SÉCURITÉ DANS LES RÉSEAUX

K. KHAWAM

LES TIERCES PARTIES DE CONFIANCE

Agenda

- Les tierces parties de confiance dans les systèmes de chiffrement symétrique: les gardiens des clés.
- Les tierces parties de confiance dans les systèmes de chiffrement asymétrique: les PKI (Public Key Infrastructure).

LES TIERCES PARTIES DE CONFIANCE

- Il est possible de définir des protocoles de sécurité entre des entités paires mais tous les protocoles utilisés en pratique s'appuient sur un 3ème partenaire. Celui-ci possède deux propriétés :
  - Il est le gardien des données qui permettent d'authentifier les participants d'un échange :
    - clé symétrique, clé publique, mots de passe
  - Il certifie la validité de l'association entre un nom d'entité et la donnée correspondante.

- Ce partenaire s'appelle :
  - Dans les systèmes basés sur le chiffrement symétrique : le **Gardien des clés**.
  - Dans les systèmes à clés publiques : l'**Autorité de Certification**.

LES TIERCES PARTIES DE CONFIANCE

- Il doit réaliser les opérations suivantes :
  - Contrôler l'identité réelle des participants potentiels à un échange.
  - Générer la donnée d'authentification.
  - Remplir un rôle de serveur des données d'authentification.
  - Enfin, si par hasard la donnée est compromise, le partenaire fiable doit invalider la donnée d'authentification et faire connaître cette invalidation.

LES TIERCES PARTIES DE CONFIANCE
Le gardien des clés

- Le partenaire fiable est le dépositaire de toutes les clés, stockées dans un fichier dont chaque enregistrement contient :
  - Le nom de l'entité
  - Sa clé
  - La période de validité de cette clé
  - Un marqueur permettant de marquer la clé si elle est invalidée.

- Ce fichier doit être protégé en intégrité et en confidentialité.

- Le gardien connaît toutes les clés, y compris la sienne. Chaque utilisateur connaît uniquement sa clé.

LES TIERCES PARTIES DE CONFIANCE
Le gardien des clés

- Les règles d'usage d'une clé doivent être bien définies à sa création et contrôlées lors de son utilisation.

- Lorsqu'une clé est très précieuse, elle doit être est utilisée très rarement.

LES TIERCES PARTIES DE CONFIANCE
Le gardien des clés

- Une donnée est soumise par *x* au gardien chiffrée avec la clé de *y*.
  - x demande le transchiffrement.
- Le gardien déchiffre la donnée avec la clé de *y*, il vérifie que la donnée déchiffrée peut être déchiffrée pour *x*.
- Il chiffre la donnée avec la clé de *x* et la renvoie à celle-ci. En général, la date de transchiffrement est ajoutée dans le message de réponse.
- Les clés ne sont donc jamais transmises via le réseau, sauf lors de la création.

LES TIERCES PARTIES DE CONFIANCE

Le gardien des clés :

Hiérarchie des clés symétriques

- Dans un système de clés symétriques, la constitution de la base de clés suit en général la méthode suivante:
  - Le système est hiérarchisé en un gardien des clés maître, des gardiens de clés secondaires et des machines utilisateurs.
  - Initialement une clé racine est créée.
  - La clé racine est transportée souvent manuellement et stockée sur chaque gardien des clés.
    - Elle ne peut servir qu'à chiffrer des clés pour les gardiens secondaires.

LES TIERCES PARTIES DE CONFIANCE

Le gardien des clés :

Hiérarchie des clés symétriques

- Le gardien maître crée alors des clés pour chaque gardien secondaire. Chaque clé est chiffrée avec la clé maître et envoyées au gardien secondaire via le réseau.

- Lorsqu'un utilisateur est introduit dans le réseau, le gardien lui envoie sa propre clé, après contrôle d'identité, par un canal sûr.

- Le gardien génère la clé de l'utilisateur et l'envoie chiffrée avec sa propre clé, mais quand 2 utilisateurs veulent établir une session de sécurité, ils échangent une clé de session.

- Taille des clés et systèmes cryptographiques varient d'un niveau à l'autre.
  - Les nivaux hauts utilisent les systèmes les mieux protégés.
  - À chaque niveau la durée de vie des clés est inférieure à celle du niveau supérieur.

LES TIERCES PARTIES DE CONFIANCE

Le gardien des clés : Kerberos

- Kerberos constitue le standard des systèmes de distribution des clés symétriques utilisé dans Internet, en particulier par les organismes de recherche et d'enseignement.

- Kerberos met en communication trois entités :
  - Le client : un programme/utilisateur sur une machine donnée. Ce sera l'utilisateur x.
  - Le serveur : un programme requis par l'entité client par exemple le serveur de fichier. Ce sera dans la suite le serveur y.
  - Le centre de distribution des clés, appelé **KDC** (Key Distribution Center)

- Pour fonctionner, Kerberos nécessite une synchronisation des horloges de toutes les machines du réseau

LES TIERCES PARTIES DE CONFIANCE
Le gardien des clés : Kerberos

- Pour pouvoir utiliser un serveur, Kerberos réalise un protocole de distribution de clés de session qui respecte les étapes suivantes :
  1. x s'authentifie auprès du KDC.
  2. x demande un ticket d'utilisation du serveur y au KDC. Un ticket au sens de Kerberos comporte essentiellement une clé de session et différentes informations annexes détaillées plus loin.
  3. Quand x sollicite le serveur y, il utilise le ticket que lui a remis le KDC qu'il met dans sa requête.

- Eléments du protocole :
  - A : Une clé utilisée par x pour s'authentifier qui, en général, est dérivée d'un mot de passe. Cette clef est connue de x et de Kerberos.
  - SA : La clé de session de x, connue de x et de Kerberos.
  - B : La clé privée du serveur y.
  - KDC : La clé de Kerberos connue de lui seul.
  - KXY : La clé de session déterminée entre client et serveur.
  - Ticket : Le ticket donné à un client x pour utiliser un serveur y.

LES TIERCES PARTIES DE CONFIANCE
Le gardien des clés : Kerberos

Étape 1 : authentification du client

- x commence par envoyer une requête d'authentification contenant son identifiant à Kerberos.

- Kerberos lui renvoie un message contenant une clé de session (SA) personnelle et un ticket de contrôle d'accès TGT (Ticket Granting Ticket). L'ensemble est chiffré avec la clé de x, **A**.
  - TGT est constitué de l'identifiant de x, de la clé (SA) et d'une date d'expiration du TGT (en général la durée de validité est de quelques heures).
  - Le TGT est chiffré avec la clé KDC de Kerberos.

- Seul x peut déchiffrer la réponse et récupérer la clé (SA) et TGT, mais seul Kerberos peut déchiffrer TGT.
  - Il est à remarquer que la clé **A** de x n'a pas été transmise.

LES TIERCES PARTIES DE CONFIANCE
Le gardien des clés : Kerberos

Étape 2 : obtention du ticket d'accès au serveur

- Quand x désire (durant la période de validité de son ticket d'authentification) utiliser le service du serveur y, il adresse à Kerberos une requête d'accès à ce serveur. Cette requête contient outre le nom du serveur, le TGT et la date courante chiffrée avec SA.

- À la réception de cette demande, Kerberos déchiffre TGT, récupère la clé (SA), déchiffre la date avec SA et vérifie que cette date est voisine de son heure courante.
  - Ceci prouve que x est bien le demandeur puisqu'il est le seul à pouvoir chiffrer avec **SA** et qu'il ne s'agit pas d'une vieille requête rejouée.

- Kerberos vérifie les droits d'accès de x au serveur y dans une ACL. Si x a bien le droit d'accès, Kerberos délivre un ticket d'accès = {le nom de x, une clé de session pour x et y **KXY**, et une date d'expiration du ticket d'accès}. Le tout est chiffré avec la clé du serveur y.
  - La réponse finale contiendra le nom du serveur y, le ticket ainsi que la clef de session KXY, le tout chiffré avec SA.
  - Cette opération doit être répétée à chaque accès au serveur y.

LES TIERCES PARTIES DE CONFIANCE
Le gardien des clés : Kerberos

Étape 3 : accès au serveur applicatif

- Dans un délai compatible avec la durée de validité du ticket, x va demander au serveur y d'exécuter la transaction pour laquelle il a obtenu le ticket.
  - Il envoie donc à ce serveur une requête avec le ticket et joint la date courante *date_courante* chiffrée avec la clé de session KXY.

- Le serveur y déchiffre le ticket, récupère la clé KXY, vérifie que le ticket n'est pas périmé (que la date envoyée par x n'est pas ancienne).

- y renvoie à x un message avec la date envoyée par x incrémentée de 1.
  - Mis à part Kerberos, seul x a pu chiffrer la *date_courante* avec KXY.
  - Mis à part x et Kerberos, seul y a pu déchiffrer le ticket et donc récupérer KXY.
  - Le contrôle de date fait par y authentifie x et protège conte le rejeu d'une vielle requête copiée au passage par l'attaquant. Le contrôle fait par x sur la date modifiée authentifie y.

- À la fin de cette étape, y et x ont une clé de session partagée qui va servir à authentifier les échanges de la transaction demandée au serveur y et à protéger en intégrité et confidentialité les données échangées.

LES TIERCES PARTIES DE CONFIANCE
Le gardien des clés : Kerberos

Implantation et extensions de Kerberos

- Il existe de très nombreuses implantations de Kerberos. Elles sont réalisée au-dessus du protocole UDP.
- L'usage le plus intéressant est celui d'une authentification dans un intranet et, dans ce cas, la version au-dessus d'UDP est suffisante.

Sécurité de Kerberos

- La possibilité de rejouer des requêtes, bien que la procédure de datation ait pour but d'éviter cela, les messages peuvent être rejoué, **pendant la durée de vie du ticket**.
- Kerberos est sensible aux attaques dites de paris de mot de passe.
- Toute la confiance est mise dans le logiciel implémentant Kerberos.

LES TIERCES PARTIES DE CONFIANCE
L'autorité de certification

- Elle a pour responsabilité de créer et de publier des certificats.

- L'utilisation des clefs publiques repose sur la confiance en l'entité d'origine.
  - Quand une liaison sécurisée est établie entre 2 utilisateurs, rien ne prouve que l'un d'entre eux ne soit pas un imposteur.

- Pour pouvoir utiliser une clef publique avec sécurité, il faut donc que le récepteur puisse savoir à qui appartient cette clef publique et à quoi sert elle.

LES TIERCES PARTIES DE CONFIANCE
L'autorité de certification : certificat

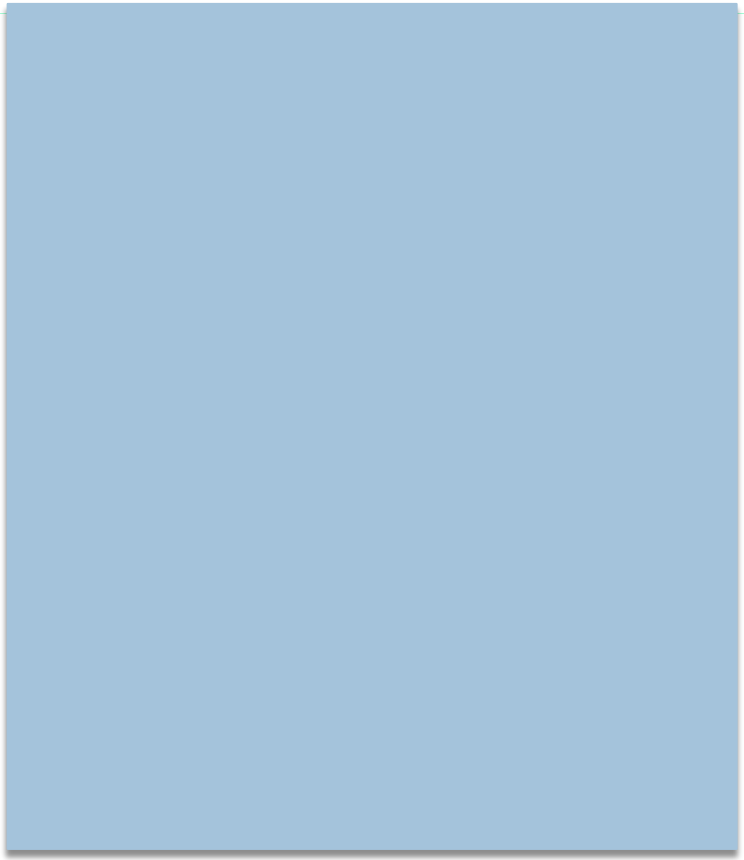
- Document électronique qui associe une clé publique à une entité afin d'en assurer la validité.

- Son objet est de certifier une clé publique.
  - Un certificat peut servir à établir un ou plusieurs faits dont la confirmation:
    - De l'identité d'une personne, d'une société, ou d'un État,
    - De l'exactitude d'un identifiant, d'un document, etc.
    - De l'existence de certains attributs d'une personne…

- Il est délivré par une CA et est signé par cette dernière qui possède elle-même un certificat.

- Rôle du certificat : non-usurpation d'identité.

LES TIERCES PARTIES DE CONFIANCE
L'autorité de certification : certificat



Signé par la clé privée de la CA

LES TIERCES PARTIES DE CONFIANCE
L'autorité de certification : certificat

Contenu du certificat

- Le certificat est composé de 2 parties :
  - Partie contenant les informations (Data)
  - Partie contenant la signature de l'autorité de certification

- Exemples d'informations :
  - Version du certificat
  - Numéro de série du certificat
  - Type de méthodes de signature (algorithmes et paramètres)
  - Identification de la CA
  - Période de validité du certificat
  - Nom distinctif du propriétaire
  - Clé publique

- Signature de la CA sur l'ensemble des champs précédents

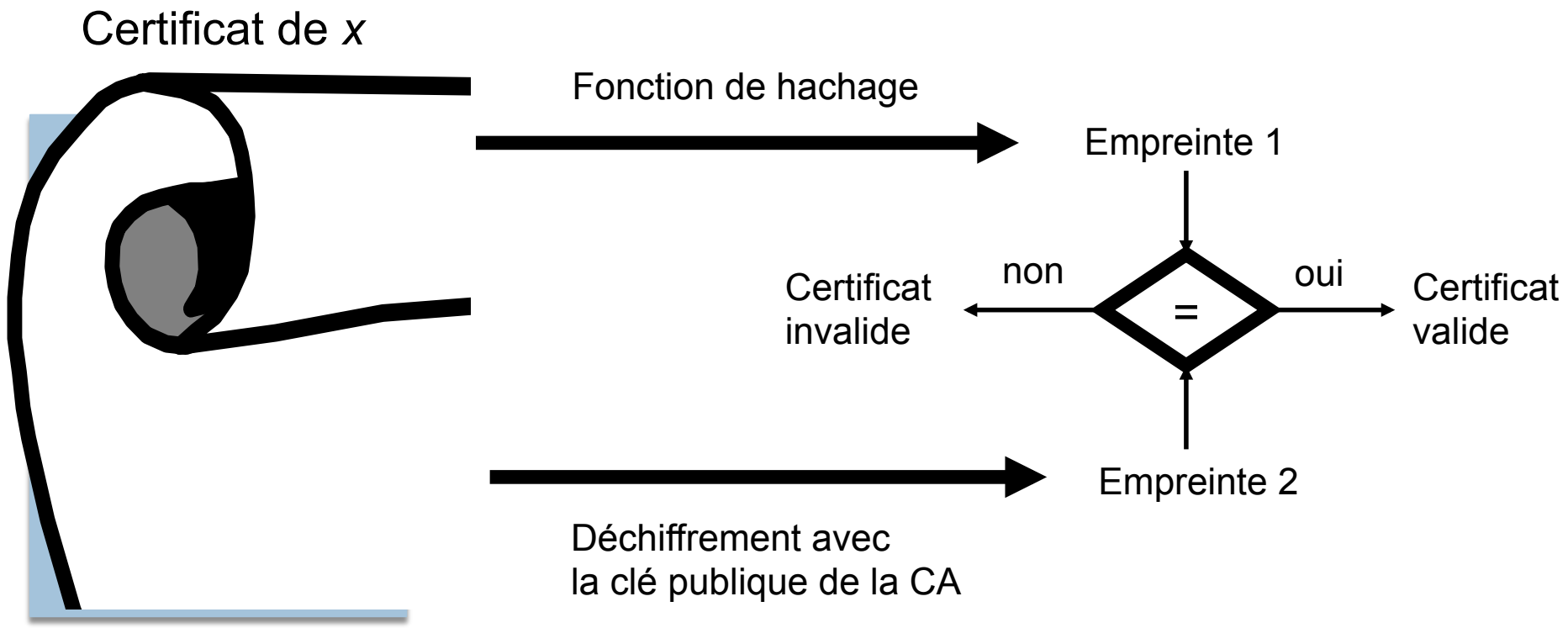
LES TIERCES PARTIES DE CONFIANCE
L'autorité de certification : certificat

Vérification d'un certificat

- Vérifier la date de validité du certificat et l'usage prévu pour ce certificat.
- Vérifier si le certificat est révoqué en utilisant la liste de révocation de la CA émettrice.
- Vérifier si la CA est une CA de confiance.
- Vérifier la signature du certificat.

LES TIERCES PARTIES DE CONFIANCE
L'autorité de certification : certificat

- La vérification s'effectue avec la clé publique de l'autorité de certification:



LES TIERCES PARTIES DE CONFIANCE
L'autorité de certification

- La CA possède elle-même un certificat (auto-signé ou délivré par une autre CA)

- La CA utilise sa clé privée pour créer des certificats et donc se porte garante de l'identité qui se présentera avec ce certificat

- Elle peut être :
  - Organisationnelle
  - Spécifique à un corps de métier
  - Institutionnelle

LES TIERCES PARTIES DE CONFIANCE
L'autorité de certification

La CA doit essentiellement :

- Recevoir et enregistrer les demandes de certificat,
- Vérifier l'identité du demandeur selon une procédure définie,
- Publier les certificats,
- En cas de compromission ou à la demande du titulaire, révoquer un certificat et publier cette révocation,
- Publier l'ensemble des procédures utilisées.

LES TIERCES PARTIES DE CONFIANCE

L'autorité de certification : le modèle de confiance

- La notion de confiance est une notion complexe. Elle est définie dans la recommandation X.509 comme telle:
  - Une entité A fait confiance à une entité B lorsque A suppose que B se comportera tel que A l'attend.

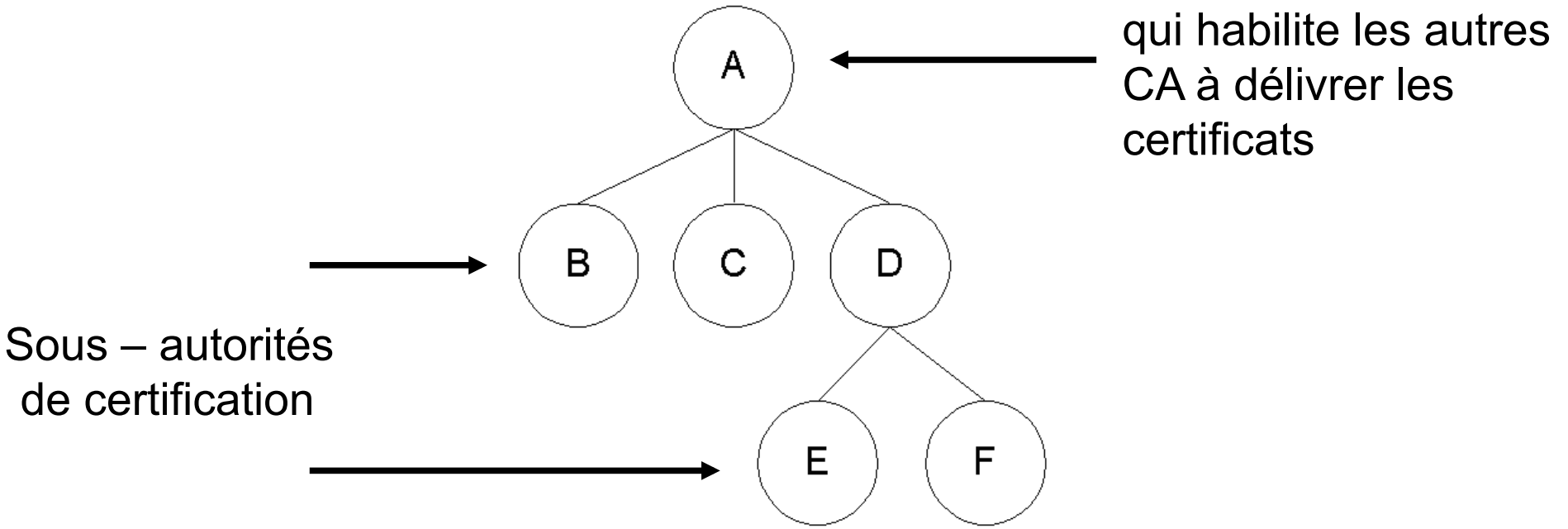
- Dans la plupart des modèles de confiance, une règle s'applique à la notion de confiance: c'est la transitivité
  - Si A fait confiance à B et B fait confiance à C, alors A fait confiance à C.

LES TIERCES PARTIES DE CONFIANCE
L'autorité de certification : le modèle de confiance

- Il existe deux types de certification :
  - Certification hiérarchique : modèle de confiance centralisé car toute la confiance repose sur une CA qui est appelée la CA mère
  - Certification croisée (Cross-certification) : utile pour créer une confiance entre deux organismes ayant chacun une CA qui n'appartiennent pas à la même arborescence

LES TIERCES PARTIES DE CONFIANCE
L'autorité de certification : le modèle de confiance

- Le modèle hiérarchique

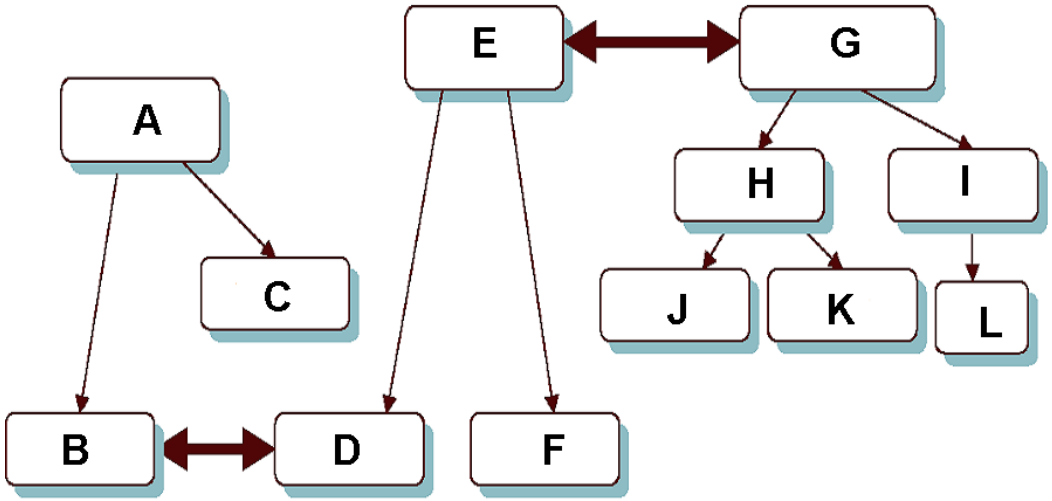


Une autorité de certification habilite une autre autorité de certification en signant sa clé publique

LES TIERCES PARTIES DE CONFIANCE

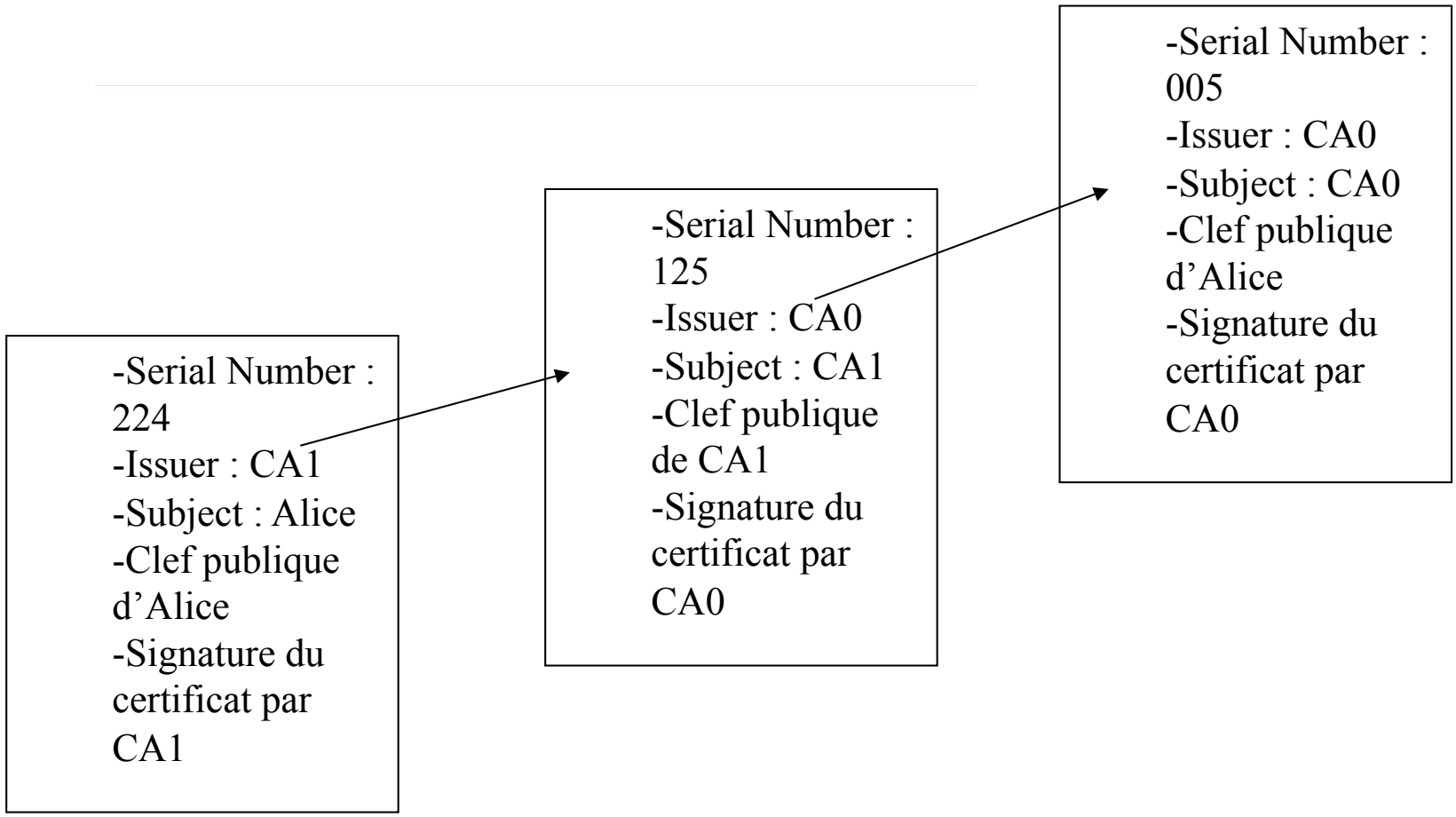
L'autorité de certification : le modèle de confiance

- La certification croisée
  - Les CAs se font mutuellement confiance dans leur domaine de confiance



LES TIERCES PARTIES DE CONFIANCE

L'autorité de certification : le modèle de confiance



LES TIERCES PARTIES DE CONFIANCE
Hiérarchie des CA

- Un certificat n'a pas de caractère confidentiel. Par contre, il doit être intègre et doit pouvoir être vérifié en utilisant la clé publique de l'autorité qui l'a signé.

- Exemple idéal :
  - En haut de la hiérarchie, se trouve une CA dont la qualité est reconnue de tous.

LES TIERCES PARTIES DE CONFIANCE
Hiérarchie des CA

- L'avantage de ce système est de pouvoir hiérarchiser les formes d'un certificat en fonction de son usage.
- On assigne une durée de vie à un certificat et une longueur de clé importante pour les niveaux hauts de la hiérarchie et moindre pour les bas. Les certificats sont donc typés
- Chaque CA doit publier tous les moyens organisationnels et techniques qu'elle met en œuvre pour générer et assurer la sécurité de chaque type de certificats qu'elle gère.
  - Ceci est appelé une **politique de certification**.
- La contrepartie de cette organisation est la lourdeur technique et sociale qu'elle engendre.

Système à clés publiques non hiérarchisés : les modèles PGP

- Le logiciel de sécurisation de transfert de messages PGP (Pretty Good Privacy) propose une organisation plus communautaire

- **PGP** est un crypto-système inventé par Philip Zimmermann, un analyste informaticien.

- Le principe est simple: x ayant un certificat de y en lequel il a confiance, le signe et l'envoie à z qui connaît x en qui il a confiance.
  - Les amis des amis étant des amis, z reçoit le certificat envoyé par x, contrôle la signature de x et fait alors confiance au certificat de y.

- Il pose une question philosophique : la confiance est-elle une relation transitive ?

Système à clés publiques non hiérarchisés : les modèles PGP

- **La révocation d'un certificat PGP**
  - Seul le détenteur du certificat ou un autre utilisateur, désigné comme autorité de révocation par le détenteur du certificat, a la possibilité de révoquer un certificat PGP.
  - La désignation d'une autorité de révocation est utile, car la révocation, par un utilisateur PGP, de son certificat est souvent due à la perte du mot de passe de la clef privée correspondante.
    - Un certificat X. 509 peut uniquement être révoqué par son émetteur.
  - Quand un certificat est révoqué, il est important d'en avertir ses utilisateurs potentiels.

Système à clés publiques non hiérarchisés: les modèles PGP

- PGP utilise le meilleur de la cryptographie symétrique et de la cryptographie asymétrique
  - Objectif : offrir à tout le monde un moyen de préserver la confidentialité d'une information.

- PGP fonctionne suivant le principe suivant :
  - Compression du message.
  - Chiffrement du message : une clé de session aléatoire est générée et le message est chiffré par un algorithme symétrique à l'aide de cette clé de session.
  - Chiffrement de la clé de session : la clé de session est chiffrée en utilisant la clé publique du destinataire (RSA)
  - Envoi et réception du message : l'expéditeur envoie le couple message chiffré / clé de session chiffré au destinataire.

Système à clés publiques non hiérarchisés: les modèles PGP

- PGP offre les fonctionnalités suivantes :
  - **Signature électronique et vérification de l'intégrité des messages Chiffrement des fichiers locaux**
  - **Génération de clefs publiques et privées**
  - **Gestion des clefs**
  - **Certification de clefs**
  - **Révocation, désactivation, enregistrement de clefs**

Système à clés publiques non hiérarchisés : les modèles PGP

- Le certificat PGP comprend :
  - Le numéro de version PGP
  - La clé publique du détenteur du certificat
  - Les informations du détenteur du certificat (identité : nom, ID, photo, etc.)
  - La signature numérique du détenteur du certificat
  - La période de validité du certificat
  - L'algorithme de chiffrement symétrique (IDEA, 3DES)

- Dans PGP, toute personne peut agir en tant que CA et donc peut valider le certificat d'un autre utilisateur PGP
  - Pas de CA mère
  - Confiance basée sur la proximité sociale.

- Le fait qu'un seul certificat puisse contenir plusieurs signatures est l'un des aspects uniques du format du certificat PGP.

FORMAT DES DONNÉES CRYPTOGRAPHIQUES

- **ASN.1** (*Abstract Syntax Notation One*) est un standard international destiné à décrire les données échangées dans les protocoles de télécommunication (modèle OSI).
  - Il est mis en œuvre dans un grand nombre d'applications (gestion de réseaux, messagerie, sécurité, téléphonie, Internet, etc.).

- **XML** (*eXtended Markup Language*) est dérivé de travaux d'IBM.

- Bien que destinés à répondre à des besoins différents, il s'agit d'exemples de « langages de types »
  - Les particularités de ASN.1 et XML sont qu'ils ne peuvent faire que cela et que, la valeur d'une variable d'un type donné étant connue, il lui correspond une représentation binaire unique.

FORMAT DES DONNÉES CRYPTOGRAPHIQUES

- ASN.1 et XML sont donc un moyen pour spécifier une représentation de types indépendante des machines
  - Exemple: un type **point** dans le plan peut être décrit en ASN.1 par:

    Point ::= APPLICATION 0 IMPLICIT SEQUENCE

    {

    xCoord INTEGER,

    yCoord INTEGER

    }
    - Le transfert d'une variable de type point ayant la valeur (5,4) est représenté par la séquence hexadécimale 6006020105020104.

- Ces langages, plus particulièrement ASN.1, sont utilisés dans les normes des protocoles de sécurité pour décrire des types de certificats, fichiers signés, chiffrés…

FORMAT DES DONNÉES CRYPTOGRAPHIQUES

- Structure de data de Fooprotocol en ASN.1:
  - FooProtocol DEFINITIONS ::= BEGIN

    FooQuestion ::= SEQUENCE { trackingNumber INTEGER, question IA5String }

    FooAnswer ::= SEQUENCE { questionNumber INTEGER, answer BOOLEAN } END
- Exemple de message correspondant au Fooprotocol:
  - myQuestion FooQuestion ::= { trackingNumber 5, question "Anybody there?" }
- Pour envoyer ce message à travers le réseau, ASN.1 définit une multitude de règles de codage:
  - DER (Distinguished Encoding Rule)

FORMAT DES DONNÉES CRYPTOGRAPHIQUES

- Voici la structure de données résultantes codées en DER (nombres en hexadécimal):
  - 30 -- tag indicating SEQUENCE
  - 13 -- length in octets
  - 02 -- tag indicating INTEGER
  - 01 -- length in octets
  - 05 -- value
  - 16 -- tag indicating IA5String
  - 0e -- length in octets
  - 41 6e 79 62 6f 64 79 20 74 68 65 72 65 3f -- value ("Anybody there?" in ASCII)

30 13 02 01 05 16 0e 41 6e 79 62 6f 64 79 20 74 68 65 72 65 3f

FORMAT DES DONNÉES CRYPTOGRAPHIQUES

Codage en XML

XML est un métalangage qui offre la possibilité de définir les balises dont on a besoin et de leur associer une interprétation.

- <FooQuestion>
  <trackingNumber>5
  </trackingNumber>
  <question>Anybody there?
  </question>
  </FooQuestion>

FORMAT DES DONNÉES CRYPTOGRAPHIQUES

Importance de XML

- Un avantage par rapport à ASN.1 est la lisibilité de XML mais il est tout à fait possible de réaliser avec ASN.1 ce qu'on fait avec XML
- XML est flexible, ce qui limite les problèmes d'interopérabilité.
- XML nécessite une puissance de calcul pour le traitement beaucoup plus faible que celle de l'ASN.1

FORMAT DES DONNÉES CRYPTOGRAPHIQUES

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>[……]</ds:CanonicalizationMethod>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"></ds:SignatureMethod>
     <ds:Reference URI="#IcarePaquet">
          <ds:Transforms>[……]</ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
<ds:DigestValue>PlUx3g+Sh92GDPCl+v+e760hyTs=</ds:DigestValue></ds:Reference></ds:SignedInfo>
<ds:SignatureValue>EhgqW6AxKZVJfu8HKm4HqsnO0MszMZP9UnRvyPGCwaepIdja/oroSSltfHOCJkar8JACEWMRdnd5W
0Nof81/h4tluIhd/r7bVqgZYu27NLQ=</ds:SignatureValue>
<ds:KeyInfo>[……]</ds:KeyInfo>
<ds:Object Id="IcarePaquet">
<AttributeCertificate>
     <CertificateInfo><Version>V1.0</Version>
       <Type>AttributeCertificate</Type>    <Id>57</Id></CertificateInfo>
     <Content>
        <Issuer>
              <DN>EMAILADDRESS=demerjia@enst.fr, CN=JacquesDemerjian CA, O=ENST, L=PARIS</DN>
              <X509Data>MIICW[……]+EGHJjR</X509Data>
        </Issuer>
        <Holder>
           <Identity>
              <UserDN>EMAILADDRESS=thomas@icare1.tai, CN=SYLVAIN</UserDN>
              <Serial>1</Serial>
              <PublicKey>MIGfMA0[…….]AQAB</PublicKey>
           </Identity>
        </Holder>
        <Validity>
           <ValidityFrom>2003/06/25 10:18:14</ValidityFrom>
           <ValidityTo>2003/06/30 00:00:00</ValidityTo>
       </Validity>
        <Attribute>
           <Droits>Administrateur</Droits>
           <Couleur>Jaune</Couleur>
           <Langue>Français</Langue>
           <Application>Convertisseur Euros</Application>
           <Resource>http://localhost:8080/portail/index.jsp</Resource>
        </Attribute>
     </Content>
</AttributeCertificate>
</ds:Object>
</ds:Signature>
```

Les standards

- Les standards PKCS (Public Key Cryptographic Standards)
  - Ensemble de standards pour cryptographie à clé publique.
  - Développé par un consortium RSA, Sun, Apple, Microsoft, DEC, Lotus et MIT.
  - Parmi les algorithmes supportés : RSA, Diffie-Hellman.

- Le standard X509 :
  - Conçu pour fournir des services de répertoires sur de grands réseaux informatiques

Les standards PKCS

Standard	Description
PKCS # 1	Standard de chiffrement. Ce standard défini des mécanismes pour le chiffrement et la signature des données utilisant les systèmes de chiffrement à clés publiques RSA
PKCS # 3	Standard pour le protocole d'échange de clés Diffie-Hellman
PKCS # 5	Standard pour le chiffrement à base de mot de passe. Ce standard décrit une méthode pour générer une clé secrète à partir d'un mot de passe
PKCS # 6	Standard de certificats étendus. Ce standard a été « oublié » en faveur du standard X509 v3
PKCS # 7	Standard pour les échanges de messages cryptographiques
PKCS # 8	Standard pour le stockage des clés privées
PKCS # 9	Définit des types d'attributs utilisés dans les autres standards PKCS
PKCS # 10	Standard pour les demandes de certification
PKCS # 11	Standard pour les interfaces de programmation pour les périphériques cryptographiques comme les cartes à puces
PKCS # 12	Standard pour l'échange d'informations personnelles. Ce standard définit un format pour le stockage et le transport de clés privées et des certificats
PKCS # 13	Standard pour la cryptographie à base de courbes elliptiques
PKCS # 14	Standard pour la génération de nombres pseudos-aléatoires. En cours de développement
PKCS # 15	Standard sur les « cryptographiques tokens »

Les standards X509

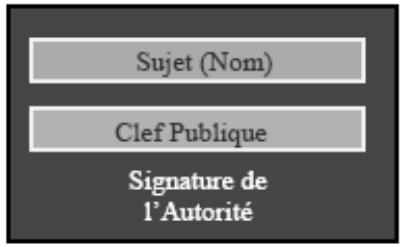
- X509 : standard pour les infrastructures à clé publique
  - Un format standard de certificat numérique
  - Un modèle de référence pour les PKI

- Historique : format standardisé par l'ISO à 4 reprises
  - X509 v1 : 1988
  - X509 v2 : 1993 (v1 + 2 nouveaux champs)
  - X509 v3 : 1996 (ISO – ANSI – ITU) (v2 + extensions)
  - X509 v4 : 2003

- Ce standard a été conçu en particulier pour l'authentification (on parle souvent d'authentification X509) et la signature numérique.

Les standards X509

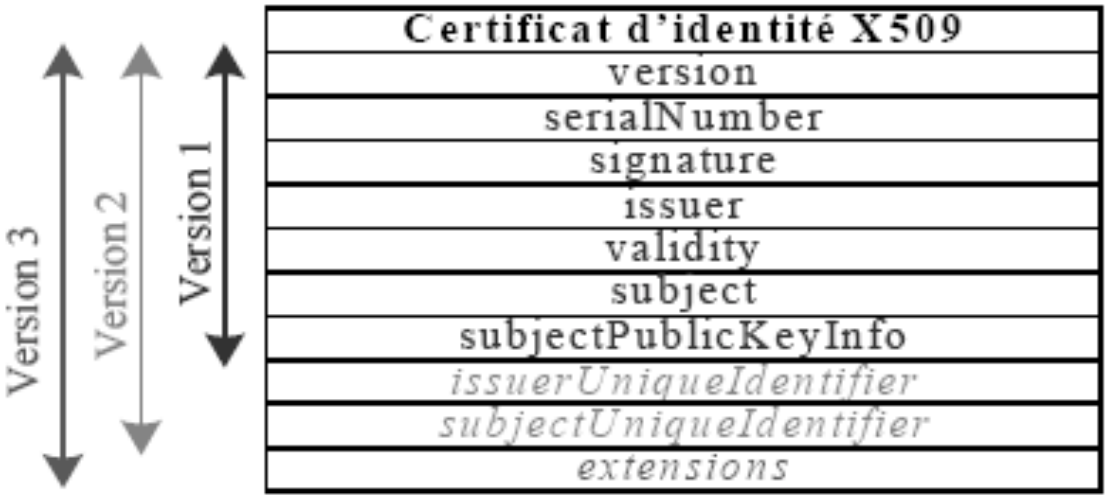
- La norme X.509 définit 2 types de certificats :
  - Le certificat de clef publique joint une valeur de clef publique et une identité (Nom de l'utilisateur auquel appartient le certificat, subject X. 500 name)



  - Le certificat d'attributs joint une identité et des attributs (Droits de l'identité) servant à véhiculer des autorisations.

Les standards X509

- La v1 avait pour but de décrire les méthodes d'authentification et de contrôle d'accès aux annuaires X.500.
- La v2 a ajouté 2 champs pour supporter le contrôle d'accès aux répertoires, qui sont les champs "issuer unique identifier" et "subject unique identifier".
- Enfin pour permettre l'ajout d'autres informations (attributs ou privilèges) dans un certificat, la v3 a introduit le concept d'extension qui sont optionnelles.



Les standards X509

Format d'un certificat X509

- Les principaux champs :
  - Numéro de version (*certificate format version*)
  - Numéro de série (*certificate serial number*)
  - Algorithme de signature (*signature algorithm identifier for CA*)
  - Nom de la CA émettrice (*issuer X.500 name*)
  - Validité (*validity period*)
  - Nom de l'utilisateur (*subject X.500 name*)
  - Clé publique du sujet (*subject public key*)
  - Algorithme utilisé avec la clé publique (*subject public key information*)
  - Signature de la CA

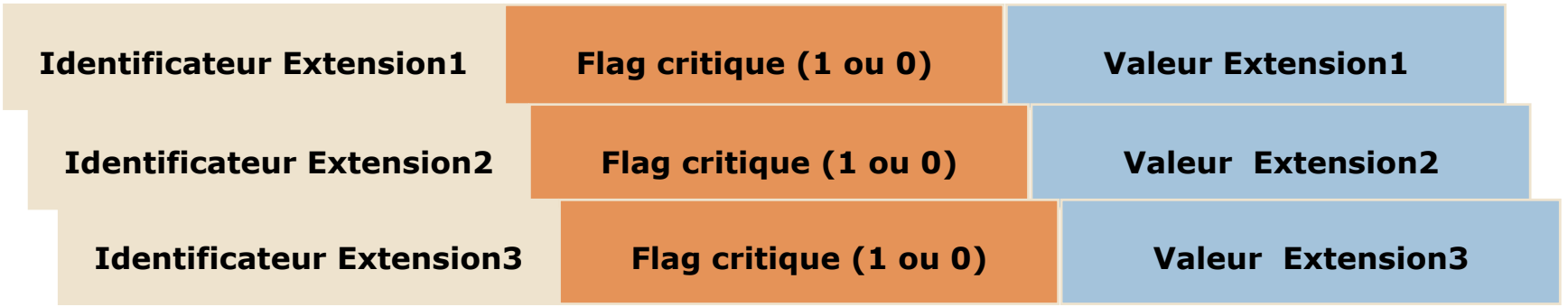
Les standards X509

Format d'un certificat X509

- Champs optionnels
  - IssuerUniqueIdentifier (v2)
    - Identifie de façon unique la clé utilisée par la CA pour signer le certificat (cas où la CA a utilisé plusieurs clés depuis sa mise en œuvre)
  - SubjectUniqueIdentifier (v2)
    - Différencie entre plusieurs clés publiques, issues par la même CA, appartenant à un même détenteur
  - Extensions (v3) : permettent de spécifier l'usage et de définir des contraintes par rapport aux autres CA
    - Informations sur les clés, sur l'utilisation du certificat
    - Attributs des utilisateurs et des CA
    - Contraintes de la certification croisée (contrôler et limiter la confiance envers d'autres CA)
  - Ces extensions possèdent 3 champs : Type, Criticality, Value

Les standards X509

- **Les extensions sont classées en 4 catégories:**
  - Les extensions d'information sur la clé et la politique de sécurité
  - Les extensions d'informations sur le détenteur et l'émetteur
  - Les extensions de contraintes sur le chemin de certification
  - Les extensions de révocation



Un certificat X509

```
Certificate ::= SIGNED { SEQUENCE{
                        version [0]                 IMPLICIT Version DEFAULT v1,
                        serialNumber                CertificateSerialNumber,
                        signature                   AlgorithmIdentifier,
                        issuer                                  Name,
                        validity                                Validity,
                        subject                                 Name,
                        subjectPublicKeyInfo        SubjectPublicKeyInfo,
                        issuerUniqueIdentifier      [1] IMPLICIT UniqueIdentifier OPTIONAL,
                -- If present, version must be v2 or v3
                        subjectUniqueIdentifier     [2] IMPLICIT UniqueIdentifier OPTIONAL
                -- If present, version must be v2 or v3
                        extensions                  [3] Extensions OPTIONAL
                -- If present, version must be v3 -- }
                        }
Version ::= INTEGER { v1(0), v2(1), v3(2) }
CertificateSerialNumber ::= INTEGER
AlgorithmIdentifier ::= SEQUENCE {
        algorithm               ALGORITHM.&id({SupportedAlgorithms}),
        parameters                      ALGORITHM.&Type ({SupportedAlgorithms}
                                                        {@algorithm}) OPTIONAL }
SupportedAlgorithms ALGORITHM ::= { ... }
Validity ::= SEQUENCE { notBefore UTCTime, notAfter UTCTime }
SubjectPublicKeyInfo ::= SEQUENCE { algorithm   AlgorithmIdentifier,
                                                subjectPublicKey    BIT STRING      }
Time ::= CHOICE {               utcTime UTCTime, generalizedTime GeneralizedTime }
SIGNED { ToBeSigned } ::= SEQUENCE {
                        toBeSigned ToBeSigned,
                        encrypted ENCRYPTED { HASHED {ToBeSigned }}
                                                        }
```

Les standards X509

Informations sur les clés :

- Key usage
  - non-repudiation, certificate signing, CRL signing, digital signature, data signature, symetric key encryption for key transfert, Diffie-Hellman key agreement
- Private Key Usage Period
- CRL Distribution Point
- Authority Key Identifier
- Subject Key Identifier

Les standards X509

Attributs des utilisateurs et des CA

- Ce groupe d'extensions permet de mieux spécifier l'identification des utilisateurs et des certificats.
  - Subject Alternative Name : spécifie une ou plusieurs informations sur le propriétaire du certificat
  - Issuer Alternative Name : spécifie une ou plusieurs informations sur la CA

Extensions de révocation

- CRL Distribution Points
- Freshest CRL

Les standards X509

Informations sur l'utilisation du certificat :

- Certificate Policies : ce champ spécifie la Politique de Certification (PC) qui a présidé à l'émission du certificat. Les Politiques de Certification sont représentées par des OID (Object Identifier).
  - Plusieurs politiques servent à protéger la CA de toute responsabilité:

    « *Verisign disclaims any warranties … Verisign makes no representation that any CA or user to which it has issued a digital ID is in fact the person or the organisation it claims to be… Verisign makes no insurance of the accuracy, authenticity, integrity, or reliability of information* »

- Policy Mappings : ce champ ne concerne que les Co-certificats.

Les standards X509

Contraintes sur la co-certification

- Basic Constraints: indique si un utilisateur est un utilisateur final ou si c'est une CA
- Name Constraints: permet aux administrateurs de restreindre les domaines de confiance
- Policy Constraints: (co-certificats) permet de spécifier les politiques de certification acceptables pour les certificats dépendants de co-certificat

Les standards X509

X509 certificate - version: **1**

certificate serial no: **199609130001**
AC algorithm: **ISA_MD4_RSADIS9796**
AC public key name : **AC_TST**
AC distinguished name : **/C=FR/L=Paris/O=ORG1/CN=USERI**
Owner algorithm: **ISA_RSA**
Owner algorithm parameter: **USER1**
Public Key modulus:

ff ff ff ff 1c dd b3 86 2c e9 93 d6 9b b2 37 c3
92 3c cb 66 de 3d db 6c 89 f9 59 d4 20 0b 5b d1
ef f2 la a4 c7 d1 9c d3 a4 35 b6 4f 38 24 cd 5d
e1 38 f8 1c e5 6e ec cd 4e 5a f0 f5 fe ac d8 f1

Public Key exponent:

01 00 01

AC identification: **1000000000001**
Owner identification : **1234567890123**
Signature algorithm parameter: **AC_TST**
Signature:

57 85 d4 3b 4a 0e 29 8a b6 dc 1d 6b 81 8a 90 89
f2 84 0b 23 99 c8 ec 69 60 53 8f 56 7e 64 9d 9f
6c c8 43 30 fc f2 6c a8 77 0b 5d be d9 be d9 7f
bc 57 85 0b 0d 78 44 57 ca 4c 8c 3f d1 62 f9 72

Les standards X509

Limites des certificats X.509v3

- Les extensions de certificats X.509v3 sont des champs qui permettent de rendre l'utilisation des certificats plus flexible.

- Mais elles rendent bien souvent les applications traitant ces certificats incompatibles entre elles

Les usages de certificats :
Messagerie S/MIME

- Secure Multipurpose Internet Mail Extensions est développé par RSA

- Objectif : chiffrer et signer les messages électroniques de type MIME

- La sécurité du message S/MIME est apportée par le message PKCS7/CMS et est inclus dans le corps de celui-ci. La partie sécurisée du message est donc le corps du message uniquement.

Les usages de certificats :
Messagerie S/MIME

- Le standard S/MIME repose sur le principe de chiffrement à clé publique.

- Les différentes parties d'un message électronique, codées selon le standard MIME, sont chacune chiffrée à l'aide d'une clé de session.
  - Seul le destinataire peut ainsi ouvrir le corps du message, à l'aide de sa clé privée (confidentialité et l'intégrité du message reçu).

- La signature du message est chiffrée à l'aide de la clé privée de l'expéditeur.

Les usages de certificats :
Messagerie S/MIME

- PKCS7 et CMS (Cryptographic Message Syntax) définissent des types génériques pour la représentation de données sur lesquelles on applique des opérations cryptographiques.

- Les différents types de messages sont:
  - **Data**: n'importe quelle suite binaire;
  - **SignedData**: une suite binaire signée avec une ou plusieurs signatures.
  - **EnvelopedData** : une suite binaire chiffrée avec un crypto-système symétrique utilisant une clé de session.
  - **DigestedData** : une suite binaire et un résumé de cette suite.
  - **EncryptedData** : une suite binaire chiffrée, sans autre donnée.
  - **AuthenticatedData** : une suite binaire protégée en intégrité
  - **MAC AuthenticatedData** : une suite binaire protégée en intégrité par un MAC ou une fonction de hachage chiffrée avec un crypto-système symétrique.

Infrastructure de Gestion des Clefs

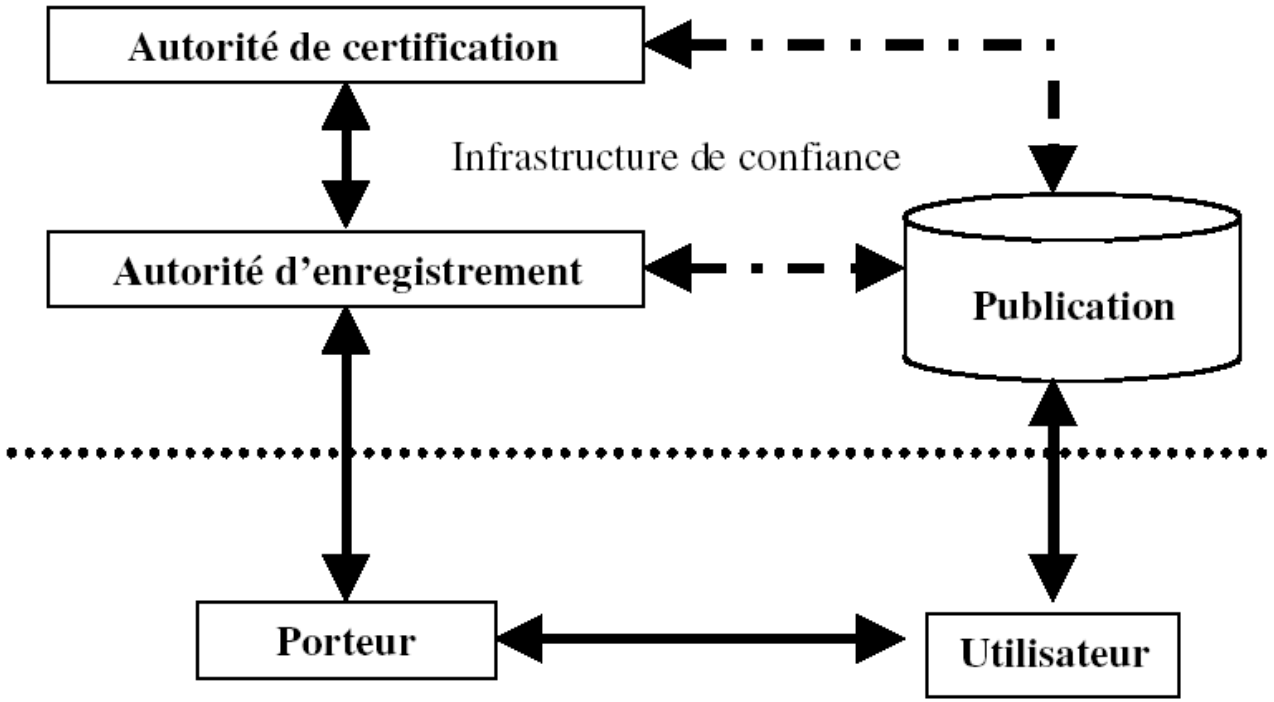
Définition

- PKI signifie "Public Key Infrastructure" traduit en français par ICP (Infrastructure à Clefs Publiques) ou IGC (Infrastructure de Gestion des Clefs).

- Fonctions principales d'une PKI
  - Gestion de la génération et de la distribution des paires de clés publique/privée
  - Protection des clés privées
  - Liaison entre les clés publiques et les clés privées données
  - Émission et révocation des certificats
  - Publication des certificats
  - Fourniture d'un service de séquestre et de recouvrement des clés privées

- Les acteurs d'une PKI
  - Les autorités d'enregistrement (RA, Registration Authority)
  - Les autorités de certification (CA, Certification Authority)
  - Les porteurs de certificats
  - Les utilisateurs de certificats
  - Les services de publication des certificats

Infrastructure de Gestion des Clefs



Infrastructure de Gestion des Clefs

Autorité d'enregistrement

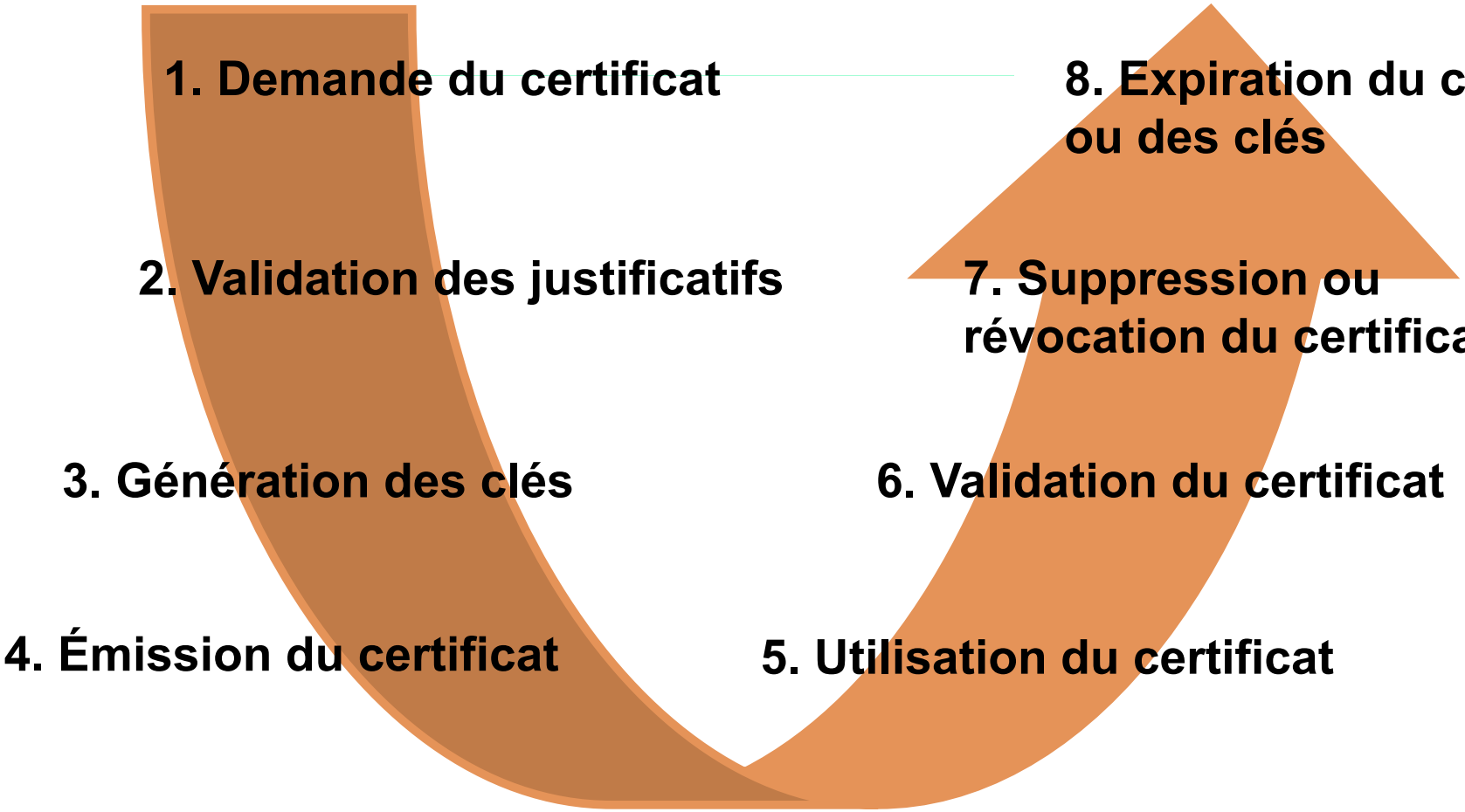
- Organisme responsable de l'**identification** et de l'**authentification** des entités qui demandent un certificat
  - Ne signe pas les certificats
  - Examine les pièces justificatives de celui qui demande le certificat
- La RA possède une paire de clés certifiée pour s'authentifier auprès de la CA et pour accomplir les tâches qui lui incombent
- Elle sert d'intermédiaire pour la distribution de supports physiques de certificats et de mot de passes utilisés dans les échanges avec les utilisateurs

Infrastructure de Gestion des Clefs

Opérateur de certification

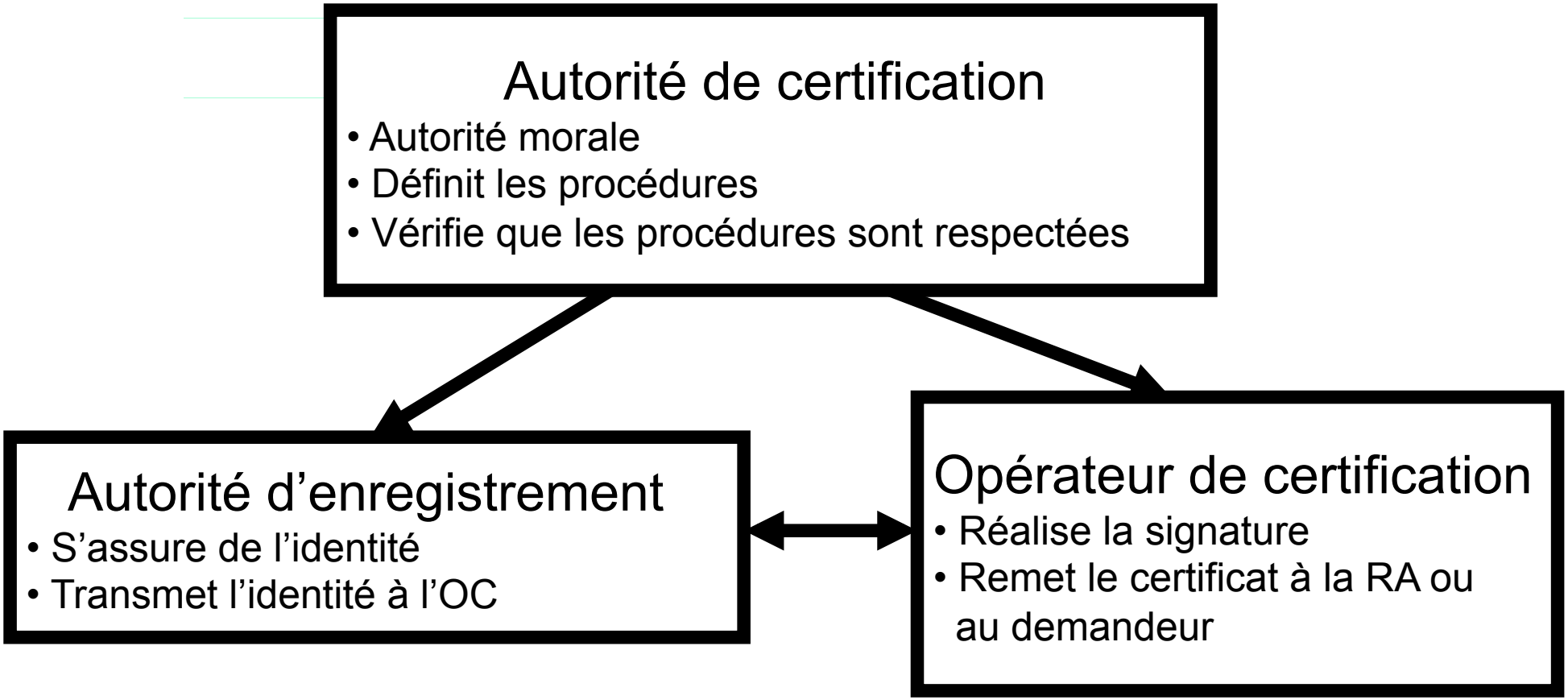
- Organisme qui a la responsabilité technique de l'élaboration des certificats, leur distribution, leur révocation,…
  - Exemples : CertPlus, Gemplus, etc.
- L'AC délègue à l'Opérateur de Certification toutes les opérations nécessitant l'usage de la clé privée de l'AC :
  - création et distribution sécurisée des certificats, révocation, production de cartes à puces…
- Il gère en collaboration avec la RA les cycles de vie des certificats.

Infrastructure de Gestion des Clefs
Cycle de vie d'un certificat

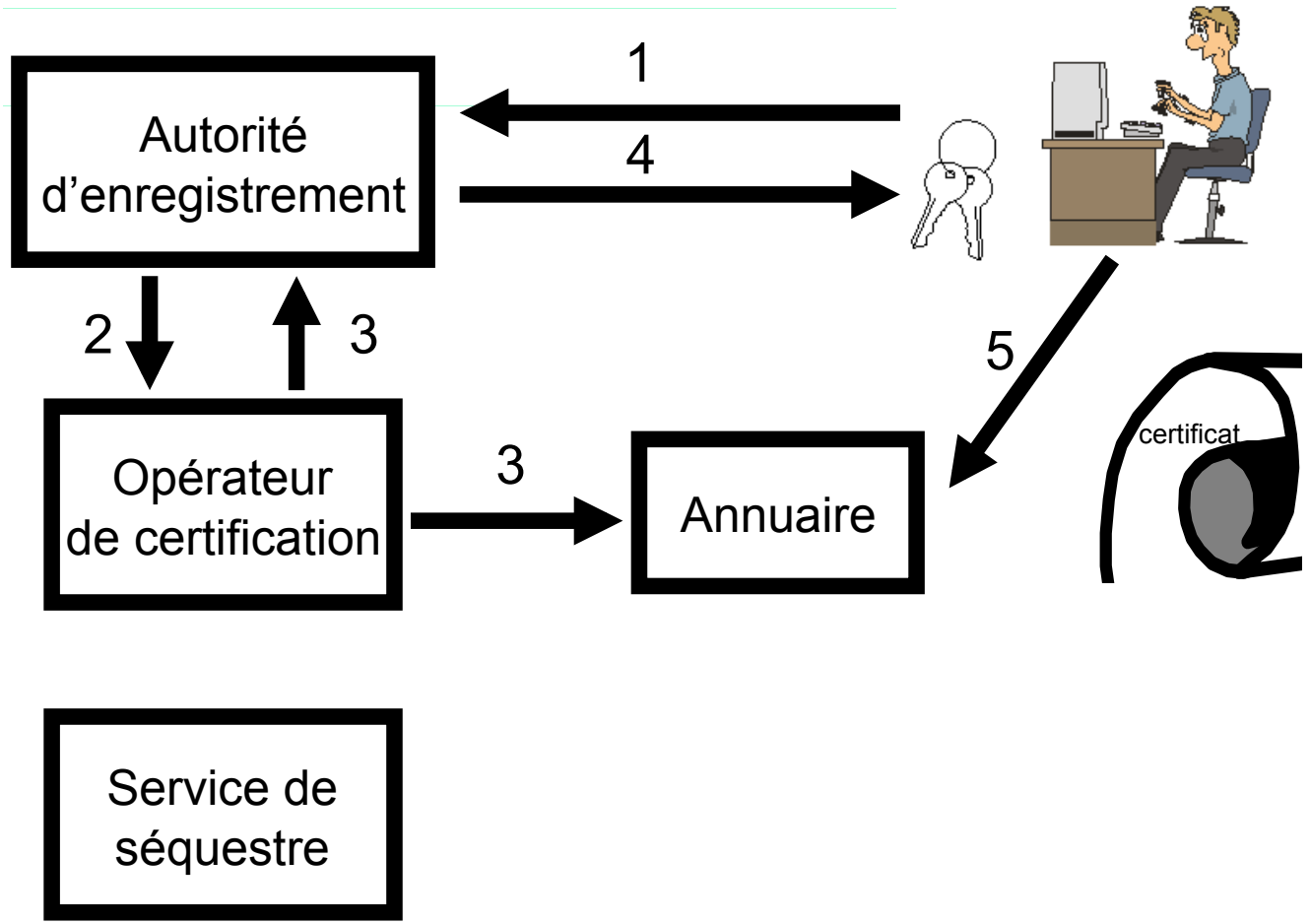


Infrastructure de Gestion des Clefs

Relations entre les acteurs de certification



Infrastructure de Gestion des Clefs
Scénario de demande d'un certificat



Infrastructure de Gestion des Clefs
Génération de la clé secrète

- Scénario 1 :
  - Les utilisateurs génèrent eux-mêmes leur clé secrète
    - L'utilisateur doit délivrer sa clé publique à la CA pour avoir un certificat
    - Ce scénario est recommandé pour une clé servant à la signature dont l'unicité assure la non-répudiation des échanges

- Scénario 2 :
  - La CA génère la clé secrète
    - Mais copie et remise des clés de façon sûre à l'utilisateur
    - Ce scénario est recommandé pour une clé servant au chiffrement qui doit être séquestrée

Infrastructure de Gestion des Clefs
Le service de publication

- Les certificats émis par une PKI doivent être rendus publiques afin que les différents partenaires qui les utilisent puissent s'échanger leur clé publique.
  - Pour cela, les certificats sont publiés dans un annuaire d'accès libre.

- L'utilisation d'un annuaire présente, par contre, un certain nombre d'inconvénients :
  - La génération d'un trafic réseau important.
  - Il faut savoir s'il est simple de déployer une solution capable de supporter la charge d'un ensemble conséquent d'utilisateurs.
  - Une autre question centrale reste celle du contrôle des accès.

Infrastructure de Gestion des Clefs
Le service de publication

- Un annuaire est comme une base de données

- Ses principales caractéristiques sont :
  - dédié à la lecture, plus qu'à l'écriture
  - offre une vue statique des données
  - mises à jour simples

- Un service d'annuaire est en plus :
  - un protocole réseau qui permet l'accès à l'annuaire
  - un modèle de réplication
  - un modèle de distribution des données

Infrastructure de Gestion des Clefs
Le service de publication

- La structure de cet annuaire est libre mais le mode d'accès à distance fait l'objet de normes visant l'interopérabilité du service

- Généralement, les accès en lecture à l'annuaire sont totalement libres, mais celles qui concerne le dépôt d'informations sont par contre réglementés.

- La norme X509 définit le contenu des certificats et leur syntaxe de transfert, leurs formes binaires lors d'un appel sur le réseau.

Infrastructure de Gestion des Clefs
Le service de publication

- Le protocole consacré en matière d'annuaire est LDAP (Lightweight Directory Access Protocol)

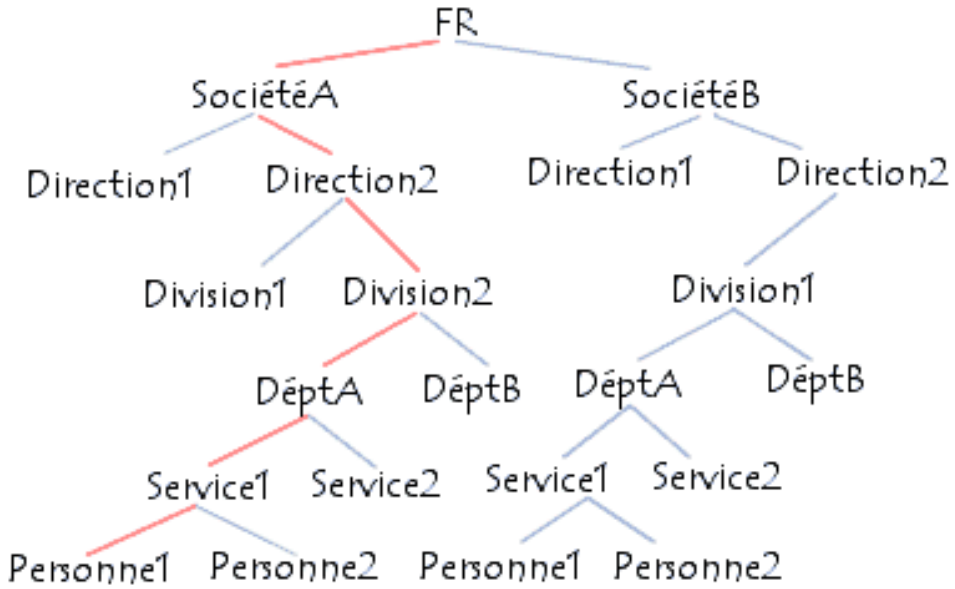
- LDAP définit :
  - Un protocole réseau
  - Un modèle d'information
  - Un espace de nommage
  - Un modèle de distribution.

- Une implantation simplifiée de X500 (DAP) sur TCP/IP (port standard 389).
  - Des données organisées sous forme d'une hiérarchie de couples {attribut, valeur}

Infrastructure de Gestion des Clefs
Le service de publication

- Les données LDAP sont structurées dans une arborescence hiérarchique.
- Chaque nœud de l'arbre correspond à une **entrée** de l'annuaire ou *directory service entry* (DSE) et au sommet de cette arbre (DIT) se trouve la *racine* ou *suffixe.*
- Ce modèle est en fait repris de X500 mais dans un contexte local.
- Les entrées correspondent à des *objets* abstraits ou issus du monde réel, ou des paramètres de configuration. Elles contiennent un certain nombre de champs appelés *attributs* dans lesquelles sont stockées des valeurs.

Infrastructure de Gestion des Clefs
Le service de publication



Infrastructure de Gestion des Clefs

Politique de certification

- Un ensemble de règles indiquant, ce pour quoi le certificat est applicable et par qui, et quelles sont les conditions de sa mise en œuvre au sens juridique, administratif et technique.

- Les facteurs pris en compte :
  - Les utilisateurs
  - Les moyens de collecte de l'information
  - La durée de vie de certificats
  - Le support matériel/logiciel des certificats
  - Le recouvrement des clés
  - La sécurité
  - Les services nécessitant une haute disponibilité
  - L'impact sur les structures existantes
  - La formation et l'information des utilisateurs

La RFC 2527 propose un plan type et décrit ce que doit obligatoirement contenir ce document

Infrastructure de Gestion des Clefs

Politique de certification

- Précise les règles de gestion des clés et des certificats
- Fixe les procédures à appliquer et les cas d'application
  - Identification des cas de gestion des clés et certificats
  - Rédaction des énoncés de pratiques de certification (CPS) pour chaque cas
  - Audit des outils et logiciels pour les failles techniques
- S'inscrit dans la politique de sécurité générale
  - Définition de la confidentialité des informations …

Infrastructure de Gestion des Clefs
Énoncés de pratiques de certification

- Description exhaustive de la façon dont la totalité des exigences énoncés dans la PC seront mises en place et observées par la CA
- Description détaillée de l'implantation effective des services offerts et des procédures associés à la gestion du cycle de vie des certificats
- Lien entre PC et CPS

Infrastructure de Gestion des Clefs
La liste de révocation

- CRL est une liste qui contient tous les certificats révoqués
- Nécessaire pour qu'un utilisateur puisse vérifier la validité d'un certificat
- Une CRL a un format standardisé et est signée à l'aide de la clé privée de la CA émettrice

Infrastructure de Gestion des Clefs
Révocation de certificat

- Cas de révocation :
  - Compromission de la clé secrète (perte, vol, …)
  - Modification des données d'authentification, des droits, …
- La vérification du certificat de *x* est la responsabilité de ses correspondants
- Méthode X509 : publication périodique dans le répertoire de la CA des CRL signées par la CA
- Une CRL contient :
  - L'algorithme de signature utilisé par la CA pour signer cette liste
  - L'émetteur
  - La date de mise à jour
  - La date de la prochaine mise à jour (optionnel)
  - La liste de couple (n° de série, date de révocation) listant les certificats révoqués
  - Signature de l'émetteur

Infrastructure de Gestion des Clefs
Révocation de certificat

- **Exemple de CRL**

Certificate Revocation List (CRL):

Version: 1 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: /C=FR/L=Paris/O=Albert\xE9 Dupont/OU=Certificate Authority/CN=prism CA/Email=ca@prism.fr

Last Update: Jan 6 2:10:15 2008 GMT

Next Update: Fév. 10 2:10:15 2008 GMT

Revoked Certificates:

Serial Number: 05

Revocation Date: Oct 6 2:10:21 2007 GMT

Signature Algorithm: md5WithRSAEncryption d5:92:09:ec:da:9f:cd: 46:bc:ef:05:85:f7:b8:01:b3:f5:60: ...

Infrastructure de Gestion des Clefs
Révocation de certificat

- L'avantage de la CRL est sa simplicité, sa richesse en information et son faible risque système.

- La taille de la CRL constitue son inconvénient majeur

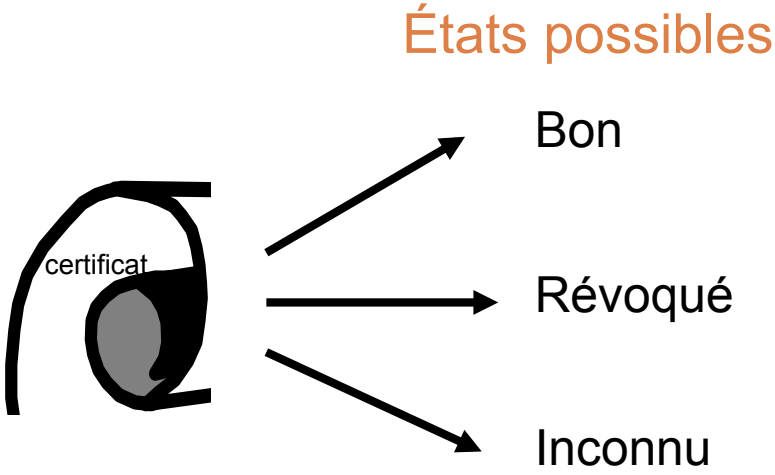
- Plusieurs façons d'implémenter la révocation de certificats :
  - Le mécanisme de publication périodique est la méthode la plus utilisée.
  - Le mécanisme de révocation en ligne (exemple : Online Certificate Status Protocol, OCSP)

- Pour garantir sa fraîcheur, la CRL contient la date de sa prochaine mise à jour.
  - une implosion des requêtes CRLs.

Infrastructure de Gestion des Clefs
Révocation de certificat : OCSP

- Protocole qui vérifie l'état du certificat
  - Les messages OCSP sont codés en ASN.1
  - Les messages peuvent être transportés par différents protocoles applicatifs.

- Les communications OCSP étant de la forme "requête/réponse", les serveurs OCSP sont appelés répondeurs OCSP.

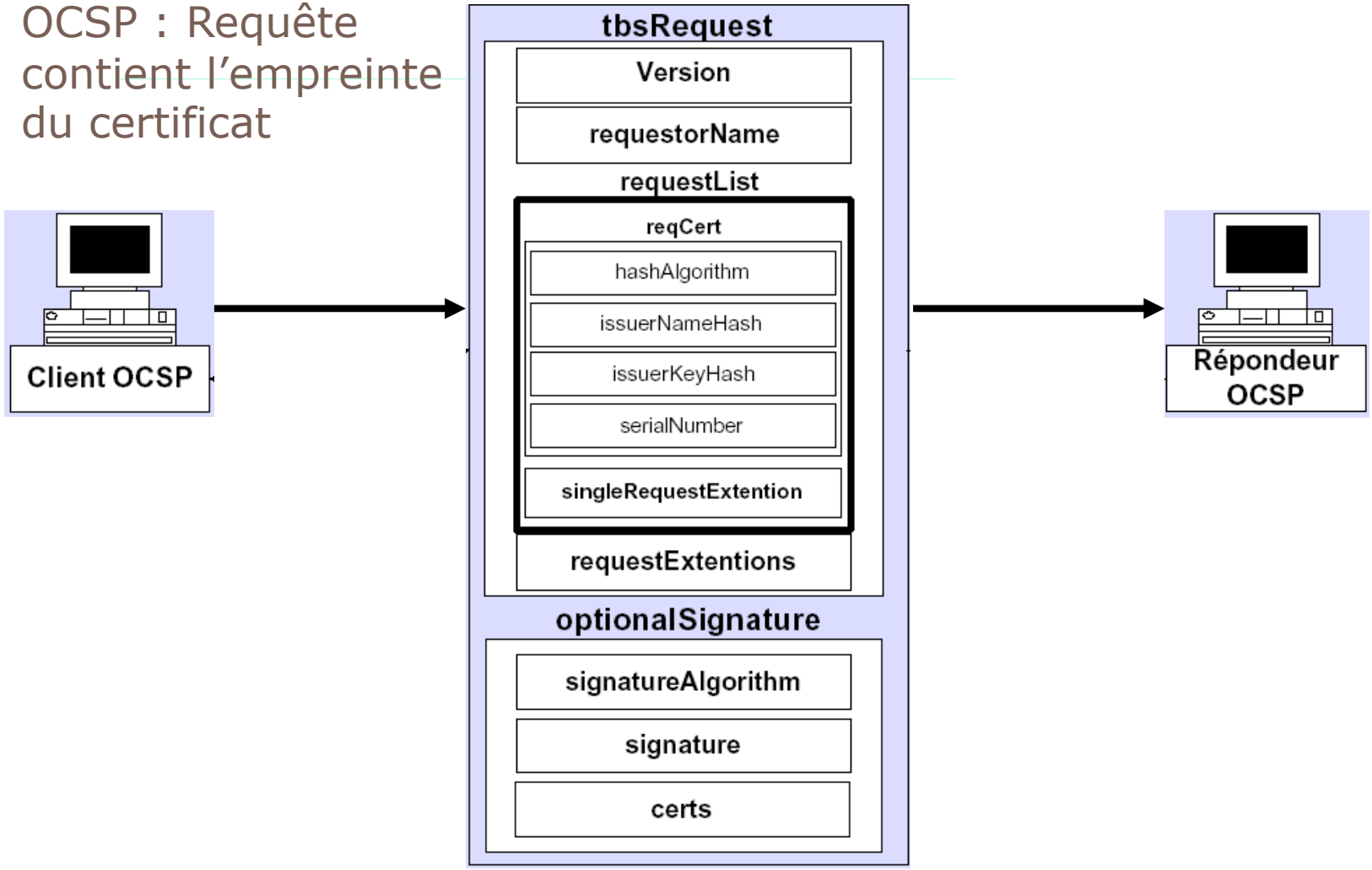


Infrastructure de Gestion des Clefs
Révocation de certificat : OCSP

- **Avantage par rapport aux CRL**
  - OCSP fournit des informations sur le statut du certificat plus à jour.
  - Le client n'a plus besoin de récupérer lui-même la CRL.
  - Le client n'a plus à traiter lui-même la CRL.
    - Le répondeur OCSP valide la remontée du chemin de certification.
  - Les CRL peuvent être comparées à une "liste de mauvais clients" d'une banque...
  - C'est le répondeur OCSP qui récupère les différents certificats constitutifs d'une chaîne de certificats et les CRL.

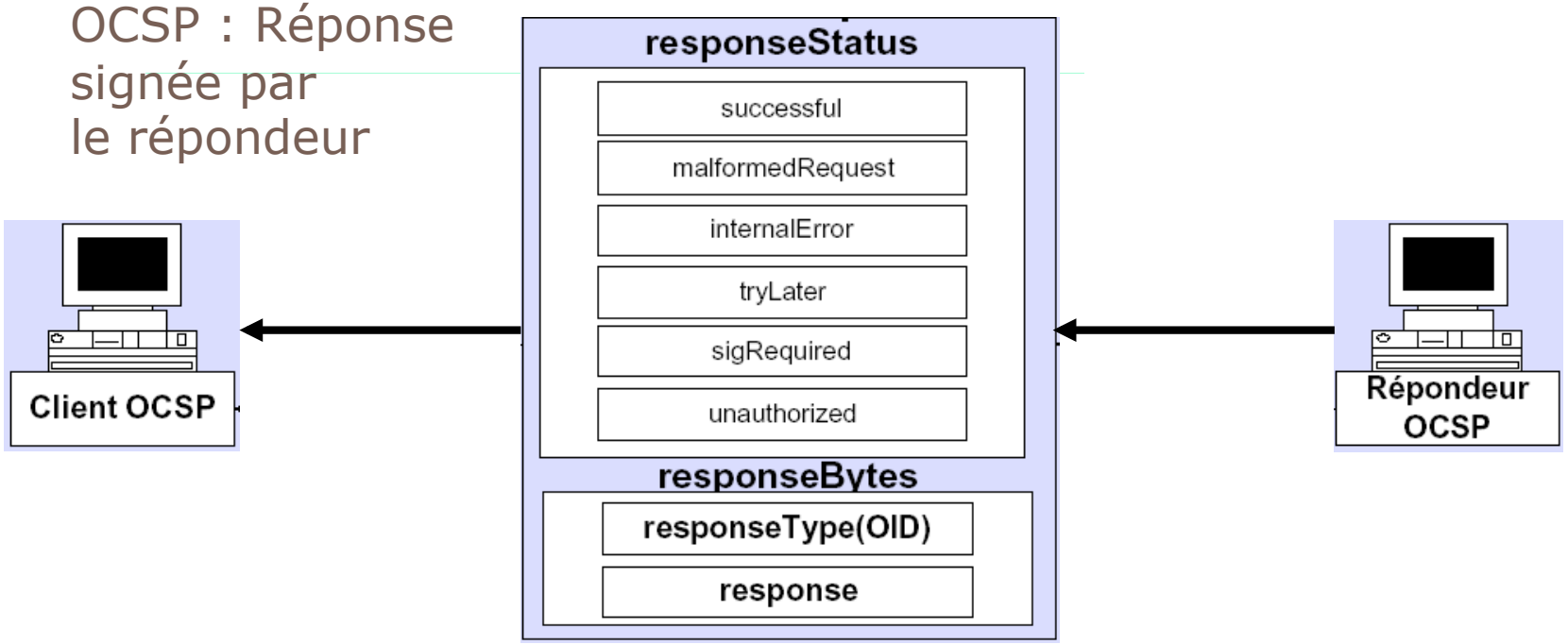
Infrastructure de Gestion des Clefs
Révocation de certificat : OCSP

OCSP : Requête contient l'empreinte du certificat



Infrastructure de Gestion des Clefs
Révocation de certificat : OCSP

OCSP : Réponse signée par le répondeur



Infrastructure de Gestion des Clefs PKIX

- PKI X509
  - Groupe de travail de l'IETF, 1995
- But: développer une PKI basée sur les certificats X509 pour Internet, IPKI pour Internet PKI

- PKIX utilise les certificats d'une PKI et les certificats d'attributs (AC pour Attribute Certificate) d'une PMI (Privilege Management Infrastructure)

- Composants :
  - Instanciation des certificats X509v3 et des listes de révocation X509v2
  - Protocoles d'exploitation pour la distribution des certificats et des listes de révocation
  - Protocoles de gestion pour les échanges entre les différents composants de la PKI
  - Règles d'usage et des considérations pratiques

Infrastructure de Gestion des Clefs
SPKI

- Simple PKI
  - Groupe de travail IETF créé en 1996
- But: définir une PKI et un format de certificats propres à l'IETF, simples et adaptés à l'ensemble des applications sur Internet

- Un certificat n'est plus « un moyen qui lie une clé à une identité » mais, un moyen d'attribuer des permissions au détenteur d'une clé

- Un certificat ou autre objet SPKI peut comporter, suivant sa fonction, tout ou une partie des champs suivants :
  - Émetteur
  - Sujet
  - Permission de délégation
  - Autorisation
  - Date et/ou test de validité

Infrastructure de Gestion des Clefs
SPKI

- Un certificat SPKI contient donc un ensemble d'attributs et d'autorisations

- Un certificat SPKI relie une autorisation à une clef publique, sans exiger nécessairement l'identité du détenteur de la clef privée correspondante.

- SPKI (codé en XML) a été proposé pour devenir une alternative au X.509 basé sur les PKIX.

Infrastructure de Gestion des Clefs
SPKI

- Les tests de validation sont de 3 types :
  - CRL temporisée
  - Revalidation temporisée
  - Revalidation à usage unique

- SPKI ne se charge pas de la distribution des certificats ➔ DNSSEC (Domain Name System SECurity)
  - Extension de DNS développée par l'IETF (RFC 2535)
  - Services fournis :
    - Distribution de clés ou de certificats
    - Authentification des données gérées par DNS
    - Authentification des requêtes et des transactions
    - ➔ DNSSEC transforme DNS en une PKI
  - Les extensions :
    - Key Resource Record
    - Cert Resource Record
    - Champ SIG

Infrastructure de Gestion des Clefs
SPKI

- Pour les petits systèmes, les propositions de SPKI offrent une vitesse de traitement élevée

- Malgré sa souplesse d'utilisation et de mise en œuvre, SPKI, utilisé pour des fins d'autorisation, ne s'est jamais imposé face à son concurrent X.509

- Son infrastructure décentralisée permet de mettre en œuvre de manière rapide une plate-forme de certification.

Infrastructure de Gestion des Clefs

Certificat d'Attributs

- Pourquoi ?
  - Besoin d'une gestion plus fine du contrôle d'accès : rules-based, role-based, rank-based
- Représente un lien fort entre l'identité du porteur et un attribut
- Les attributs ne sont pas inclus dans le certificat d'identité :
  - Ils peuvent être émis par une entité qui n'a aucun rapport avec la CA
  - La durée de vie d'un attribut peut être différente de celle du certificat d'identité

Infrastructure de Gestion des Clefs

Certificat d'Attributs

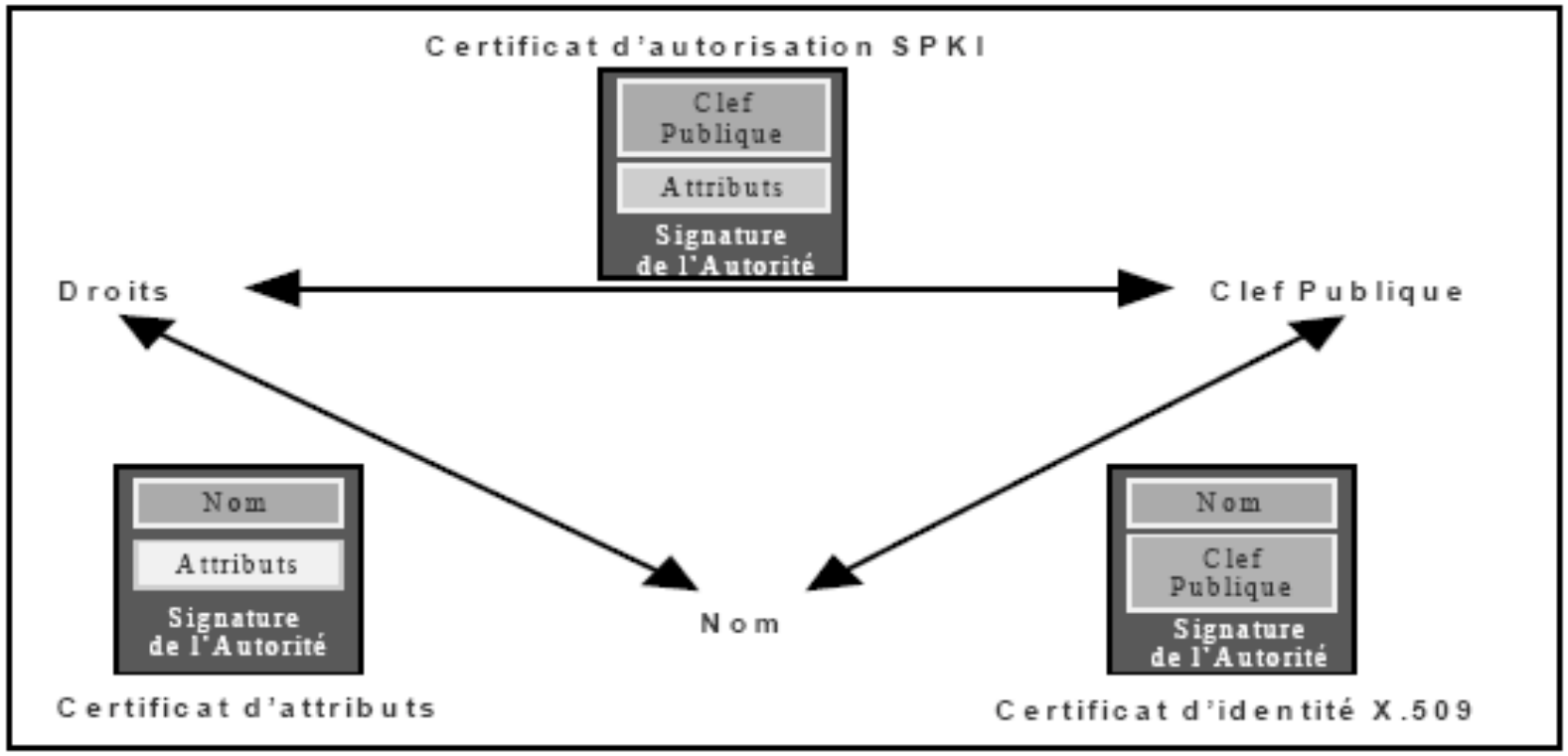
- Pour permettre l'ajout d'informations, telles que des attributs ou des privilèges, dans un certificat d'identité, la version trois de X.509 a introduit des options d'extension sous forme de blocks d'informations.

- La solution proposée par l'ITU-T est de scinder un certificat X.509 en deux :
  - un certificat d'identité qui consigne des informations sur l'identité
  - un certificat d'attributs qui enregistre des informations sur les attributs

- Cette solution simplifiera énormément le processus d'émission des certificats et pourra, dans certaines situations, éliminer le problème de la révocation.

Infrastructure de Gestion des Clefs

Certificat d'Attributs



Infrastructure de Gestion des Clefs

Certificat d'Attributs: les services offerts

- Un certificat d'attributs peut servir à :
  - Pour une personne
  - Pour un document ou un autre objet

- L'accès au certificat d'attributs relatif à une personne doit être autorisé par celle-ci ou par une personne en autorité par rapport à elle.

- L'utilisation du certificat d'attributs rend possible
  - La délégation des droits
  - La signature avec un rôle
  - Le contrôle de la multi-signature électronique.

Infrastructure de Gestion des Clefs

Certificat d'Attributs: les services offerts

L'habilitation/la délégation

- Une entité A fournit un certificat d'attributs à une entité B, pour qu'elle puisse effectuer en son nom des actions pendant une durée déterminée.
  - Le certificat d'attributs de B est composé de :
    - ses droits, son identificateur, le temps de validité des droits, l'identifiant de A, la signature de A, la capacité de B à déléguer à un tiers.

- B peut donc, dans certains cas et dans les mêmes conditions, habiliter à C et/ou D la signature de A, et ainsi de proche en proche pour créer une chaîne de délégation de signature dans laquelle le niveau de confiance ne se dégrade pas.

- Au total, ce schéma se présente comme une solution dans laquelle le propriétaire de l'application n'a pas besoin de stocker les droits des personnes autorisées, il a uniquement besoin de connaître le haut de la hiérarchie.

Infrastructure de Gestion des Clefs

Certificat d'Attributs: les services offerts

La certification de rôles

- Afin d'associer un pouvoir à une personne, en particulier le droit de signer, la sécurité emploie le concept de rôle.
  - Une identité peut jouer un ou plusieurs rôles, comme elle peut ne jouer aucun.

- Dans ce contexte, il y a quatre scénarios possibles :
  - Plusieurs entités liées à un rôle.
  - Une seule entité liée à un rôle.
  - Plusieurs rôles liés à une entité.
  - Une entité sans rôle.

- Exemple de rôles :
  - Direction de projet,
  - Direction de projet, signature des congés du personnel,
  - Direction de projet, embauche du personnel

Infrastructure de Gestion des Clefs

Certificat d'Attributs: les services offerts

Multi-signature électronique contrôlée

- La multi-signature électronique (appelée aussi signature de groupe) se base sur les mêmes principes que ceux de la signature électronique classique.

- Service utilisant le certificat d'attributs.
  - Celui-ci permet d'étendre la multi-signature d'un document en ajoutant des autorisations ou des contraintes particulières.

- Dans ce service, on attache un certificat d'attributs à un document:
  - Il indique les entités (clefs publiques ou identificateur) qui peuvent signer le document.
  - Il établit l'ordre dans lequel les signataires doivent signer le document.

Infrastructure de Gestion des Clefs
PMI (IGP)

- De plus en plus de systèmes exigent des règles d'accès qui ne sont pas présentes dans les certificats à clef publique, ni dans leurs extensions.
  - Privileges Management Infrastructure ou Infrastructure de gestion de privilèges.

- La PMI est une réponse au besoin d'autorisation d'accès aux ressources qui comprend :
  - Une autorité de gestion des attributs
  - Une politique d'attributs décrivant les attributs des entités
  - Une interface pour appliquer ces attributs aux ressources

- Entités :
  - Autorité d'Attributs (AA)
  - Service de publication des certificats d'attributs
  - Les listes de révocation des certificats d'attributs (ACRL, Attributes CRL)

Infrastructure de Gestion des Clefs
Composants avancés d'une PKI

- Service d'estampillage
- Service de levée de litiges
- Centre d'évaluation de la sécurité :
  - Audit et contrôle des différents composants de la PKI

Infrastructure de Gestion des Clefs

Composants avancés d'une PKI

- Service de séquestre et de recouvrement de clé:
  - Archivage et recouvrement des clés privées de chiffrement en cas de problèmes
  - Techniques de sauvegarde des clés de chiffrement

Infrastructure de Gestion des Clefs
Déploiement d'une PKI

- Identification du besoin (pourquoi faire?)
- Cadre d'utilisation :
  - Cadre non contractuel
  - Cadre contractuel privé
  - Droit public
- Volume des transactions
- Nombre d'utilisateurs
- D'après Carl Ellison and Bruce Schneier dans "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure", il existe 10 risques dans le déploiement
  - http://www.counterpane.com/pki-risks.pdf

Infrastructure de Gestion des Clefs
Déploiement d'une PKI

- Risque 1
  - A qui doit on faire confiance et pour faire quoi ?
- Risque 2
  - Qui utilise ma clé ?
  - Il est difficile de protéger une clé secrète
- Risque 3
  - Quel est le niveau de sécurité des systèmes de vérification ?

Infrastructure de Gestion des Clefs
Déploiement d'une PKI

- Risque 4
  - Comment être sûr que la clé publique correspond à la bonne personne ?
  - Un certificat associe une clé publique à une personne.
  - Mais il est difficile de savoir, quand on reçoit le certificat d'une personne, s'il s'agit effectivement de la personne que l'on connaît

- Risque 5
  - La CA est elle une autorité ?
  - La CA est une autorité par le fait qu'elle génère les certificats
  - Mais est-elle réellement certifiée ?
    - Les certificats délivrés par cette CA n'ont aucune valeur si elle n'est pas certifiée par une autorité reconnue
  - Comment contrôler la confiance des PKI acceptées comme PKI de confiance dans les applications en milieu ouvert (e-commerce)

Infrastructure de Gestion des Clefs
Déploiement d'une PKI

- Risque 6
  - L'utilisateur fait-il partie de l'architecture sécurisée ?
- Risque 7
  - Quel modèle de PKI choisir ?
- Risque 8
  - Jusqu'à quel point l'utilisation des certificats est-elle sûre?

Infrastructure de Gestion des Clefs
Déploiement d'une PKI

- Risque 9
  - L'utilisation des certificats pose des problèmes de protection des données personnelles
- Risque 10
  - Comment faire confiance à la révocation?