



Certificats

Cryptographie à clé publique

Partie: 2

Prof:Mme F.Omary

2020-2021

Introduction

✚ **Les algorithmes de chiffrement asymétrique sont basés sur le partage entre les différents utilisateurs d'une clé publique.**

Généralement le partage de cette clé se fait au travers d'un annuaire électronique, ou bien d'un site web.

✚ **Ce mode de partage a une grande lacune :**

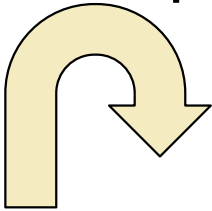
Rien ne garantit que la clé est bien celle de l'utilisateur à qui elle est associée

Introduction (suite)

✖ **En effet un pirate peut corrompre la clé publique présente dans l'annuaire en la remplaçant par sa clé publique.**

Ainsi, le pirate sera en mesure de déchiffrer tous les messages ayant été chiffrés avec la clé présente dans l'annuaire.

Motivations

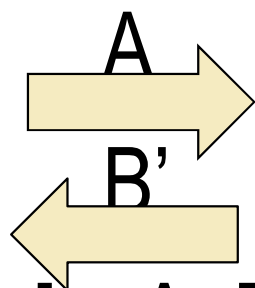
- ⚡ Attaque classique du protocole d'échange de clef secrète de **Diffie-Hellman**:
- ⚡ Oscar coupe la ligne de communication entre Alice et Bob avant qu'ils ne commencent le partage de la clef (émission de A et B):
Attaque dite « **Man-in-the middle** »
- ⚡ Idée générale : Oscar se fait passer pour Bob auprès d'Alice et simultanément pour Alice auprès de Bob 
- ⚡ Il peut lire toutes les communications entre Alice et Bob avec la clef qu'ils pensent avoir construite ensemble en secret.



Alice

génère a

$$A = g^a \bmod p$$



(dispose de $[a, A, B', p]$)

Clé secrète:

$$K_A = B'^a \bmod p$$

Oscar

génère b' et a'

$$B' = g^{b'} \bmod p$$

$$A' = g^{a'} \bmod p$$

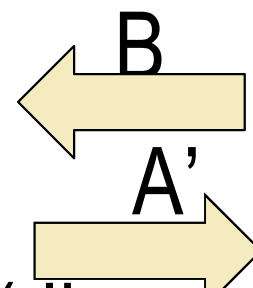
Clés secrètes

K_A et K_B

Bob

génère b

$$B = g^b \bmod p$$



(dispose de $[b, A', B, p]$)

Clé secrète:

$$K_B = A'^b \bmod p$$

Message intercepté par: Man-in-the middle



Alice

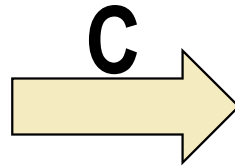


$$C = E_{K_A}(M)$$



Oscar

Bob



$$M = D_{K_A}(C)$$

$$M' = E_{K_B}(M)$$

A thick yellow arrow pointing to the right, with the letter 'M'' above it, representing the modified message.
$$M = D_{K_B}(C)$$

Une solution: certificat

- ✦ Ainsi un certificat permet d'associer une clé publique à une entité afin d'en assurer la validité
- ✦ C'est en quelque sorte une carte d'identité de la clé publique délivrée par une « **Autorité de Certification** » ou **AC** (CA en anglais)

Autorité de Certification

Autorité de Certification :

✚ l'Autorité de Certification (AC), véritable Tiers de Confiance, garantit la validité des éléments contenus dans le certificat.

✚ AC est chargée de:

- délivrer les certificats numériques,
- leur assigner une date de validité
- garantir l'identité de son propriétaire

Structure d'un Certificat

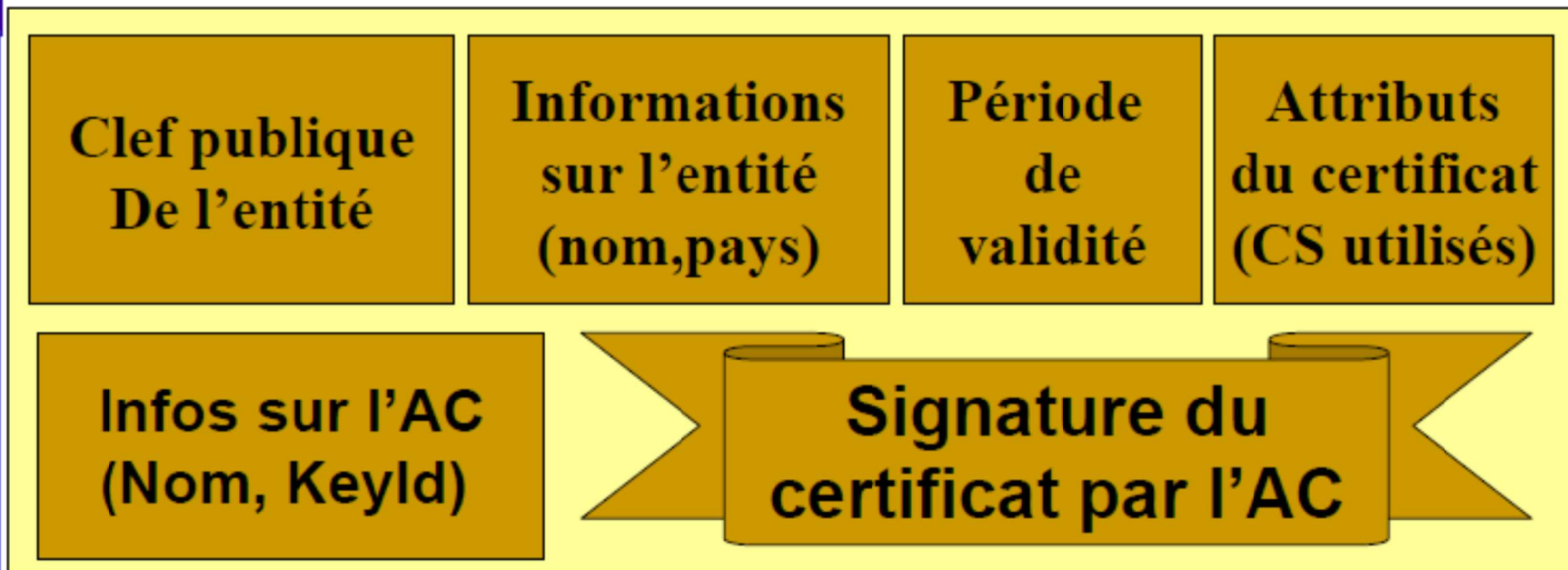
✚ **Les certificats sont des petits fichiers divisés en deux parties :**

- La partie contenant les informations
- La partie contenant la signature de l'autorité de certification

Structure d'un Certificat

- ✱ La structure des certificats est normalisée par le standard X.509 de l'UIT qui définit les informations contenues dans le certificat :
 - la clé publique de son détenteur et des informations sur son identité
 - le nom distinctif de l'autorité de certification
 - La date de début de validité du certificat ;
 - La date de fin de validité du certificat ;
 - la signature électronique (chiffrement de l'empreinte par clé privée) de l'autorité de certification.

Structure d'un Certificat



Comment cela fonctionne ?

- ✚ **L'ensemble des informations contenues dans le certificats «informations+clé publique du demandeur» sont signés pas l'autorité de certification**
- ✚ **Cela signifie qu'une fonction de hachage crée une empreinte de ces informations**

Comment cela fonctionne ?

- ✦ Puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification
- ✦ La clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature de l'**AC**

Comment cela fonctionne ?

Certificat

Informations

- Autorité de certification : Verisign
- Nom du propriétaire : Jeff PILLOU
- Email : webmaster@commentcamarche.net
- Validité : 04/10/2001 au 04/10/2002
- Clé publique : 1a:5b:c3:a5:32:4c:d6:df:42
- Algorithme : RC5

Signature

3b:c5:cF:d6:9a:Bd:c3:c6



*Clé privée de
l'autorité de
certification*

Comment cela fonctionne ?

- ✚ Pour vérifier le certificat les utilisateurs auront recours à la clé publique de l'autorité de certification.
- ✚ Même principe des signatures électronique

Comment cela fonctionne ?

✖ Lorsque le demandeur veut communiquer avec une autre personne, il se procure le certificat qui est signé par **AC**, ce certificat contient sa clé publique

- Il calcule le haché (condensé) à l'aide de la fonction de hachage.
- Il déchiffre la signature de l'autorité de certification
- Il compare les deux hachés

Si il y'a égalité, la clé publique est certifiée

Comment cela fonctionne ?

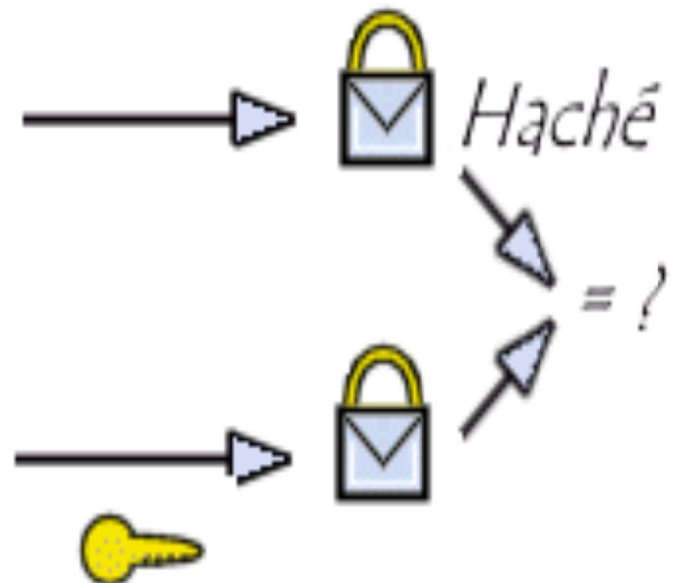
Certificat

Informations

- Autorité de certification : Verisign
- Nom du propriétaire : Jeff PILLOU
- Email : webmaster@commentcamarche.net
- Validité : 04/10/2001 au 04/10/2002
- Clé publique : 1a:5b:c3:a5:32:4c:d6:df:42
- Algorithme : RC5

Signature

3b:c5:cF:d6:9a:Bd:e3:c6



Déchiffrement à l'aide
de la clé publique de
l'autorité de certification

Exemple de Certificat

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 13805 (0x35ed)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=FR, O=CNRS, CN=CNRS-Standard

Validity

Not Before: Apr 24 14:09:48 2006 GMT

Not After : Apr 24 14:09:48 2008 GMT

Subject: C=FR, O=CNRS, OU=UMR7606,
CN=src.lip6.fr/emailAddress=postmaster@lip6.fr

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:ec:29:c5:24:d6:4d:e4:b5:31:71:46:2f:15:64:

...

a6:ee:85:31:22:de:74:d8:d1:5f:8a:32:e0:b3:d7:

84:e4:8f:ab:66:92:ad:f8:eb

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:FALSE

Netscape Cert Type:

SSL Client, SSL Server

X509v3 Key Usage: critical

Digital Signature, Non Repudiation, Key Encipherment

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication

Netscape Comment:

Certificat serveur CNRS-Standard

X509v3 Subject Key Identifier:

79:F7:B4:D3:D8:E9:B8:ED:3C:A1:85:A6:DD:FA:68:CC:74:8C:82:1F

X509v3 Authority Key Identifier:

keyid:67:59:A5:E5:07:74:49:03:EF:05:CF:CC:2E:A4:18:D5:10:C8:9E:3C

DirName:/C=FR/O=CNRS/CN=CNRS

serial:02

X509v3 Subject Alternative Name:

DNS:src.lip6.fr

X509v3 CRL Distribution Points:

URI:http://crls.services.cnrs.fr/CNRS-Standard/getder.crl

Signature Algorithm: sha1WithRSAEncryption

54:a4:1c:c2:21:fd:06:9b:df:bd:50:4b:d2:ae:e0:3f:46:64:

Signatures de certificat

On distingue différents types de certificats selon le niveau de signature par exemple :

- **Les certificats auto-signé** : sont des certificats à usage interne. Signés par un serveur local, ce type de certificat permet de garantir la confidentialité des échanges au sein d'une organisation
- **Les certificats signés par un organisme de certification** : sont nécessaires lorsqu'il s'agit d'assurer la sécurité des échanges avec des utilisateurs anonymes

Révocations de Certificats

✚ CRL=« certificat revocation list »

✚ Les CRL: liste des certificats révoqués, liste signée par la CA

- Similaire à l'opposition des CB/chèque en cas de vol.
- Pas encore de CRL incrémentale(le certificat contient une url du fichier de crl)
- La révocation est une limite théorique au modèle des PKIs

✚ Les navigateurs doivent vérifier par eux-même les CRL