Vous n'aurez plus d'excuses pour ne pas passer à TLS !

Laurent SPAGNOL – Université de Reims Champagne-Ardenne - DSI

HTTP sans le « S », c'est le mal !

- Entre le client et le serveur, les communications en clair sont exposées aux attaques :
  - Suis-je écouté ?
  - Les données sont-elles authentiques ?

HTTP**S** (TLS en général)

- Permet de chiffrer les données entre le client et le serveur
- Permet de s'assurer que le serveur est bien celui qu'il prétend être

La PKI

- Est basée sur des couples de clés asymétriques
- Sur la signature des certificats par des autorités de confiance
- Ces dernières sont connues des clients
- Mais la PKI est un business …

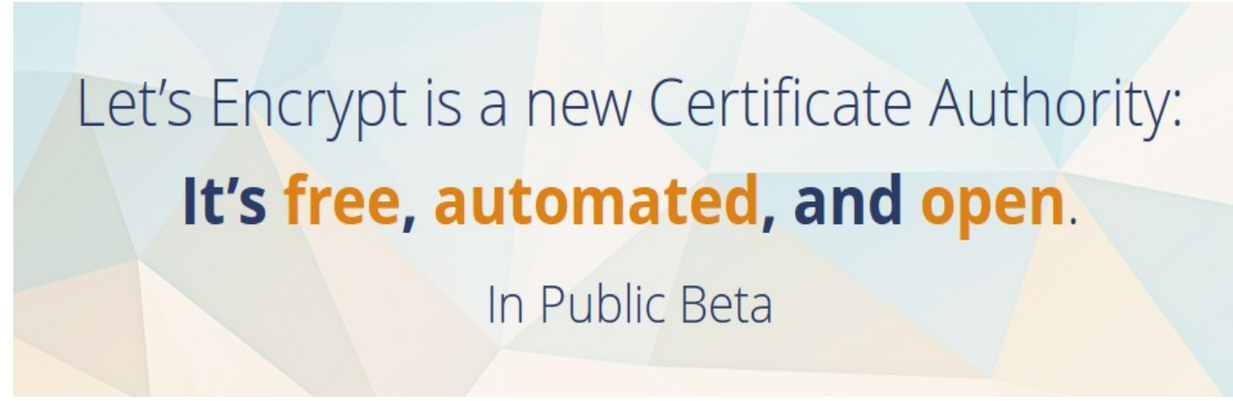
  → Les services non protégés par TLS sont (trop) nombreux

*Un jour, les navigateurs ne feront plus que du HTTP**S,** et les certificats auto-signés ne seront peut-être plus acceptés ...*

Let's Encrypt est arrivé !

- CA signé par un certificat racine

  → **reconnu par les navigateurs** et les bidules mobiles
- Supporte les noms multiples (« Subject Alternative Name »)
- **Procédure automatisée**, basée sur le protocole « ACME »
- Service **GRATUIT**



Les « acteurs » ?

- Service fourni par « Internet Security Research Group (ISRG) »
- Sponsorisé par (entre-autres) :
  - La fondation Mozilla
  - Cisco
  - Facebook!
  - …

Comment ça fonctionne ?

- Installer le client (libre) Let's Encrypt :
  - *git clone* …
- Générer (ou renouveler) le certificat :
  - *./letsencrypt …*
- Le protocole « ACME » fait le reste !
- Vous n'avez plus qu'à installer votre certificat :)

« Le côté obscur »

- Client disponible uniquement pour les systèmes *x, mais il est possible de générer un certificat pour une autre machine
- Les certificats sont valides pendant 90 jours → inciter l'automatisation des opérations de renouvellement
- Le « wildcard » : c'est pas bien !

Des questions ? → http<u>S</u>://letsencrypt.org