Stop your local dev Without HTTPS !

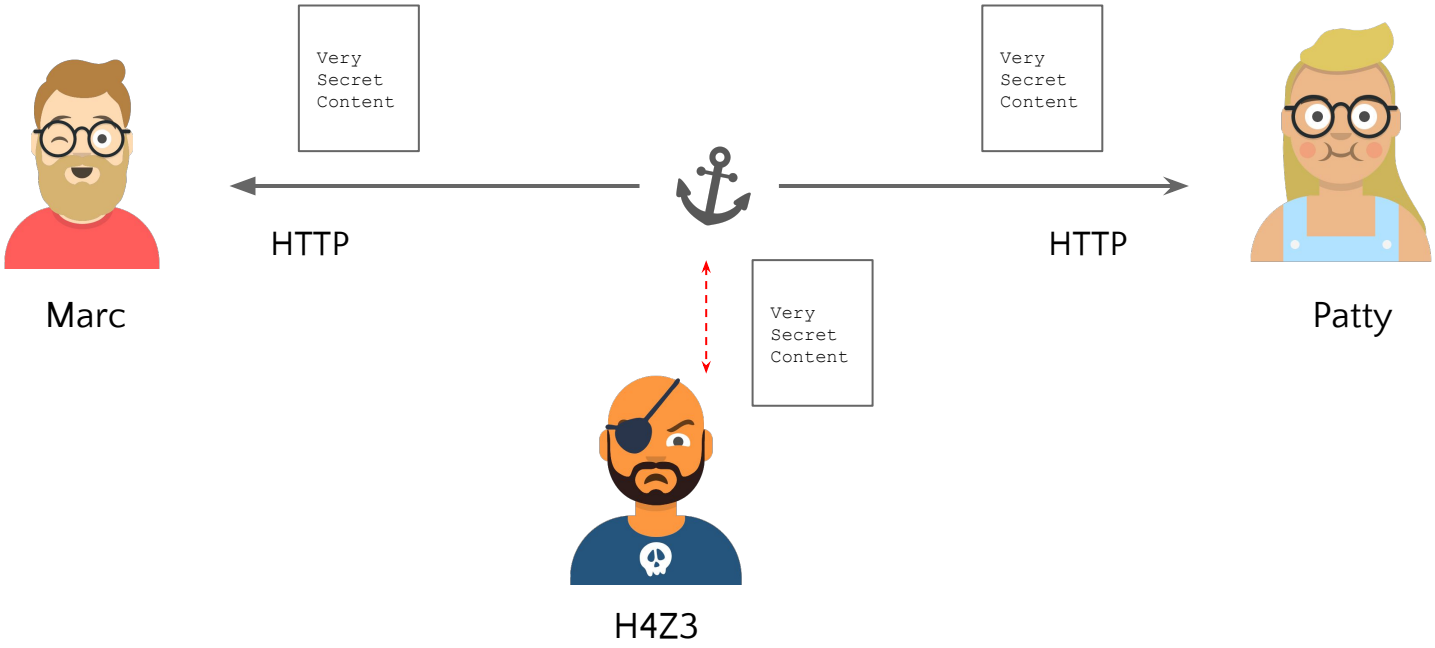
Understand and manage certificates

Julien Rollin – @TalanLabs – Ruche 22/10/2020

Why ?

“

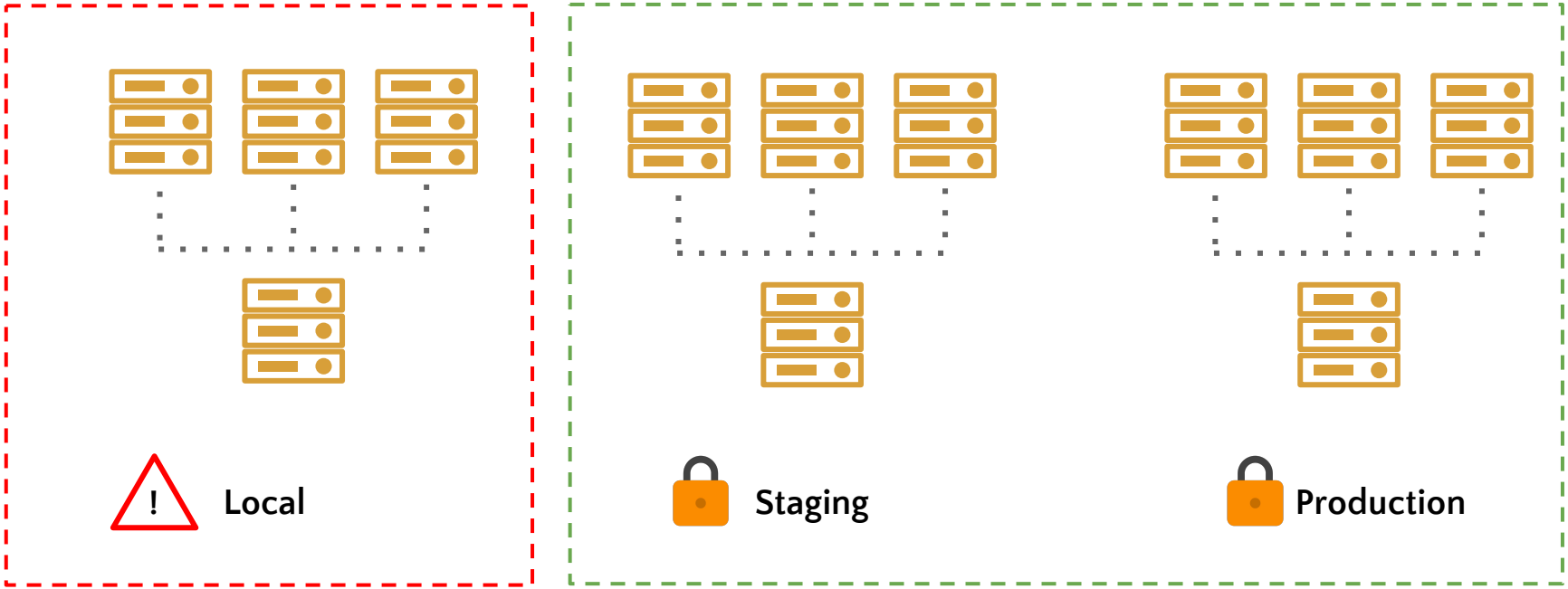
Man in the middle



Google (and others)

- SEO ranking factor
- HTTPS required for Progressive Web App
- Required for proper Secured Auth Flow

Application Secured by design ?



HTTPS everywhere !

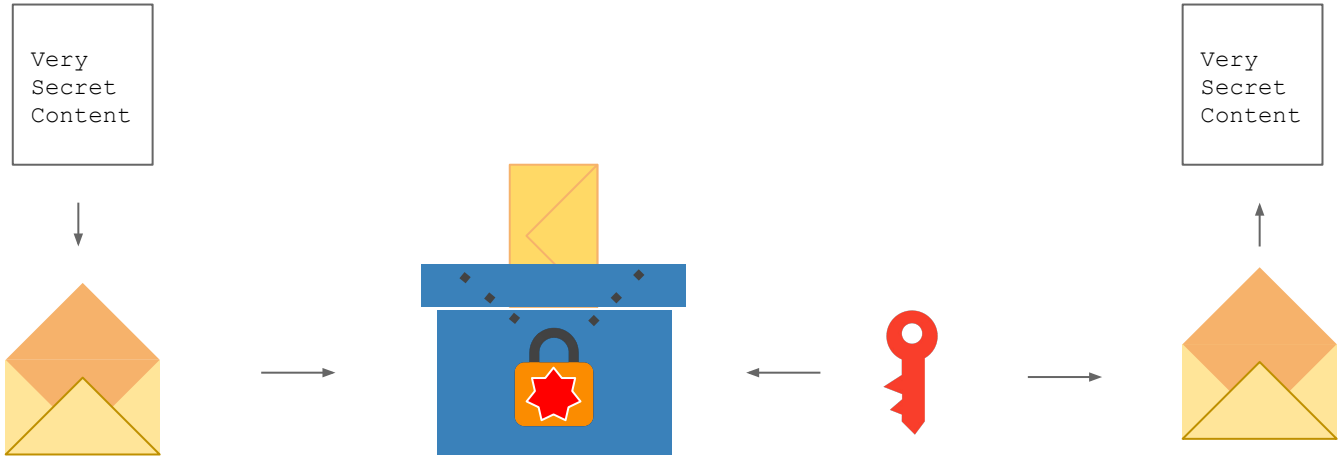
“

HTTPS Key points

- Ensure Data encryption
- Ensure Data integrity
- Ensure Authentification

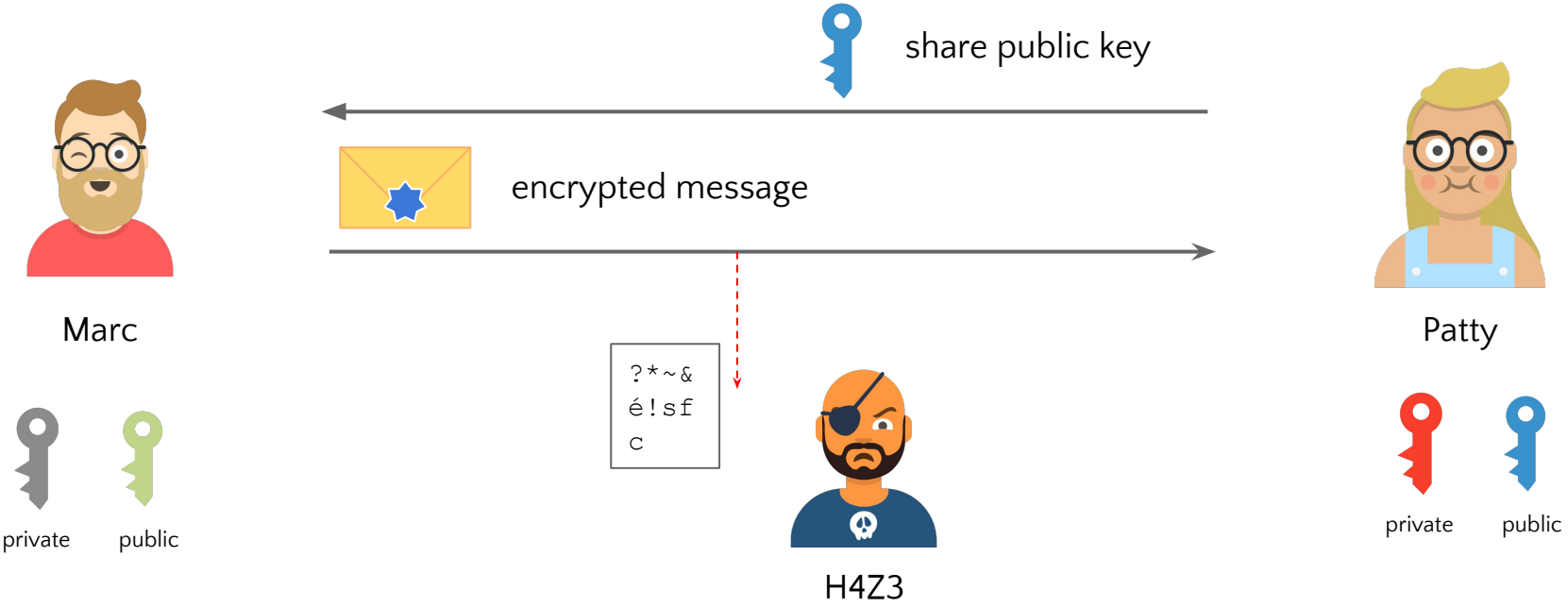
Asymetric key encryption

- Key Pair : Private + public
- Public key can be shared with anybody
- Private key must not be shared
- Only Private key can decrypt data encrypted

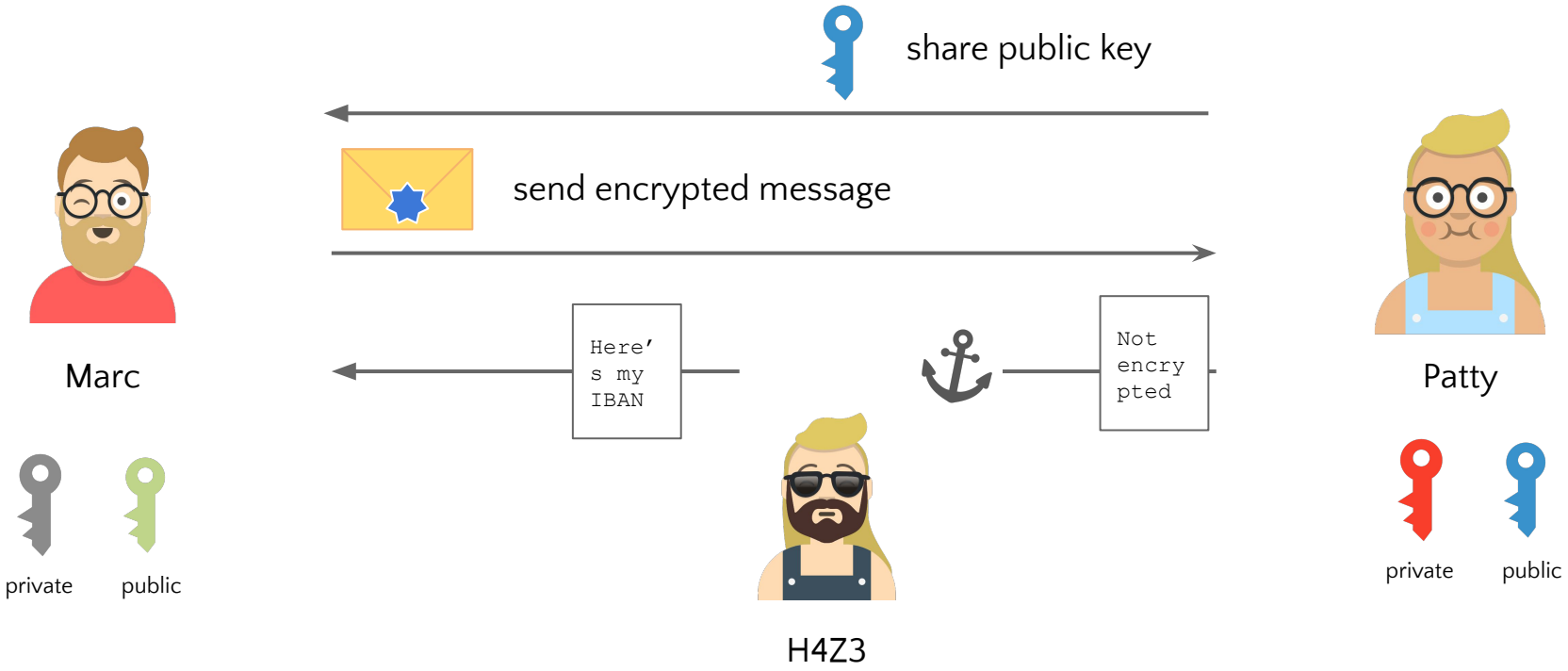


Private / public key

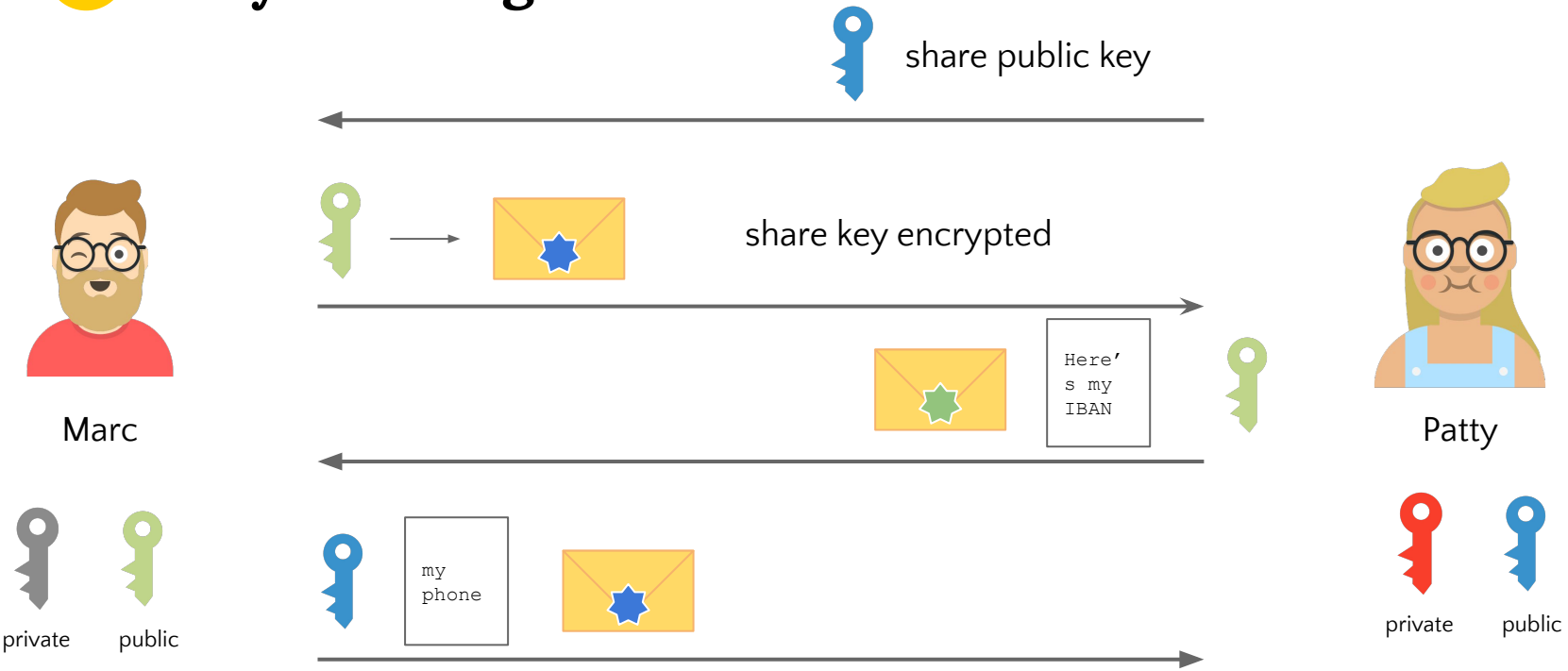
Encrypt message sent to Patty

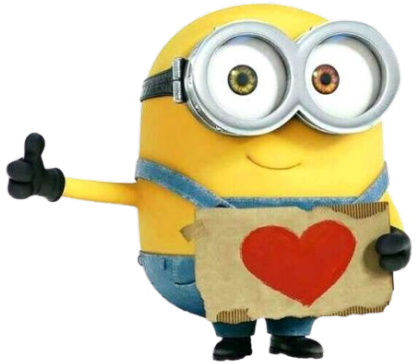


Man in the middle is still possible



Key exchange



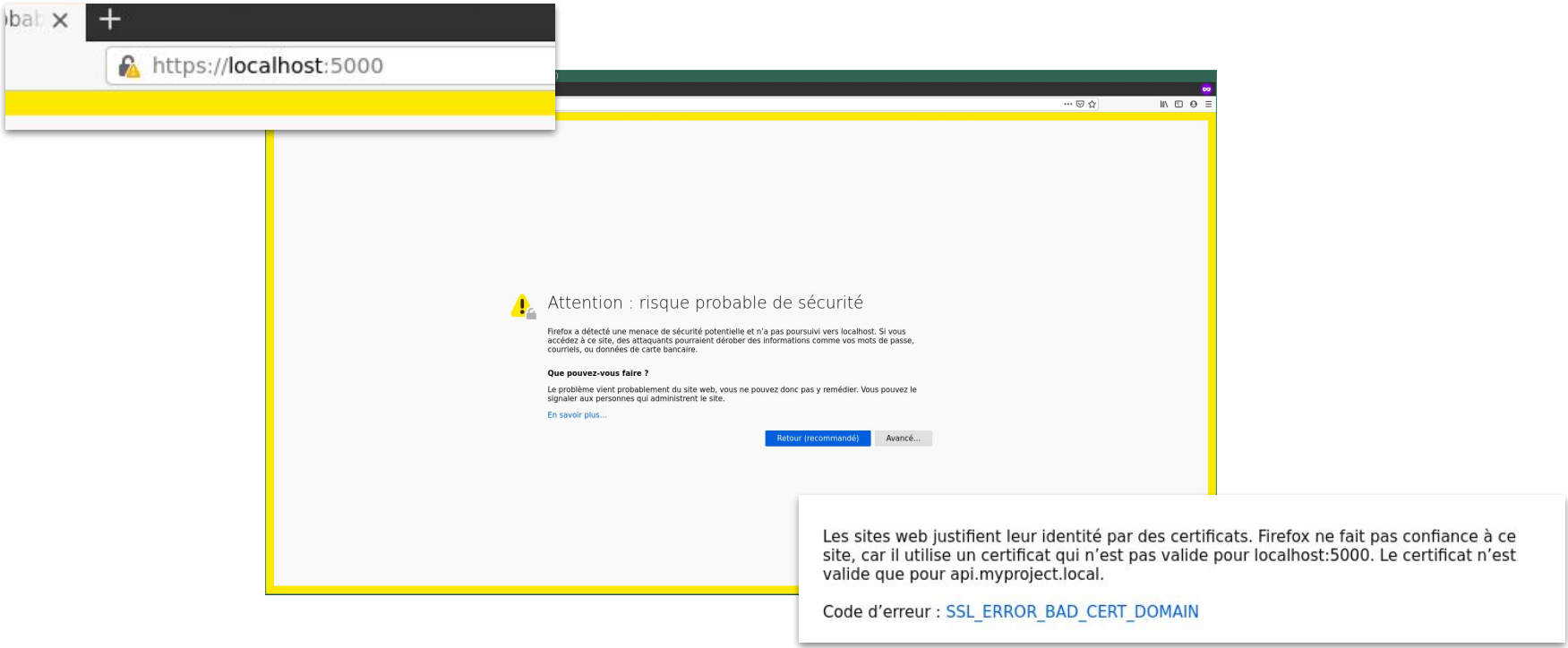


We can share our little secrets !

“

Workflow on local

- Generate certificate SSL
- Configure Server with certificate infos
- Run Server !

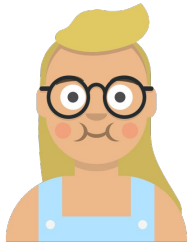

https://localhost:5000
Attention : risque probable de sécurité
Firefox a détecté une menace de sécurité potentielle et n'a pas poursuivi vers localhost. Si vous accédez à ce site, des attaquants pourraient dérober des informations comme vos mots de passe, courriels, ou données de carte bancaire.
Que pouvez-vous faire ?
Le problème vient probablement du site web, vous ne pouvez donc pas y remédier. Vous pouvez le signaler aux personnes qui administrent le site.
En savoir plus...
Retour (recommandé)
Avancé...
Les sites web justifient leur identité par des certificats. Firefox ne fait pas confiance à ce site, car il utilise un certificat qui n'est pas valide pour localhost:5000. Le certificat n'est valide que pour api.myproject.local.
Code d'erreur : SSL_ERROR_BAD_CERT_DOMAIN

What ??

How to trust Key ownership ?

Marc

Patty public key



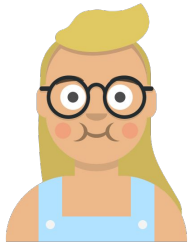
Patty

Replace Patty public key

Patty (H4Z3)

Encrypted communication with hacker key !

How to trust Key ownership ?



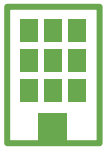
Patty

Patty public key

Marc

check Pub Key and Certificate

Yes, you can trust Pub key !

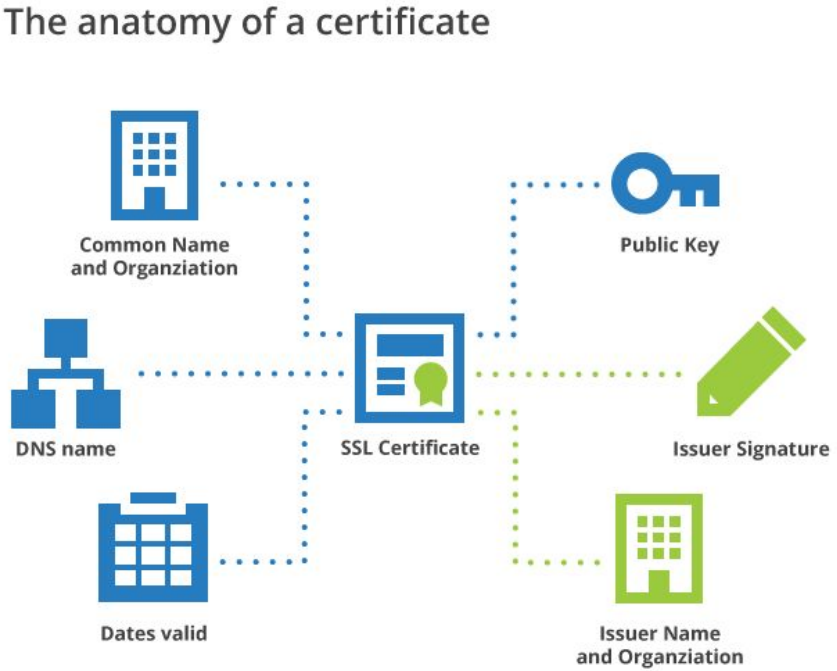


Certificate Authority
Trusted Store

Patty
(H4Z3)

Certificate is like a passport

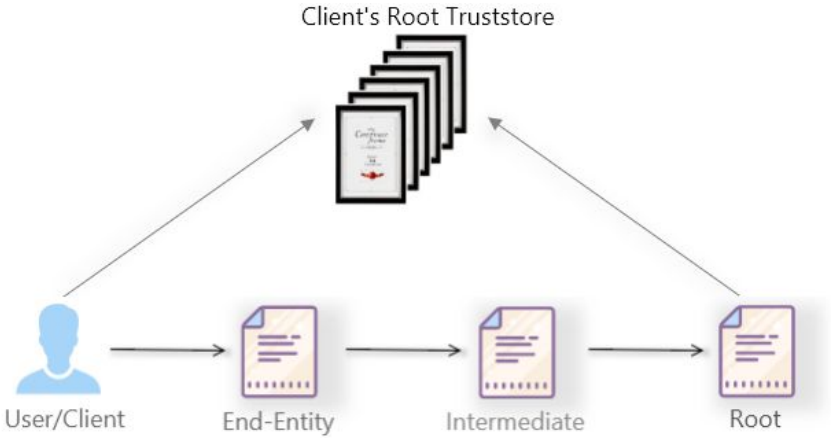
- Ensure ownership with Trust authority
- standard X.509
  - Name of the entity that owns the public key
  - Name of the entity that issued the certificate
  - Time period of validity
  - public key
  - hostname(s)
  - digital signature (with private key)

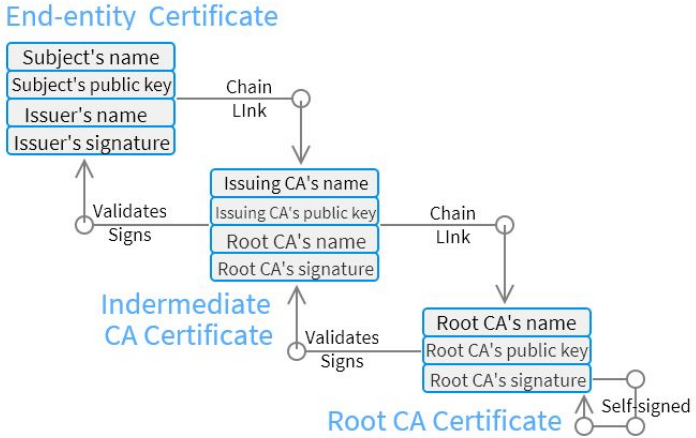


Schema from Cloudflare

Intermediate CA and CA chain of trust

- Root certificate: The Trust Anchor
  - keept offline
- Intermediate certificate: The Issuing CA
  - online
- Server Certificate: The End-Entity
  - on the application server





Certificate chain of trust (schema from keyfactor)

To summup

“

Steps

- Generate private key for your domain
- Generate Certificate Signing Request
- Create Root Certificate Authority
- Sign you domain certificate with CA
- Add Root Certificate to your Trust Store
- Configure your app
- Run it !

Demo Time !

“

Thanks !

“

Credits

- Minions : oeuvre de Sergio Pablos
- Les Minions (Minions) est un film d'animation américain réalisé par Kyle Balda et Pierre Coffin, sorti en 2015.
- Images from google images...