

Échange sécurisé de courriels

David Mentré

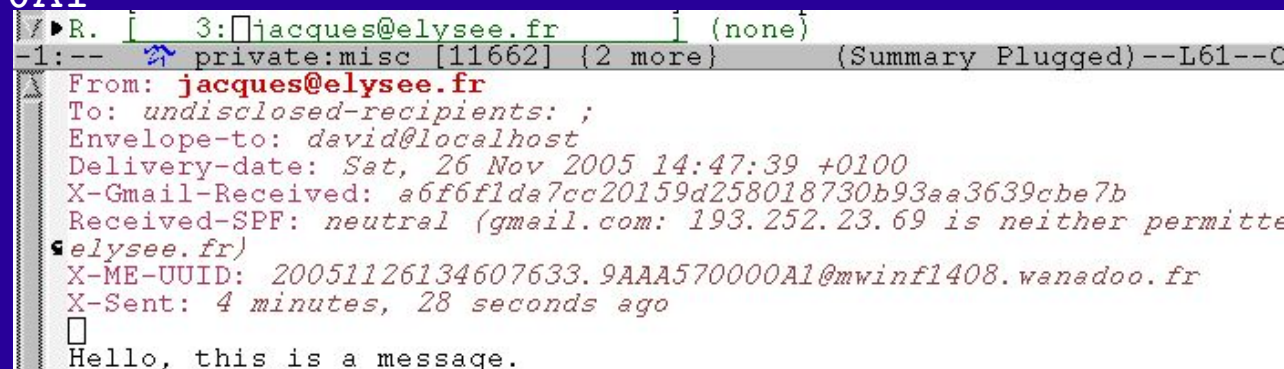
(très fortement inspiré par une présentation similaire de Thomas Petazzoni)

Pourquoi utiliser des courriels sécurisés ?

- Transfer de courriel est fait avec Simple Mail Transfer Protocol (SMTP, RFC 821)
- Pas d'authentification !
 - aucune garantie qu'un courriel provient de l'expéditeur
 - aucune garantie qu'un courriel n'a pas été modifié en cours de route
- Le courriel est envoyé en clair !
 - comment cacher le contenu au seul destinataire ?

Pourquoi authentifier un courriel ?

```
$ telnet smtp.wanadoo.fr 25
Trying 193.252.23.66...
Connected to smtp.wanadoo.fr.
Escape character is '^]'.
220 mwinfl1408.wanadoo.fr ESMTP ABO *****
HELO toto.com
250 mwinfl1408.wanadoo.fr
MAIL FROM:<jacques@elysee.fr>
250 Ok
RCPT TO:<david.mentre@gmail.com>
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Hello, this is a message.
.
250 Ok: queued as 9AAA570000A1
QUIT
221 Bye
```



The screenshot shows an email client interface with the following details:

- From: **jacques@elysee.fr**
- To: undisclosed-recipients: ;
- Envelope-to: david@localhost
- Delivery-date: Sat, 26 Nov 2005 14:47:39 +0100
- X-Gmail-Received: a6f6flda7cc20159d258018730b93aa3639cbe7b
- Received-SPF: neutral (gmail.com: 193.252.23.69 is neither permitted nor disallowed)
- X-ME-UUID: 20051126134607633.9AAA570000A1@mwinfl1408.wanadoo.fr
- X-Sent: 4 minutes, 28 seconds ago
- Content: Hello, this is a message.

Pourquoi cacher le contenu ?

```
[...]  
T 192.168.1.2:32801 -> 213.228.0.169:25 [AP]  
  MAIL FROM:<gnupgtest1@free.fr> SIZE=487..  
[...]  
T 192.168.1.2:32801 -> 213.228.0.169:25 [AP]  
  RCPT TO:<thomas.petazzoni@enix.org>..  
[...]  
T 192.168.1.2:32801 -> 213.228.0.169:25 [AP]  
  DATA..  
[...]  
T 192.168.1.2:32801 -> 213.228.0.169:25 [AP]  
  Message-ID: <417401D7.3080302@free.fr>..Date: Mon, 18 Oct 2004 19:48:07 +0200..From: GnuPG Test 1  
<gnupgtest1@free.fr>..User-Agent: Mozilla Thunderbird 0.8 (X11/20040926)..X-Accept-Language: en-us,  
en..MIME-Version: 1.0..To: thomas.petazzoni@enix.org..Subject: Nouvelles !..X-Enigmail-Version:  
0.86.1.0..X-Enigmail-Supports: pgp-inline, pgp-mime..Content-Type: text/plain; charset=ISO-8859-1;  
format=flowed..Content-Transfer-Encoding: 8bit....Salut !....Je suis . GULLIVER !....Thomas....  
[...]  
T 192.168.1.2:32801 -> 213.228.0.169:25 [AP]  
  QUIT..  
T 213.228.0.169:25 -> 192.168.1.2:32801 [AP]  
  221 Bye..
```

Objectifs du courriel sécurisé

- Confidentialité
 - contenu uniquement lisible par le destinataire
- Authentification
 - être sûr que l'expéditeur(trice) est effectivement bien lui/elle
- Non répudiation
 - personne ne peut dire qu'il/elle n'a pas envoyé un courriel
 - **partiellement** résolu (authentifie la source mais pas la date)
- Disponibilité
 - on peut toujours envoyé un courriel à un destinataire (pas résolu)

Plan

- Théorie (ultra-simplifiée) : mécanismes cryptographiques
 - cryptographie symétrique
 - cryptographie asymétrique
- Architecture : en qui avoir confiance ?
 - Infrastructure à clé publique (*Public Key Infrastructure* : PKI)
 - Réseau de confiance (*Web of Trust*)
- Le réseau de confiance en pratique
 - utilisation de GnuPG et Thunderbird/Enigmail

Partie I : Mécanismes cryptographiques

Cryptographie symétrique

- Utiliser un secret entre deux parties : la clé secrète
 - $\text{chiffré} := C(\text{clé}, \text{msg}) \rightarrow \text{chiffré} \rightarrow \text{msg} := D(\text{clé}, \text{chiffré})$
 - alias cryptographie à clé secrète
- De nombreux algorithmes : DES, AES, Twofish, ...
 - petits soucis à résoudre : choisir un algorithme, une taille de clé, ...
- Le gros problème : comment échanger une clé entre deux personnes qui ne se connaissent pas ?

Cryptographie asymétrique

- Une **paire** de clés : une clé publique et une clé privée
 - chiffrer avec la clé publique et déchiffrer avec la clé privée
 - signer avec la clé privée et vérifier avec la clé publique
 - alias cryptographie à clé publique
- Principal avantage ?
 - diffuser la clé publique tout en gardant la clé privée permet d'échanger des courriels sécurisés
 - une seule clé à diffuser
- Algorithmes : Diffie-Hellman, RSA (Rivest, Shamir, Adleman)

Cryptographie asymétrique : chiffrage



Alphonse chiffre avec
la clé **publique** de Bob

Bob déchiffre avec sa
clé **privée**

Cryptographie asymétrique : signature



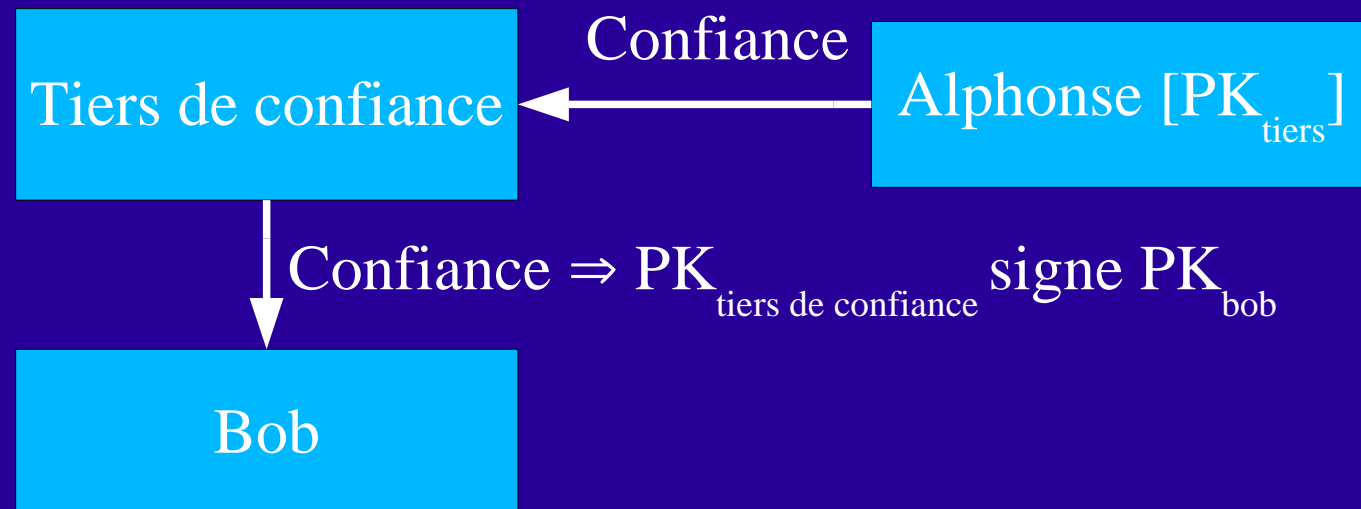
Alphonse signe avec
sa clé **privée**

Bob vérifie la signature
avec la clé **publique**
d'Alphonse

Partie II : Comment construire la confiance ?

Architecture : en qui croire ?

- **LE** problème : comment être sûr qu'une clé publique donnée est effectivement **la** clé publique de quelqu'un ?
 - faire signer par quelqu'un de confiance la clé publique d'autres
 - connaître la clé publique de la personne de confiance



⇒ Infrastructure à clé publique et Réseau de confiance

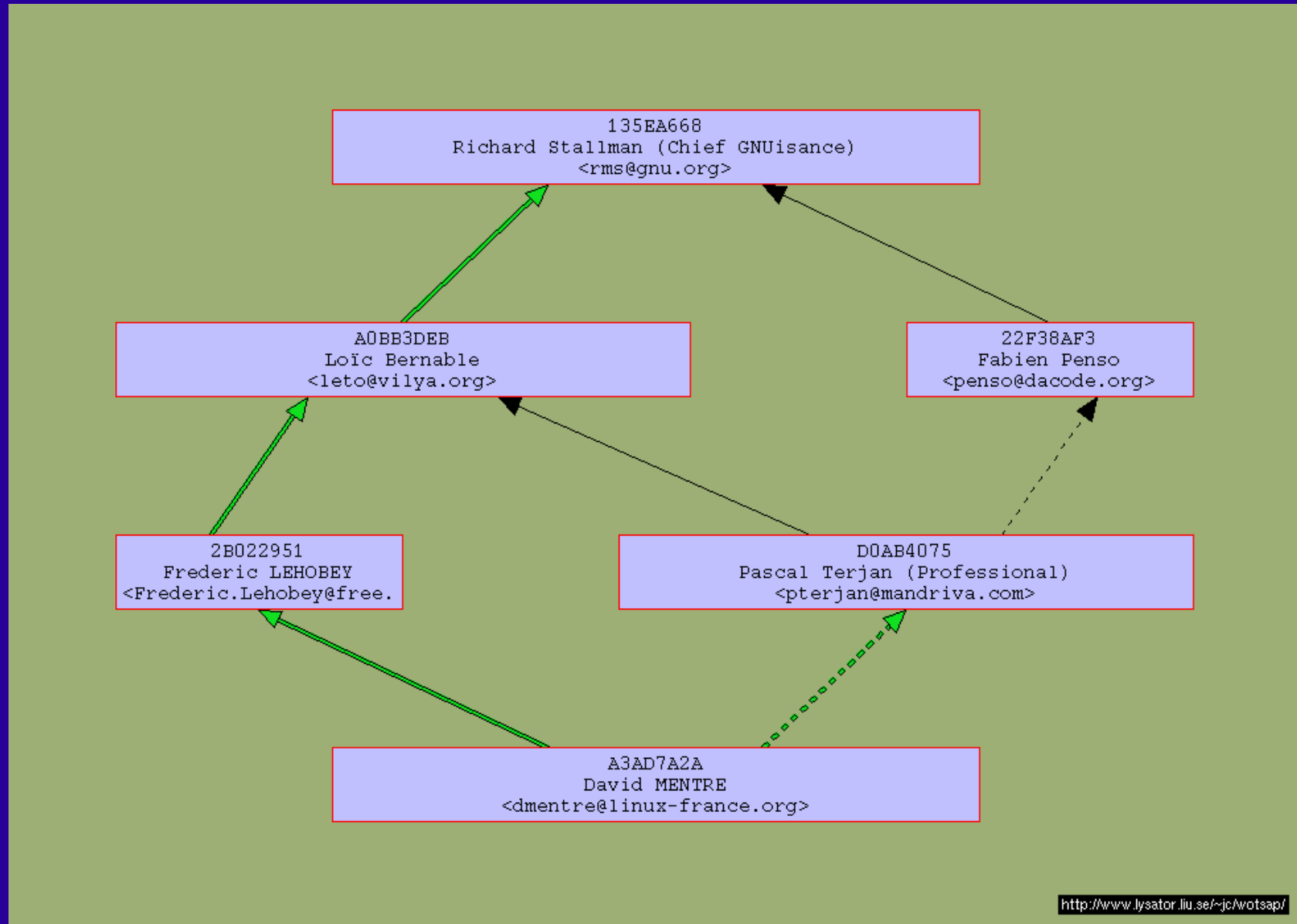
Infrastructure à clé publique (PKI)

- Construite sur des Autorités de Certification (CA : *Certificate Authority*) vues comme des tiers de confiance (standard X.509)
- Un CA par entreprise ou département
 - les CA sont organisés en une hiérarchie
- Une Autorité de Certification
 - produit le certificat qu'une clé publique est correcte pour elle
 - révoque les certificats
- Courriel sécurisé avec une PKI : S/MIME (RFC 3851)
- Désavantage : pas de CA pour le monde !

Réseau de confiance : principe

- Philosophie : vous faites confiance dans les personnes que vous avez physiquement rencontré et les personnes en qui elles font elles-même confiance \Rightarrow graphe de confiance
- Idée originale : PGP (Pretty Good Privacy)
- Standard : OpenPGP (RFC 2440)
- La confiance est exprimée par la signatures de clés publiques :
 - « Si j'ai vérifié la clé publique de quelqu'un, je la signe. Vous pouvez me faire confiance pour la vérification de signature. »

Réseau de confiance : un exemple



webware.lysator.liu.se/jc/wotsap

(Parenthèse) Au-delà du courriel : le web

- SSL (*Secure Socket Layer*) et TLS (*Transport Layer Security*)
 - utilise la cryptographie asymétrique pour l'établissement de connexion et l'authentification
 - utilise la cryptographie symétrique pour l'échange de données
 - utilise une Infrastructure à clé publique avec des Autorités de Certification privées (Verisign, RSA Security, etc.)

Certificat sur le web : un exemple

The screenshot shows a Mozilla Firefox browser window displaying the website <https://linuxfr.org/pub/>. The browser's address bar shows the URL and a lock icon, indicating a secure connection. The browser's menu bar includes 'Fichier', 'Edition', 'Affichage', 'Aller à', 'Marque-pages', 'Outils', and 'Aide'. The browser's toolbar includes navigation buttons (back, forward, home, stop, reload) and a search bar.

The 'Informations sur la page' (Page Information) window is open, showing the 'Sécurité' (Security) tab. It displays the following information:

- Identité du site Web vérifiée**
Le site Web linuxfr.org supporte l'authentification pour la page que vous allez voir. L'identité du site Web a été vérifiée par Association LinuxFr, une autorité de certificat que vous avez choisie pour cette tâche.
- Voir** Voir le certificat de sécurité qui vérifie l'identité du site Web.
- Connexion chiffrée : chiffrement de haut niveau (AES-256 256 bit)**
La page que vous voyez a été chiffrée avant sa transmission sur Internet. Le chiffrement rend très difficile aux personnes non autorisées la visualisation de la page durant son transit entre ordinateurs. Il est donc très improbable que quelqu'un puisse lire cette page durant son transit sur le réseau.

The 'Détails du certificat : "linuxfr.org"' (Certificate Details: "linuxfr.org") window is also open, showing the 'Général' (General) tab. It displays the following information:

- Ce certificat a été vérifié pour les utilisations suivantes :**
 - Certificat client SSL
 - Certificat serveur SSL
- Émis pour**
 - Nom commun (CN): linuxfr.org
 - Organisation (O): Association LinuxFr
 - Unité d'organisation (OU): Les admins réunis
 - Numéro de série: 00
- Émis par**
 - Nom commun (CN): linuxfr.org
 - Organisation (O): Association LinuxFr
 - Unité d'organisation (OU): Les admins réunis
- Validité**
 - Émis le: 14.10.2002
 - Expire le: 01.03.2030
- Empreintes numériques**
 - Empreinte numérique SHA1: CE:09:53:F0:B2:69:CD:58:3D:95:E5:72:26:A3:6B:73:C6:C2:4E:FE
 - Empreinte numérique MD5: 2C:97:D6:AA:1E:AC:0B:9B:D5:A8:19:42:07:92:AB:71

Un autre exemple d'actualité

The screenshot shows a Mozilla Firefox browser window with the address bar displaying `https://cfspart.impots.gouv.fr/portal/dgi/public/perso?pageld=pna2par&sfid=30`. Two security-related dialog boxes are open over the browser content.

Informations sur la page

Général | Formulaires | Liens | Média | Sécurité

Identité du site Web vérifiée

Le site Web `cfspart.impots.gouv.fr` supporte l'authentification pour la page que vous allez voir. L'identité du site Web a été vérifiée par Thawte Consulting cc, une autorité de certificat que vous avez choisie pour cette tâche.

[Voir](#) Voir le certificat de sécurité qui vérifie l'identité du site Web.

Connexion chiffrée : chiffrement de haut niveau (RC4 128 bit)

La page que vous voyez a été chiffrée avant sa transmission sur Internet. Le chiffrement rend très difficile aux personnes non autorisées la visualisation de la page durant son transit entre ordinateurs. Il est donc très improbable que quelqu'un puisse lire cette page durant son transit sur le réseau.

Détails du certificat : "cfspart.impots.gouv.fr"

Général | Détails

Ce certificat a été vérifié pour les utilisations suivantes :

Certificat serveur SSL

Émis pour

Nom commun (CN)	cfspart.impots.gouv.fr
Organisation (O)	DIRECTION GENERALE DES IMPOTS
Unité d'organisation (OU)	Provided by TBS INTERNET http://www.tbs-certificats.com/
Numéro de série	3F:65:67

Émis par

Nom commun (CN)	Thawte Premium Server CA
Organisation (O)	Thawte Consulting cc
Unité d'organisation (OU)	Certification Services Division

Validité

Émis le	26.05.2005
Expire le	26.05.2007

Empreintes numériques

Empreinte numérique SHA1	C5:0B:AB:47:AD:F5:E5:E7:B5:C8:92:4A:50:9C:16:BD:04:9F:81:0E
Empreinte numérique MD5	AB:A1:1C:96:EE:E4:A5:FE:C0:E8:62:4E:18:D2:24:7E

[Aide](#) [Fermer](#)

Partie III : Le courriel sécurisé en pratique

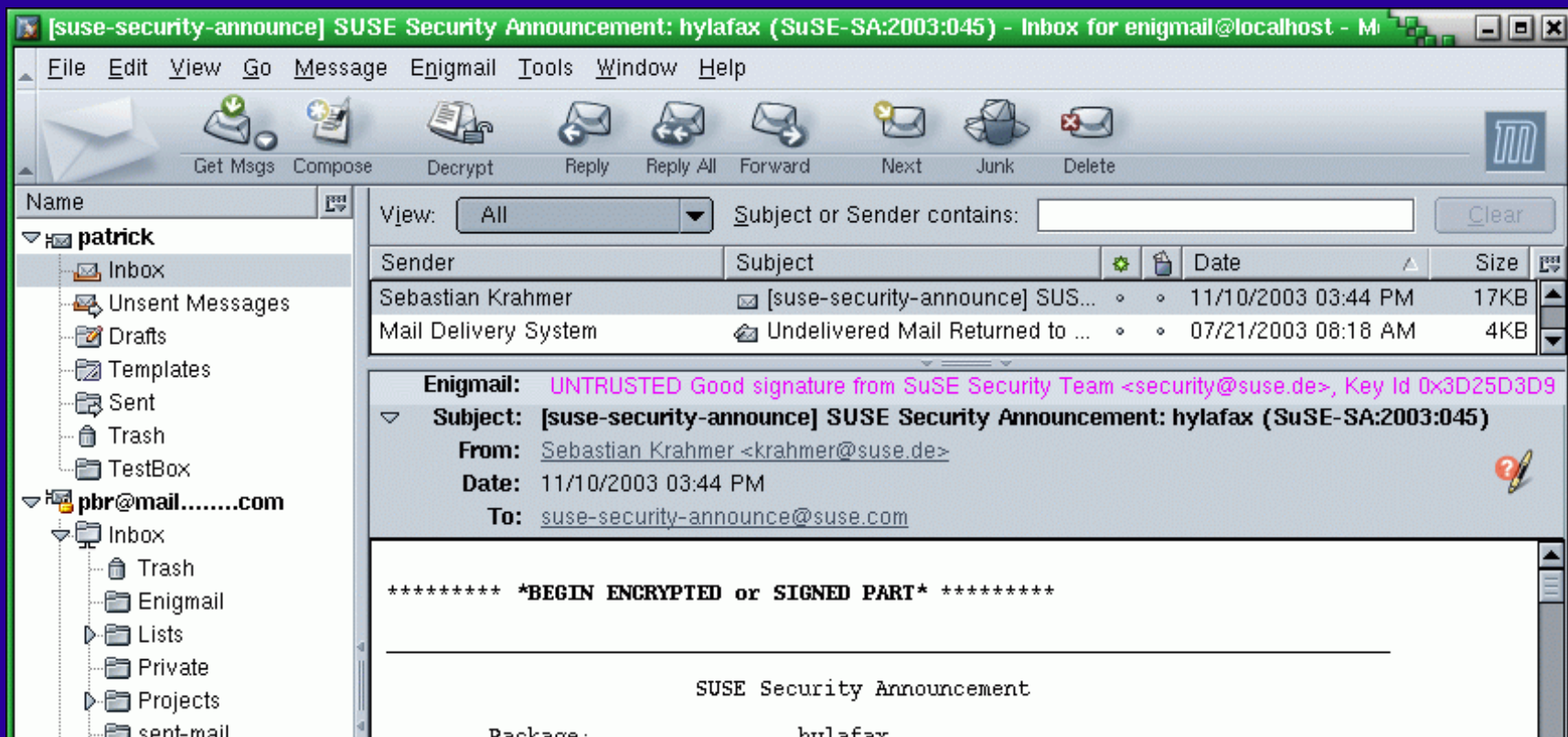
Exemples avec GnuPG et Thunderbird/Enigmail

Courriels sécurisés en pratique : GnuPG

- GnuPG : GNU Privacy Guard (gnupg.org)
- Logiciel libre
 - donc vous pouvez vérifier son fonctionnement interne
- Contient :
 - un outil en ligne de commande
 - des algorithmes de cryptographie symétrique et asymétrique
 - le protocole OpenPGP pour l'échange de courriels sécurisés (chiffrage et signature)
 - le stockage et la vérification des clés publiques des correspondants

Courriels sécurisés au quotidien

- Tous les logiciels de courriels supportent OpenPGP
 - e.g. GPGol : greffon pour Outlook
 - e.g. Enigmail : extension pour Mozilla Thunderbird



Créer votre paire de clés

- Créer votre paire de clés

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

- Créer un certificat de révocation

– au cas où votre clé serait perdue (ou son mot de passe !) ou volée

```
$ gpg --output revoke.asc --gen-revoke  
mykey
```

- Lister les clés stockés dans votre trousseau

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

Composants d'une clé publique

```
$ gpg --list-keys --fingerprint dmentre
pub      1024D/A3AD7A2A 2004-10-03
        Key fingerprint = 5996 CC46 4612 9CA4 3562
                           D7AC 6C67 9E96 A3AD 7A2A
uid      David MENTRE <dmentre@linux-france.org>
uid      David MENTRE <dmentre@ras.eu.org>
uid      David MENTRE <david.mentre@wanadoo.fr>
uid      David MENTRE <david.mentre@gmail.com>
sub      1024g/65B52967 2004-10-03
```

- Identifiant de clé : **A3AD7A2A**
- Empreinte utilisée pour vérifier l'exactitude d'une clé :

5996 CC46 4612 9CA4 3562

D7AC 6C67 9E96 A3AD 7A2A

5996 CC46 4612 9CA4 3562 D7AC 6C67 9E96 A3AD 7A2A

Créer votre paire de clé avec Enigmail

The screenshot shows the 'Génération de clef OpenPGP' (OpenPGP Key Generation) window. At the top, the title bar reads 'Génération de clef OpenPGP'. Below it, the 'Compte / ID utilisateur' (Account / User ID) field contains 'David MENTRE <mentre@tcl.ite.mee.com> - ITE-TCL\Mentre\dme'. A checked checkbox 'Utiliser la clef générée pour l'identité sélectionnée' (Use the generated key for the selected identity) is present. Below this, there is an unchecked checkbox 'Pas de phrase secrète' (No passphrase). The 'Phrase secrète' (Passphrase) and 'Répétez la phrase secrète' (Repeat the passphrase) fields both contain '*****'. A 'Commentaire' (Comment) field is empty. The 'Expiration de la clef' (Key expiration) section has a tab labeled 'Avancé' (Advanced). In this section, 'La clef expire dans' (The key expires in) is set to '5' 'années' (years). A checked checkbox 'La clef n'expire jamais' (The key never expires) is also visible. At the bottom left, there are two buttons: 'Générer la clef' (Generate the key) and 'Annuler' (Cancel). At the bottom right, there is a 'Console de génération de clefs' (Key generation console) section containing a 'NOTE: La génération d'une clef peut prendre plusieurs minutes. Ne quittez pas l'application tant que la génération est en cours. La navigation intensive sur le web ou les opérations intenses sur les disques durs pendant la génération de la clef augmenteront l'entropie et accéléreront le processus. Vous serez averti quand l'opération sera terminée.' Below the note is a progress bar.

Génération de clef OpenPGP

Compte / ID utilisateur David MENTRE <mentre@tcl.ite.mee.com> - ITE-TCL\Mentre\dme

☒ Utiliser la clef générée pour l'identité sélectionnée

☐ Pas de phrase secrète

Phrase secrète ***** Répétez la phrase secrète *****

Commentaire

Expiration de la clef Avancé

La clef expire dans 5 années ☒ La clef n'expire jamais

Générer la clef Annuler

Console de génération de clefs

NOTE: La génération d'une clef peut prendre plusieurs minutes. Ne quittez pas l'application tant que la génération est en cours. La navigation intensive sur le web ou les opérations intenses sur les disques durs pendant la génération de la clef augmenteront l'entropie et accéléreront le processus. Vous serez averti quand l'opération sera terminée.

Créer un certificat de révocation



Échange manuel de clés

- Exporter une clé

```
$ gpg --output david.gpg --armor --export  
dmentre
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
Version: GnuPG v1.4.1 (GNU/Linux)
```

```
mQGibEFgIo8RBACrRlbrLm+Il/8+KBXwR+Ek2TaF3Q+F5UUhsy07kyl+8gAG9CGl  
Azj4t3InMwnGOyGZR5jg5q5wH/m2T4+vaeVXY0TaqRitgHoA1dSkgYK0TYeBJaOY  
[...]
```

Envoyer le fichier `david.gpg` au destinataire

- Importer une clé

```
$ gpg --import david.gpg
```

- Pas très pratique à utiliser !

Échange de clé avec un serveur

- Plusieurs serveurs sur Internet, par ex. `pgp.mit.edu`
- Importer/exporter clés et signatures de/vers un serveur
 - envoyer votre clé vers un serveur

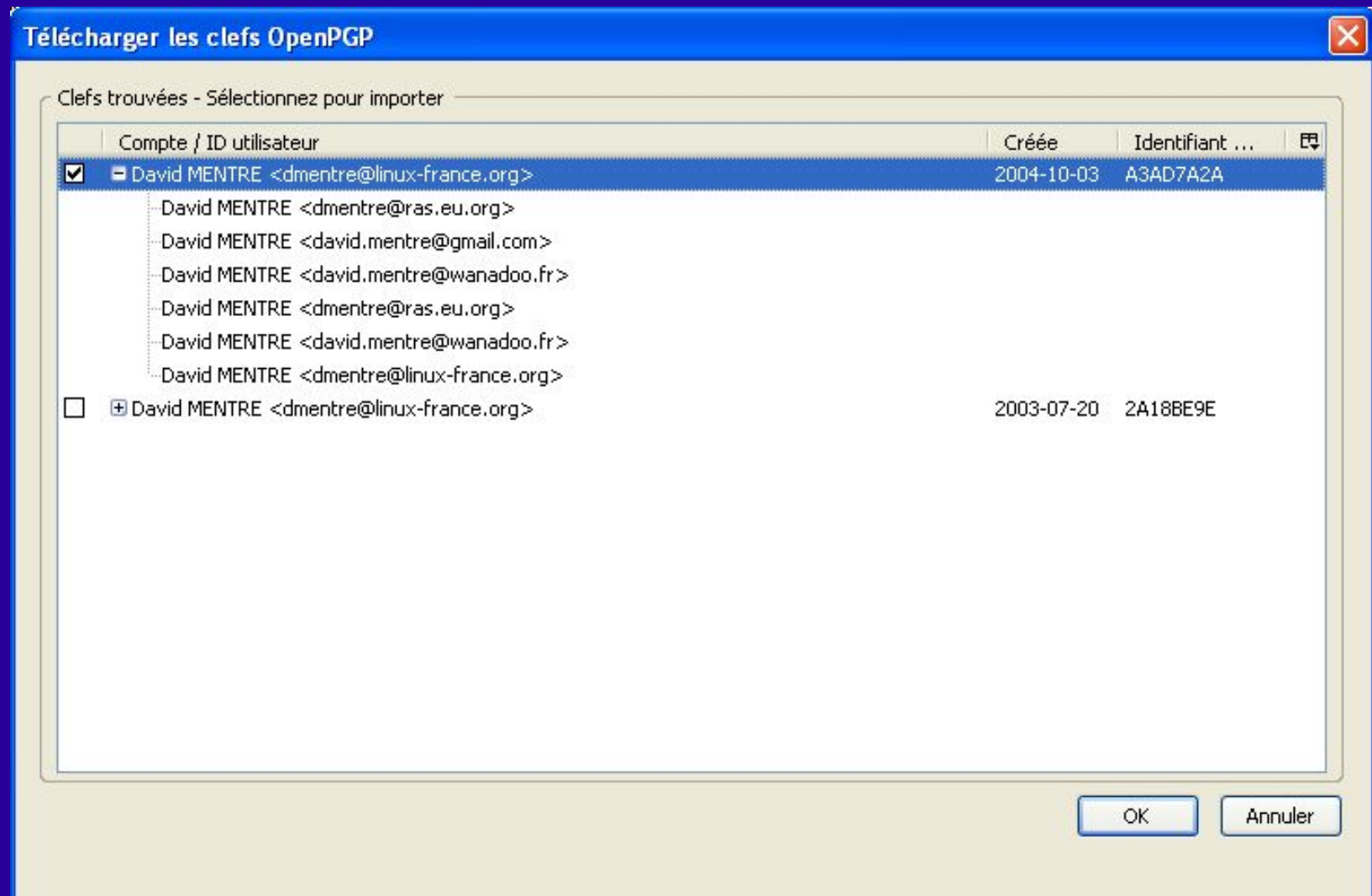
```
$ gpg --keyserver pgp.mit.edu --send-key dmentre
```
 - importer une clé d'un serveur

```
$ gpg --keyserver pgp.mit.edu --search-key  
alphonse@domain.com
```
- Rafraichir les clés à partir d'un serveur

```
$ gpg --refresh-keys
```
- Serveurs permettent l'échange de clé \Rightarrow un seul export nécessaire

Échange de clé avec Enigmail

- Après une recherche de la clé « dmentre »...



Comment signer la clé d'un autre ?

1. Récupérer la clé d'un serveur de clé

```
$ gpg --search-key dmentre avec le courriel
```

```
$ gpg --recv-key A3AD7A2A avec l'identifiant de clé
```

2. Vérifier l'empreinte (*fingerprint*)

3. Signer la clé

```
$ gpg --edit-key dmentre
```

```
> sign    Vérifiez l'empreinte à cette étape !!
```

```
> quit
```

4. Exporter la clé signée vers un serveur de clé

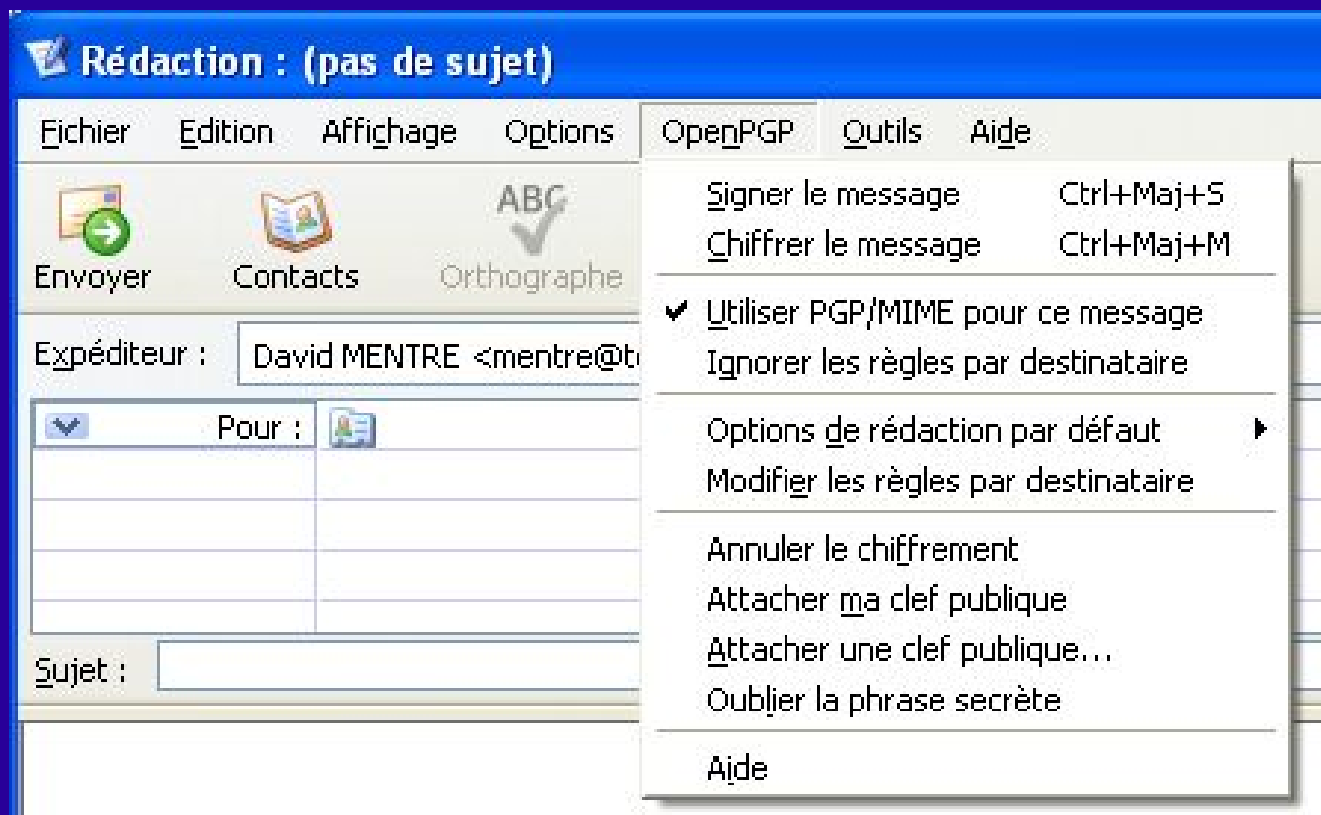
```
$ gpg --send-key dmentre
```

Comment signer une clé avec Enigmail



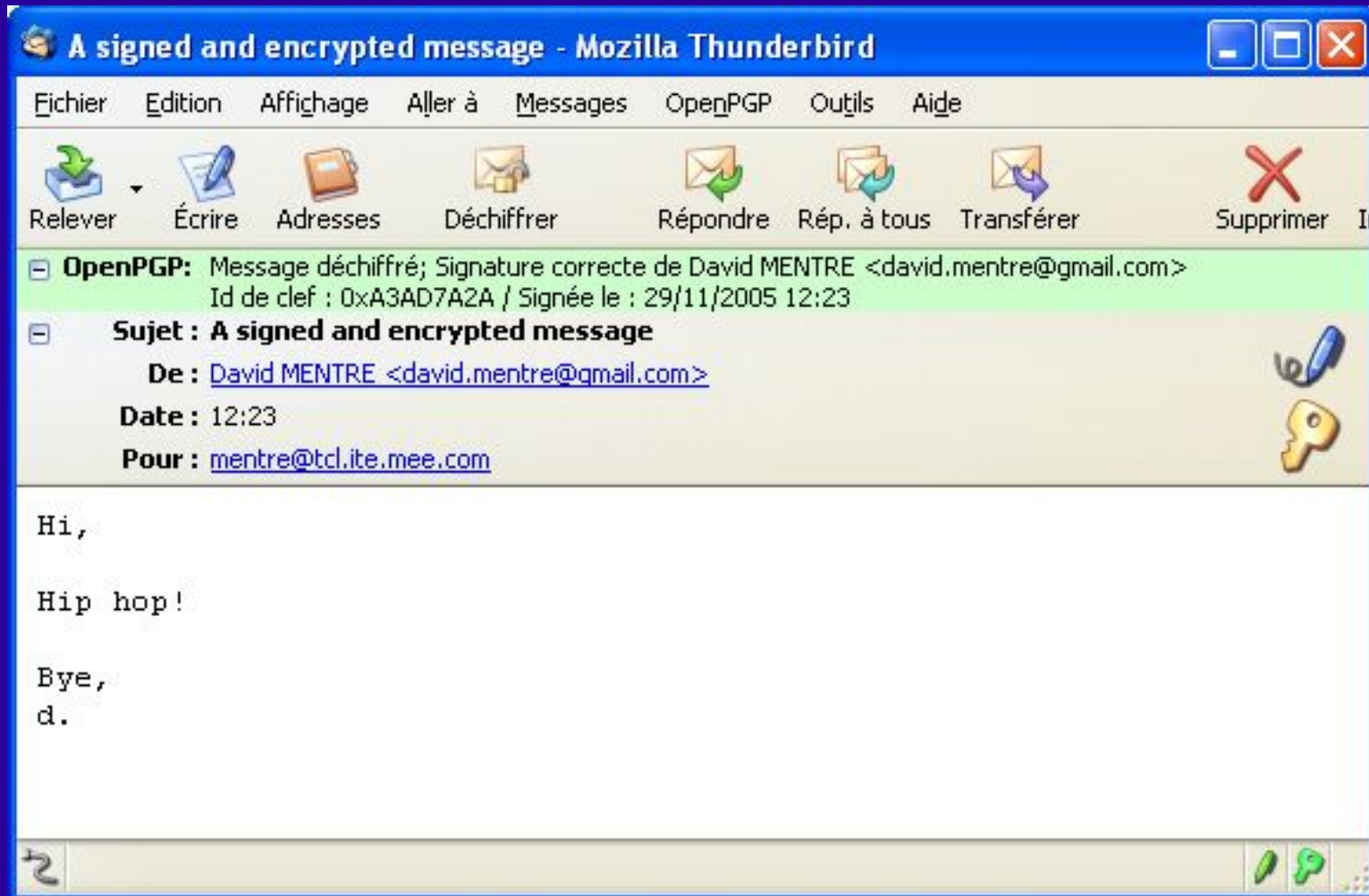
Envoyer un courriel sécurisé

- Utilisez simplement l'interface de votre logiciel de courriel



Recevoir un email chiffré et signé

- Les logiciels de courriel déchiffrent automatiquement le contenu et vérifient la signature



Contenu d'un message chiffré et signé

Date: Tue, 29 Nov 2005 14:52:33 +0100

From: David MENTRE <mentre@tcl.ite.mee.com>

MIME-Version: 1.0

To: david.mentre@gmail.com

Subject: encrypted email content

Content-Type: multipart/encrypted;
protocol="application/pgp-encrypted";
boundary="-----enig31236E9C912440E0D951EF74"

Lines: 61

This is an OpenPGP/MIME encrypted message (RFC 2440 and 3156)

-----enig31236E9C912440E0D951EF74

Content-Type: application/pgp-encrypted

Content-Description: PGP/MIME version identification

Version: 1

-----enig31236E9C912440E0D951EF74

Content-Type: application/octet-stream; name="encrypted.asc"

Content-Description: OpenPGP encrypted message

Content-Disposition: inline; filename="encrypted.asc"

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

Version: GnuPG v1.4.2 (MingW32)

hQEOA2CDNspltSlnEAP5AReLVv/HOC7JT5Ni1O2dd5mdbC8/UySdgD4IolLsYQAQ9
DvUMKVVIrqJYk0DSCwd9UewHFjURMtHwBC2tFM4ZZO2GnE0YodJIMYhRC5zZr9tM

Échange de fichier sécurisé (hors courriel)

- Chiffrer un fichier pour quelqu'un

```
$ gpg --output doc.enc --encrypt  
    --recipient user@domain.org doc
```

- Déchiffrer un fichier reçu

```
$ gpg --output doc --decrypt doc.enc
```

- Signer un fichier avec votre signature

```
$ gpg --output doc.sig --detach-sig doc
```

- Vérifier un fichier signé

```
$ gpg --verify doc.sig doc
```

Pour conclure...

- Un courriel standard est comme une carte postale...
... donc l'échange de courriels sécurisés est une nécessité !
- Cryptographie symétrique et asymétrique sont utilisées simultanément pour sécuriser les échanges de données
- Architecture à utiliser, dépend du contexte :
 - PKI : utilisé fréquemment au sein d'une entreprise
 - Réseau de confiance : échanges internationaux
- Une fois que votre clé publique est sur un serveur, l'échange de courriels sécurisé n'est pas très difficile

Liens

- GnuPG : gnupg.org
- Enigmail pour Mozilla Thunderbird : enigmail.mozdev.org
- Détails légaux : www.ssi.gouv.fr
- Trouver un chemin de confiance entre vous et un autre :
www.cs.uu.nl/~henkp/henkp/pgp/pathfinder/
webware.lysator.liu.se/jc/wotsap

Des questions ?

