From centralized certification systems to more internet-like ones

Alexandre Kervadec[1]

[1] Master 2 Informatique RSM

29 janvier 2016

université de BORDEAUX
Collège Sciences et technologies

Sommaire

1 Les systèmes en place
- X.509 et CAs
- PGP
- SKIP

2 Les systèmes en cours de développement
- DANE
- Sovereign keys
- CATA

université de BORDEAUX
Collège Sciences et technologies

Les systèmes en place

Certificats X.509 et CAs (Certification Authority)

PGP (Pretty Good Privacy)

SKIP (Simple Key management for Internet Protocols)

X.509 et CAs

On distingue 3 différentes entités :

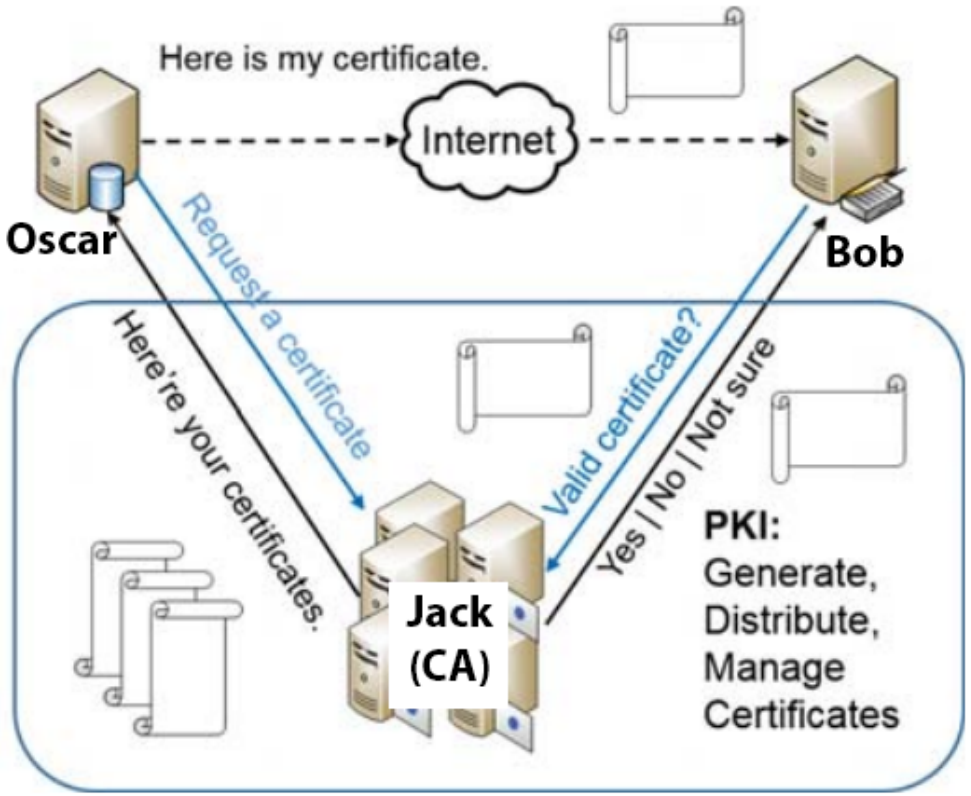
Certification Authority [1] : entité qui contrôle l'authentification et la gestion des certificats digitaux

Subscriber : l'entité qui envoie des données au **CA** pour les ajouter à son certificat. C'est l'entité en qui l'**user** veut avoir confiance

User : demande des information au **CA** sur la validité du certificat que lui a envoyé un **subscriber**

1. CA

X.509 et CAs


Here is my certificate.
Internet
Oscar
Bob
Request a certificate
Here're your certificates.
Valid certificate?
Yes | No | Not sure
Jack
(CA)
PKI:
Generate,
Distribute,
Manage
Certificates

PGP

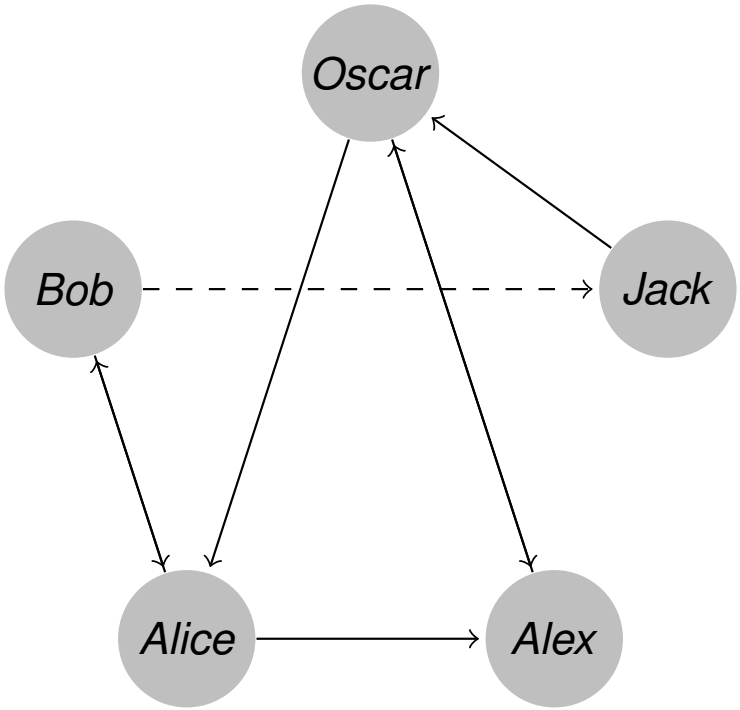


FIGURE – Communities of trust : Jack introduces Oscar to Bob's public-key certificate before Bob receives it.

PGP

PGP inclut un certificat à clefs publiques et une chaîne de confiance(un **introducer**).

Les niveaux de confiance pour un certificat sont :

- Undefined : on ne peut pas dire si la cle publique est valide ou pas
- Marginal : la clef publique **peut** être valide, mais on ne peut pas en être sûr
- Complete : on est sûr que la clef publique est valide

PGP

Les niveaux de confiance pour une chaîne de confiance (**introducer**) sont :

Full : on peut faire totalement confiance à la clef publique pour introduire une nouvelle clef publique

Marginal : la clef publique **peut** introduire une nouvelle clef publique, mais on ne peut pas en être sûr

Untrustworthy : on ne doit pas faire confiance à cette clef publique pour en introduire une nouvelle

SKIP

SKIP (Simple Key-Management for Internet Protocol) implémente une chaîne d'authentificateurs de noeuds, où chaque noeud stocke ses informations dans une sorte de **directory service** [2].

Etant donné que SKIP ne supporte pas la translation d'adresse (NAT par exemple), ce système est inutile.

2. annuaire

Les systèmes en cours de développement

DANE (DNS-Based Authentication of Named Entities)

Sovereign keys Les clefs souveraines par l'EFF [3]

CATA (Certificate Authority Transparency and Auditability)

3. Electric Frontier Foundation

DANE

Ce système est arrivé avec une simple question : *Pourquoi utiliser une nouvelle infrastructure de confiance alors que nous utilisons déjà DNS pour résoudre les noms de domaine ?*

DANE utilise un nouveau champ dans la requête DNS [4] : le champ **TLSA**.

```
_443._tcp.www.example.com. IN TLSA (
 0 0 1 d2abde240d7cd3ee6b4b28c54df0&34b9
   7983a1d16e8a410e4561cb106618e971 )
```

4. Sécurisé avec DNSEC

DANE

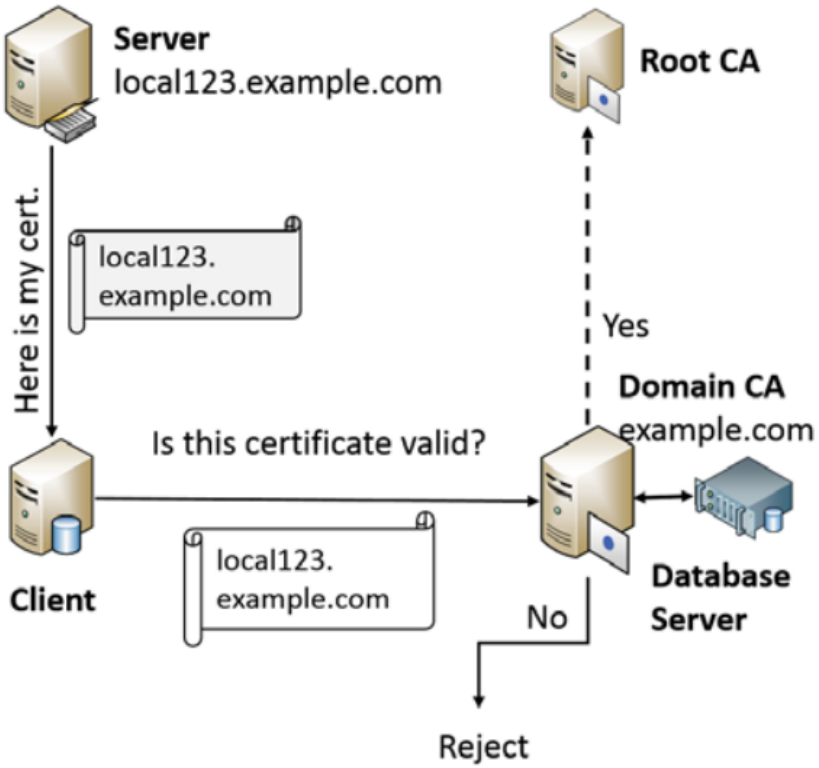


FIGURE – Fonctionnement de DANE

Sovereign keys

Le système de clefs souveraines s'appuie sur des **timeline servers**, qui seront en nombre restreint [5], gérant une liste publique dans laquelle on ne peut que faire des ajouts.
Des clefs souveraines sont un couple de clefs cryptographiques où la clef publique est associée à un nom de domaine. Cette association est enregistrée dans les **timeline servers** cités précédemment.

Cycle de vie des clefs souverraines :

1. Génération de la pair de clefs
2. Preuve de contrôle du domaine concerné (en utilisant PKI ou DANE)
3. Ajout de la clef publique associée au nom de domaine dans les timeline servers

5. Environ une vingtaine tout au plus

CATA

Ce système se résume en une liste publique de certificats. Ainsi, chaque administrateur peut vérifier qu'il n'y a pas de fraude.
Ceci dit, beaucoup de questions restent à résoudre :

- Qui doit gérer ces listes ?
- Combien de listes doivent être créées ?
- Comment la révocation doit fonctionner ?
- Qu'arrive-t-il si un certificat n'est plus disponible ?

Questions

Avez-vous des questions ?