

Les certificats numériques

Dr. Noureddine Chikouche
Université de M'sila

<https://sites.google.com/view/chikouchenoureddine>

Plan du cours

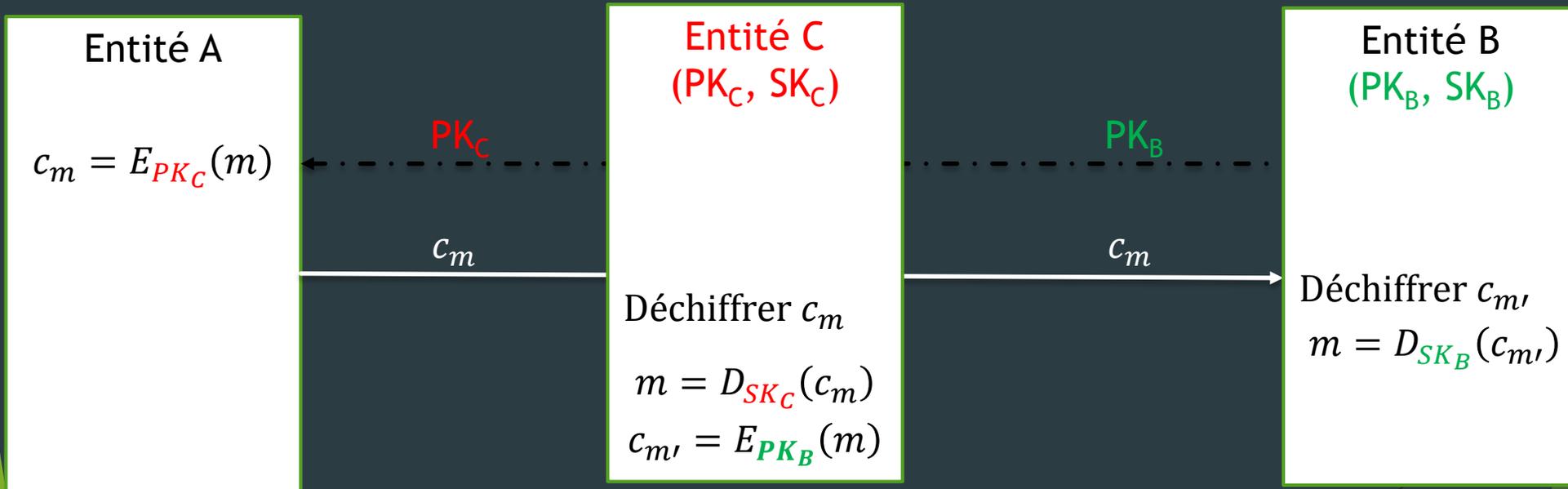
- ▶ Introduction
- ▶ Infrastructure de Gestion de Clés
- ▶ Certificats de clés publiques
- ▶ Annuaire électronique LDAP
- ▶ Service d'authentification X509

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.



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. ⁷

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.
- ▶ **Systeme 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.

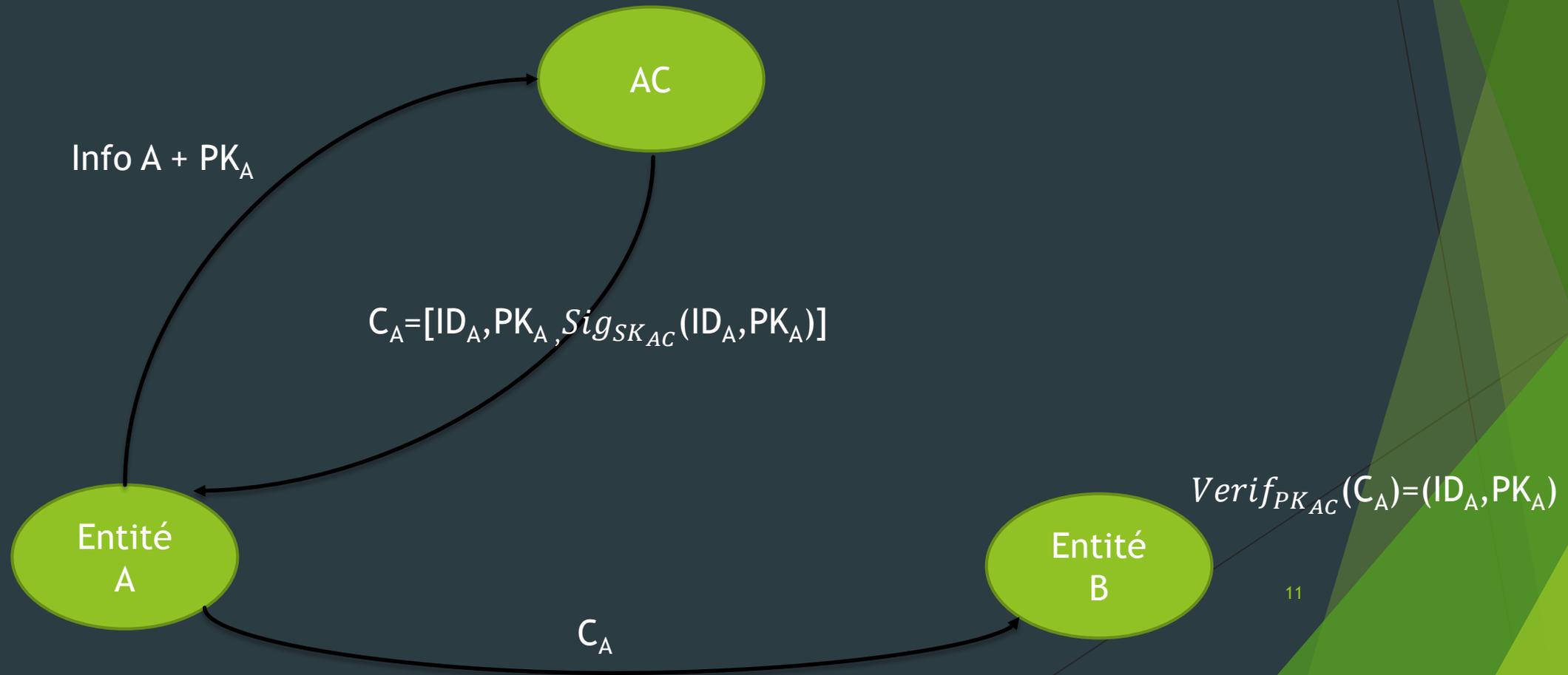
Certificats numériques

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 une autorité de certification (AC), ainsi que différentes informations la concernant (nom, email, etc...).
- ▶ Pour envoyer (IDA, PK_A), 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).

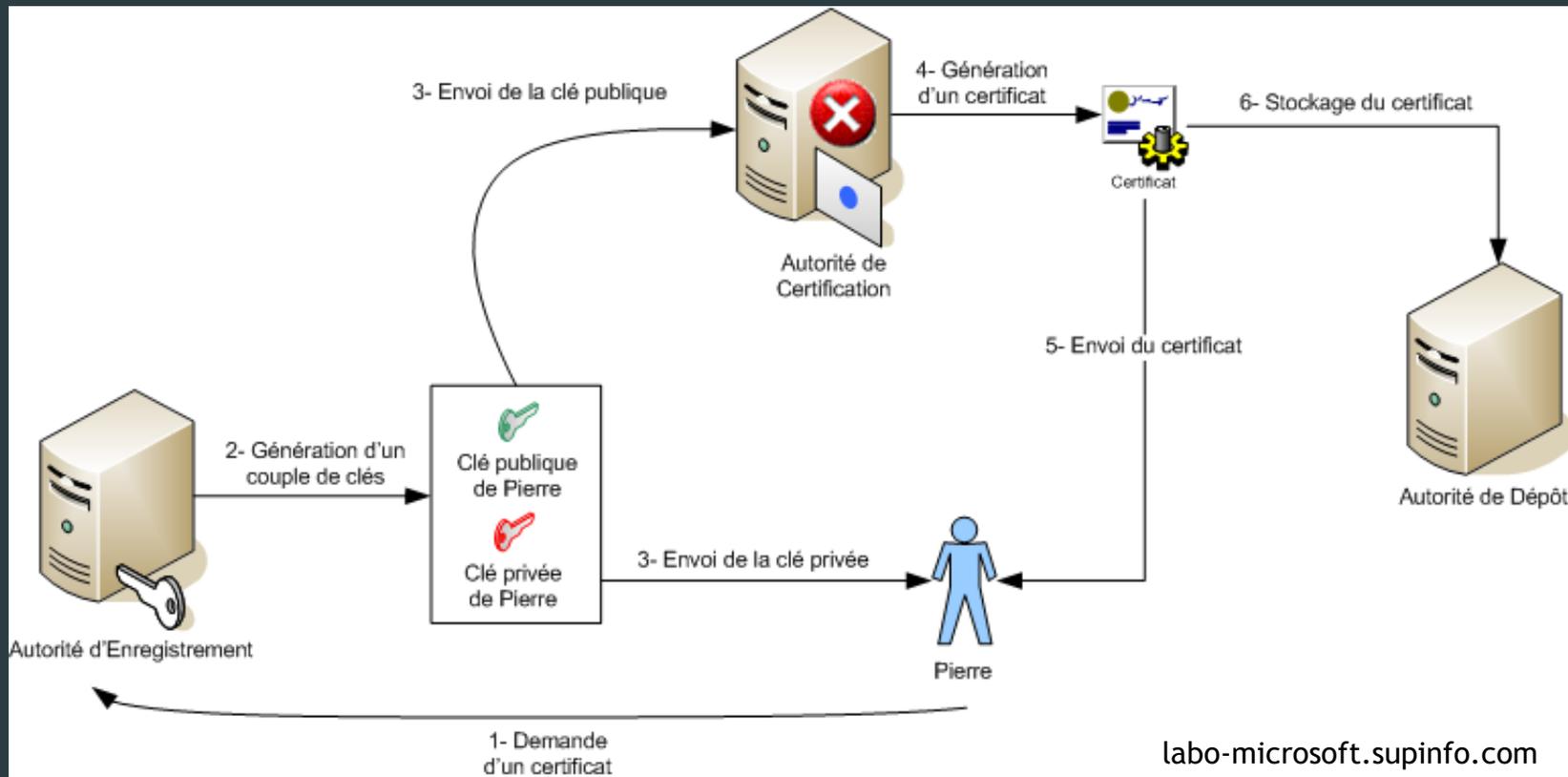
Certificats numériques

- ▶ 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'expiration.
- ▶ 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

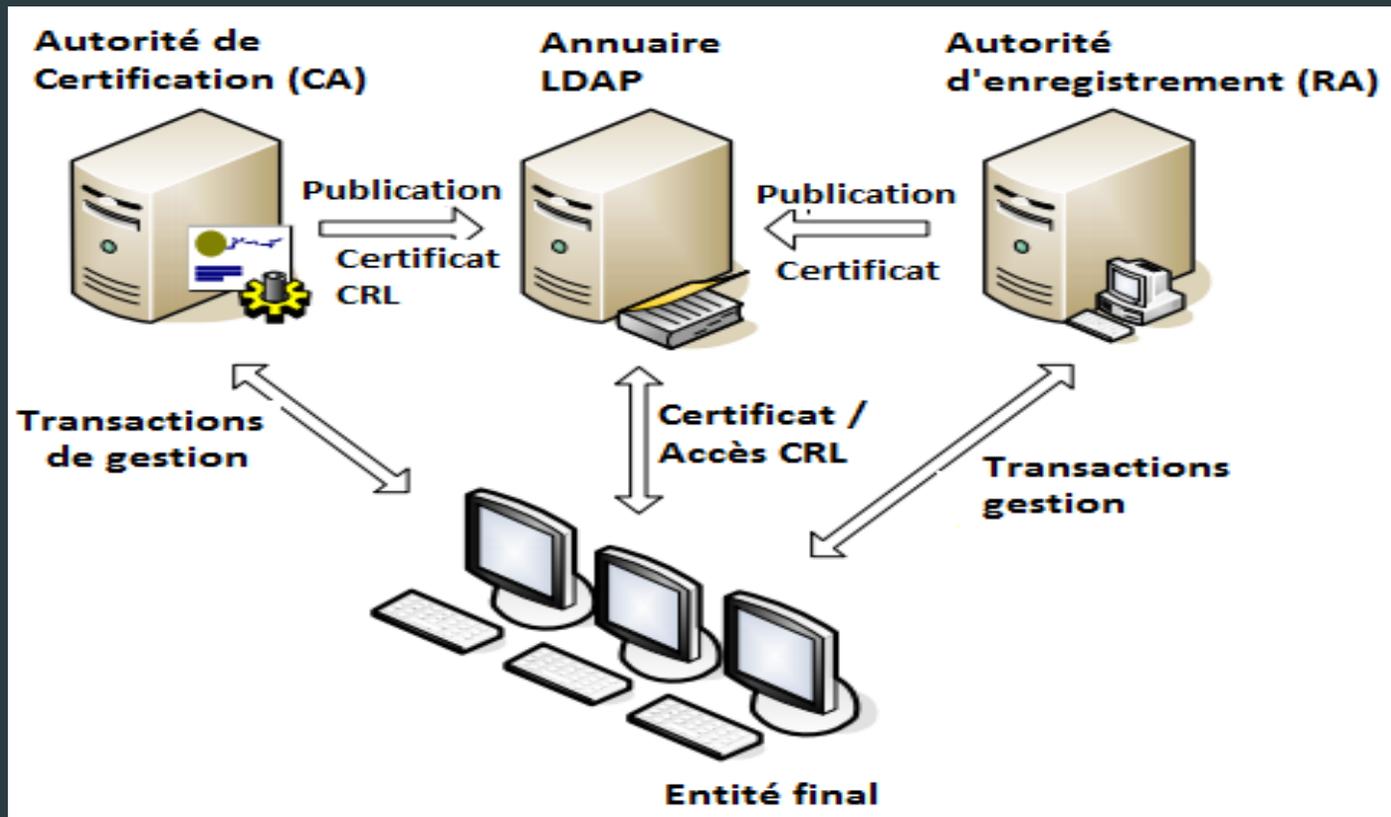
- ▶ L'annuaire est un rassemblement structuré des données sur des machines, des ressources, et des personnes.
- ▶ L'annuaire électronique est un type de base de données spécifique permettant de sauvegarder les clés publiques de chaque utilisateur et offrant la possibilité de recherche selon des critères 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.

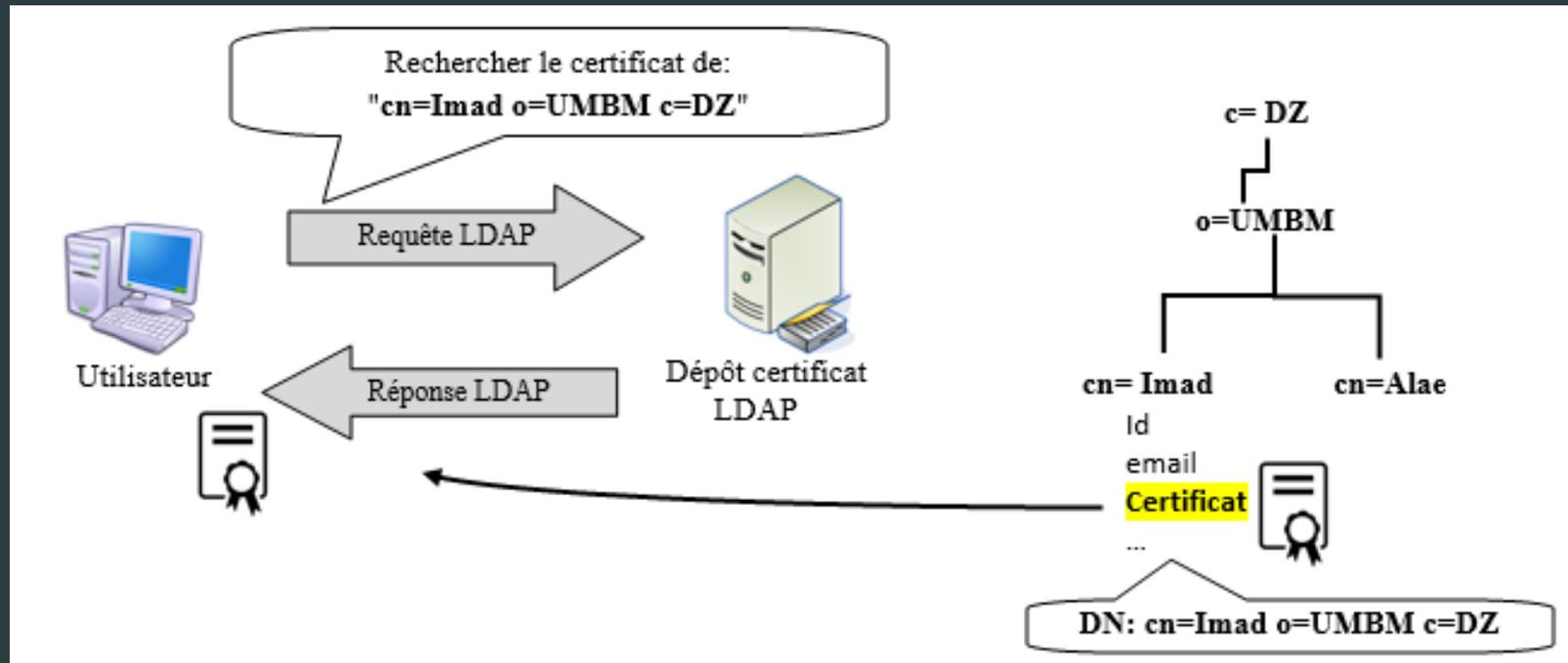
Annuaire électronique LDAP

► 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.

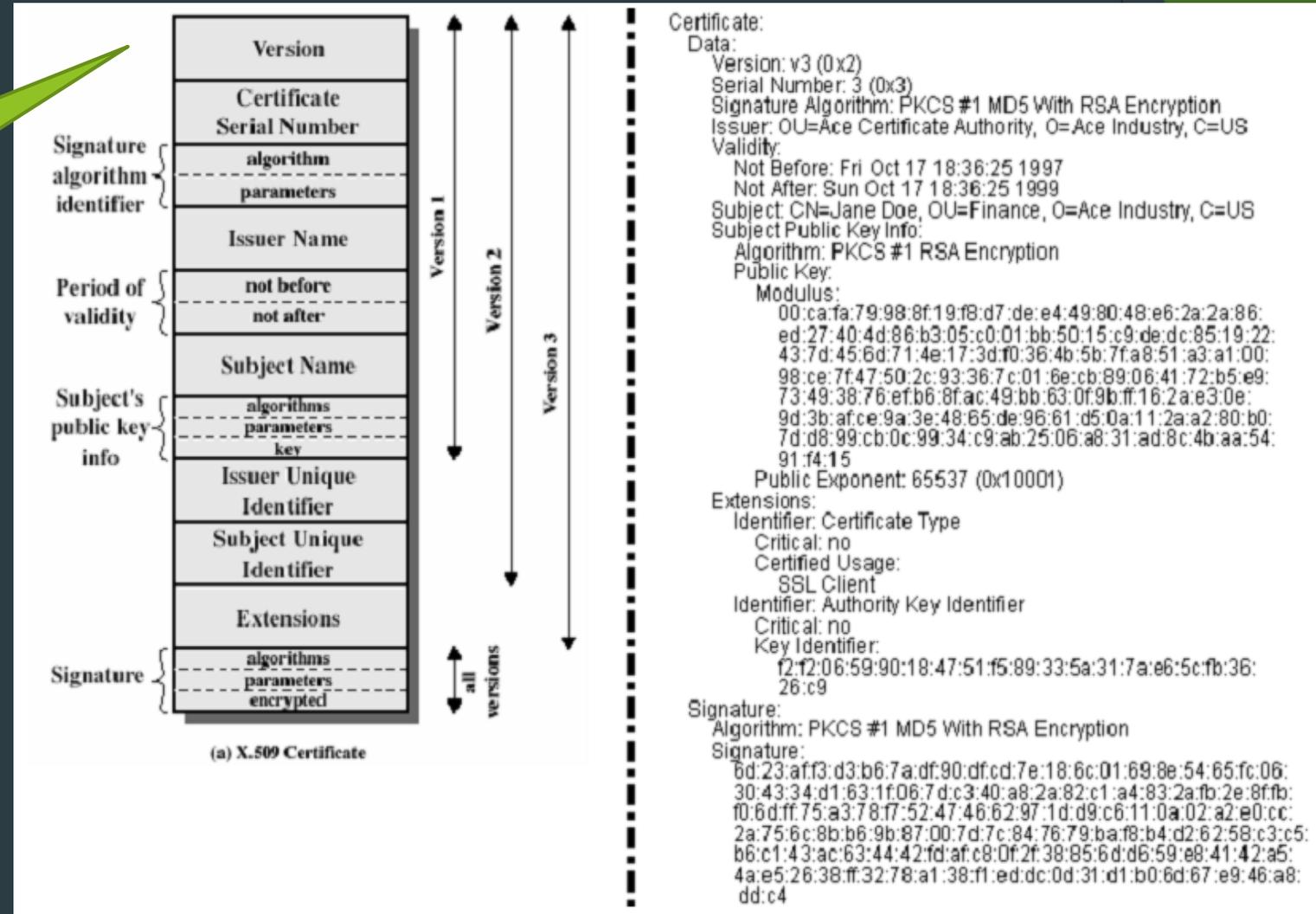
Service d'authentification X509

- ▶ 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

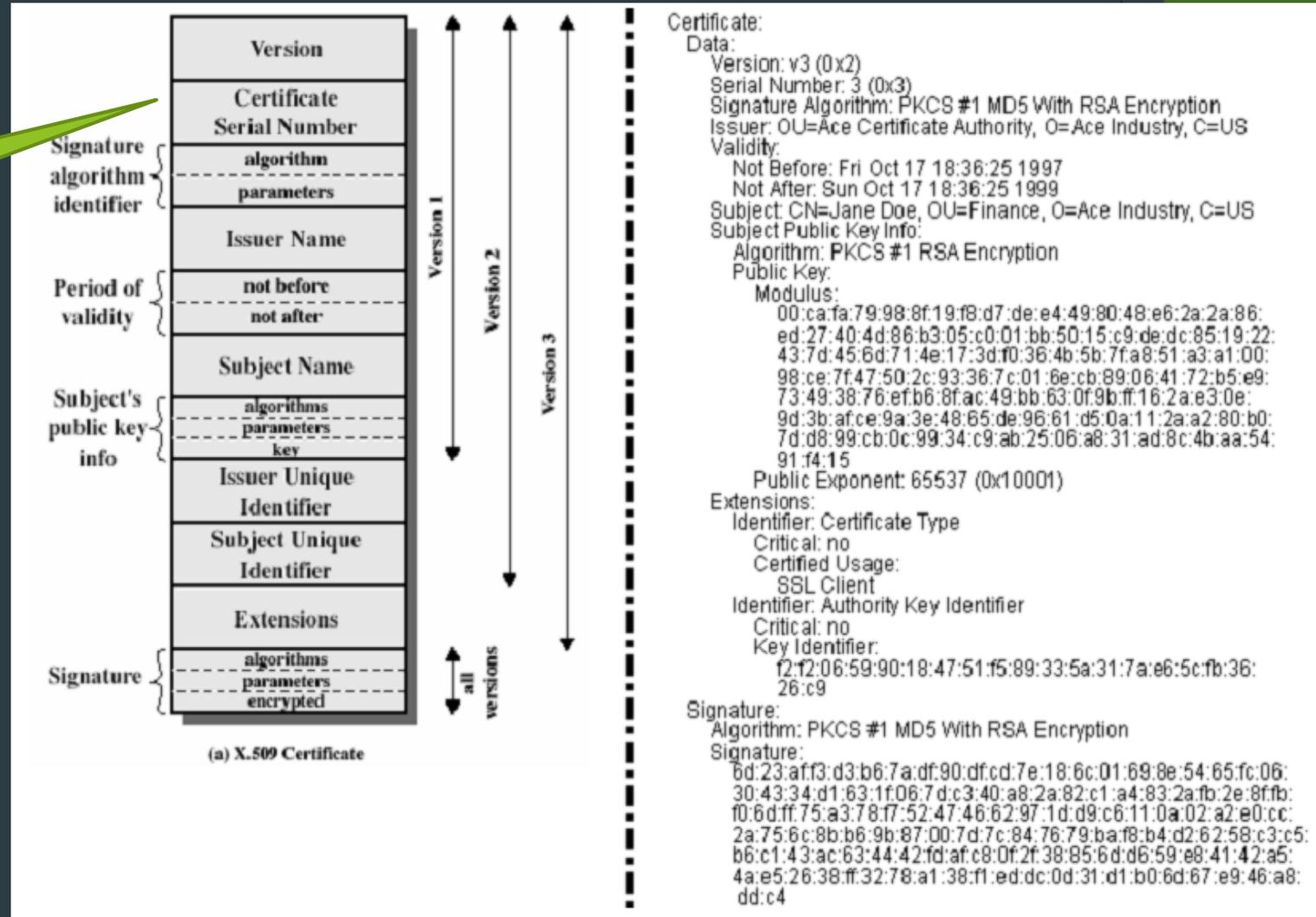
version du certificat : 1, 2 ou 3,



Service d'authentification X509

Structure du certificat

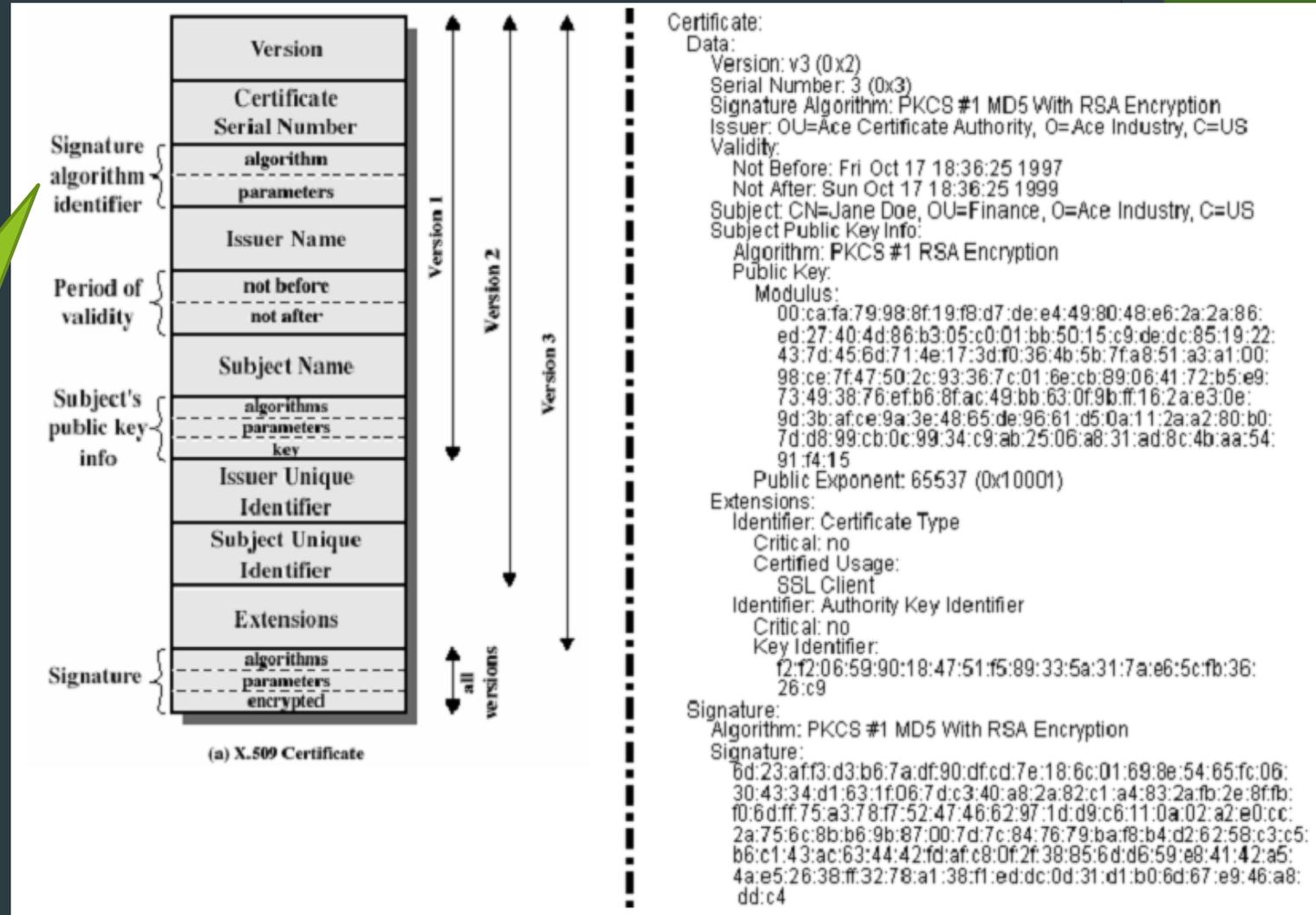
Numéro de série unique pour l'autorité de confiance qui a établi le certificat qui l'identifie de façon unique



Service d'authentification X509

Structure du certificat

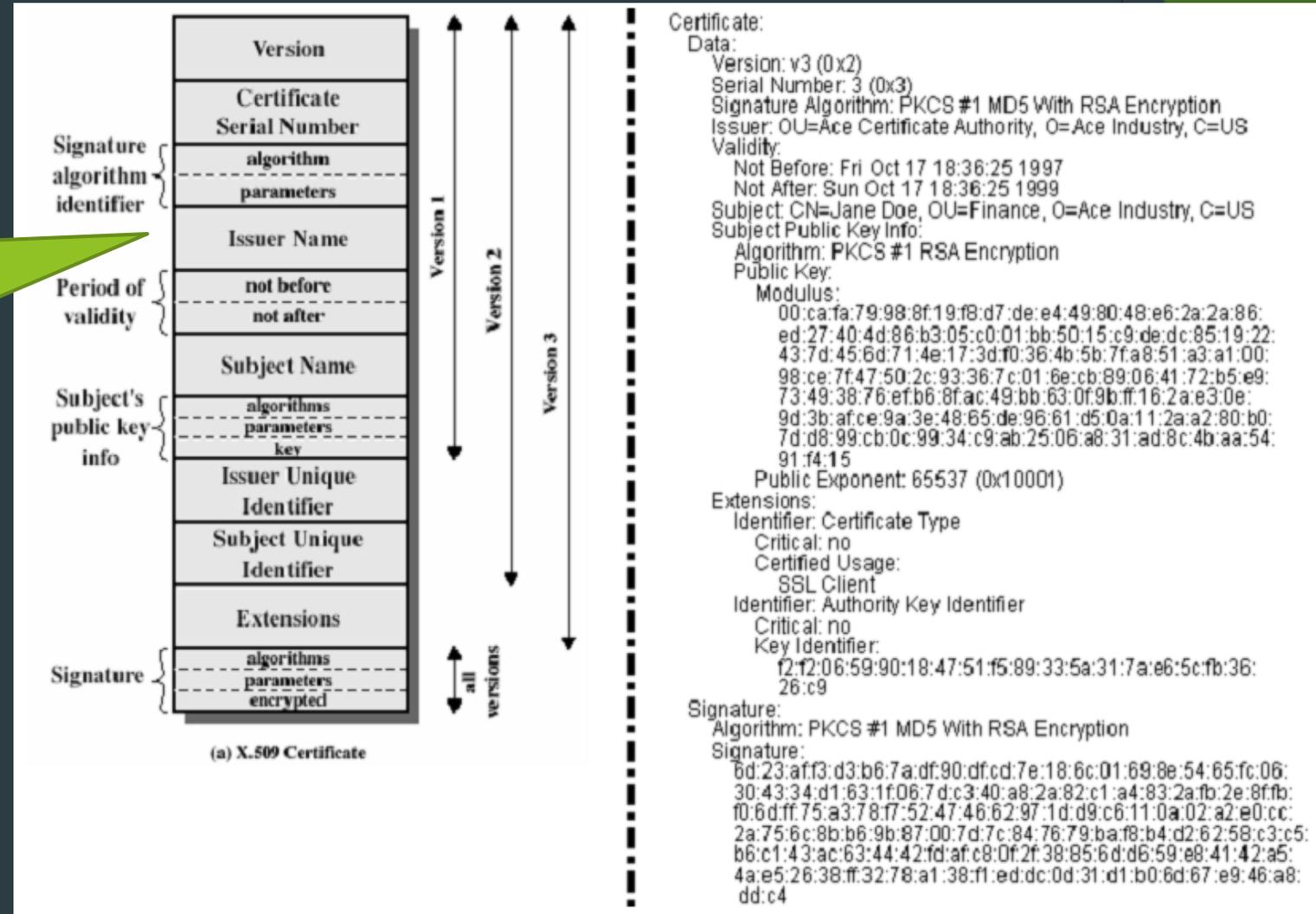
Les algorithmes utilisés pour signer le certificat.
Exemple : RSA with SHA



Service d'authentification X509

Structure du certificat

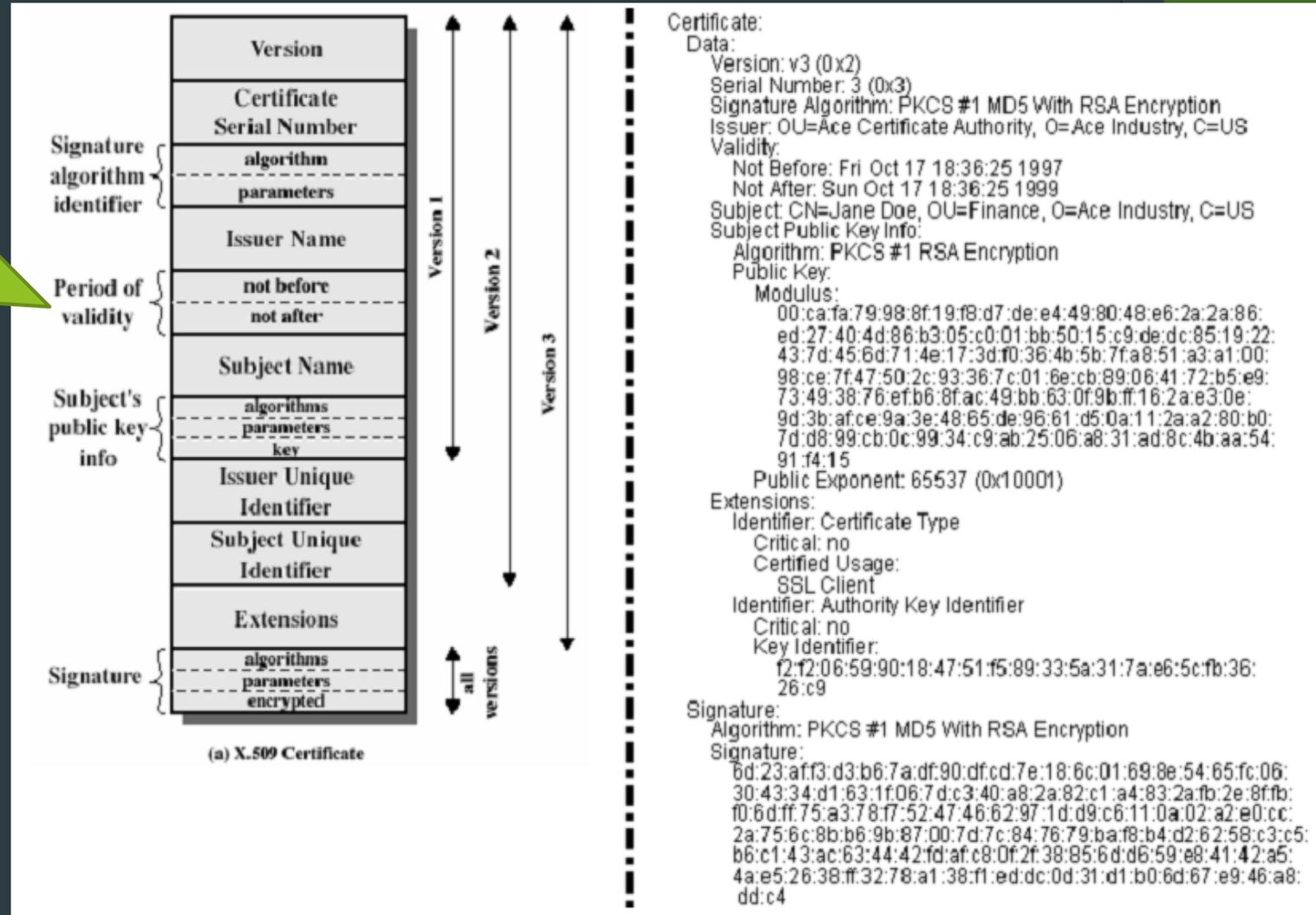
Nom de l'émetteur du certificat



Service d'authentification X509

Structure du certificat

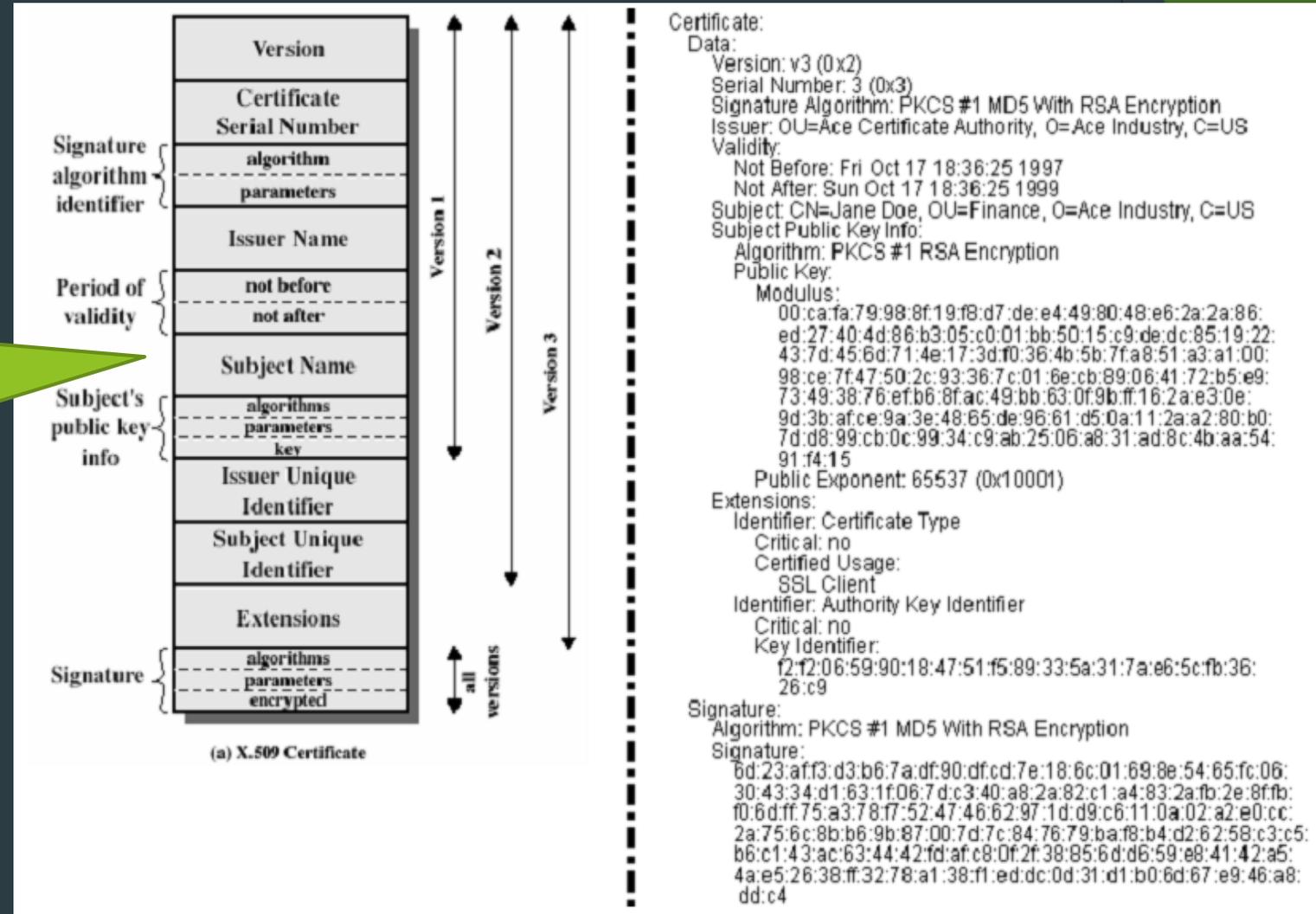
Période de validité du certificat. Donne les dates de début et de fin de validité



Service d'authentification X509

Structure du certificat

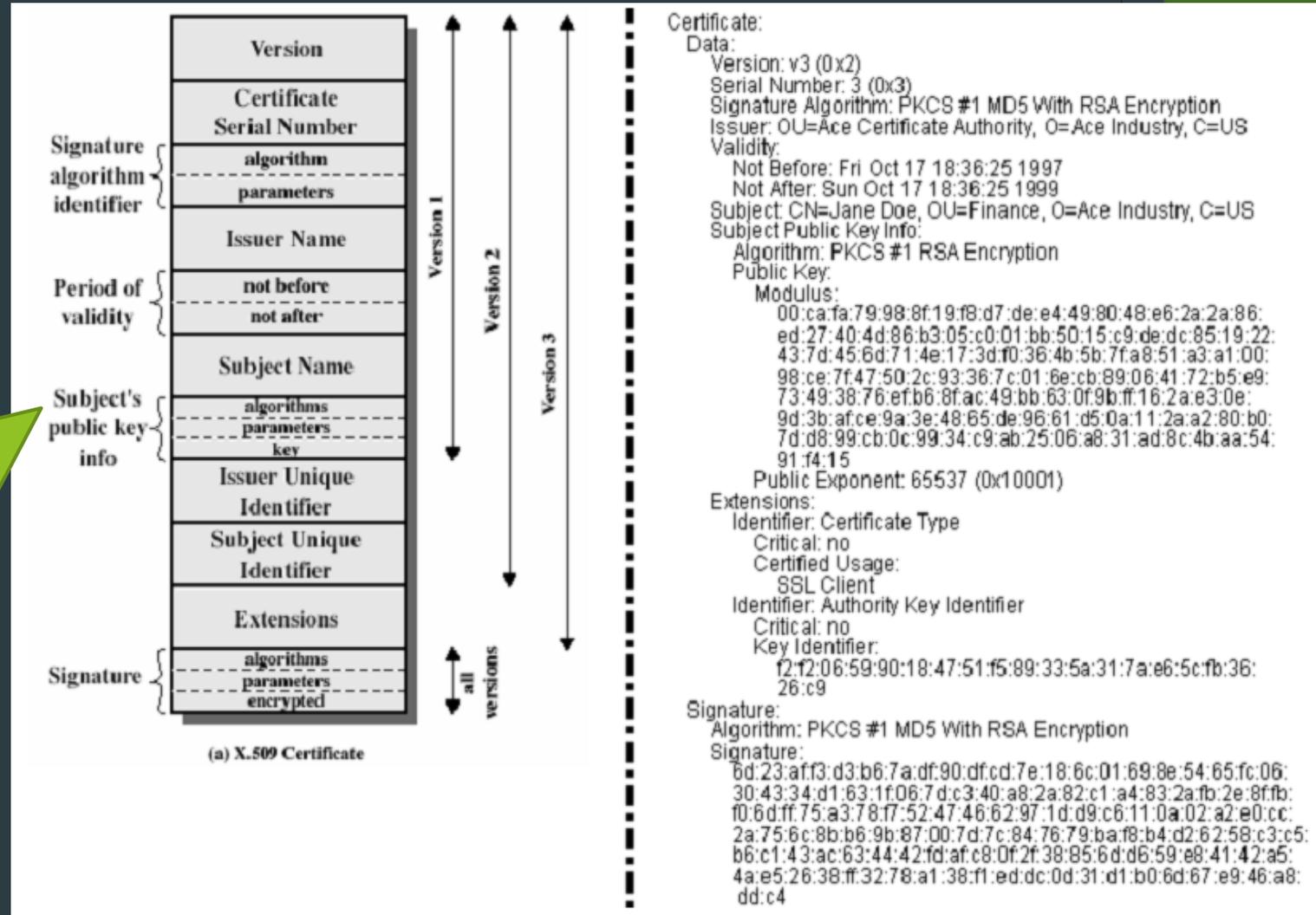
Nom de propriétaire du certificat



Service d'authentification X509

Structure du certificat

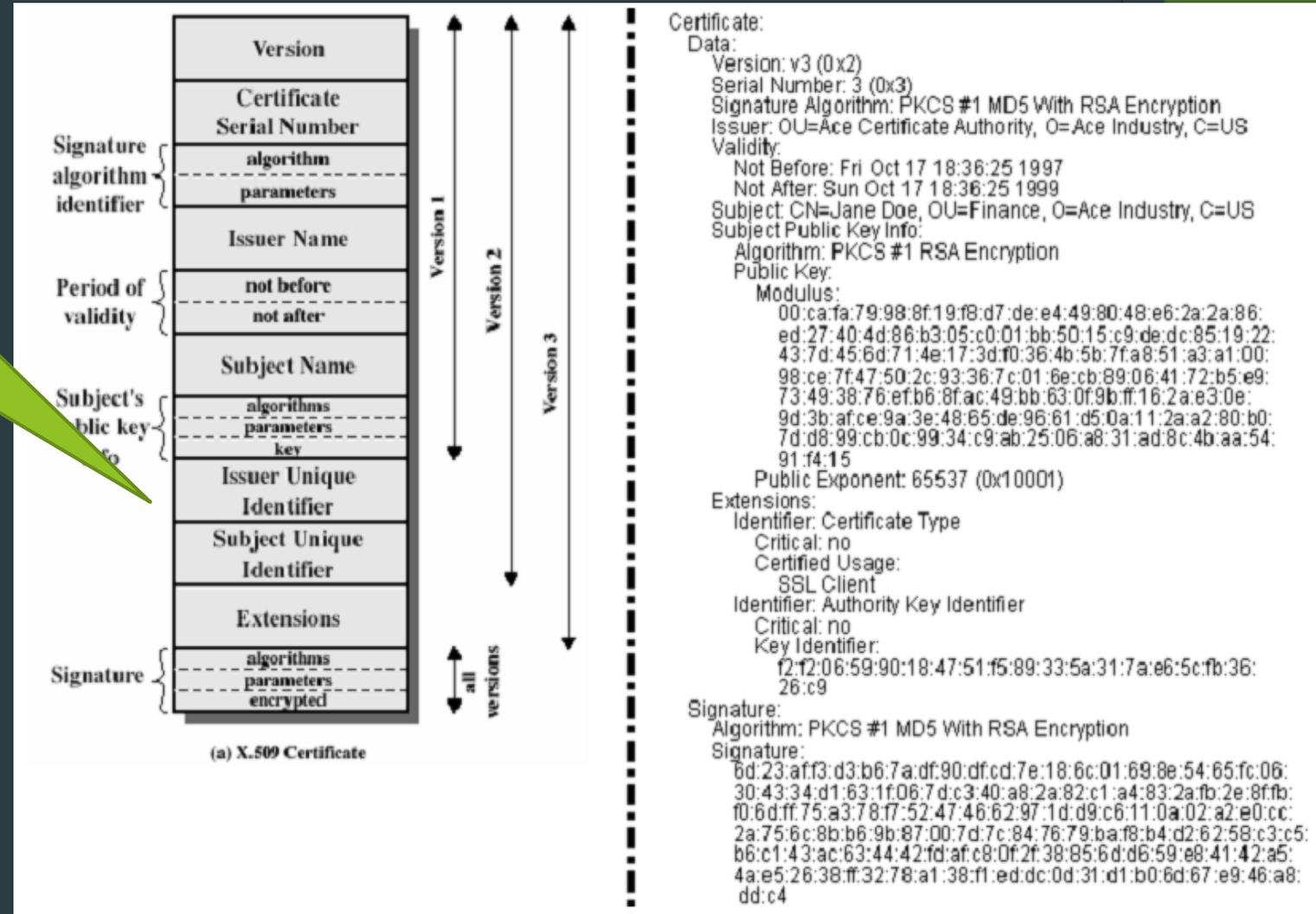
la valeur de la clé publique du détenteur du certificat et les algorithmes avec lesquels elle doit être utilisée. Exemple : RSA with MD5)



Service d'authentification X509

Structure du certificat

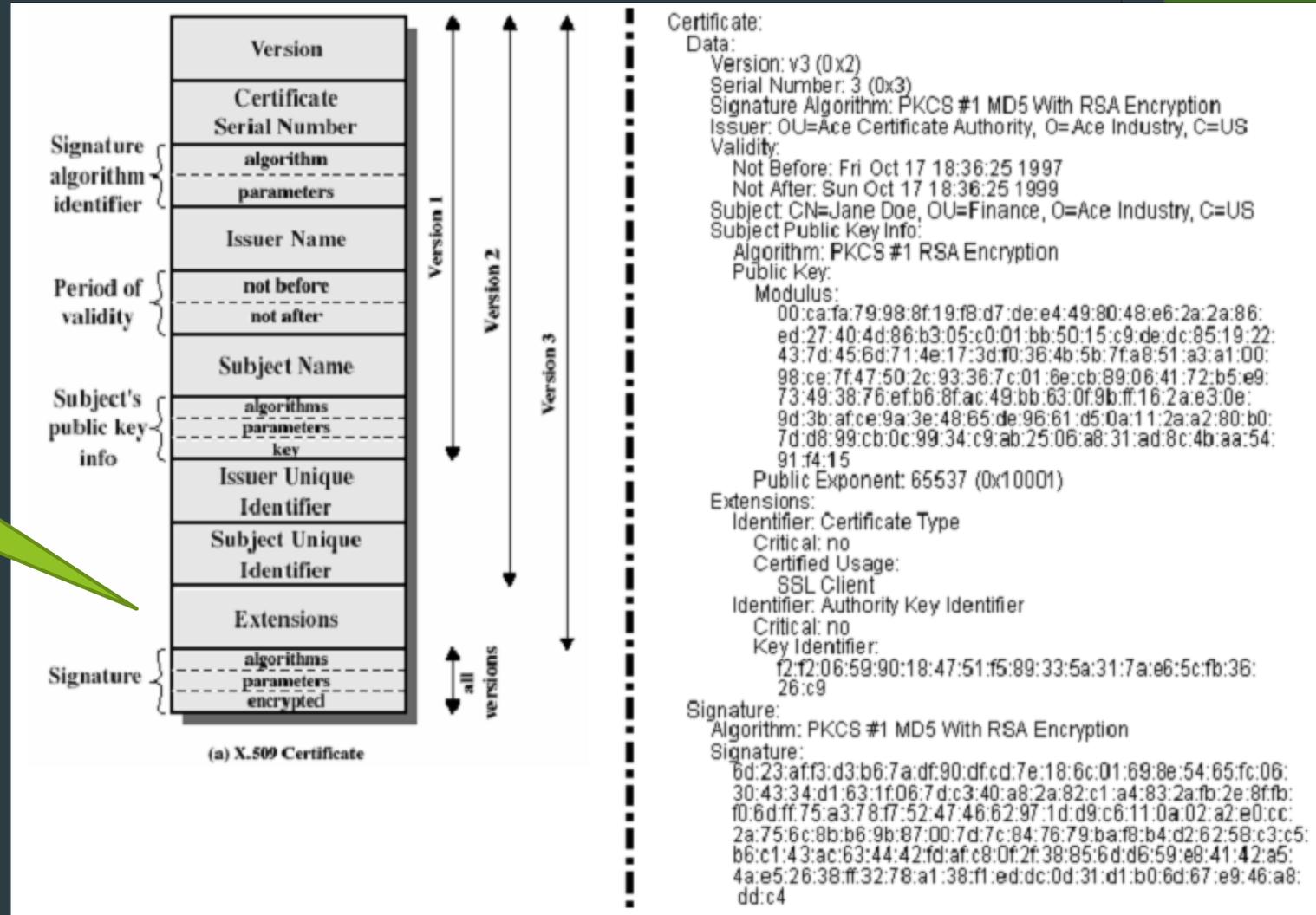
Extensions optionnelles introduites avec la version 2 de X.509.



Service d'authentification X509

Structure du certificat

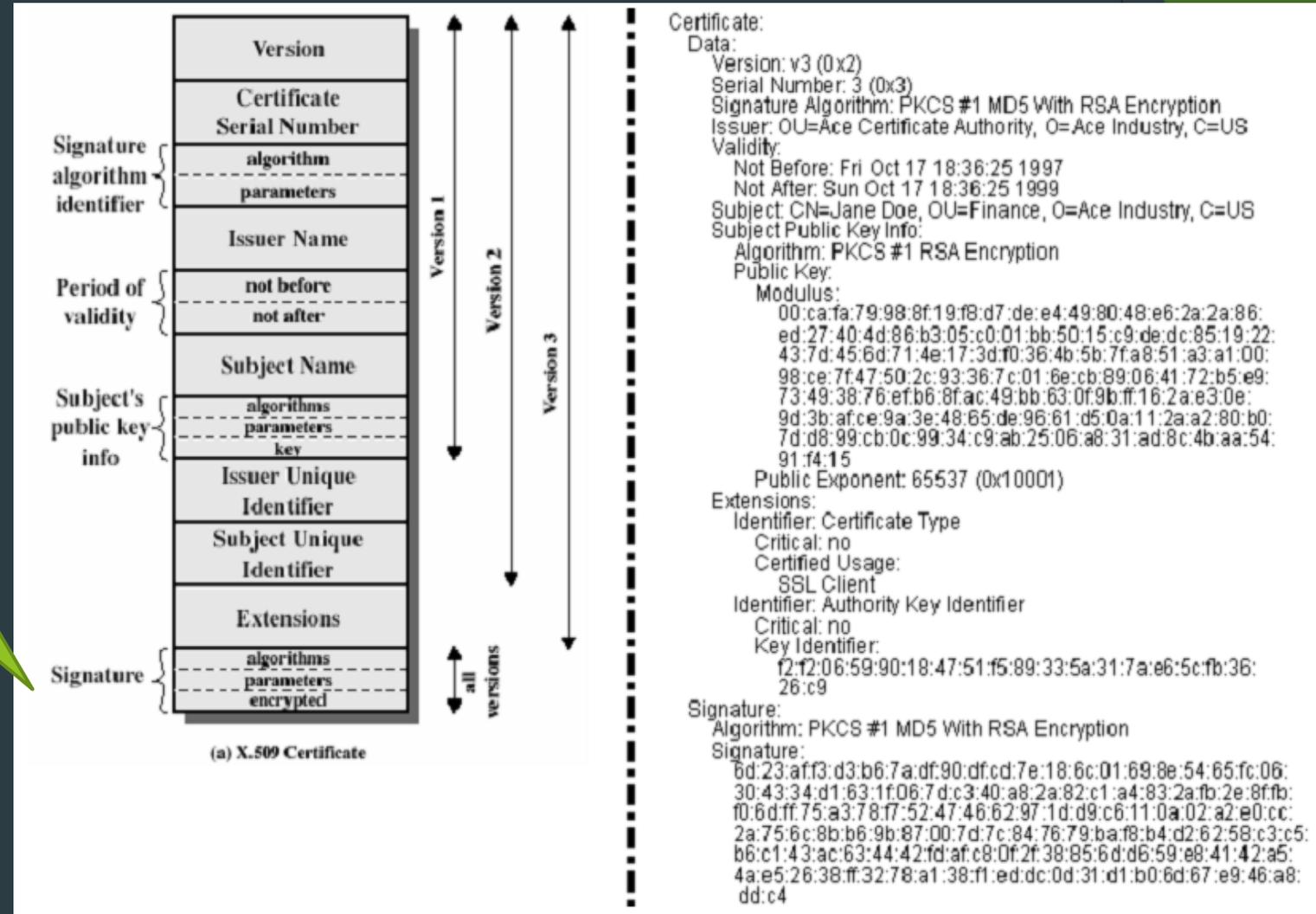
Extensions génériques optionnelles, introduites avec la version 3 de X.509.



Service d'authentification X509

Structure du certificat

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



Pratique: Exemple de certificat

The image shows a screenshot of the Internet Options dialog box in Windows XP. The 'Contenu' tab is selected. The 'Certificats' section is visible, with the 'Certificats...' button circled in red. An arrow points from this button to the 'Options avancées' dialog box. In the 'Options avancées' dialog, the 'Rôle du certificat' section is expanded, showing a list of roles with checkboxes. The 'Authentification du serveur' checkbox is checked. The 'Format d'exportation' section is also expanded, showing a dropdown menu with 'Binaire codé DER X.509 (*.cer)' selected, which is also circled in red. An arrow points from the 'Avancé...' button in the 'Certificats' dialog to this dropdown menu. The 'Options avancées' dialog also has a 'Fermer' button at the bottom right.

Options Internet

Général Sécurité Confidentialité **Contenu** Connexions Programmes Avancé

Gestionnaire d'accès

Le contrôle d'accès vous permet de contrôler le type de contenu Internet qui peut être visualisé sur cet ordinateur.

Activer...

Certificats

Utiliser les certificats pour vous identifier clairement, autorités de certification et les éditeurs.

Effacer le statut SSL Certificats...

Certificats

Rôle prévu : <Tout>

Personnel Autres personnes Autorités intermédiaires Autorités principales de confiance

Délivré à Délivré par Date d'e... Nom convivial

Exporter... Supprimer

Avancé...

Affichage

Fermer

Options avancées

Rôle du certificat

Sélectionnez un ou plusieurs types à faire figurer dans la liste Types d'utilisations avancés.

Rôles du certificat :

- Authentification du serveur
- Authentification du client
- Signature du code
- Messagerie électronique sécurisée
- Enregistrement des informations de date
- Signature de liste d'approbation Microsoft

Format d'exportation

Sélectionnez le format d'exportation pour la commande glisser-déplacer par défaut lorsqu'un certificat est glissé vers un dossier de fichiers.

Format d'exportation : Binaire codé DER X.509 (*.cer)

Inclure tous les certificats dans le chemin d'accès de certification



Pratique: Exemple de certificat

The image shows a Windows Internet Options dialog box with the 'Contenu' tab selected. The 'Certificats' section is active, and the 'Certificats...' button is highlighted. A separate 'Certificats' dialog box is open, showing a list of certificates under the 'Autorités principales de confiance' tab. The 'Certificat' dialog box is also open, displaying the details of a selected certificate.

Internet Options - Certificates

Rôle prévu : <Tout>

Autres personnes | Autorités intermédiaires | **Autorités principales de confiance** | Émetteurs

Délivré à	Délivré par	Date d'expiration
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Mi...	31/12/1999
Deutsche Telekom Root CA 1	Deutsche Telekom Ro...	10/07/2019
Deutsche Telekom Root CA 2	Deutsche Telekom Ro...	10/07/2019
DST (ANX Network) CA	DST (ANX Network) CA	09/12/2018
DST (NRF) RootCA	DST (NRF) RootCA	08/12/2008
DST (UPS) RootCA	DST (UPS) RootCA	07/12/2008
DST RootCA X1	DST RootCA X1	28/11/2008
DST RootCA X2	DST RootCA X2	27/11/2008

Certificat

Général | Détails | Chemin d'accès de certification

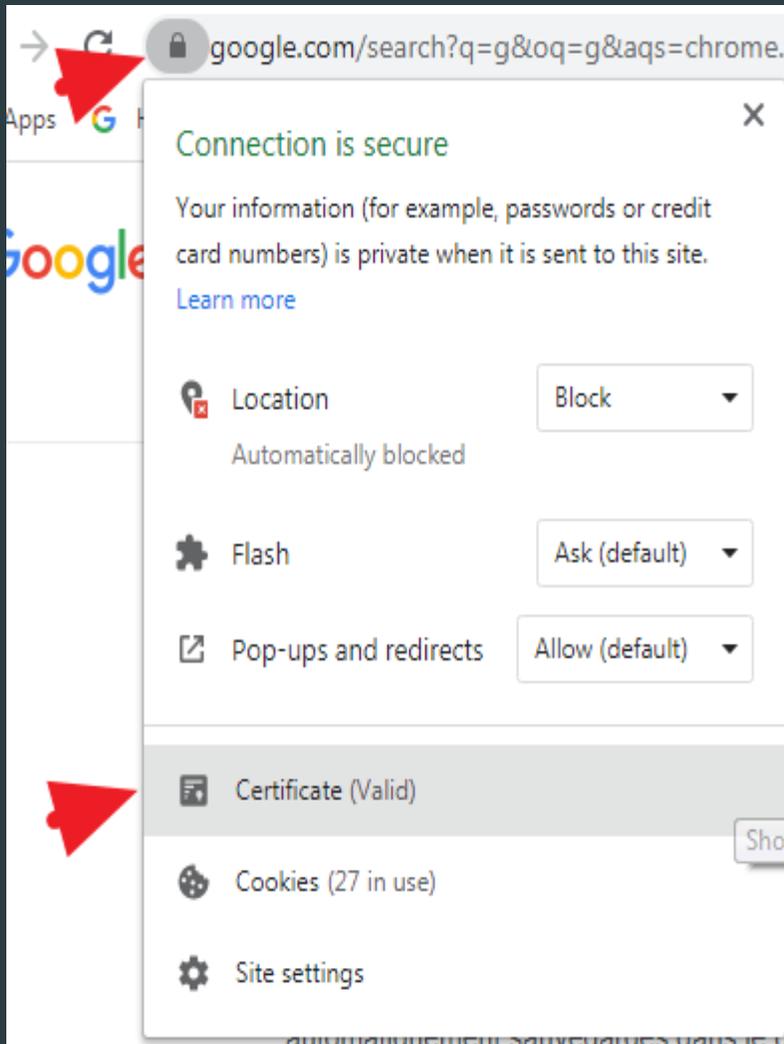
Afficher : <Tout>

Champ	Valeur
Version	V3
Numéro de série	24
Algorithme de signature	md5RSA
Émetteur	Deutsche Telekom Root CA 1, ...
Valide à partir du	vendredi 9 juillet 1999 12:34:00
Valide jusqu'au	mercredi 10 juillet 2019 00:59:00
Objet	Deutsche Telekom Root CA 1, ...
Clé publique	RSA (1024 Bits)

30 81 89 02 81 81 00 d0 dd 9b 0c a0 17 44
44 0f af 21 40 73 67 56 f0 3e 69 68 11 ba
d9 37 f2 81 ae c3 24 ac 69 a1 cd fc a6 18
55 56 ff 8b 9f 32 c1 db e7 78 2c 39 db 60



Pratique: Certificat Google



→ google.com/search?q=g&oq=g&aqs=chrome.

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.
[Learn more](#)

Location Block
Automatically blocked

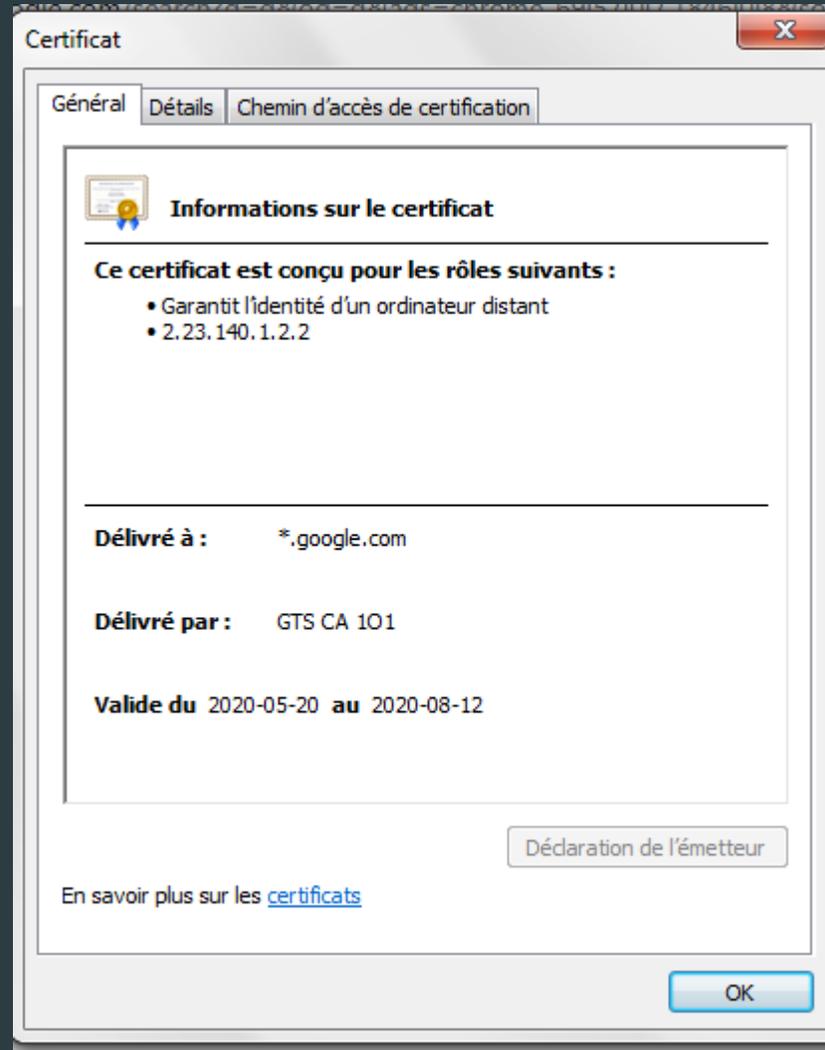
Flash Ask (default)

Pop-ups and redirects Allow (default)

Certificate (Valid) Show

Cookies (27 in use)

Site settings



Certificat

Général Détails Chemin d'accès de certification

 **Informations sur le certificat**

Ce certificat est conçu pour les rôles suivants :

- Garantit l'identité d'un ordinateur distant
- 2.23.140.1.2.2

Délivré à : *.google.com

Délivré par : GTS CA 101

Valide du 2020-05-20 **au** 2020-08-12

[Déclaration de l'émetteur](#)

En savoir plus sur les [certificats](#)

OK

Pratique: Installation d'un certificat

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

