

Berichten versleutelen en ondertekenen met PGP

Koos van den Hout

`mailto:koos@kzdoos.xs4all.nl`

HCC PCgg netwerkgroep 23 Mei 2009

1 Inhoud

- * Eventueel inleiding versleuteling
- * Korte geschiedenis van PGP
- * PGP in e-mail
- * Het verschil met s/mime

2 Inleiding versleuteling

* Private key / symmetrische versleuteling

Zelfde sleutel voor encryptie en decryptie

* Public key / assymetrische versleuteling

1976: Whitfield Diffie en Martin Hellman

3 Korte geschiedenis van PGP

1991 PGP 1.0 RSA en Bass-O-Matic

1992 PGP 2.0 RSA en IDEA

1993 Rechtszaak tegen Zimmerman

1994 PGP 2.62 US

1995 PGP 2.62i Internationaal

1996 Rechtszaak tegen Zimmerman gestopt

1997 PGP 5.0 DH keys

1997 PGP source als boek

1999 GnuPG geen IDEA meer, CAST5

4 PGP in e-mail

Versleutelen:

-----BEGIN PGP MESSAGE-----

Version: GnuPG v1.4.6 (GNU/Linux)

hQIOA4UBlZfNElorEAgA59SlTE20Q3Iq8KfnLfqm0BebchkFIQHZOTjeYDeQ+Tpj
8dyb72dFHZg76opmDjVIib9Q6kxjDCWjbMQFBV5i1I1ER+3WY/BnXmXklY4MBKWR
BI6uXF5pUoHjOFJBUR4sT/+TAW+zAZ86PY0erbWGXmGoLIAbifslxB4iPChKwfCN
KQfpG60Y00kvL+puDJ03YzCrV1Qjq+j/mMwm5wt+eAd3MNekH1qD41elu03SLrfa
4VqCaqJN+lp8oHym5iDsifDES9plTNRdHvVNsmpkDP0gy7Qdpr9z2ik6ydZw6WvG
iRcRUrpLdhsOFHEwMIKLQuhb9/KAbZ2NSgHQWYX72gf/dOvIeisGudJtpiwYV6bc
tR3L3kcjNaTbJb3MtLaSogfXJHsoXaUzBELODBoBVo0hmjb7Tlex36zIJWMT9DTR
m1V32yP/DRMDwak4Wfrq4/vtAWn0y2VVQ/2unIbFCQEBK7BRxaa0YqJnEcUm2e/T
zTuFHpRbng5NJgvu1Aeau2LmPVsAzT/C42MxrJ/ZzqHLBwl4lrJRczxHxpe+z/ZH
u8V0Ha8BYCg1eBHNAI+GGb/3Mz27n9MTprQYqeD3AFuaJ/6K82JUesip0AMfQviW
bqXCWSnqPbNCwTsFIqNEdTcb+XJkXbV2jv86Ah9oArLQHcPnyuKuhB/nF4Wt2Q+u
utJZAVRAwQHxrjjurYAZKGoDyQPdW4kL8Ths/4pcIWOeDJF8I8VvA5j1hMNHrVA7
rTfWv2mVrYdanIpW5CaHy0nJdMBIqAhkasgYawgSm+N5zeEUjtdLqD0Lv/c=
=R0Mo

-----END PGP MESSAGE-----

Ondertekenen:

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

test voor GnuPG

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.6 (GNU/Linux)

iD8DBQFKFt2kLGY7XfDXwmMRAisEAJ4yYTaeXOaissksXCFI0P6mWnbBXwCghk7/

NNmcMXwFLUyHSD0uuxTu8C8=

=3o2p

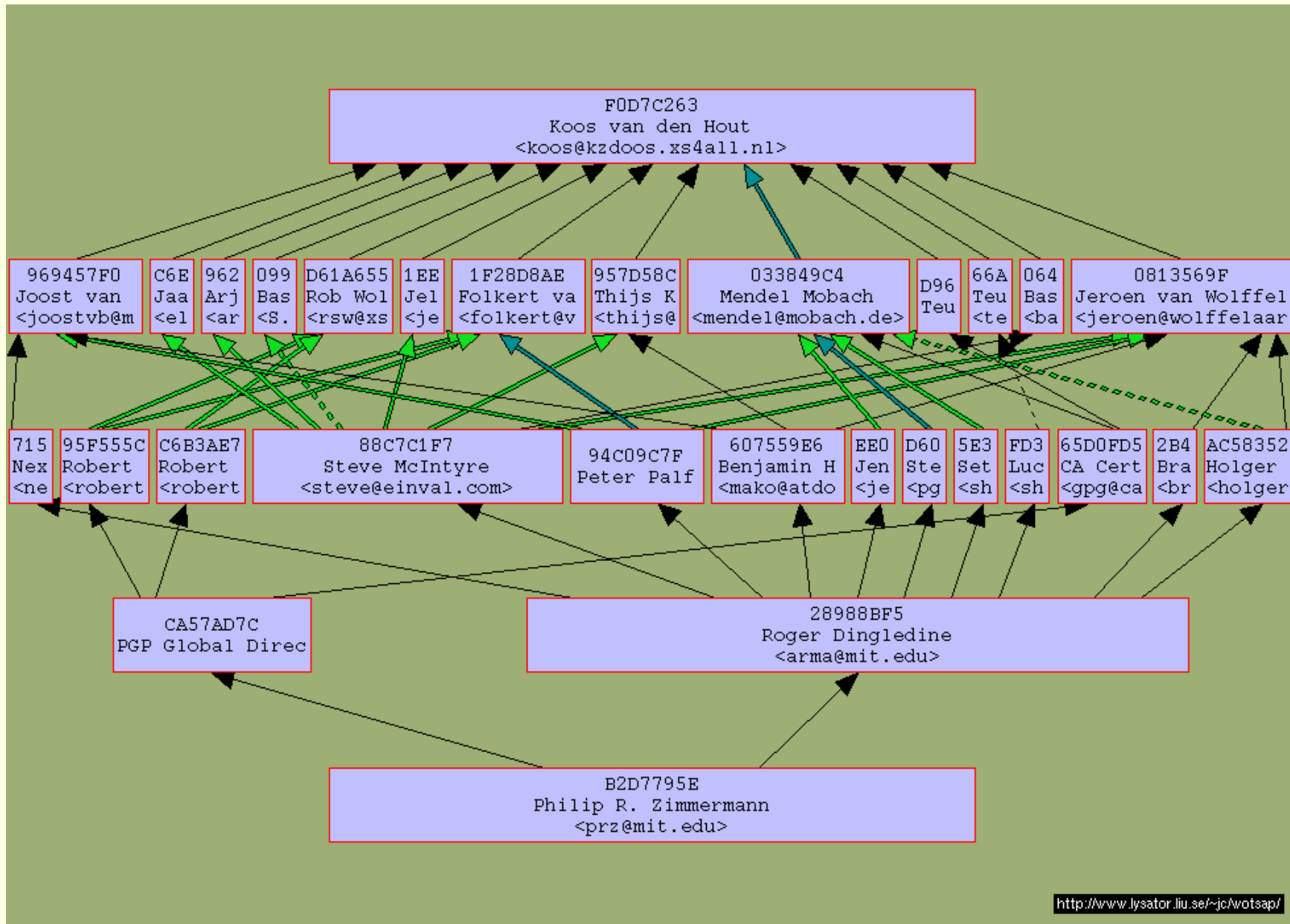
-----END PGP SIGNATURE-----

5 Het verschil met s/mime

* s/mime: tree of trust

Persoon - intermediate CA - root CA

* pgp: web of trust



http://www.pcgg.nl/

File Edit View History Bookmarks Tools Help Now: Partly Sunny, 17° C

http://www.pcgg.artbeeweb.nl/news.php ntp.xs4all.nl

madwifi diversity Stats wwwlinks urlurl omroep.nl/gids Homepage Koos va... Flickr: Photos from ...

WIGLE - Wireless Geographic Log... The Legendary Curry & van Inkel... Voipsolutions.be uw online shop... Doe mee ... met de PCgg: Nie...

hcc[!]pc

Netwerken[!]pc

Geachte Bezoeker,

[HIER] kunt u meer vinden over uw Webgroep - lidmaatschap.
[HIER] kunt u meer vinden over uw (algemene) lidmaatschap.
[HIER] kunt u meer vinden over uw PCgg Kern - lidmaatschap.

WIST U DAT...

wij het zeer op prijs stellen wanneer u uw mening over ons en onze website in het Gastenboek noteert?
Dan krijgen onze gasten bij hun eerste bezoek meteen een indruk.

6 oktober Open Dag Apeldoorn
Webmaster, vr 14 sep '07 - 10:24 // reactie: 0

PCgg en HCC Apeldoorn organiseren op 6 oktober een Open Dag.

10.00 zaal open voor publiek
10.30 presentatie Ms Vista backup / restore, door Eddy Huibers, PCgg
10.30 presentatie Ms Vista, door Deik Doeve, Windows gg
10.30 presentatie Digitale TV, door Giovanni Barbarino, Multi Media gg
13.30 presentatie Voip, Koos v/d Hout, PCgg
13.30 presentatie Ms Vista, door Deik Doeve, Windows gg
13.30 presentatie Digitale TV, door Giovanni Barbarino, Multi Media gg
16.00 ALV PCgg, met plan & begroting 2008

Web Wedstrijd 2007
Webmaster, zo 26 aug '07 - 10:14 // reactie: 0

U hebt het in het linkermenu wellicht al ontdekt: we zijn een Web Wedstrijd gestart, waarbij de kans op een prijs groter is bij eerdere deelname. Een extra reden tot registratie, en een goede reden om e diverse mogelijkheden op deze site eens te verkennen.

Vaste bezoekers van deze voopagina hebben dus een voorsprong, anderen worden de komende weken geïnformeerd via diverse mailings.

Voor meer details kunt u terecht in het Forum (Overzicht, web wedstrijd), of direct via de extra optie in het hoofdmenu.

We wensen u alvast succes,
Webmaster en PCgg best uur

Welkom Koos van den Hout

Instellingen
 Profiel
 Uitloggen

Weergroep Menu

Open | sluit het menu

- PCgg Start
- Agenda
- Routebeschrijving
- Nieuwste bijdragen
- Hoe kan ik... Reageren
- Elektronica
- Fotografie
- Grafisch
- Netwerken
- Video
- De Vereniging
- Website

Hoofdmenu

- Start
- WEDSTRIJD
- Nieuw(s)...
- Veelgestelde vragen
- Meer lezen...
- Verwijzingen
- Computer problemen?
- Discussie / Forum...
- Galerij
- Downloads...
- Gastenboek
- Website...
- Zoeken

Done