ACME

Benefits of deploying an Internet security protocol inside your corporate network

Christophe BROCAS

Hack.lu 2023 | October 18th, 2023

SÉCURITÉ SOCIALE
l'Assurance Maladie
Agir ensemble, protéger chacun

Christophe Brocas

Christophe Brocas

Security engineer @ Assurance Maladie

Focus: security & network protocols

Christophe Brocas

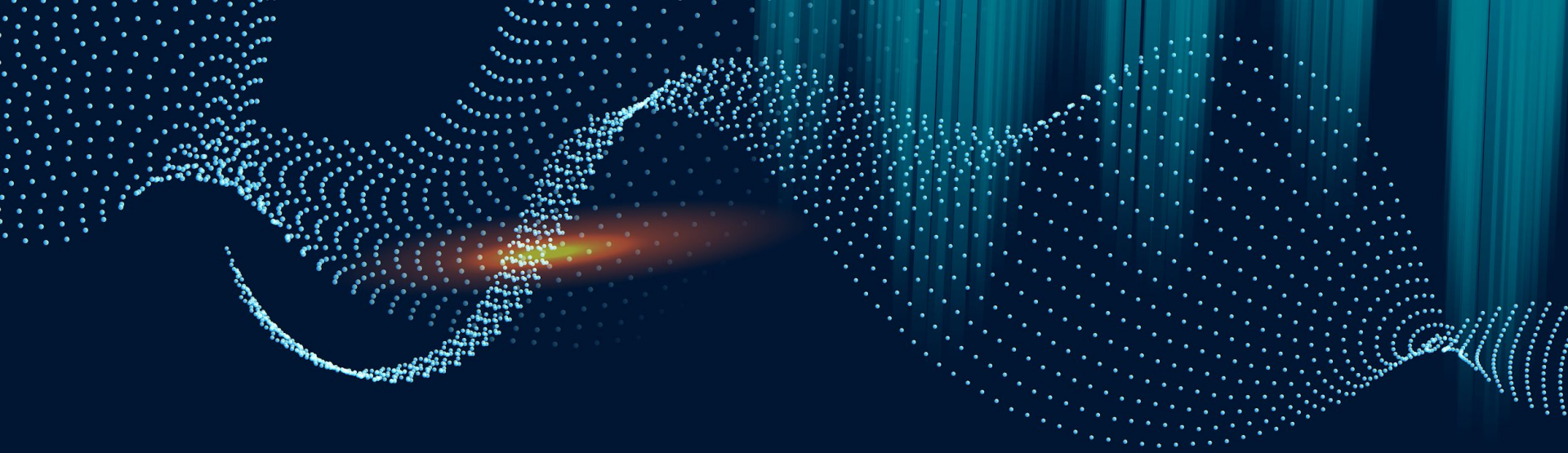
Security engineer @ Assurance Maladie

Focus: security & network protocols

Co-founder & organizer of Pass the SALT

Free Software & Security conference

But let’s start with a short poll about ACME! 🙂



01 The Problem

Private PKI fails to provide certificates to *all* apps

TL;DR version

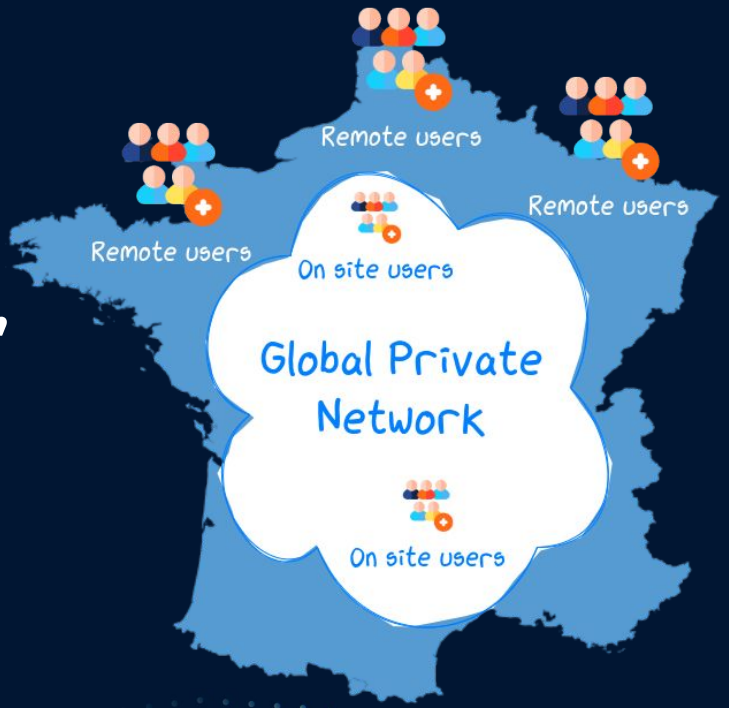
Our internal web apps are not all HTTPS accessed.
(*expired certs, self-signed certs, certs signed by custom PKI are not correct HTTPS, right?*)

Our private PKI is part of the problem.

Longer story

80.000 colleagues.

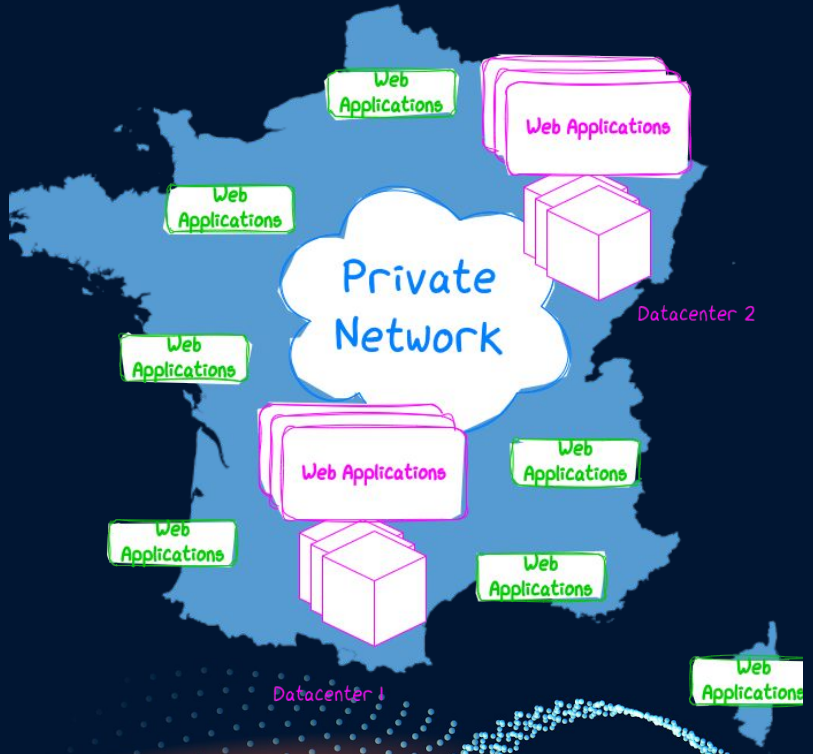
Connected, on site or remotely, to a global private network.



Many applications

Hundreds of internal web applications at national level.

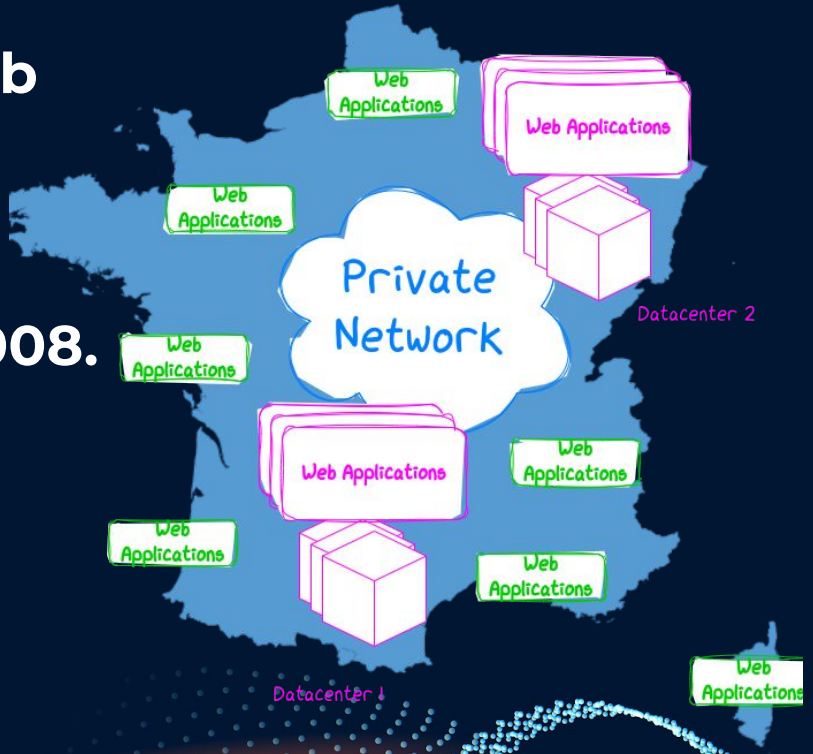
And more at local level.



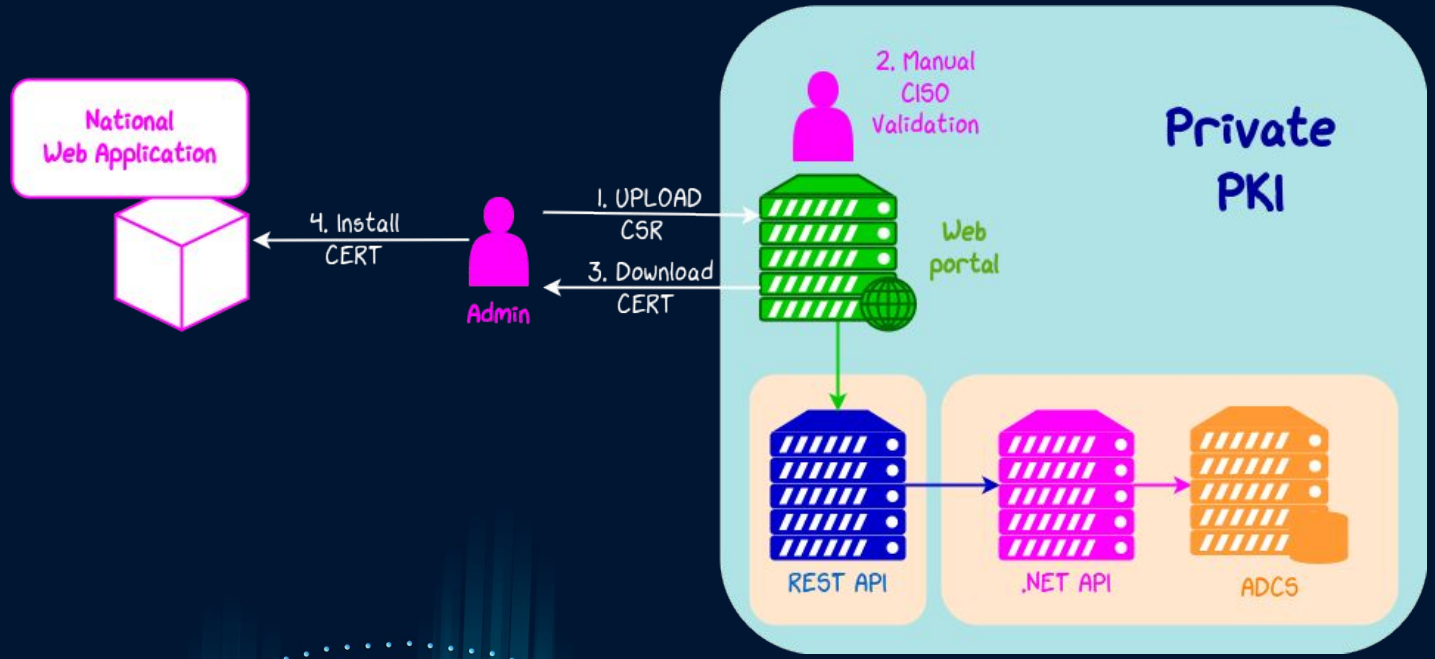
HTTPS

HTTPS required for internal web applications.

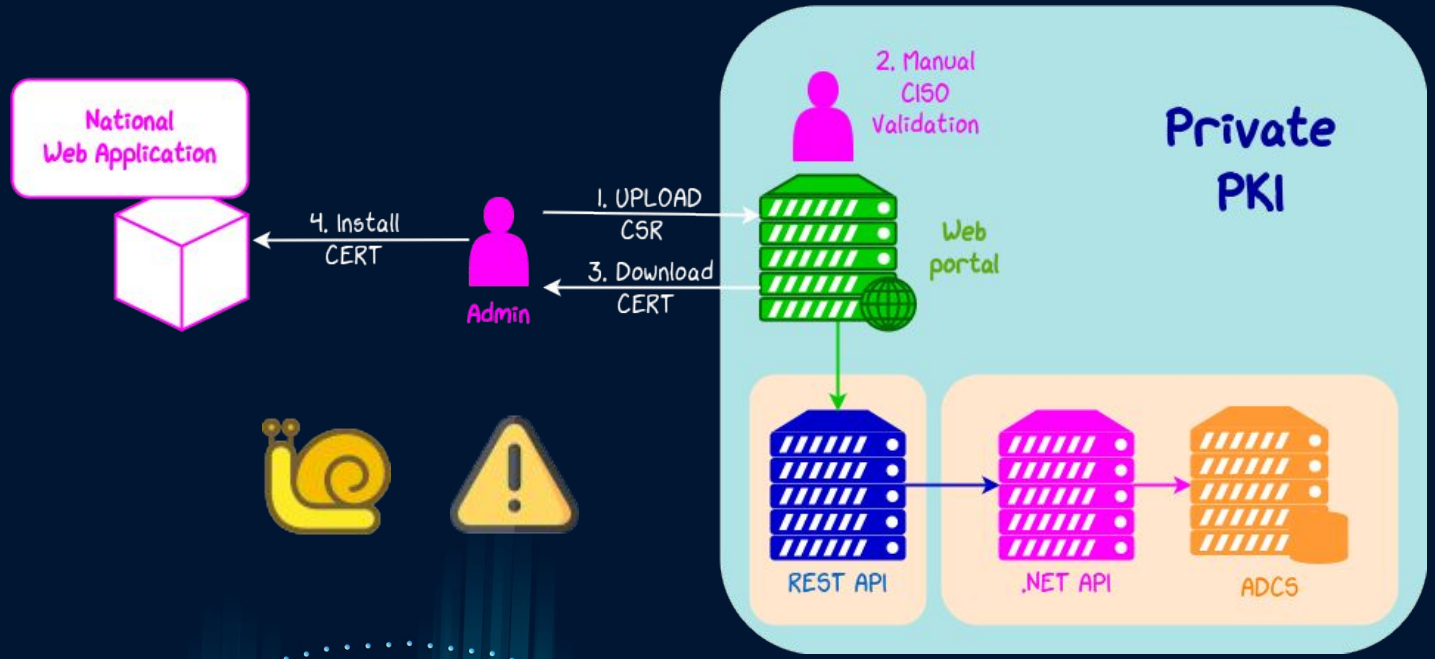
A private PKI available since 2008.



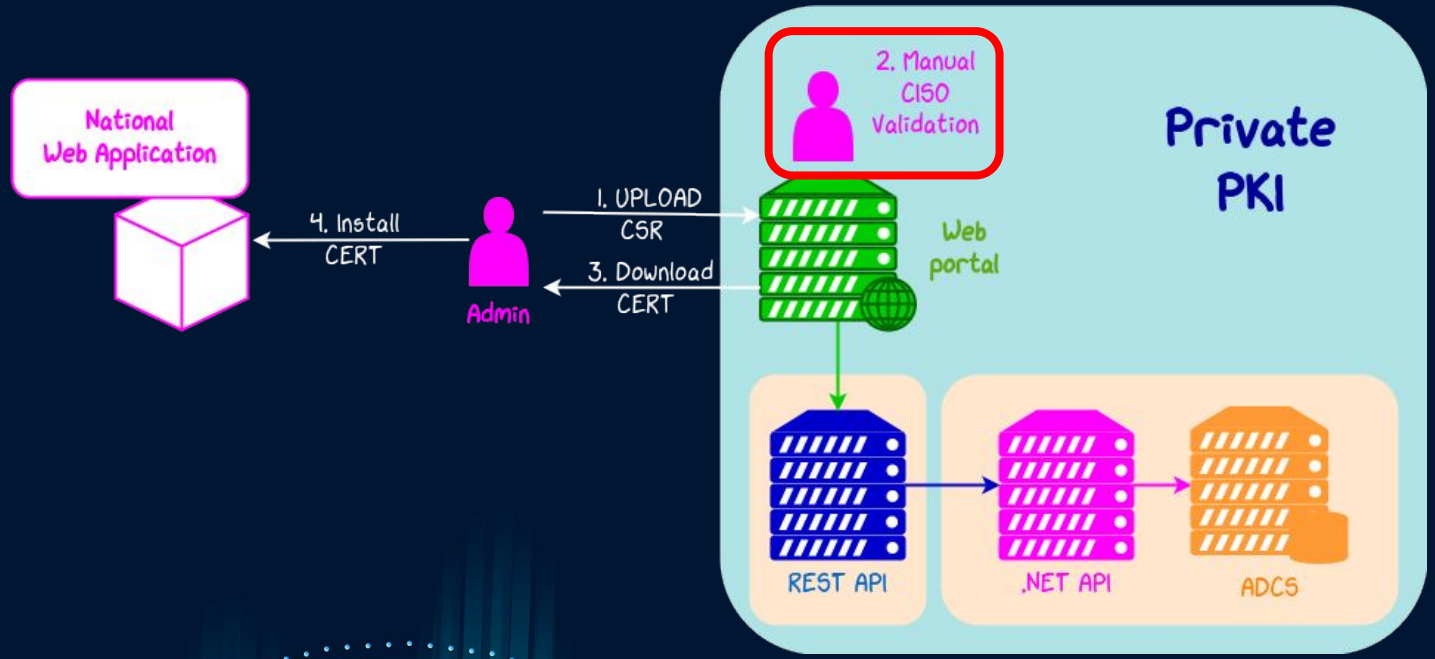
1 Private PKI, 2 Workflows



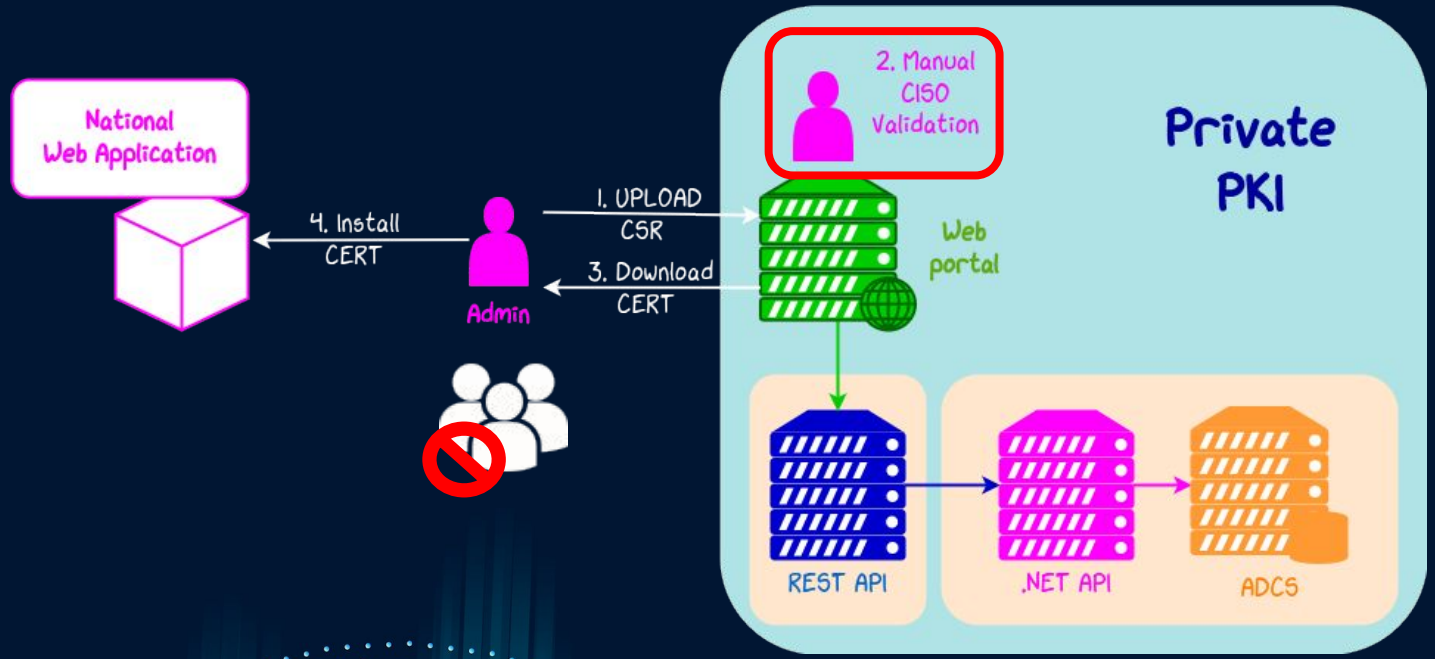
1 Private PKI, 2 Workflows



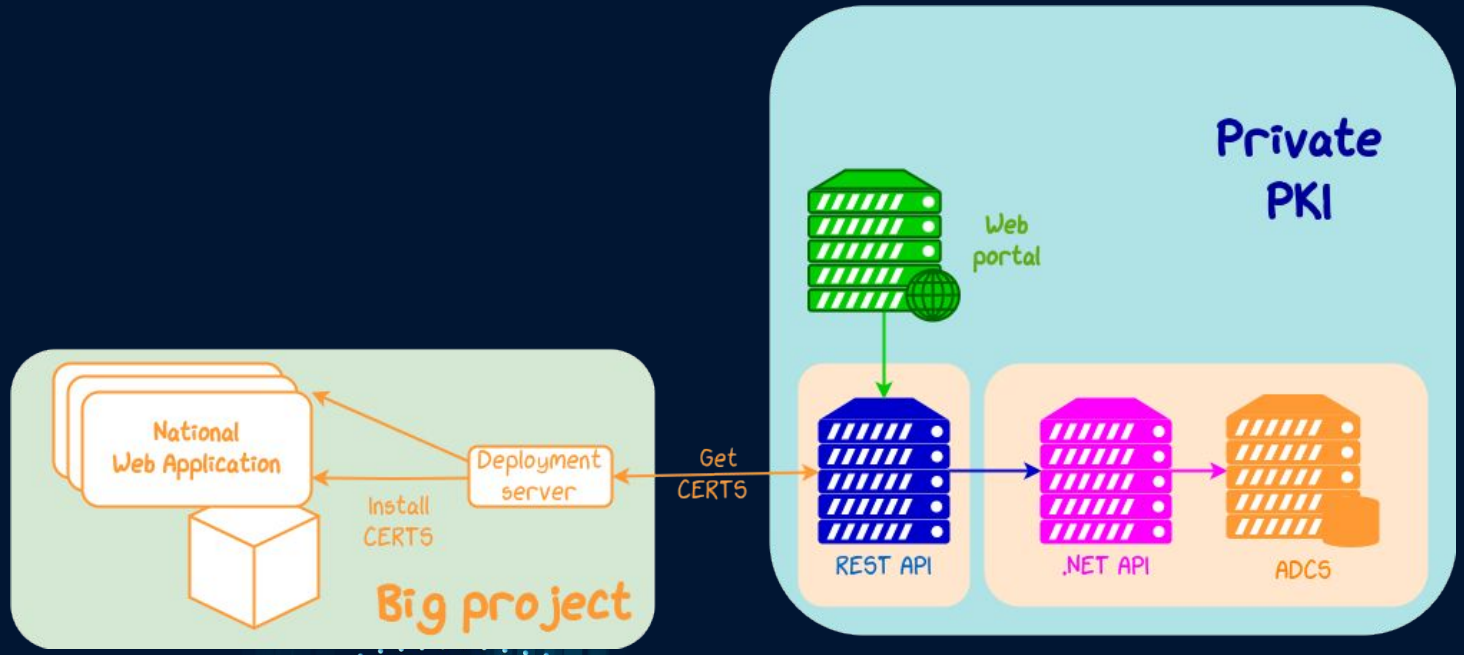
1 Private PKI, 2 Workflows



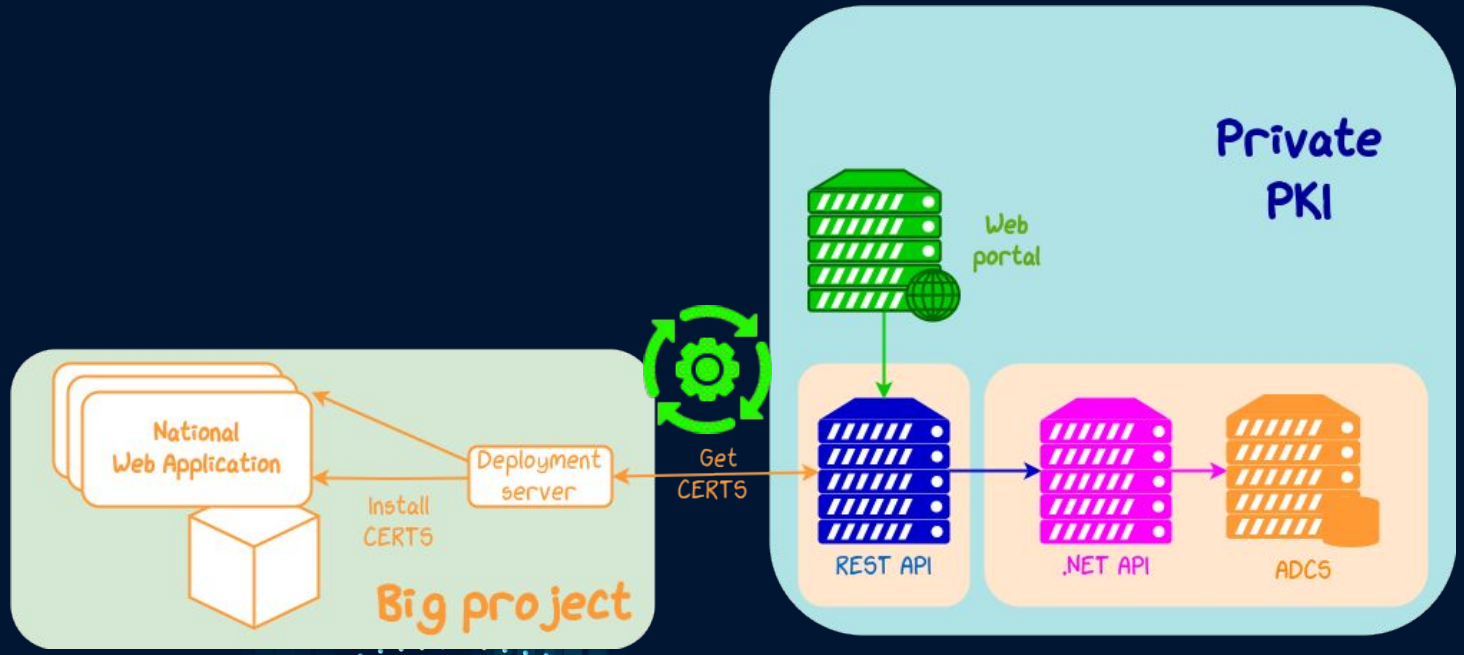
1 Private PKI, 2 Workflows



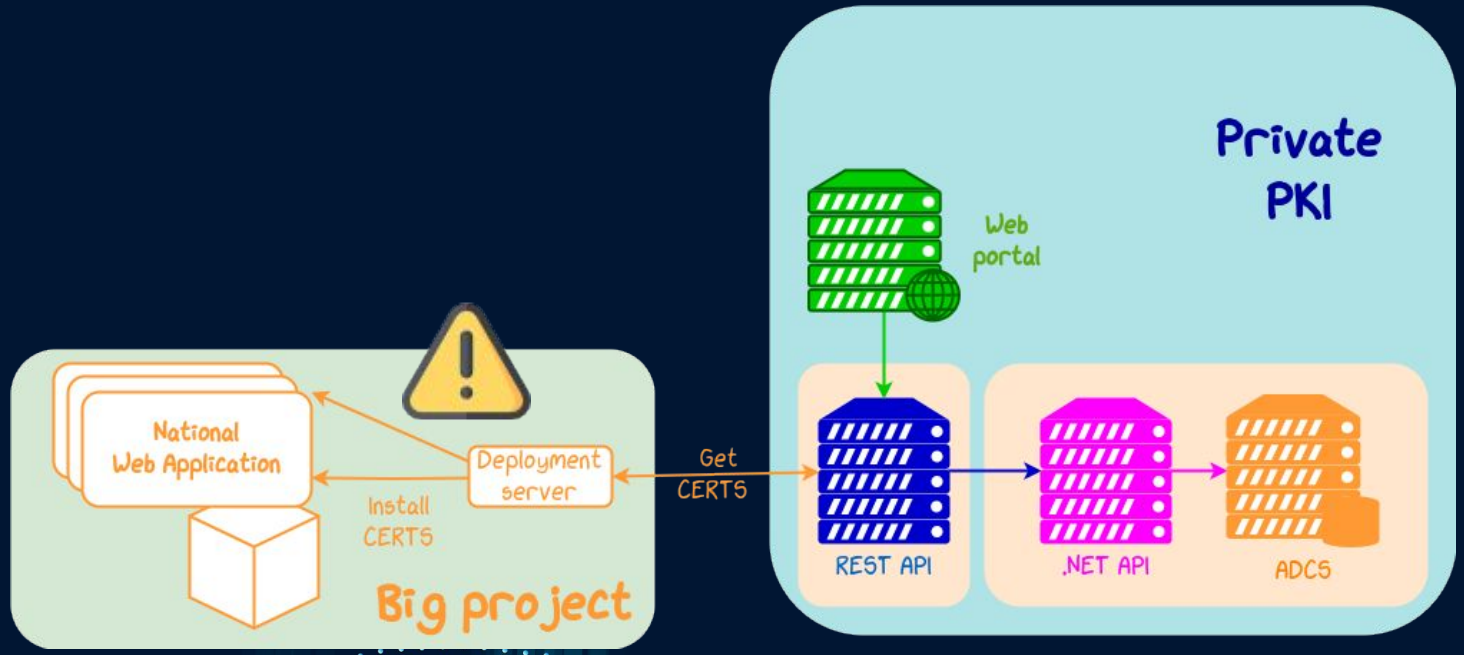
1 Private PKI, 2 Workflows



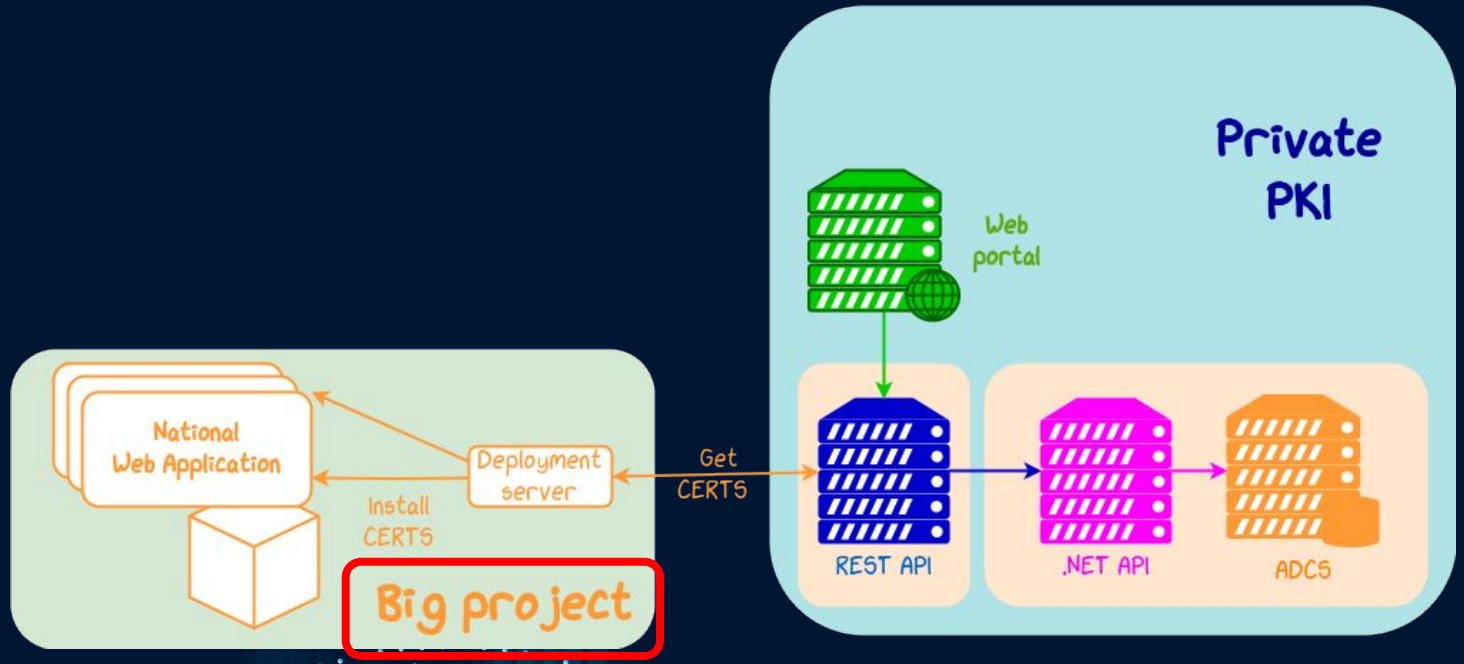
1 Private PKI, 2 Workflows



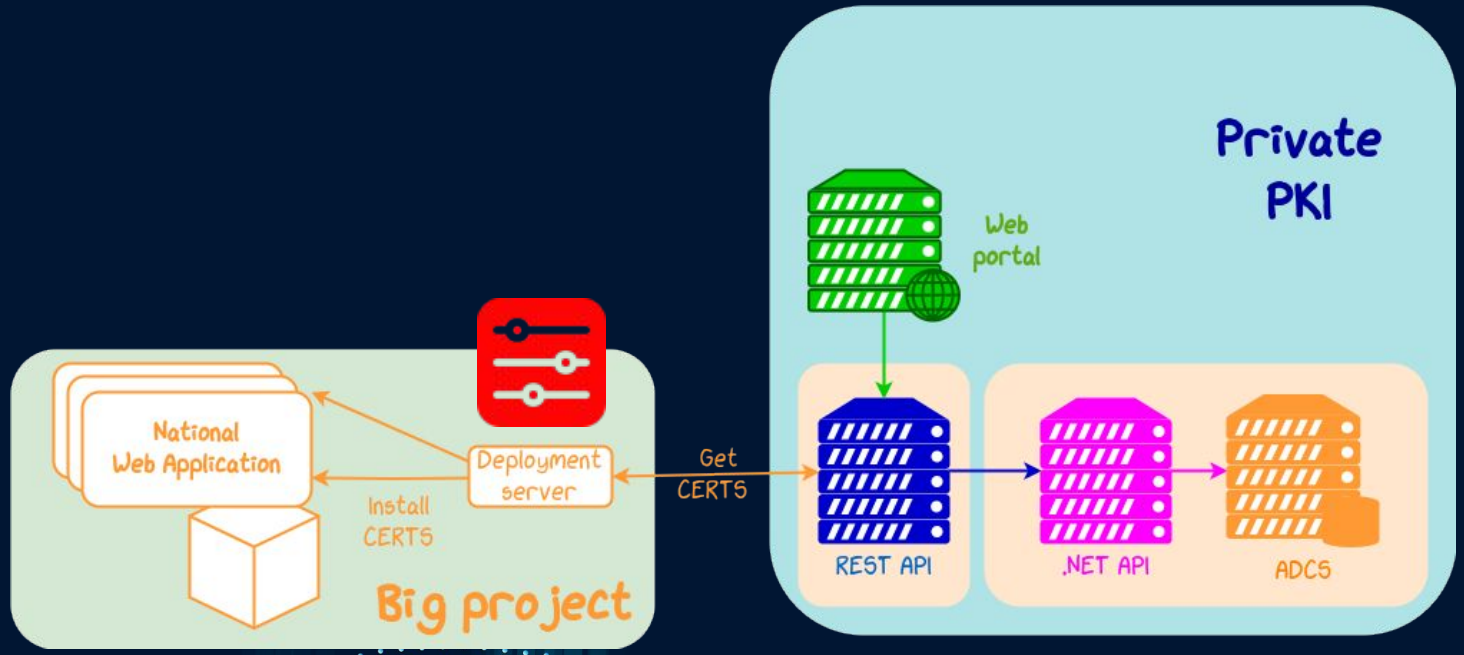
1 Private PKI, 2 Workflows



1 Private PKI, 2 Workflows

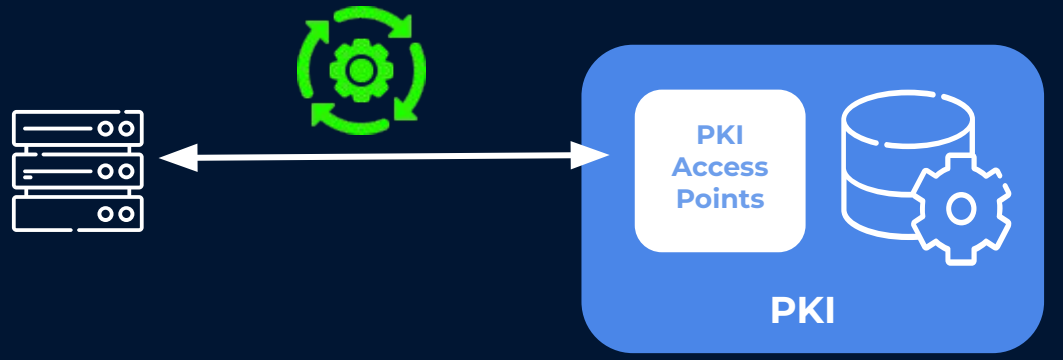


1 Private PKI, 2 Workflows



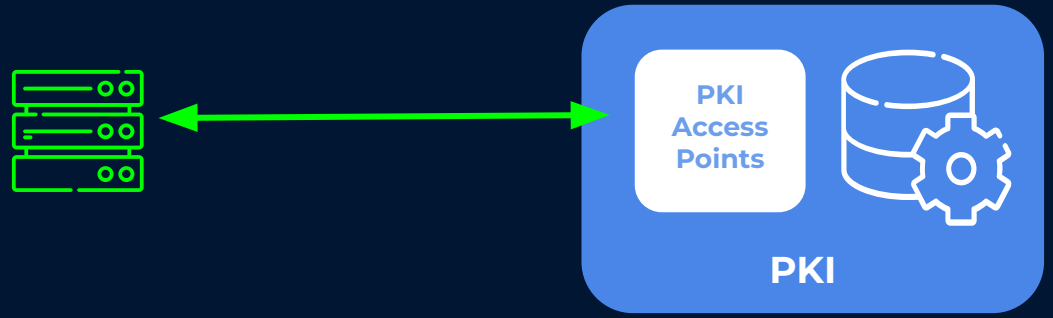
What We Need

What We Need



Certificate issuance

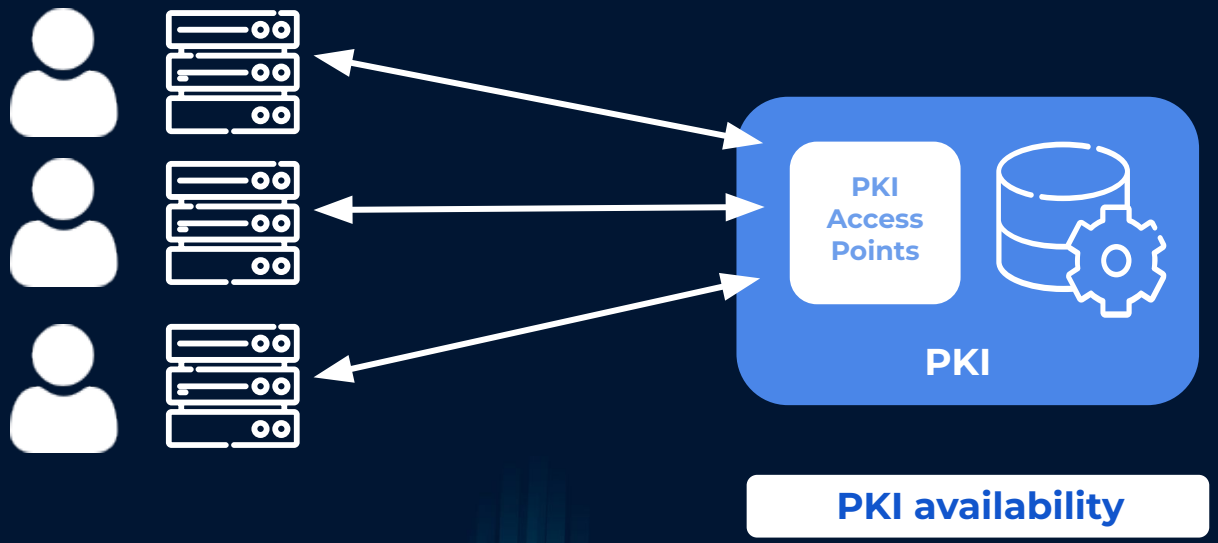
What We Need



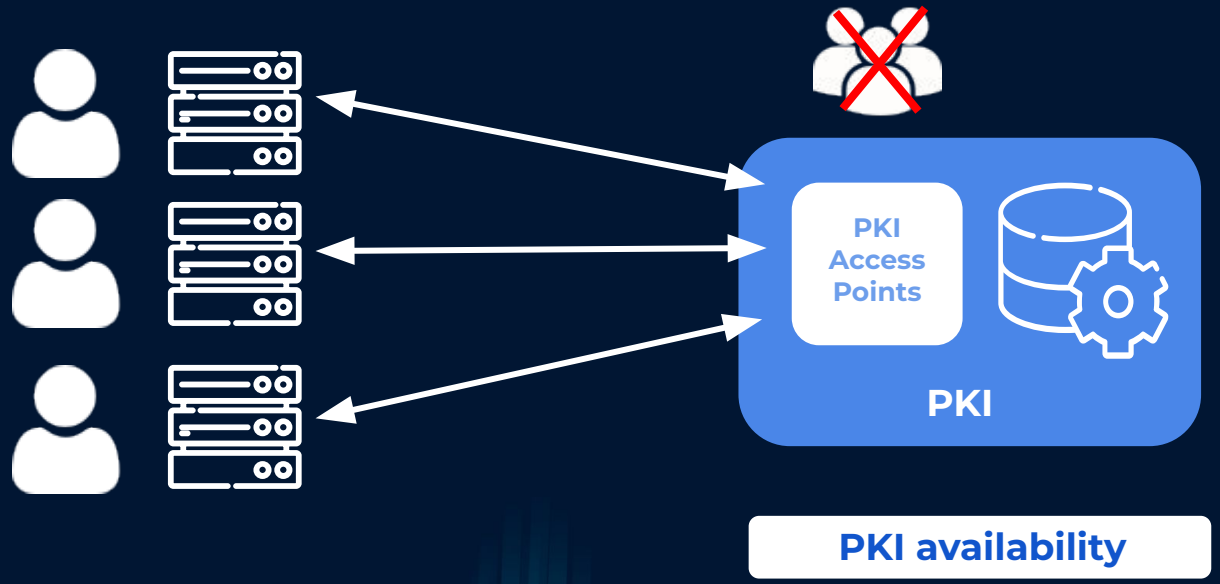
Request validation

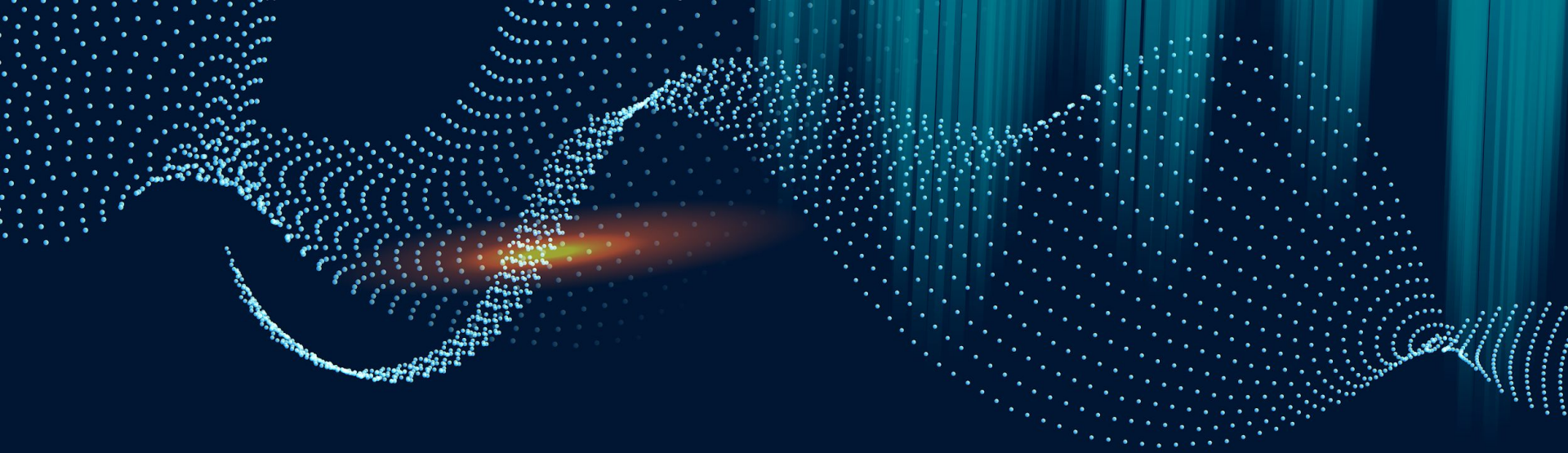
What We Need

What We Need



What We Need

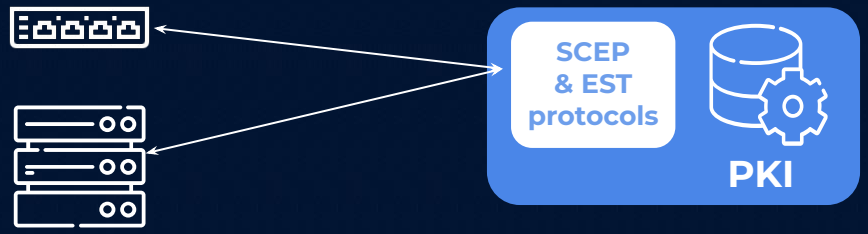




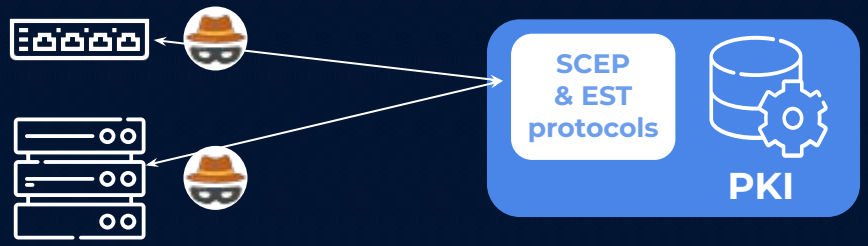
02 Building a solution

Automated protocols to obtain TLS server certificates

Existing solutions in private PKI ecosystem



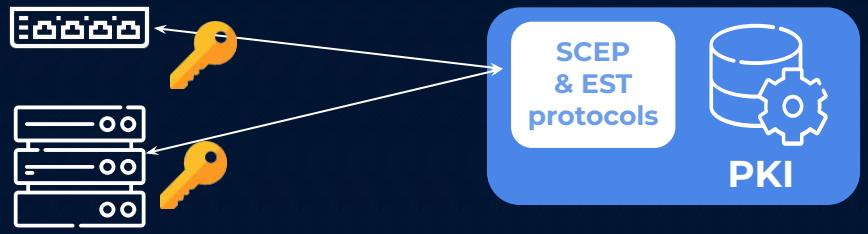
Existing solutions in private PKI ecosystem



But

- Security problems

Existing solutions in private PKI ecosystem



But

- Security problems
- Enrollment required

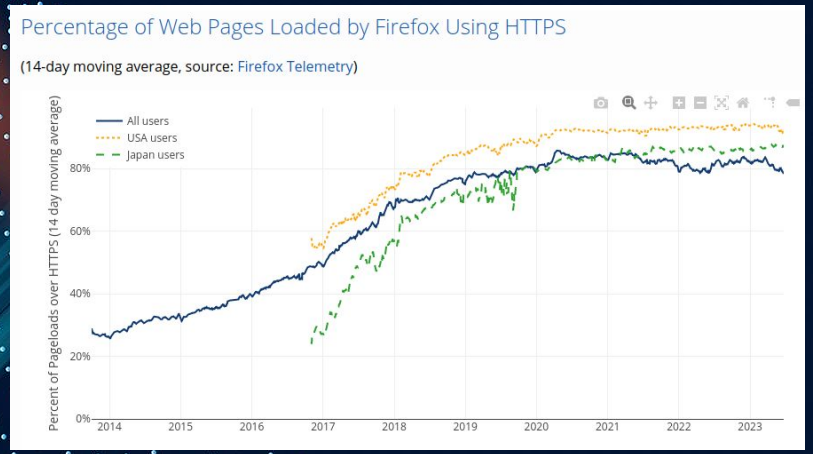
Existing solutions in private PKI ecosystem

But

- Security problems
- Enrollment required
- Clients

TLS server certificates issuance on the Internet?

Let's Encrypt



- Free & automated public CA
- Issues TLS server certificates
- Launched in 2015.

Impact on Web traffic:

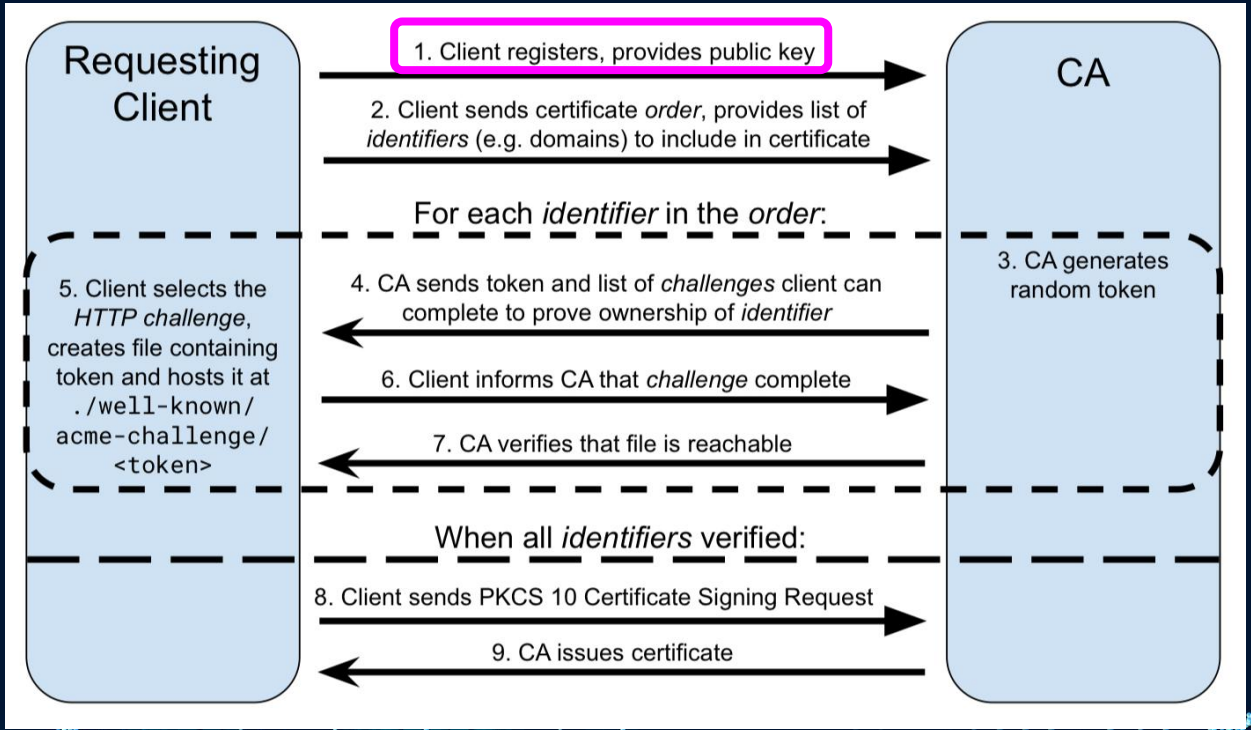
- 2014 **~ 27%** HTTPS
- 2023 **> 80%** HTTPS

→ Powered by the **ACME protocol**

How ACME has changed the Web?

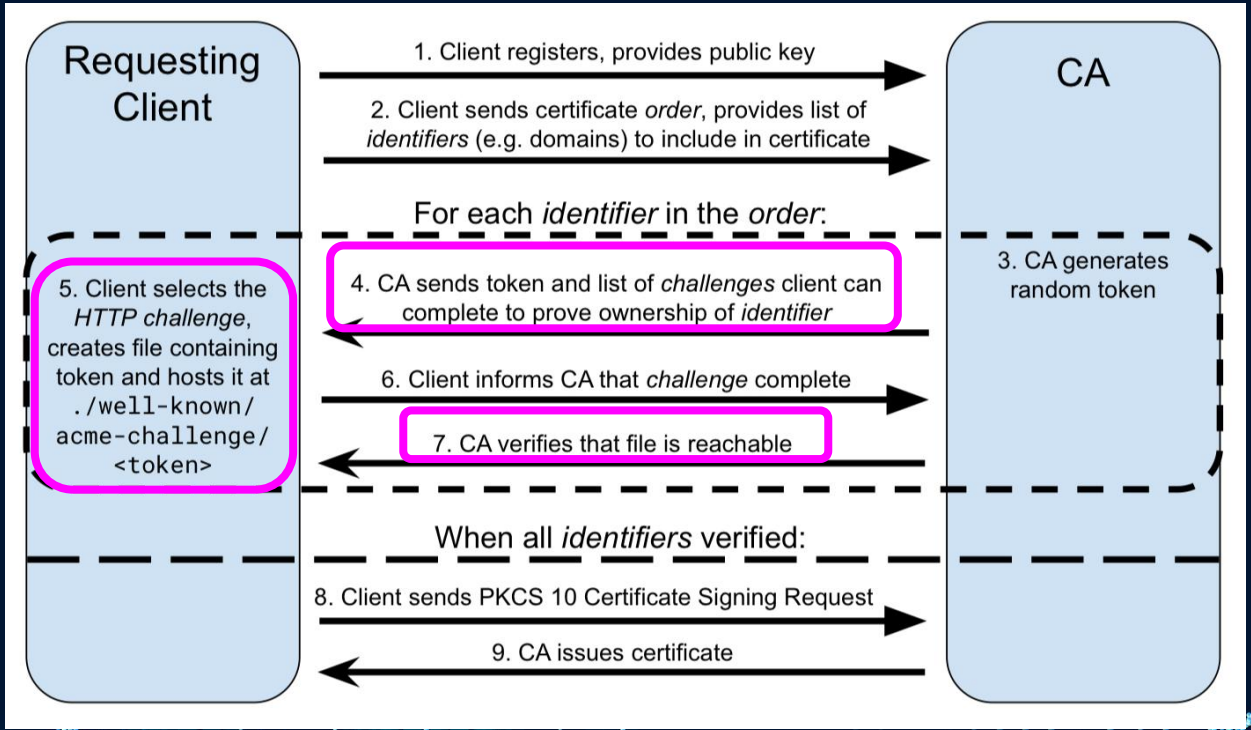
- **Fully automated protocol**
- **Open standard** (RFC 8555)
- **Secured protocol & robust implementation**

ACME : How does it work?



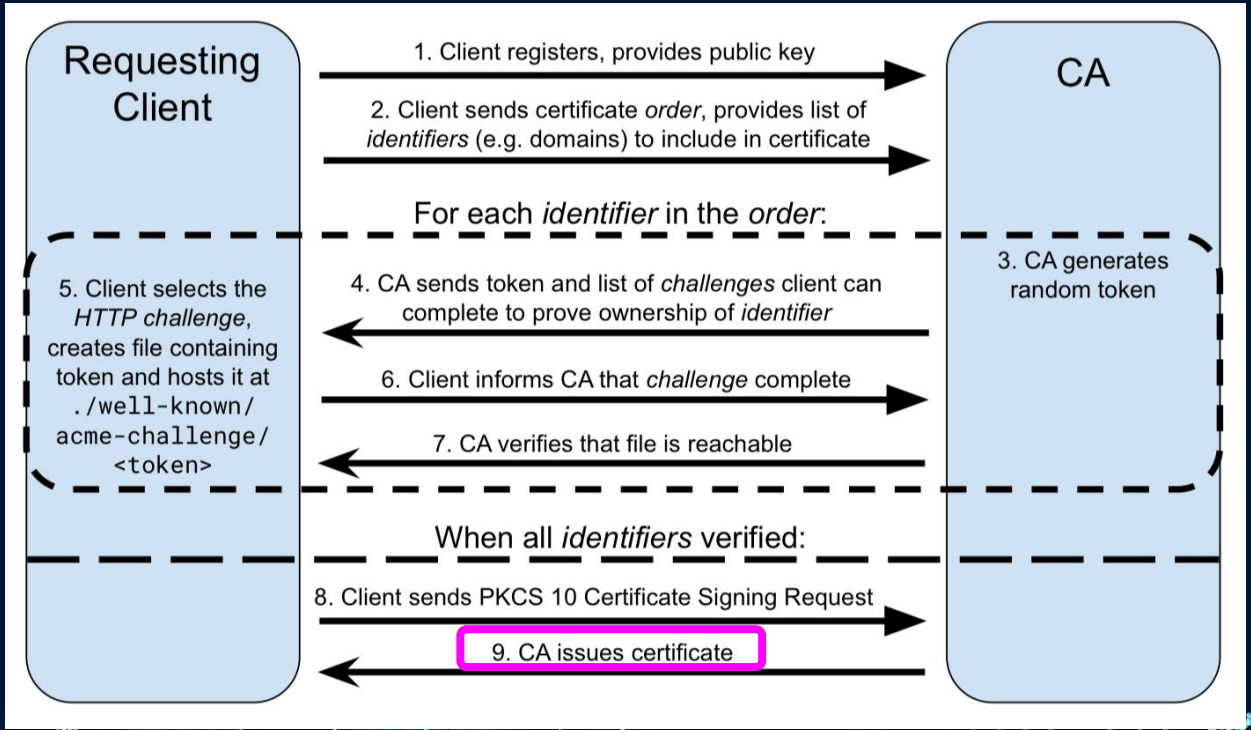
"Let's Encrypt: an automated certificate authority to encrypt the entire web." Aas et al. CCS'19. Figure 2. Src: https://par.nsf.gov/servlets/purl/10222849

ACME : How does it work?



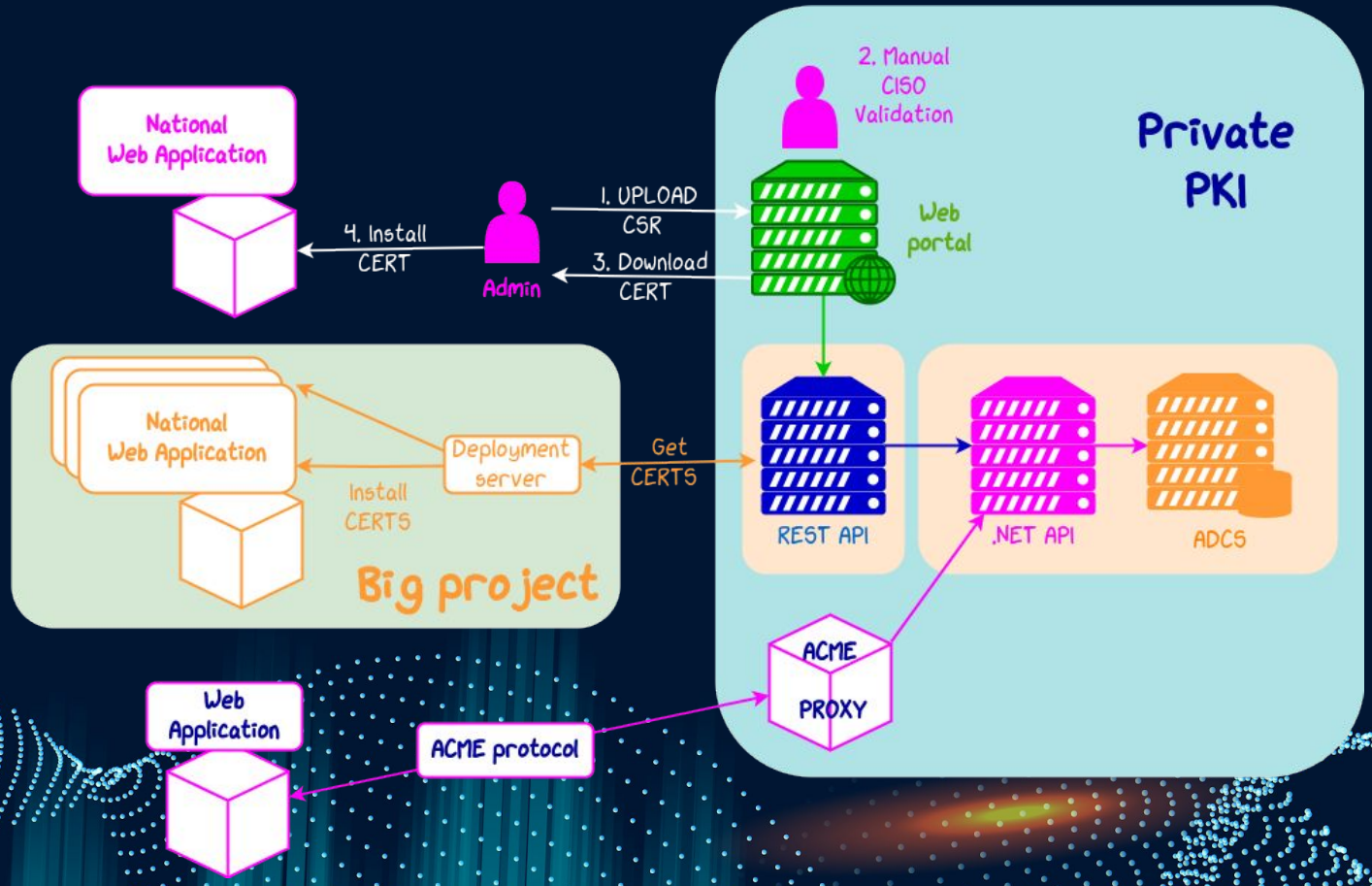
"Let's Encrypt: an automated certificate authority to encrypt the entire web." Aas et al. CCS'19. Figure 2. Src: https://par.nsf.gov/servlets/purl/10222849

ACME : How does it work?



"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

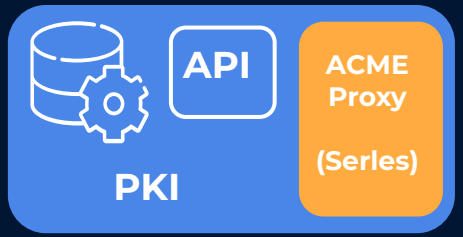
Private PKI: adding ACME



ACME adoption: what our team provides

ACME adoption: what our team provides

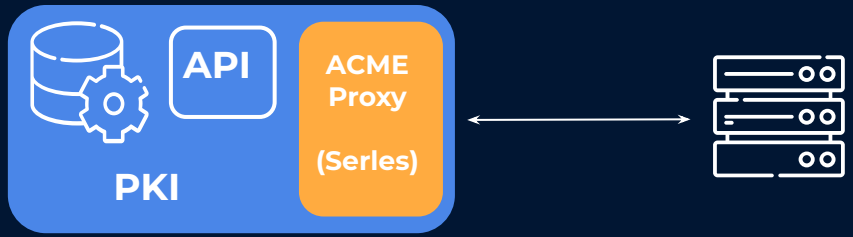
An **ACME proxy**, **open to all** on the private network
*(based on **Serles*:** an **open source ACME proxy**, written in Python)*



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

ACME adoption: what our team provides

An **ACME proxy**, **open to all** on the private network
*(based on **Serles*:** an **open source ACME proxy**, written in Python)*

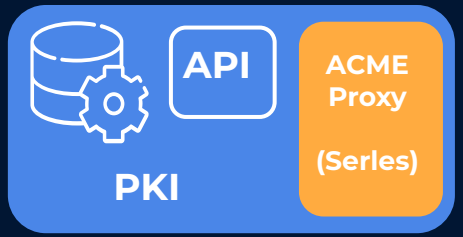


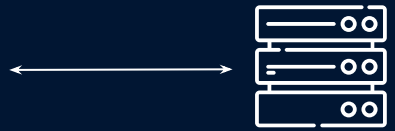
A reference **ACME client** for Linux and Windows
*(**lego**:** an **open source ACME client**, written in Go)*

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

ACME adoption: what our team provides

An **ACME proxy**, **open to all** on the private network
*(based on **Serles*:** an **open source ACME proxy**, written in Python)*





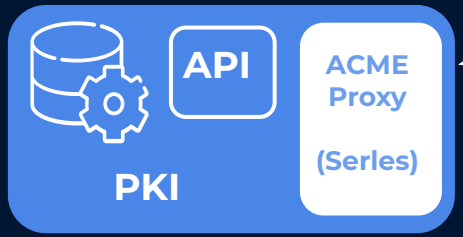
A reference **ACME client** for Linux and Windows
*(**lego**:** an **open source ACME client**, written in Go)*

Support & evangelism:

- Documentation website ;
- Webinars ;
- Support to admins for installation & first usage ;
- Support to architects/projects for specific ACME clients or use cases.

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

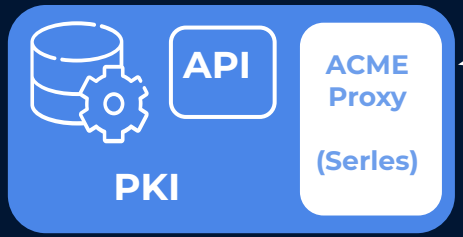
ACME adoption: what our users are also doing



Others ACME clients & platforms

(ex: acme.sh on AIX, network appliances ...)

ACME adoption: what our users are also doing

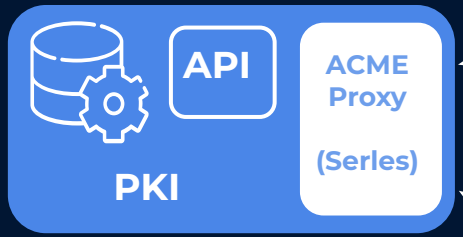


Others ACME clients & platforms

(ex: acme.sh on AIX, network appliances ...)

Middlewares (Caddy, Apache, Traefik...) with embedded ACME support

ACME adoption: what our users are also doing



Others ACME clients & platforms

(ex: acme.sh on AIX, network appliances ...)

Middlewares (Caddy, Apache, Traefik...) with embedded ACME support

Getting **"client+server auth" certificate** during VM/server creation (**Ansible ACME client**) in order to do mTLS more easily.

ACME new use case

In 2022, a new RFC draft: `draft-bweeks-acme-device-attest-01`(*)

- **Goal:** obtaining a *client* certificate for a device
- **Condition:** validating some of its properties (device identity, certificate key protected by a secure cryptoprocessor)
- New challenge: `device-attest-01`, based on attestation.

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

ACME new use case

In 2022, a new RFC draft: `draft-bweeks-acme-device-attest-01`(*)

- **Goal:** obtaining a *client* certificate for a device name
- **Condition:** validating some of its properties (device identity, certificate key protected by a secure cryptoprocessor)
- New challenge: `device-attest-01`, based on attestation.

Early stage

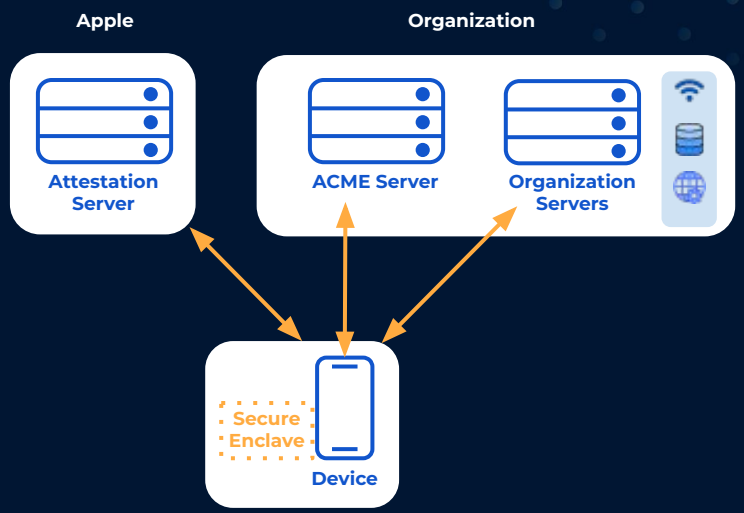
For the moment, the RFC draft **does not:**

- say **how to validate** the attestation
- nor **how to trust** the device identity

Tasks are very platform-dependant.

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

ACME new use case: how to get client certificate



First implementation (*): **Apple** in its **MDM solution** in 2022.

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

ACME in private networks

TAKE AWAY

Upgrade your internal PKI

- With peace of mind
  - IMPORTANT Secured domain validation
  - Automated protocol tested at scale

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

ACME in private networks

TAKE AWAY

Upgrade your internal PKI

- With peace of mind
  - IMPORTANT Secured domain validation
  - Automated protocol tested at scale
- For everybody
  - PKI open to all
  - IMPORTANT No enrollment
  - IMPORTANT No need to change your PKI

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

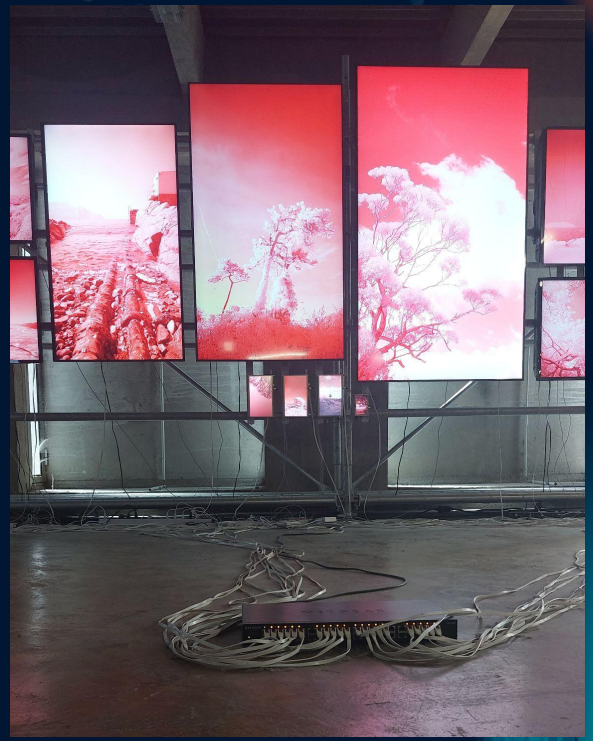
ACME in private networks

TAKE AWAY

Automation

FACT

- Legacy | 140 applications switch to TLS in 2 months



ACME in private networks

TAKE AWAY

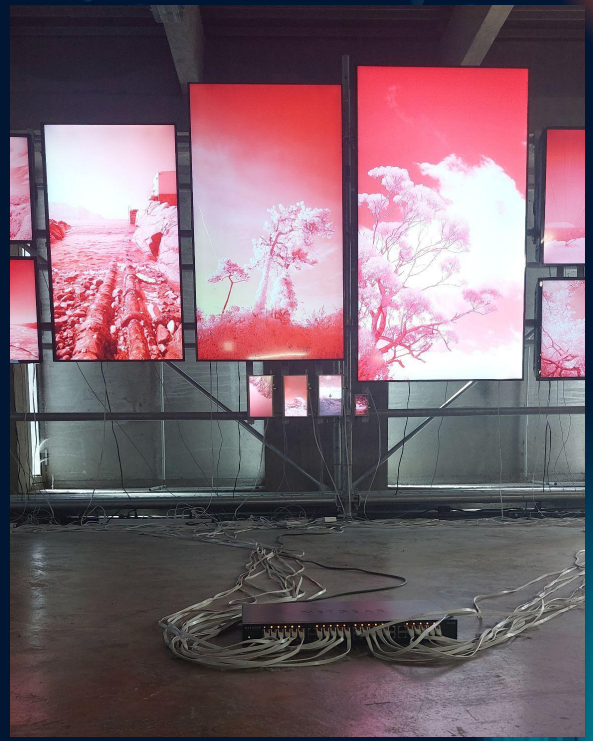
Automation

FACT

- Legacy | 140 applications switch to TLS in 2 months

- Devops | dedicated PKI no more needed
- Devops | Certificates first class citizen

- Security can be easy and efficient



ACME in private networks

TAKE AWAY

Autonomy

IMPORTANT

- Enforcing a protocol, not the tooling
- Diversity in ACME tools helps a lot to get very diverse users (devs, netops, admins ...)
- *"Already used on Internet"* factor

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

ACME in private networks

TAKE AWAY

Capitalize on new use cases

- During server provisioning
  - Ansible ACME playbook
  - Certificate with server+client authent key usage
  - → Server has mTLS capability from the start

FACT

- New use cases are coming (RFC for client cert & TPM)
- Other challenges (DNS) available

"Eat ACME, it is good for your IT!"

Thanks! Questions?

Contact:

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