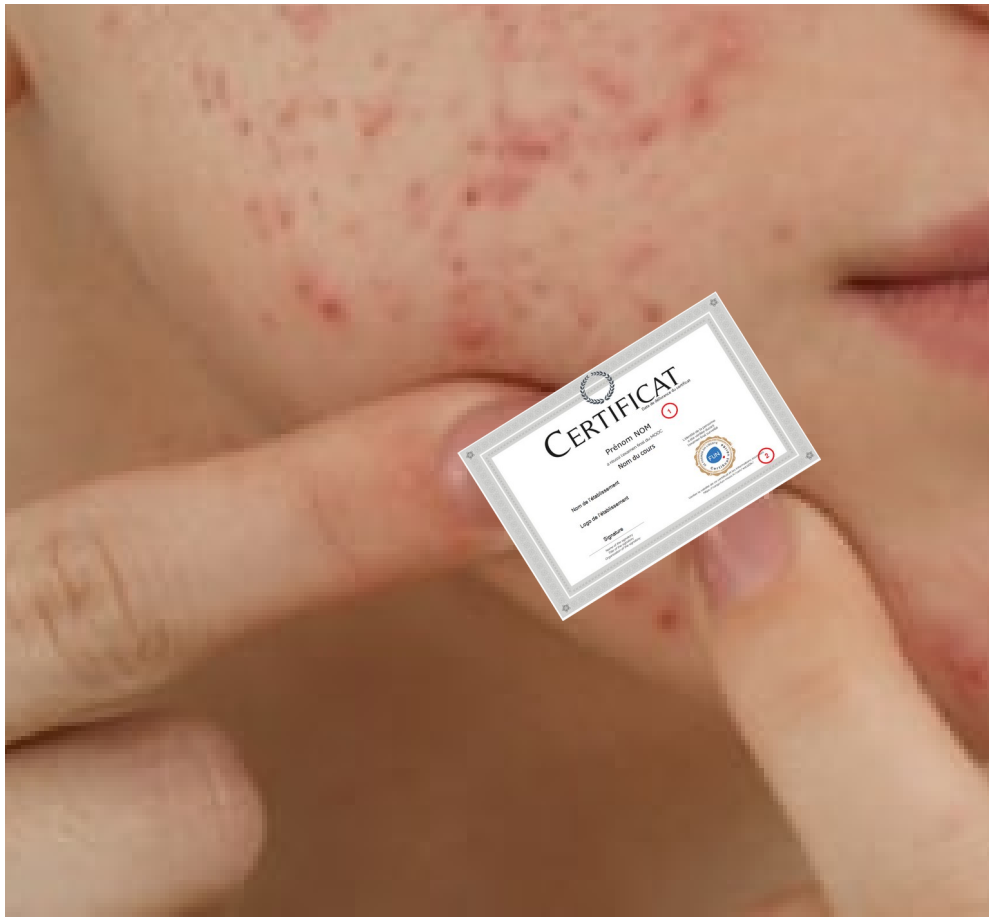
ACME,

la gestion des certificats

ne vous donnera plus de boutons !



Auteurs : Christophe Saillard, Thomas Keller et Mathieu Misslin

Gestion des certificats

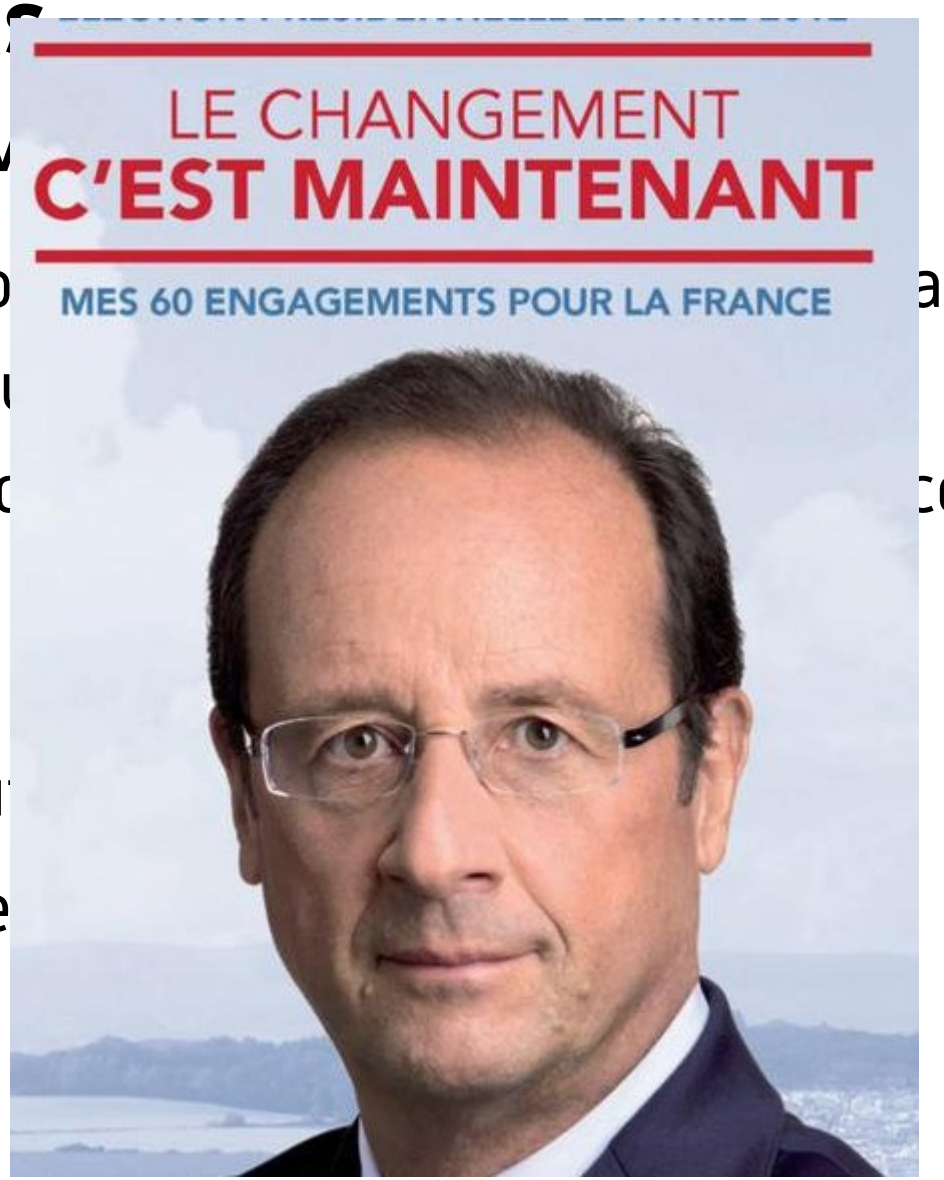
Comment on faisait avant avant ?

- Un certificat par serveur souvent dans unistra.fr ou u-strasbg.fr
- Renouvellement manuel tous les 3 ans au fil de l'eau
- Nécessité d'une validation de la demande de création de certificat via la DNUM
- Bilan
  - Clairement un frein à l'utilisation des certificats
  - Des oublis de renouvellement

Gestion des certificats

Comment on faisait av

- Un certificat par serveur so asbg.fr
- Renouvellement manuel tou
- Nécessité d'une validation c certificat via la DNUM
- Bilan
  - Clairement un frein à l'u
  - Des oublis de renouvelle
- Il fallait que ça change…



Gestion des certificats

Comment on faisait avant ou après avant avant ?

- Un certificat wildcard dans le sous-domaine astro.unistra.fr
- Donc un **seul** certificat pour **tous** les serveurs et services
- Renouvellement **manuel tous les ans sur tous les serveurs**
- Bilan
  - Plus simple à gérer car un seul certificat utilisé
  - Mais un renouvellement manuel assez fastidieux et chronophage
  - Certains services n'aiment pas les certificats Wildcard…

Gestion des certificats

27 janvier 2022, le jour où tout bascule

Gestion des certificats

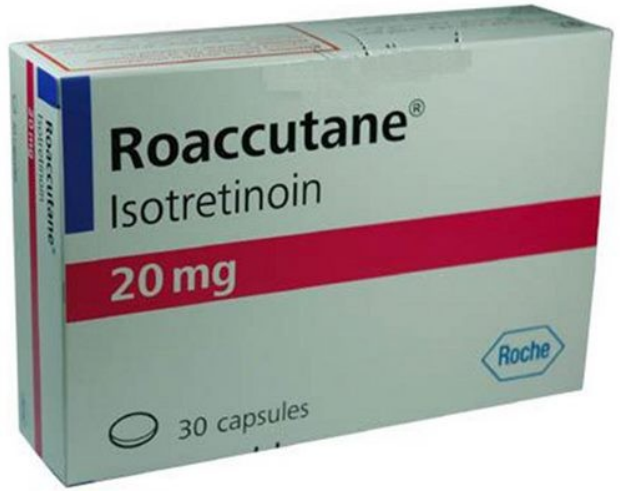
27 janvier 2022, le jour où tout bascule

- Jeudi froid, en plein dry january, une annonce anodine lors de la réunion des correspondants sécurité…

Gestion des certificats

27 janvier 2022, le jour où tout bascule

- Jeudi froid, en plein dry january, une annonce anodine lors de la réunion des correspondants sécurité…
- On découvre ACME par SECTIGO



ACME c'est quoi ?

- Source : https://tapas.unistra.fr/_media/securite/cssi_2022.pdf

  - **Automated Certificate Management Environment**

  - Protocole de communication
  - Echange entre AC et serveur web
  - Déploiement d'une PKI (X.509) à faible coût
  - Pour le service Let's Encrypt (ISRG)
  - Standard IETF : RFC 8555 (mars 2019)
  - Nombreux clients dans divers langages
  - Certbot, l'un des plus répandus (repris par EFF)

ACME c'est quoi ?

- Source : https://tapas.unistra.fr/_media/securite/cssi_2022.pdf

  - Comment ça fonctionne ?
  - Le client fait tout le travail :
    - Connexion à l'API Sectigo
    - Authentification (compte)
    - Demande de certificat
    - Récupération du certificat signé par l'AC

ACME c'est quoi ?

- Source : https://tapas.unistra.fr/_media/securite/cssi_2022.pdf

  - Pour qui ?
    - Un hébergement de sites web (5+)
    - Un orchestrateur de conteneurs
  - Pré-requis
    - Un compte ACME chez Sectigo
    - Un client installé sur votre/vos site(s)

ACME c'est quoi ?

- Source : https://tapas.unistra.fr/_media/securite/cssi_2022.pdf

  - Pour qui ?
    - Un hébergement de sites web (5+)
    - Un orchestrateur de conteneurs
  - Pré-requis
    - Un compte ACME chez Sectigo
    - Un client installé sur votre/vos site(s)

ACME c'est quoi ?

- Source : https://tapas.unistra.fr/_media/securite/cssi_2022.pdf

- Pour qui ?
  - Un hébergement de sites web (5+)
  - Un orchestrateur de conteneurs

- Pré-requis
  - Un compte ACME chez Sectigo
  - Un client installé sur votre/vos site(s)

ACME c'est quoi ?

- Source : https://tapas.unistra.fr/_media/securite/cssi_2022.pdf

- Pour qui ?
  - Un hébergement de sites web (5+)
  - Un orchestrateur de conteneurs

- Pré-requis
  - Un compte ACME chez Sectigo
  - Un client installé sur votre/vos site(s)

Vite on contacte le Cert Osiris pour activer ce compte !

ACME c'est quoi ?

- Source : https://tapas.unistra.fr/_media/securite/cssi_2022.pdf

- Pour qui ?
  - Un hébergement de sites web (5+)
  - Un orchestrateur de conteneurs

- Pré-requis
  - Un compte ACME chez Sectigo
  - Un client installé sur votre/vos site(s)

Vite on contacte le Cert Osiris pour activer ce compte !

Vite on teste avec Certbot !

ACME c'est quoi ?

- Source : https://tapas.unistra.fr/_media/securite/cssi_2022.pdf

  - Points importants

    - Uniquement sur les domaines gérés sur Osiris
    - Certificat 365 jours, revalidé 1 mois avant
    - Le compte ACME doit être activé **une fois**

- Documentation
  - https://services.renater.fr/tcs/acme
  - https://sectigo.com/resource-library/what-is-acme-protocol

Comment déployer mon premier certificat avec ACME ?

Perçons le secret

- J'installe mon serveur Web et j'active HTTPS
- J'installe Certbot sur le serveur concerné (apt, snap…)
- Je lance la commande certbot avec tous les paramètres nécessaires

Certbot certonly --non-interactive --apache --agree-tos --email it@astro.unistra.fr --server https://acme.sectigo.com/v2/OV --eab-kid *SECRET* --eab-hmac-key *SECRET* --cert-name ov-acme-demo.astro.unistra.fr --domain acme-demo.astro.unistra.fr

Si tout c'est bien passé les certificats et la clé sont présents sur le serveur :

```
root@acme-demo:/etc/letsencrypt/live/ov-acme-demo.astro.unistra.fr# ll

lrwxrwxrwx 1 root root  53 Feb  9 10:27 cert.pem -> ../../archive/ov-acme-demo.astro.unistra.fr/cert4.pem

lrwxrwxrwx 1 root root  54 Feb  9 10:27 chain.pem -> ../../archive/ov-acme-demo.astro.unistra.fr/chain4.pem

lrwxrwxrwx 1 root root  58 Feb  9 10:27 fullchain.pem -> ../../archive/ov-acme-demo.astro.unistra.fr/fullchain4.pem

lrwxrwxrwx 1 root root  56 Feb  9 10:27 privkey.pem -> ../../archive/ov-acme-demo.astro.unistra.fr/privkey4.pem
```

Comment déployer mon premier certificat avec ACME ?

Perçons le secret

- Je fais pointer ma configuration apache vers le certificat fullchain et la clé

  SSLCertificateFile /etc/letsencrypt/live/ov-acme-demo.astro.unistra.fr/fullchain.pem

  SSLCertificateKeyFile /etc/letsencrypt/live/ov-acme-demo.astro.unistra.fr/privkey.pem

- Je redémarre mon serveur apache…

- Le renouvellement se fera automatiquement :

```
root@acme-demo:/etc/letsencrypt/live/ov-acme-demo.astro.unistra.fr# systemctl list-timers | grep -E 'UNIT|certbot'
NEXT                        LEFT          LAST                        PASSED       UNIT                         ACTIVATES
Thu 2023-02-09 12:29:54 CET 1h 11min left Thu 2023-02-09 06:28:04 CET 4h 50min ago certbot.timer              certbot.service
```

Comment déployer mon premier certificat avec ACME ?

Perçons le secret

- Les infos liées au renouvellement sont là :

```
root@acme-demo:/etc/letsencrypt/renewal# cat ov-acme-demo.astro.unistra.fr.conf
# renew_before_expiry = 30 days
version = 0.40.0
archive_dir = /etc/letsencrypt/archive/ov-acme-demo.astro.unistra.fr
cert = /etc/letsencrypt/live/ov-acme-demo.astro.unistra.fr/cert.pem
privkey = /etc/letsencrypt/live/ov-acme-demo.astro.unistra.fr/privkey.pem
chain = /etc/letsencrypt/live/ov-acme-demo.astro.unistra.fr/chain.pem
fullchain = /etc/letsencrypt/live/ov-acme-demo.astro.unistra.fr/fullchain.pem

# Options used in the renewal process
[renewalparams]
account = 2bbda1c804b533242f2149e5cdad52b3
#server = https://acme.sectigo.com/v2/OV
server = https://acme.sectigo.com/v2/OV
authenticator = apache
installer = apache
```

Comment déployer mon premier certificat avec ACME ?
Perçons le secret

- Les Renewal hooks
  - Le redémarrage des services est automatisé avec apache ou nginx
  - Si vous utilisez d'autres services, il faut utiliser le mode « standalone » et paramétrer des « renewal hooks » pour préciser quelle(s) commande(s) lancer avant et/ou après le renouvellement

ACME à l'OBAS

- Cas d'usages et mode de gestion
  - **Ansible utilisé autant que possible…**
  - Sur chaque serveurs Web
    - Déploiement du Certbot via un playbook Ansible
    - Renouvellement automatisé avec redémarrage du service
  - Interfaces de managements IDRAC/ILO
    - Certificats initialisés depuis un serveur central puis poussé vers les serveurs grâce à un playbook
  - Applications Kubernetisées
    - Utilisation d'un service « cert-manager » interne à K8S qui gère les créations de certificats (via ACME)
  - Les cas particuliers (HAP, LDAP)
    - Lancement manuel du Certbot

ACME à l'OBAS

- Cas d'usages et mode de gestion, nos conseils
  - Recensez vos certificats
  - Créez-vous des alertes vérifier le bon renouvellement