Premier retour sur Let's Encrypt

Pierre-Yves Bonnetain
py.bonnetain@ba-consultants.fr

B&A Consultants – BP 70024 – 31330 Grenade-sur-Garonne

15 décembre 2015

B&A Consultants

- Cabinet de conseil en sécurité informatique créé en 1996.
- Conseils, suivi et assistance en sécurité informatique.
- Audits de sécurité, de configurations, de code...
- Tests d'intrusion, tests d'applications.
- Réponse à incidents, analyses *post-mortem*.
- Analyses de risques, gestion des risques sur l'information.
- Ingéniérie de la sécurité informatique, recherche de solutions.
- Formations à la sécurité informatique.
- Expertise judiciaire (civile ou pénale) et expertises privées.
- Animateur de ReSIST, groupe de travail régional de l'OSSIR (`www.ossir.org/resist`)

Plan

Principe

- `https://letsencrypt.org/`
- Favoriser l'adoption massive de TLS, notamment pour les serveurs Web
- en automatisant **toutes** les phases de gestion des certificats
- y compris le déploiement sur le serveur Web et sa configuration
- et le renouvellement des certificats

En résumé

TLS pour le serveur *Fan de Twilight* de mes nièces.

Une brève histoire du temps

- 18 novembre 2014 : lancement
- 14 septembre 2015 : signature du premier certificat
- 15 octobre 2015 : version béta privée (sur invitation)
- 19 octobre 2015 : certificat racine `Let's Encrypt` signé par Iden Trust
- 3 décembre 2015 : version béta publique
- en 2016 : mise en production ?

Les versions béta

Limitation du nombre de requêtes par domaine (5/semaine), par IP (10/3 h), par compte (300/semaine)

Fonctionnement classique

Note

Le fonctionnement décrit peut changer, notamment lors de la mise en production réelle.

- AC comme les autres (gratuite)
- Apporter une « preuve de propriété » du nom concerné
- Tout le reste est (pratiquement) automatique :
  - Demande du certificat
  - Configuration du serveur Web (Apache, ngnix)
  - Renouvellement
- Révocation possible

Attention

Nous n'avons pas testé la configuration automatique du serveur Web.

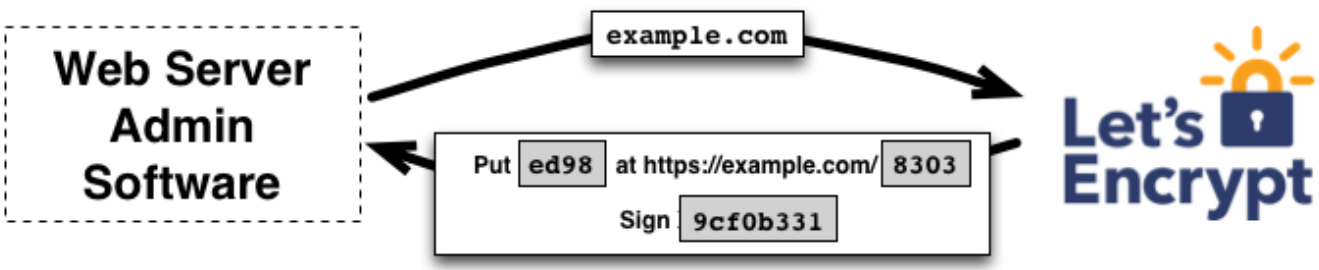
Plan

Automatic Certificate Management Environment

- Protocole ACME : `https://github.com/letsencrypt/acme-spec` et `https://github.com/ietf-wg-acme/acme/`
- Lors du premier échange avec serveurs ACME
  - envoi clé publique client
  - information d'identité (adresse électronique)
- Deux principales étapes
  - Preuve de propriété du nom (Domain Validation)
  - Gestion du certificat (soumission, renouvellement, révocation)
- Message envoyé par serveurs ACME un amois avant expiration certificat

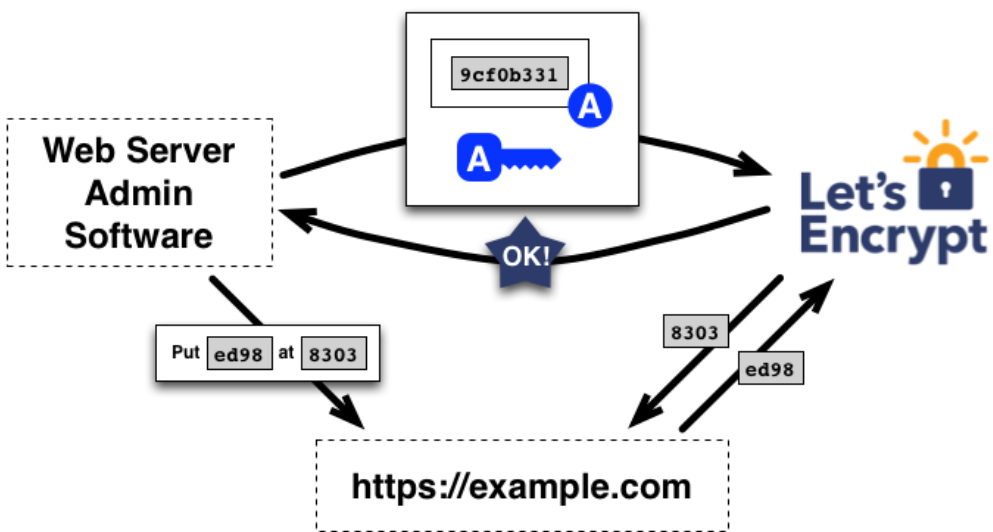
La preuve de propriété

- Via un enregistrement spécifique dans le DNS (théoriquement)
- ou via une URL spécifique
- le « spécifique » étant défini par le serveur ACME à l'enrôlement
- le serveur LE va récupérer ce challenge signé par la clé privée du client
- et le valide (ou pas) avec la clé publique reçue au préalable



La preuve de propriété

- Via un enregistrement spécifique dans le DNS (théoriquement)
- ou via une URL spécifique
- le « spécifique » étant défini par le serveur ACME à l'enrôlement
- le serveur LE va récupérer ce challenge signé par la clé privée du client
- et le valide (ou pas) avec la clé publique reçue au préalable



Premier inconvénient

- Validation par URL ⇒ accès à l'URL
- Donc serveur doit être accessible depuis Internet
- Ennuyant pour systèmes purement internes
- Et pour serveurs non-HTTP
- Peut demander quelques « adaptations » pour la phase de preuve de propriété

Validation via DNS

Posera le même type de difficulté : exposition temporaire nom privé

Certificats publiés

Certificats produits par LE sont publiés (`certificate-transparency.org` et `crt.sh`). Quid des serveurs privés ?

Certificats produits

`https://crt.sh/?Identity=<regExp SQL>&iCAID=7395`

crt.sh Identity Search

Criteria	Identity LIKE '%[redacted]%'; Issuer CA ID = 7395

Issuer Name	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X1		
Certificates (2)	Not Before	Not After	Subject Name
	2015-12-05	2016-03-04	CN=[redacted]
	2015-12-05	2016-03-04	CN=[redacted]

Clients ACME

- Client officiel en python
  `https://github.com/letsencrypt/letsencrypt`
- Avec nombreuses dépendances (au moins sous Gentoo)
- Nécessité d'être `root` si installation automatique des certificats
- Clients alternatifs (shell, C, etc.) en cours de développement

Il y a (un peu) de choix de clients

Reste à valider les composants – surtout si exécution `root`
Qualité de codage variable

Client officiel

- Très peu de documentation. Option `--help all`, sinon lire le code ☺
- Clé privée générée de 2048 bits (par défaut)
- Vérifie si existe déjà certificat LE pour domaines demandés
- Testé sans installation automatique du certificat (`--manual certonly`)
- Par défaut, repose sur serveur ACME de tests : *Happy Hacker Fake CA*
- Serveur de production `https://acme-v01.api.letsencrypt.org`

Obtention d'un certificat

```
letsencrypt --config-dir ~/etc/letsencrypt/
   --work-dir ~/lib/letsencrypt/
   --logs-dir ~/tmp/letsencrypt/
   --domains <liste>
   --server https://acme-v01.api.letsencrypt.org
   --manual certonly
```

- `config-dir` : répertoire où se trouvent les fichier importants
- `work-dir` : répertoire de travail. Contient quoi ?
- `logs-dir` : journalisation
- `domains` : noms DNS, séparés par virgules, **sans espaces**
- `server` : utiliser le serveur de production
- `certonly` : pas d'installation automatique

Certificats multi-noms

- Extension `Subject Alt Name` reconnue
- Il suffit de donner plusieurs noms sur la ligne de commande
- Chacun de ces noms doit être validé

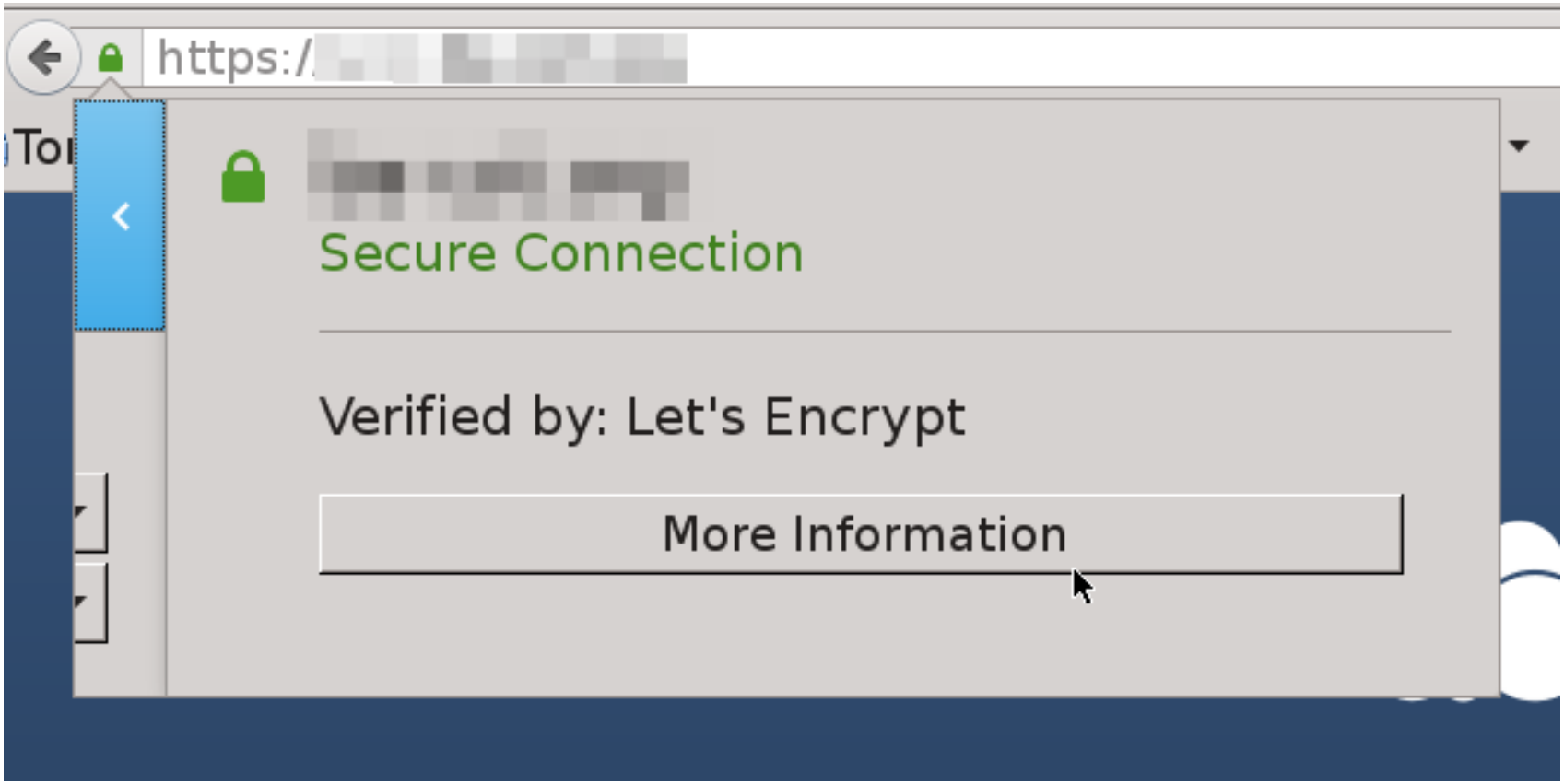
Ca donne quoi ?

```
Make sure your web server displays the following content at
http://[redacted]/.well-known/acme-challenge/TSJc6d9-Ce6n60FlcEIEbPHAcuFkxGw
TT2cP7VqL798 before continuing:

TSJc6d9-Ce6n60FlcEIEbPHAcuFkxGwTT2cP7VqL798.FV5YhedqScD-c8Y1gHbGCvUJUduG6xLveJSf
4kSUEmQ

Content-Type header MUST be set to text/plain.

If you don't have HTTP server configured, you can run the following
command on the target server (as root):

mkdir -p /tmp/letsencrypt/public_html/.well-known/acme-challenge
cd /tmp/letsencrypt/public_html
printf "%s" TSJc6d9-Ce6n60FlcEIEbPHAcuFkxGwTT2cP7VqL798.FV5YhedqScD-c8Y1gHbGCvUJ
UduG6xLveJSf4kSUEmQ > .well-known/acme-challenge/TSJc6d9-Ce6n60FlcEIEbPHAcuFkxGw
TT2cP7VqL798
# run only once per server:
$(command -v python2 || command -v python2.7 || command -v python2.6) -c \
"import BaseHTTPServer, SimpleHTTPServer; \
SimpleHTTPServer.SimpleHTTPRequestHandler.extensions_map = {'': 'text/plain'}; \
s = BaseHTTPServer.HTTPServer(('', 80), SimpleHTTPServer.SimpleHTTPRequestHandle
r); \
s.serve_forever()"
Press ENTER to continue
```

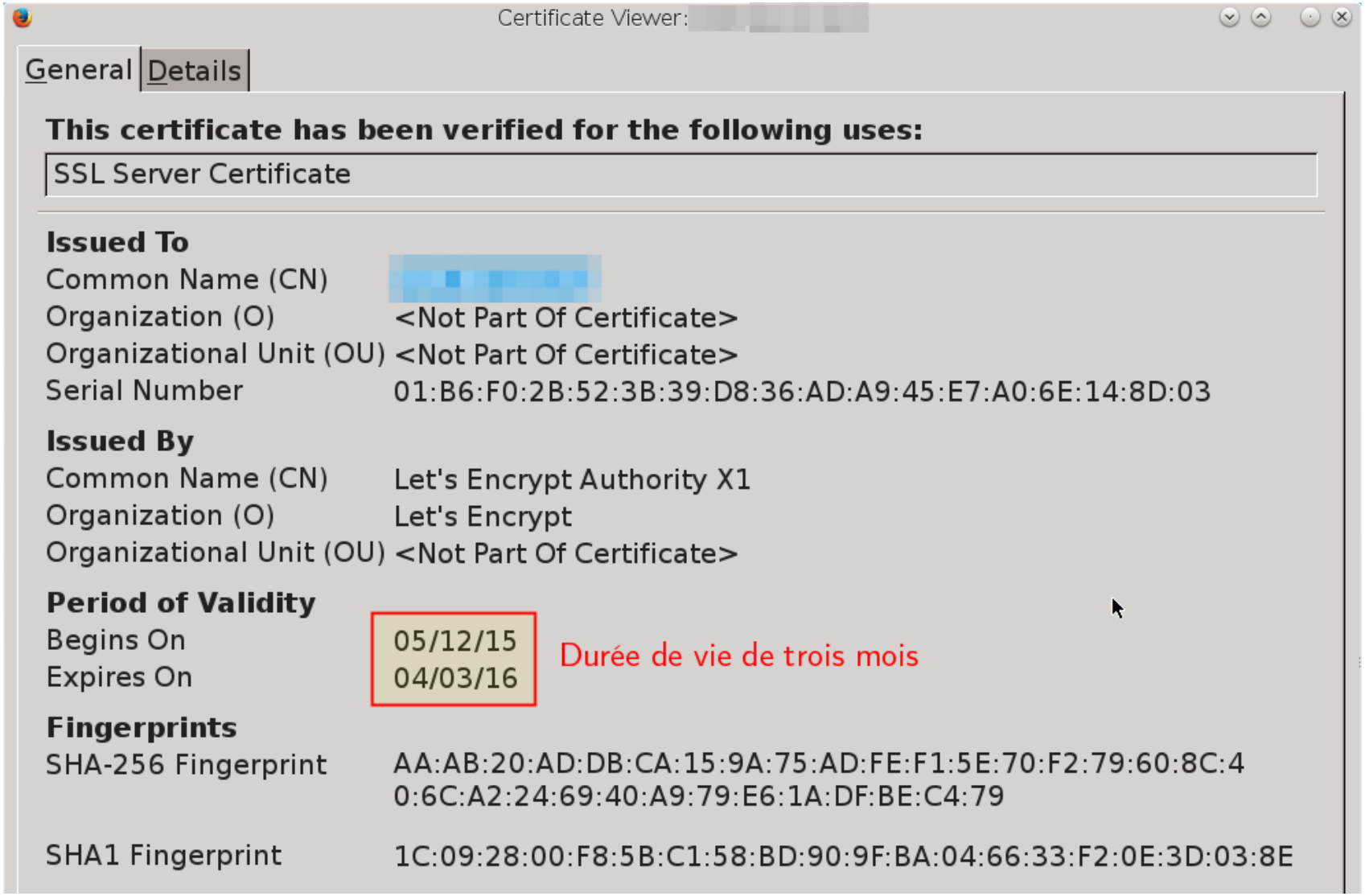
Ca donne quoi ?

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /home/pyb/etc/letsencrypt/live/[redacted]fullchain.pem. Your
   cert will expire on 2016-03-04. To obtain a new version of the
   certificate in the future, simply run Let's Encrypt again.
pyb@veterini ~ $
```

Ca donne quoi ?



Ca donne quoi ?



Révocation d'un certificat

```
1 letsencrypt --config-dir ~/etc/letsencrypt/
2     --work-dir ~/lib/letsencrypt/
3     --logs-dir ~/tmp/letsencrypt/
4     --domains <nom>
5     --manual
6     --server https://acme-v01.api.letsencrypt.org
7     --cert-path <chemin>/letsencrypt/live/<nom>/cert.pem
8     revoke
```

- `--cert-path` : chemin complet vers le certificat à révoquer

Attention

Fonctionnalité cliente qui semble avoir été peu testée.

Plan

Client officiel

- Lourd, pas sympathique, pas convivial
- Manque cruel de documentation
- Quand ça marche, rien à redire
- Quand ça ne marche pas, comprendre l'erreur est difficile même en utilisant les journaux (`--log-dir`)

D'un autre côté

C'est une version béta. On peut espérer des améliorations dans l'avenir.

Donc

Pas encore prêt pour un déploiement pour les masses.

Encore du travail

- Validation via DNS
- OCSP (passage à l'échelle ?)
- Clients ACME plus simples, plus ciblés
- Serveurs ACME internes, pour systèmes privés

LetsEncrypt va-t-il tuer les AC classiques ?

- Avenir sombre pour AC qui n'apporte pas de plus-value à la production de certificats
- Pour les autres besoins...
  - Pas de certificats joker (`*.mondomaine.amoi`)
  - Pas de certificats « Organization Validated » ou « Extended Validation »

A savoir

Pas d'obligation d'utiliser les serveurs de LE. Il suffit d'accéder à un serveur respectant le protocole ACME.

Plan