Utiliser GNUPG

Frédéric Praca

Rotomalug

29 mars 2004

partie

Introduction

Cette présentation a pour but de traiter des points suivants :

- Pourquoi utiliser GNUPG ?

Cette présentation a pour but de traiter des points suivants :

- Pourquoi utiliser GNUPG ?
- Un peu d'histoire de la cryptographie

Cette présentation a pour but de traiter des points suivants :

- Pourquoi utiliser GNUPG ?
- Un peu d'histoire de la cryptographie
- La philosophie GNUPG

Cette présentation a pour but de traiter des points suivants :

- Pourquoi utiliser GNUPG ?
- Un peu d'histoire de la cryptographie
- La philosophie GNUPG
- Quelques commandes utiles

Cette présentation a pour but de traiter des points suivants :

- Pourquoi utiliser GNUPG ?
- Un peu d'histoire de la cryptographie
- La philosophie GNUPG
- Quelques commandes utiles
- Les frontaux pour GNUPG

Cette présentation a pour but de traiter des points suivants :

- Pourquoi utiliser GNUPG ?
- Un peu d'histoire de la cryptographie
- La philosophie GNUPG
- Quelques commandes utiles
- Les frontaux pour GNUPG
- La Keysigning party

Internet

Internet est devenu en quelques années le plus grand espace d'échange d'information du monde. Dans cet espace, se côtoient toutes sortes de personnes et comme dans toute société, elles ne sont hélas pas toutes bien intentionnées.

La sécurité sur Internet

Plusieurs problèmes sont inhérents à l'aspect virtuel et global d'Internet :

La sécurité sur Internet

Plusieurs problèmes sont inhérents à l'aspect virtuel et global d'Internet :

- Le problème de la vérification de l'identité de votre interlocuteur

La sécurité sur Internet

Plusieurs problèmes sont inhérents à l'aspect virtuel et global d'Internet :

- Le problème de la vérification de l'identité de votre interlocuteur
- Le problème de la confidentialité de votre conversation

Le courriel

Le courriel

- Application primordiale du Net

Le courriel

- Application primordiale du Net
- Certainement la plus utilisée

Le courriel

- Application primordiale du Net
- Certainement la plus utilisée
- Une des plus anciennes (RFC 821 Simple Mail Transfer Protocol. J. Postel. Aug-01-1982)

Le courriel

- Application primordiale du Net
- Certainement la plus utilisée
- Une des plus anciennes (RFC 821 Simple Mail Transfer Protocol. J. Postel. Aug-01-1982)

En raison ou en dépit de son grand âge (et bien qu'elle ait été plusieurs fois modifiée), cette application n'est pas exempte de problèmes de sécurité

Problème du courriel

Le courriel possède deux gros problèmes :

Problème du courriel

Le courriel possède deux gros problèmes :

- Il circule en clair sur le réseau

Problème du courriel

Le courriel possède deux gros problèmes :

- Il circule en clair sur le réseau
- C'est un protocole ASCII (ie. lisible par un être humain)

Problème du courriel

Le courriel possède deux gros problèmes :

- Il circule en clair sur le réseau
- C'est un protocole ASCII (ie. lisible par un être humain)

Le courriel n'est donc pas une lettre mais *une carte postale*

Exemples

- Le fait qu'il circule en clair et qu'il soit ASCII permet à l'aide d'un outil approprié (un sniffer réseau comme *Ethereal* ou *tcpdump*) de lire tout le contenu des courriels lors du transfert de la machine expéditrice à la machine destinataire.

Exemples

- Le fait qu'il circule en clair et qu'il soit ASCII permet à l'aide d'un outil approprié (un sniffer réseau comme *Ethereal* ou *tcpdump*) de lire tout le contenu des courriels lors du transfert de la machine expéditrice à la machine destinataire.
- Le fait que le protocole soit en ASCII permet à n'importe quel humain de jouer le rôle d'un client courriel vis-à-vis du serveur. Il peut ainsi entrer lui-même la valeur de chaque champ (le champ *From* en est un bon exemple). La conséquence est que l'on peut se faire passer pour n'importe qui.

Conclusion intermédiaire

GNUPG permet de résoudre ces problèmes :

Conclusion intermédiaire

GNUPG permet de résoudre ces problèmes :

- de chiffrer vos messages et donc de mettre une enveloppe sur votre carte postale

Conclusion intermédiaire

GNUPG permet de résoudre ces problèmes :

- de chiffrer vos messages et donc de mettre une enveloppe sur votre carte postale
- de signer vos messages afin de garantir votre identité (Authentification)

Conclusion intermédiaire

GNUPG permet de résoudre ces problèmes :

- de chiffrer vos messages et donc de mettre une enveloppe sur votre carte postale
- de signer vos messages afin de garantir votre identité (Authentification)
- et d'autres choses encore...

Les débuts

L'art de la cryptographie remonte à l'antiquité avec plusieurs algorithmes :

- Le rouleau de papier des Grecs

Les débuts

L'art de la cryptographie remonte à l'antiquité avec plusieurs algorithmes :

- Le rouleau de papier des Grecs
- Le code de César

Les débuts

L'art de la cryptographie remonte à l'antiquité avec plusieurs algorithmes :

- Le rouleau de papier des Grecs
- Le code de César
- La substitution monoalphabétique (a resisté jusqu'au IX^{e} siècle)

Ça se complique

- 1586 : Le carré de Vigenère (resistera jusqu'en 1854)

Ça se complique

- 1586 : Le carré de Vigenère (resistera jusqu'en 1854)
- 1926 : Gilbert Vernam invente un chiffre indéchiffrable (prouvé par Shannon)

Ça se complique

- 1586 : Le carré de Vigenère (resistera jusqu'en 1854)
- 1926 : Gilbert Vernam invente un chiffre indéchiffrable (prouvé par Shannon)
- Seconde guerre mondiale : Enigma ($\simeq 159.10^{18}$ clefs possibles)

Aujourd'hui

Il existe un nombre important d'outils cryptographiques :

Aujourd'hui

Il existe un nombre important d'outils cryptographiques :

- DES

Aujourd'hui

Il existe un nombre important d'outils cryptographiques :

- DES
- AES

Aujourd'hui

Il existe un nombre important d'outils cryptographiques :

- DES
- AES
- RSA

Aujourd'hui

Il existe un nombre important d'outils cryptographiques :

- DES
- AES
- RSA
- El Gamal

Aujourd'hui

Il existe un nombre important d'outils cryptographiques :

- DES
- AES
- RSA
- El Gamal

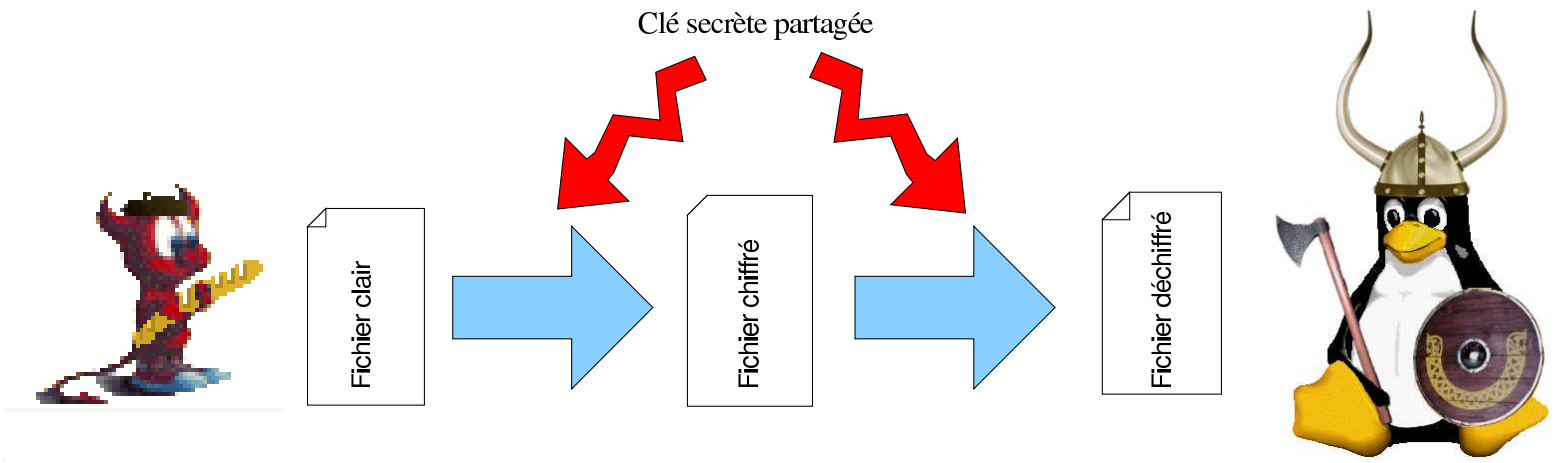
Les deux premiers étant symétriques et les deux suivants asymétriques

Cryptographie symétrique

Il s'agit de la cryptographie dans laquelle les deux parties communicantes partagent la clé de chiffrement.
Ainsi, clé de chiffrement = clé de déchiffrement

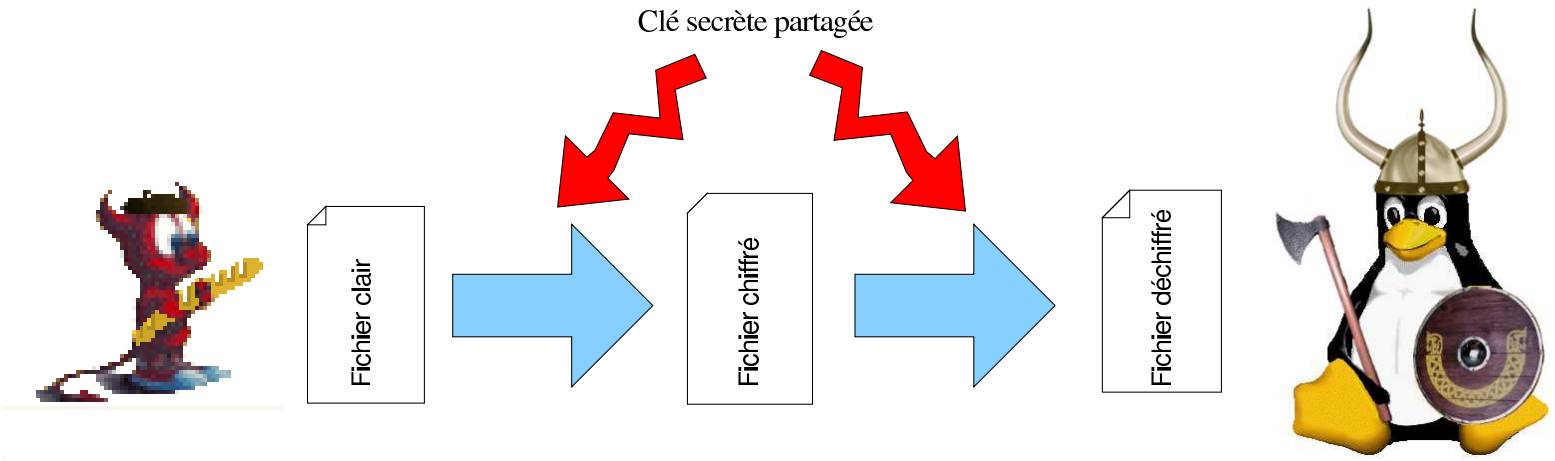
Cryptographie symétrique

Il s'agit de la cryptographie dans laquelle les deux parties communicantes partagent la clé de chiffrement.
Ainsi, clé de chiffrement = clé de déchiffrement



Cryptographie symétrique

Il s'agit de la cryptographie dans laquelle les deux parties communicantes partagent la clé de chiffrement.
Ainsi, clé de chiffrement = clé de déchiffrement



C'est le cas des algorithmes antiques.

Cryptographie asymétrique

Le but de ce type de cryptographie est de ne pas partager de clé de chiffrement commune.
On utilise alors :

Cryptographie asymétrique

Le but de ce type de cryptographie est de ne pas partager de clé de chiffrement commune.
On utilise alors :

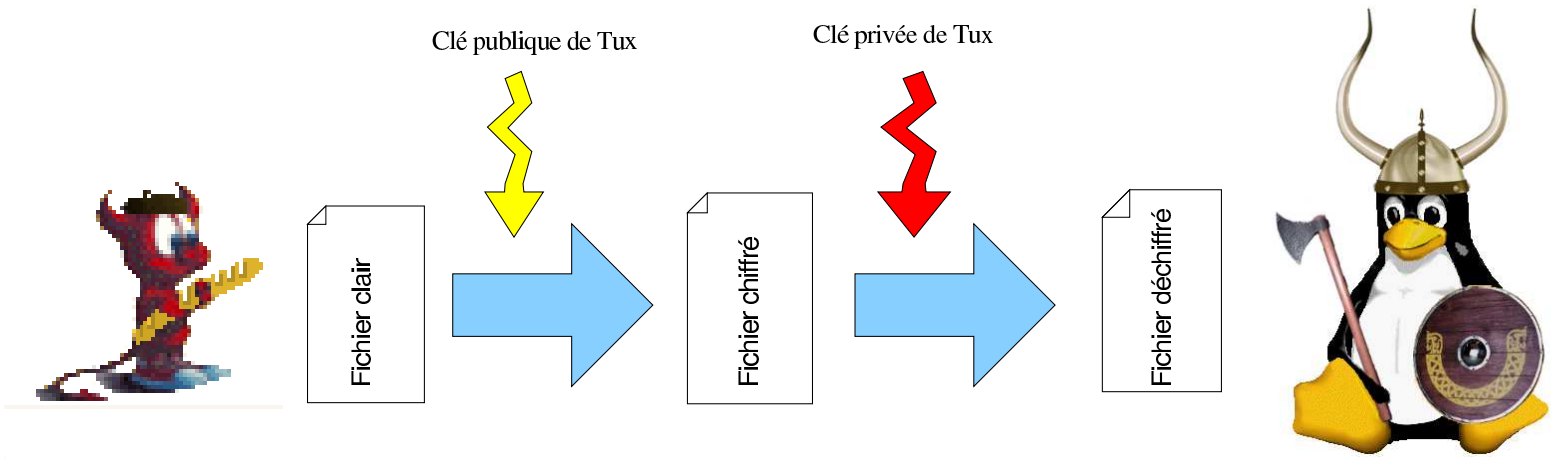
- une clé publique connue de tous

Cryptographie asymétrique

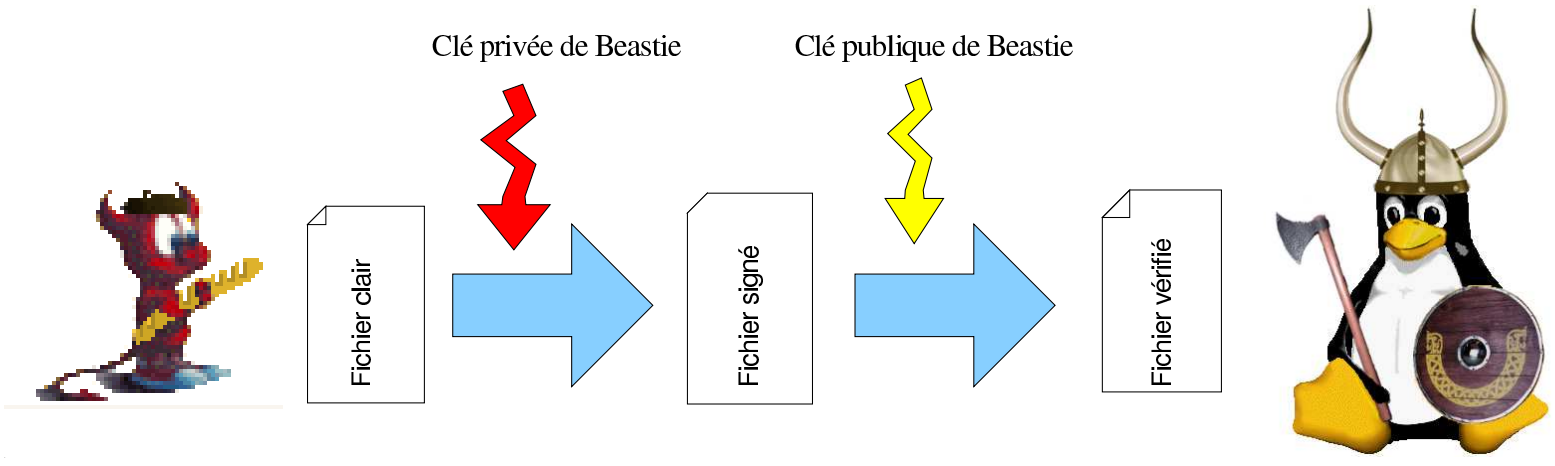
Le but de ce type de cryptographie est de ne pas partager de clé de chiffrement commune.
On utilise alors :

- une clé publique connue de tous
- et une clé privée personnelle et confidentielle.

Chiffrement



Signature


Clé privée de Beastie
Clé publique de Beastie
Fichier clair
Fichier signé
Fichier vérifié

Fiabilité Chiffrement-Signature

Chiffrement : pas de problème, le message reçu étant chiffré avec notre clé privée.
Signature : Qui se cache derrière la signature ?

La toile de confiance

- Elle introduit la notion de confiance entre les utilisateurs

La toile de confiance

- Elle introduit la notion de confiance entre les utilisateurs
- Elle permet de certifier les signatures

Comment ça marche ?

En plusieurs étapes :

Comment ça marche ?

En plusieurs étapes :

- signer la clé d'une personne

Comment ça marche ?

En plusieurs étapes :

- signer la clé d'une personne
- attribuer un degré de confiance à cette personne (inconnu, pas confiance, marginalement, complètement)

Comment ça marche ?

En plusieurs étapes :

- signer la clé d'une personne
- attribuer un degré de confiance à cette personne (inconnu, pas confiance, marginalement, complètement)

Le degré de confiance conditionne la validité des clés signées par cette personne.

Propagation de la validité

Quatre critères rendent une clé valide :

Propagation de la validité

Quatre critères rendent une clé valide :

- vous avez signé la clé

Propagation de la validité

Quatre critères rendent une clé valide :

- vous avez signé la clé
- la clé a été signée par une personne en qui vous avez toute confiance

Propagation de la validité

Quatre critères rendent une clé valide :

- vous avez signé la clé
- la clé a été signée par une personne en qui vous avez toute confiance
- la clé a été signée par trois clés en qui vous avez une confiance marginale

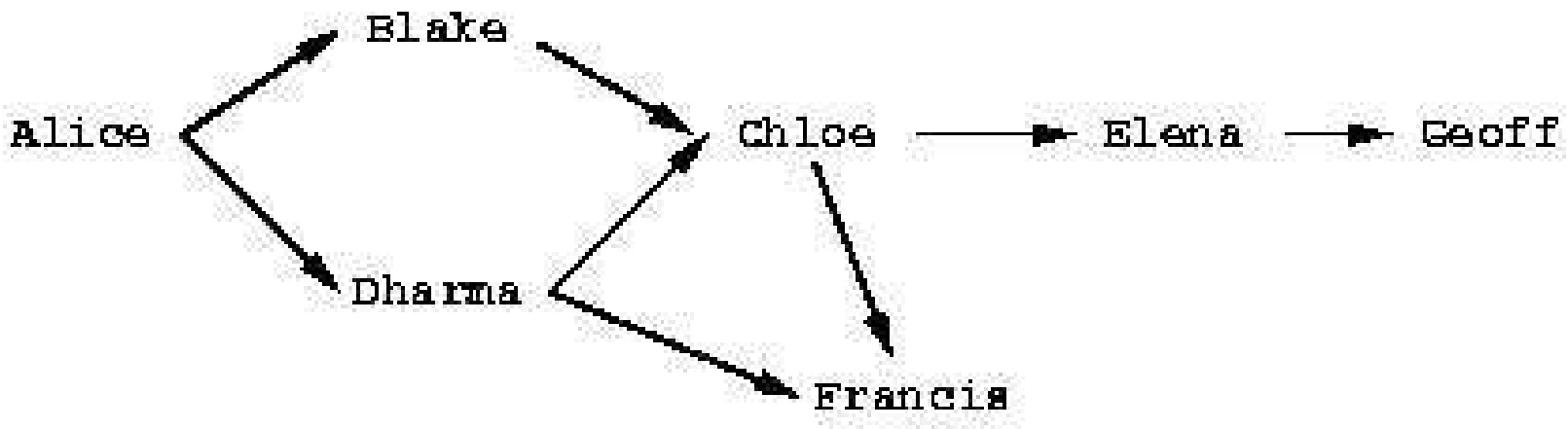
Propagation de la validité

Quatre critères rendent une clé valide :

- vous avez signé la clé
- la clé a été signée par une personne en qui vous avez toute confiance
- la clé a été signée par trois clés en qui vous avez une confiance marginale
- le chemin des clés signées conduisant de cette clé à votre clé mesure moins de 5 étapes

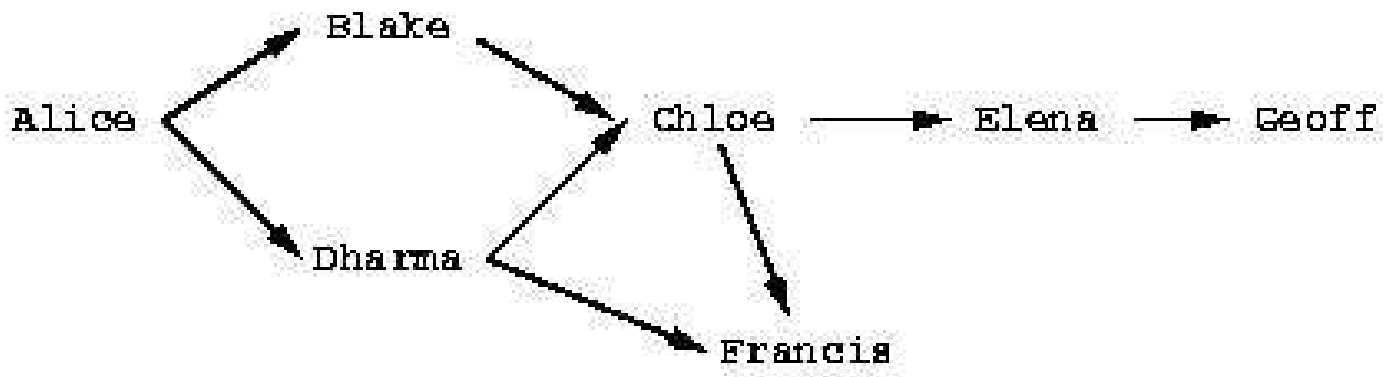
Exemple de toile de confiance

Alice possède la toile de confiance qui suit:



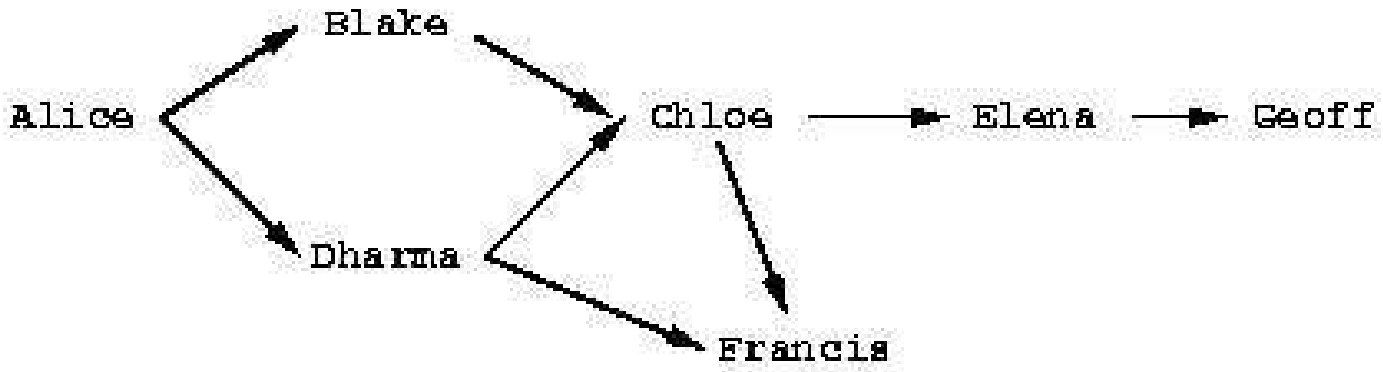
Exemple de toile de confiance (2)

Confiance		*Validité*	
marginale	*complète*	*marginale*	*complète*
	Dharma		Blake Chloé Dharma,Francis



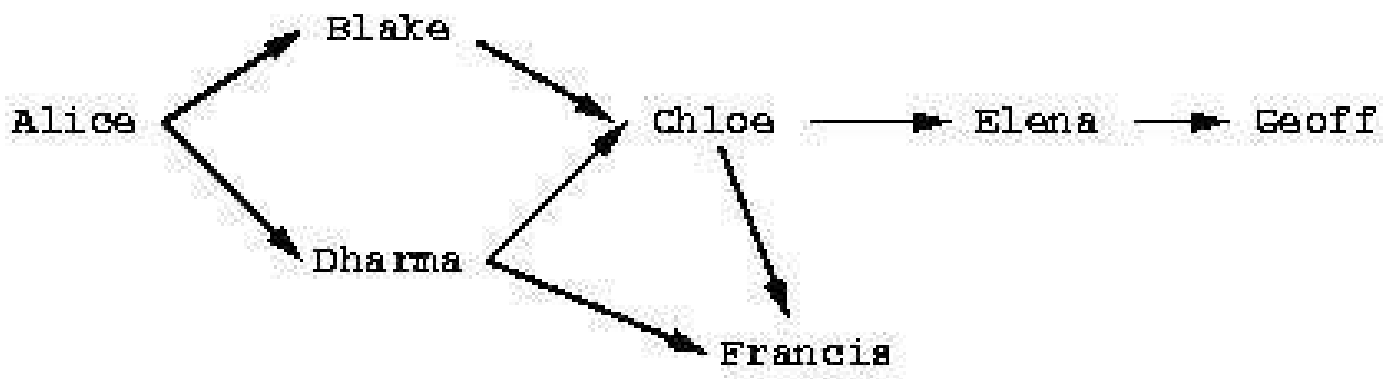
Exemple de toile de confiance (3)

Confiance		*Validité*	
marginale	*complète*	*marginale*	*complète*
Blake Dharma		Francis	Blake Chloé, Dharma



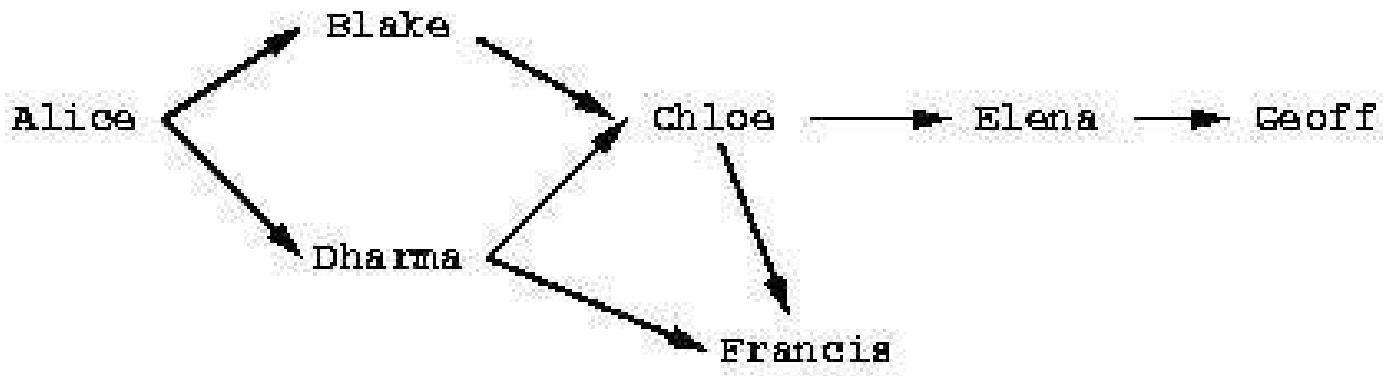
Exemple de toile de confiance (4)

Confiance		*Validité*	
marginale	*complète*	*marginale*	*complète*
Blake Chloé Dharma		Elena	Blake,Chloé Dharma, Francis



Exemple de toile de confiance (5)

Confiance		*Validité*	
marginale	*complète*	*marginale*	*complète*
	Blake Chloé Elena		Blake Chloé Elena, Francis



Conséquences de la toile

Conséquences :

Conséquences de la toile

Conséquences :

- Augmentation rapide du nombre de personnes de confiance

Conséquences de la toile

Conséquences :

- Augmentation rapide du nombre de personnes de confiance
- Meilleure sécurité lors des échanges sur le Net

Conséquences de la toile

Conséquences :

- Augmentation rapide du nombre de personnes de confiance
- Meilleure sécurité lors des échanges sur le Net
- Plus le chemin de propagation est court plus il faut de clés signées

Création et révocation de clés

- Création : *gpg –gen-key*

Création et révocation de clés

- Création : *gpg –gen-key*
- Révocation : *gpg –output revoke.asc –gen-revoke*

Création

```
fred@dagobah:~/LateX%gpg --gen-key
gpg (GnuPG) 1.0.7; Copyright (C) 2002 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.

gpg: Warning: using insecure memory!

gpg: please see http://www.gnupg.org/faq.html for more information
Please select what kind of key you want:
   (1) DSA and ElGamal (default)
   (2) DSA (sign only)
   (4) ElGamal (sign and encrypt)
   (5) RSA (sign only)
Your selection?
```

Création (2)

```
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) 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) 0
Key does not expire at all
Is this correct (y/n)? y
```

Création (3)

```
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: Frédéric Praca
Email address: frederic.praca@freebsd-fr.org
Comment:
You are using the ‘iso-8859-1’ character set.
You selected this USER-ID:
    "Frédéric Praca <frederic.praca@freebsd-fr.org>"

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

La révocation

La commande de révocation produit ce type de fichier :

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.6 (FreeBSD)
Comment: For info see http://www.gnupg.org
Comment: A revocation certificate should follow

iEkEIBECAAkFAjzjgpsCHQMACgkQ4TZnnwGsbV1U5UCeJoM+O89jwcqWH+Ilb4lH
RoZiRN4An3jond2fgjVrNrl7WnWn3ofpMowI
=W4+s
-----END PGP PUBLIC KEY BLOCK-----
```

Utilisation de sa clé

L'utilisation de la clé se fait pour :

Utilisation de sa clé

L'utilisation de la clé se fait pour :

- la signature : *gpg –clearsign nomFichier*

Utilisation de sa clé

L'utilisation de la clé se fait pour :

- la signature : *gpg –clearsign nomFichier*
- le chiffrement : *gpg –armor –encrypt nomFichier*

Signature

```
gpg: Warning: using insecure memory!
gpg: please see http://www.gnupg.org/faq.html for more information

You need a passphrase to unlock the secret key for
user: "Frederic PRACA (Blackknight) <frederic.praca@freebsd-fr.org>"
1024-bit DSA key, ID 01AC6D5D, created 2002-04-04

Enter passphrase:
```

Signature (2)

La commande *gpg –clearsign nomFichier* produit ce type de fichier ASCII :

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Bienvenue à l'install-party
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.7 (FreeBSD)

iD8DBQFABRBa4WZnnwGsbVORAjQ1AJwPfnVWMBWsDsgBMrG3W7TYMOcG4wCfcEL0
Svk85zJ5y5w01pyISPM12hI=
=xI5J
-----END PGP SIGNATURE-----
```

gpg –sign nomFichier produit quand à elle un fichier binaire

Vérification de la signature

La signature d'un fichier est vérifiée à l'aide de
gpg –verify nomFichierSigne

Autre possibilité de signature

Il est aussi possible de fournir une signature dans un fichier indépendant avec *gpg –detach-sign nomFichier*

Chiffrement

```
gpg: Warning: using insecure memory!
gpg: please see http://www.gnupg.org/faq.html for more information
You did not specify a user ID. (you may use "-r")

Enter the user ID.  End with an empty line: LD
gpg: AC5BBF9A: There is no indication that this key really belongs to the owner
1024g/AC5BBF9A 2002-05-16 "Laurent DUBEC (LD) <laurent.dubec@libertysurf.fr>"
             Fingerprint: 651C C2F6 43A0 0F5E EC50  6B88 BE1F 64C4 AC5B BF9A

It is NOT certain that the key belongs to its owner.
If you *really* know what you are doing, you may answer
the next question with yes

Use this key anyway? y
Added 1024g/AC5BBF9A 2002-05-16 "Laurent DUBEC (LD) <laurent.dubec@libertysurf.fr>"

Enter the user ID.  End with an empty line:
```

Chiffrement (2)

La commande de chiffrement *gpg –armor –encrypt nomFichier* produit un fichier ASCII comme suit:

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.0.7 (FreeBSD)

hQEOA74fZMSsW7+aEAP/WBO7U2WRlqj0Nu4WXbiofDJp2P4CgZaQTQrc3m1iyn7c
yRmSYe7pdmlvHD77E8X3nddhesj1riWh7YGJC0tA6AjLuqusUk1kb/qGbSV0DamM
JkcOr2n9o/HRLIJHwSvKDVFH47mgwSVu9KPy/QHT5YICq3nl8m5V0dX58WDFkrkD
/2pa8mccAnB6a3YVw4zUi24zCjODOELYtoeuEIK23dtwW0qIs7jjLcOSD23hxpJc
xvCC3i7sPkyQ0frr8v/MUb7Y+GuTUUF/WbKVgofqHTRRWiSwFdaEFck/vFK5kFQd
jzd5bcmcbHK2w/OREm8faByUnsS50zKONZJ4Y12fOj5H0mABTwuwPb6e8eXNzbjJ
C+5Mg4fGhTHULek8z651vv3ak2SkJyOMwc1xviTnqcZ4sNTl+VmsU8i2C24xCIAc
iBpoqnEGS75Tkr7mzL8NYSeZFjfFdIlau27EEzeS5WekWMw=
=ahQa
-----END PGP MESSAGE-----
```

C'est l'option *–armor* qui permet d'avoir une sortie ASCII

Déchiffrement

La commande pour déchiffrer un message est simplement *gpg –decrypt nomFichier*.
Tel quel, la sortie est la sortie standard. Il faut lui adjoindre l'option *–output nomFichierDechiffre* pour obtenir un fichier ASCII.
Dans le cas d'un fichier signé, la signature est vérifiée.

Gestion des clefs

La population du trousseau de clefs GnuPG est nécessaire pour :

- chiffrer vos messages

Gestion des clefs

La population du trousseau de clefs GnuPG est nécessaire pour :

- chiffrer vos messages
- vérifier les signatures

Commandes de gestion de trousseau

Plusieurs commandes permettent la gestion de vos clefs :

- *gpg –list-keys [ids clés]* : liste l'ensemble des clefs stockées dans votre trousseau

Commandes de gestion de trousseau

Plusieurs commandes permettent la gestion de vos clefs :

- *gpg –list-keys [ids clés]* : liste l'ensemble des clefs stockées dans votre trousseau
- *gpg –list-sigs [ids clés]* : idem que précédent avec la liste des signatures en plus

Commandes de gestion de trousseau

Plusieurs commandes permettent la gestion de vos clefs :

- *gpg –list-keys [ids clés]* : liste l'ensemble des clefs stockées dans votre trousseau
- *gpg –list-sigs [ids clés]* : idem que précédent avec la liste des signatures en plus
- *gpg –fingerprints [ids clés]* : idem *list-keys* mais avec les *fingerprints* utilisés lors des keysigning parties

Commandes de gestion de trousseau

Plusieurs commandes permettent la gestion de vos clefs :

- *gpg –list-keys [ids clés]* : liste l'ensemble des clefs stockées dans votre trousseau
- *gpg –list-sigs [ids clés]* : idem que précédent avec la liste des signatures en plus
- *gpg –fingerprints [ids clés]* : idem *list-keys* mais avec les *fingerprints* utilisés lors des keysigning parties
- *gpg –edit-key id clé* : permet d'ajuster la confiance d'une clé, de signer la clé, revoquer une clé

Commandes de gestion de trousseau

Plusieurs commandes permettent la gestion de vos clefs :

- *gpg –list-keys [ids clés]* : liste l'ensemble des clefs stockées dans votre trousseau
- *gpg –list-sigs [ids clés]* : idem que précédent avec la liste des signatures en plus
- *gpg –fingerprints [ids clés]* : idem *list-keys* mais avec les *fingerprints* utilisés lors des keysigning parties
- *gpg –edit-key id clé* : permet d'ajuster la confiance d'une clé, de signer la clé, revoquer une clé
- *gpg –export [ids clés]* : permet d'exporter une ou plusieurs clés

Commandes de gestion de trousseau

Plusieurs commandes permettent la gestion de vos clefs :

- *gpg –list-keys [ids clés]* : liste l'ensemble des clefs stockées dans votre trousseau
- *gpg –list-sigs [ids clés]* : idem que précédent avec la liste des signatures en plus
- *gpg –fingerprints [ids clés]* : idem *list-keys* mais avec les *fingerprints* utilisés lors des keysigning parties
- *gpg –edit-key id clé* : permet d'ajuster la confiance d'une clé, de signer la clé, revoquer une clé
- *gpg –export [ids clés]* : permet d'exporter une ou plusieurs clés
- *gpg –import [nomsFichiers]* : permet d'importer des clés depuis un ou plusieurs fichiers

Les serveurs de clés

Les serveurs de clés stockent des clés publiques.
L'intérêt est :

Les serveurs de clés

Les serveurs de clés stockent des clés publiques.
L'intérêt est :

- d'avoir accès aux clés avec un lien au Net

Les serveurs de clés

Les serveurs de clés stockent des clés publiques.
L'intérêt est :

- d'avoir accès aux clés avec un lien au Net
- de remettre sa clé à jour (et donc récupérer les nouvelles signatures)

Les serveurs de clés

Les serveurs de clés stockent des clés publiques.
L'intérêt est :

- d'avoir accès aux clés avec un lien au Net
- de remettre sa clé à jour (et donc récupérer les nouvelles signatures)
- de récupérer une clé ayant servi à signer un message

Les serveurs de clés (2)

Les commandes liées aux serveurs de clés sont :

Les serveurs de clés (2)

Les commandes liées aux serveurs de clés sont :

- *gpg –recv-keys ids clés* : permet de récupérer des clés par leur identifiant

Les serveurs de clés (2)

Les commandes liées aux serveurs de clés sont :

- *gpg –recv-keys ids clés* : permet de récupérer des clés par leur identifiant
- *gpg –send-keys noms clés* : permet d'envoyer des clés (et pas seulement la sienne)

Les serveurs de clés (2)

Les commandes liées aux serveurs de clés sont :

- *gpg –recv-keys ids clés* : permet de récupérer des clés par leur identifiant
- *gpg –send-keys noms clés* : permet d'envoyer des clés (et pas seulement la sienne)
- *gpg –search-keys noms clés* : permet de rechercher une clé par une sorte de requête sur son nom

Les serveurs de clés (2)

Les commandes liées aux serveurs de clés sont :

- *gpg –recv-keys ids clés* : permet de récupérer des clés par leur identifiant
- *gpg –send-keys noms clés* : permet d'envoyer des clés (et pas seulement la sienne)
- *gpg –search-keys noms clés* : permet de rechercher une clé par une sorte de requête sur son nom

Il faut noter que l'option *–keyserver URL-serveur* doit toujours être présente pour toutes ces commandes

Le reste

Le reste se trouve dans :

Le reste

Le reste se trouve dans :

- l'excellente page de manuel (*man 1 gpg*)

Le reste

Le reste se trouve dans :

- l'excellente page de manuel (*man 1 gpg*)
- l'excellent manuel de GnuPG en Français (voir GnuPG.org)

Le reste

Le reste se trouve dans :

- l'excellente page de manuel (*man 1 gpg*)
- l'excellent manuel de GnuPG en Français (voir GnuPG.org)
- le Web en général

Les frontaux

Les frontaux se découpent en deux catégories :

Les frontaux

Les frontaux se découpent en deux catégories :

- Les logiciels de gestion de trousseau

Les frontaux

Les frontaux se découpent en deux catégories :

- Les logiciels de gestion de trousseau
- Les logiciels de messagerie

Les logiciels de gestion de clés

Deux grands se partagent le “marché” sous Linux et consorts :

Les logiciels de gestion de clés

Deux grands se partagent le “marché” sous Linux et consorts :

- GPA, l’outil officiel et partie intégrante du projet GnuPG

Les logiciels de gestion de clés

Deux grands se partagent le “marché” sous Linux et consorts :

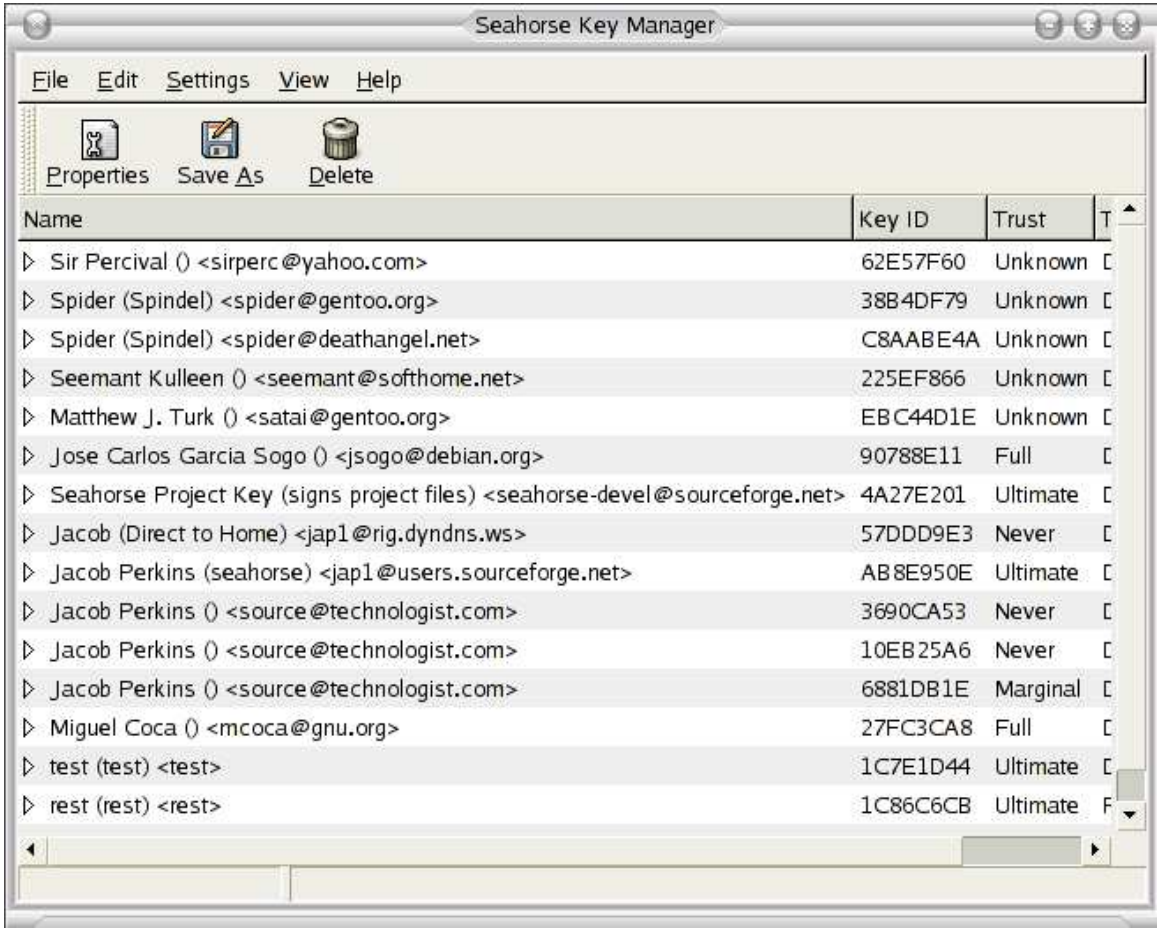
- GPA, l’outil officiel et partie intégrante du projet GnuPG
- SeaHorse, un outil Gnome

Les logiciels de gestion de clés

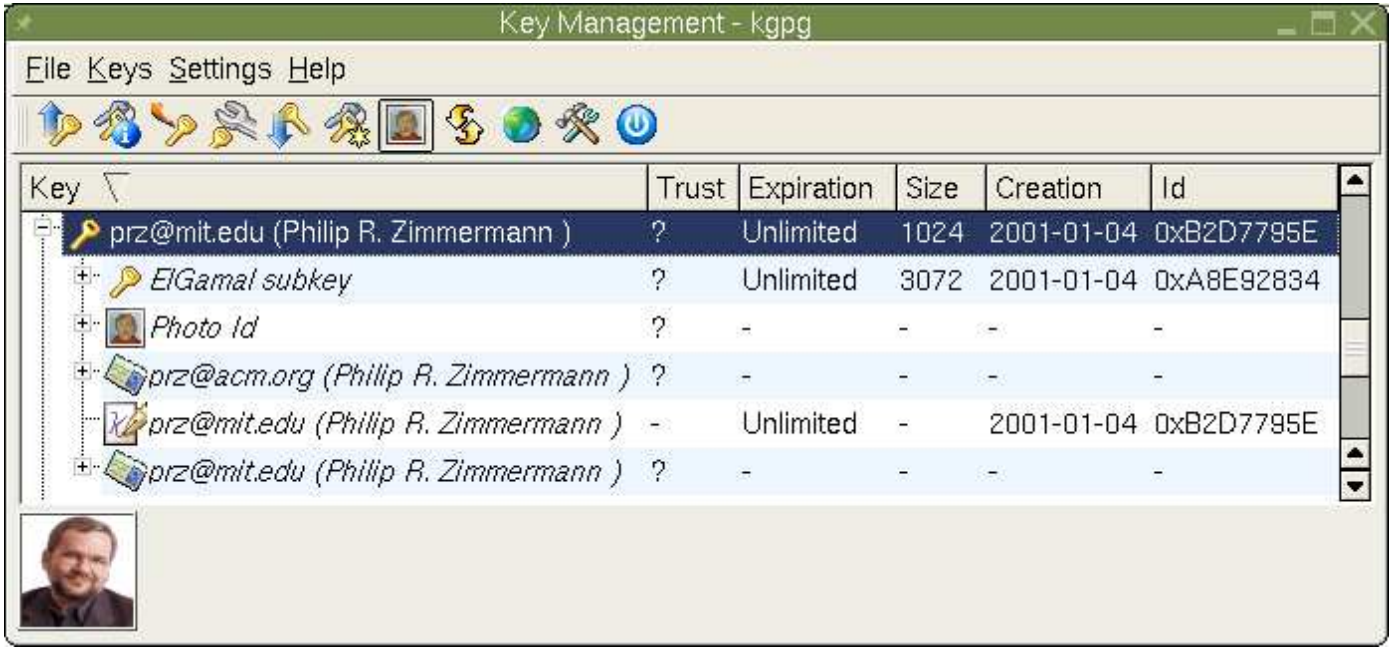
Deux grands se partagent le “marché” sous Linux et consorts :

- GPA, l’outil officiel et partie intégrante du projet GnuPG
- SeaHorse, un outil Gnome
- KGPG, l’outil KDE

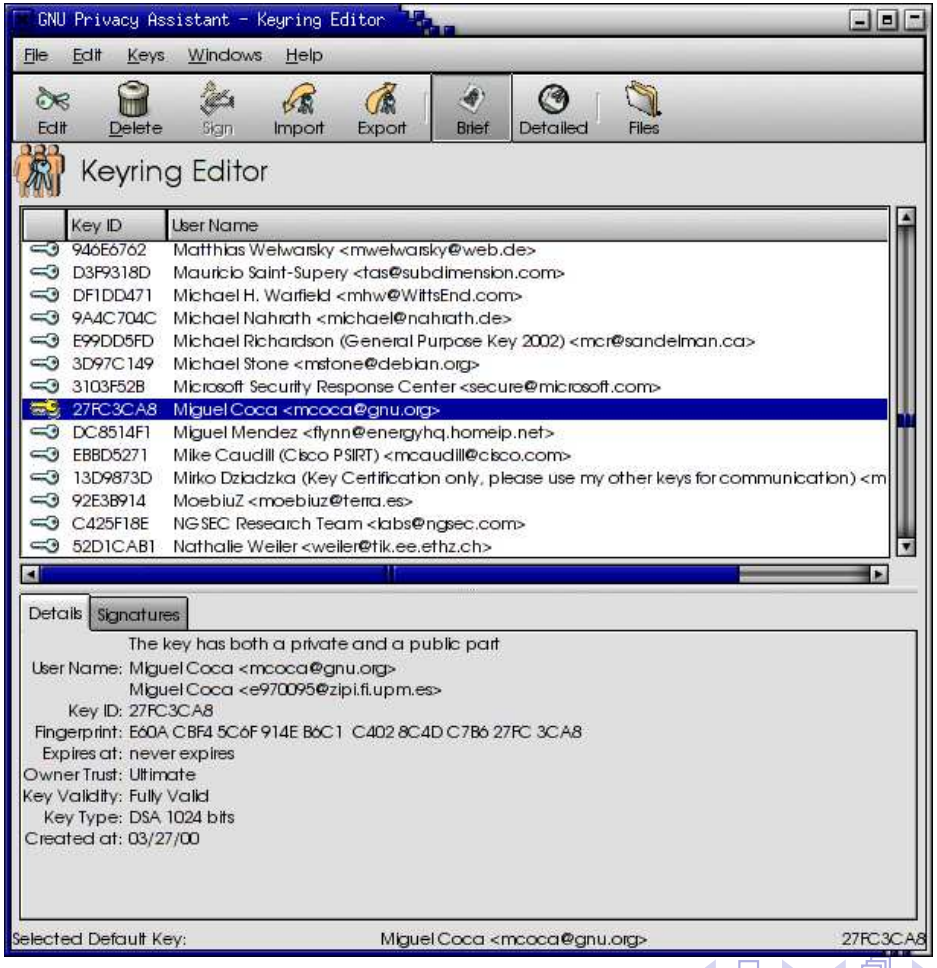
Quelques copies d'écran



Quelques copies d'écran



Quelques copies d'écran



Les logiciels de messagerie

A peu près tous les logiciels de messagerie supportent GnuPG :

Les logiciels de messagerie

A peu près tous les logiciels de messagerie supportent GnuPG :

- Mozilla : au travers d'un greffon Enigmail

Les logiciels de messagerie

A peu près tous les logiciels de messagerie supportent GnuPG :

- Mozilla : au travers d'un greffon Enigmail
- Kmail

Les logiciels de messagerie

A peu près tous les logiciels de messagerie supportent GnuPG :

- Mozilla : au travers d'un greffon Enigmail
- Kmail
- Evolution

Les logiciels de messagerie

A peu près tous les logiciels de messagerie supportent GnuPG :

- Mozilla : au travers d'un greffon Enigmail
- Kmail
- Evolution
- Sylpheed

Les logiciels de messagerie

A peu près tous les logiciels de messagerie supportent GnuPG :

- Mozilla : au travers d'un greffon Enigmail
- Kmail
- Evolution
- Sylpheed
- GNUMail

Les logiciels de messagerie

A peu près tous les logiciels de messagerie supportent GnuPG :

- Mozilla : au travers d'un greffon Enigmail
- Kmail
- Evolution
- Sylpheed
- GNUMail
- Mutt, Pine et bien d'autres

La Keysigning Party

Déroulement :

- Présenter une carte de visite sur laquelle figure vos noms, prénoms, e-mail et *fingerprint*
- Présenter une pièce d'identité pour vérification de la concordance des infos
- L'organisateur vous présente sa clé et sa pièce d'identité
- L'organisateur signe votre clé
- La liste des clés signés sera disponible en ligne et sera elle-même signée ;-)