ACME

Apports (Sécurité) d'un protocole Internet dans un réseau privé

Christophe BROCAS - Sécurité@Assurance Maladie

RUMP SSTIC 2023

Notre existant :
Une PKI interne, deux manières d'obtenir des certificats TLS serveurs

Workflow manuel sur portail web

API

Inconvénients

Process manuel

- Lenteur
- Pertinence des contrôles Sécurité
- Pas scalable

API

- Utile que pour les gros projets
- Clés d'API à gérer

Impact : usage des certificats non généralisé à l'ensemble du SI (80.000 utilisateurs, dizaines de milliers de serveurs).

Let’s Encrypt & ACME

Let’s Encrypt a réussi à passer à l’échelle la signature de certificats TLS sur Internet.

Elle l’a fait grâce à ACME, protocole ouvert et automatisé.

Idée : et si on utilisait ACME dans notre SI interne ?

Intérêt d'ACME ?

ACME automatise les contrôles de Sécurité, la délivrance et le renouvellement des certificats TLS serveurs.

La scalabilité sécurisée est possible.

Idée : et si on utilisait ACME dans notre SI interne ?

Intérêt d'ACME ?

ACME automatise les contrôles de Sécurité, la délivrance et le renouvellement des certificats TLS serveurs.

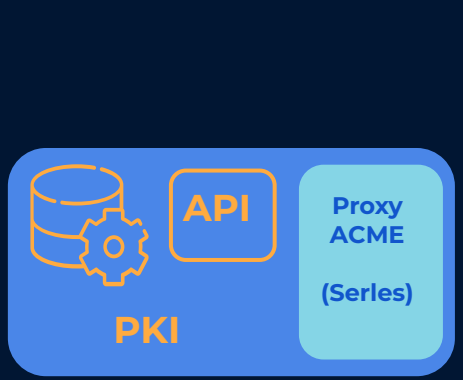
La scalabilité sécurisée est possible.

Client & proxy ACME

On a trouvé et déployé un proxy ACME devant notre PKI. Des outils du marché existent aussi.

On ne supporte qu'un client (lego) mais on documente l'usage de l'API ACME v2.

Cas d'usage d'ACME



Service web sur Linux avec client ACME Lego

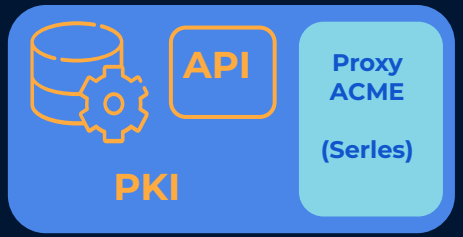
Usage documenté et supporté

Service web sur Windows avec client ACME Lego

Usage documenté et supporté en best effort

Passage à l'échelle de la délivrance de certificats :
- sans ajout de personne
- sans modification d'organisation
- avec une Sécurité éprouvée.

Cas d'usage d'ACME



Service web sur Linux avec client ACME Lego

Usage documenté et supporté

Service web sur Windows avec client ACME Lego

Usage documenté et supporté en best effort

Middlewares (Apache, Traefik, HAProxy etc) avec client ACME embarqué

Enrôlement de certificat client à la création des serveurs (client ACME Ansible)

Cas d'usages apportés par les architectes et les admins.

Passage à l'échelle de la délivrance de certificats :
- sans ajout de personne
- sans modification d'organisation
- avec une Sécurité éprouvée.

Takeaway

Quels sont les apports d'ACME comme protocole Internet dans un réseau privé ?

- ✓ Diversité de langages et de technologies pour les clients ACME
- ✓ Appropriation de l'automatisation de l'obtention des certificats par des publics très variés au sein de la DSI (sysadmins, architectes, dévs, ingénieurs réseaux etc)
- ✓ Passage à l'échelle de la signature de certificats TLS serveurs sans moyen supplémentaire (personnel, organisationnel).

Avec une Sécurité du protocole éprouvée sur Internet.

Merci !

Des questions?

christophe.brocas@assurance-maladie.fr | @cbrocas

Blog : https://assurancemaladiesec.github.io/

ON RECRUTE 😍 : 2 postes CSIRT
https://cnam-coll.talent-soft.com/offre-de-emploi/emploi-expert-e-securite-du-si-csirt-h-f_4390.aspx