Let's encrypt

Matthieu Herrb

Capitoul - 23 juin 2016

https://homepages.laas.fr/matthieu/talks/letsencrypt.pdf

Introduction

https://letsencrypt.org

- Nouvelle autorité de certification
- Fournit des certificats X.509 **serveur** Domain Validated gratuits
- Projet soutenu (entre autres) par l'EFF, Mozilla, Akamai, Cisco et OVH
- Destiné à généraliser le chiffrement TLS pour les services internet (HTTPS/SMTPS/IMAPS,...)
- Déploiement simplifié grâce au protocole ACME

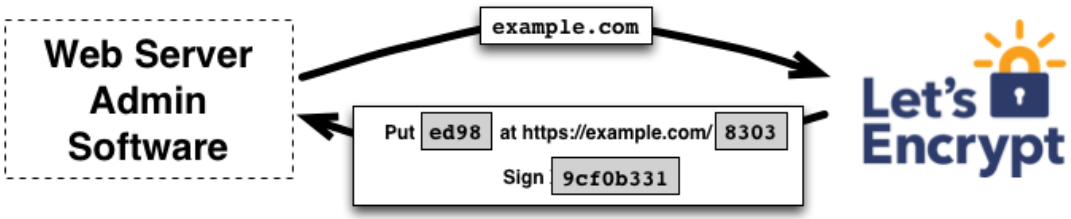
- Dans nos milieux, alternative à Terena/Digicert :
  - pour des tests
  - pour des domaines non connus de Renater
  - **éliminer les certificats auto-signés**

Le protocole ACME

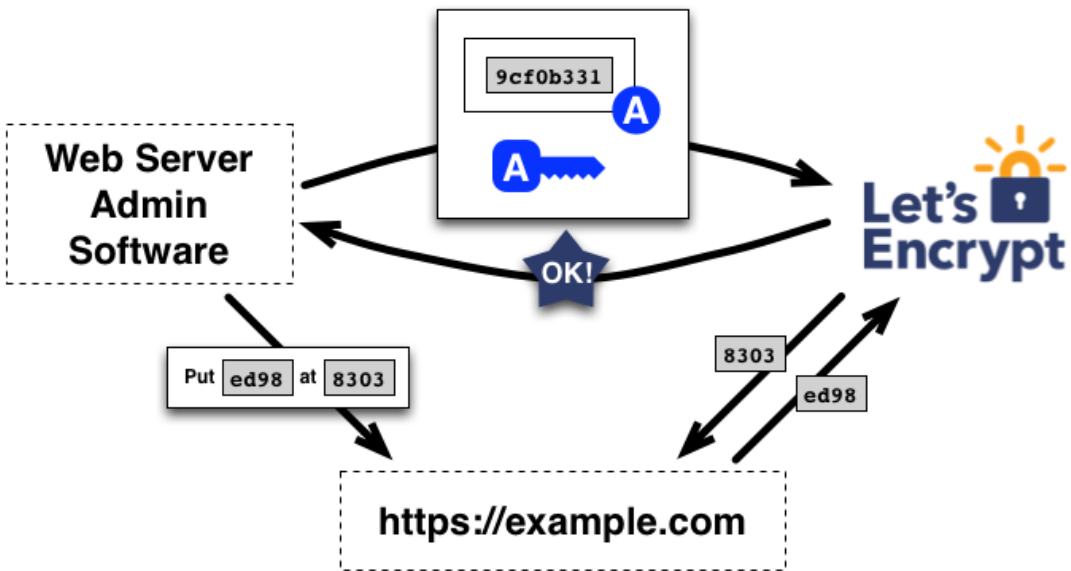
Automated **C**ertificate **M**anagement **E**nvironment

https://tools.ietf.org/html/draft-ietf-acme-acme-02

Challenge :



Autorisation :



Certbot: le client ACME standard

https://certbot.eff.org/

Demande initiale :

```
# yum install certbot
# certbot certonly --rsa-key-size 4096
```

→ certificat dans /etc/letsencrypt/live/

Renouvellement :

```
# certbot renew --rsa-key-size 4096
```

(via cron ou équivalent)

Autres clients

https://letsencrypt.org/docs/client-options/

À noter :

- acme-tiny (Python, 200 lignes)
- letskencrypt (C, séparation privilèges à la OpenBSD)
- lua-resty-auto-ssl (plugin lua pour nginx)
- plugin pour HAProxy
- Clients intégrés aux produits Gandi, Synology et bientôt OVH ?

Bilan

Bien

- certificats reconnus & gratuits
- facile à utiliser pour des cas standards
- aide à la configuration du serveur Web
- protocole ouvert et code libre

Moins bien

- client standard : beaucoup de code exécuté avec privilèges
- seulement serveurs DV
- moins simple pour serveurs non publics
- expiration 90 jours $\rightarrow$ automatiser le renouvellement
- ... confiance à long terme ?