen bent.

Eerst een lijstje met algemene documentatie, en websites:

- Het *Wikipedia* artikel over PGP, met ook informatie over andere PGP programma's dan GnuPG, en informatie over de geschiedenis van PGP: http://en.wikipedia.org/wiki/PGP. (Het *Nederlandse artikel* over PGP is helaas minder uitgebreid. Je kunt *helpen*!) Daarnaast is er een goed Duitstalig Wiki Books boek op http://de.wikibooks.org/wiki/GnuPG beschikbaar.
- Nederlandstalige introductie, met meer aandacht voor de technische achtergrond: GnuPG Mini Howto op http://www.dewinter.com/gnupg_howto/dutch/GPGMiniHowto.html.
- De GnuPG Gentoo Gebruikersgids: http://www.gentoo.org/doc/nl/gnupg-user.xml, een Nederlandse vertaling van de *GnuPG Gentoo User Guide*. Een algemene inleiding in GnuPG, met o.a. ook een beschrijving van Kgpg, een grafisch interface voor GnuPG. (Lees ook het Engelse origineel; in oktober 2008 was de vertaling niet helemaal up to date.)
- *The GNU Privacy Handbook* op http://www.gnupg.org/gph/en/manual.html. Zeer uitgebreid.
- GnuPG, The Gnu Privacy Guard: http://gnupg.org/. Met uitgebreide lijst van plugins en

frontends: http://www.gnupg.org/related_software/frontends.html.
- PGP & GPG -- Email for the Practical Paranoid, een (Engelstalig) boek van *Michael W. Lucas*, uitgegeven in april 2006 door *No Starch Press*; ISBN: 1-59327-071-2.
- De PGP Users mailing lijst: http://www.cryptorights.org/lists/pgp-users/. Hier kun je terecht met vragen over het gebruik van GnuPG en andere PGP software. Engelstalig.
- "A Practical Introduction to GNU Privacy Guard in Windows" door *Brendan Kidwell* op http://www.glump.net/dokuwiki/gpg/gpg_intro.

Over keysigning parties:

- Een beknopt document over keysigning, dat in het bijzonder meer aandacht besteed aan de noodzaak van serieus omgaan met het web of trust: http://www.debian.org/events/keysigning.
- Een meer uitgebreid document, met bespreking van de achtergronden van deze parties, is *GnuPG Keysigning Party HOWTO*, door *V. Alex Brennen* op http://www.cryptnet.net/fdp/crypto/. Dit document is ook in (veel) vertalingen beschikbaar.
- Het *signing-party Debian package* bevat een stel handige scriptjes om het papierwerk voor en na een party af te handelen.
- De *Fingerprint Cards* webapplicatie, door *James Moore*, genereert een pdf met kleine kaartjes met je PGP fingerprint en een foto; handig voor keysigning parties.
- *Efficient Group Key Signing Method*, een methode om keysigning party's te organiseren.

Over analyze van het Web of Trust:

- http://dtype.org/keyanalyze/
- http://pgp.cs.uu.nl/ Henk Penning's PGP pagina's, met http://pgp.cs.uu.nl/doc/top_1000.html: top 1000 van "best connected keys". Ook heel leuk zijn de statistieken per key, b.v. *deze (van mijn key)* en de plaatjes van ranking per key over de tijd, b.v. *deze (van mijn andere key)*;
- http://the.earth.li/~noodles/pathfind.html
- http://www.biglumber.com/x/web
- http://www.lysator.liu.se/~jc/wotsap/ (met mooie plaatjes)

In deze FAQ schrijven we dat je alleen de naam van degene van wie je de key tekent, verifieert. Je kunt echter ook de e-mailadressen die aan de key hangen verifiëren. Software die dat mogelijk maakt is caff (CA - fire and forget) op http://pgp-tools.alioth.debian.org/. (Ik denk dat Skami op http://alioth.debian.org/projects/skami inmiddels verouderd is; er was geen activiteit tussen 2005-07 en 2008-10.)

5.2 Heb je misschien nog wat specifieke tips?

Twee tips: eentje over manieren om keys te verifiëren, en eentje over key revocation.

In dit document gaan we ervan uit dat je Ander ontmoet voordat je haar key sign-t. Er is ook een andere manier om de fingerprint van Ander over een veilig kanaal te ontvangen, en de identiteit van Ander te verifiëren: vraag aan Ander dit:

- Stuur 1 cent van jouw persoonlijke bankrekening naar mijn bankrekening;
- Geef je e-mailadres en key fingerprint in het omschrijvingsveld;
- Stuur me een e-mailtje met bericht dat je de overboeking hebt gemaakt.

Als er te weinig ruimte is voor de hele fingerprint in het omschrijvingsveld, vraag dan om zoveel mogelijk van de laatste karakters van de fingerprint (of vraag om 2 overboekingen om alle informatie over de lijn te krijgen). Als Ander dat allemaal gedaan heeft, kun je de key van Ander

tekenen. (Met dank aan *Folkert van Heusden* voor deze tip.) Pas echter op: er zijn mensen met verstand van zaken die schrijven: *keysigning requires to meet in person for a reason*.

Key revocation: In de sectie *Genereer een PGP/GnuPG key* schreven we dat je een revocation certificate moest maken. Als je vermoedt dat iemand anders je private key gestolen heeft, dan kun je je key niet meer gebruiken. Die is dan immers niet meer van jou alleen. Ook anderen zul je op de hoogte moeten stellen dat jouw key niet meer te vertrouwen is. Dat doe je door je revocation certificate te publiceren. Wanneer mensen dan je key downloaden van het keyserver netwerk, zullen ze zien dat de key ongeldig is verklaard. (De key wordt niet verwijderd van het netwerk.)

Ga als volgt te werk: Zorg dat je revocation certificate in een bestand `revoce.asc` staat. Doe dan

```
$ gpg --import revoce.asc
```

(Je kunt controleren dat dit gelukt is: als je `gpg --list-key jouwemailadres` uitvoert, dan staat er bij je key het woord "revoked".) Publiceer je publieke key, waar nu het revocation certificate aan hangt, door

```
$ gpg --keyserver=subkeys.pgp.net --send-key keyidvanander
```

te doen.

DANK

Dank aan Juul, Marianne Driessen, Stijn, en Ton voor het proeflezen van deze tekst. Dank aan Arjan Broos, Ronald van Engelen, Rop Gonggrijp, Maarten Horden, Thijs Kinkhorst, Benedikt Kratz, Matthijs Langenberg, Virginie Moerenhout, Teun Nijssen, Aldo Plomp en Anton Sluijtman voor het geven van aanvullingen. Dank aan Lionel Elie Mamane voor het suggereren van Anubis. Dank aan Henk Penning voor het noemen van de PGP Wiki pagina. Dank aan Jack Raats voor het suggereren van GPGrelay. Dank aan Arvid Gibas voor het suggereren van de GnuPG Gentoo Gebruikersgids. Dank aan Bug Hunter.

VERSIE

Versie --.

COPYRIGHT

Copyright (C) 2003, 2004, 2005, 2006, 2007, 2008 Joost van Baal

Dit document is vrije software; je kunt het verspreiden en/of wijzigen onder de bepalingen van de GNU Algemene Publieke Licentie, zoals uitgegeven door de Free Software Foundation; oftewel versie 2 van de Licentie, of (naar vrije keuze) een latere versie.

Dit document is verspreid in de hoop dat het nuttig zal zijn maar *zonder enige garantie*; zelfs zonder de impliciete garantie van *verkoopbaarheid of geschiktheid voor een bepaald doel*. Zie de GNU Algemene Publieke Licentie voor meer details.

Een kopie van de GNU Algemene Publieke Licentie is beschikbaar op http://www.gnu.org/copyleft/gpl.html en op aanvraag via de Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Broncode voor dit document is beschikbaar op http://mdcc.cx/gnupg/gpg_5_min.azm en wordt tegen kostprijs door *de auteur* beschikbaar gesteld.

AUTEUR

Joost van Baal <joostvb-gnupg-5-min@mdcc.cx>