PKI « Public Key Infrastructure »

ACHRAF FAYAD

ECE

2017/2018

The main goals of Cryptography

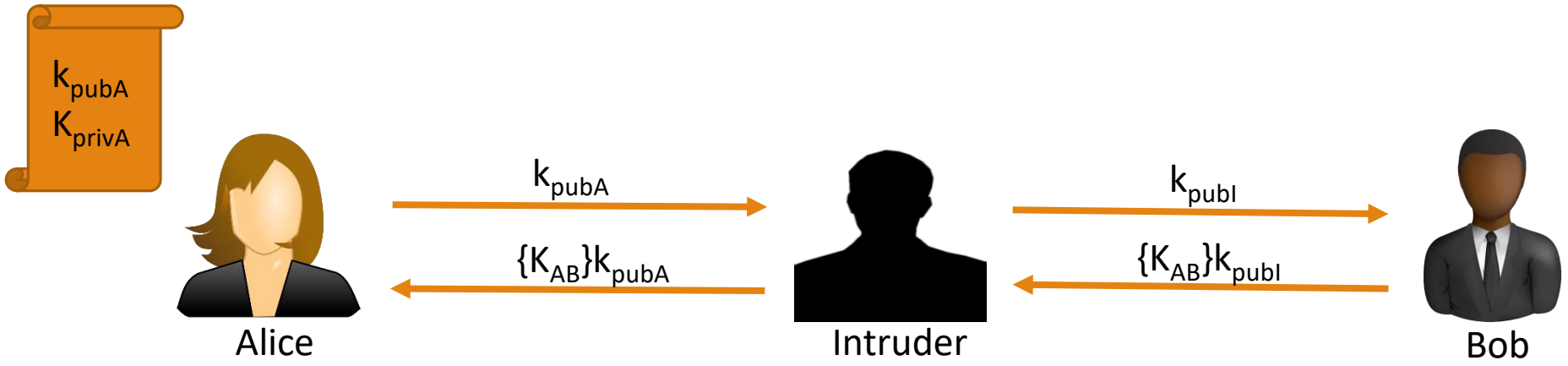
- **Privacy or confidentiality**
  - It is the service used to keep the content of information secret from all but those authorized one to have it. There are numerous of approaches that provide confidentiality, cryptography deals with protection through mathematical algorithms which render data unintelligible.
- **Data Integrity**
  - It refers to the unauthorized manipulation of data.
- **Authentication**
  - It is a service related to identification. This function applies to both entity authentication and data origin authentication.
- **Non-repudiation:**
  - It is a service which prevents an entity from denying previous commitments or action.

Problem related of symmetric cryptography

- Key distribution :
  - Symmetric crypto requires how to securely share the key (K_{AB})
- Digital Signature (non repudiation)
  - Not possible with symmetric crypto
- Intergrity:
  - Not possible with symmetric crypto

How to authenticate public keys ?

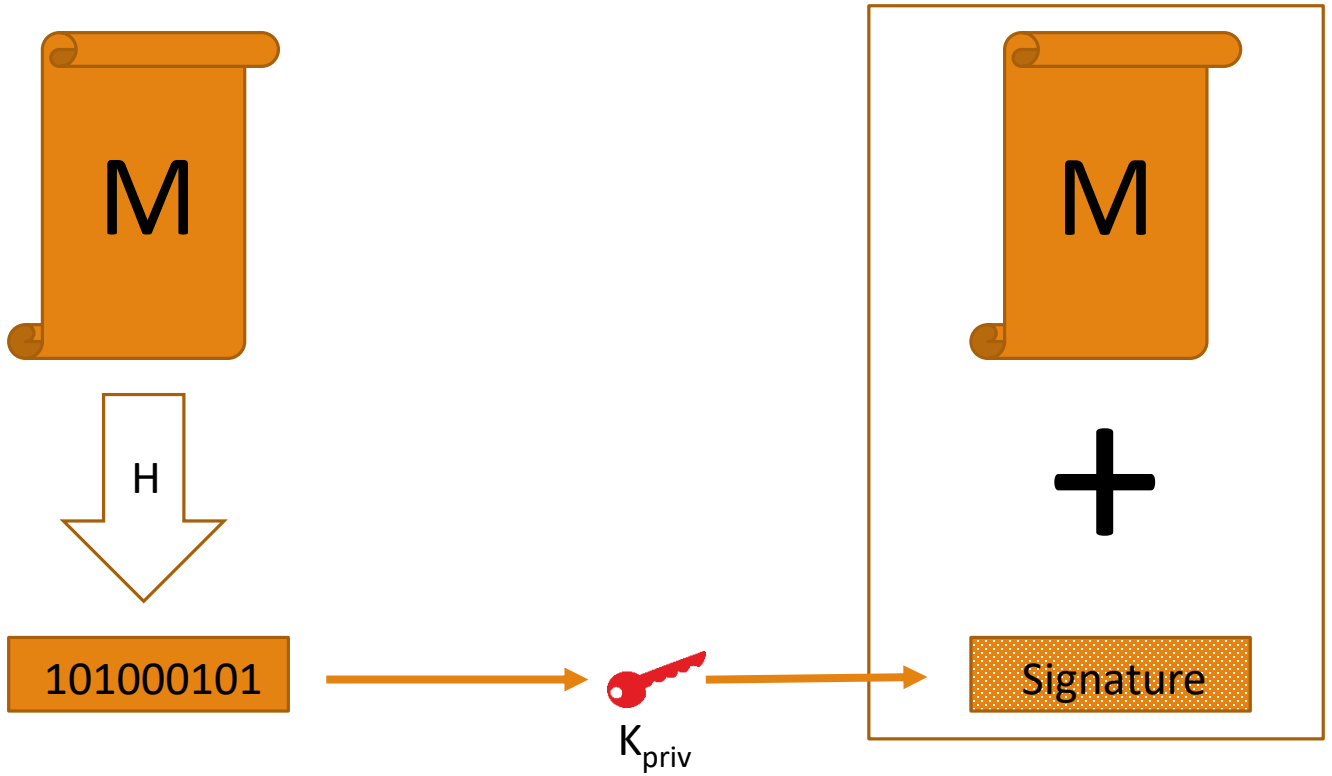
The public keys are not authenticated: When Bob receives a public key which is allegedly from Alice, he has no way of knowing whether it is in fact his.



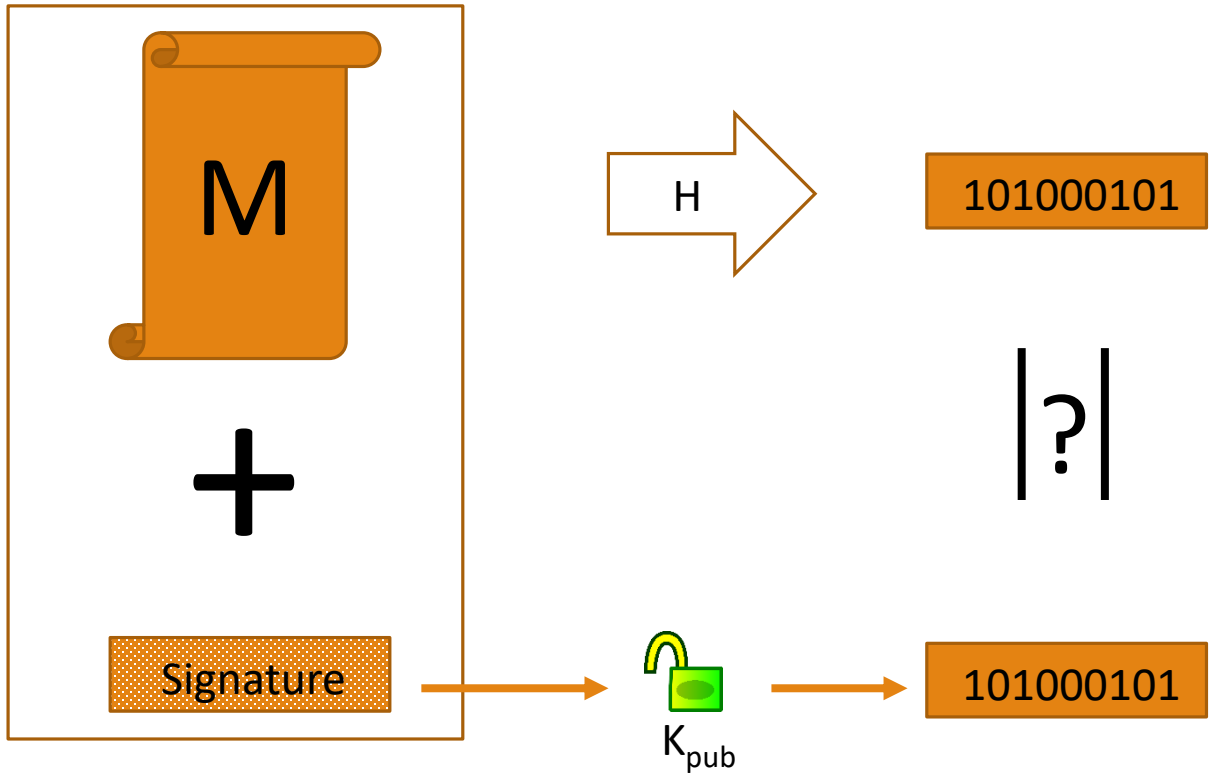
The attack works always by the same pattern: Intruder replaces the public key from one of the parties by his own key.

Digital Signatures / signing

- We can use digital signatures to:
  - Control access to data
  - Allow users to authenticate themselves to a system,
  - Allow users to authenticate data,
  - Sign ‘real’ documents.



Digital Signatures / Verification



Digital certificate

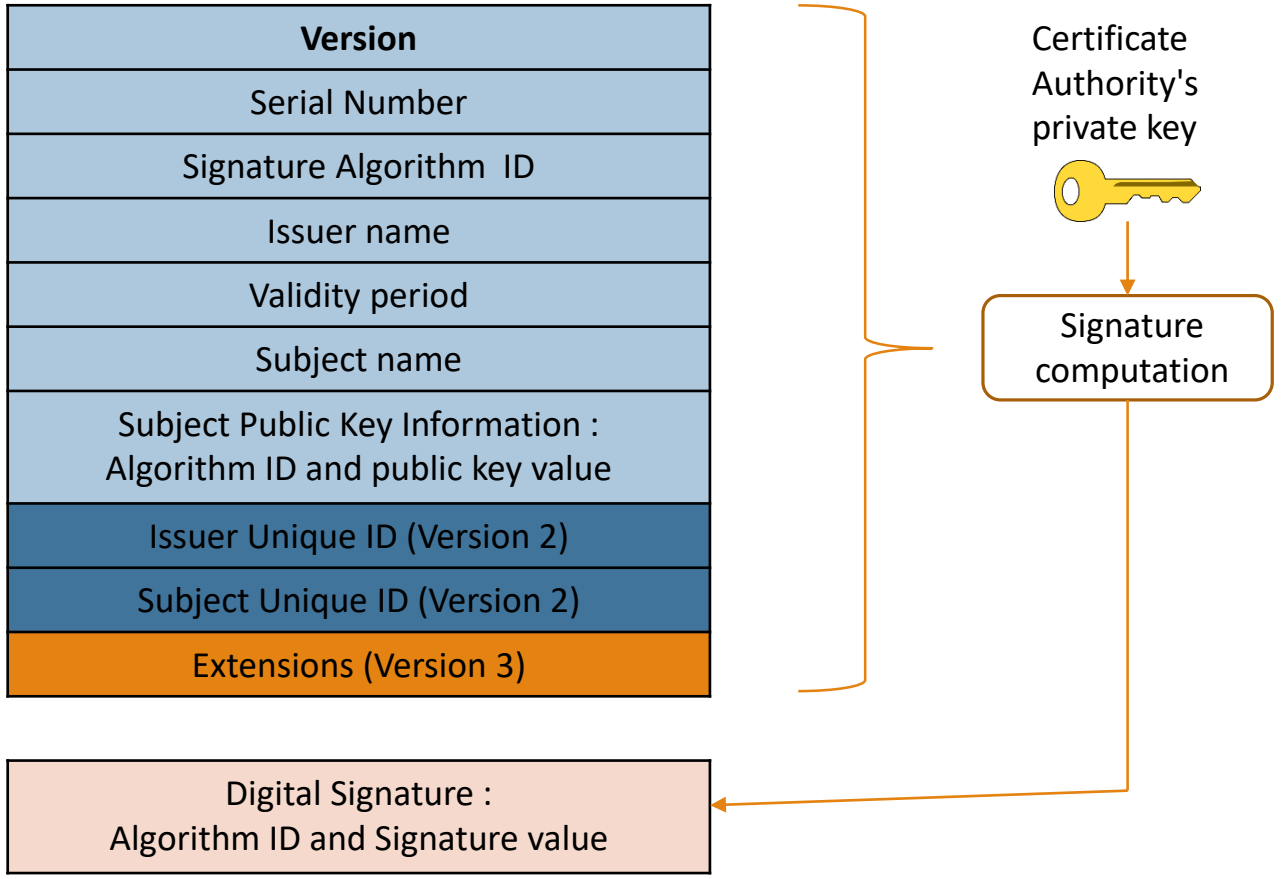
- A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI).
- The Certificate authority acts as a middleman that both computers trust.
- Usage of Digital Certificate:
  - Identification
  - Confidentiality
  - Integrity
  - Access Control
  - Non-repudiation

Digital certificate

- Several cases of use certificates :
- Client Certificate :
  - To authenticate an user.
- Server Certificate:
  - To authenticate a server
- CA Certificate
  - To sign certificates

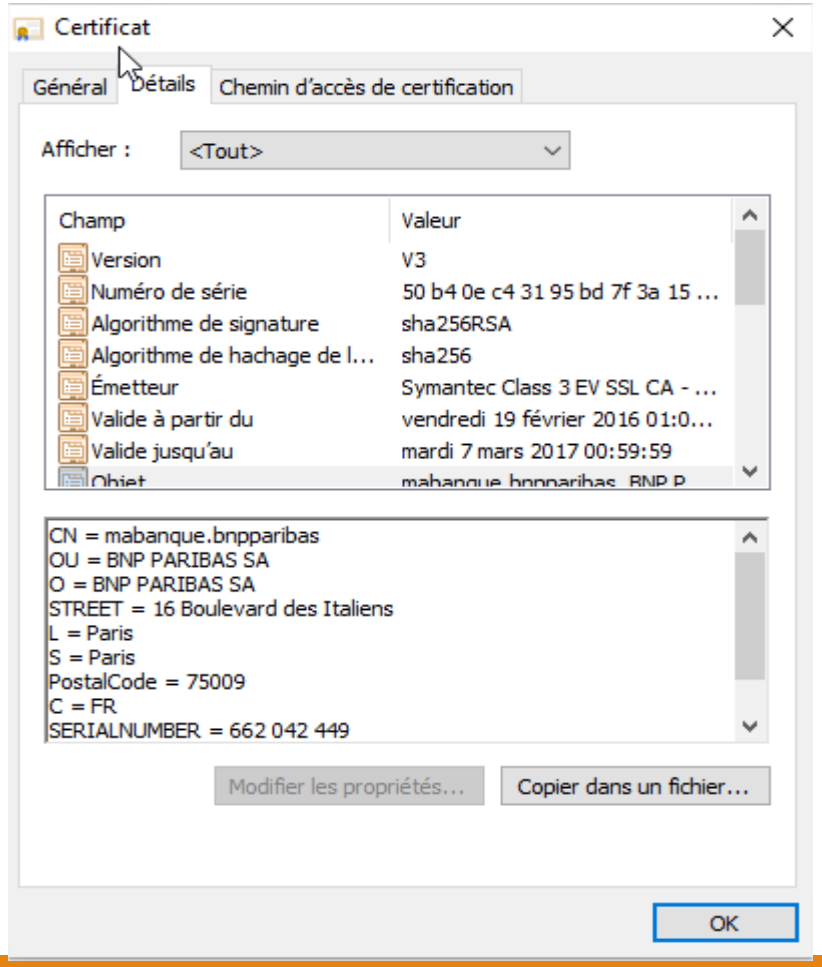
Certificate X.509 Standard

- Standard:
  - ITU-T X.509(03/2000), or ISO/IEC 9594-8 Certificates of public key and attributs
  - RFC 3280: (profil definition based on X509)
- Versions :
  - 1988 : v1
  - 1993 : v2 = v1 + 2 new Fields
  - 1996 : v3 = v2 + extensions



Certificate X.509 Standard

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
50:b4:0e:c4:31:95:bd:7f:3a:15:d5:b8:07:ea:3d:12
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G3
Validity
Not Before: Feb 19 00:00:00 2016 GMT
Not After : Mar 6 23:59:59 2017 GMT
Subject: 1.3.6.1.4.1.311.60.2.1.3=FR/businessCategory=Private Organization/serialNumber=662 042 449, C=FR/postalCode=75009, ST=Paris, L=Paris/street=16 Boulevard des Italiens, O=BNP PARIBAS SA, OU=BNP PARIBAS SA, CN=mabanque.bnpparibas
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus: . 00:c6:17:..... b:06:f8:
d4:79
……;
Signature Algorithm: sha256WithRSAEncryption
74:4a:69:2f……ec:fc:f7:89:09:ac:ea:93:c9:3a:b8:19:59:db:d2:
11:d8:89:b1



Certificate X.509 Standard – Revocation

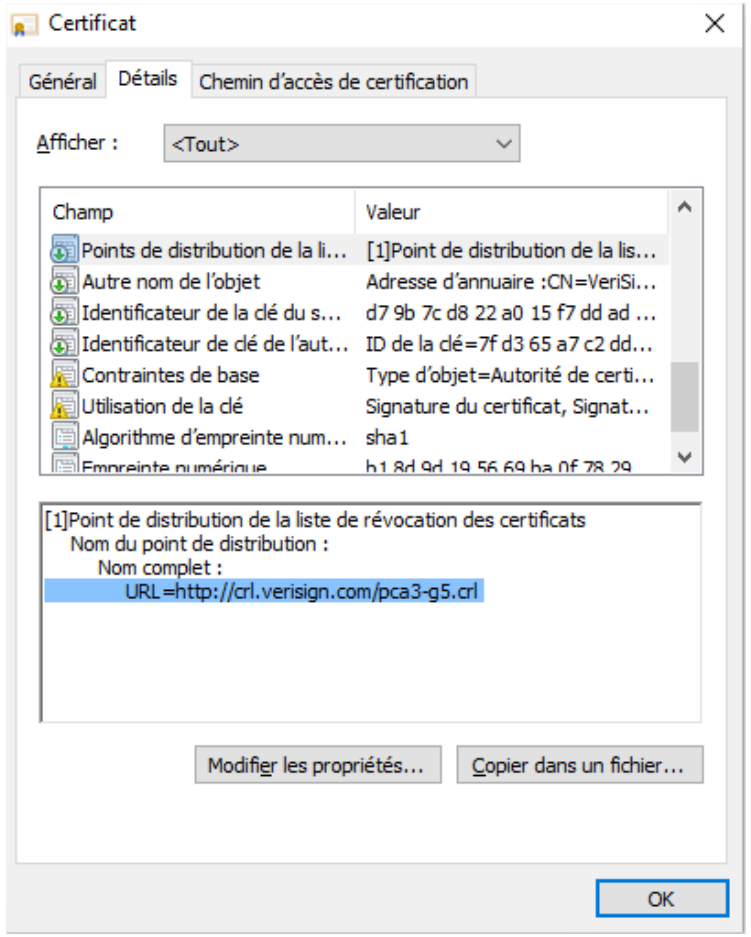
- A certificate can be revoked when:
  - The private key of the authority is compromised
  - The private key associated with the certificate is compromised
  - Change in status of the certificate's owner
  - Suspension of the certificate's owner
  - A certificate was obtained by fraud
  - A change in the status of the certificate subject as an entity approved

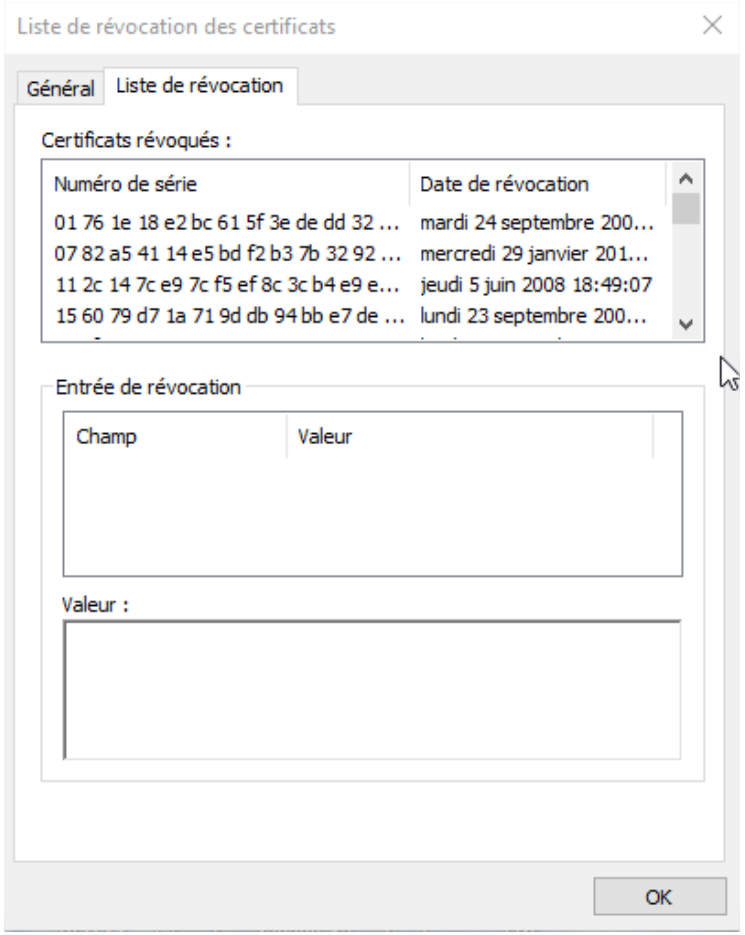
- The revocation authority and the certification authority may be the same entity.

Certificate X.509 Standard – Revocation

- Different methods of revocation:
  - CRLs (Certificate Revocation List)
  - CRL Distribution Points
  - Delta CRLs
  - OCSP (Online Certificate Status Protocol)
    - Real-time verification
  - SCVP (Simple Certificate Validation Protocol)
    - Allows a client to offload certificate to a server
- A Certificate contains in a extension one or more methods and server address (or servers) and CRL file.
  - http://crl.verisign.com/pca3.crl-g5.crl

Certificate X.509 Standard – Revocation

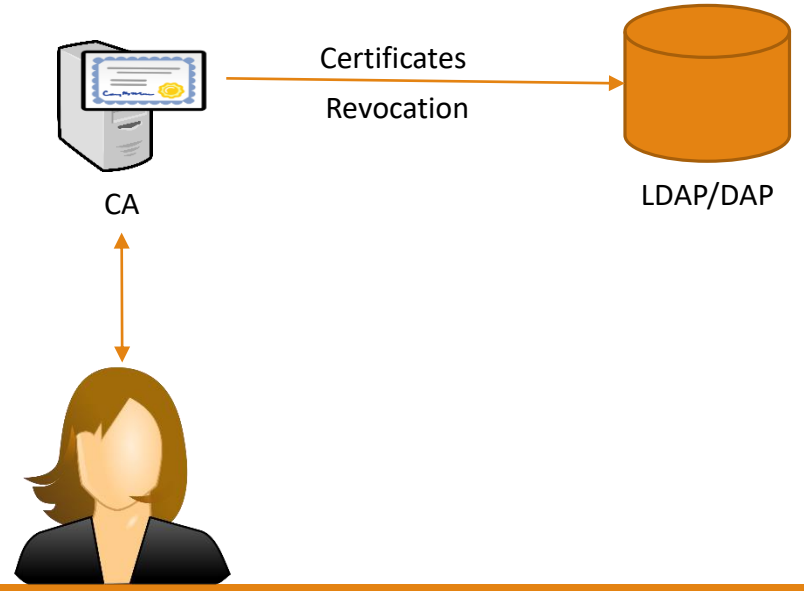




PKI - Public Key Infrastructure

- Provide and manage the security elements that allow the implementation of the security services based on asymmetric cryptography:
  - Authentication, identification, no repudiation , digital signature.
- Establish a trusted third.
- And verification, certification, revocation and publication of public keys.

CA verify the authenticity of request, sign and publish the certificate



Certificate Authority - CA

A CA based system works as follows:

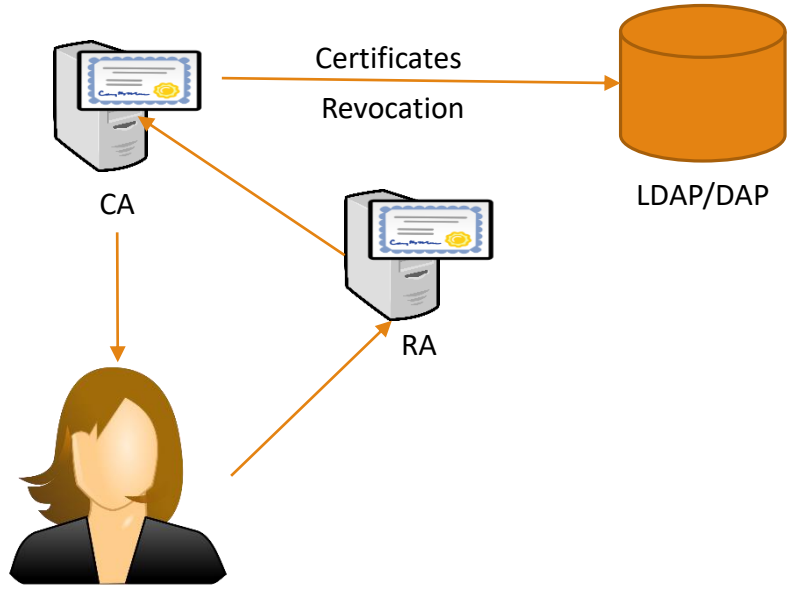
- All users have a trusted copy of the public key of the CA.
- The CA's job is to digitally sign data strings containing the following information (Alice, Alice's public key).
- This data string, and the associated signature is called a digital certificate. The CA will only sign this data if it truly believes that the public key really does belong to Alice.
- When Alice now sends you her public key, contained in a digital certificate, you now trust that the purported key really is that of Alice, since you trust the CA to do its job correctly.

A CA has the own Certificate :

- Self-signed
- Or delivered by another CA

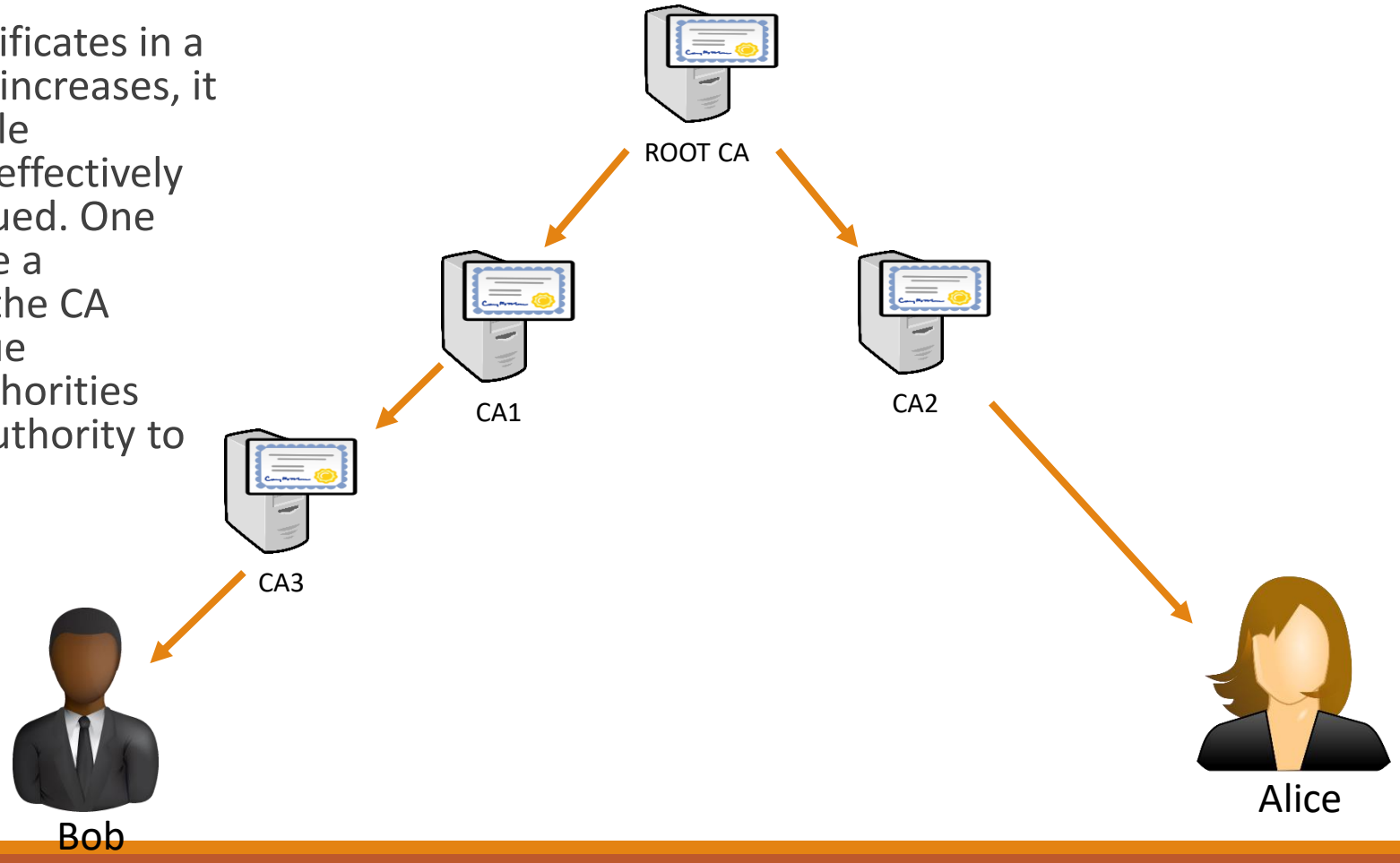
Registration Authority RA

- CA checks with a registration authority RA to verify information provided by the requestor of a digital certification.
  - If the RA verifies the requestor's information, the CA can issue a certificate.

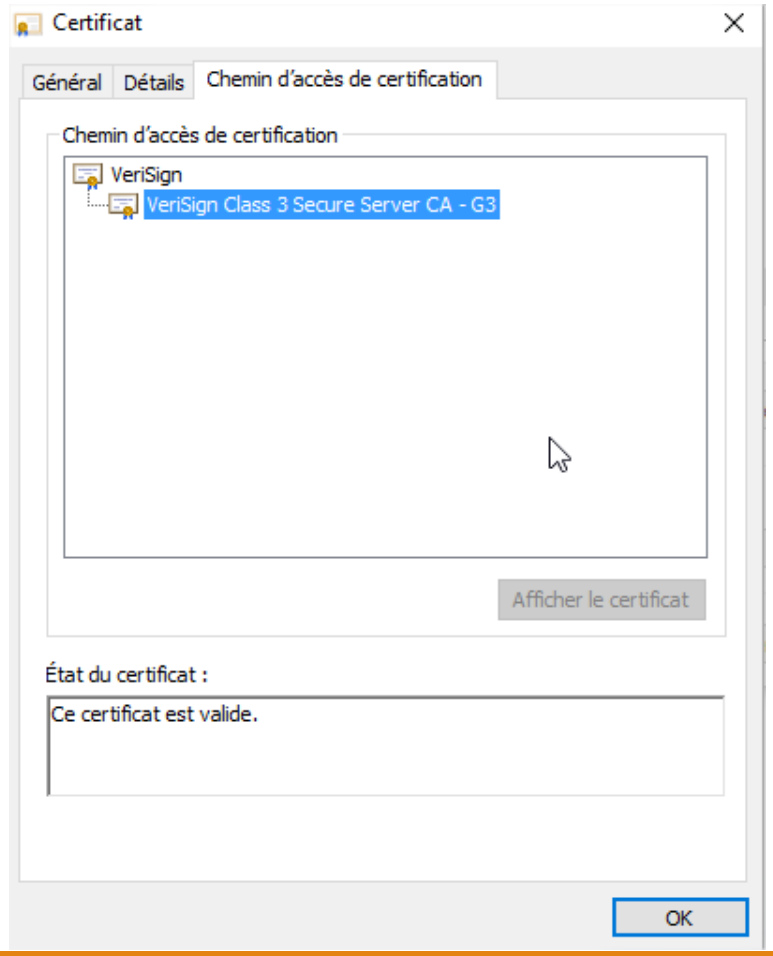


Trust Models - Certification hierarchy

- As the number of issued certificates in a public key infrastructure (PKI) increases, it can become difficult for a single certification authority (CA) to effectively track the certificates it has issued. One way to address this is to create a certificate hierarchy in which the CA delegates the authority to issue certificates to subordinate authorities which can, in turn, delegate authority to their subordinates

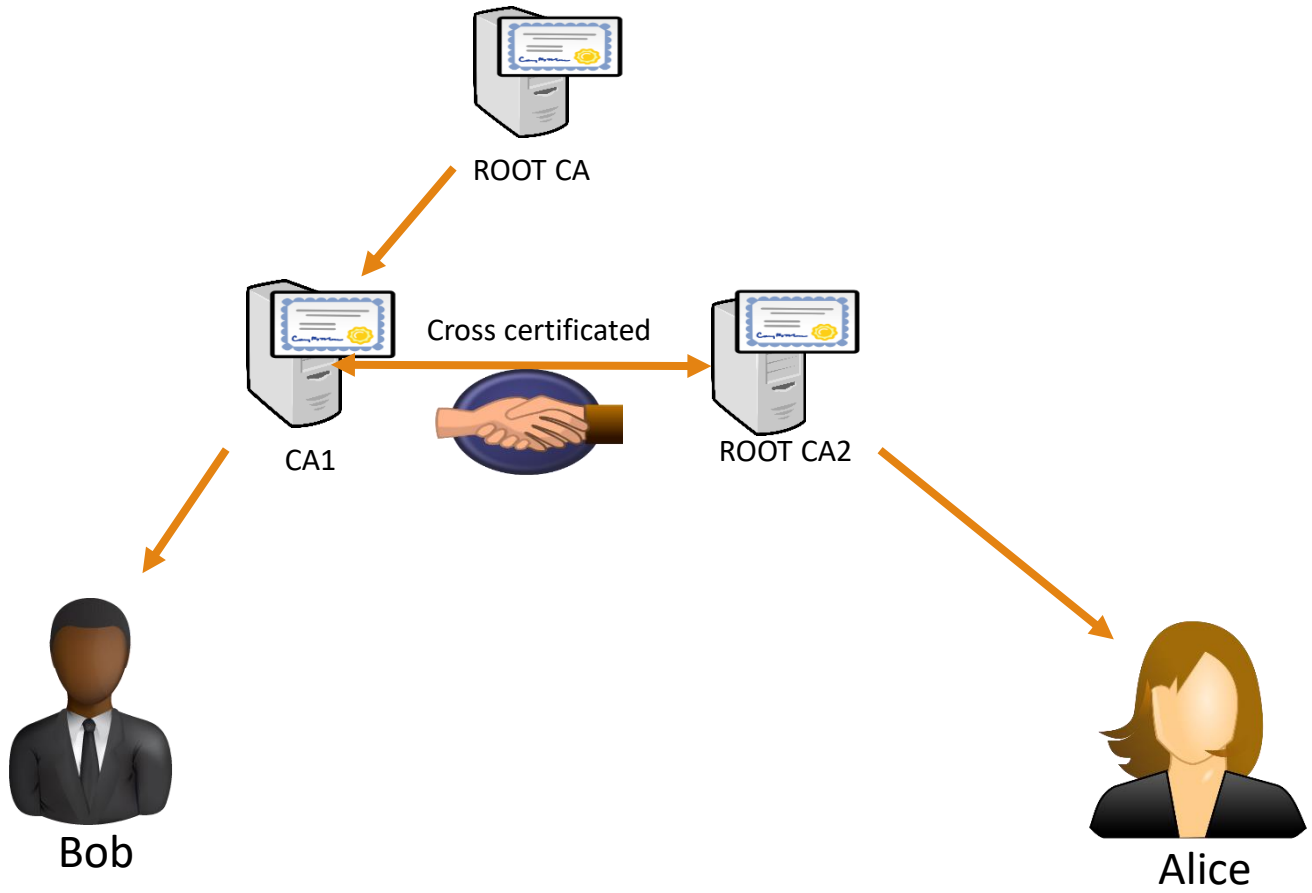


Trust Models - Certification chain



Trust Models - Cross certification

- Cross certification enables entities in one public key infrastructure (PKI) to trust entities in another PKI. This mutual trust relationship is typically supported by a cross-certification agreement between the certification authorities (CAs) in each PKI.



Default list of Certificate Authorities