Chapitre 5

Mécanismes cryptographiques de la sécurité

Remarques:

1) Ce document constitue un aperçu général (plan détaillé) des chapitres sur les notions cryptographiques

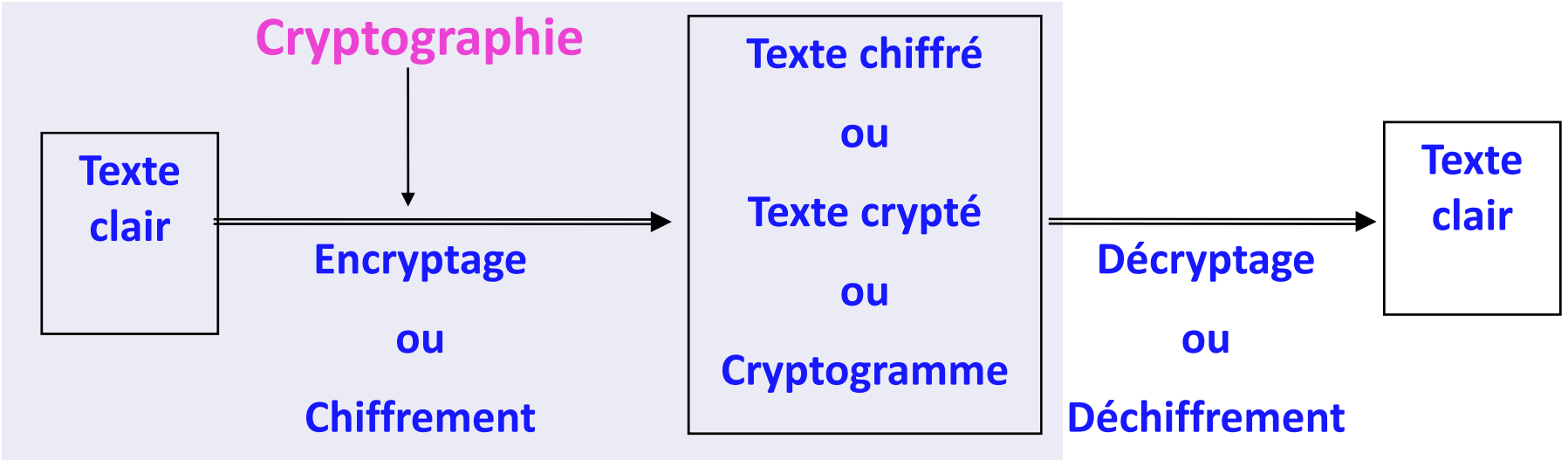
2) Ce document doit être complété par les notes de cours

Définitions

- Cryptologie (Cryptology) :
  - Science (branche des mathématiques) des communications secrètes.
  - Composée de deux domaines d'études complémentaires :
    - Cryptographie
    - Cryptanalyse.

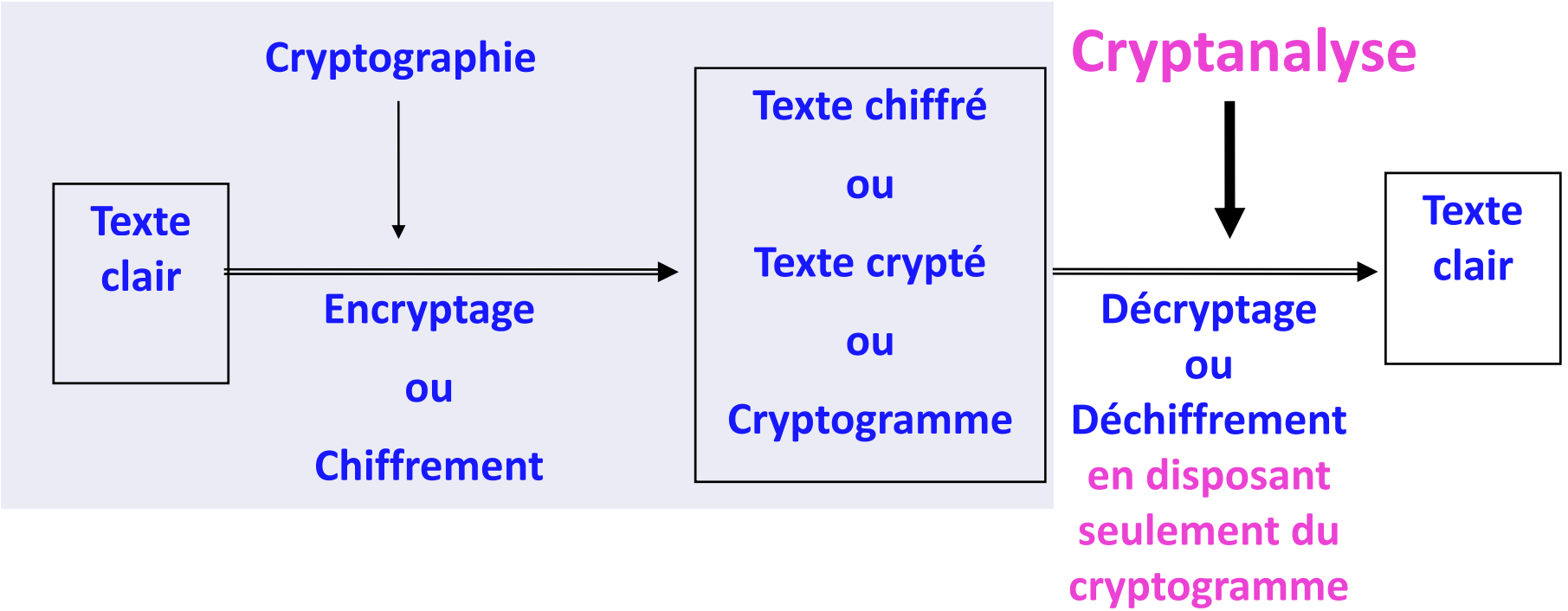
Définitions

- Cryptographie (cryptography) = Chiffrement=Encryptage
  - Ensemble des méthodes et techniques qui permettent de transformer un message afin de le rendre incompréhensible pour quiconque n'est pas doté du moyen de le déchiffrer.
    - On parle d'***encrypter*** (***chiffrer***) un message,
    - Le code résultant s'appelle ***cryptogramme***.
    - L'action inverse s'appelle ***décryptage*** (***déchiffrement***).



Définitions

- Cryptanalyse (cryptanalysis)
  - **Art de révéler les messages** qui ont fait l'objet d'un encryptage.
  - Lorsqu'on réussie, au moins une fois, à **déchiffrer un cryptogramme**, on dit que l'**algorithme** qui a servi à l'encrypter a été **cassé**.



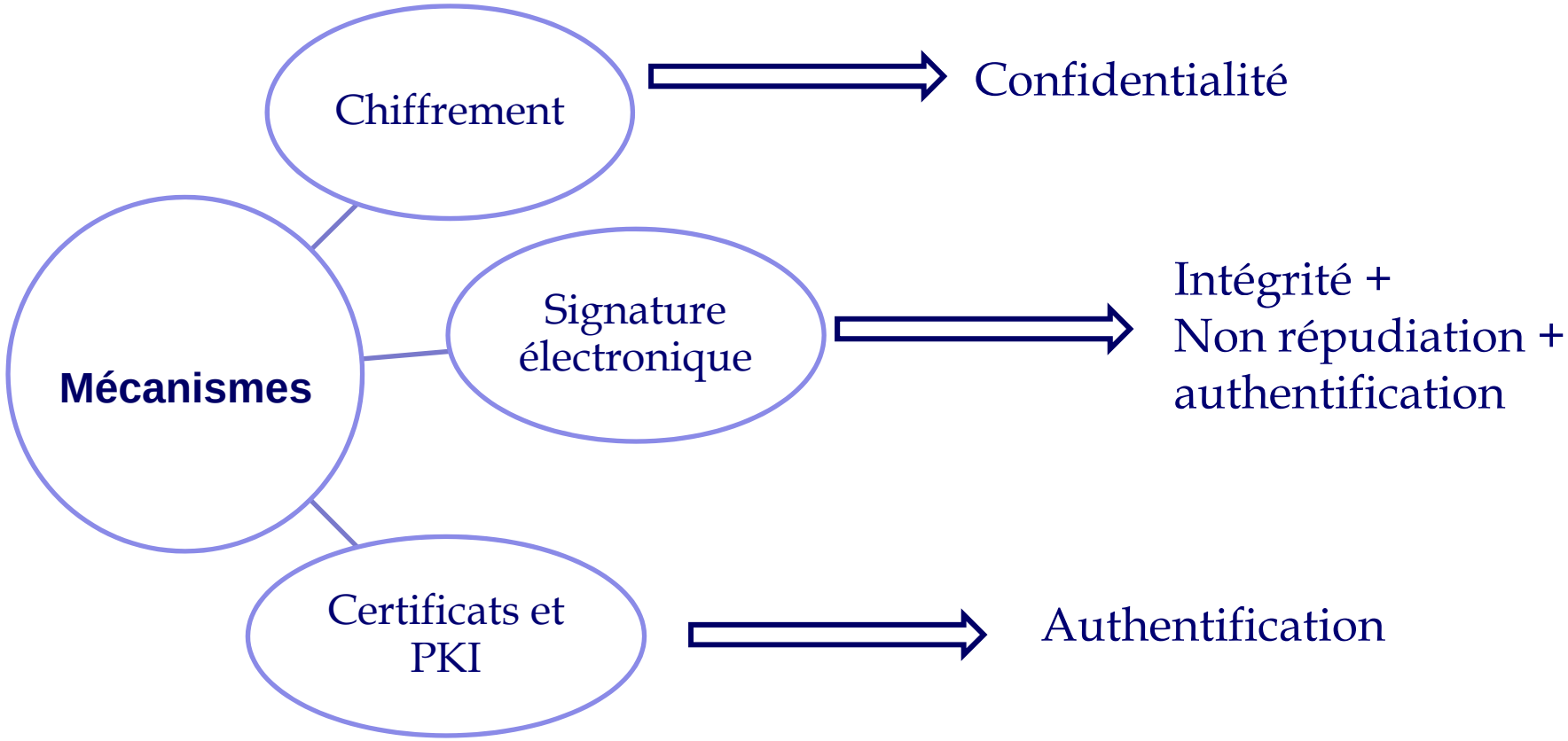
Définitions

- Clé :
  - Information qui sera utilisée pour encrypter et / ou décrypter un message.

    *On peut cependant concevoir un algorithme **qui n'utilise pas de clé**, dans ce cas c'est lui-même qui constitue le secret et son principe représente la clé*

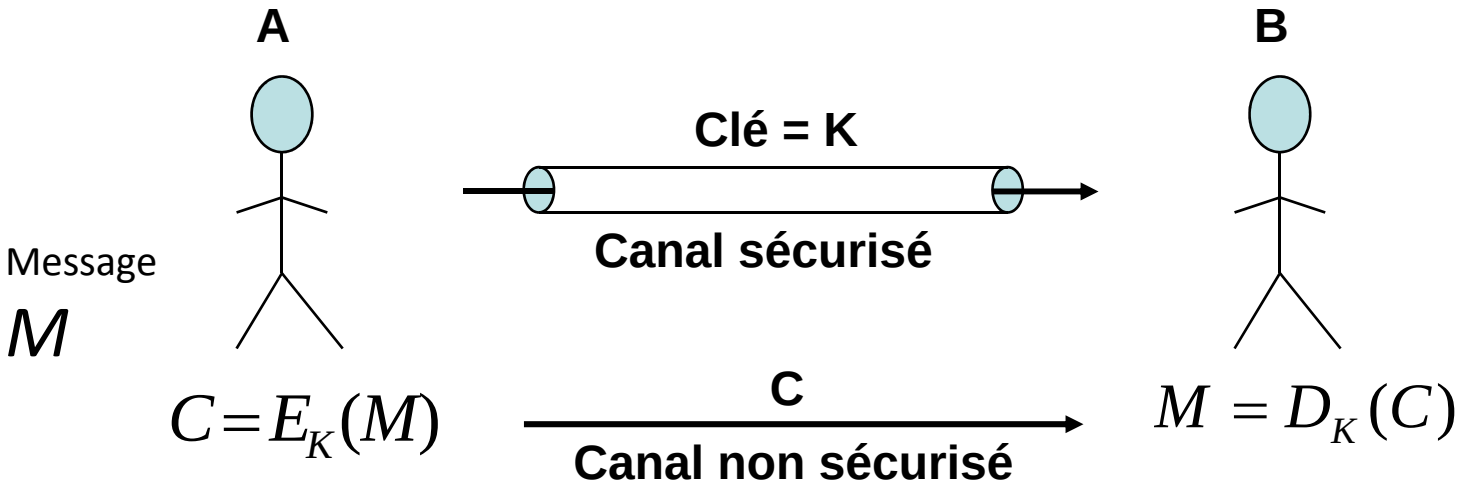
- Crypto système:
  - Ensemble composé d'un algorithme, de tous les textes en clair, de tous textes chiffrés et de toutes clés possibles.

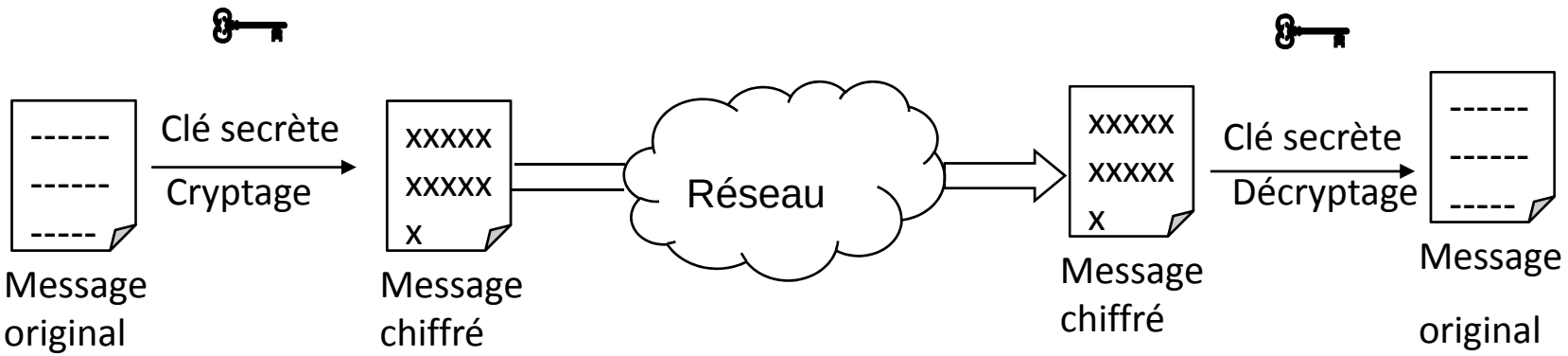
Mécanismes cryptographiques de la sécurité



Chiffrement

- Chiffrement symétrique

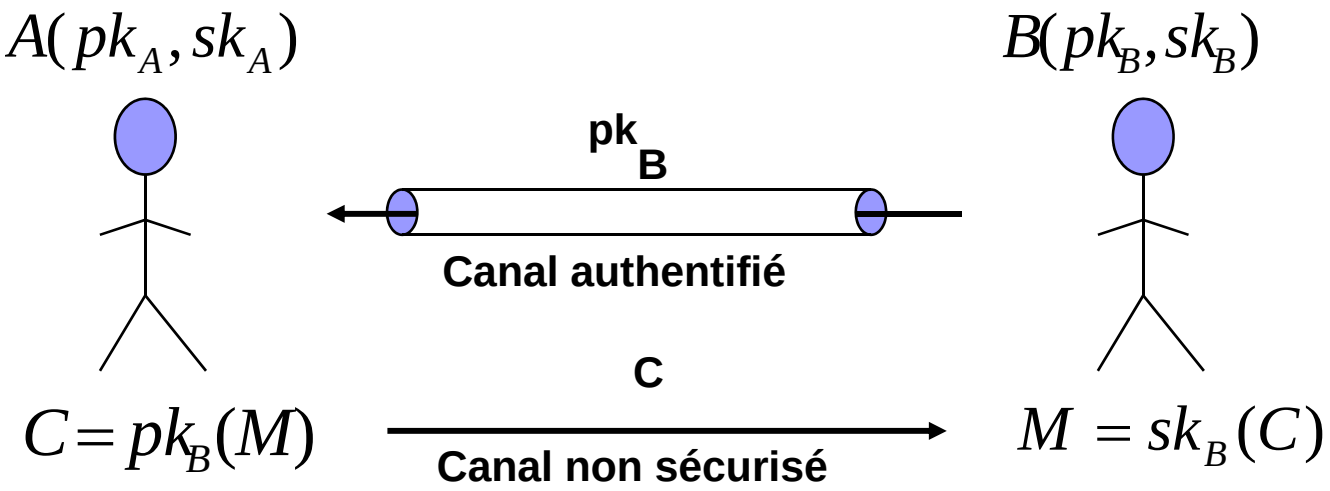


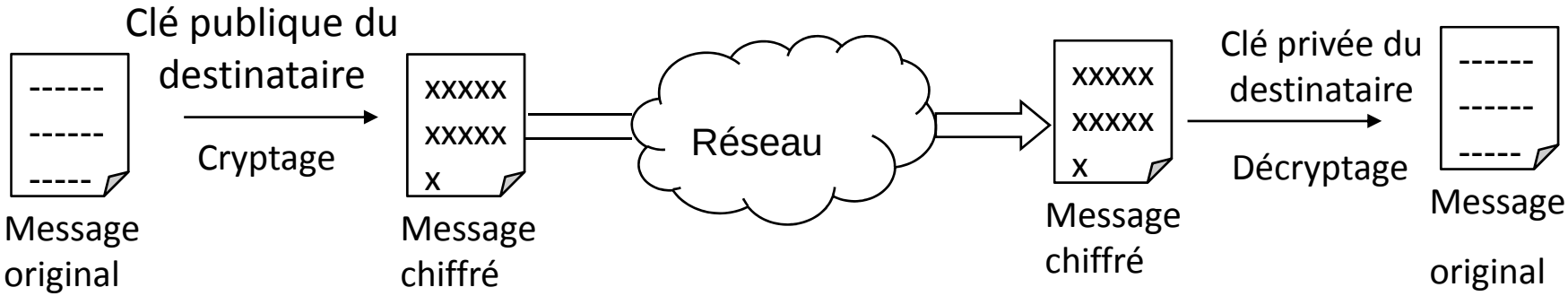


- Exemples: DES, AES, IDEA…

Chiffrement

- Chiffrement asymétrique

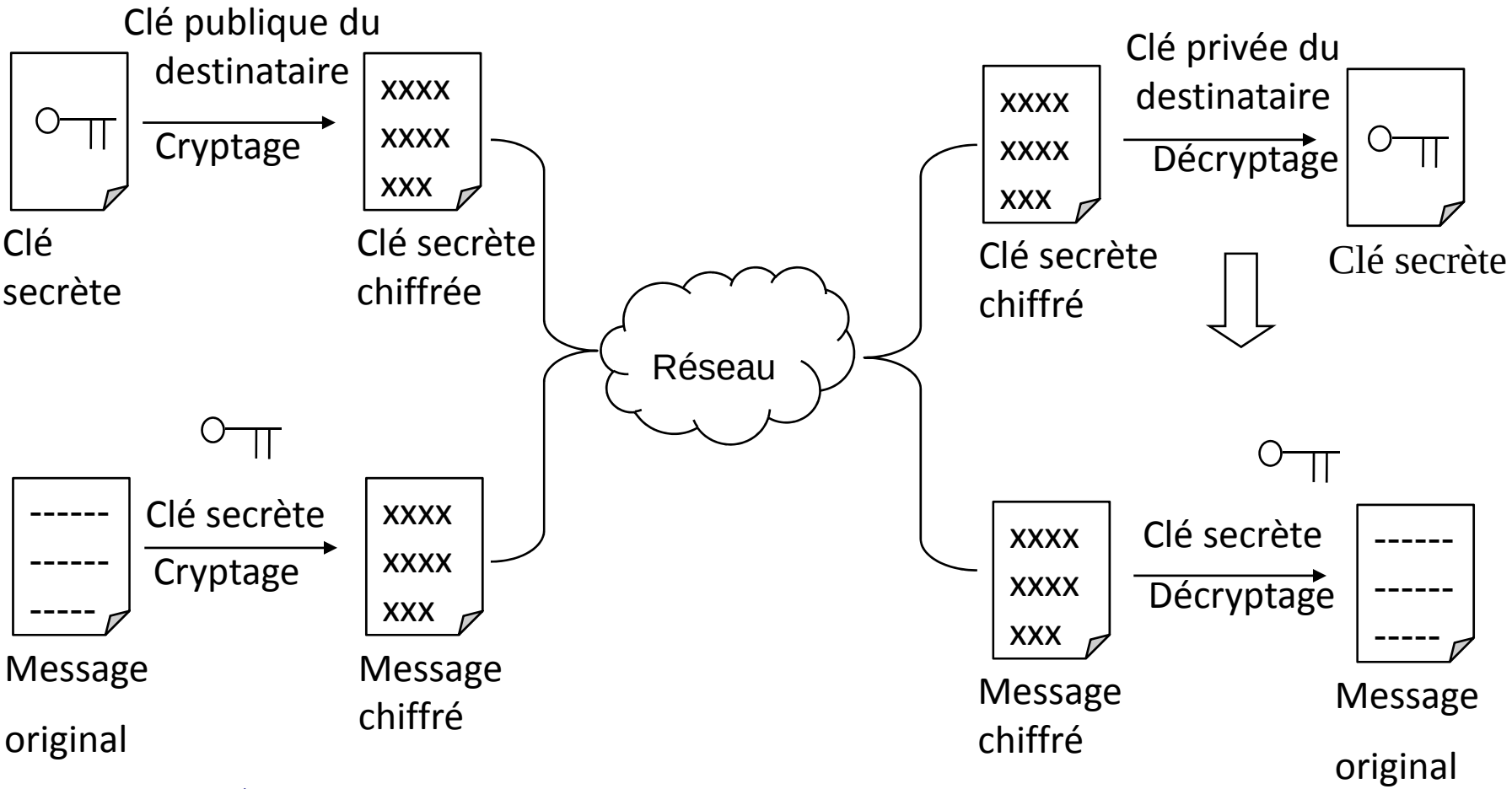




- Exemples: RSA, Rabin, Elgamal…

Chiffrement

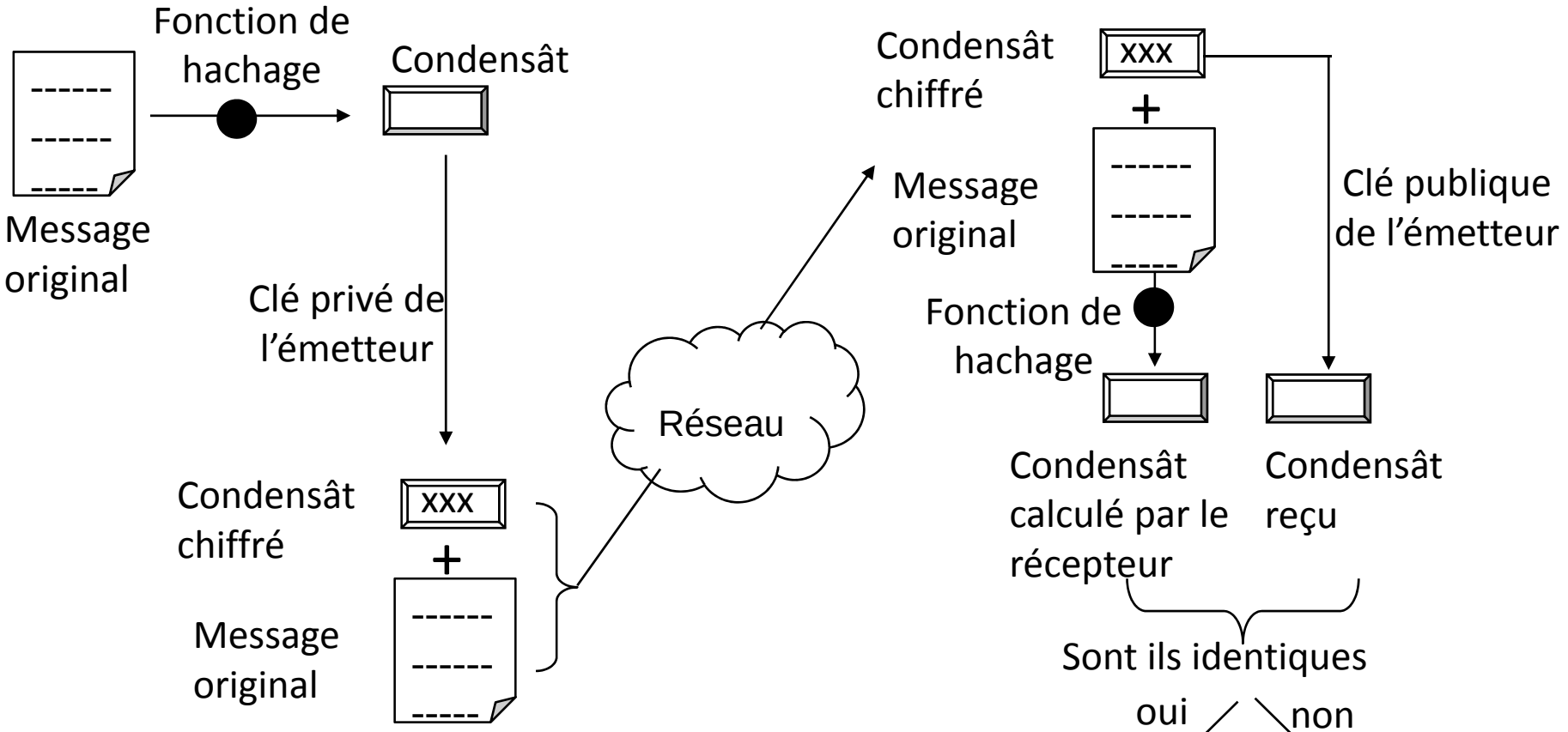
- Chiffrement hybride



- Exemples: PGP, GnuPG

Signature électronique

- Permet l'authentification, l'intégrité et la non répudiation



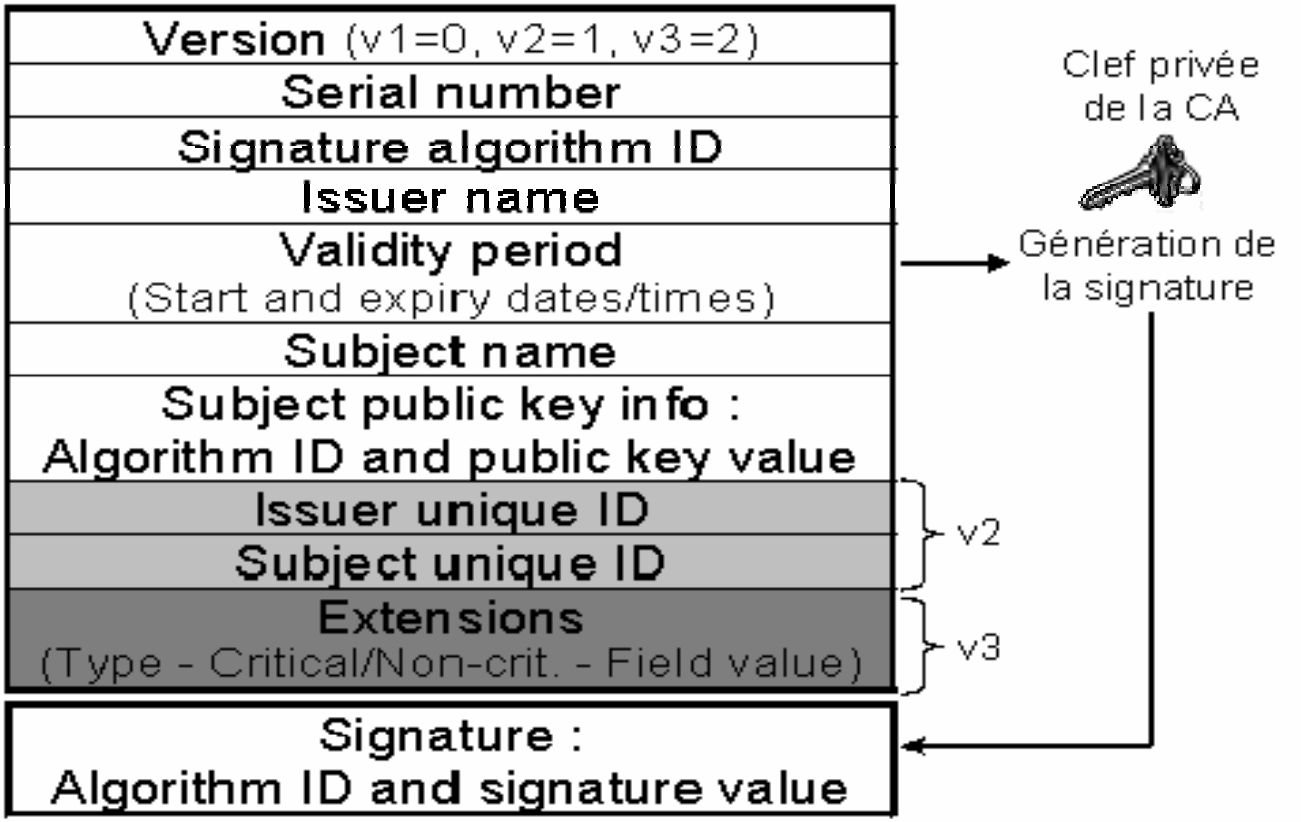
- Exemples: signatures RSA, Elgamal, Rabin, Schnorr, ESIGN…

- Fonction de hashage
  - H (M) = C
    - M est de taille quelconque
    - C est de taille fixe (16 ou 20 octets)
      - appelé condensât, ou empreinte, ou fingerprint, ou message digest
  - Fonction à sens unique
  - Si H (M_1) = C_1 ,
    - il est très difficile de trouver :
      M_2 différent de M_1 tel que H (M_2) = C_1
  - Usage : checksums, « intégrité »

- Exemples
  - MD5, SHA-1

Certificat numérique

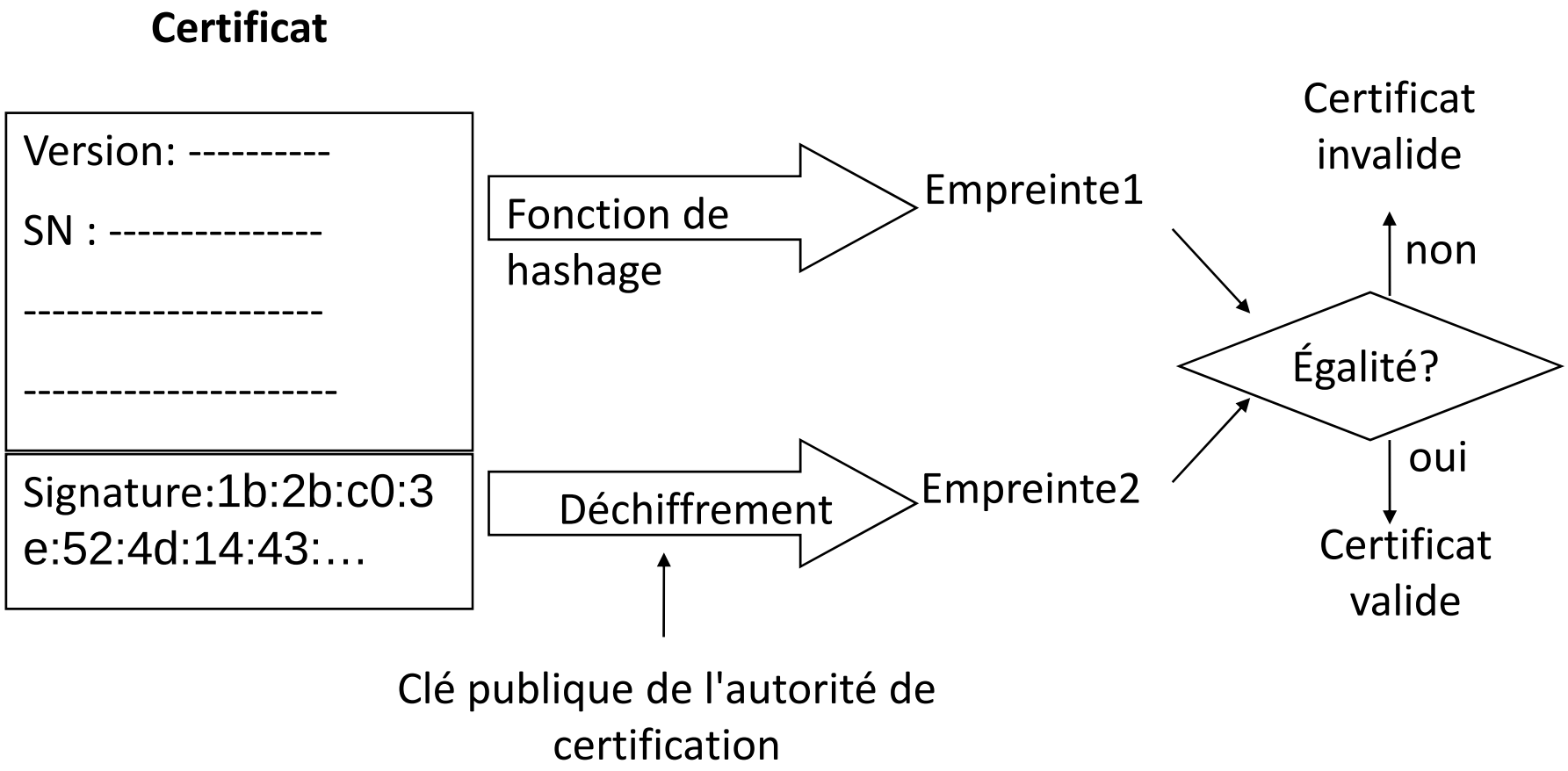
- Permet l'authentification
  - Garantit l'appartenance d'une clé publique à une entité
- Principal format: **certificats X.509**



Certificat numérique

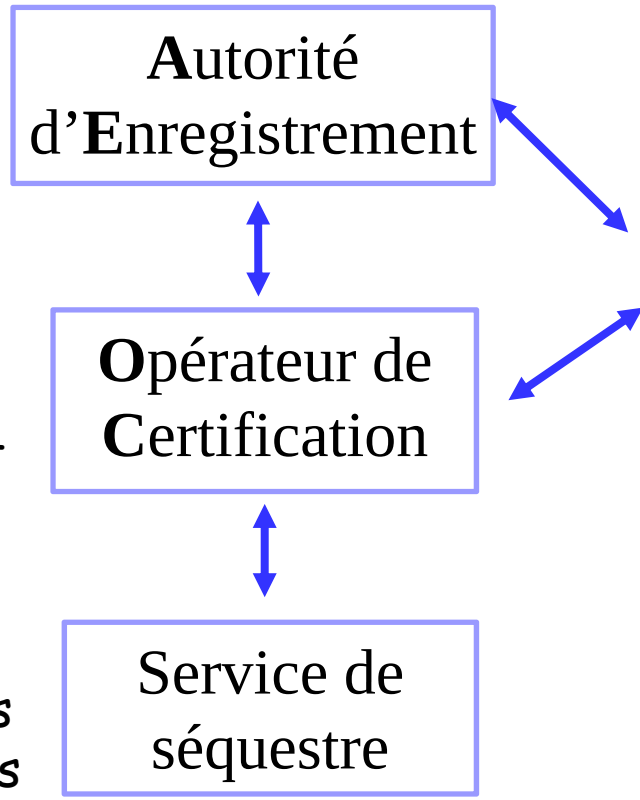
- *Serial number* :
  - Numéro de série du certificat (propre à chaque CA).
- *Signature Algorithm ID :*
  - Identifiant du type de signature utilisée.
- *Issuer Name :*
  - *Distinguished Name (DN)* de CA qui a émis ce certificat.
- *Subject Name :*
  - *Distinguished Name (DN)* du détenteur de la clé publique.
- *Subject public key info :*
  - Informations sur la clé publique du certificat.
- *Signature :*
  - Signature numérique du CA sur l'ensemble des champs

Vérification d'un certificat



PKI: Public Key Infrastructure

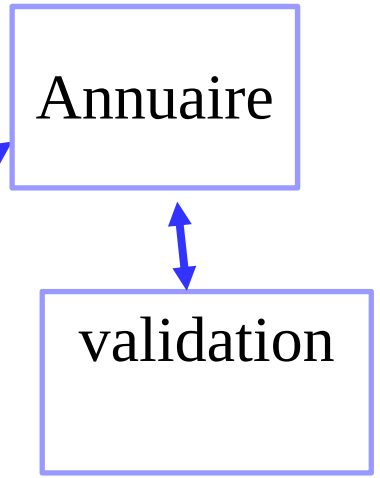
Traitement des demande de:
- Création
- Révocation
- Renouvellement de certificats



- Création
- Révocation
- Renouvellement de certificats

Archiver les clés privées/publiques

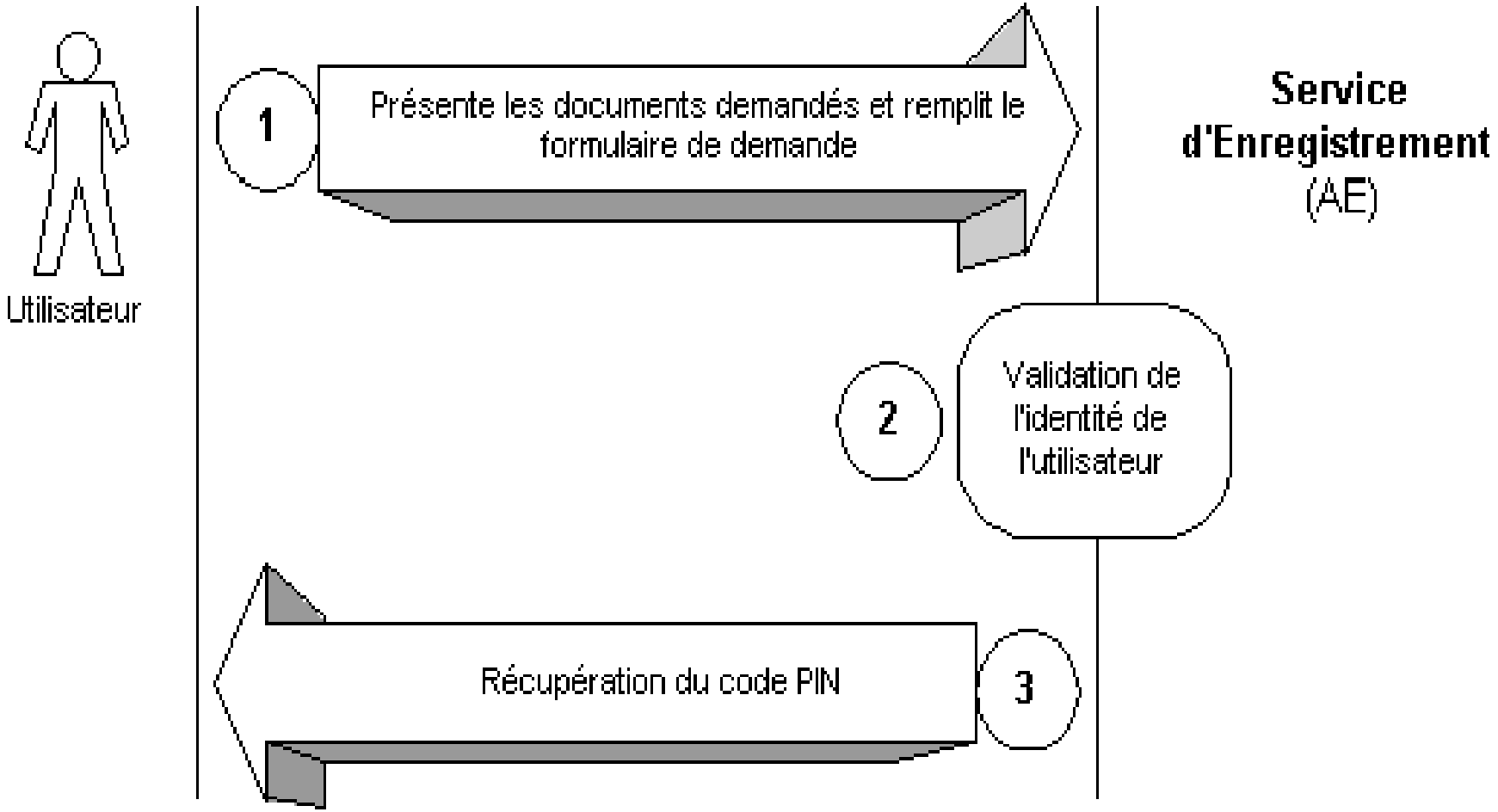
Publication des certificats émis ou révoqués



Vérifier la validité des certificats

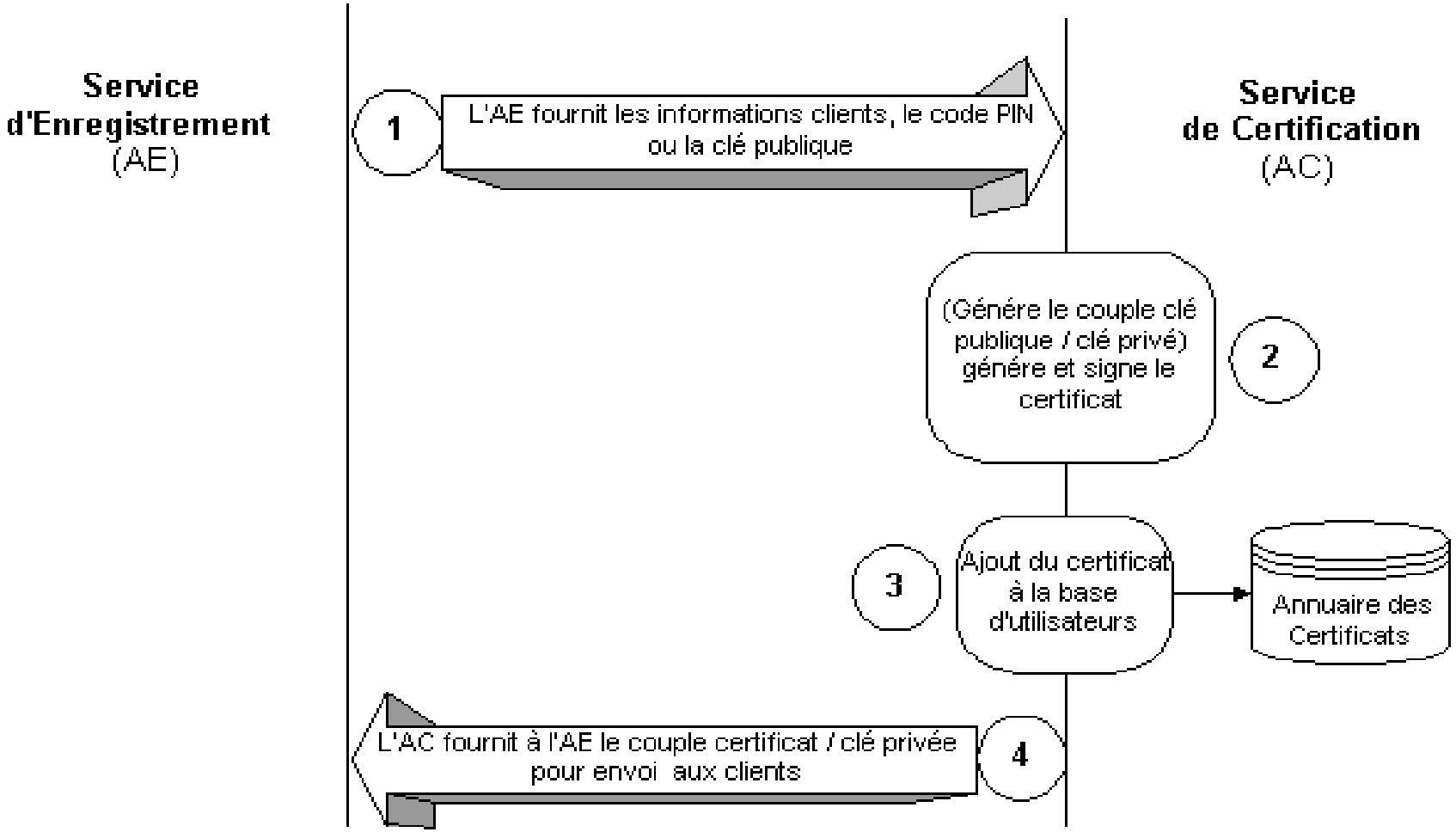
PKI: Exemple de fonctionnement

- Enregistrement



PKI: Exemple de fonctionnement

- Création de certificats



PKI: Fonctionnement