ACME

Bénéfices du déploiement d'un protocole Internet de Sécurité en réseaux privés

Christophe BROCAS

Capitole du Libre 2023 | 19 novembre 2023

Christophe Brocas

Christophe Brocas

Ingénieur Sécurité @ Assurance Maladie

Focus : Sécurité & protocoles réseaux

Christophe Brocas

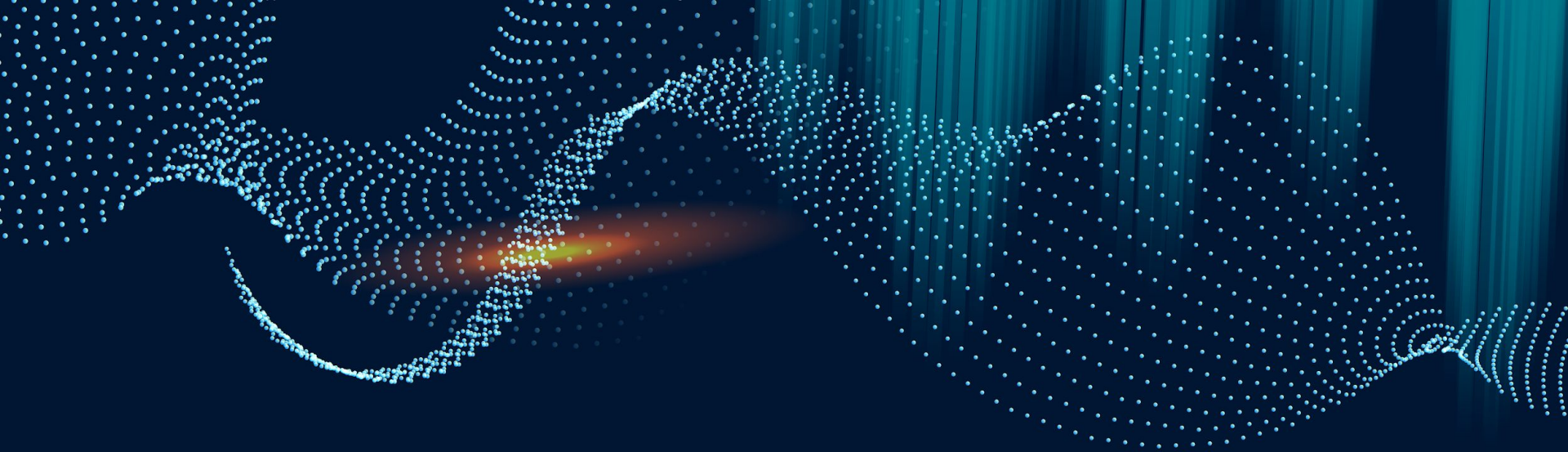
Ingénieur Sécurité @ Assurance Maladie

Focus : Sécurité & protocoles réseaux

Co-fondateur & organisateur de Pass the SALT

Conférence dédiée aux Logiciels Libres et à la Sécurité

Mais commençons par un court sondage concernant ACME ! 🙂



01 | Le Problème

Échec d’une PKI privée à fournir des certificats à toutes les applications

La version courte

Nos applications web internes ne sont pas toutes accédées en HTTPS.

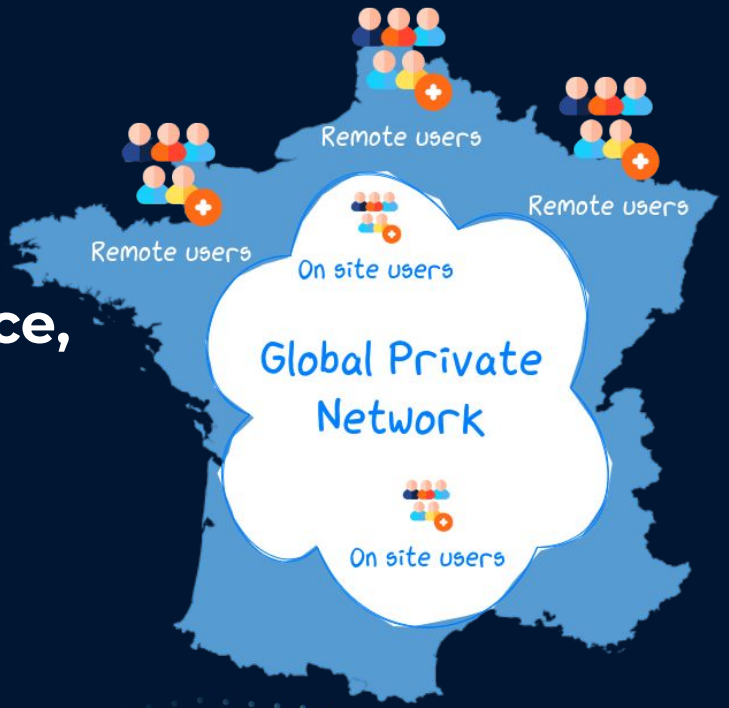
(*certificats expirés, certificats auto-signés, certificats signés par une PKI inconnue des terminaux ...*)

Notre PKI privée est une partie du problème.

Version longue

80.000 collègues.

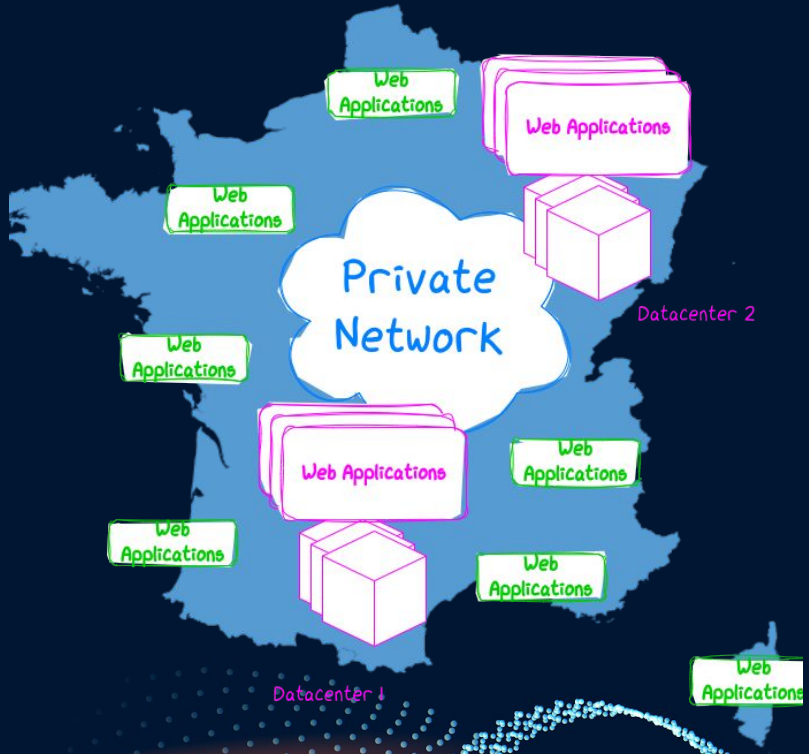
Connectés, sur site ou à distance,
à un même réseau privé.



Nombreuses applications

Des centaines d’applications web internes au niveau national.

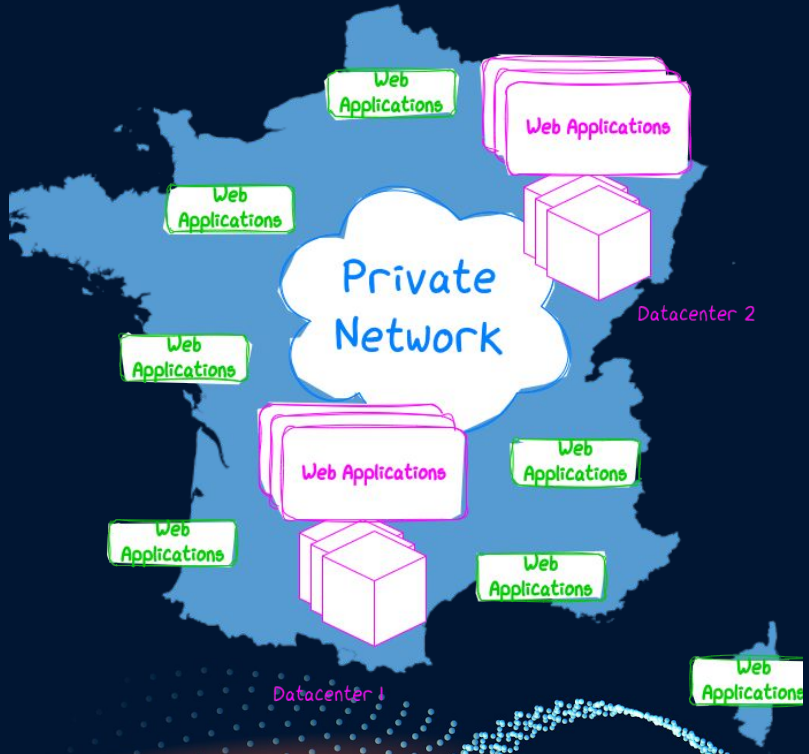
Et encore plus au niveau local.



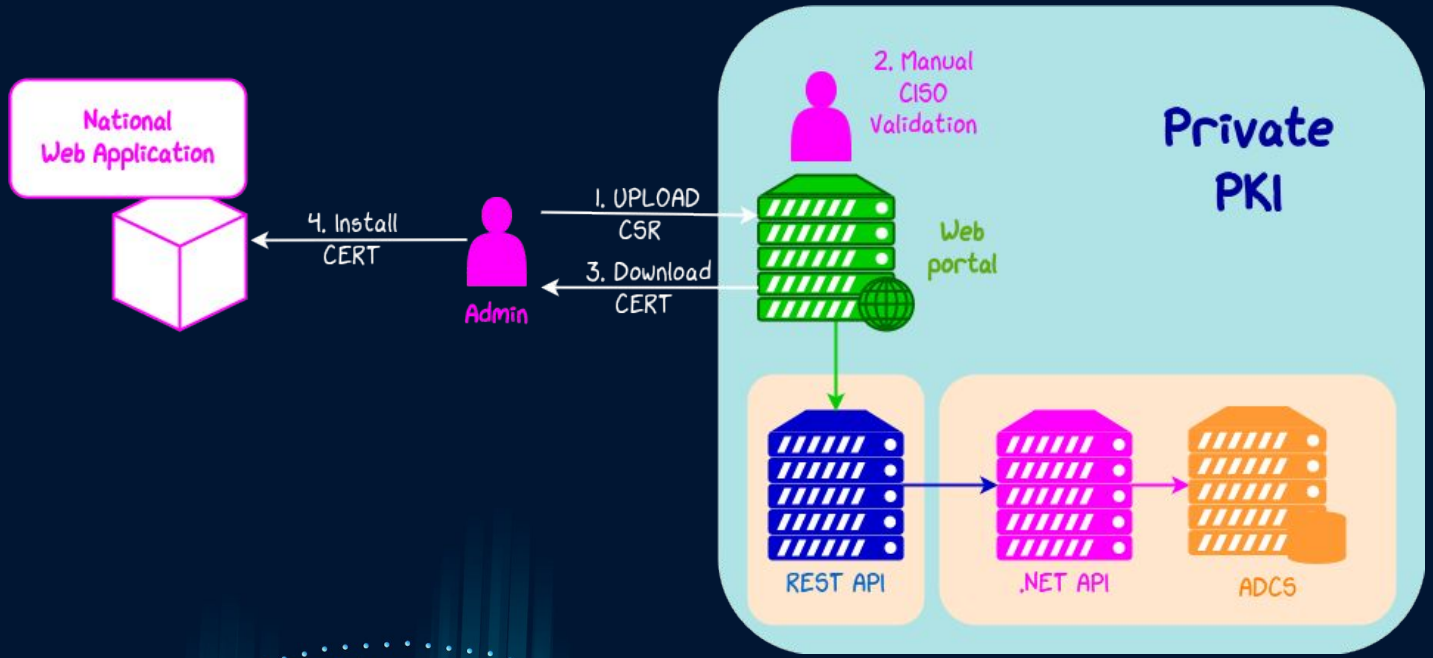
HTTPS

HTTPS est requis pour nos applications web internes.

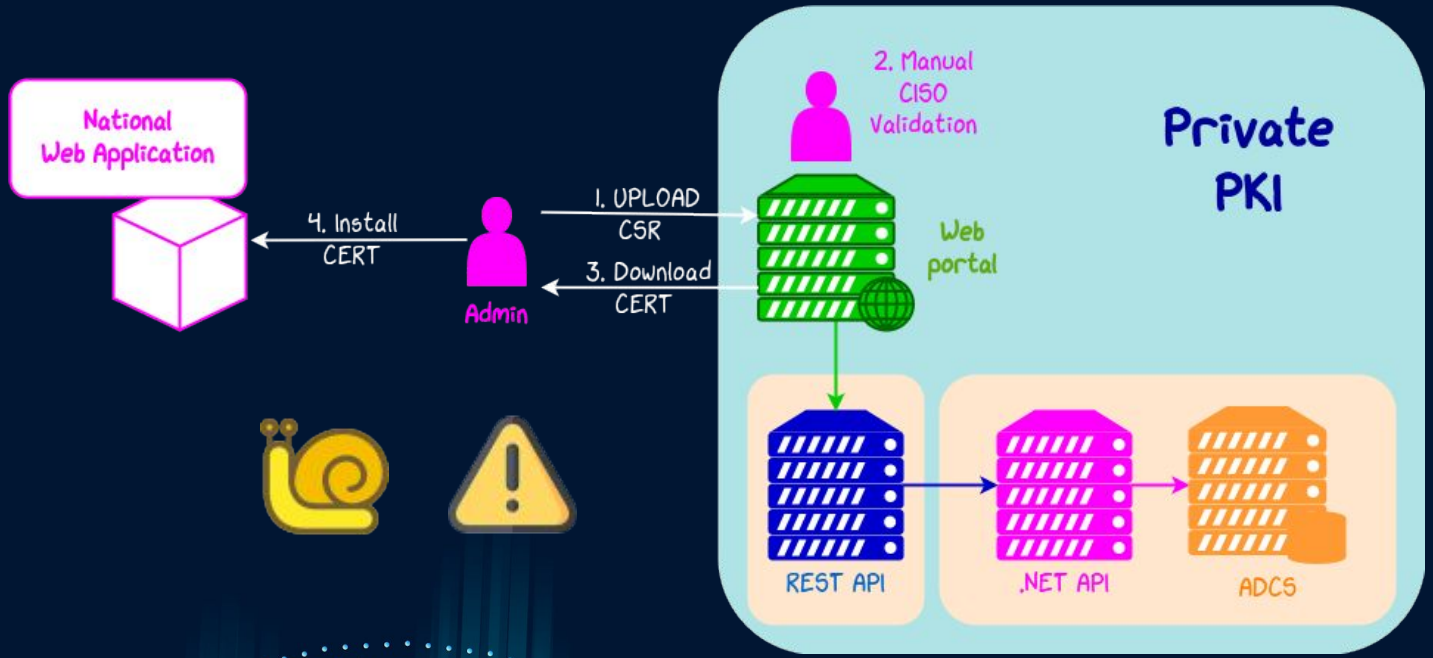
Une PKI privée est disponible depuis 2008.



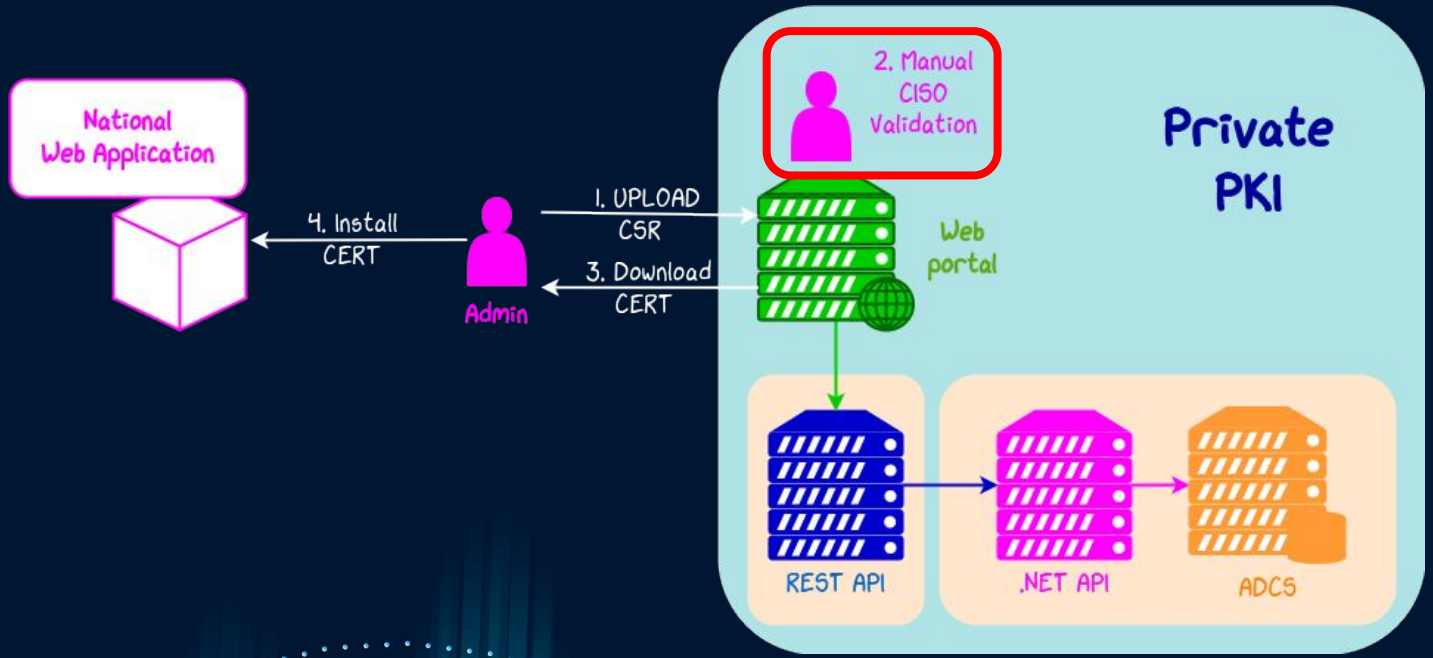
1 PKI privée, 2 Workflows



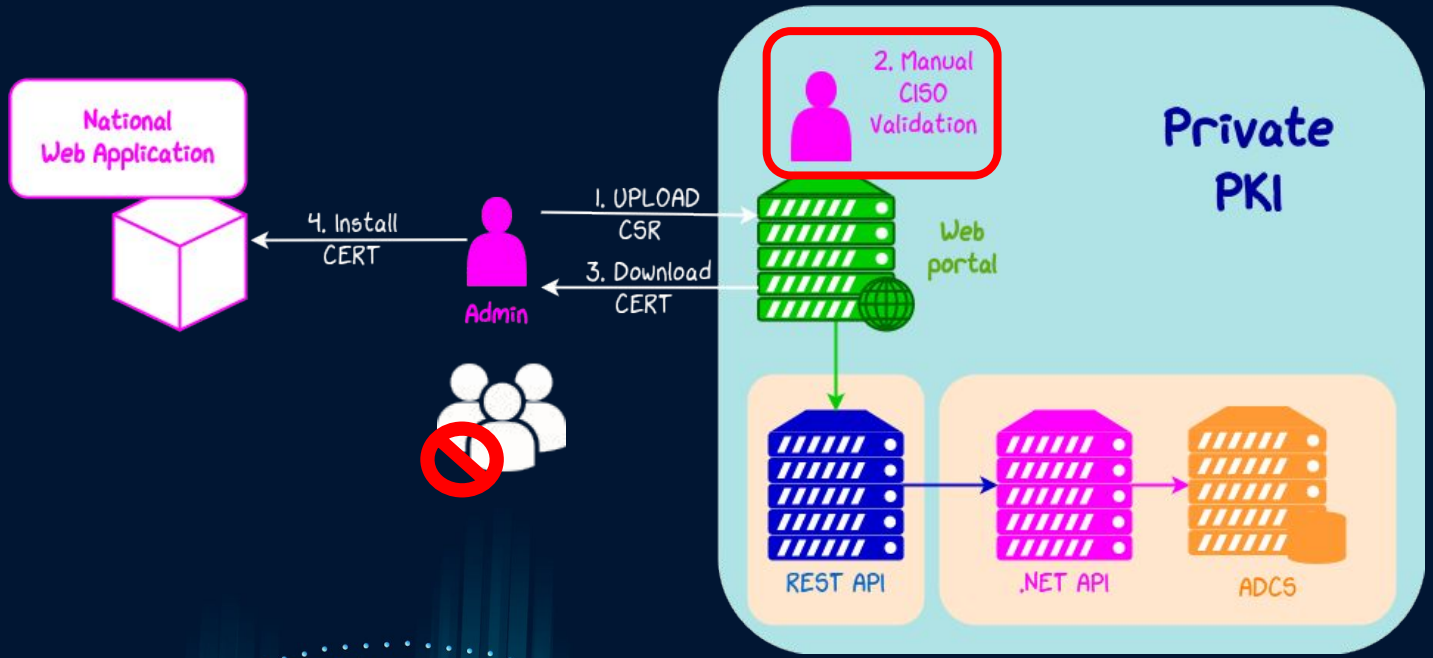
1 PKI privée, 2 Workflows



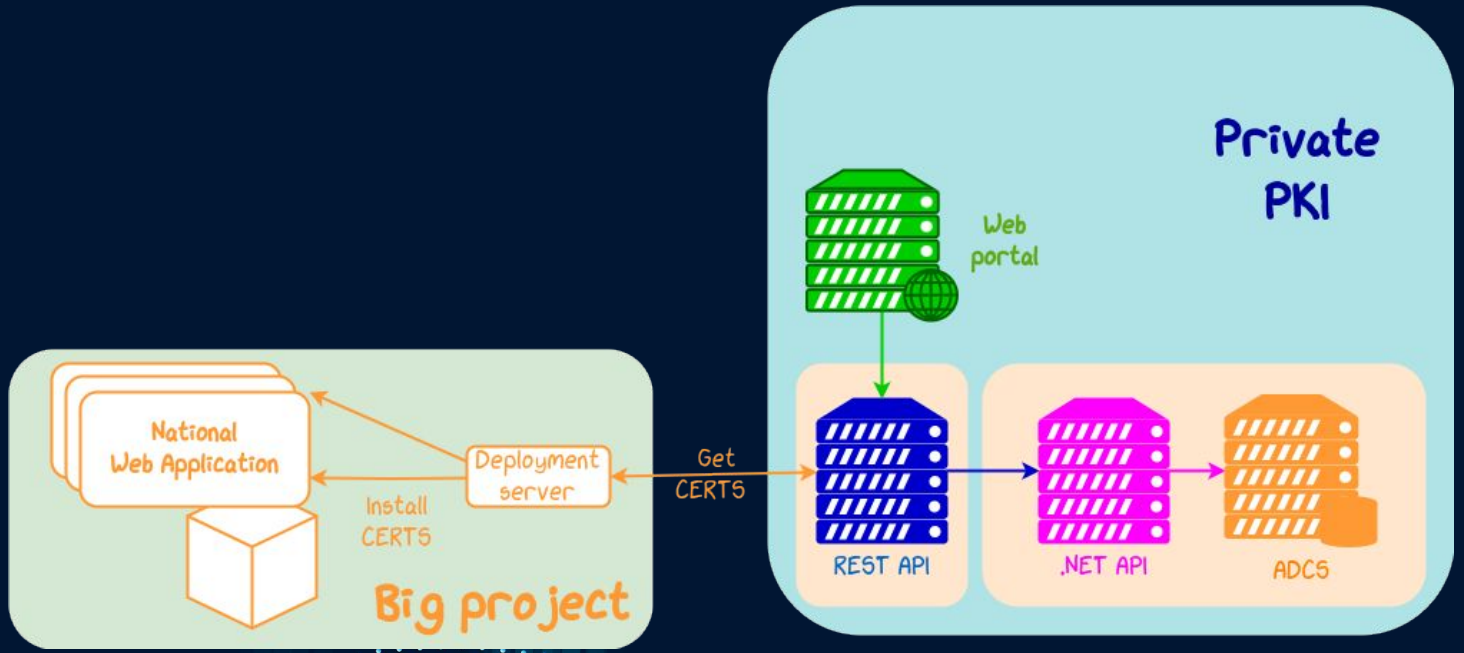
1 PKI privée, 2 Workflows



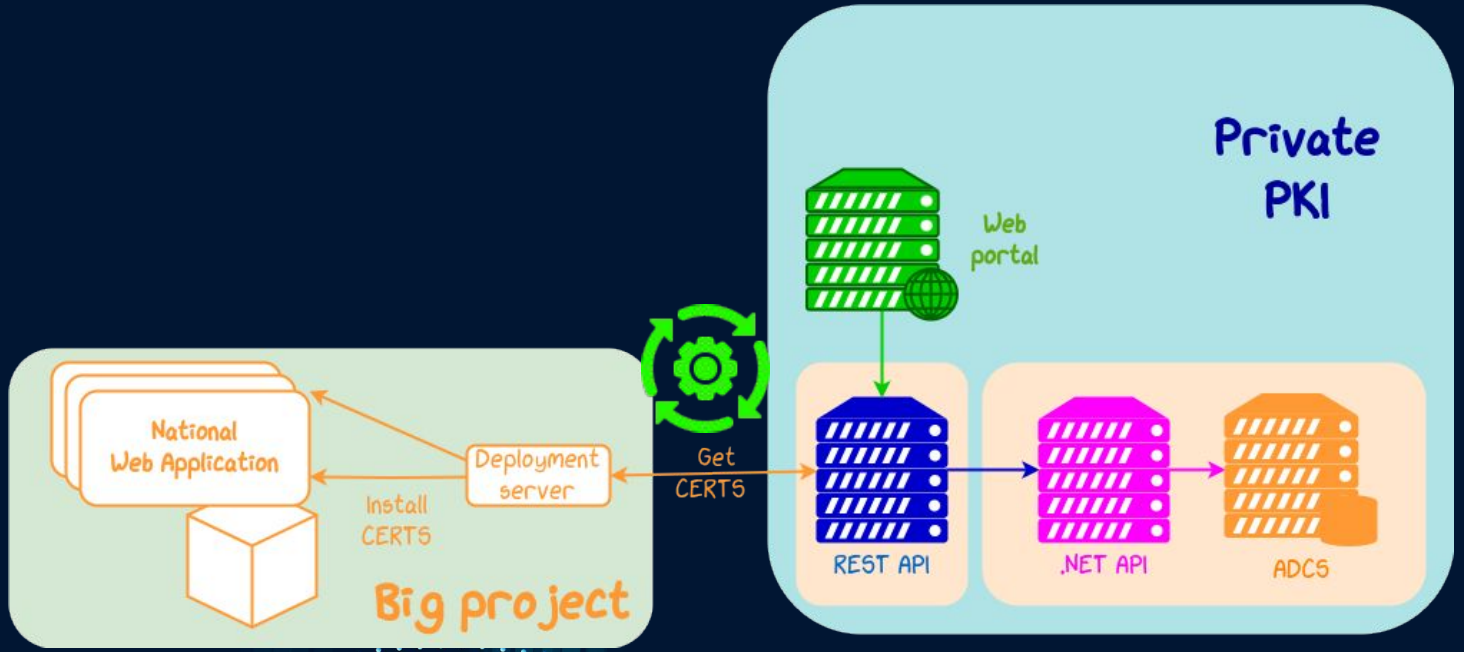
1 PKI privée, 2 Workflows



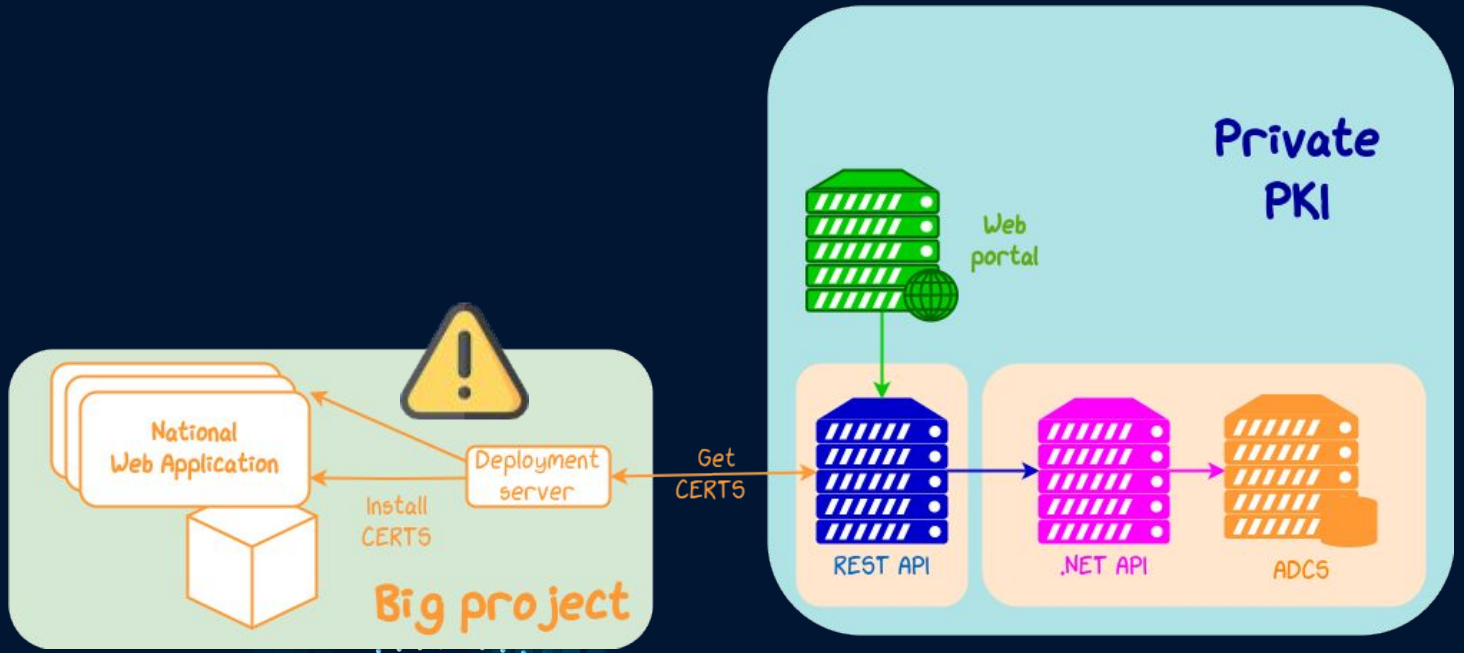
1 PKI privée, 2 Workflows



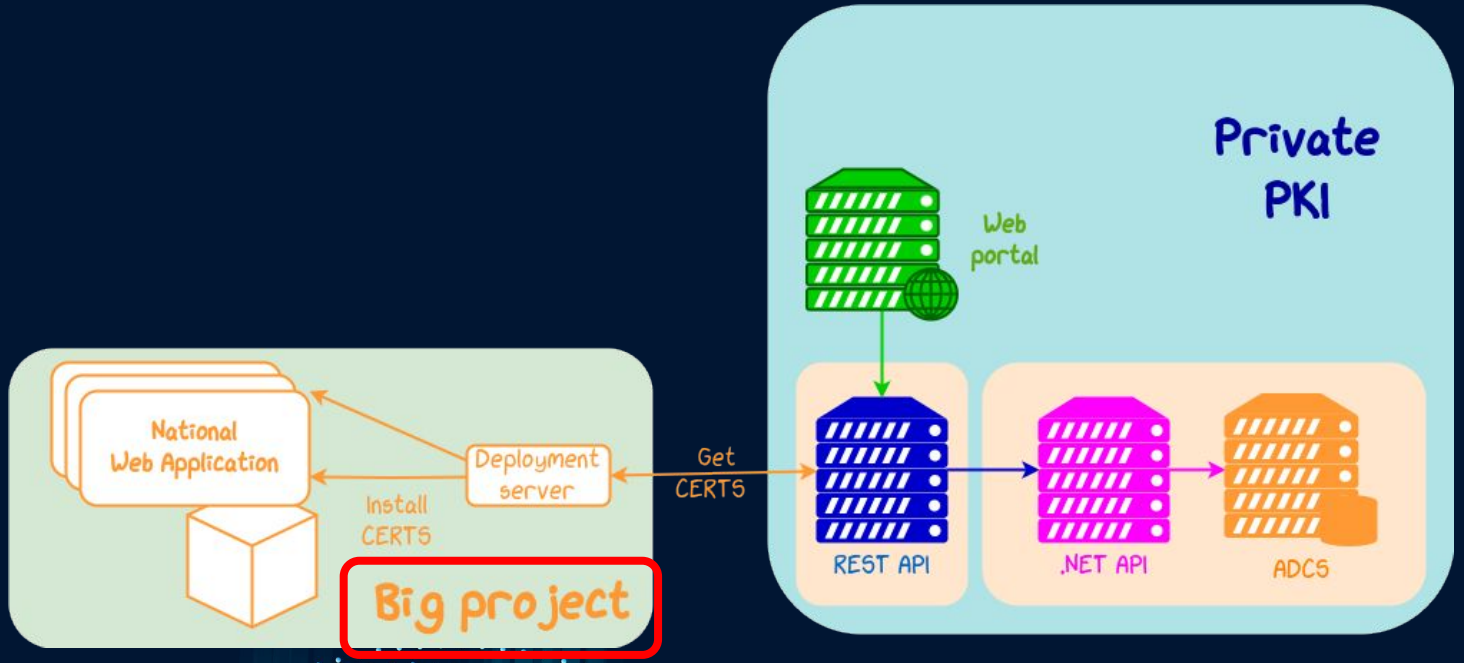
1 PKI privée, 2 Workflows



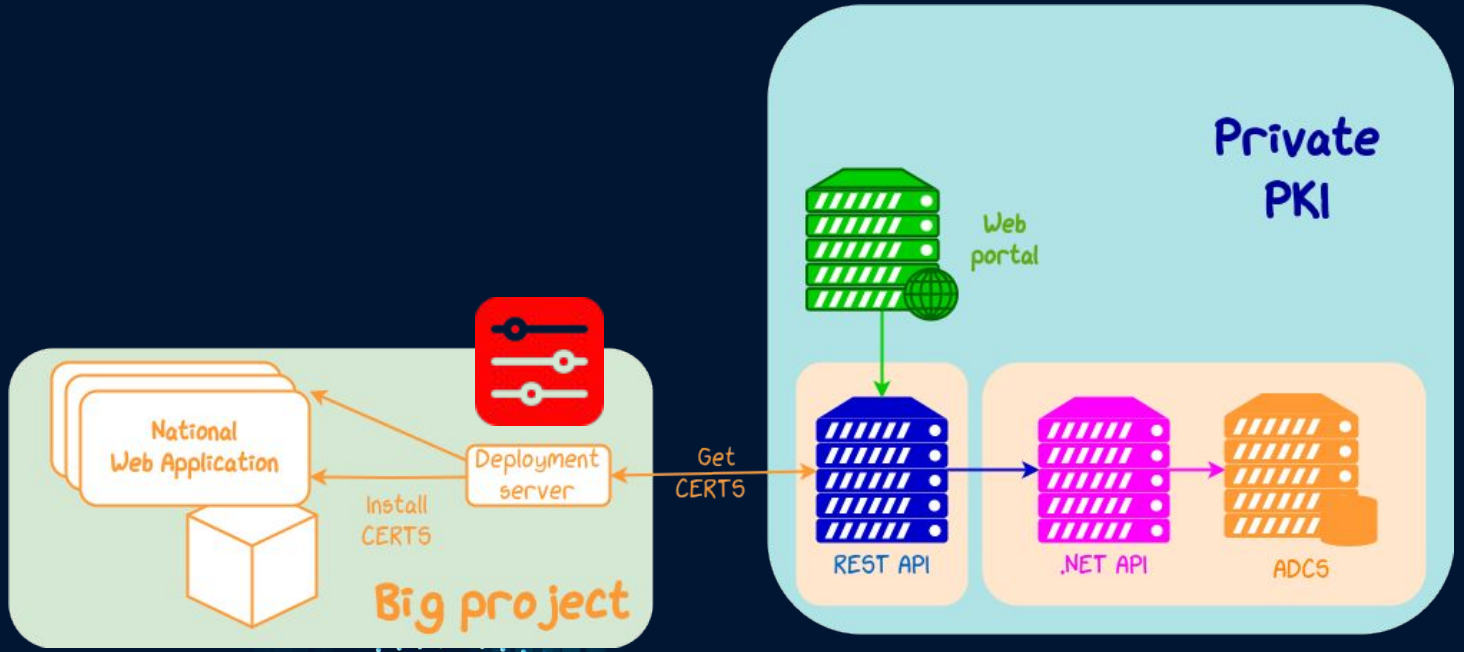
1 PKI privée, 2 Workflows



1 PKI privée, 2 Workflows

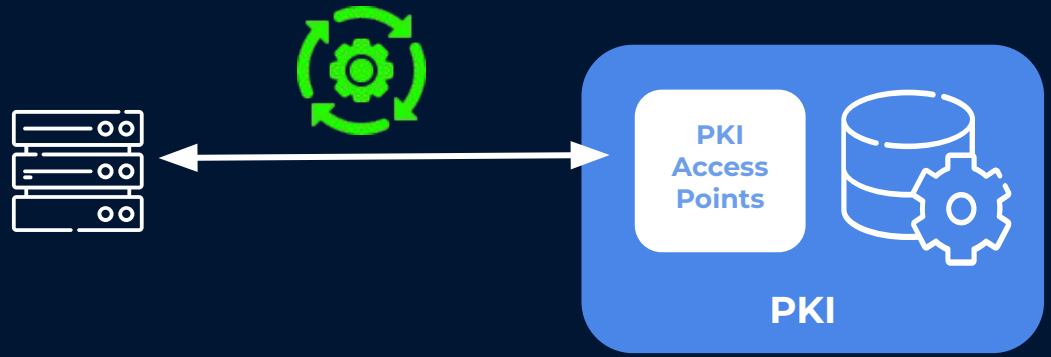


1 PKI privée, 2 Workflows



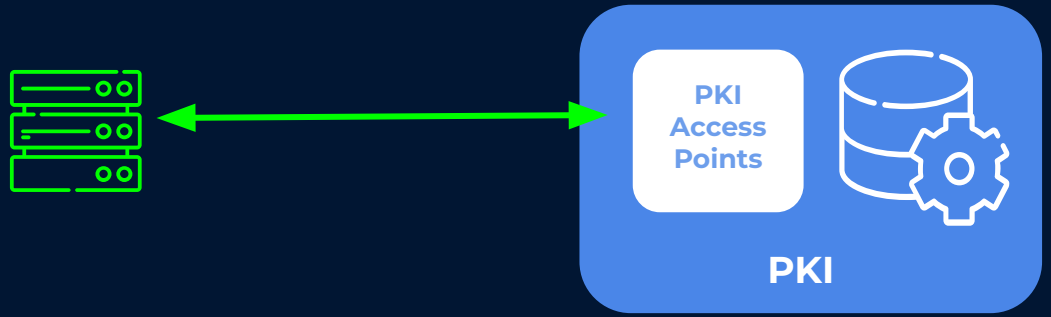
Nos besoins

Nos besoins



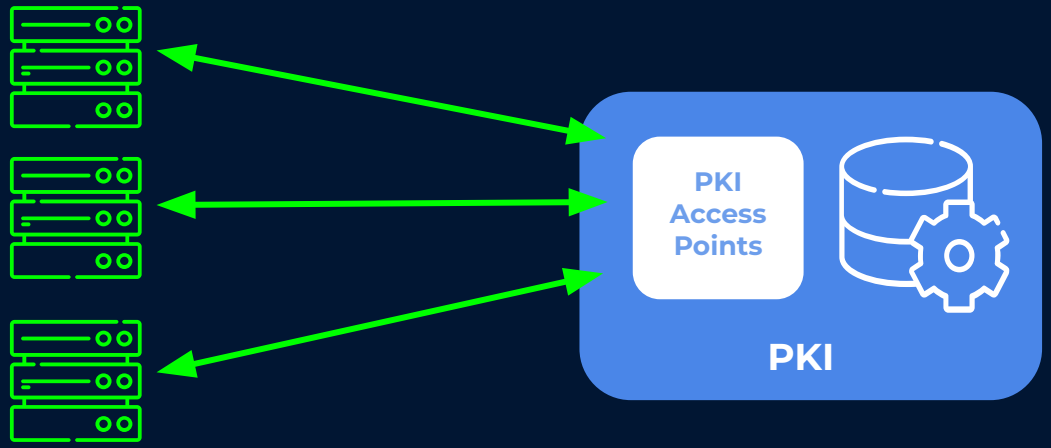
Émission de certificats

Nos besoins



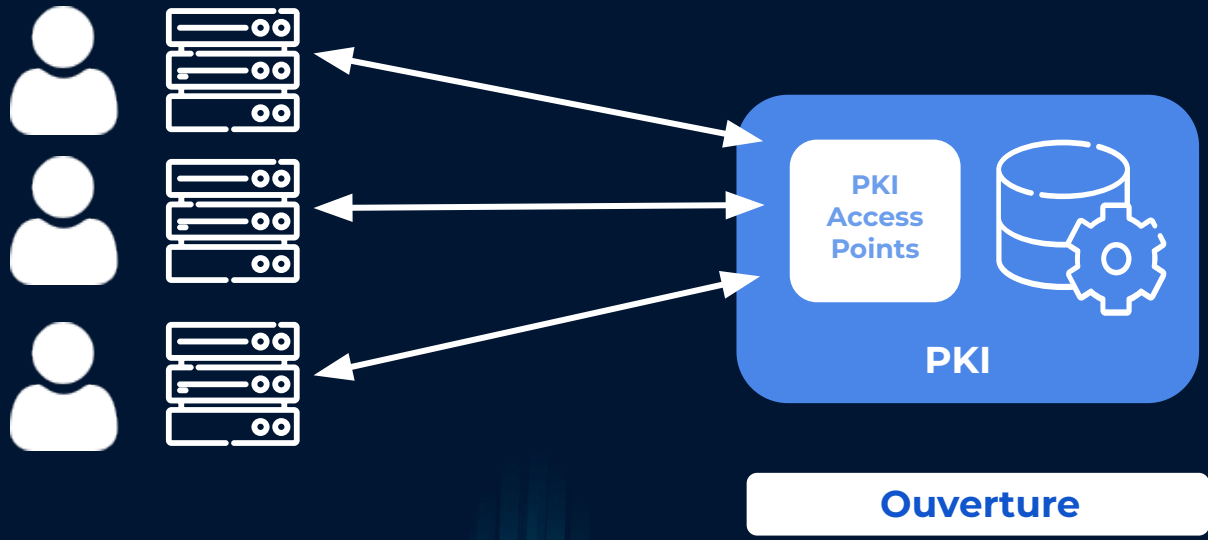
Validation des requêtes

Nos besoins



Validation des requêtes

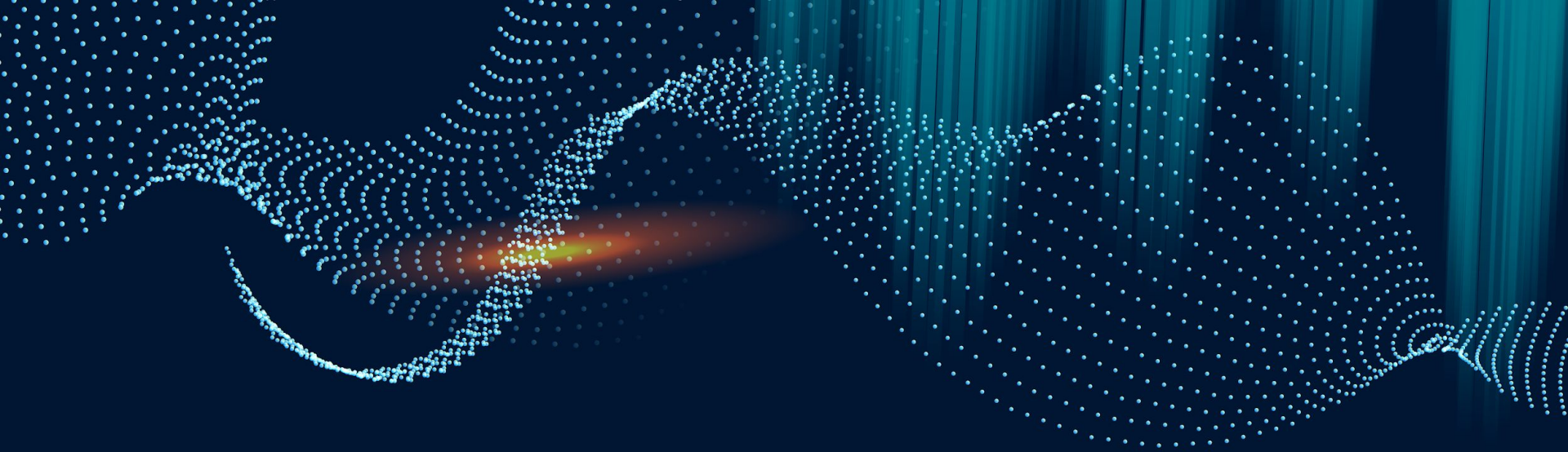
Nos besoins



Ouverture

Nos besoins

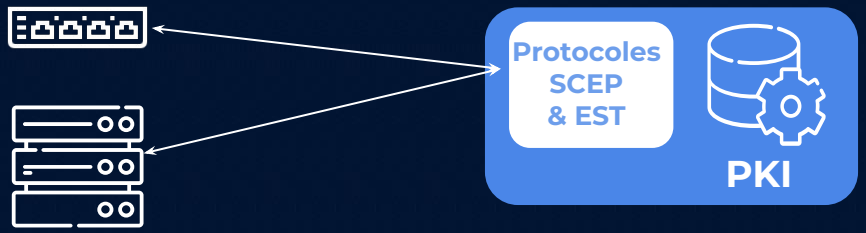
Pas de ressources en +



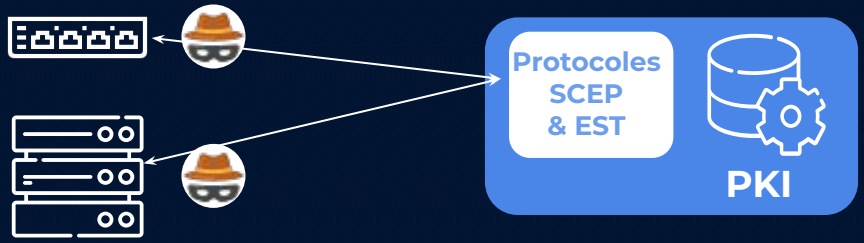
02 Bâtir notre solution

Protocoles automatisés d’obtention de certificats TLS serveur

Solutions existantes dans l'écosystème PKI privées



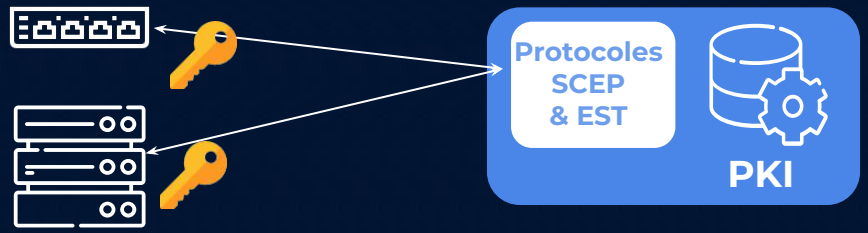
Solutions existantes dans l'écosystème PKI privées



Mais

- Problèmes de Sécurité

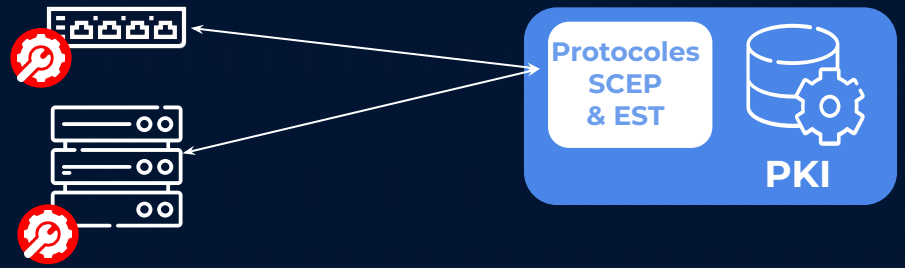
Solutions existantes dans l'écosystème PKI privées



Mais

- Problèmes de Sécurité
- Enrôlement nécessaire

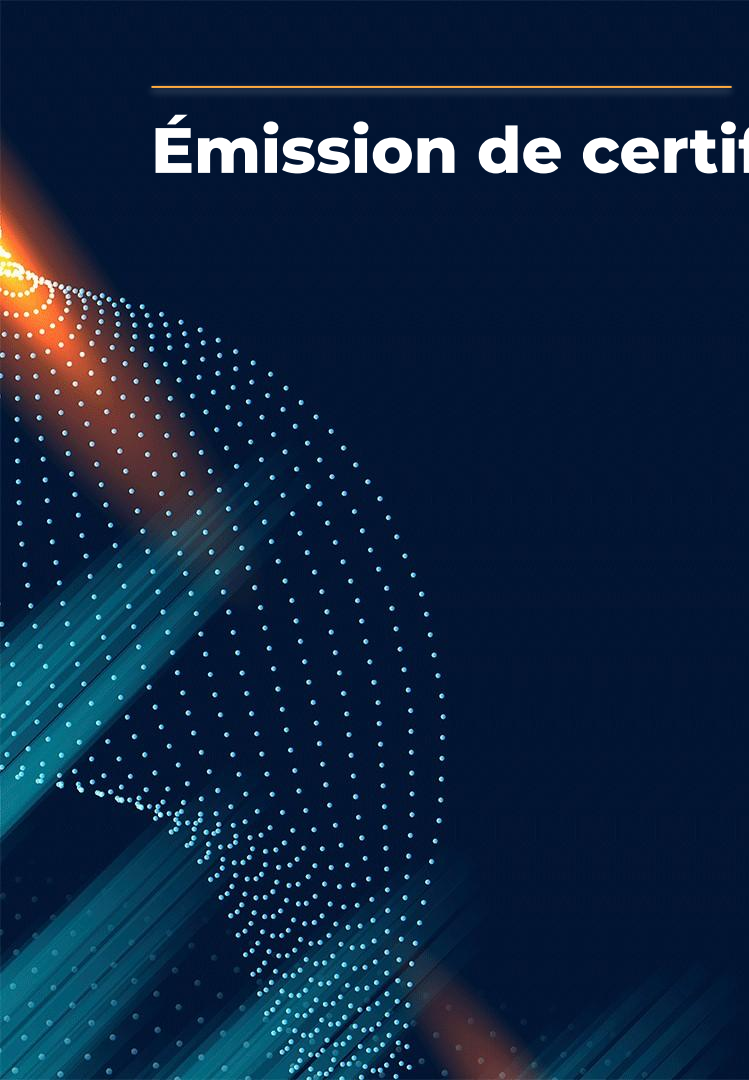
Solutions existantes dans l'écosystème PKI privées



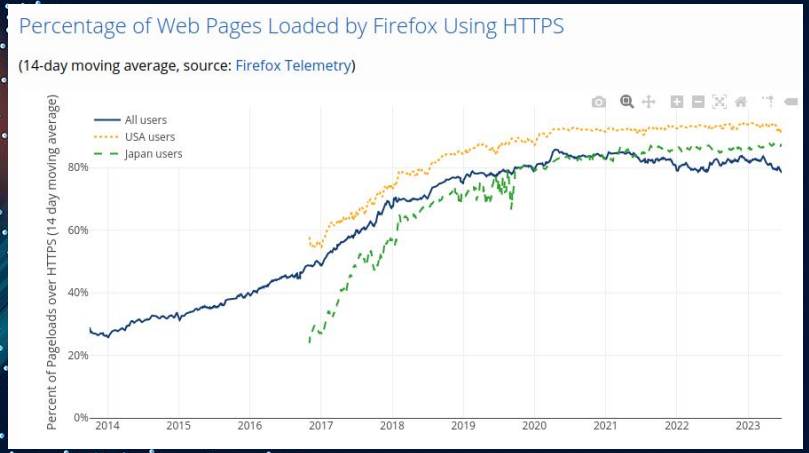
Mais

- Problèmes de Sécurité
- Enrôlement nécessaire
- Clients

Émission de certificats TLS serveur sur Internet ?



Let’s Encrypt



- Autorité de certification gratuite et automatique
- Signe des certificats TLS serveur
- Lancée en 2015.

Impact sur le trafic web :

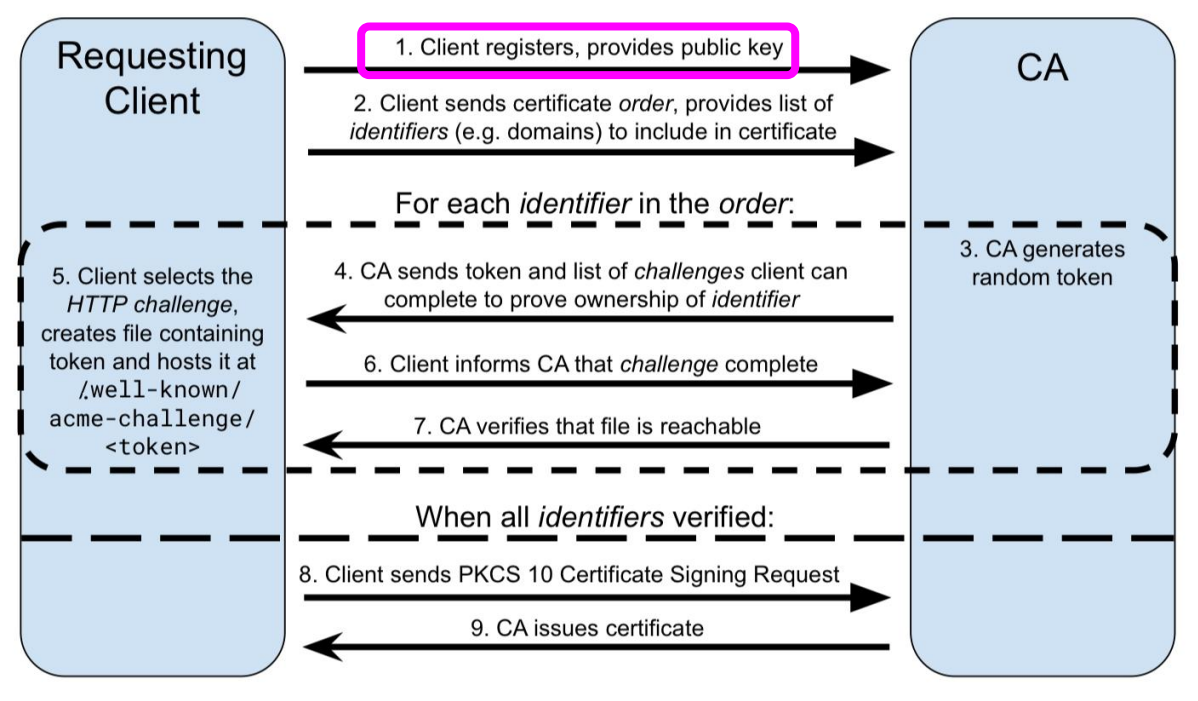
- 2014 **~ 27%** HTTPS
- 2023 **> 80%** HTTPS

→ repose sur le **protocole ACME**

Comment ACME a changé le Web ?

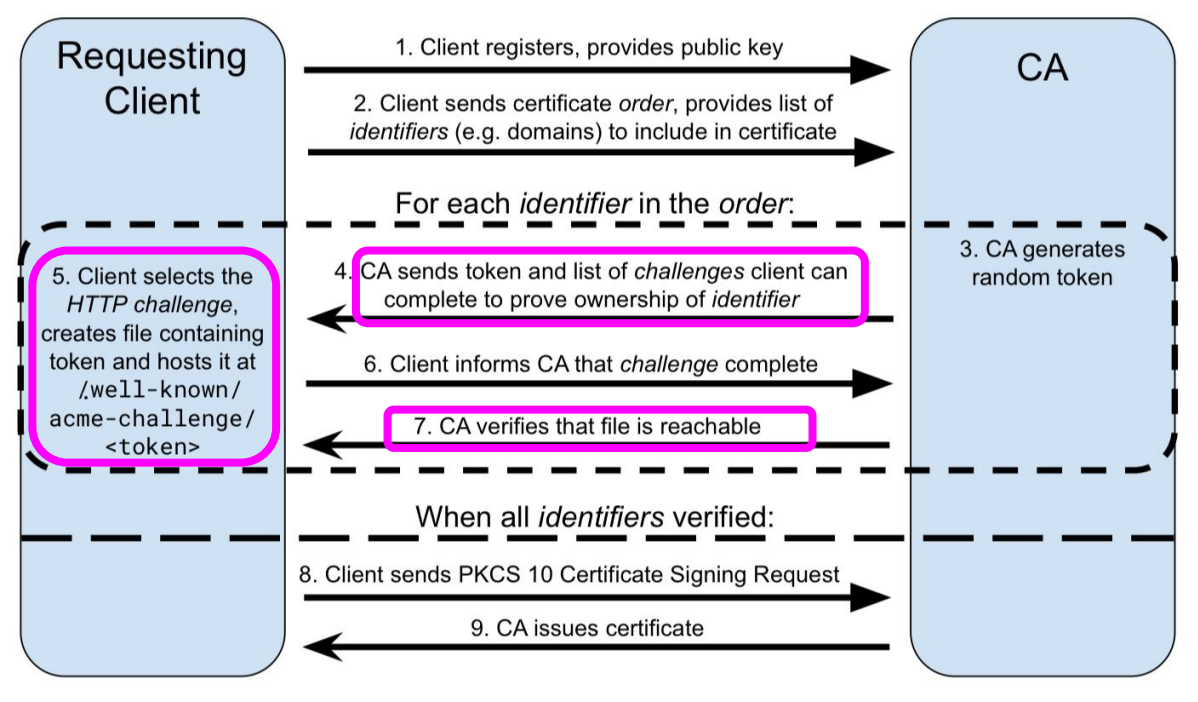
- **Protocole entièrement automatisé**
- **Standard ouvert** (RFC 8555)
- **Protocole sécurisé & implémentation robuste**

ACME : comment cela fonctionne ?



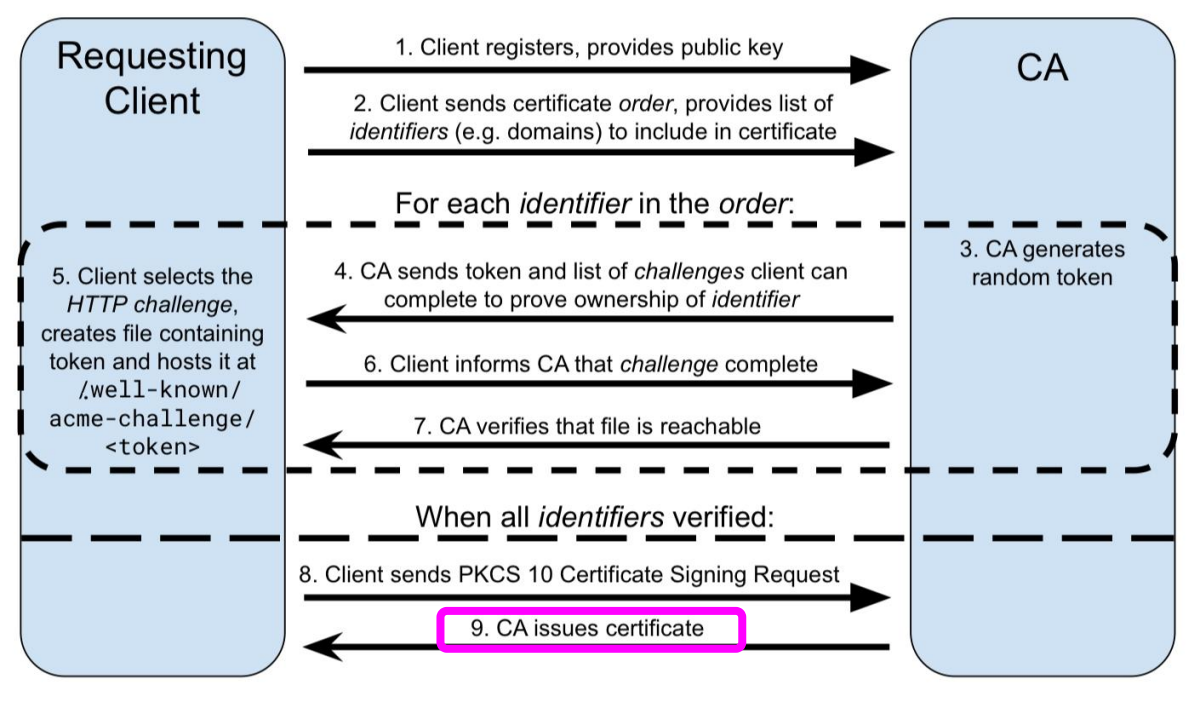
"Let's Encrypt: an automated certificate authority to encrypt the entire web." Aas et al. CCS'19. Figure 2. Src: https://par.nsf.gov/servlets/purl/10222849

ACME : comment cela fonctionne ?



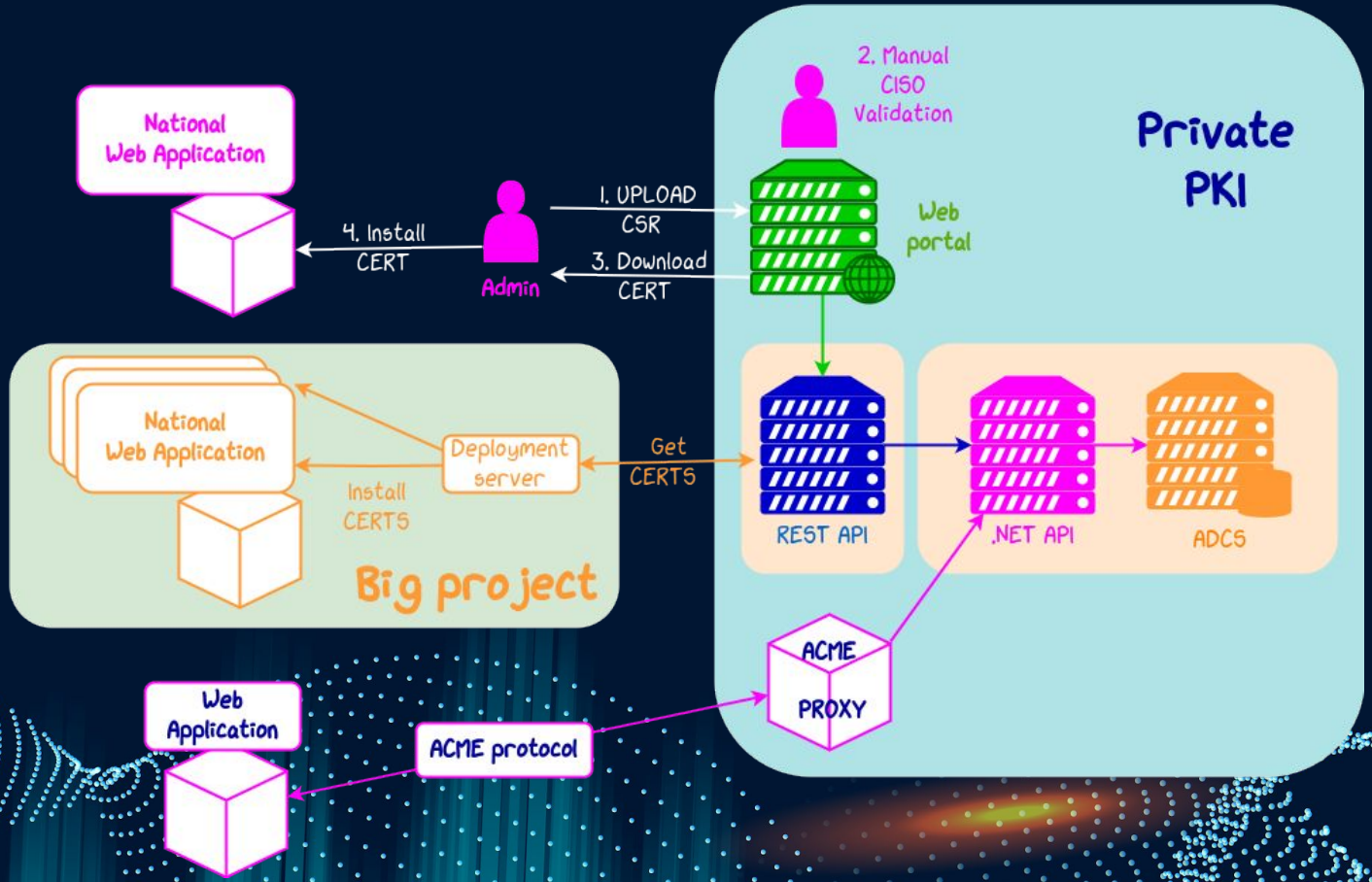
"Let's Encrypt: an automated certificate authority to encrypt the entire web." Aas et al. CCS'19. Figure 2. Src: https://par.nsf.gov/servlets/purl/10222849

ACME : comment cela fonctionne ?



"Let's Encrypt: an automated certificate authority to encrypt the entire web." Aas et al. CCS'19. Figure 2. Src: https://par.nsf.gov/servlets/purl/10222849

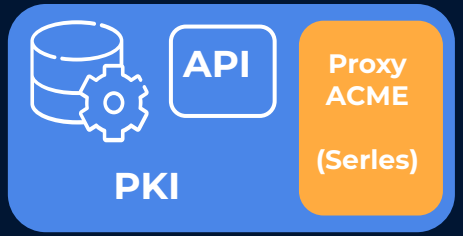
PKI privée : ajout d'ACME



Adoption d’ACME : ce qu’a apporté notre équipe

Adoption d'ACME : ce qu'a apporté notre équipe

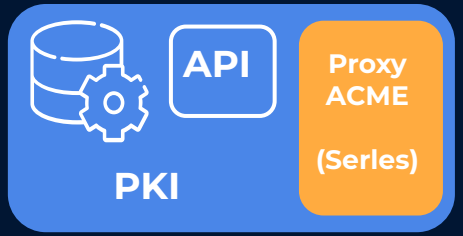
Un **proxy ACME**, **ouvert à tous** sur le réseau privé
*(basé sur l'outil **Serles*** : **proxy ACME open source**, écrit en Python)*



* : https://github.com/dvtirol/serles-acme

Adoption d'ACME : ce qu'a apporté notre équipe

Un **proxy ACME**, **ouvert à tous** sur le réseau privé
*(basé sur l'outil **Serles*** : **proxy ACME open source**, écrit en Python)*

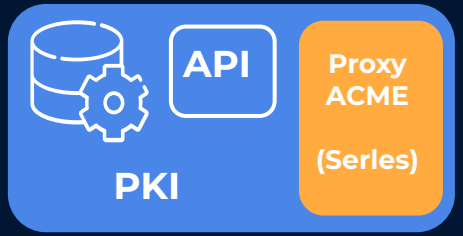


Un **client ACME** de référence pour Linux & Windows
*(**lego**** : un **client ACME open source**, écrit in Go)*

* : https://github.com/dvtirol/serles-acme
** : https://github.com/go-acme/lego

Adoption d'ACME : ce qu'a apporté notre équipe

Un **proxy ACME**, **ouvert à tous** sur le réseau privé
*(basé sur l'outil **Serles*** : **proxy ACME open source**, écrit en Python)*



Un **client ACME** de référence pour Linux & Windows
*(**lego**** : un **client ACME open source**, écrit in Go)*

Support & évangélisation :

- Site web de documentation ;
- Webinaires ;
- Support aux admins pour installation & 1er usage ;
- Support aux architectes & projets pour un usage de clients ACME ou des cas d'usages spécifiques.

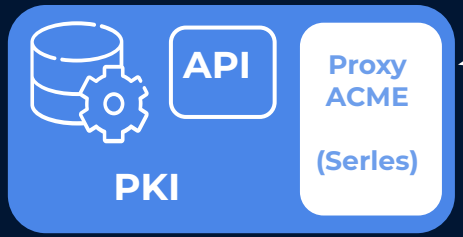
* : https://github.com/dvtirol/serles-acme
** : https://github.com/go-acme/lego

Adoption d'ACME : ce que les utilisateurs ont aussi fait

D'autres clients ACME & plateformes

(ex : acme.sh sur AIX, appliances réseaux ...)

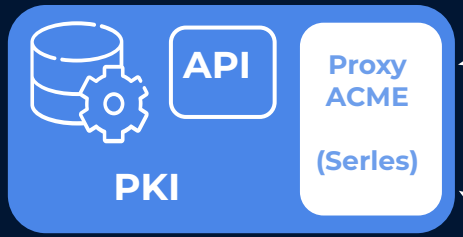
Adoption d'ACME : ce que les utilisateurs ont aussi fait



D'autres clients ACME & plateformes
(ex : acme.sh sur AIX, appliances réseaux ...)

Middlewares (Caddy, Apache, Traefik...) avec un support d'ACME embarqué

Adoption d'ACME : ce que les utilisateurs ont aussi fait



D'autres clients ACME & plateformes
(ex : acme.sh sur AIX, appliances réseaux ...)

Middlewares (Caddy, Apache, Traefik...) avec un support d'ACME embarqué

Obtenir un **certificat "client+server auth"** pendant la création du serveur/VM (**client ACME Ansible**) afin de faire du mTLS plus facilement.

ACME nouveau cas d'usage

En 2022, sort un nouveau draft de RFC : `draft-bweeks-acme-device-attest-01`(*)

- **But :** obtenir un certificat client pour un périphérique
- **Condition :** vérifier un certain nombre de ses propriétés (identité du périphérique, clé privée protégée par un cryptoprocesseur)
- Nouveau challenge : `device-attest-01`, basé sur une attestation.

(*) https://www.ietf.org/archive/id/draft-bweeks-acme-device-attest-01.html

ACME nouveau cas d'usage

En 2022, sort un nouveau draft de RFC : `draft-bweeks-acme-device-attest-01`(*)

- **But :** obtenir un certificat client pour un périphérique
- **Condition :** vérifier un certain nombre de ses propriétés (identité du périphérique, clé privée protégée par un cryptoprocesseur)
- Nouveau challenge : `device-attest-01`, basé sur une attestation.

Prémisces

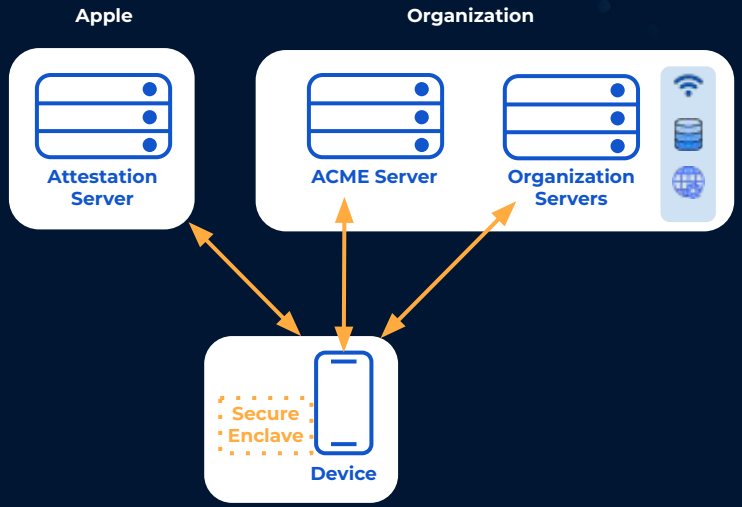
Pour le moment, la draft de cette RFC **ne dit pas :**

- **comment valider** l'attestation
- ni **comment vérifier** l'identité du périphérique

Ces tâches sont très dépendantes des plateformes des différents périphériques.

(*) https://www.ietf.org/archive/id/draft-bweeks-acme-device-attest-01.html

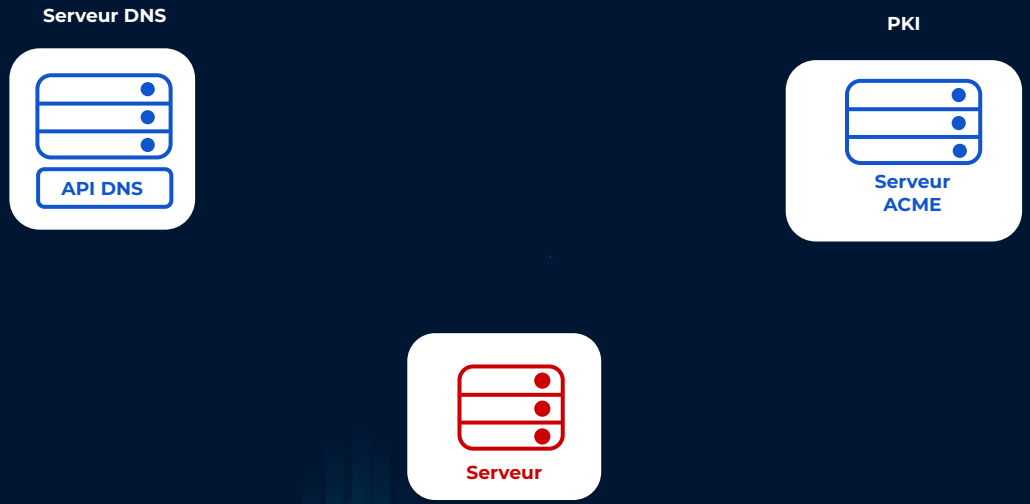
ACME nouveau cas d'usage : comment obtenir un certificat client



Première implementation* : **Apple** dans sa **solution MDM** en 2022.

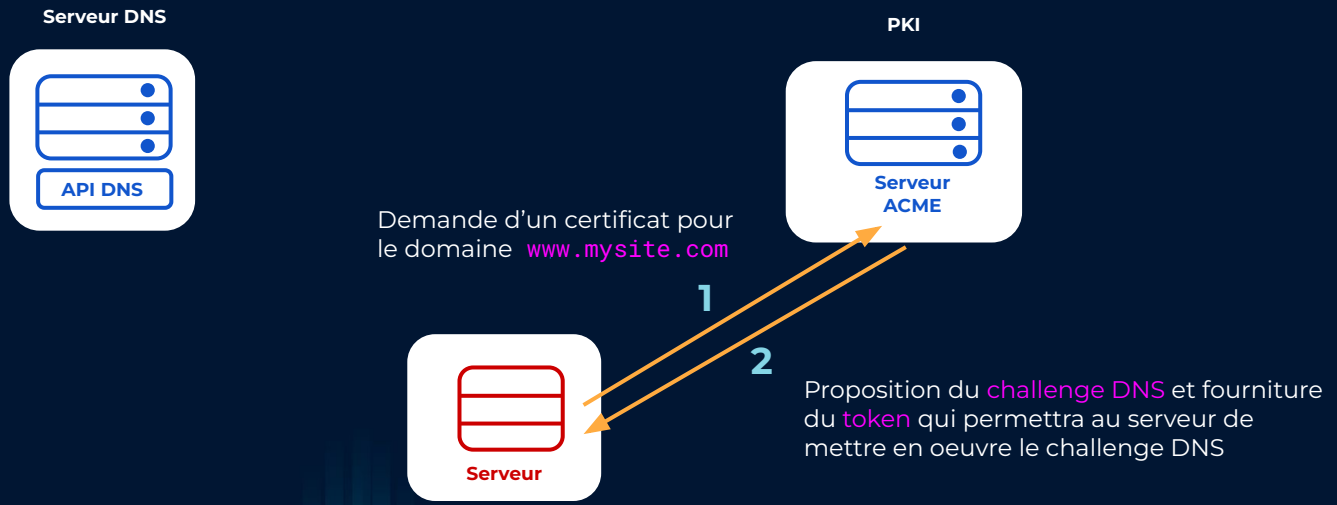
* : https://developer.apple.com/videos/play/wwdc2022/10143/

Digression #1 : challenge DNS-01

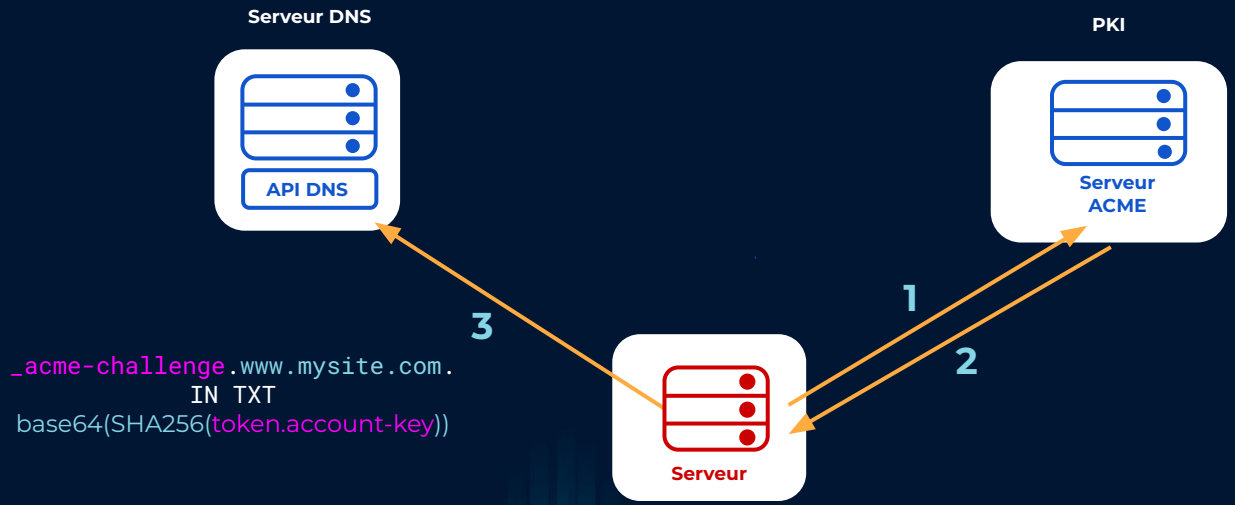


Digression #1 : challenge DNS-01

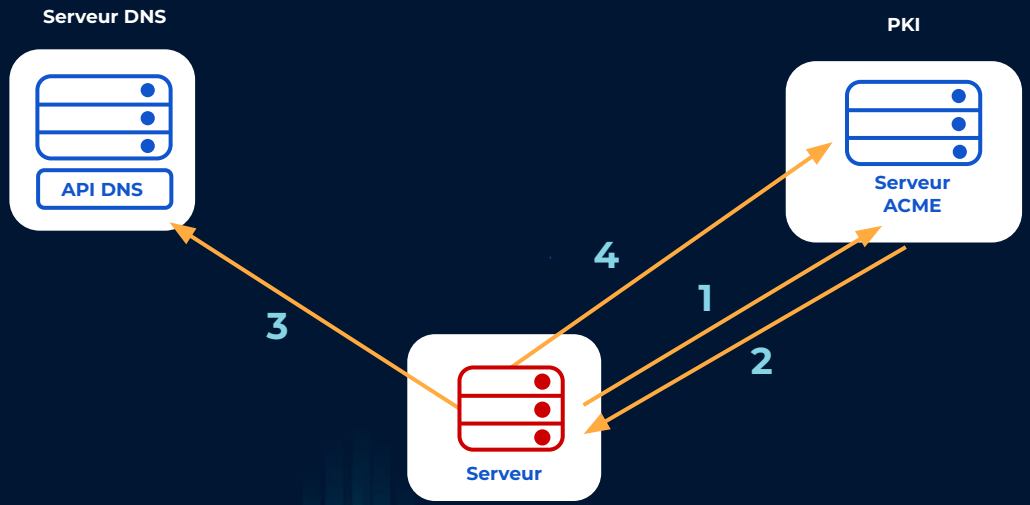
Digression #1 : challenge DNS-01



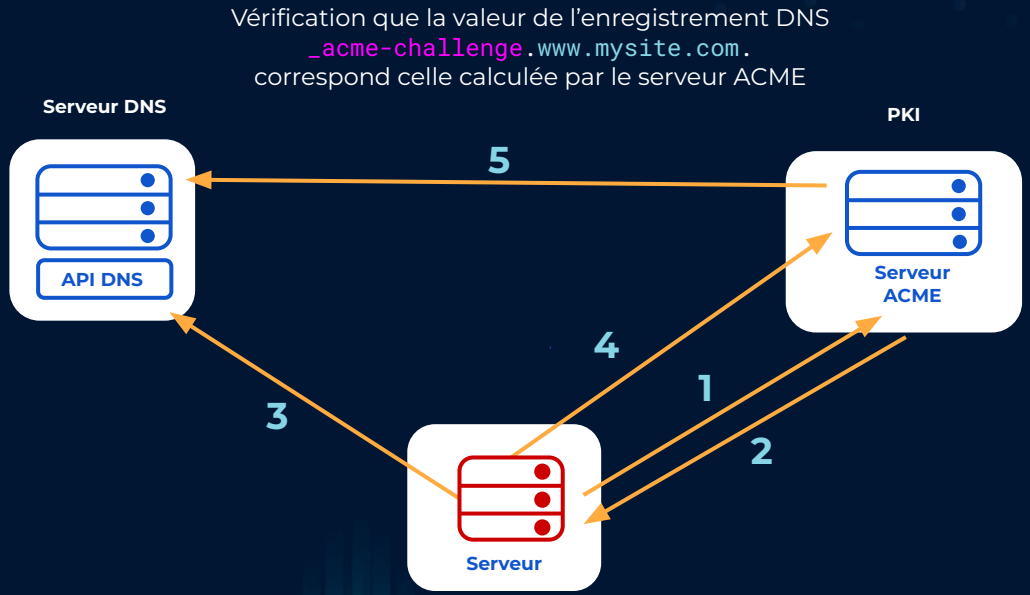
Digression #1 : challenge DNS-01



Digression #1 : challenge DNS-01



Digression #1 : challenge DNS-01



Digression #2 : architecture

1) Mode Autorité d'Enregistrement

Exemples de Logiciels libres dispo : Serles, SmallStep step-ca en mode RA*

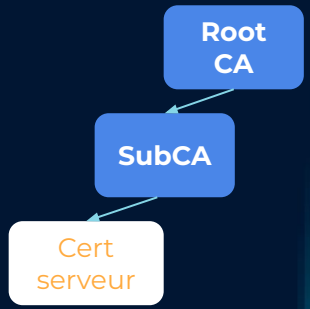
* : https://smallstep.com/docs/step-ca/registration-authority-ra-mode/

Digression #2 : architecture

1) Mode Autorité d'Enregistrement

Exemples de Logiciels libres dispo : Serles, SmallStep step-ca en mode RA*

C'est la PKI existante qui signe les certificats, **pas besoin de MAJ les certificats d'AC** sur les postes et serveurs.
Bonus : pas de **clé privée** à protéger.
Ex. cas d'usage : ajout d'ACME à une PKI disposant d'une API



* : https://smallstep.com/docs/step-ca/registration-authority-ra-mode/

Digression #2 : architecture

2) Mode Autorité de Certification déléguée

Exemple de Logiciel libre dispo : SmallStep step-ca*

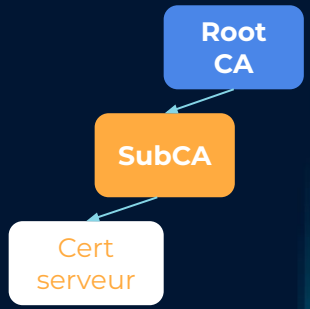
* : https://smallstep.com/docs/step-ca/

Digression #2 : architecture

2) Mode Autorité de Certification déléguée

Exemple de Logiciel libre dispo : SmallStep step-ca*

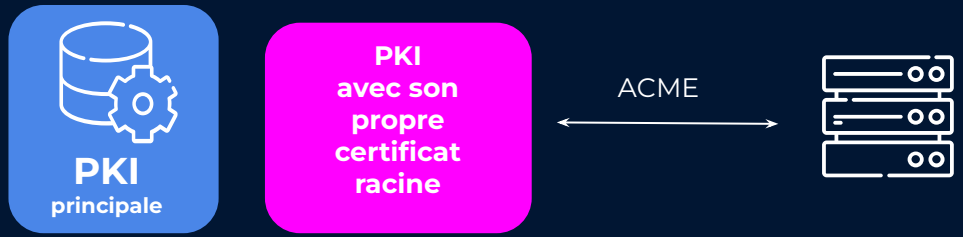
C'est une nouvelle PKI qui signe les certificats. Mais son certificat de signature a été signé par la PKI principale. **Pas besoin de MAJ les certificats d'AC** sur les postes et serveurs.
Ex. cas d'usage : PKI principale non dotée d'une API.



* : https://smallstep.com/docs/step-ca/

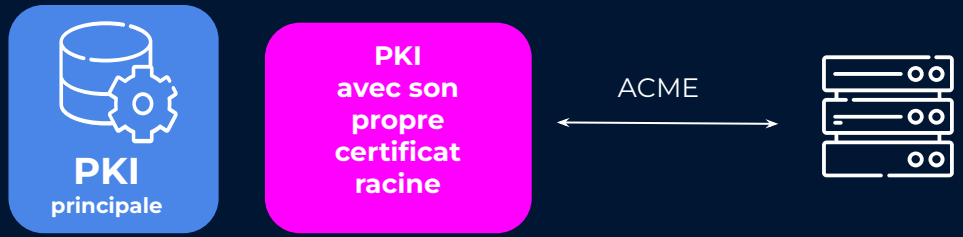
Digression #2 : architecture

3) Mode Autorité de Certification dédiée

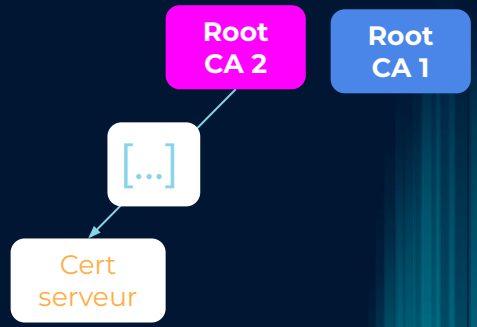


Digression #2 : architecture

3) Mode Autorité de Certification dédiée



Cette nouvelle PKI signe ses certificats avec sa propre racine de confiance. Les postes et serveurs doivent importer cette nouvelle racine de confiance.
Ex. cas d'usage : PKI délivrant des certificats à une infra ou un SI spécifique.



ACME en réseaux privés

TAKE AWAY

Améliorez votre PKI interne

- De manière sereine
  - IMPORTANT Validation sécurisée demande certificat
  - Protocole automatisé, testé à l'échelle.

Image of Jeremy Brooks, under CC By-NC licence: https://www.flickr.com/photos/jeremybrooks/3048525206/

ACME en réseaux privés

TAKE AWAY

Améliorez votre PKI interne

- De manière sereine
  - Validation sécurisée demande certificat
  - Protocole automatisé, testé à l'échelle
- Pour tous
  - PKI ouverte à tout le monde
  - Pas d'enrôlement (mais EAB disponible)
  - Pas besoin de changer votre PKI

Image of Jeremy Brooks, under CC By-NC licence: https://www.flickr.com/photos/jeremybrooks/3048525206/

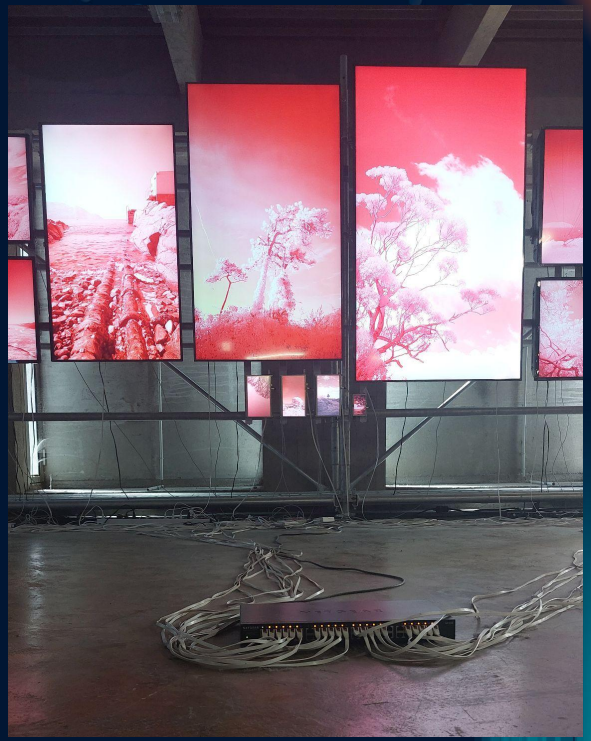
ACME en réseaux privés

TAKE AWAY

Automatisation

FACT

- Legacy | 140 applications ont migré vers TLS en 2 mois



ACME en réseaux privés

TAKE AWAY

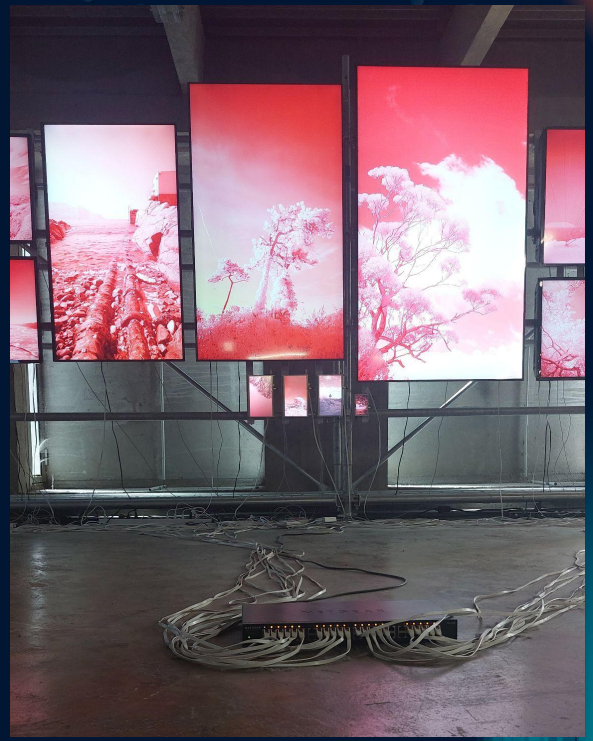
Automatisation

FACT

- Legacy | 140 applications ont migré vers TLS en 2 mois

- Devops | Une PKI dédiée n'est plus nécessaire
- Devops | Certificats, citoyens de première classe

- Bonus : La Sécurité peut être facile et efficace



ACME en réseaux privés

TAKE AWAY

Autonomie

IMPORTANT

- **Imposer un protocole, pas l'outillage**
- **La diversité des outils ACME aide à obtenir l'adhésion de beaucoup d'utilisateurs (devs, netops, admins ...)**
- **Le facteur *"déjà utilisé sur Internet"***

Image of Guilherme Cardoso, under CC By-NC licence: https://www.flickr.com/photos/guiskatenator/3228023835/

ACME en réseaux privés

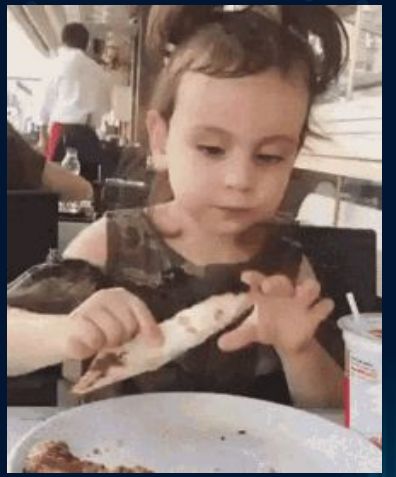
TAKE AWAY

Capitaliser sur de nouveaux cas d'usage

- Pendant la phase de provisioning des serveurs
  - Playbook Ansible ACME
  - Certificat avec un usage de la clé authent server+client
  - → Serveur peut faire du mTLS dès sa création

FACT

- De nouveaux cas d'usage arrivent (RFC pour cert client & TPM)
- D'autres challenges (ex : DNS) sont disponibles



"Manger de l'ACME, c'est bon pour votre IT !"

Merci ! Des questions?

Contact :

- christophe.brocas@assurance-maladie.fr
- twitter: @cbrocas
- mastodon: @cbrocas@infosec.exchange