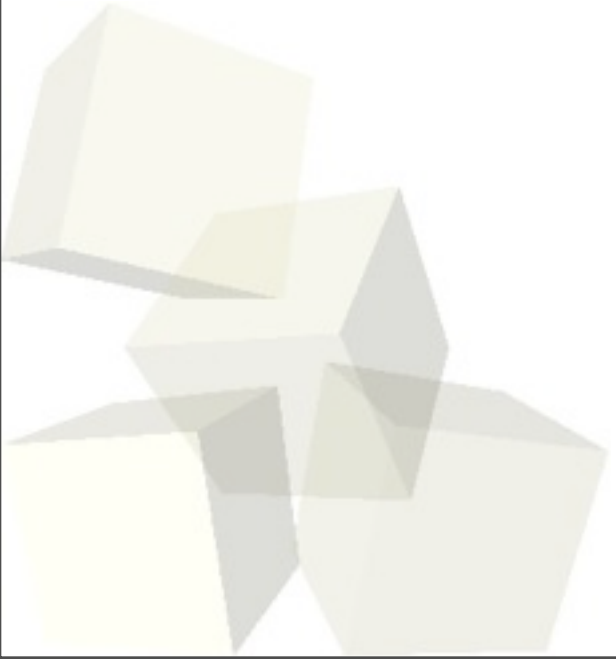
Introduction au PKI
Public Key Infrastructure



Problèmes génériques

- Performances médiocres :
  - Utilisation de clé de session.
  - Utilisation de fonctions hash.
- Certification des clés publiques :
  - Garantir/vérifier la relation clé/utilisateur.
  - PKI : Public Key Infrastructure.

Public Key Infrastructure (PKI)

- Objectif :
  - Garantir la validité des clés publiques
- Principes :
  - Autorités de Certification
  - Distribution des clés publiques des AC
  - Certificats d'une clé publique = signature de la clé par l'AC correspondante

- Distribution des clefs publiques
  - Idée de départ
    - → Simple annuaire des clefs publiques
  - Problèmes à résoudre
    - → Distribuer les clefs de façon authentifiée et intègre
    - → Stocker les clefs de façon sûre (protection en intégrité)
      - Limiter le nombre de clefs à stocker
  - Solution = certificats et hiérarchies de certification
    - → Élément de transport d'une clef publique, dont l'authenticité est vérifiable de façon autonome
    - → Authentification : Lie une clef publique à son possesseur
    - → Intégrité : Toute modification du certificat sera détectée

Certificat

- **Certificat**
  - Certificat = Structure de données
    - ➔ Permet de lier une clef publique à différents éléments, au moyen de la signature d'une autorité de confiance :
      - Nom du propriétaire de la clef
      - Dates de validité
      - Type d'utilisation autorisée
      - …
    - ➔ Format actuel : X.509v3, profil PKIX
  - Émis par une autorité de certification (**Certificate Authority – CA**)
    - ➔ Garantit l'exactitude des données
    - ➔ Certificats vérifiables au moyen de la clef publique de la CA, seule clef à stocker de façon sûre
  - Listes de révocation **(Certificate Revocation List – CRL)**
    - ➔ Permettent de révoquer des certificats avant leur expiration normale

- Les certificats sont des fichiers divisés en deux parties
  - La partie contenant les informations
  - La partie contenant la signature de l'autorité de certification

- La structure des certificats est normalisée par le standard X.509 de l'UIT (X.509v3), qui définit les informations contenues dans le certificat :
  - La **version** de X.509 à laquelle le certificat correspond ;
  - Le **numéro de série** du certificat ;
  - L'**algorithme de chiffrement** utilisé pour signer le certificat ;
  - Le **nom** (DN, pour Distinguished Name) de l'autorité de certification émettrice ;
  - La **date de début de validité** du certificat ;
  - La **date de fin de validité** du certificat ;
  - L'**objet de l'utilisation de la clé publique** ;
  - La **clé publique** du propriétaire du certificat ;
  - La **signature** de l'émetteur du certificat (thumbprint).

Certificat

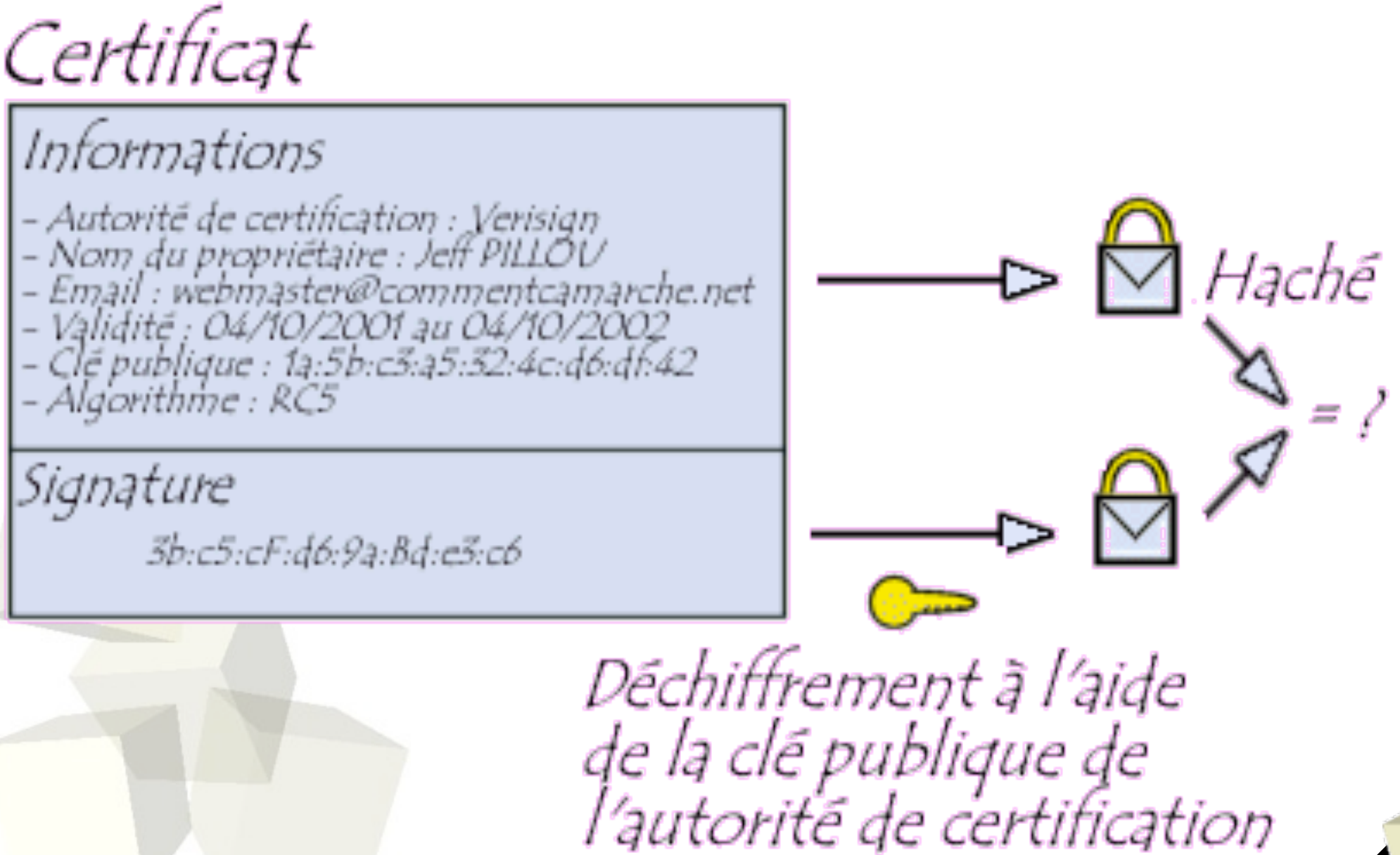
Informations

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

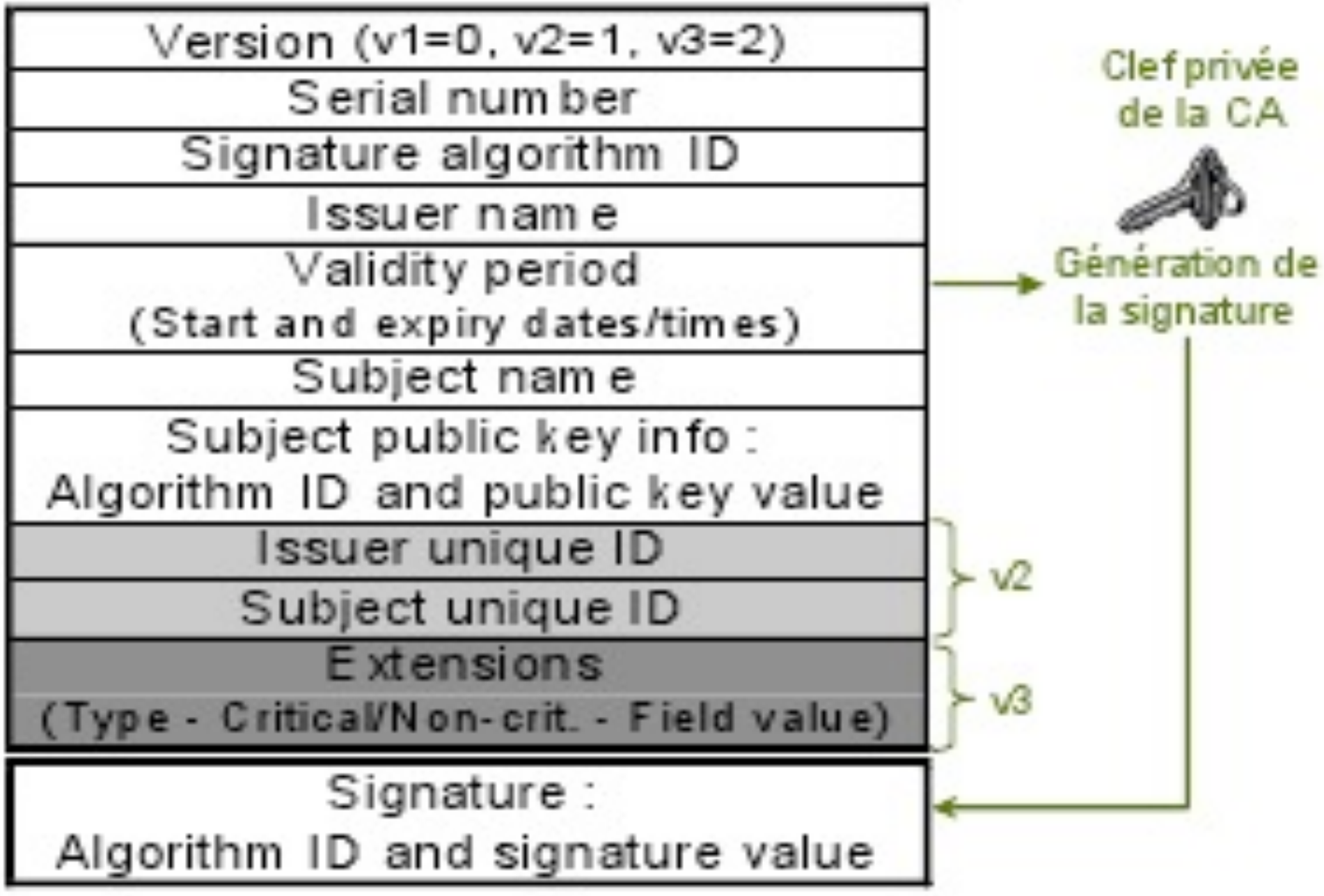
Signature

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

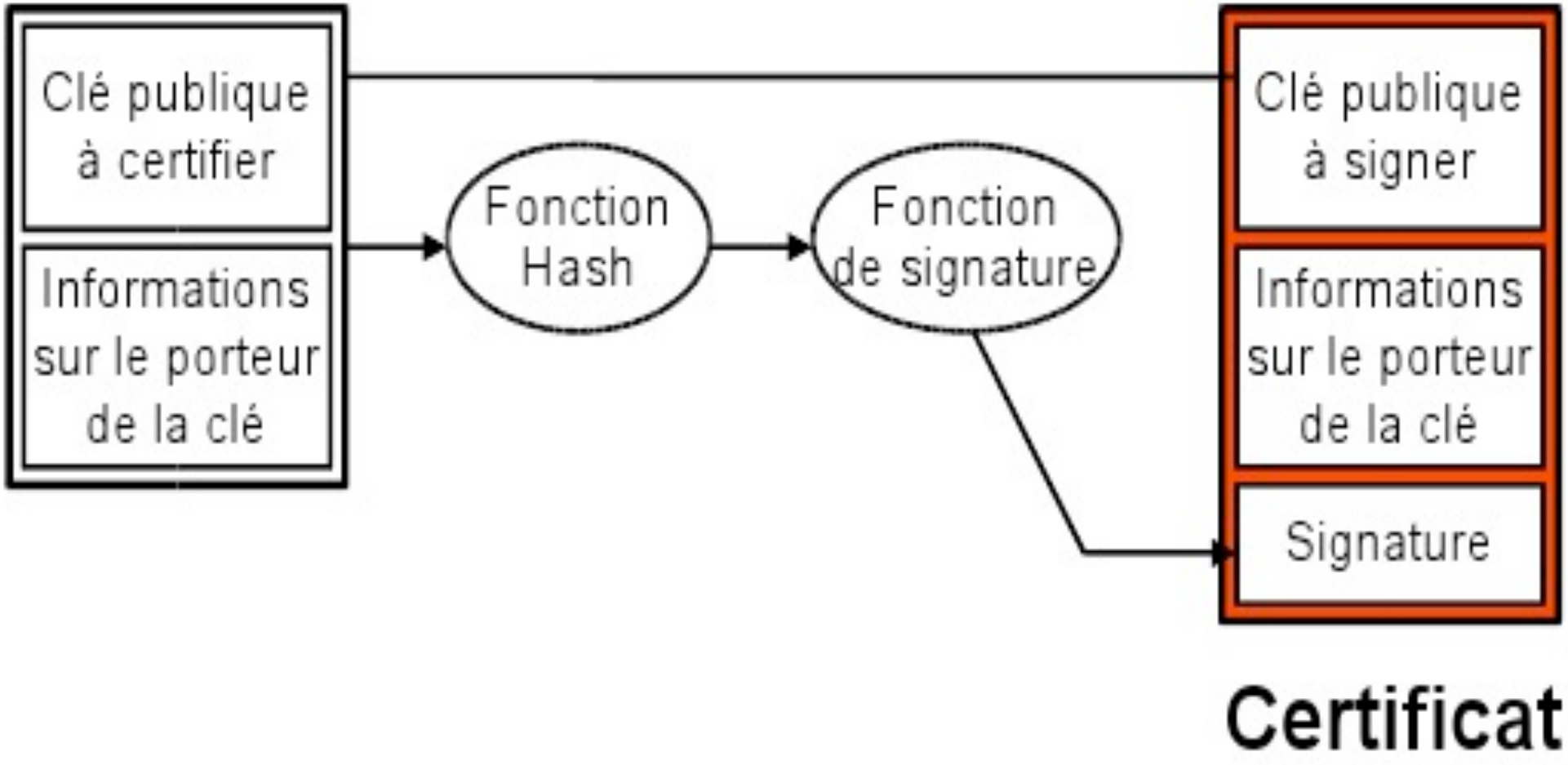
- Vérification d'un certificat :



Les certificats X.509v3



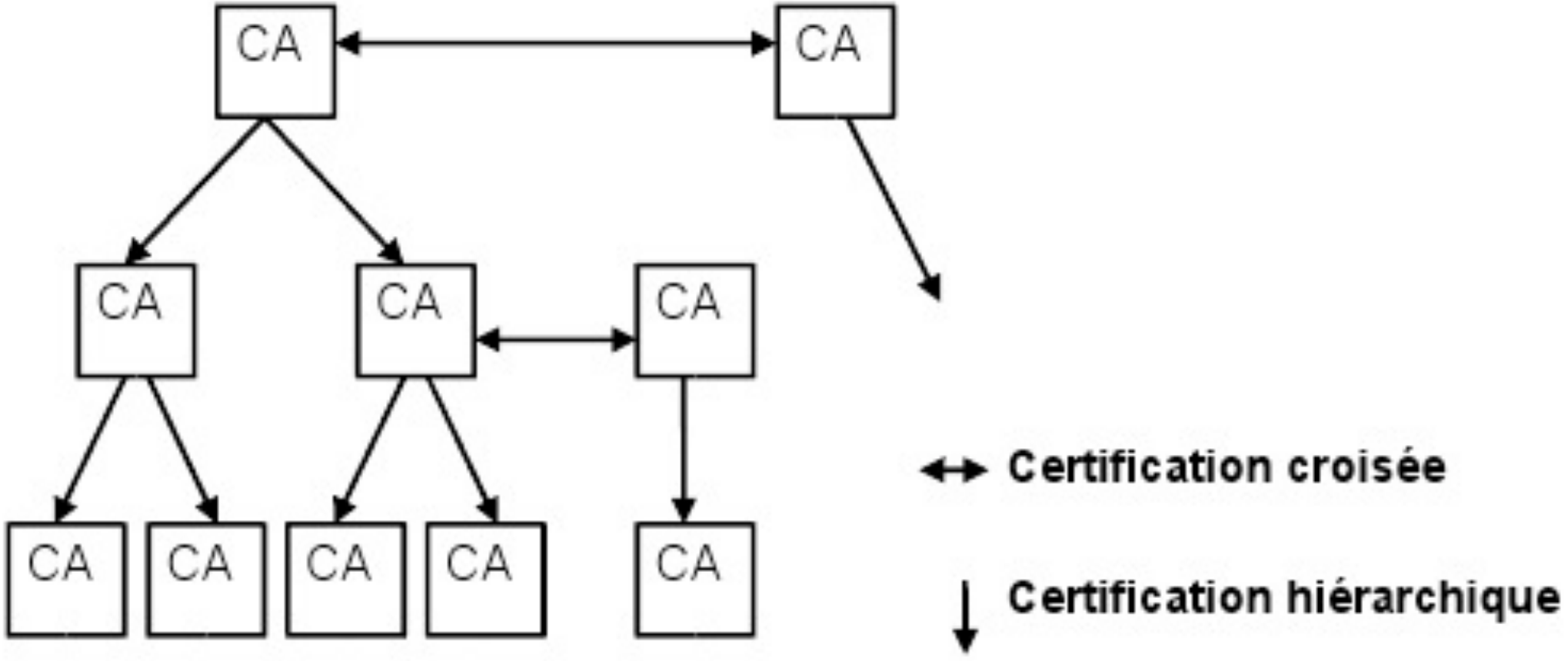
Gestion/certification de clé



PKI

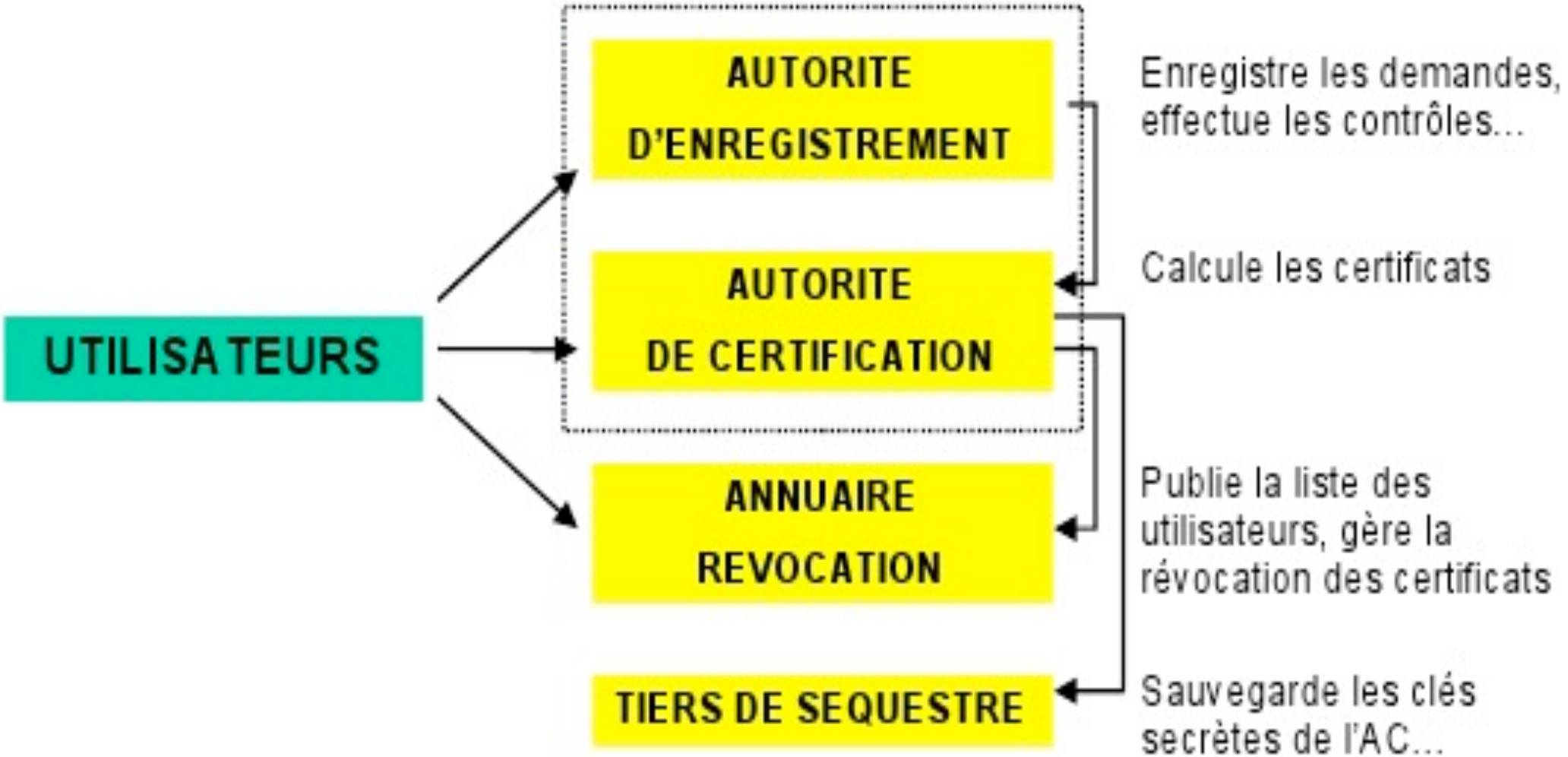
Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI)



Autorités de certification

Public Key Infrastructure (PKI)



Gestion/certification de clé

- Organisation d'un PKI