Eleven labs

Messagerie sécurisée avec OpenPGP

eleven-labs.com

Eleven labs

OpenPGP

Protocole d’échange de messages chiffrés

Gestion d’une identité numérique

- Toile de confiance

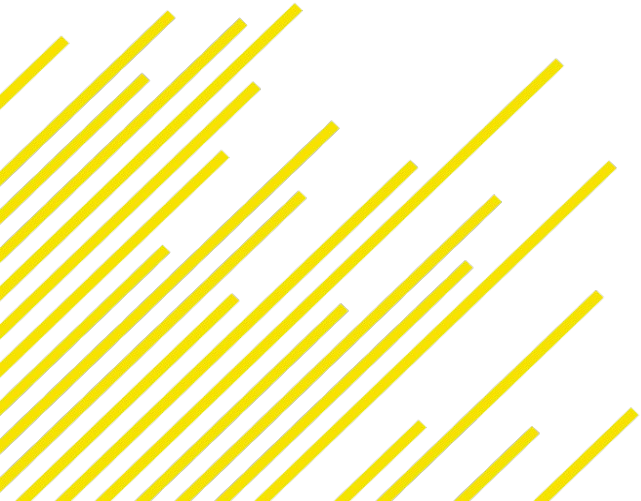
Authentification des messages

Décentralisé

Eleven labs

Problématique

Comment authentifier un utilisateur et sécuriser les messages dans une application ?



Eleven Labs

Sommaire

Les concepts OpenPGP

Authentification d’un utilisateur

Chiffrement et déchiffrement des messages

Implémentation et démo

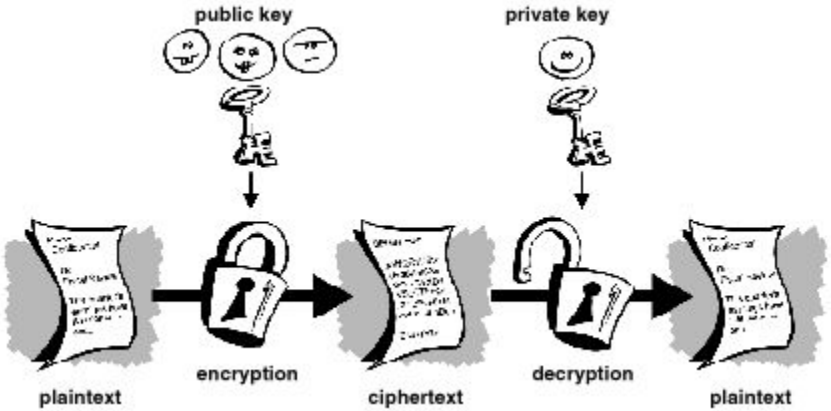
Eleven Labs

Sommaire

Eleven labs

Chiffrement asymétrique

Clef publique / clef privée



Eleven labs

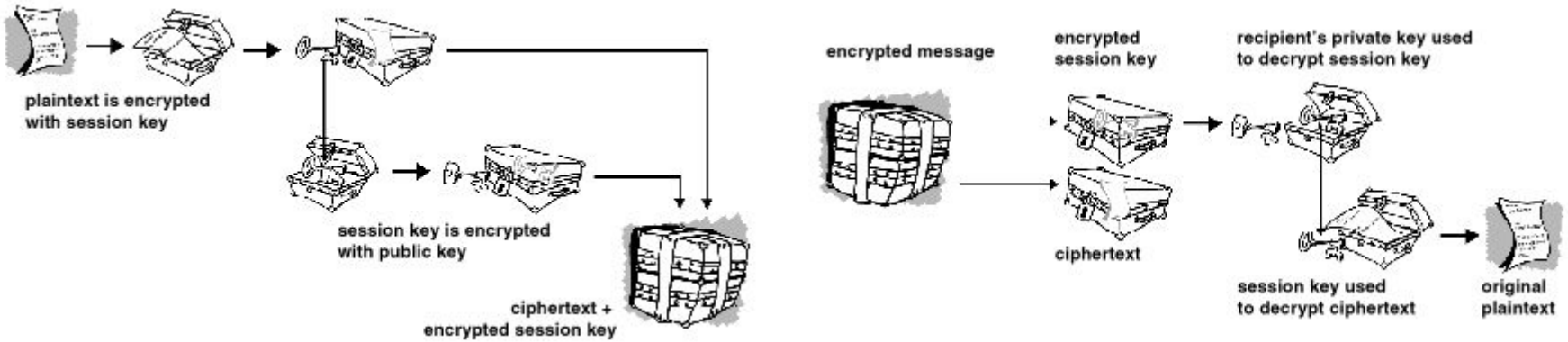
OpenPGP, PGP, GnuPG ?

OpenPGP : standard de chiffrement/déchiffrement RFC 4880

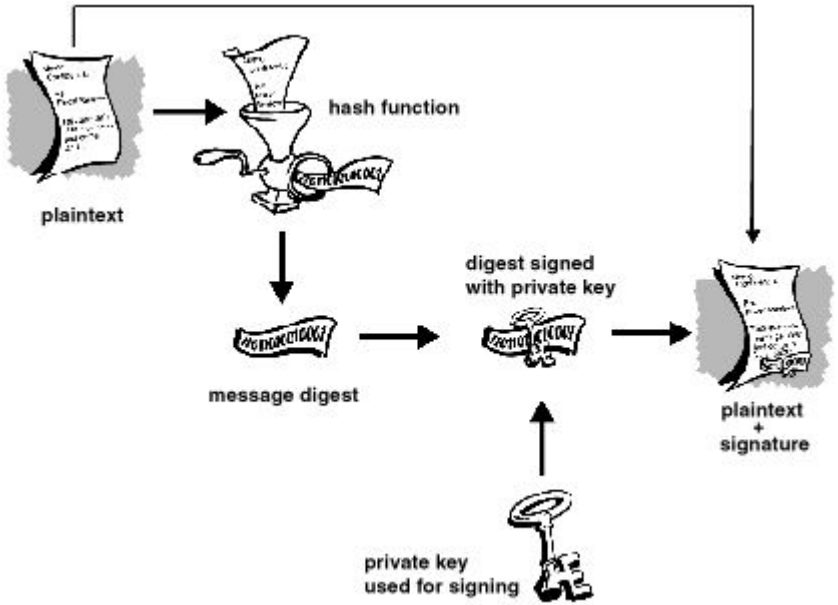
PGP : implémentation fermée d'OpenPGP

GnuPG : implémentation ouverte d'OpenPGP

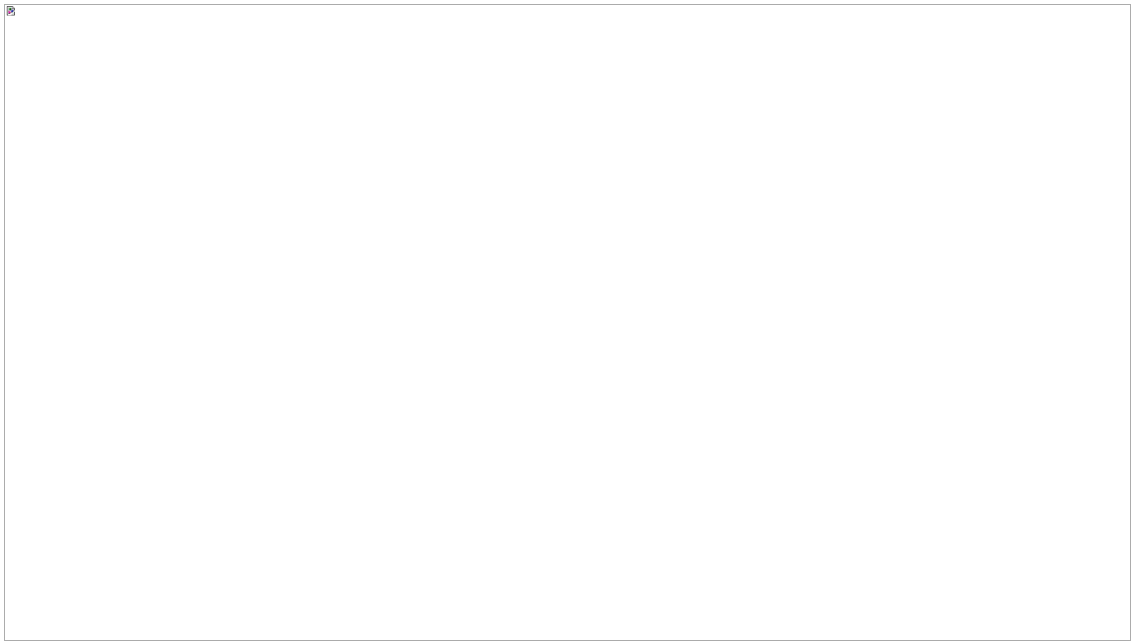
Fonctionnement OpenPGP



Signature des messages



Toile de confiance

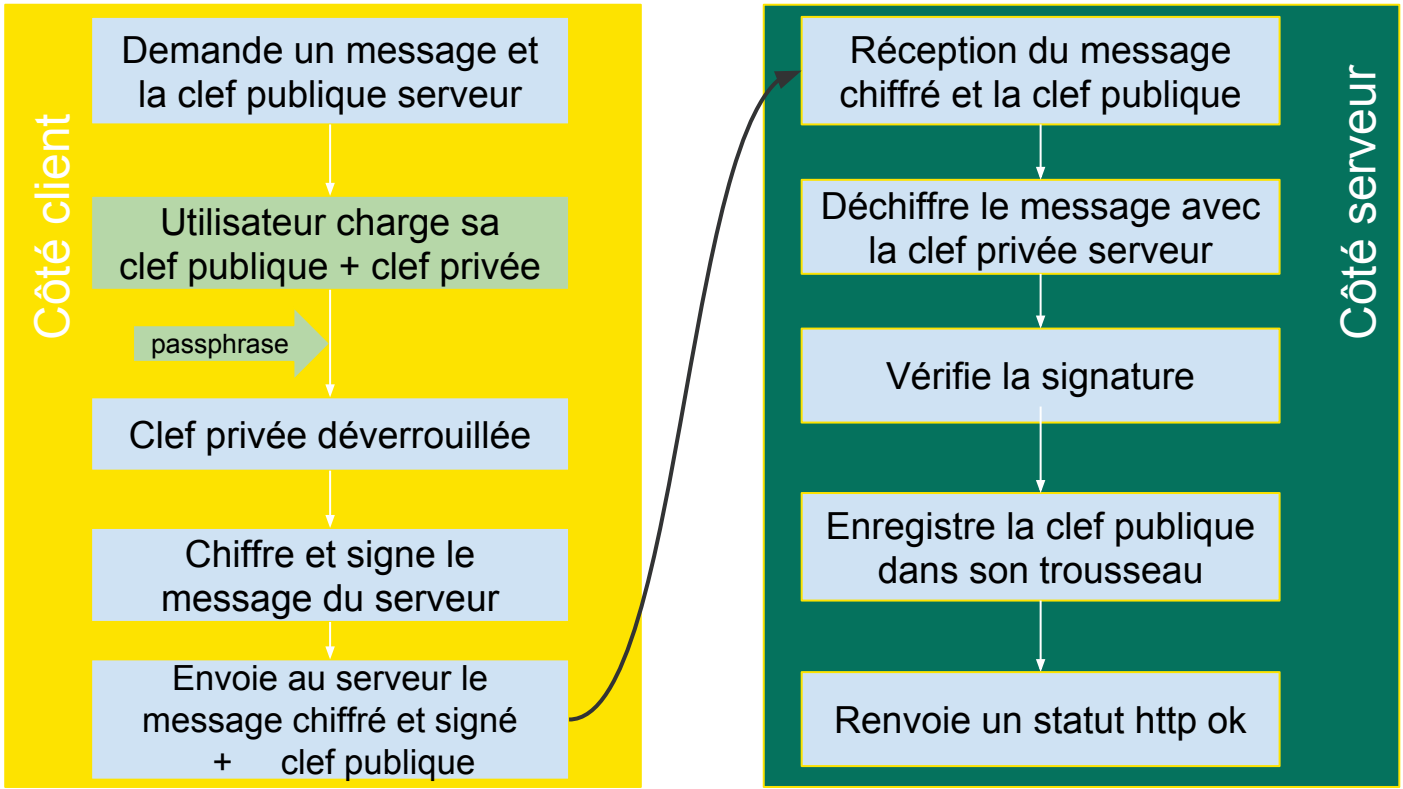


Eleven labs

Sommaire

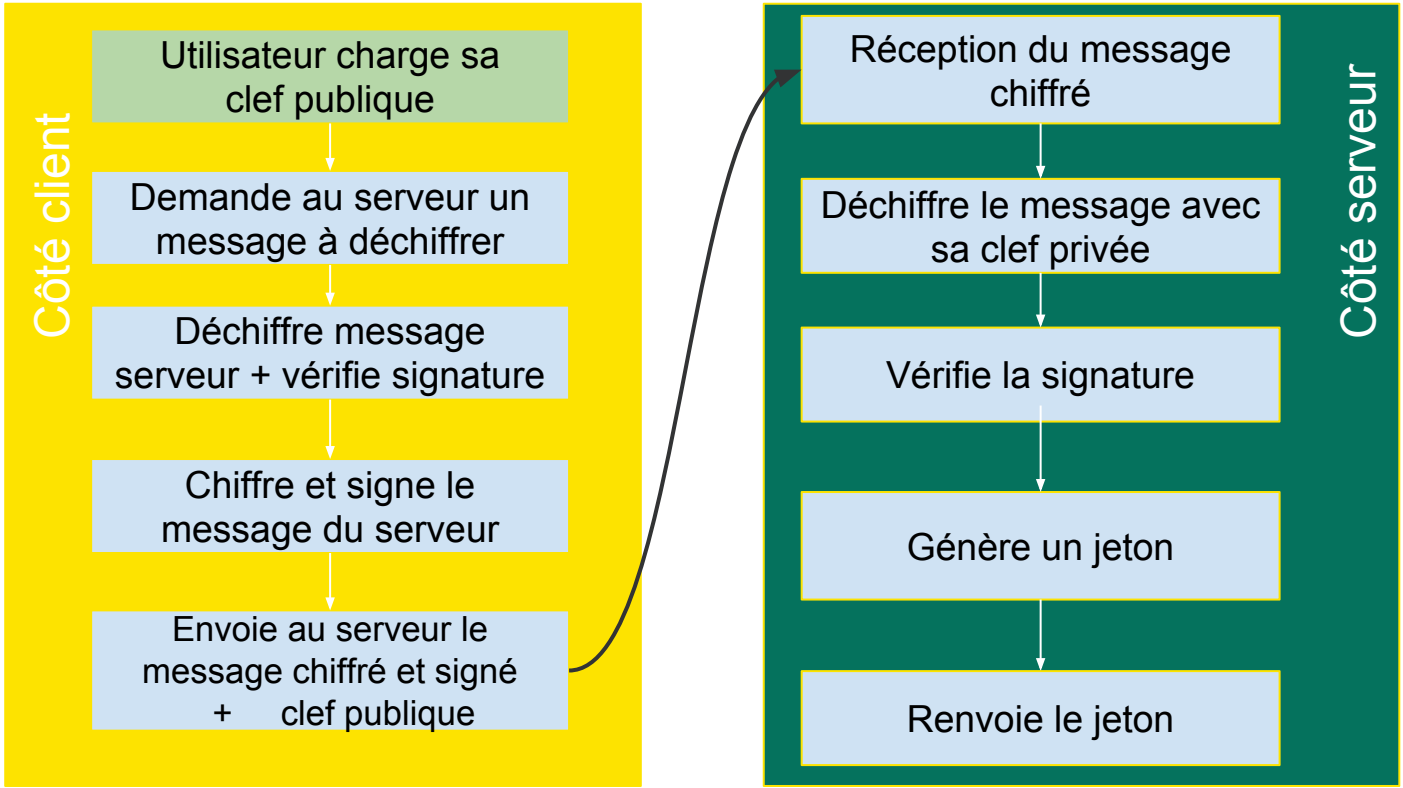
Eleven labs

Séquence d'inscription



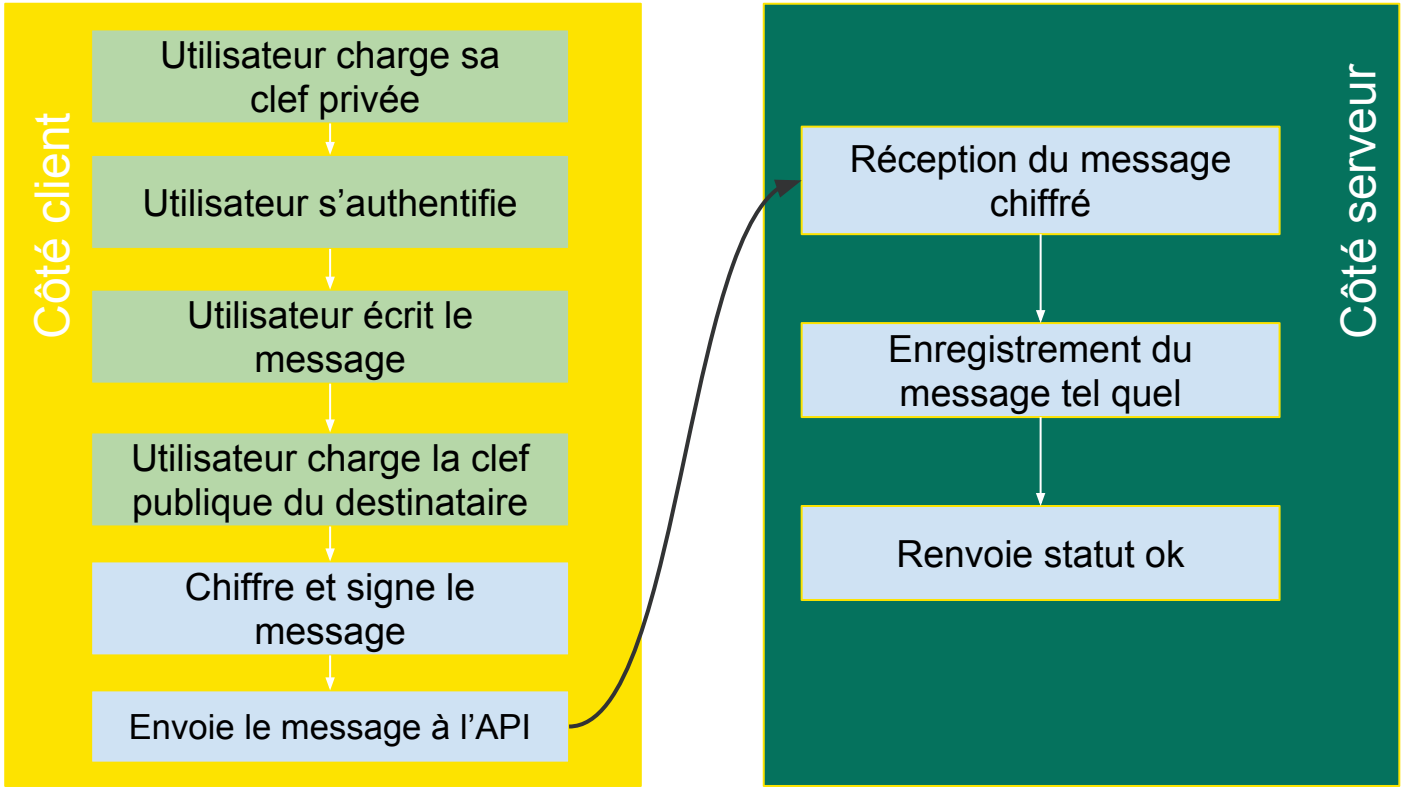
Eleven labs

Séquence d'authentification

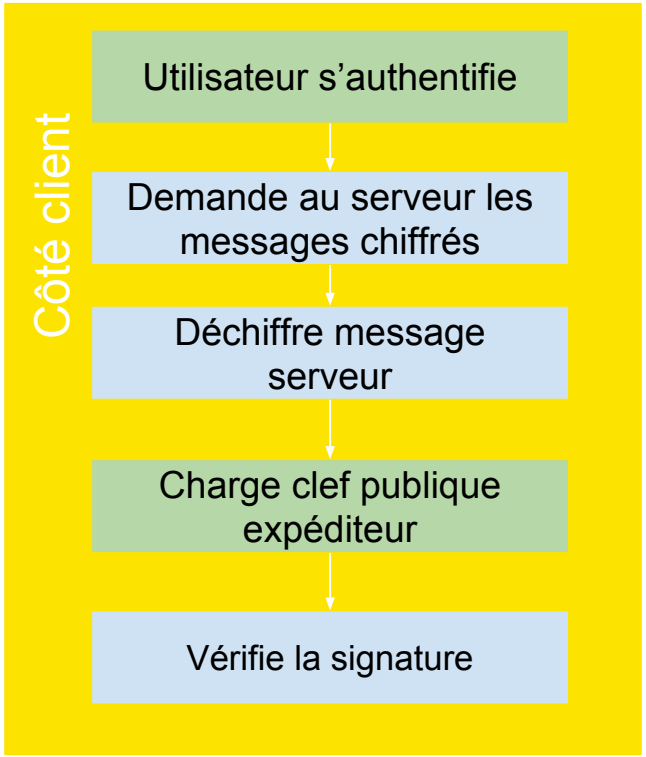


Eleven labs

Enregistrer un message



Lecture des messages



Eleven Labs

Sommaire

Eleven Labs

Implémentation

Côté client : OpenPGP.js

Côté serveur : Symfony 3 + extension PHP GnuPG + Redis

Eleven labs

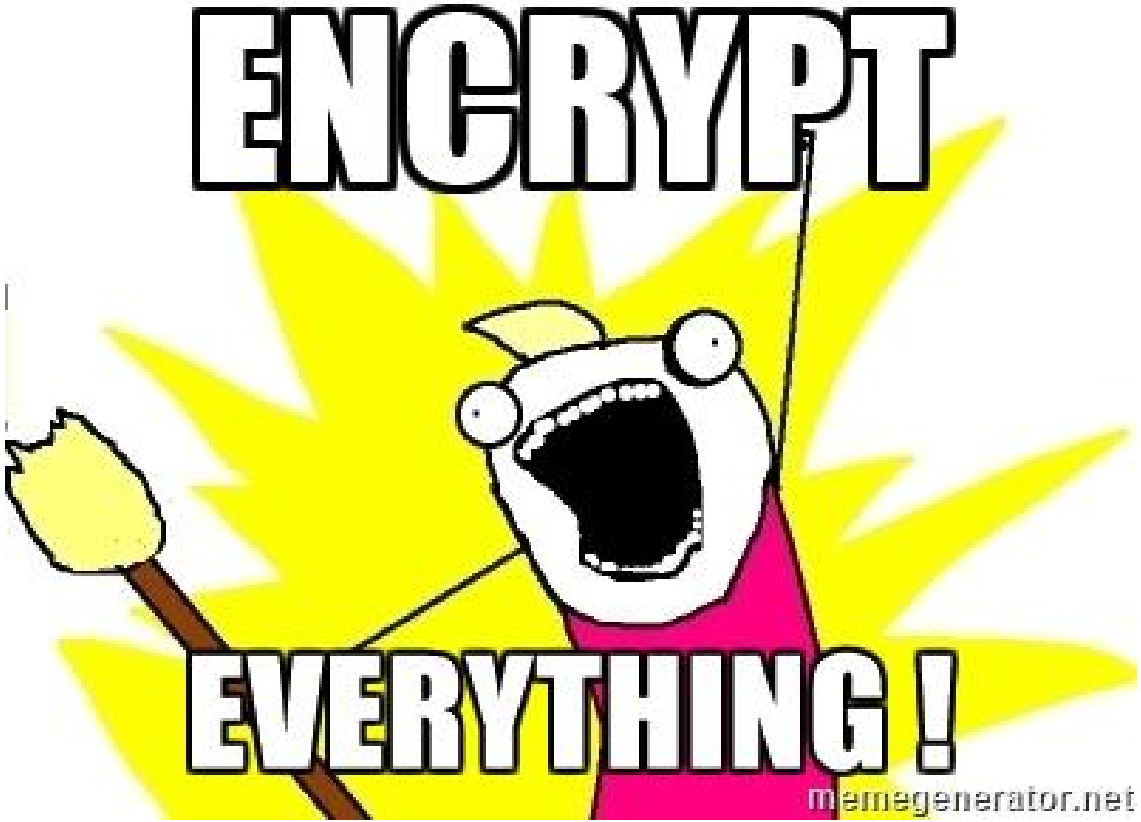
Démo

https://openpgp.piaf.eu

Conclusion

Concept expérimental

Découverte du fonctionnement OpenPGP


ENCRYPT
EVERYTHING !
memegenerator.net

Eleven labs

Références

http://zacharyvoase.com/2009/08/20/openpgp/
https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html
https://tools.ietf.org/html/rfc4880
https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process
https://tools.ietf.org/html/rfc4253#page-15
https://github.com/openpgpjs/openpgpjs
http://php.net/manual/fr/book.gnupg.php
https://cran.r-project.org/web/packages/gpg/vignettes/intro.html#web_of_trust