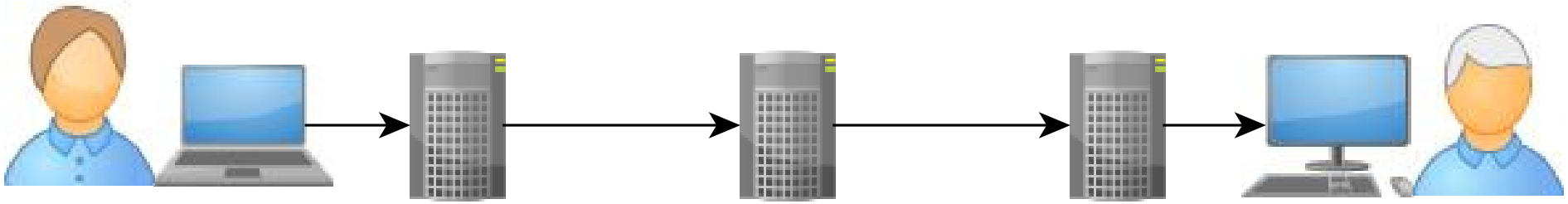
Introduction à la sécurisation de ses mails

MicroJoe

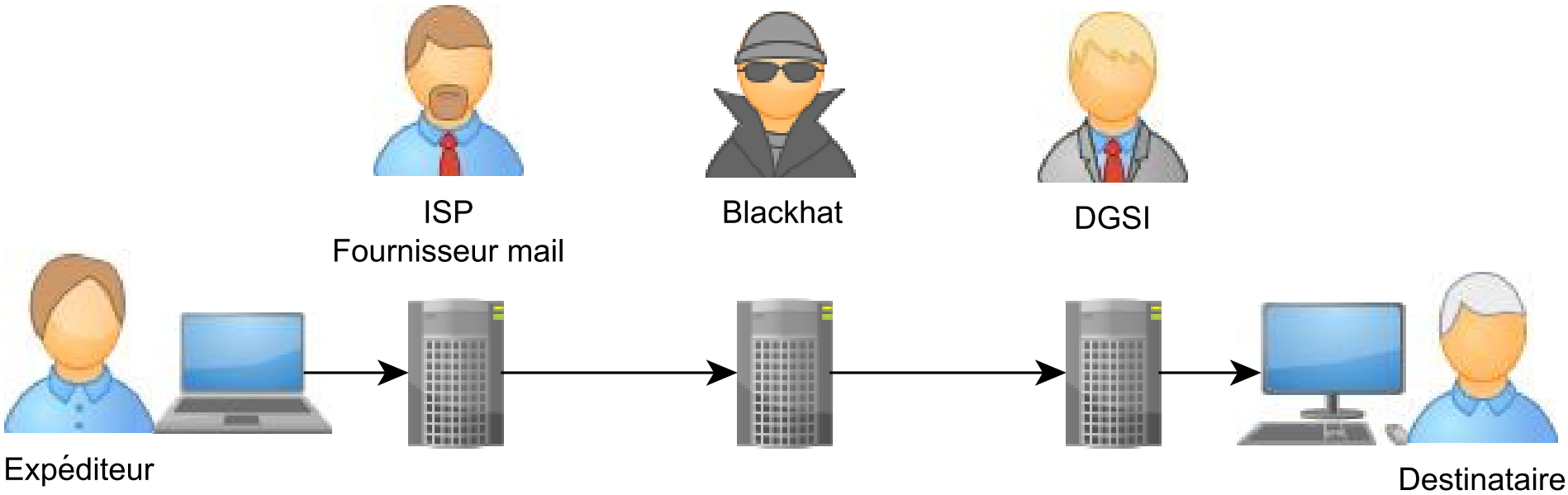
HAUMTalks

15 octobre 2014

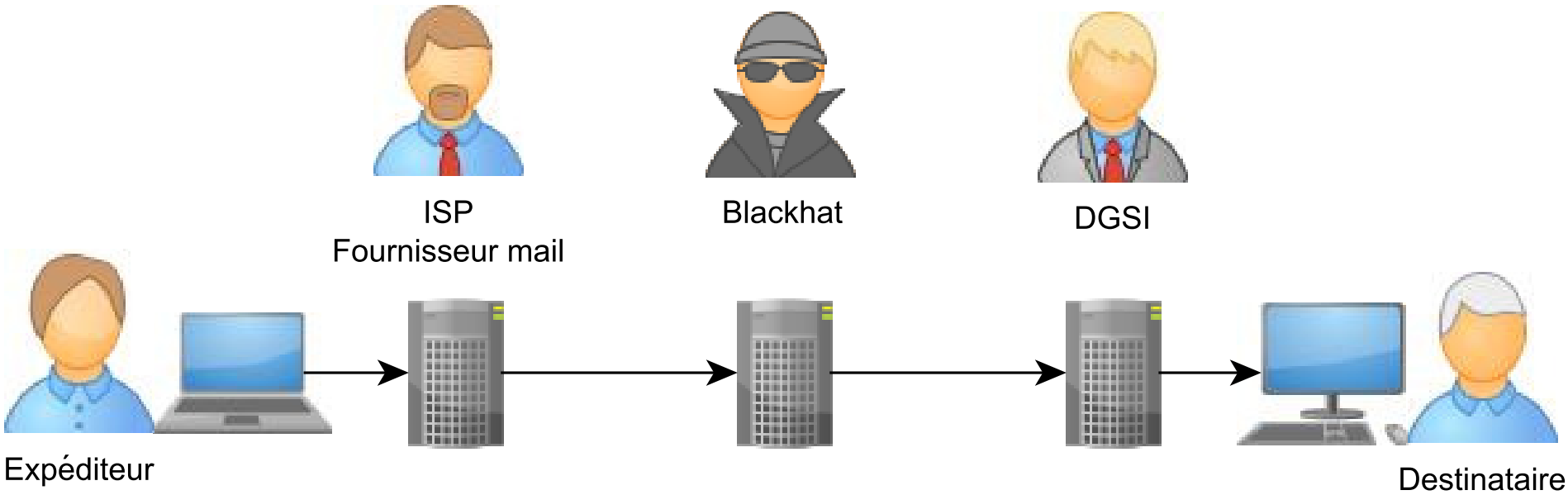
Distribution du courrier



Distribution du courrier



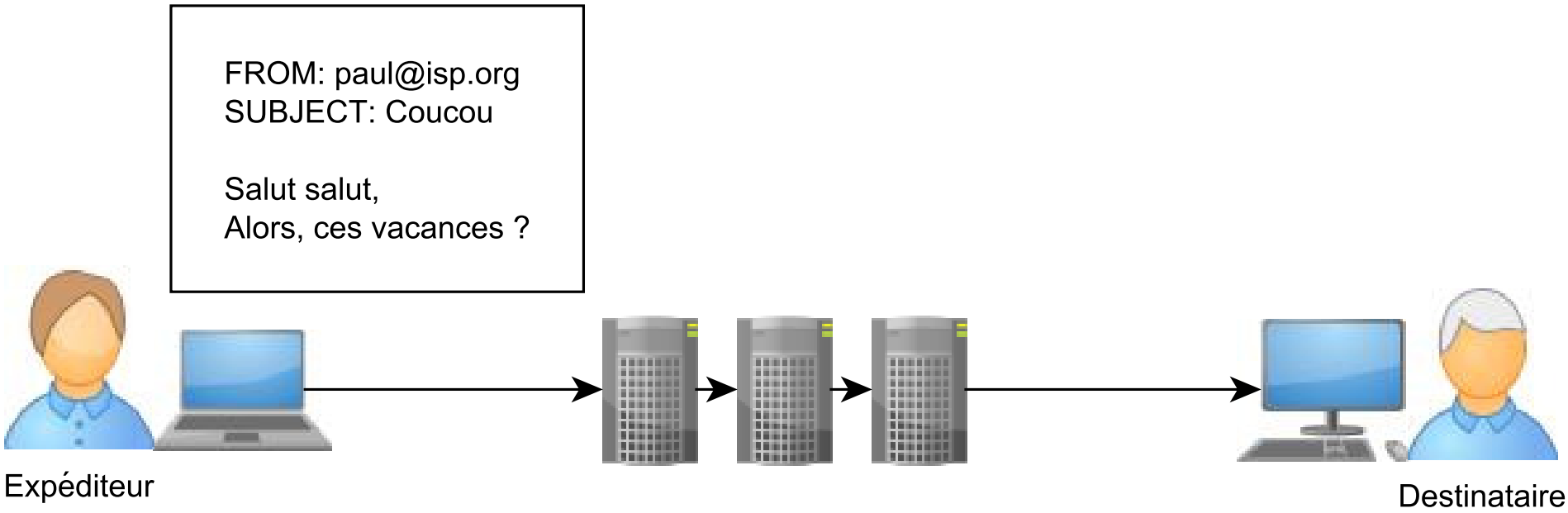
Distribution du courrier



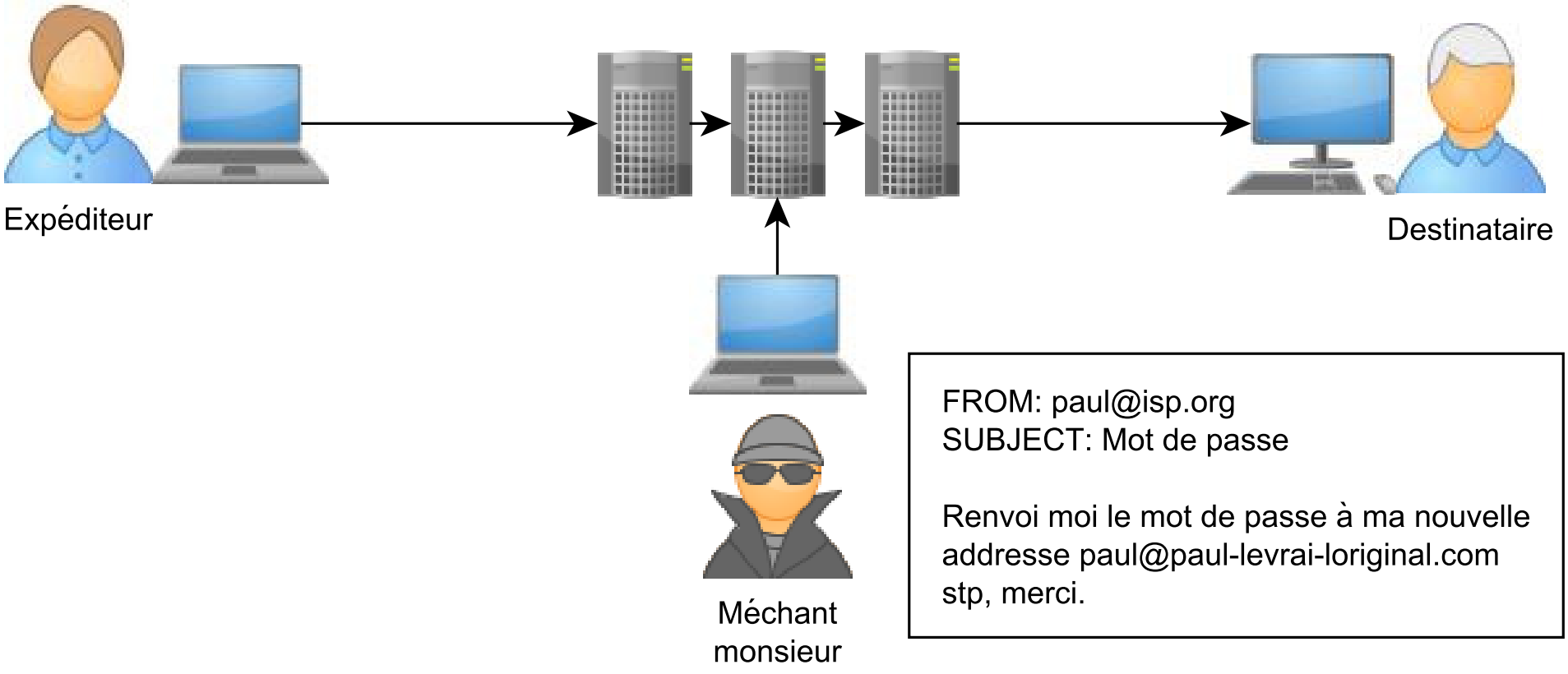
Problème

Contenu du mail accessible pendant la distribution.

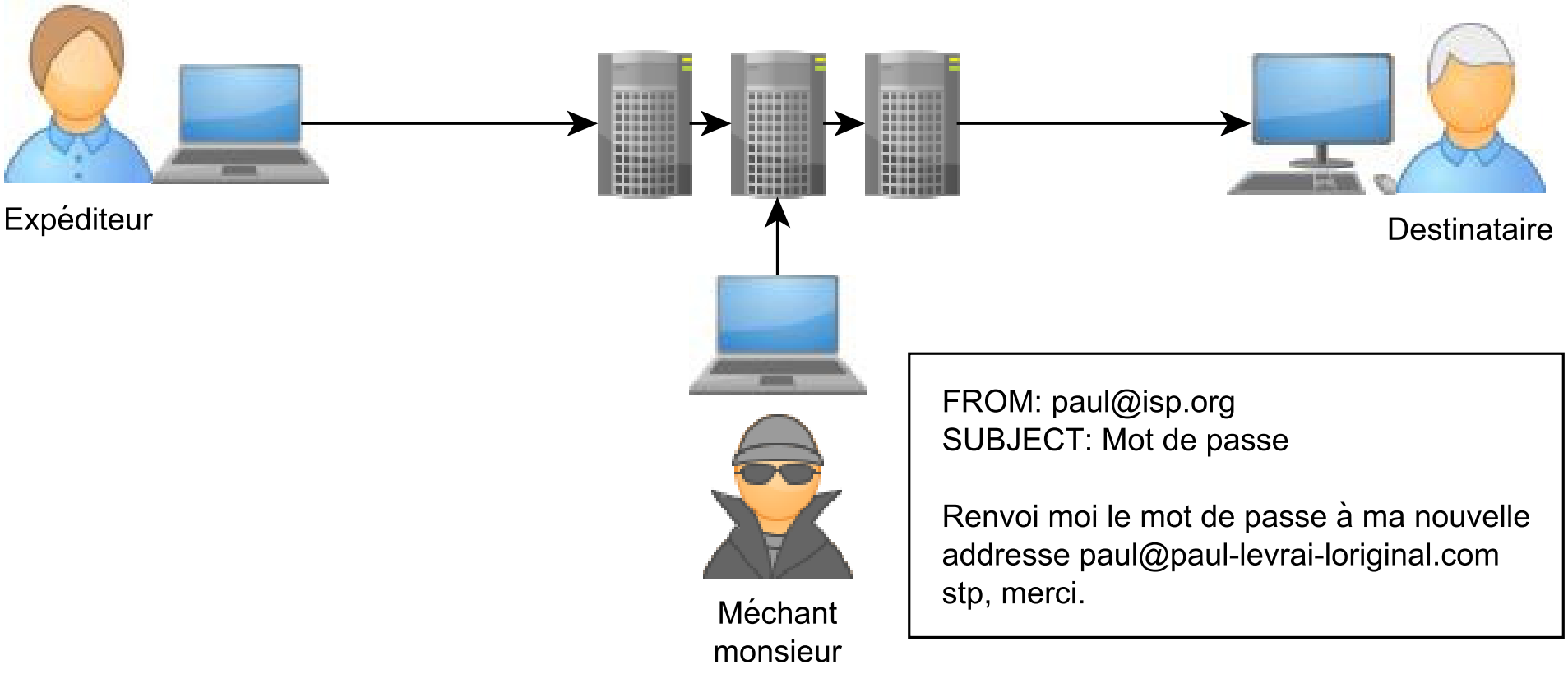
Envoi avec addresse bidon



Envoi avec addresse bidon



Envoi avec addresse bidon



Problème

Aucune certitude sur la provenance d'un mail.

Principe clés publiques/privées

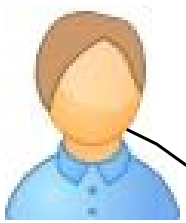
Clé publique

Rôle : permet de chiffrer des messages.
Disponibilité : tout le monde peut y avoir accès

Clé privée

Rôle : Permet de déchiffrer des messages.
Disponibilité : aucune, doit être gardée secrète

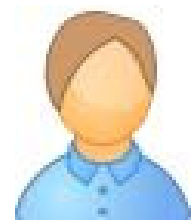
Chiffrer/déchiffrer



Clé PUBLIQUE

Clé PRIVÉE

Expéditeur



Clé PUBLIQUE

Clé PRIVÉE

Destinataire

FROM: paul@isp.org
SUBJECT: Wassup?

Salut,
Comment ça va ?

FROM: paul@isp.org
SUBJECT: Wassup?

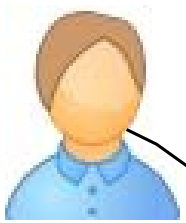
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2.0.17 (MingW32)

hQEMA/+ePNDuoKA8AQf/aFyThdp+
tub0ijp5B1kM7xrfSEkrbDG7B7ab+Vv
PGyDEQgzBdrw17vWl28oHVaMdfAK
o7L5yvvRfVHQfiFigDrKgCJsPp69jC
-----END PGP MESSAGE-----

FROM: paul@isp.org
SUBJECT: Wassup?

Salut,
Comment ça va ?

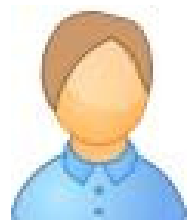
Apposition de signature



Clé PUBLIQUE

Clé PRIVÉE

Expéditeur



Clé PUBLIQUE

Clé PRIVÉE

Destinataire

FROM: paul@isp.org
SUBJECT: Wassup?

Salut,
Comment ça va ?

FROM: paul@isp.org
SUBJECT: Wassup?

-----BEGIN PGP SIGNED MESSAGE-----
Salut,
Comment ça va ?
-----BEGIN PGP SIGNATURE-----

iQA/AwUBN78ib3S9RCOKzj55
CDxKAFyaaGa835l1vpbFkAJk
=3r/N
-----END PGP MESSAGE-----

Signature OK

FROM: paul@isp.org
SUBJECT: Wassup?

Salut,
Comment ça va ?

Choix de méthode de sécurisation

destination	privée	publique
chiffrer	déconseillé	non
signer	déconseillé	oui
chiffrer+signer	oui	non

Logiciels de chiffremment et signature

OpenPGP format définit par l'IETF

PGP *Pretty Good Privacy*
logiciel pionnier semi-libre (1991)

GPG *GNU Privacy Guard*
équivalent libre de PGP

Intégration avec les clients mails

Thunderbird	plugin Enigmail
Mutt	natif
Re-Alpine	plugin Topal
Mail.app	plugin GPGMail

Le cas des webmails

- Envoi de la clé privée sur le serveur pour chiffer sur le serveur
- Extensions de navigateur pour chiffrer localement (quand dispo.)

Partage de clé publique

- Serveurs de clés publics (MIT, etc.)
- Hébergé sur son site/blog/...

Péremption de clé

- Choix de la durée de vie de la clé
- Plutôt préférer des clés à durée de vie courtes
- Révocation manuelle

Signature de clé

- Permet d'approuver la clé générée IRL
- Besoin de carte d'identité/d'un permis/etc.
- Se fait en réunion à une *signing-party*
- Pourquoi pas faire une *signing-party* au Mans

Questions