Les certificats numériques

Dr. Noureddine Chikouche
Université de M'sila
https://sites.google.com/view/chikouchenoureddine

Plan du cours

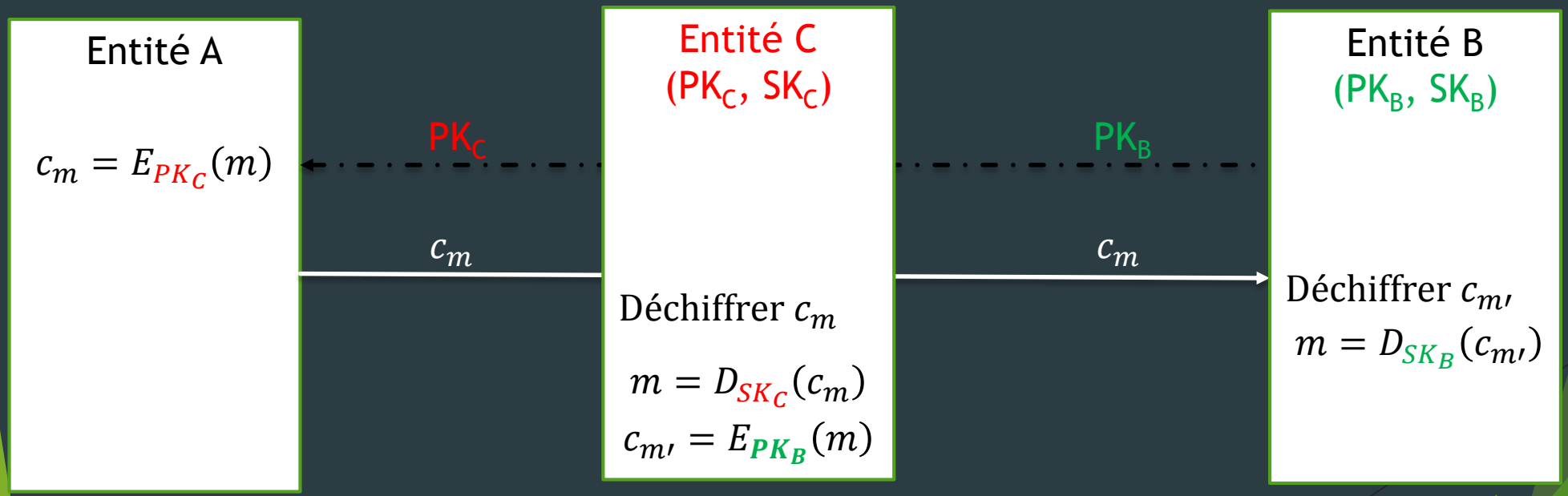
- Introduction
- Infrastructure de Gestion de Clés
- Certificats de clés publiques
- Annuaire électronique LDAP
- Service d'authentification **X509**

Introduction

- Dans notre vie, la carte d'identité et le passeport sont utilisés pour certifier l'identité d'une personne. Ces pièces sont délivrés par une autorité étatique.
- Dans la cryptographie asymétrique, comment certifier une clé publique ?

Introduction

- Dans le cryptosystème asymétrique, le problème de distribution de clés secrètes est résolu, mais le problème d'authentification d'utilisateurs liés à la clé reste continu.



Entité A et B pensent communiquer entre eux

Infrastructure de gestion de clés

- Une infrastructure de gestion de clés (*PKI: Public Key Infrastructure*) est un système qui permet de gérer et distribuer des certificats et des listes de certificats révoqués aux entités finales.
- L'objectif principal du PKI est d'authentifier la clé publique d'une entité (individu, organisation etc.) par créer une certificat numérique pour fournir une confiance entre les utilisateurs.
- Utilisant cette certificat, la communication entre les entités dans le réseau de communication public (e.g. Internet) est sécurisée.

Infrastructure de gestion de clés

PKI fournit quatre services principaux:

- Fabriquer des bi-clés,
- Certifier des clés publiques et publier de certificats,
- Révoquer des certificats,
- Gérer la fonction de certification.

Infrastructure de gestion de clés

Le système PKI utilise trois entités pour gérer les certificats numériques:

- ***Autorité de certification (AC, Certification Authority CA):*** elle est chargée de délivrer des certificats numériques et de valider les listes de révocation.
- Ce certificat numérique est signé par l'AC à l'aide de sa propre clé privée. AC ne peut délivrer un certificat qu'après avoir confirmé tous les justificatifs d'identité.
- N'importe quel utilisateur ayant accès au AC peut obtenir un certificat de celui-ci, mais seul le AC peut modifier un certificat.
- Les mobiles, les SE, et les navigateurs ont mis en place des programmes «d'adhésion » pour les AC autorisées.
- Exemples des AC: Verisign, CertPlus, SSL.com, RapidSSL, GlobalSign, etc.

Infrastructure de gestion de clés

- ***Autorité d'enregistrement (RA: Registration Authority):*** est une entité intermédiaire entre le demandeur du certificat et l'AC afin de vérifier l'identité du demandeur.
- ***Système de publication et de distribution de certificat:*** ou l'autorité de dépôt est une entité sa fonction est la publication et la distribution des certificats qui sont délivrés par l'autorité de certification.
  - Par exemple, l'annuaire LDAP et serveur Web.

Certificats numériques

- Les algorithmes de chiffrement asymétrique ne garantissent pas que la clé publique soit bien celle de l'utilisateur à qui elle est associée.
- Un certificat est un fichier de données vérifiable. Il permet d'associer une clé publique à un utilisateur pour assurer la validité (carte d'identité de la clé publique).
- Pour assurer l'intégrité des clés publiques, il faut qu'elles soient publiées avec un certificat.
- Différentes applications Web peuvent insister pour utiliser un certificat particulier. Par exemples: systèmes de banque, systèmes e-commerce, etc.
- Exemple de certificat: certificat SSL pour les serveurs et les sites web.

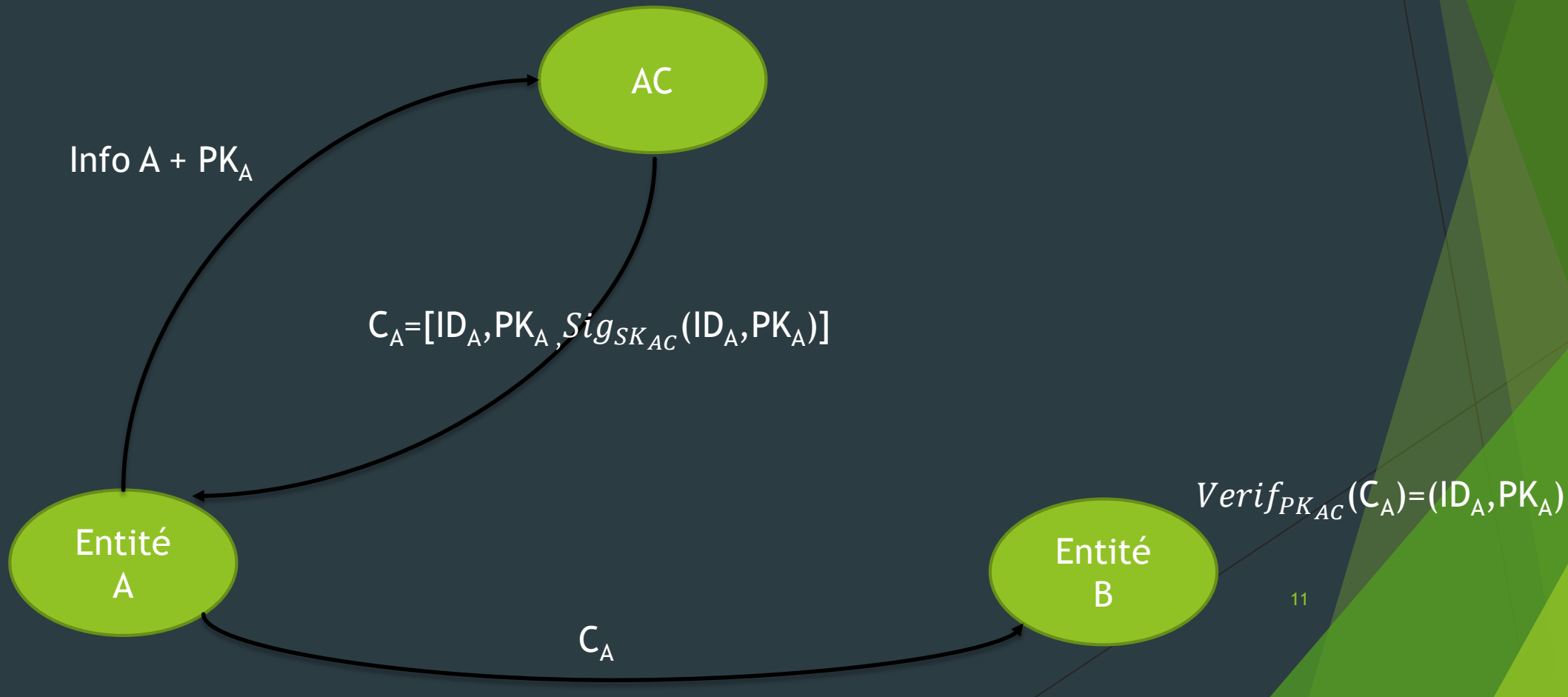
Certificats numériques

Propriétés :

- Les utilisateurs ayant accès au AC peuvent obtenir un certificat de celui-ci, mais seul le AC peut modifier un certificat.
- Les utilisateurs peuvent lire un certificat pour déterminer le nom et la clé publique du propriétaire du certificat.
- Les utilisateurs peuvent vérifier que le certificat provient réellement du AC et n'est pas contrefait.
- Le AC est seul qui peut créer et mettre à jour des certificats.
- Les utilisateurs peuvent vérifier la validité des certificats (Denning-1983).

Certificats numériques

Certification de clé publique



Certificats numériques

Certification de clé publique

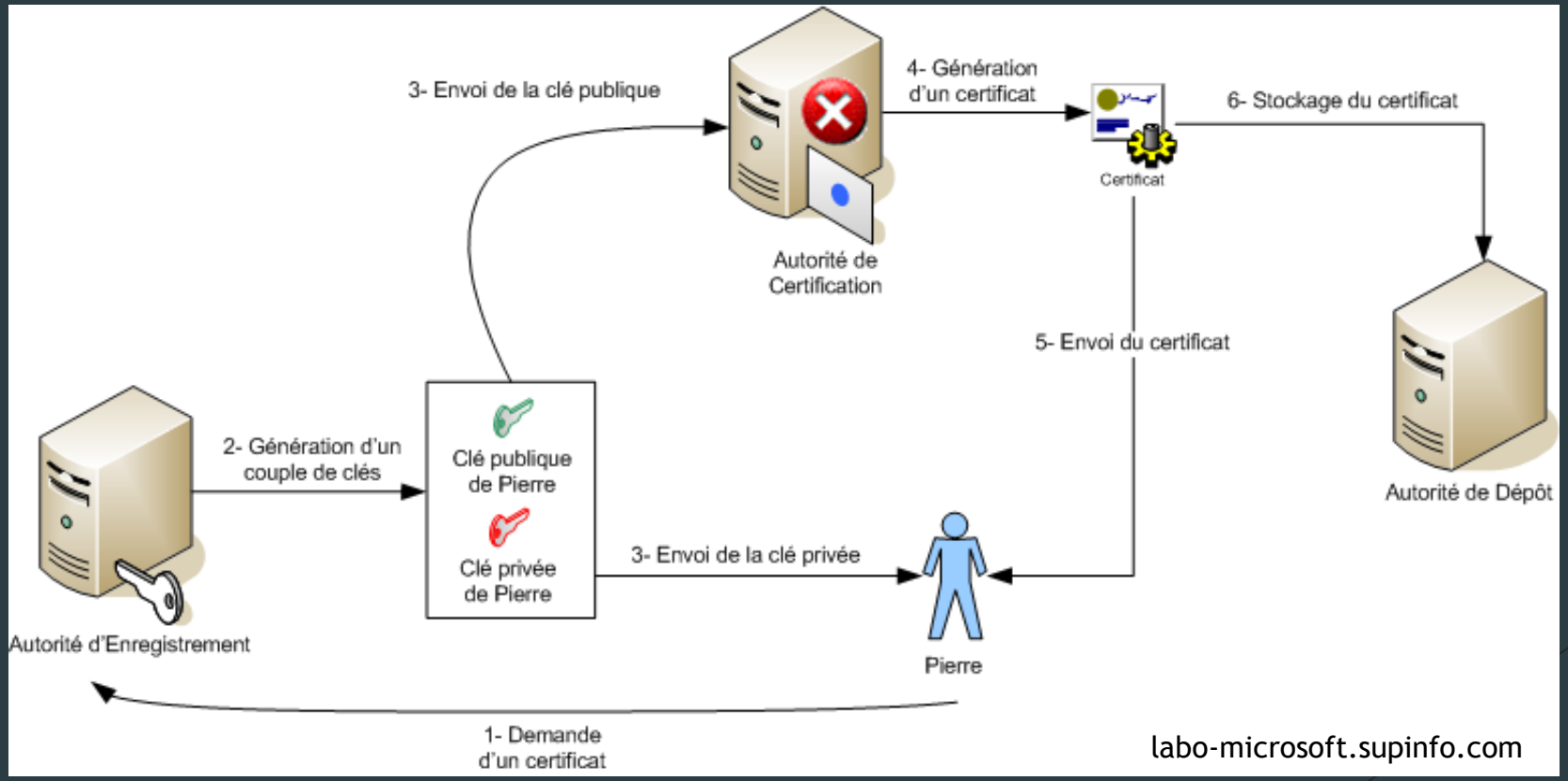
- L'utilisateur A veut certifier que sa clé publique lui appartient.
- A envoie sa clé publique (PK_A) à un autorité de certification (AC), ainsi que différentes informations la concernant (nom, email, etc...).
- Pour envoyer (IDA, PKA), A utilise un canal de communication authentifié. L'AC crée le certificat de l'entité A porte son propre nom, une date limite de validité, et surtout une signature numérique.
- Cette signature est réalisée grâce à la clé privée de AC (SK_{AC}) et à un algorithme de hachage (ex.RSA et le SHA).

Certificats numériques

- L'AC fournit un certificat tel que: $C_A=[ID_A,PK_A, Sig_{SK_{AC}}(ID_A,PK_A)]$
  - SK_{AC}: clé privée de l'autorité de certification,
  - $Sig_{SK_{AC}}$: signature apposée au certificat,
  - ID_A : l'ensemble des informations propres à l'entité A,
  - PK_A: la clé publique de A.
- Lorsque l'utilisateur B veut envoyer un message à A, il applique la clé publique (PK_{AC}) de l'AC.
- Cette action permet de vérifier que le certificat est bien authentique: $Verif_{PK_{AC}}(C_A)=(ID_A,PK_A)$

Certificats numériques

- Pratiquement, PKI génère également les paires de clés publiques-privées pour chaque utilisateur.



Certificats numériques

Révocation de certificat:

- La révocation de certificat ou l'invalidation de clés publiques signifie annulation de certificat avant la date d'expiratin.
- Les certificats révoqués sont enregistrés dans la **liste de révocation de certificats** (*CRL: Certificate Revocation List*).
- Cette liste est signée par l'AC.
- motifs de révocation:
  - Compromission de certificat,
  - Modification des informations de certificat.
  - Disparition de porteur de certificat.

Annuaire électronique LDAP

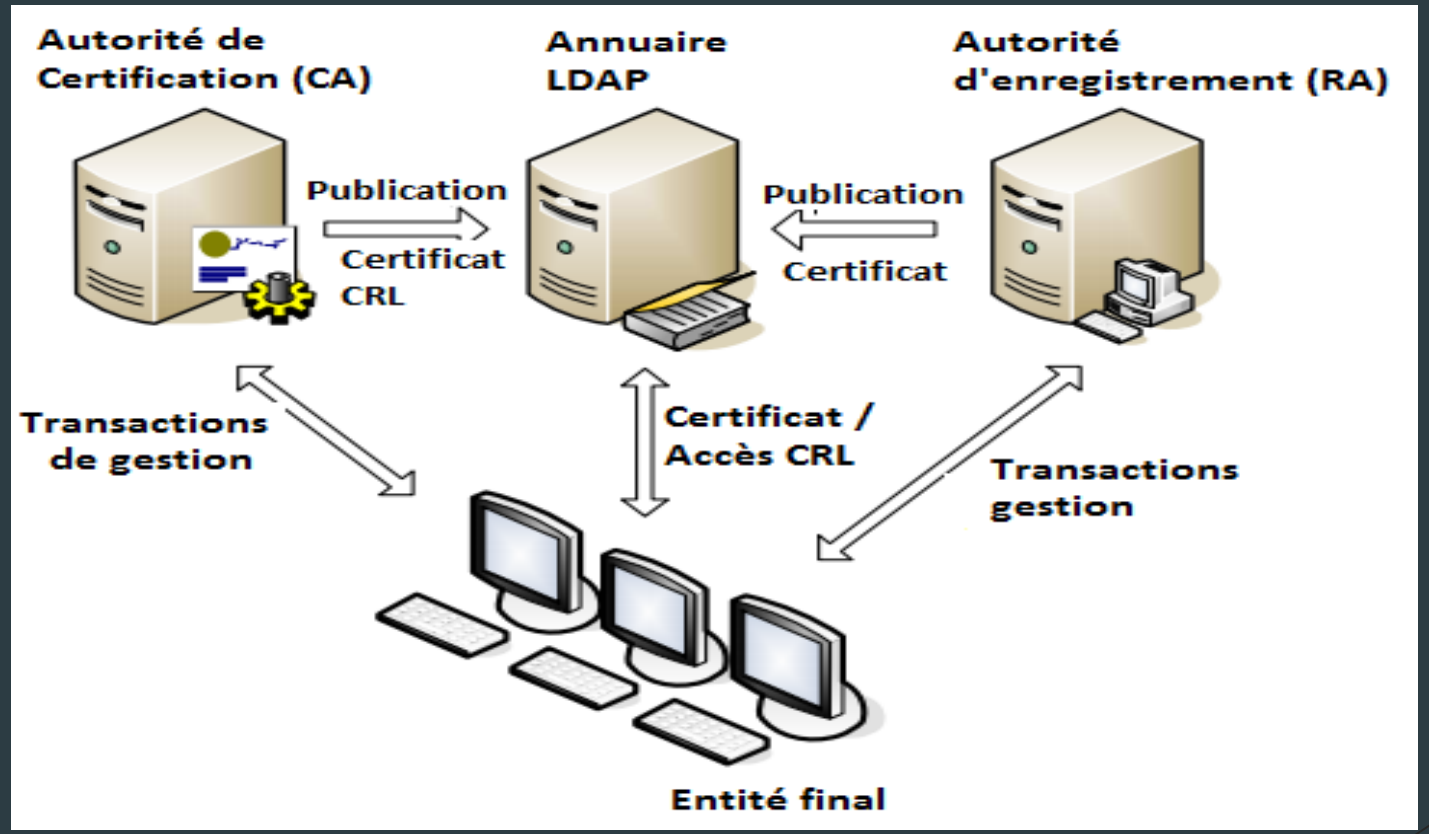
- L'annuaire est un rassemblement structuré des données sur des machines, des ressources, et des personnes.
- L'annuaire électronique est un type de base de données spécifique permettant de sauvegarder les clés publiques de chaque utilisateur et offrant la possibilité de recherche selon des critères prédéfinis.
- L'annuaire permet à stocker et diffuser des certificats dans une PKI. La plupart des annuaires existants au format LDAP (*Lightweight Directory Access Protocol*).

Annuaire électronique LDAP

- LDAP est un service d'annuaire dérivé de la norme X.500.
- C'est un mécanisme permettant la mise en œuvre, la publication et la distribution des certificats.
- La structure de l'annuaire LDAP est basée sur la représentation hiérarchique des objets nommés. C'est un arbre, où chaque nœud comprend: un identifiant unique (*DN: Distinguished Name*), un ou plusieurs classes (*objectclass*) définissant les attributs possibles, et des attributs, couple nom et sa valeur.

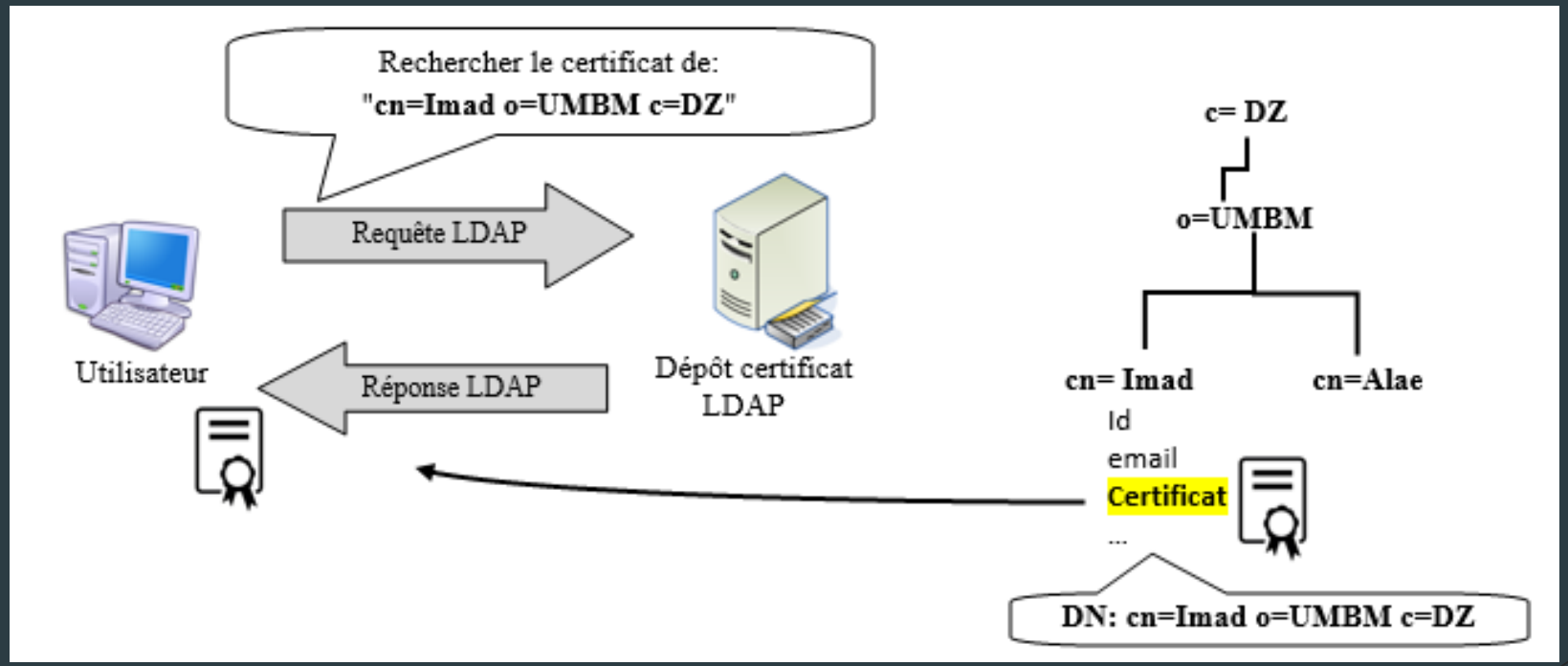
Annuaire électronique LDAP

- Architecture PKI avec LDAP



Annuaire électronique LDAP

- Accès à un certificat par LDAP



Service d’authentification **X509**

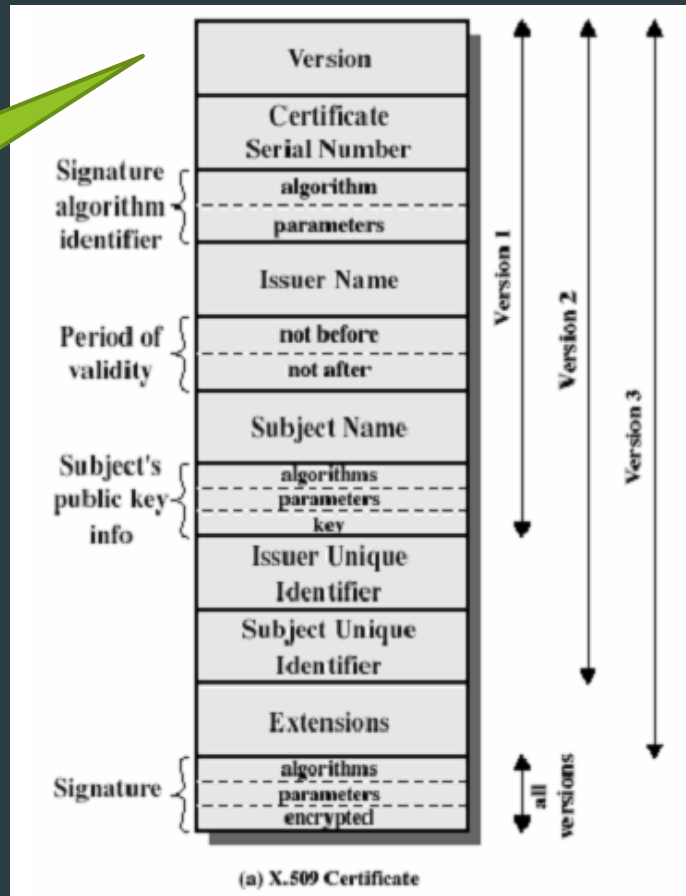
- Les formats des certificats électroniques les plus utilisés actuellement sont: X509 et OpenPGP.
- Le service d'authentification X509 s’agit d’une partie de la norme de service d’annuaire X.500 et il définit dans la norme RFC 5280.
- Le service définit le cadre pour des services d’authentification, internationalement admis pour construire un certificat de clé publique.

Service d’authentification **X509**

- Un certificat X.509 est un certificat numérique qui utilise la norme internationale d'infrastructure de clé publique X.509 (PKI) pour vérifier qu'une clé publique appartient à l'identité de l'utilisateur, de l'ordinateur ou du service contenue dans le certificat.

Service d'authentification **X509** Structure du certificat

version du certificat : 1, 2 ou 3,

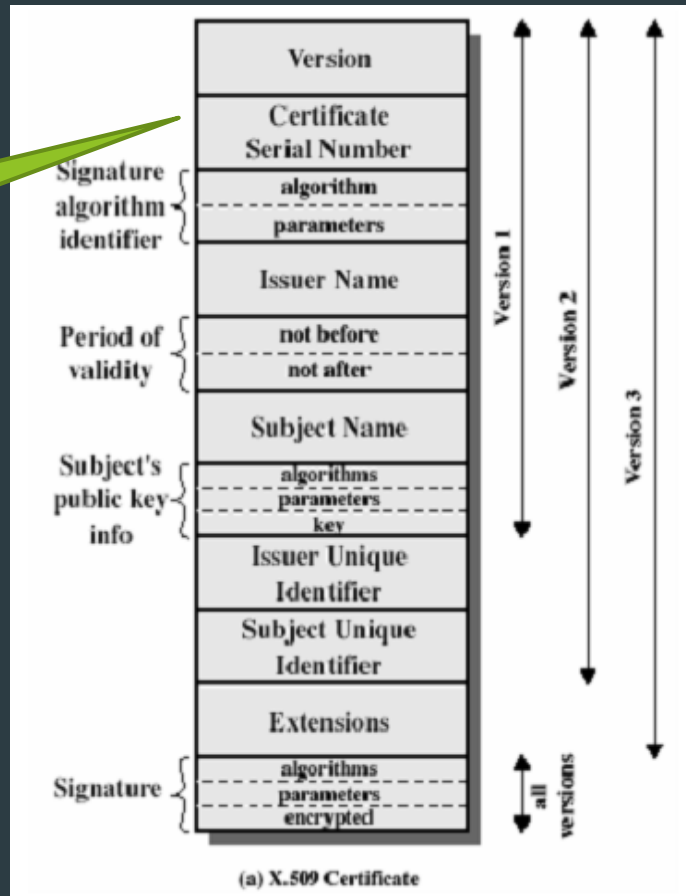


(a) X.509 Certificate

```
Certificate:
  Data:
    Version: v3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: PKCS #1 MD5 With RSA Encryption
    Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US
    Validity:
      Not Before: Fri Oct 17 18:36:25 1997
      Not After: Sun Oct 17 18:36:25 1999
    Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US
    Subject Public Key Info:
      Algorithm: PKCS #1 RSA Encryption
      Public Key:
        Modulus:
          00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
          ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
          43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
          98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
          73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
          9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
          7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
          91:f4:15
        Public Exponent: 65537 (0x10001)
    Extensions:
      Identifier: Certificate Type
        Critical: no
        Certified Usage:
          SSL Client
      Identifier: Authority Key Identifier
        Critical: no
        Key Identifier:
          f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
          26:c9
  Signature:
    Algorithm: PKCS #1 MD5 With RSA Encryption
    Signature:
      6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
      30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
      f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
      2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
      b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:
      4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:
      dd:c4
```

Service d'authentification **X509**
Structure du certificat

Numéro de série unique pour l'autorité de confiance qui a établi le certificat qui l'identifie de façon unique

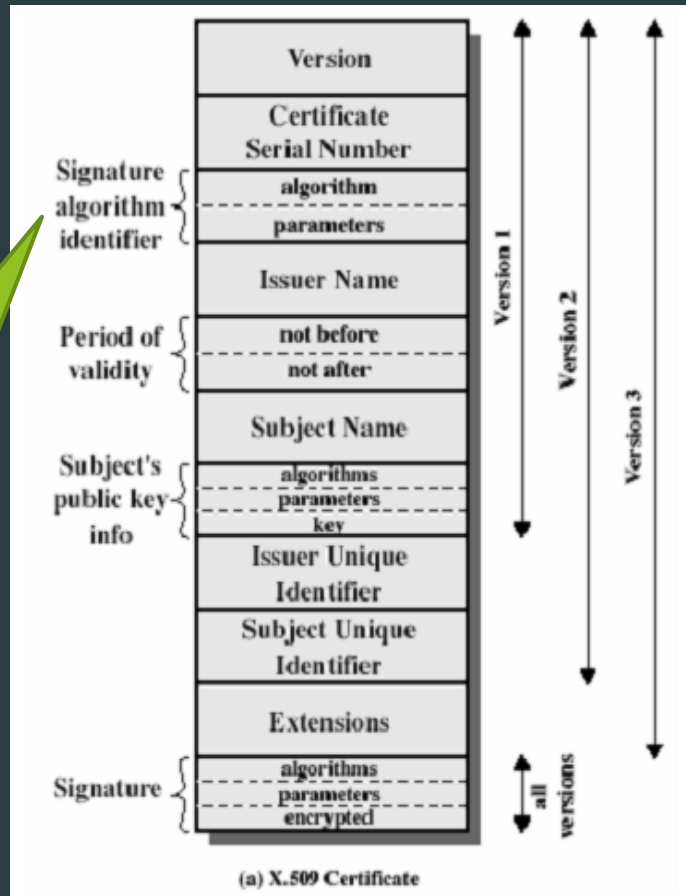


(a) X.509 Certificate

```
Certificate:
  Data:
    Version: v3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: PKCS #1 MD5 With RSA Encryption
    Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US
    Validity:
      Not Before: Fri Oct 17 18:36:25 1997
      Not After: Sun Oct 17 18:36:25 1999
    Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US
    Subject Public Key Info:
      Algorithm: PKCS #1 RSA Encryption
      Public Key:
        Modulus:
          00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
          ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
          43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
          98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
          73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
          9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
          7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
          91:f4:15
        Public Exponent: 65537 (0x10001)
    Extensions:
      Identifier: Certificate Type
        Critical: no
        Certified Usage:
          SSL Client
      Identifier: Authority Key Identifier
        Critical: no
        Key Identifier:
          f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
          26:c9
  Signature:
    Algorithm: PKCS #1 MD5 With RSA Encryption
    Signature:
      6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
      30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
      f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
      2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
      b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:
      4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:
      dd:c4
```

Service d'authentification **X509** Structure du certificat

Les algorithmes utilisés pour signer le certificat. Exemple : RSA with SHA

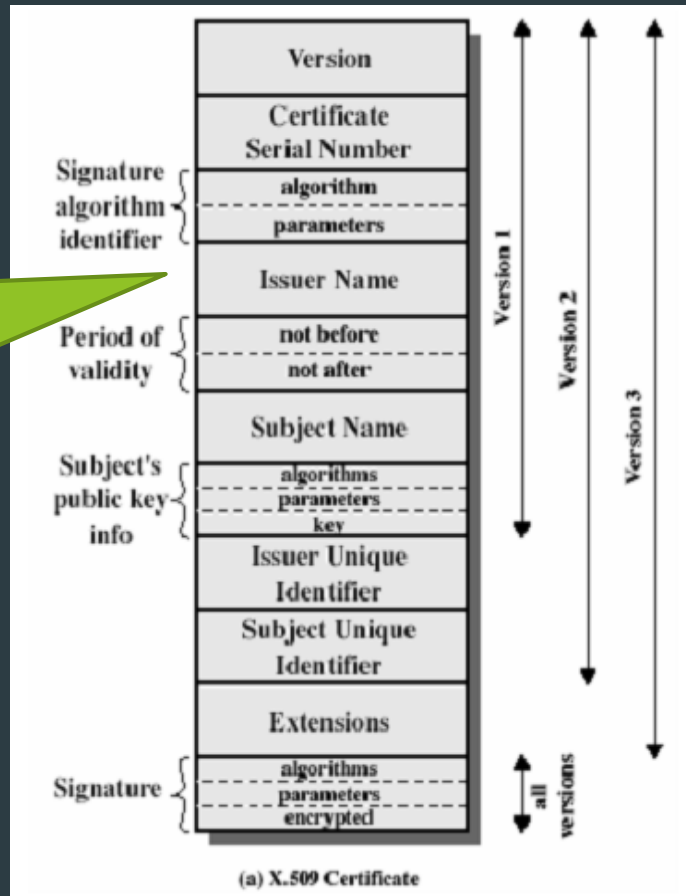


(a) X.509 Certificate

```
Certificate:
  Data:
    Version: v3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: PKCS #1 MD5 With RSA Encryption
    Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US
    Validity:
      Not Before: Fri Oct 17 18:36:25 1997
      Not After: Sun Oct 17 18:36:25 1999
    Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US
    Subject Public Key Info:
      Algorithm: PKCS #1 RSA Encryption
      Public Key:
        Modulus:
          00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
          ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
          43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
          98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
          73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
          9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
          7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
          91:f4:15
        Public Exponent: 65537 (0x10001)
    Extensions:
      Identifier: Certificate Type
        Critical: no
        Certified Usage:
          SSL Client
      Identifier: Authority Key Identifier
        Critical: no
        Key Identifier:
          f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
          26:c9
  Signature:
    Algorithm: PKCS #1 MD5 With RSA Encryption
    Signature:
      6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
      30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
      f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
      2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
      b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:
      4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:
      dd:c4
```

Service d'authentification **X509**
Structure du certificat

Nom de l'émetteur du certificat

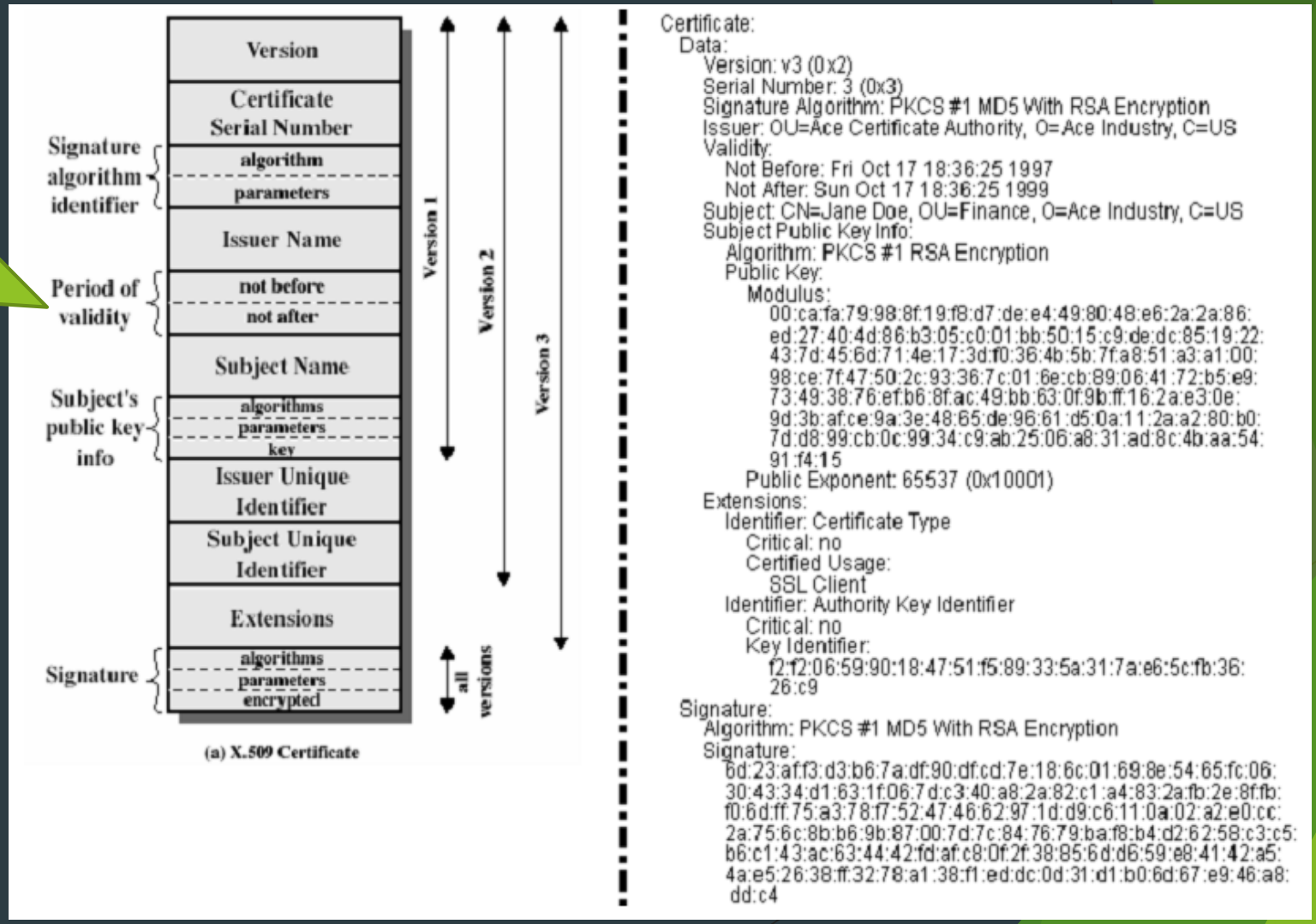


(a) X.509 Certificate

```
Certificate:
  Data:
    Version: v3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: PKCS #1 MD5 With RSA Encryption
    Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US
    Validity:
      Not Before: Fri Oct 17 18:36:25 1997
      Not After: Sun Oct 17 18:36:25 1999
    Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US
    Subject Public Key Info:
      Algorithm: PKCS #1 RSA Encryption
      Public Key:
        Modulus:
          00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
          ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
          43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
          98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
          73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
          9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
          7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
          91:f4:15
        Public Exponent: 65537 (0x10001)
    Extensions:
      Identifier: Certificate Type
        Critical: no
        Certified Usage:
          SSL Client
      Identifier: Authority Key Identifier
        Critical: no
        Key Identifier:
          f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
          26:c9
  Signature:
    Algorithm: PKCS #1 MD5 With RSA Encryption
    Signature:
      6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
      30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
      f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
      2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
      b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:
      4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:
      dd:c4
```

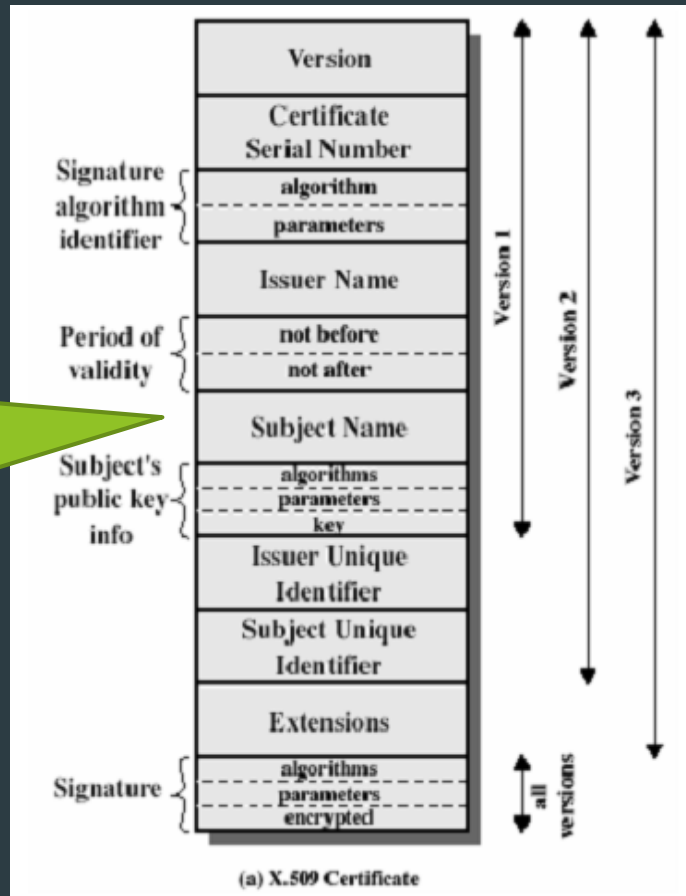
Service d'authentification **X509** Structure du certificat

Période de validité du certificat. Donne les dates de début et de fin de validité



Service d'authentification **X509** Structure du certificat

Nom de propriétaire du certificat

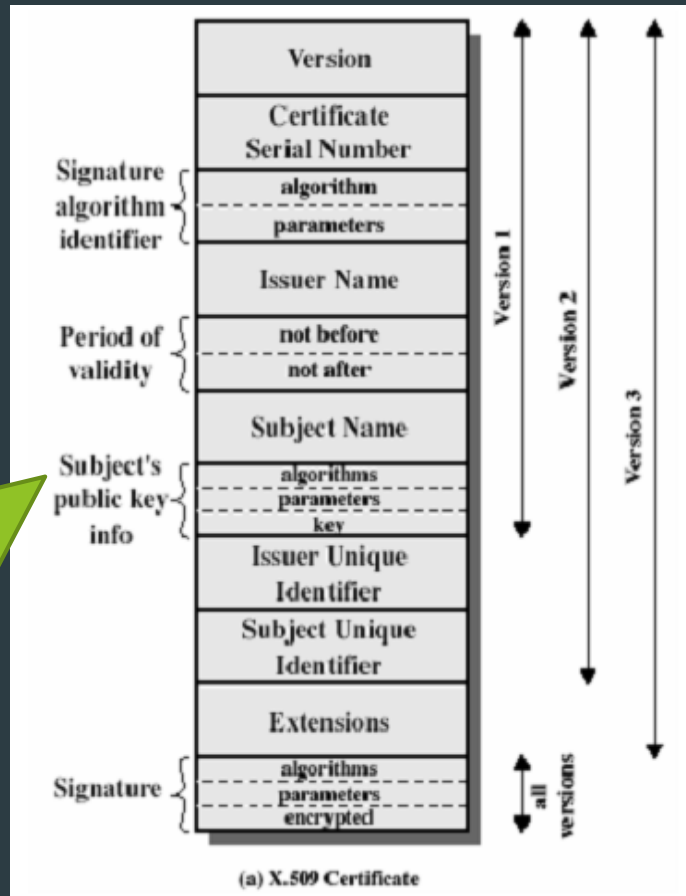


(a) X.509 Certificate

```
Certificate:
  Data:
    Version: v3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: PKCS #1 MD5 With RSA Encryption
    Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US
    Validity:
      Not Before: Fri Oct 17 18:36:25 1997
      Not After: Sun Oct 17 18:36:25 1999
    Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US
    Subject Public Key Info:
      Algorithm: PKCS #1 RSA Encryption
      Public Key:
        Modulus:
          00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
          ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
          43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
          98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
          73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
          9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
          7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
          91:f4:15
        Public Exponent: 65537 (0x10001)
    Extensions:
      Identifier: Certificate Type
        Critical: no
        Certified Usage:
          SSL Client
      Identifier: Authority Key Identifier
        Critical: no
        Key Identifier:
          f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
          26:c9
  Signature:
    Algorithm: PKCS #1 MD5 With RSA Encryption
    Signature:
      6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
      30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
      f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
      2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
      b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:
      4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:
      dd:c4
```

Service d'authentification **X509** Structure du certificat

la valeur de la clé publique du détenteur du certificat et les algorithmes avec lesquels elle doit être utilisée. Exemple : RSA with MD5)

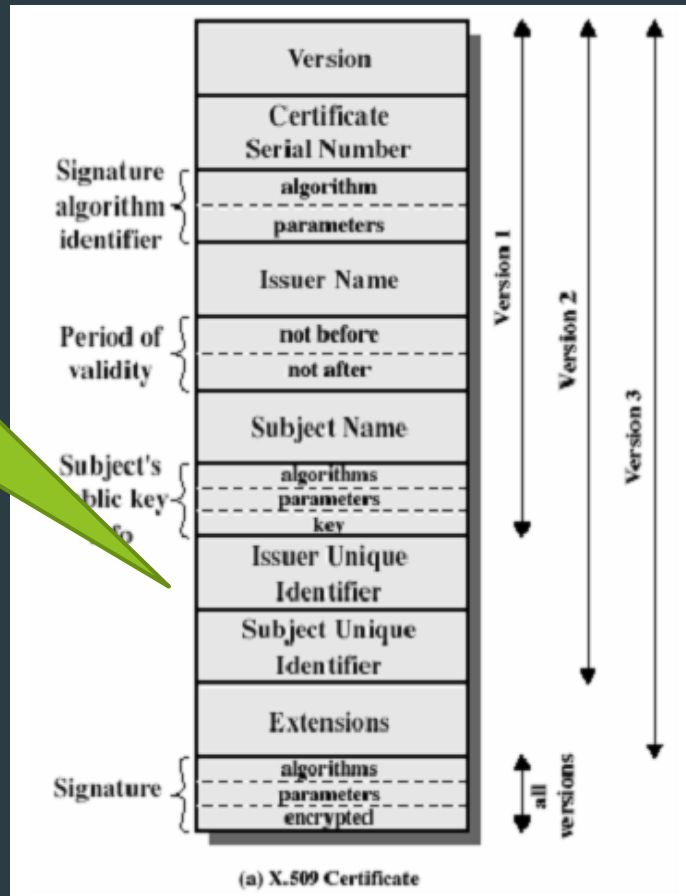


(a) X.509 Certificate

```
Certificate:
  Data:
    Version: v3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: PKCS #1 MD5 With RSA Encryption
    Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US
    Validity:
      Not Before: Fri Oct 17 18:36:25 1997
      Not After: Sun Oct 17 18:36:25 1999
    Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US
    Subject Public Key Info:
      Algorithm: PKCS #1 RSA Encryption
      Public Key:
        Modulus:
          00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
          ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
          43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
          98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
          73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
          9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
          7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
          91:f4:15
        Public Exponent: 65537 (0x10001)
    Extensions:
      Identifier: Certificate Type
        Critical: no
        Certified Usage:
          SSL Client
      Identifier: Authority Key Identifier
        Critical: no
        Key Identifier:
          f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
          26:c9
  Signature:
    Algorithm: PKCS #1 MD5 With RSA Encryption
    Signature:
      6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
      30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
      f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
      2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
      b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:
      4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:
      dd:c4
```

Service d'authentification **X509** Structure du certificat

Extensions optionnelles introduites avec la version 2 de X.509.

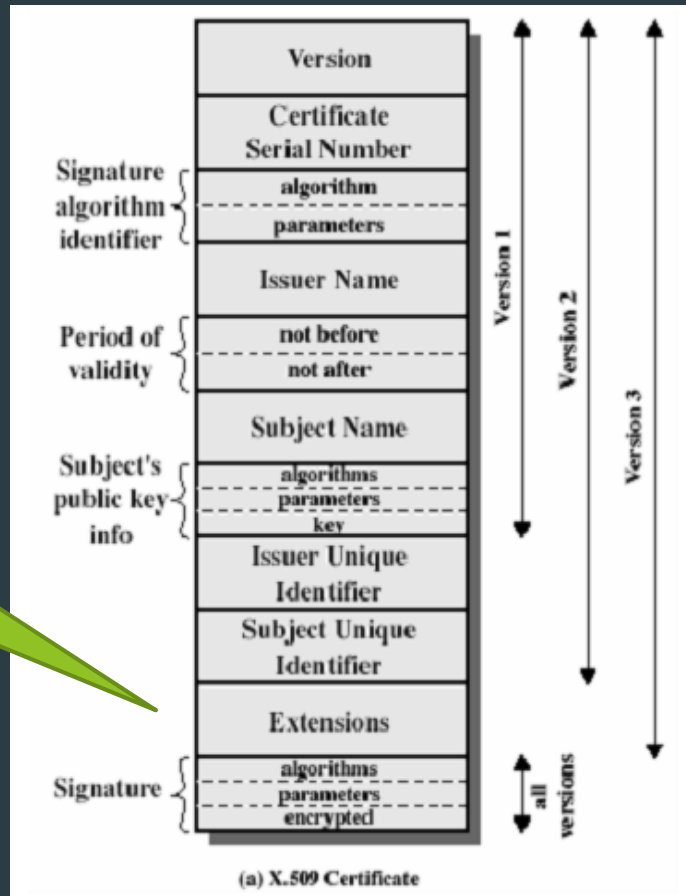


(a) X.509 Certificate

```
Certificate:
  Data:
    Version: v3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: PKCS #1 MD5 With RSA Encryption
    Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US
    Validity:
      Not Before: Fri Oct 17 18:36:25 1997
      Not After: Sun Oct 17 18:36:25 1999
    Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US
    Subject Public Key Info:
      Algorithm: PKCS #1 RSA Encryption
      Public Key:
        Modulus:
          00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
          ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
          43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
          98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
          73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
          9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
          7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
          91:f4:15
        Public Exponent: 65537 (0x10001)
    Extensions:
      Identifier: Certificate Type
        Critical: no
        Certified Usage:
          SSL Client
      Identifier: Authority Key Identifier
        Critical: no
        Key Identifier:
          f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
          26:c9
  Signature:
    Algorithm: PKCS #1 MD5 With RSA Encryption
    Signature:
      6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
      30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
      f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
      2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
      b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:
      4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:
      dd:c4
```

Service d'authentification **X509**
Structure du certificat

Extensions génériques optionnelles, introduites avec la version 3 de X.509.

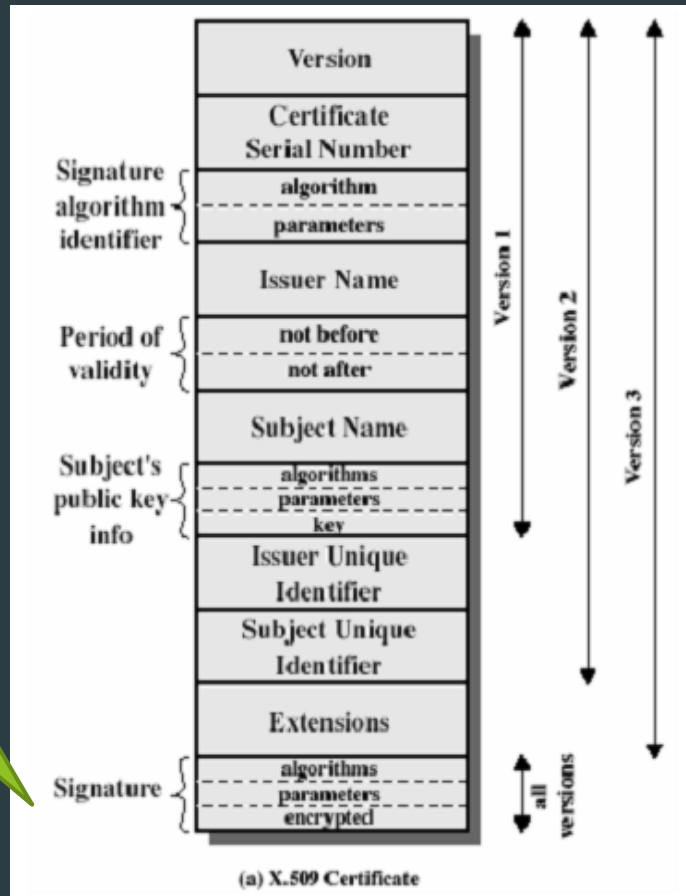


(a) X.509 Certificate

```
Certificate:
  Data:
    Version: v3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: PKCS #1 MD5 With RSA Encryption
    Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US
    Validity:
      Not Before: Fri Oct 17 18:36:25 1997
      Not After: Sun Oct 17 18:36:25 1999
    Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US
    Subject Public Key Info:
      Algorithm: PKCS #1 RSA Encryption
      Public Key:
        Modulus:
          00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
          ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
          43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
          98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
          73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
          9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
          7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
          91:f4:15
        Public Exponent: 65537 (0x10001)
    Extensions:
      Identifier: Certificate Type
        Critical: no
        Certified Usage:
          SSL Client
      Identifier: Authority Key Identifier
        Critical: no
        Key Identifier:
          f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
          26:c9
  Signature:
    Algorithm: PKCS #1 MD5 With RSA Encryption
    Signature:
      6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
      30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
      f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
      2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
      b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:
      4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:
      dd:c4
```

Service d'authentification **X509** Structure du certificat

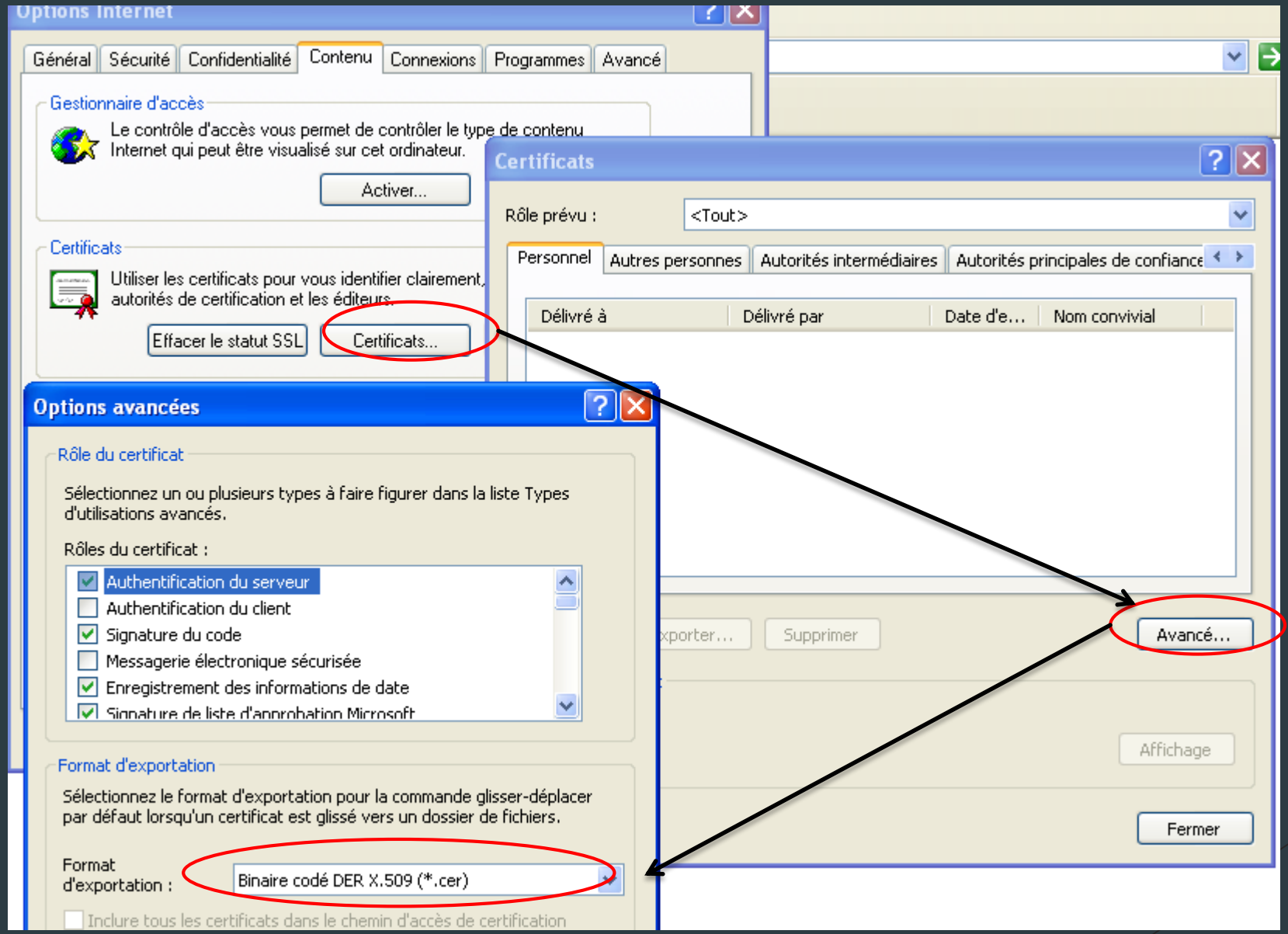
Signature numérique de la AC sur l'ensemble des champs précédents



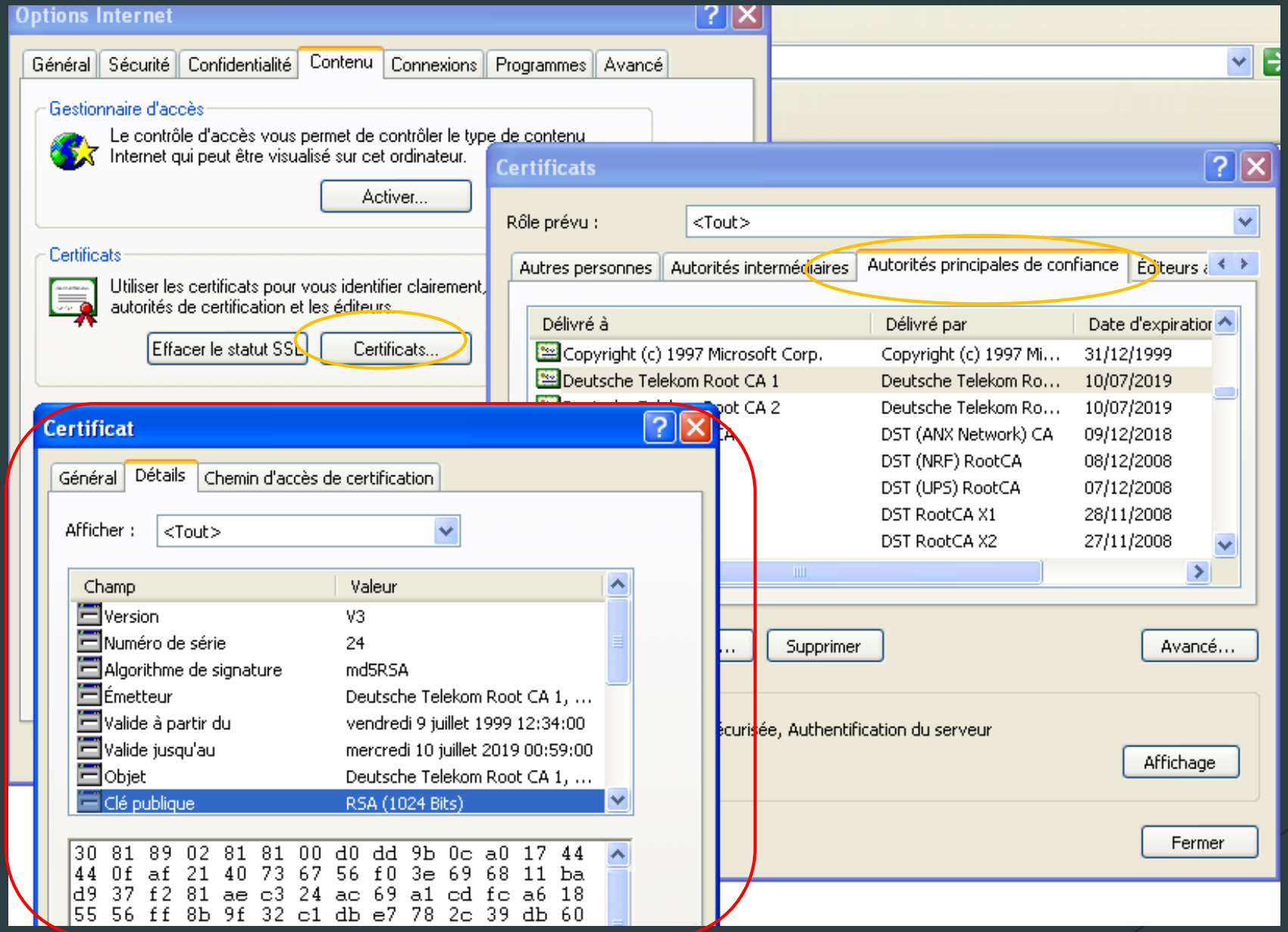
(a) X.509 Certificate

```
Certificate:
  Data:
    Version: v3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: PKCS #1 MD5 With RSA Encryption
    Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US
    Validity:
      Not Before: Fri Oct 17 18:36:25 1997
      Not After: Sun Oct 17 18:36:25 1999
    Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US
    Subject Public Key Info:
      Algorithm: PKCS #1 RSA Encryption
      Public Key:
        Modulus:
          00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
          ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
          43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
          98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
          73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
          9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
          7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
          91:f4:15
        Public Exponent: 65537 (0x10001)
    Extensions:
      Identifier: Certificate Type
        Critical: no
        Certified Usage:
          SSL Client
      Identifier: Authority Key Identifier
        Critical: no
        Key Identifier:
          f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
          26:c9
  Signature:
    Algorithm: PKCS #1 MD5 With RSA Encryption
    Signature:
      6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
      30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
      f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
      2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
      b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:
      4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:
      dd:c4
```

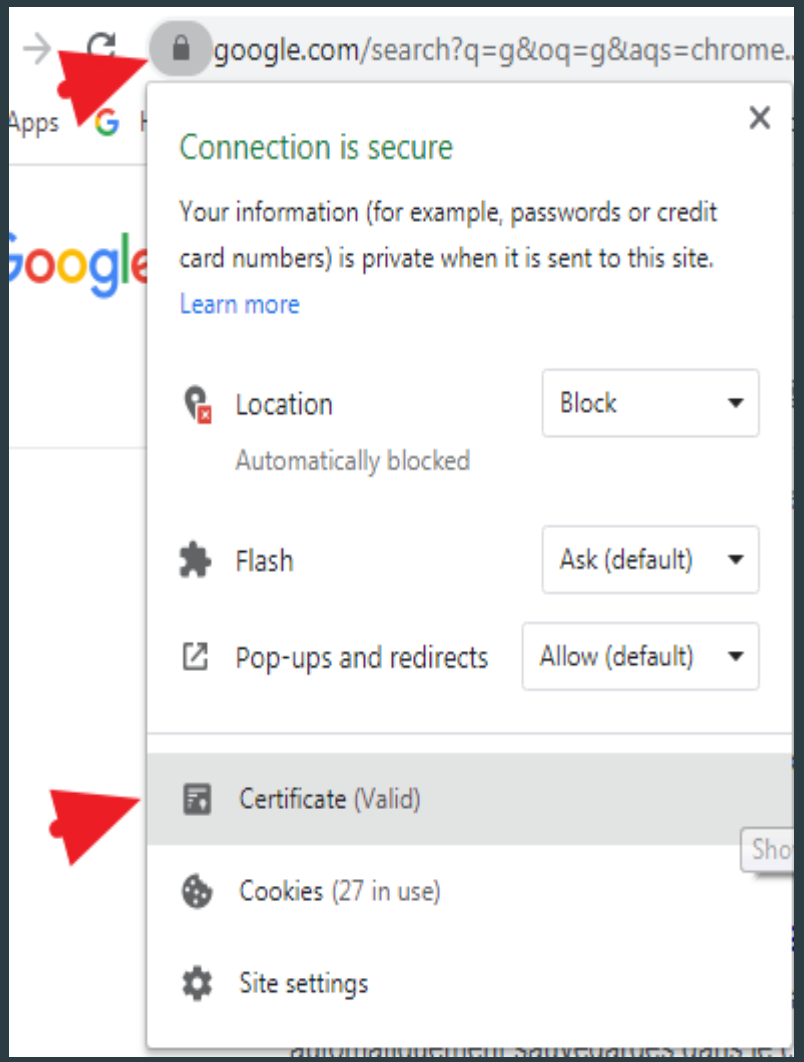
Pratique: Exemple de certificat

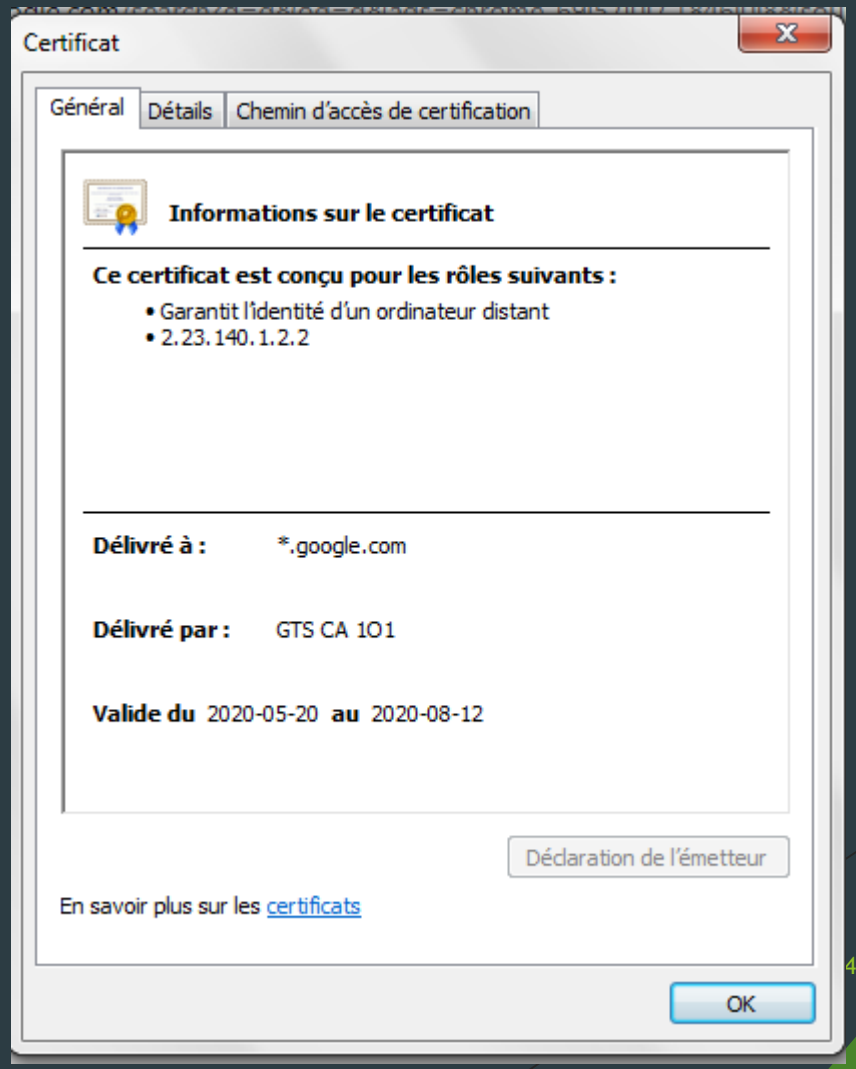


Pratique: Exemple de certificat



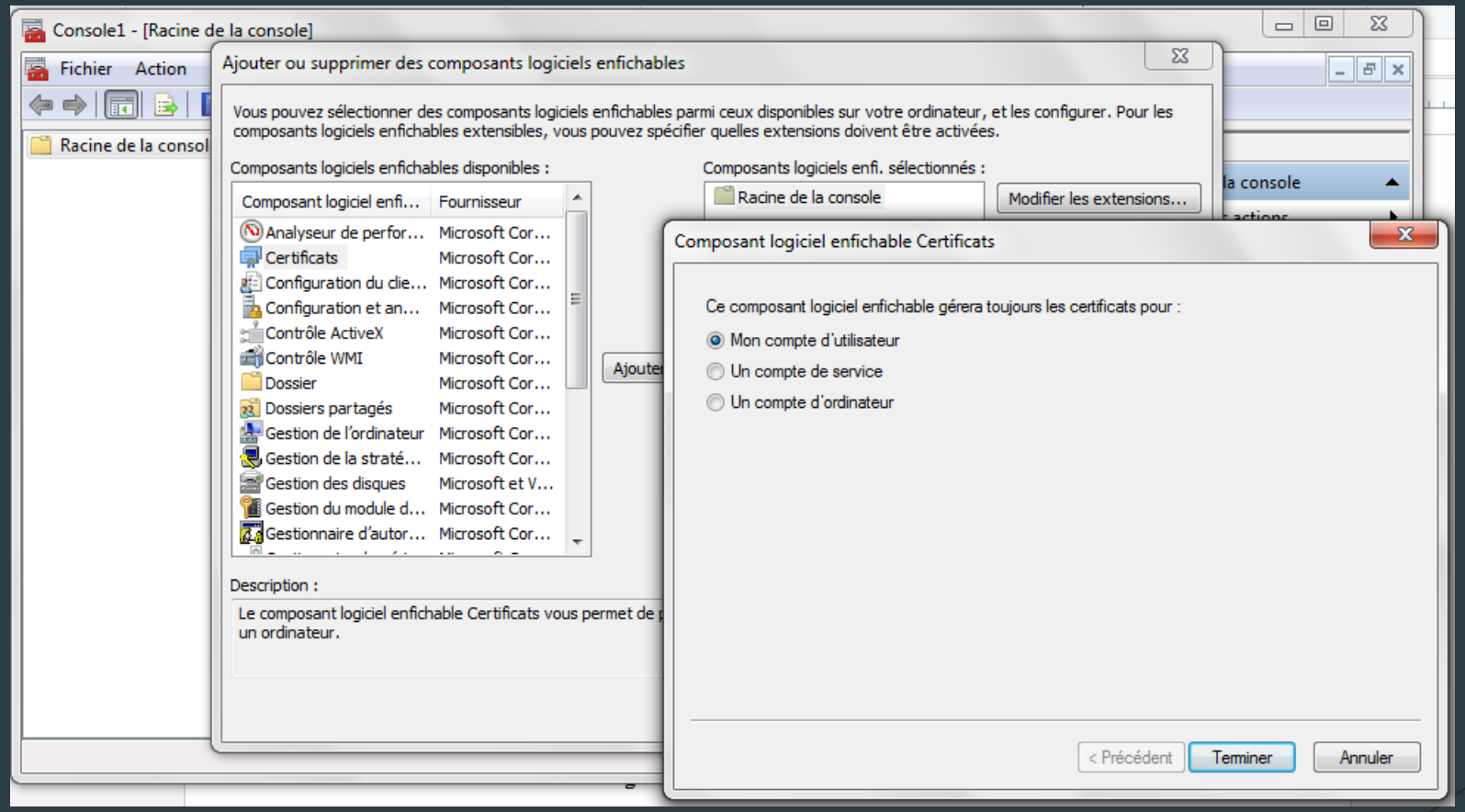
Pratique: Certificat Google





Pratique: Installation d'un certificat

- Installer un certificat depuis Windows Server avec la MMC de certificats



Lien