

Pentingnya Menggunakan GPG

Bicara soal keamanan data, ada baiknya kita mengambil sifat jaga-jaga. Itulah yang terbaik. Kita akan membahas tips dan penggunaan salah satu tool yang berguna untuk tugas jaga-jaga tersebut: gpg.

Suatu hari, katakanlah, Superman menerima sebuah dokumen OpenOffice.org dari Chinmi si Kungfu Boy. Isinya singkat saja. Intinya, Chinmi menantang Superman untuk duel, untuk membuktikan siapa yang lebih kuat: Superman atau Chinmi.

Sejenak, Superman terkejut. Superman telah mendengar tentang sifat-sifat Chinmi yang bertolak belakang dengan tantangan tersebut. Untunglah, Superman bukanlah tokoh yang cepat naik darah. Superman pun menghubungi Chinmi. Chinmi pun, setelah dikonfirmasi, mengatakan tidak pernah mengirim dokumen seperti itu. Untungnya, Superman rupanya mengerti. Keduanya memang sama-sama memiliki sifat yang baik dan cinta damai.

Asal muasal surat pun ditelusuri. Rupanya, si pengirim surat memang bukanlah Chinmi yang asli, melainkan orang lain yang berpura-pura menjadi Chinmi.

Dari skenario tersebut, kita bisa melihat bahwa dokumen merupakan sesuatu yang penting dan bisa memicu kesalahpahaman. Apabila disimpan dalam format OpenOffice.org misalnya, maka siapa saja bisa membuka dokumen tersebut dan mengintip isinya. Atau, seperti kasus Superman dan Chinmi tersebut, dokumen bisa dipalsukan dan seolah-olah dikirim dari orang lain.

Langkah pencegahan kedua kemungkinan tersebut sebenarnya tidak susah. Dokumen (yang akan dikirim) harus selalu dienkrip dengan sistem PKI (*Public Key Infrastructure*). Dalam sistem ini, seseorang akan memiliki satu pasang key: *public key* dan *private key*. Dari namanya saja, *public key* akan tersedia untuk public, sementara *private key* hanya dipegang dan diketahui oleh diri sendiri. Satu pasang key tersebut tidak dapat diselengi atau diserobot oleh teroris

misalnya. Dengan enkripsi sebesar 1024 bit, teorinya, key tersebut dapat didekrip selama lebih dari jutaan tahun.

Metode ini telah digunakan oleh banyak anggota komunitas open source. Contoh yang paling nyata adalah paket program yang Anda install. Apabila Anda mendownload RPM dari vendor distro Anda misalnya, maka pada saat instalasi, tidak akan ada pesan bahwa key tidak ditemukan. Sementara, apabila Anda mendownload paket yang tidak jelas, pada saat instalasi, pesan bahwa key tidak dikenal akan ditampilkan. Saat ini, hal seperti ini tidaklah masalah.

Namun, coba sedikit paranoid, siapa yang bisa menjamin kalau Anda mengambil paket yang asalnya tidak jelas? Bahwa Anda mengambil paket Mplayer misalnya, siapa yang menjamin kalau paket tersebut benar-benar multimedia player? Bukan multimedia player plus password logger?

Sebagai tindakan jaga-jaga, mulai saat ini, sebisa mungkin gunakanlah sistem PKI seperti yang telah dibahas. Apabila mengirim file, enkrip dulu dengan public key tujuan. Apabila mempublikasikan file, sign dulu dengan key Anda. Dan, sebagai konsekuensinya, rekan Anda juga akan mengenkripsi setiap file yang dikirim kepada Anda dengan public key Anda. Anda pun tinggal membuka enkripsinya dengan private key Anda. Pengiriman email juga dapat dilakukan dengan cara seperti ini. Email-email client populer telah mendukung penggunaan sistem PKI.

Di artikel ini, kita akan membahas tips dan contoh penggunaan sistem PKI ini menggunakan GPG.

Contoh/tip 1:

Pada contoh pertama ini, kita akan kembali pada dua tokoh yang pertama kita bahas: Superman (Clark Kent) dan Chinmi si

jago Kungfu dari Kuil Dairin. Asumsinya, Superman akan memiliki alamat email `clark@superhero.org` dan Chinmi akan memiliki email `chinmi@superhero.org`.

Setelah berkonsultasi dengan Doraemon (`doraemon@future.de`), mereka pun sepakat untuk menggunakan sistem public key. Superman dan Chinmi kembali ke negara masing-masing dan membuat key.

Di sistemnya, Superman membuka emulasi terminal dan mengetikkan perintah berikut ini:

```
$ gpg --gen-key
gpg (GnuPG) 1.2.4; Copyright (C)
2003 Free Software Foundation,
Inc.
This program comes with
ABSOLUTELY NO WARRANTY.
This is free software, and you
are welcome to redistribute it
under certain conditions. See
the file COPYING for details.

Please select what kind of key
you want:
  (1) DSA and ElGamal (default)
  (2) DSA (sign only)
  (4) RSA (sign only)
Your selection?
DSA keypair will have 1024 bits.
About to generate a new ELG-E
keypair.

                minimum keysize is
6768 bits
                default keysize is
1024 bits
nop@linux:/home/DATA/NOP/home>
gpg --gen-key
nop@linux:/home/DATA/NOP/home>
gpg --gen-key
gpg (GnuPG) 1.2.4; Copyright (C)
2003 Free Software Foundation,
Inc.
```

This program comes with
ABSOLUTELY NO WARRANTY.

This is free software, and you
are welcome to redistribute it
under certain conditions. See
the file COPYING for details.

Please select what kind of key
you want:

- (1) DSA and ElGamal (default)
- (2) DSA (sign only)
- (4) RSA (sign only)

Your selection?

DSA keypair will have 1024 bits.
About to generate a new ELG-E
keypair.

minimum keysize is
768 bits

default keysize is
1024 bits

highest suggested keysize is
2048 bits

What keysize do you want? (1024)

Requested keysize is 1024 bits

Please specify how long the key
should be valid.

0 = key does not expire

<n> = key expires in n
days

<n>w = key expires in n
weeks

<n>m = key expires in n
months

<n>y = key expires in n
years

Key is valid for? (0)

Key does not expire at all

Is this correct (y/n)? y

You need a User-ID to identify
your key; the software
constructs the user id
from Real Name, Comment and
Email Address in this form:

"Heinrich Heine (Der
Dichter) <heinrichh@duesseldorf.
de>"

Real name: Clark Kent

Email address: clark@superhero.
org

Comment: superman

You selected this USER-ID:

"Clark Kent (superman)
<clark@superhero.org>"

Change (N)ame, (C)omment,
(E)mail or (O)kay/(Q)uit? o
You need a Passphrase to protect
your secret key.

[meminta passphrase]

[konfirmasi passphrase]

[menggenerate random byte,
dipotong]

...

...

[random key generation selesai]

public and secret key created
and signed.

key marked as ultimately
trusted.

pub 1024D/ED83DB93 2004-
10-07 clark kent (superman)
<clark@superhero.org>

Key fingerprint = E16B 48B2
3C3B 88FD 4707 8876 9221 8F0E
ED83 DB93

sub 1024g/5F1B267C 2004-10-07

Superman mengisikan informasi berikut
ini:

Real name: Clark Kent

Email address: clark@superhero.org

Comment: superman

passphrase: superman

Di sisi lain, Chinmi juga mengisikan in-
formasi berikut ini:

Real name: Chinmi

Email address: chinmi@superhero.org

Comment: kungfu boy

passphrase: chinmi

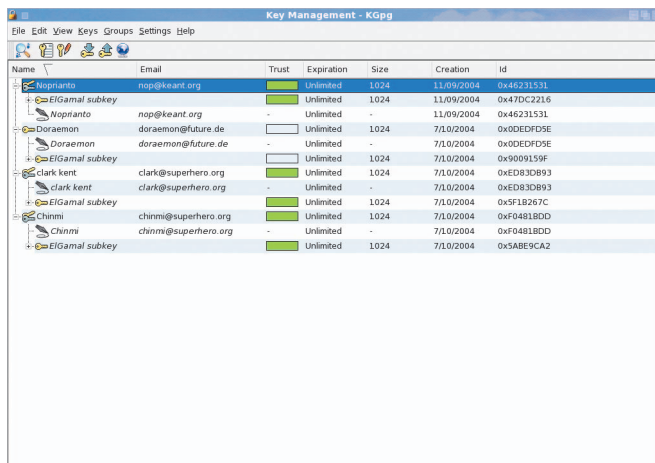
Sementara, berikut ini adalah identifikasi
pasangan key milik chinmi:

pub 1024D/F0481BDD 2004-
10-07 Chinmi (kungfu boy)
<chinmi@superhero.org>

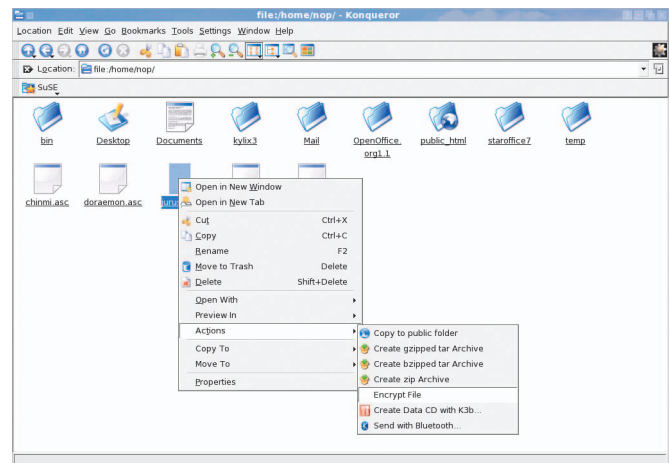
Key fingerprint = 2B72 CCC0
4762 583F 0D4B 7CE6 83F7 D492
F048 1BDD

sub 1024g/5ABE9CA2 2004-10-07

Pada contoh ini, keduanya telah berha-
sil memiliki pasangan key. Untuk membuat
key, Anda juga dapat memberikan opsi
-gen-key.



KGPG.



Mengenkrip file di Konqueror dengan bantuan KGPG.

Contoh/tip 2:

Pada contoh kedua ini, kedua superhero tersebut ingin agar public key mereka dapat diupload ke public key server superhero, tempat public key-public key para superhero dunia. Di sana, Batman dan Flash juga telah mempublikasikan public key mereka.

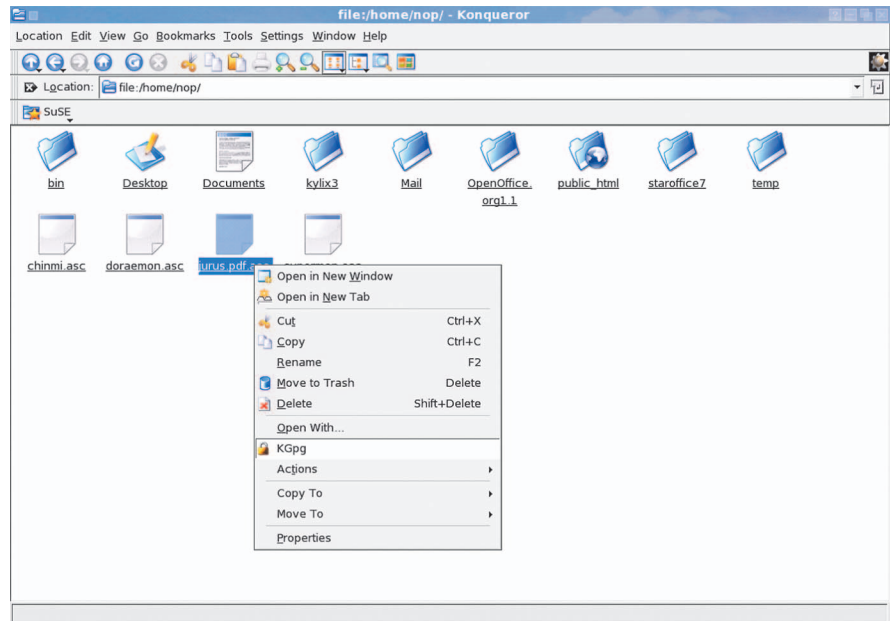
Di sistemnya, Chinmi memberikan perintah seperti ini:

```
$ gpg --armor --export chinmi > chinmi.asc
```

Berikut ini adalah isi file chinmi.asc:

```
---BEGIN PGP PUBLIC KEY BLOCK---
Version: GnuPG v1.2.4 (GNU/
Linux)
```

```
mQGibEF1N1sRBAD1B4on00aCt3HyHrKx
mxM5k1pYp0w1MVLTFvqtg8bQCXmGCrJR
zqKT80KepURoQZGmkrD42avXSnZJzXkr
I+FEj3rSjOW1RwR+B1dUTx0oUKUF7qza
Uc0F7pSkR/zMTjAXhu9JD9Ywtw4a+/
gbTTIBS9v0nQ/
jH0phblmwdvaqdwCg2VxZ
dabhfcIyo69/WPhHacC2UNMEAJHsqTly
zqtXVxIKI9vY86ZCVwErhNZN0meSJ8ud
oIrK12w6noq/WfjmkwzzcUXTyAe2dmW1
3v0DR1DF1PwB27uGh/VI01XfIZJW0g3
NbNSTKxZGHAS3XxpamxJmY4YjohXzyGh
aDmRL/MG1ffhW4J0KAD4XgltoGiLxPtf
jtvTbADCAK7WJ8v60xU2lqMLWEHoSMuG
IkvLwiri8cdwKt3VyY02K6fPsFnPa8hV
xsJev1QIzxxJlN37n1bTuxVAGdLp7U3j
M0Unsh41p7e/y1chGUfHgfM61+w/xU0t
UjEFB6Z8tg1NIh7pJShmA0bAKKZHDJM
XP4u201b+IMozW6jGbQqQ2hpbm1pIChr
dW5nZnUgYm95KSA8Y2hpbm1pQHN1cGVy
aGVyby5vcmc+iF4EExECAB4FAkF1N1sC
GwMGcWkIBwMCAwUCAwMWAEGHGE4AA
CgkQg/fUkvBIG91WiwCeKa0rrLxjQfLT
ikriqqKcuTqQa6sAn1XHAR1uAGwqRT
7BiTWQ9309+JBvuQENBEF1N1wQBAC
1FxHc
ooMKK8f0f0k4Ks/Lp1i7YiKFre14zSLz
+geVWoKArC+eJILDf8iGveecNIhFG12U
DYjoCZpJh1P+Lhti4zi3ups5JHoHdq7L
CPE7gbSS5Vns1Yd7NPIMZ73tK0/XJRJ
IP5vFhm+ECpM7eXhDpqt9/Rc61PwP3L
jjraGwADBQP8CIFEQJWJL5u2ZuMHbGWD
txJZQV4TgNHcjJXjztjZMKvbTw/5yz
ixGx1SRK0xJzqLZU0CsXLYRRN3abgr
0Rij
IACnr+7Mg81L/rqXUGRzA3GpNwiAkdzf
xe+HMeRzaDrjM3UCQNw9rGaDp2b11hb2
```



Medekrip file di Konqueror dengan bantuan KGPG.

```
qKpRzF1iLUH1VG29aXNZrz2ISQQYEQIA
CQUCQWU2XAIbDAKCRCD99SS8Egb3Ttx
AKDQoQ5GSEy1Py68vUx51huMiYtFUACf
Wo10qUhFpw8cVRdyGjDLu6I9Cju=
=2Evn
----END PGP PUBLIC KEY BLOCK----
```

Di sistemnya, Superman melakukan hal yang sama:

```
$ gpg --armor --export superman > superman.asc
```

Dengan demikian, masing-masing superhero tersebut dapat mengirimkan public key masing-masing ke <http://pubkey.superhero.org>.

Opsi `--armor` akan mengeksport public key dalam format ASCII, sementara opsi `--export` digunakan untuk mengeksport key. Sebagai catatan, untuk mengirimkan public key sekaligus, kedua superhero tersebut sebenarnya bisa mempergunakan opsi `--send-keys`.

Contoh/tip 3:

Setelah masing-masing mengupload key masing-masing, Chinmi dan Superman pun masing-masing mendownload public key rekan mereka dan mengimpornya ke dalam sistem masing-masing.

Setelah mendownload `superman.asc`, chinmi pun melakukan perintah berikut ini:

```
$ gpg -import supeman.asc
```

Begitupun dengan Superman, yang memberikan perintah berikut:

```
$ gpg -import chinmi.asc
```

Chinmi pun ingin mengetahui key siapa saja yang telah terdaftar dalam sistemnya. Maka, chinmi pun memberikan perintah:

```
$ gpg --list-keys
/home/chinmi/.gnupg/pubring.gpg
-----
pub 1024D/46231531 2004-09-11
Noprianto (Nop) <nop@keant.org>
sub 1024g/47DC2216 2004-09-11

pub 1024D/F0481BDD 2004-
10-07 Chinmi (kungfu boy)
<chinmi@superhero.org>
sub 1024g/5ABE9CA2 2004-10-07

pub 1024D/ED83DB93 2004-
10-07 clark kent (superman)
<clark@superhero.org>
sub 1024g/5F1B267C 2004-10-07

pub 1024D/0DEDFD5E 2004-
10-07 Doraemon (robotika)
<doraemon@future.de>
sub 1024g/9009159F 2004-10-07
```

Kini, chinmi dan superman dapat saling mengirim file menggunakan public key rekan masing-masing.

Contoh/tip 4:

Suatu hari, Chinmi menemukan jurus baru yang dirasanya cocok dipelajari oleh Superman. Maka, chinmi pun ingin mengirimkan *jurus.pdf* kepada Superman. Chinmi harus berhati-hati karena jurus ini bahkan katanya setara dengan jurus Dewa Petir, jurus anda-lan kuil Dairin yang terlarang. Oleh karena itu, jurus ini tidak boleh diketahui oleh siapa saja. Chinmi harus mengenkripnya dengan public key Superman sebelum mengirimkannya.

Berikut ini adalah perintah yang dilakukan oleh Chinmi:

```
$ gpg -u chinmi -sea -r
superman jurus.pdf
```

```
You need a passphrase to unlock
the secret key for
```

```
user: "Chinmi (kungfu boy)
<chinmi@superhero.org>"
```

```
1024-bit DSA key, ID F0481BDD,
created 2004-10-07
```

```
gpg: checking the trustdb
```

```
gpg: checking at depth 0
signed=0 ot(-/q/n/m/f/
u)=0/0/0/0/0/3
```

Dari perintah itu, file dengan nama *jurus.pdf.asc* pun dihasilkan. File tersebut pun dikirimkan dengan rasa tenang oleh Chinmi ke mailbox Superman.

Opsi `-u` dimaksudkan untuk bekerja sebagai user chinmi. Opsi `-s` dimaksudkan untuk sign. Opsi `-e` dimaksudkan untuk mengenkrip file dan opsi `-a` digunakan untuk menghasilkan file ASCII (*jurus.pdf.asc* secara default).

Contoh/tip 5:

Superman menerima sebuah file dengan nama *jurus.pdf.asc* dari Chinmi. Chinmi berpesan bahwa ini adalah file rahasia. Setelah dipelajari, harus segera dihapus.

Superman pun segera mendekrip file tersebut dengan private key miliknya. Berikut ini adalah perintah yang diberikan oleh Superman:

```
$ gpg --output=jurus.pdf -d
jurus.pdf.asc
```

```
You need a passphrase to unlock
the secret key for
```

```
user: "clark kent (superman)
<clark@superhero.org>"
```

```
1024-bit ELG-E key, ID 5F1B267C,
created 2004-10-07 (main key ID
ED83DB93)
```

```
gpg: encrypted with 1024-bit
ELG-E key, ID 5F1B267C, created
2004-10-07
```

```
"clark kent (superman)
<clark@superhero.org>"
```

```
gpg: Signature made Thu 07 Oct
2004 08:03:33 PM WIT using DSA
key ID F0481BDD
```

```
gpg: Good signature from "Chinmi
(kungfu boy) <chinmi@superhero.
org>"
```


Setelah mendapatkan tulisan Good signature from Chinmi, Superman pun tenang. Superman pun segera mempelajari jurus tersebut dan bertekad akan mengirimkan jurus terbangnya kepada Chinmi.

Opsi `-d` pada contoh digunakan untuk melakukan *decrypt*. Harap bersabar apabila proses dekrip berjalan cukup lambat. Terutama pada file-file yang sangat besar.

Setelah itu, keduanya mulai saling berkirim jurus dan berbagi pengetahuan bagaimana menjaga perdamaian dunia. Setelah mereka mempergunakan sistem PKI ini, tidak ada lagi kesalahpahaman yang terjadi diantara mereka.

Kita juga perlu melakukan tindakan berjaga-jaga tersebut dalam berhubungan di internet ataupun bertukar file dan pesan dalam komunitas. Sedikit repot tidak masalah, untuk tujuan yang lebih baik.

Bagi Anda yang ingin lebih mudah menggunakan sistem PKI ini, Anda bisa mempergunakan program KGPG.

KGPG adalah *front end* untuk penggunaan GPG yang jauh lebih mudah untuk digunakan. Apa yang perlu dilakukan oleh user hanyalah klak klik di sana sini. Pembuatan key, enkrip dan dekrip menjadi jauh lebih mudah! Bahkan, kabar baiknya, KGPG memiliki integrasi yang begitu tinggi dengan Konqueror sehingga enkripsi dan dekripsi file dapat dilakukan dengan sangat mudah. Selamat mencoba dan teruslah menggunakan GPG dalam komunikasi Anda di internet. 

Noprianto (noprianto@infolinux.co.id)



SLES 9

With the release of
SUSE LINUX Enterprise Server 9,
Linux goes from the back room
to the boardroom.



Whether you run a Microsoft environment, a Novell shop, a mixed-OS operation (Windows, NetWare, LINUX, Unix, etc.) or are starting from scratch, SLES 9 has something for you...

GudangLinux

The Open Source Destination
T: (021) 5793-4060 - F: (021) 5793-5557
eMail: info@gudanglinux.net
<http://www.gudanglinux.com>