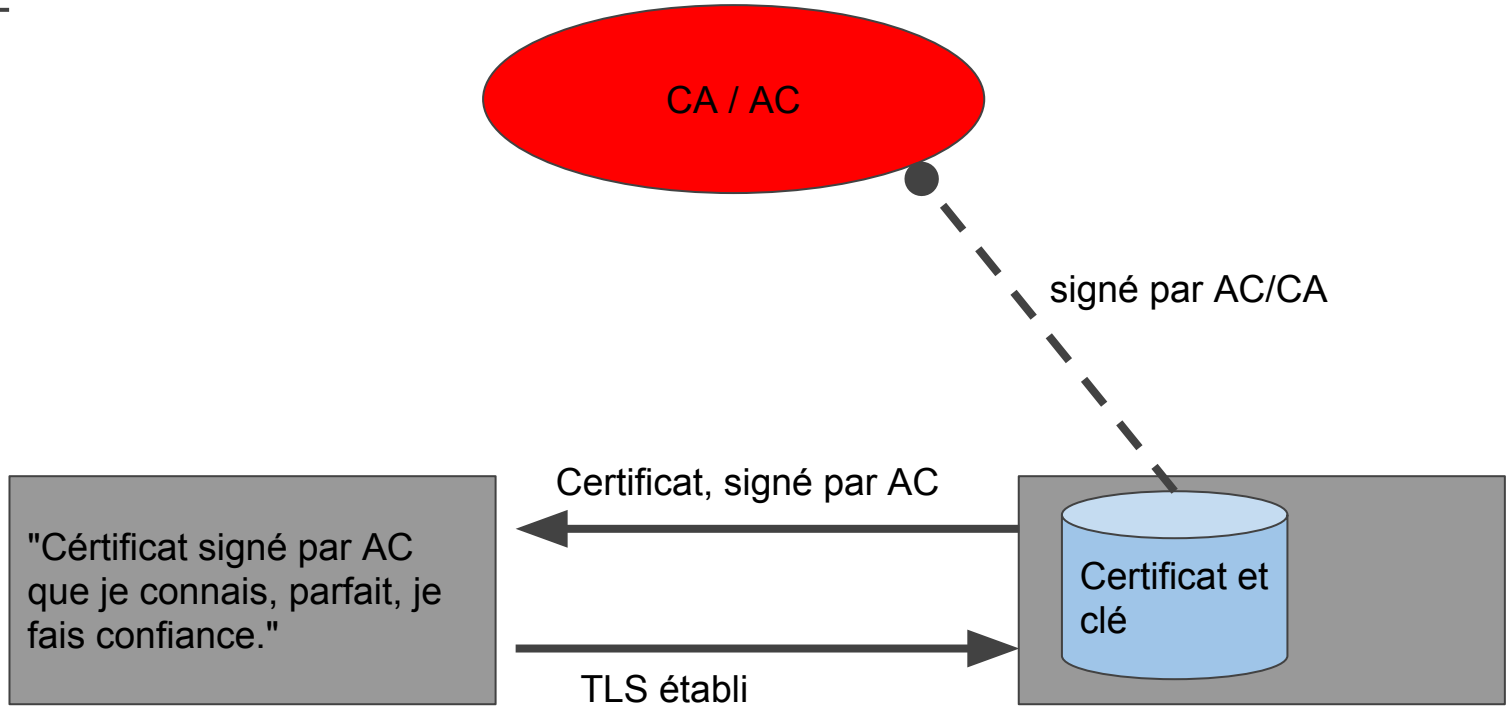
DANE

Pascal Gienger

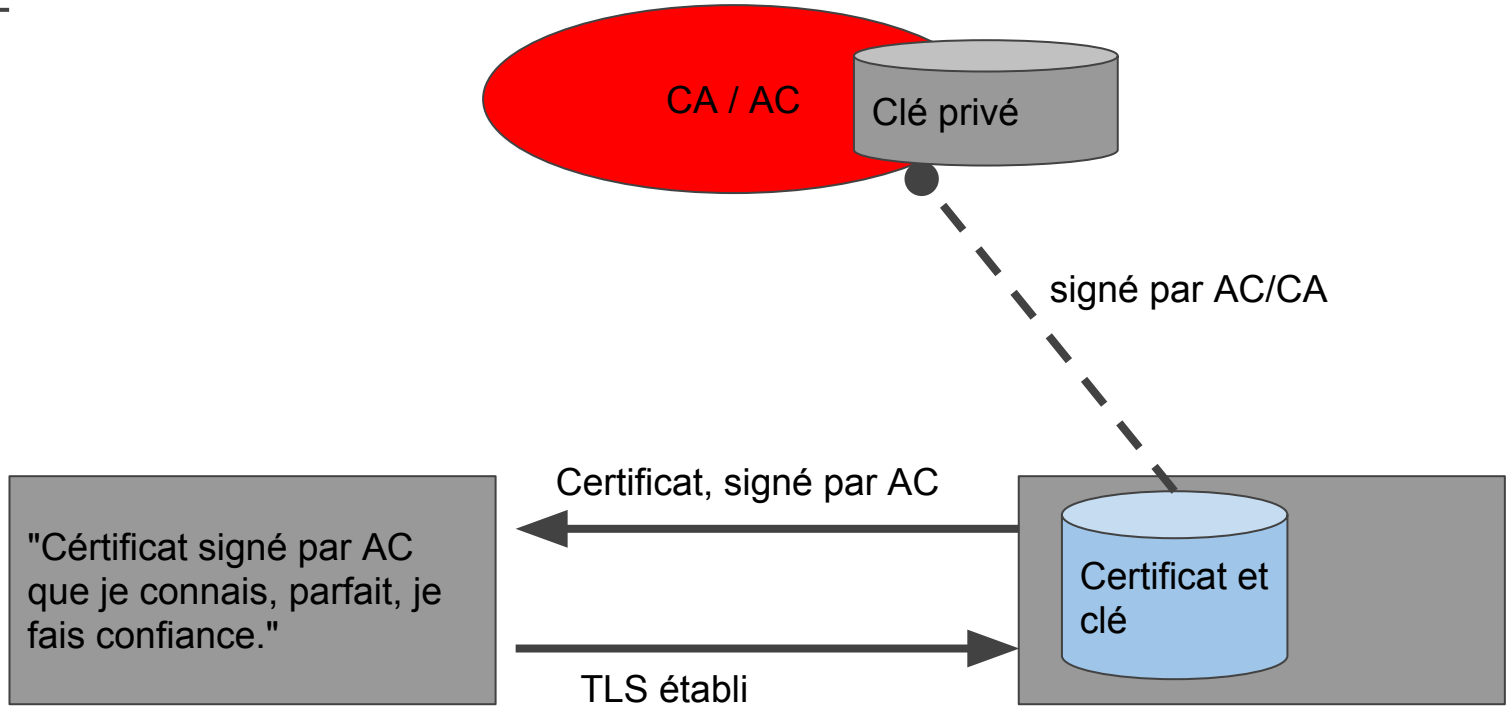
- Utilise et débogue TCP/IP depuis 1998
- Est basé en Suisse actuellement
- Gagne sa vie momentanément chez Google comme Site Reliability Engineer (Ingénieur de réliabilite/redondance)

La vie sans ou avec une AC (CA) - sécurisé par DNSSEC.

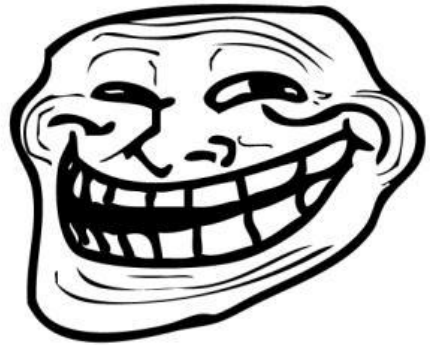
Problème

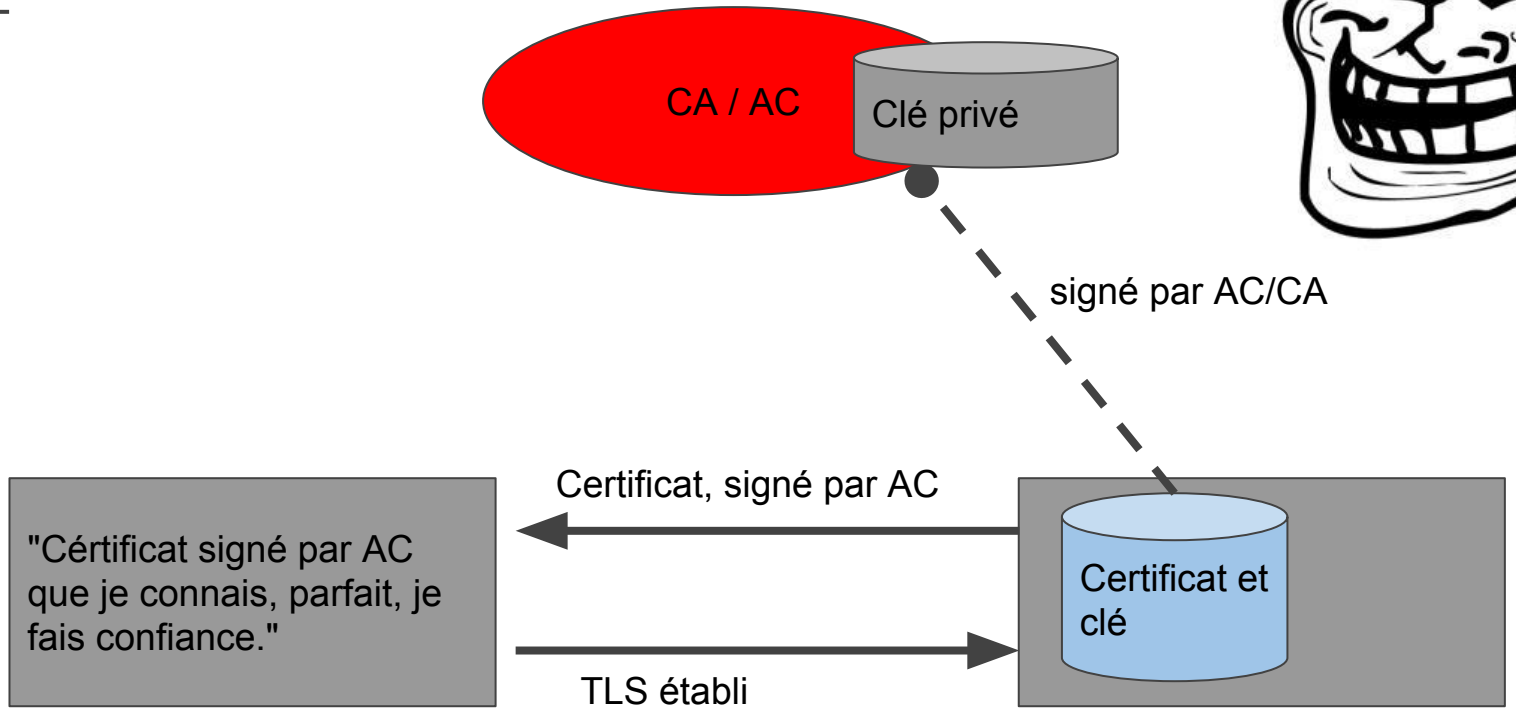

CA / AC
signé par AC/CA
Certificat, signé par AC
"Cértificat signé par AC que je connais, parfait, je fais confiance."
Certificat et clé
TLS établi

Problème

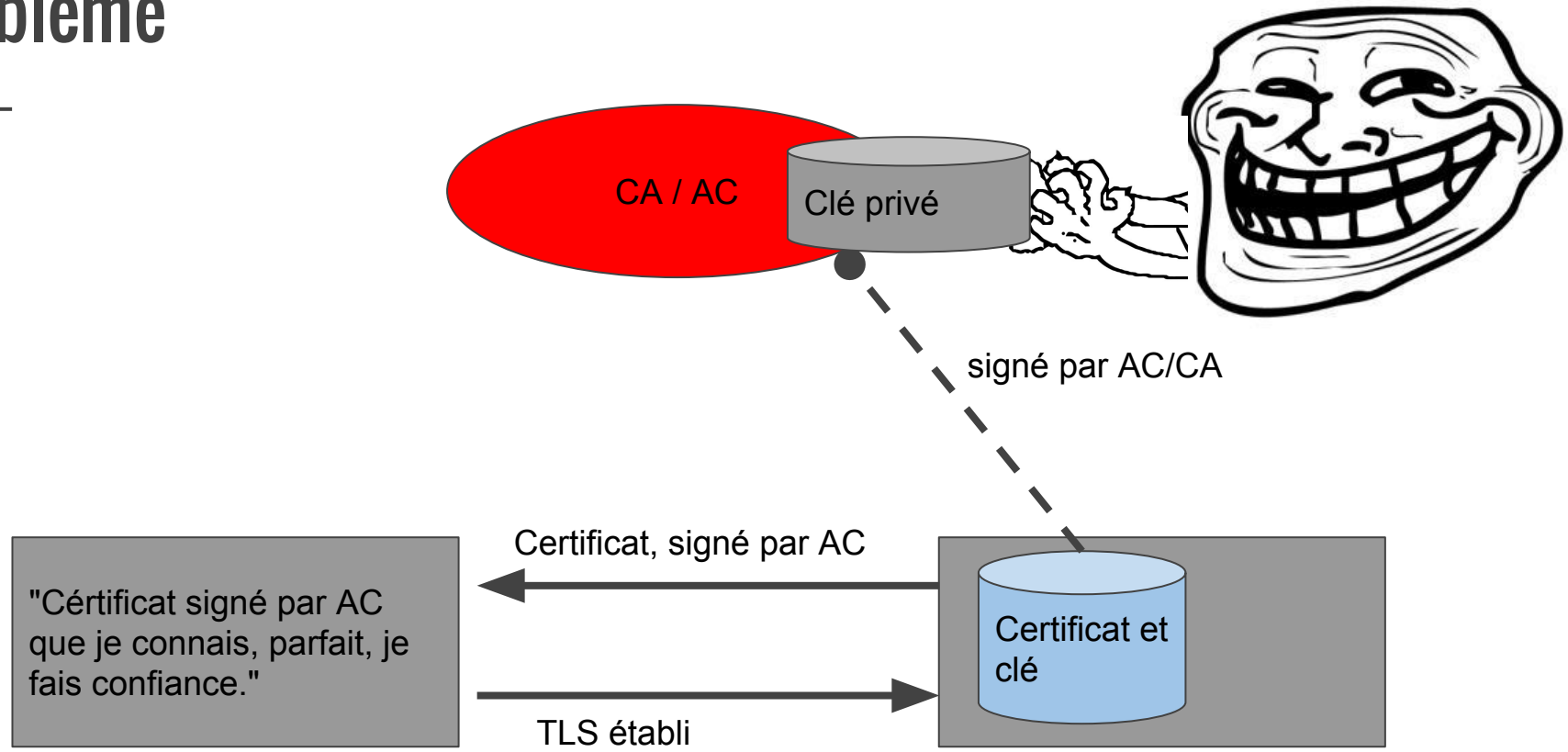

CA / AC
Clé privé
signé par AC/CA
Certificat, signé par AC
"Cértificat signé par AC que je connais, parfait, je fais confiance."
Certificat et clé
TLS établi

Problème

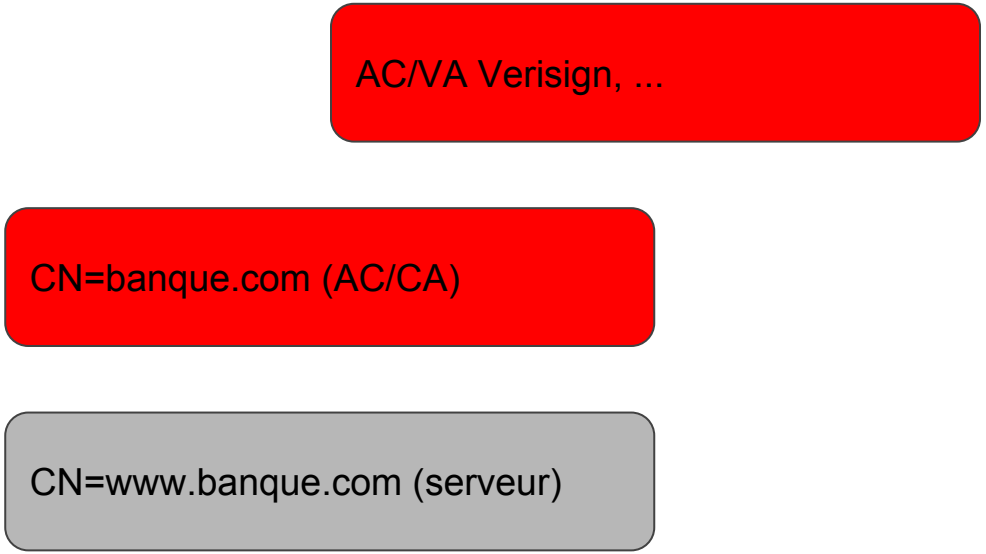



CA / AC
Clé privé
signé par AC/CA
Certificat, signé par AC
"Cértificat signé par AC que je connais, parfait, je fais confiance."
Certificat et clé
TLS établi

Problème

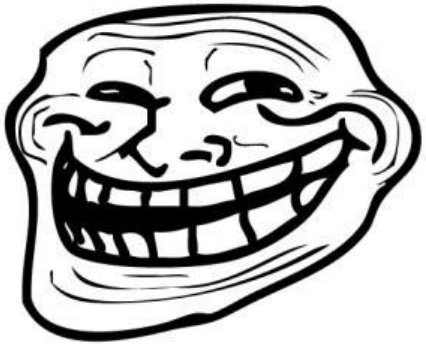

CA / AC
Clé privé
signé par AC/CA
Certificat, signé par AC
"Cértificat signé par AC que je connais, parfait, je fais confiance."
Certificat et clé
TLS établi

Problème



Problème

AC/VA Verisign, ...



CN=banque.com (AC/CA)

CN=*.banque.com (AC/CA)

CN=www.banque.com (serveur)

CN=www.banque.com (le faux)

DANE: Utiliser DNS pour des informations sur l'AC/Cert.

- Associer un certificat à un nom de domaine/entrée DNS
- Définir des contraintes sur la validité pour cette domaine/ce nom
- Possibilité d'utiliser un certificat signé par soi-même où par sa propre AC sans devoir être dépendent d'une AC commerciale
- Révoquer un certificat immédiatement pour un service/un site sans devoir relier à la propagation d'un CRL
- RFC 6698

Un nouveau enregistrement de ressource (RR): TLSA

Exemple:

```
pascal@bouake:~$ pascal@bouake:~$ dig +dnssec +answer +multi _443._tcp.www.ietf.org. TLSA
;; QUESTION SECTION:
;_443._tcp.www.ietf.org. IN TLSA
;; ANSWER SECTION:
_443._tcp.www.ietf.org.  1800 IN   TLSA 3 1 1 (
                    0C72AC70B745AC19998811B131D662C9AC69DBDBE7CB
                    23E5B514B56664C5D3D6 )
_443._tcp.www.ietf.org.  1800 IN   RRSIG TLSA 5 5 1800 (
                    20170921193329 20160921183346 40452 ietf.org.
                    EyVLWNdS8IEH8teaHiEjcPiTRcBlMGhAgCPZ0T9d9Vxv
                    mbHIcNU9FbzqqKM7xsINwST5fUASloneiJm904IwXybj
                    s+ZRVycIYruiAMz8q+ri4xzBQG1ds [...])
```

Un nouveau enregistrement de ressource (RR): TLSA

```
_443._tcp.www.ietf.org.  1800 IN   TLSA 3 1 1 (
                  0C72AC70B745AC19998811B131D662C9AC69DBDBE7CB
                  23E5B514B56664C5D3D6 )
```

Type de l'association:

0 - AC ou fingerprint du cert de l'AC acceptés. **PKIX!**
1 - Certificat ou fingerprint du certificat accepté. **PKIX!**
2 - Trust Anchor: Un cert signé par une AC pas connu/tiers. **PKIX!**
3 - Certificat ou fingerprint du certificat accepté. ~~PKIX~~

Un nouveau enregistrement de ressource (RR): TLSA

```
_443._tcp.www.ietf.org.  1800 IN   TLSA 3 1 1 (
                  0C72AC70B745AC19998811B131D662C9AC69DBDBE7CB
                  23E5B514B56664C5D3D6 )
```

Le sélecteur:

0 - Les données sont comparés avec le certificat complet
1 - Les données sont comparés avec la clé publique (Subject Public Key Info, sans données supplémentaire comme DC, CN, …).

Un nouveau enregistrement de ressource (RR): TLSA

```
_443._tcp.www.ietf.org.  1800 IN   TLSA 3 1 1 (
                  0C72AC70B745AC19998811B131D662C9AC69DBDBE7CB
                  23E5B514B56664C5D3D6 )
```

Le "matching type", à quoi la ressource va être comparé:

0 - les données complètes (le certificat complet ou le Subject Public Key Info, dépendant de la valeur avant)
1 - un hash SHA-256
2 - un hash SHA-512

Ici, les données dans le RR sont un hash SHA-256.

Et le courriel?

- Les serveurs de courriel sont chez le fournisseur, alors capable de pouvoir utiliser DNSSEC de manière propre.
- `_25._tcp.monmx.chezmoi.org. chezmoi.org.  IN MX 10 monmx.chezmoi.org.`
- **La présence d'un record TLSA rends le contact vers le serveur SMTP obligatoire.**
- Si le certificat présenté ne correspond pas au TLSA, la communication doit être annulé.
- RFC 7672

Exemple

```
example.com.                  IN MX 0 mx1.example.com.
example.com.                  IN MX 0 mx2.example.com.
_25._tcp.mx1.example.com.     IN CNAME tlsa201._dane.example.com.
_25._tcp.mx2.example.com.     IN CNAME tlsa201._dane.example.com.
tlsa201._dane.example.com.    IN TLSA 2 0 1 e3b0c44298fc1c149a…
```

(extrait du RFC 7672).