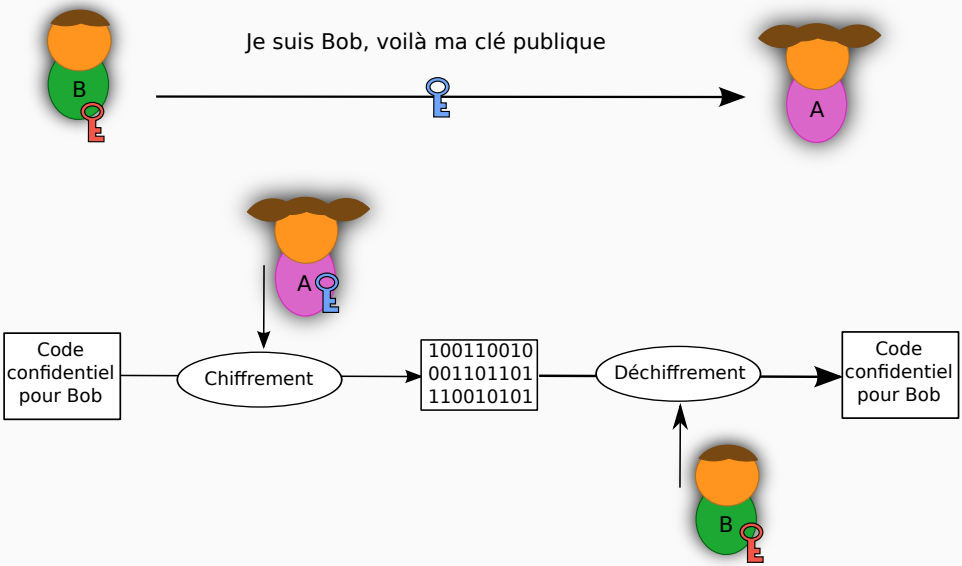
Les certificats X509

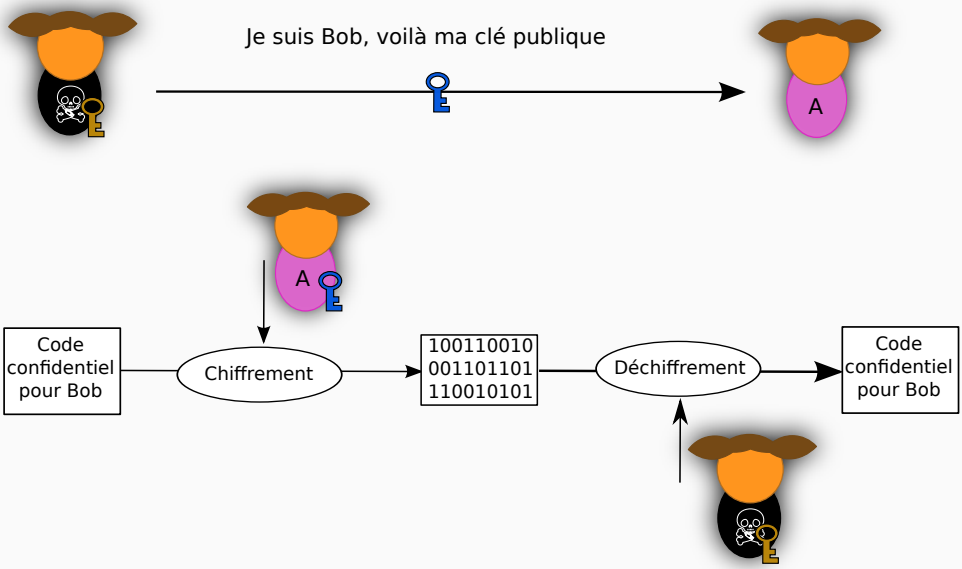
Anaïs Gantet, Benoît Camredon
TLS-SEC 2020/2021

Introduction

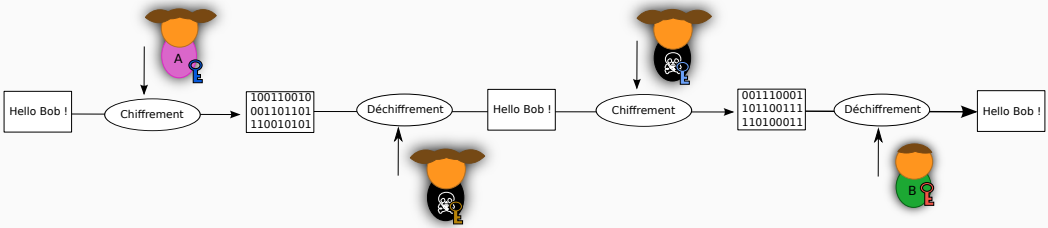
Partage de clé publique



Partage de clé publique



Partage de clé publique



Problématique

- Comment s'assurer que la clé publique que l'on détient appartient bien à la bonne personne ?

Certifier la clé publique

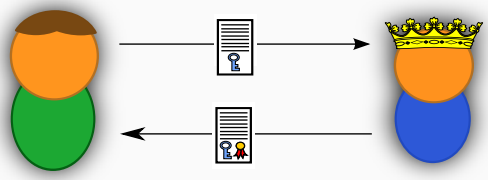
Lien l'entité à la clé

- Besoin de s'assurer de l'origine de la clé publique
- Intervention d'un tiers qui va certifier l'origine de la clé

Autorité de certification

- Tiers de confiance
- Certifier que la clé publique appartient bien à l'entité décrite
  - Vérifier l'identité de l'entité possédant la clé publique
  - Fournir les moyens nécessaires pour lier la clé publique à l'identité
  - Mettre en place un mécanisme permettant d'alerter en cas de problème

Enregistrement auprès de l'autorité de certification



Etapes de l'enregistrement

1. Constitution du dossier
2. Envoi des informations avec la clé publique (Certificate Signing Request ou `CSR`)
3. Enquête de l'autorité de certification
4. Envoi du certificat liant la clé à l'identité de la personne

Autorité de certification

La liaison Clé Publique/Identité est faite via le mécanisme de signature

Autorité de certification

- Besoin de connaitre la clé publique de l'autorité de certification

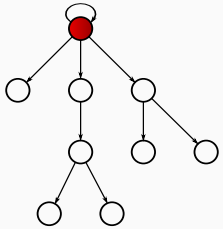
Mais...

- Problème de la poule et de l'œuf !!!
- Confiance *aveugle* en l'autorité de certification

Les Autorités de certifications les plus connues sont pré-enregistrées (`/etc/ssl/certs`)

Hiérarchie des autorités de certification

- Souplesse
- Séparation par division
- Séparation par domaine



Vérification complète

- Besoin de vérifier le chemin complet !

Certificats

Certificats

Qu'est ce que c'est ?

- Document électronique
  - Définition d'une entité
  - Date
  - Clé publique
  - Tampon d'un tiers de confiance
  - Conditions d'utilisation valides
  - ...

Objectif

- Lier la clé publique à l'entité

Plusieurs formats

- Certificats SSH
- Certificats x509
- ...

Certificats x509

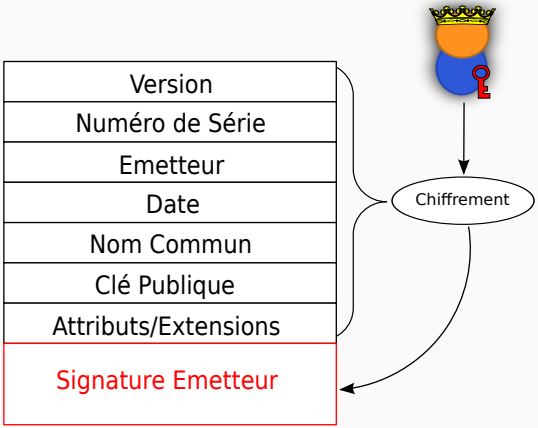
Qu'est ce que c'est ?

- Standard définissant un format de certificat à clés publiques (RFC 5280)
- Largement utilisé de nos jours (`SSL/TLS`,...)

Informations contenues

- Version
- Numéro de série
- Issuer
- Subject
- Date de validité : `notBefore`, `notAfter`
- Clé publique
- Extensions
- Signature
- ...

Structure d'un certificat



Sujet et Emetteur

Identification

- **CN** : Common Name
- **O** : Organisation
- **OU** : Organisation Unit
- **L** : Locality/City
- **ST** : State/Province
- **C** : Country

Encodage des certificats

Deux encodages principaux

- Distinguished Encoding Rules (`DER`)
  - Encodage binaire (ASN.1)
- Privacy Enhanced Mail (`PEM`)
  - Encodage ASCII : base64 du DER entourée avec `---BEGIN CERTIFICATE---` et `---END CERTIFICATE---`

Extensions X509

Qu'est ce que c'est ?

- Apparues depuis la version 3
- Ajout d'attributs supplémentaires
- Identification avec un OID

Quelques extensions

- `Basic Constraints`
  - Utilisable pour signer des certificats, profondeur de vérification
- `Subject Key Identifier`
  - Identifiant de la clé
- `Subject Alternative Name`
  - Nom associé au certificat
- `Key Usage` et `Extended Key Usage`
  - Usages autorisés de la clé

Usage et usages étendus

- Vérification de signature
- nonRepudiation
- Chiffrement de clé
- Chiffrement de données
- Accord de clé
- Vérification de signature de certificat
- Signature de CRL
- Chiffrement seul
- Déchiffrement seul
- ...

Exemple de certificat

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
        2b:9f:7e:e5:ca:25:a6:25:14:20:47:82:75:3a:9b:b9
  Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=ZA, O=Thawte Consulting (Pty) Ltd.,
            CN=Thawte SGC CA
    Validity
        Not Before: Oct 26 00:00:00 2011 GMT
        Not After : Sep 30 23:59:59 2013 GMT
    Subject: C=US, ST=California, L=Mountain View,
             O=Google Inc, CN=mail.google.com
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (1024 bit)
            Modulus:
              00:af:39:15:98:68:e4:92:fe:4f:4f:f1:bb:ff:0d:
              2e:b0:fe:25:aa:bd:68:04:67:27:ea:6c:43:4c:a7:
              6d:cb:c8:8f:7e:81:ee:87:26:25:10:12:54:33:9e:
              aa:3d:9b:8f:8e:92:b3:4b:01:e3:f9:4a:29:c3:0f:
              fd:ac:b7:d3:4c:97:29:3f:69:55:cf:70:83:04:af:
              2e:04:6e:74:d6:0f:17:09:fe:9e:20:24:24:e3:c7:
              68:9c:ac:11:bd:92:e4:b2:1b:09:f2:02:32:bb:55:
              1b:2d:16:5f:30:12:23:e2:4c:4a:8d:c2:da:3f:e1:
              b8:bf:f7:3a:b1:86:be:f0:c5
            Exponent: 65537 (0x10001)
```

```
X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:FALSE
      X509v3 CRL Distribution Points:

        Full Name:
          URI:http://crl.thawte.com/ThawteSGCCA.crl

      X509v3 Extended Key Usage:
        TLS Web Server Authentication,
        TLS Web Client Authentication,
        Netscape Server Gated Crypto
      Authority Information Access:
        OCSP - URI:http://ocsp.thawte.com
        CA Issuers -
         URI:http://www.thawte.com/repository/Thawte_SGC_CA.crt

    Signature Algorithm: sha1WithRSAEncryption
       35:80:11:cd:52:3e:84:29:fb:c1:28:e1:20:e5:02:8f:5f:71:
       65:58:1d:62:72:57:3c:e6:5e:25:61:d3:cb:ad:22:f8:d8:81:
       a4:e7:f4:ae:7c:d9:c1:6d:aa:93:0d:62:07:9f:f2:67:47:99:
       34:33:4f:3d:02:74:f4:81:d6:38:08:21:e8:e2:a1:fa:05:41:
       9c:9c:c9:f9:f3:c8:a3:ee:0d:a5:d7:50:54:5e:2f:7d:79:b7:
       7e:0a:7c:b6:e2:2c:a8:ae:fe:94:d7:cd:16:30:71:04:aa:9e:
       79:c3:d2:b6:24:a7:25:ab:f0:48:8e:2f:c3:a7:bb:50:dd:0f:
       cf:b0
```

PKI

Infrastructure permettant la gestion des certificats

- Génération de certificats
- Distribution
- Stockage
- Révocation
- ...

Révocation

Objectif

- Mettre un certificat hors service

Plusieurs méthodes

- Une base de données de certificats à ne plus utiliser (CRL)
  - Attention : Le refus d'un certificat nécessite la mise à jour de la CRL
- L'interrogation d'un serveur (OCSP)
  - Besoin d'une grande disponibilité du serveur OCSP

Les certificats en pratique

En pratique tout repose sur le bon vouloir de l'utilisateur final. . .

. . . et tout le monde sait qu'il n'est pas fiable.