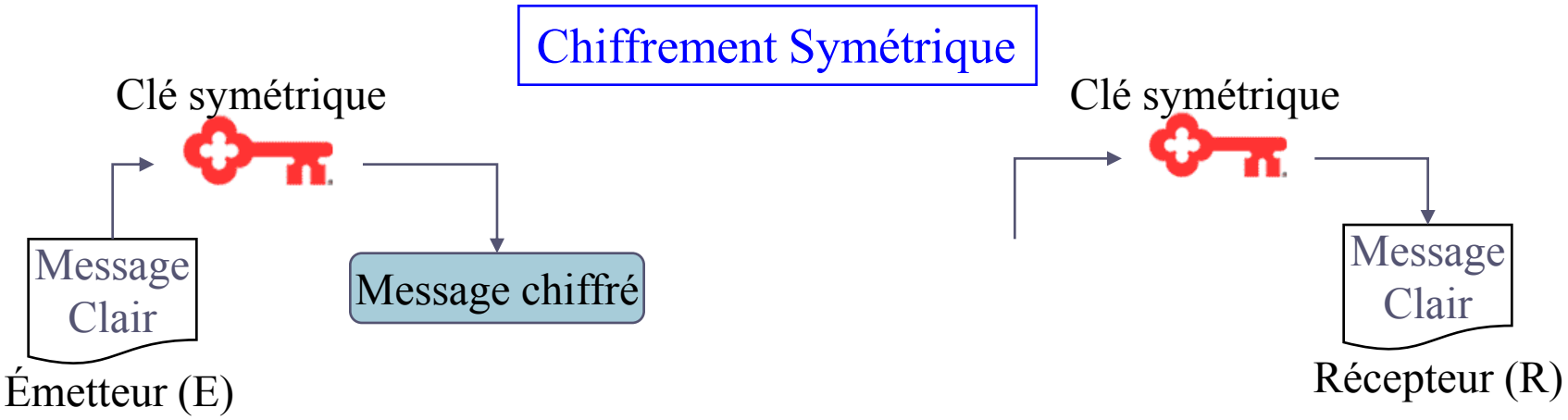
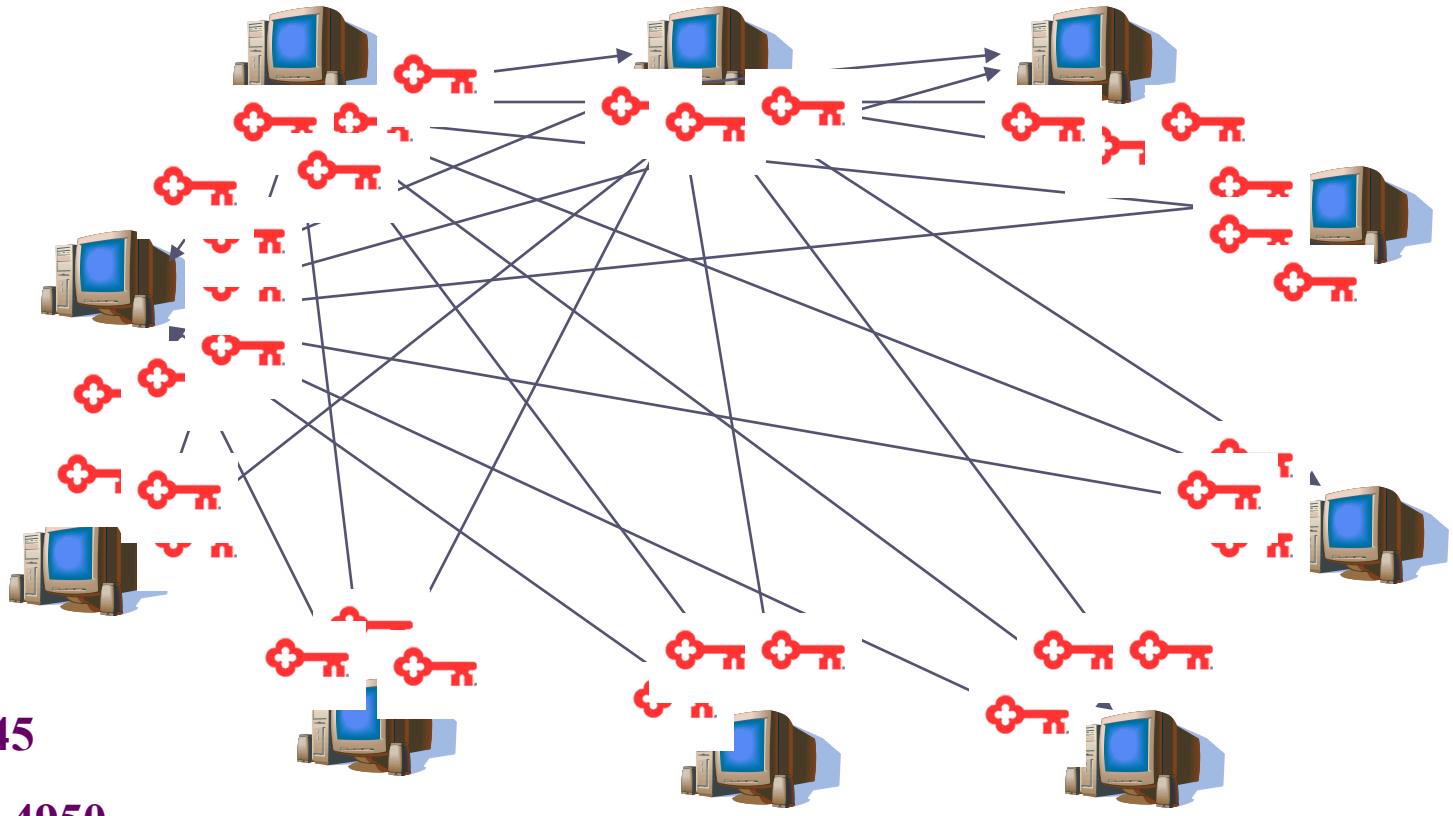
PKI: Infrastructures à Clés Publiques

Dr. Y. Challal

Contexte: Cryptographie à clé publique
Confidentialité



Contexte: Cryptographie à clé publique
Confidentialité: limite du chiffrement symétrique

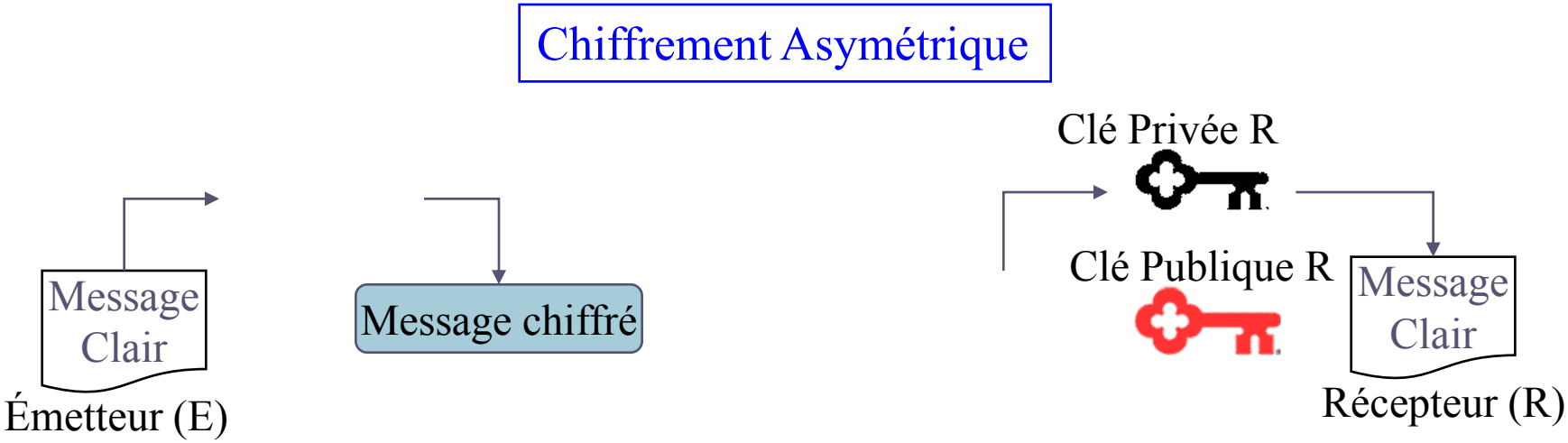


10 → 45

100 → 4950

5000 → 12.497.500

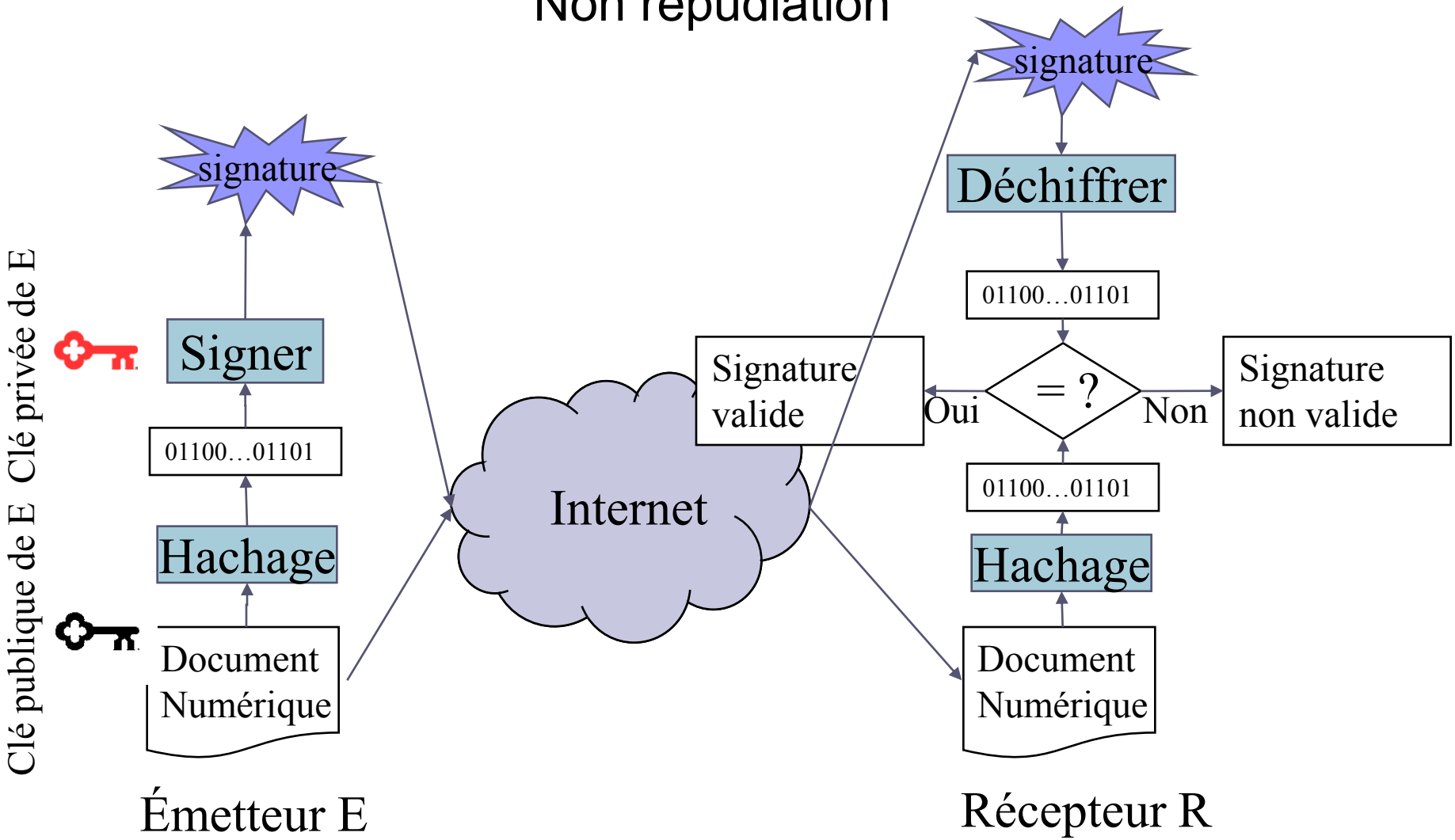
Contexte: Cryptographie à clé publique
Confidentialité



- Il suffit d'un bi-clés par utilisateur pour sécuriser les communications d'une communauté

- Il faut n bi-clés et non plus n(n-1)/2 clés symétriques

Contexte: Cryptographie à clé publique
Non répudiation



Contexte: Cryptographie à clé publique
Authentification

Défi

Hachage

Condensat

Clé privée

Chiffrement

B

Réponse

Défi

Hachage

Condensat

= ?

Condensat

Clé publique

Déchiffrement

B

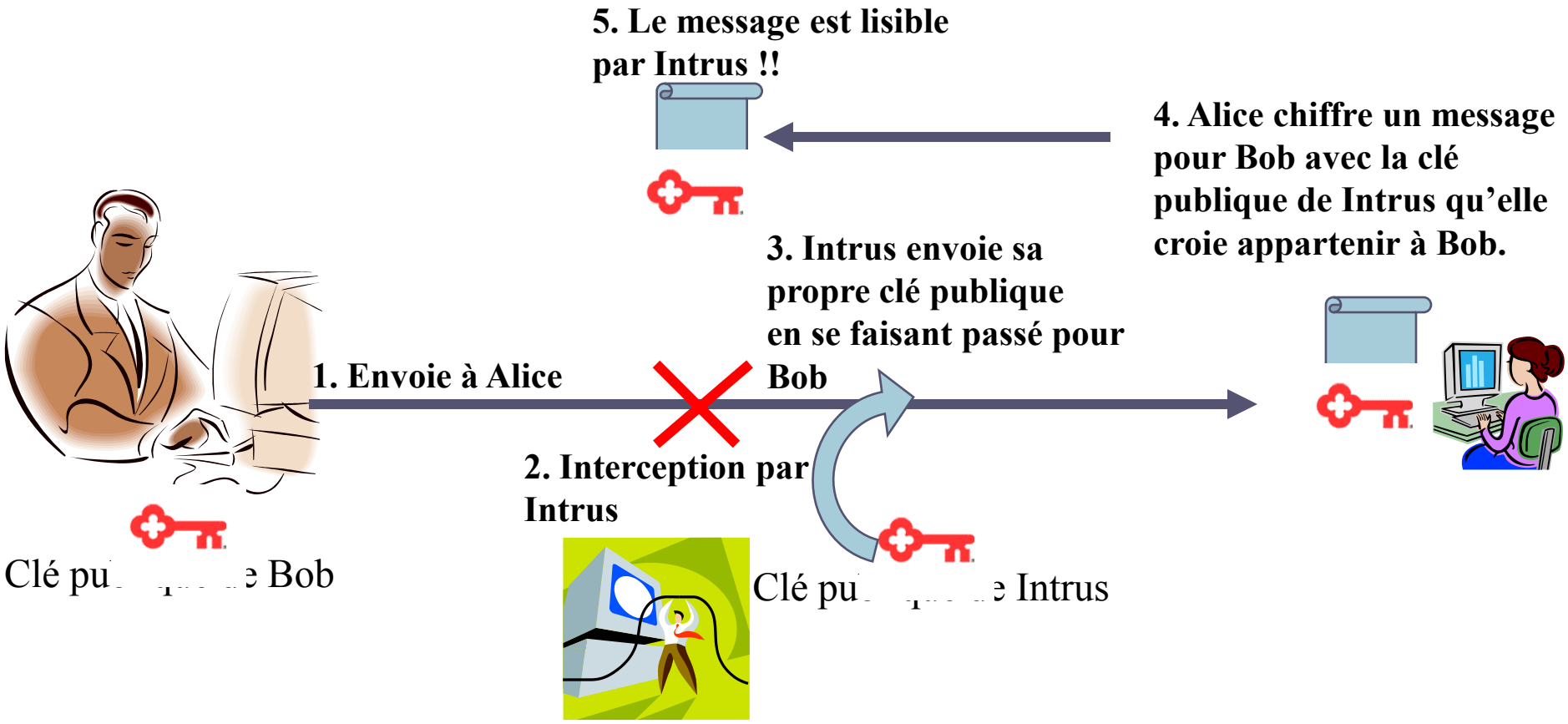
Réponse

Contexte: Cryptographie à clé publique
Limite de la cryptographie à clé publique

- **Comment garantir qu'une clé publique correspond bien à l'entité avec qui on communique ?**

- **Attaque : « man in the middle »**

Contexte: Cryptographie à clé publique
Limite de la cryptographie à clé publique



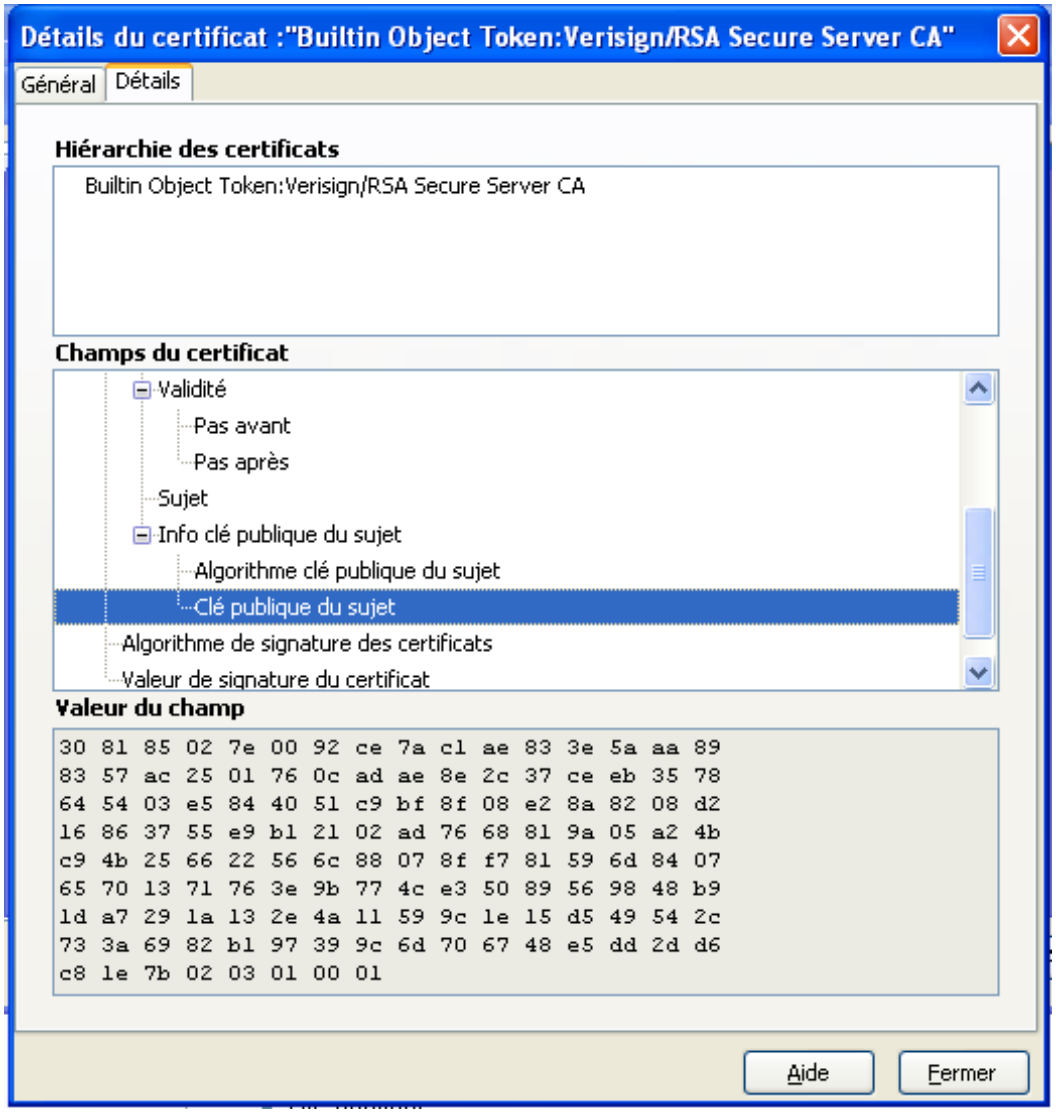
Contexte: Cryptographie à clé publique
Solution: usage de certificats à clé publique

- **Un certificat à clé publique est un certificat numérique qui lie l'identité d'un système à une clé publique, et éventuellement à d'autres informations;**
- **C'est une structure de donnée signée numériquement qui atteste sur l'identité du possesseur de la clé privée correspondante à une clé publique.**
- **Un certificat est signé numériquement par une autorité de certification à qui font confiance tous les usagers et dont la clé publique est connue par tous d'une manière sécurisée.**
- **Ainsi, afin de publier sa clé publique, son possesseur doit fournir un certificat de sa clé publique signé par l'autorité de certification.**
- **Après vérification de la signature apposée sur le certificat en utilisant la clé publique de l'autorité de certification, le récepteur peut déchiffrer et vérifier les signatures de son interlocuteur dont l'identité et la clé publique sont inclus dans le certificat.**

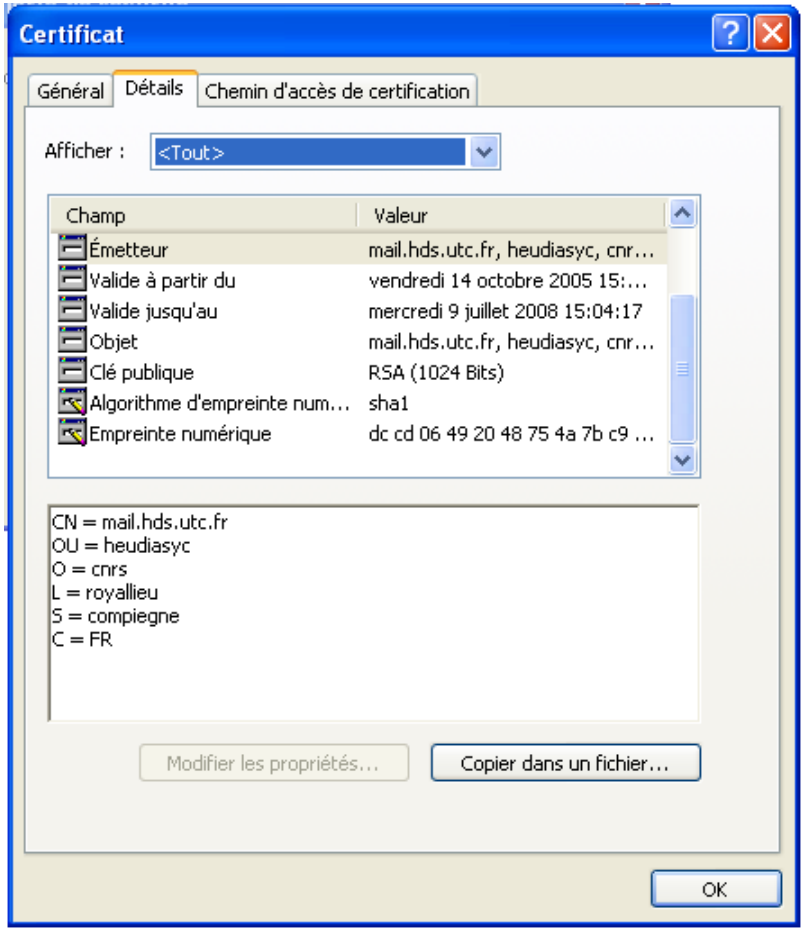
Structure d'un certificat X.509

- **Version**
- **Numéro de série**
- **Algorithme de signature du certificat**
- **Signataire du certificat**
- **Validité (dates limite)**
  - Pas avant
  - Pas après
- **Détenteur du certificat**
- **Informations sur la clé publique**
  - Algorithme de la clé publique
  - Clé publique
- **Identifiant unique du signataire (Facultatif)**
- **Identifiant unique du détenteur du certificat (Facultatif)**
- **Extensions (Facultatif)**
  - Liste des extensions...

Exemple Certificat

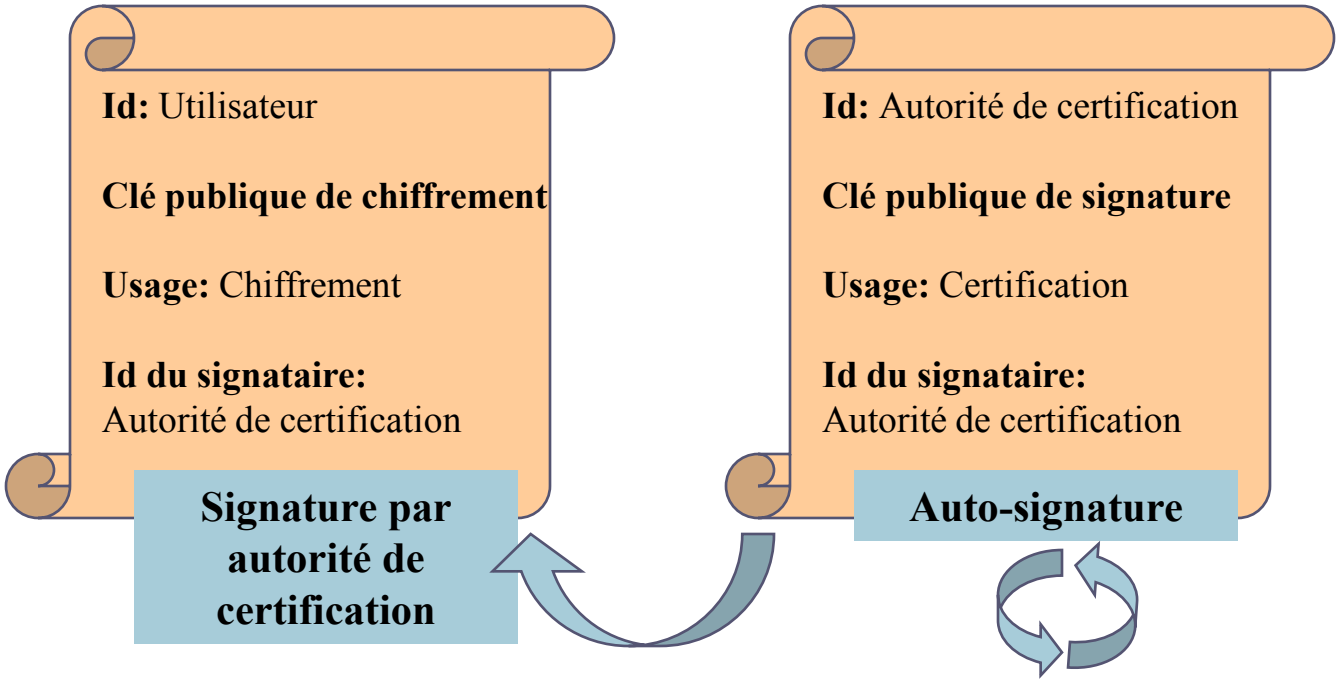


Certificats et confiance



Autorité de certification

- **Une autorité de certification est toute entité qui délivre des certificats de clé publique**



Rôle de l'autorité de certification

- **L'autorité de certification certifie la correspondance Clé publique – Identité pour l'ensemble d'une population**

- **Transitivité de la confiance**
  - A fait confiance à l'Autorité de Certification
  - L'Autorité de Certification délivre un certificat à B
  - A est assuré de l'identité de B

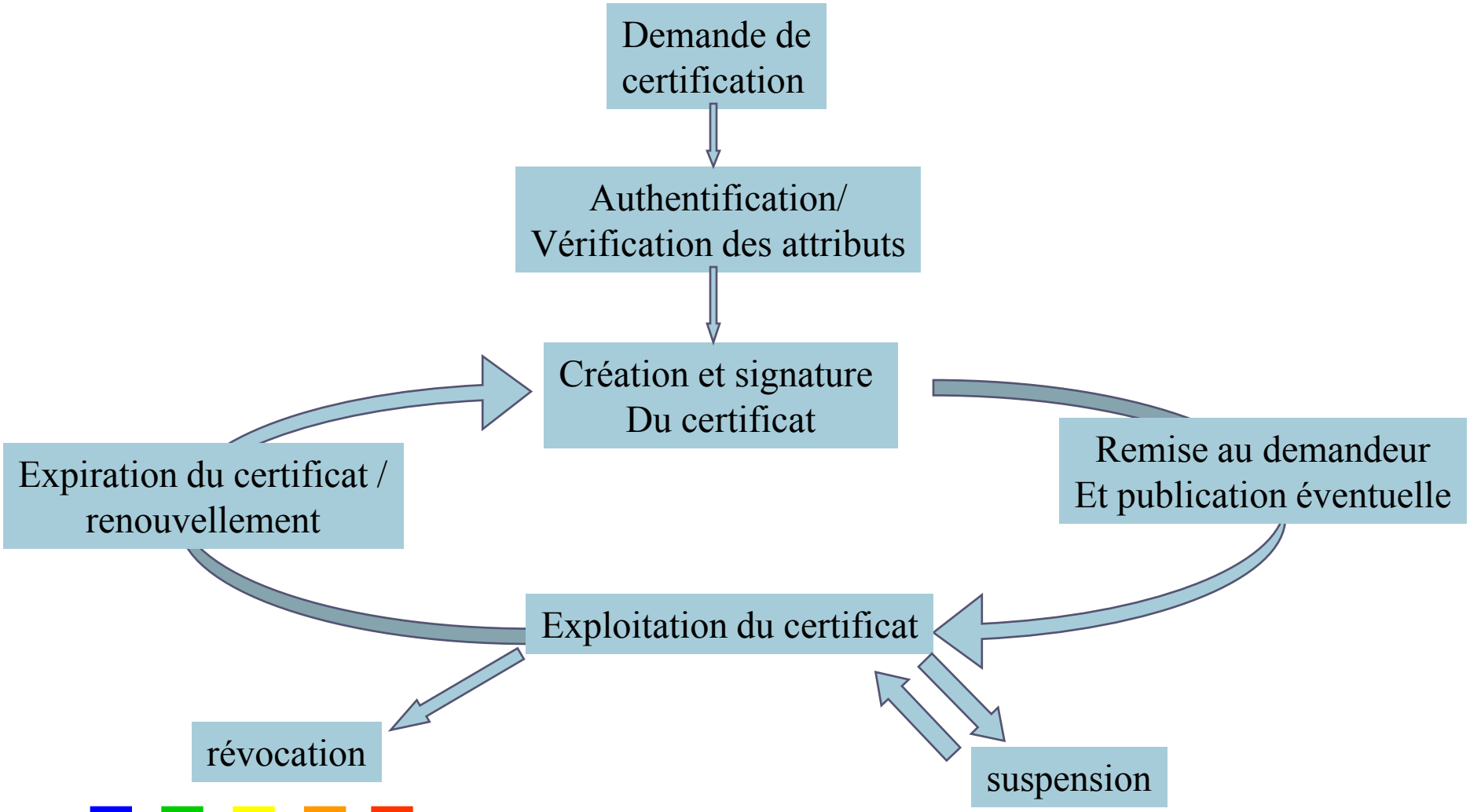
PKI: Infrastructure à clé publique

Définition d'une infrastructure à clé publique :

- **« Ensemble de composants, fonctions et procédures dédié à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique ».**

  [Politique de certification type: Ministère de l'Economie, des Finances et de l'Industrie, Fr]

PKI: Cycle de vie de certificats



Fonctions d'une PKI

- **Enregistrer et vérifier les demandes de certificats**
  - Autorité d'enregistrement
- **Créer et distribuer des certificats**
  - Autorité de certification
- **Vérification de validité de certificats**
  - Autorité de validation
- **Gérer à tout moment l'état des certificats et prendre en compte leur révocation**
  - Dépôt de listes de certificats révoqués – CRL (Certificate Revocation List)
- **Publier les certificats dans un dépôt**
  - Dépôt de certificats (Annuaire)

Modèles de confiance dans les PKI

- **Modèle monopoliste**
  - Une CA pour tout le monde
- **Modèle monopoliste avec Autorités d'enregistrement**
  - Une CA avec plusieurs Ras pour la vérification des identités, …
- **Délégation de pouvoir de certification**
  - Une CA délègue le pouvoir de certification à d'autres entités qui deviennent CA à leur tour, en leur fournissant un certificat qui certifie leur capacité d'être CA.
- **Modèle oligarchique**
  - Déploiement des produits (comme les navigateur web) avec plusieurs entités de confiance qui sont des CA. Le navigateur fera confiance à tout certificat signé par l'une de ces CA dans sa liste
- **Modèle anarchique**
  - Chaque utilisateur établit la liste des entités à qui il fait confiance

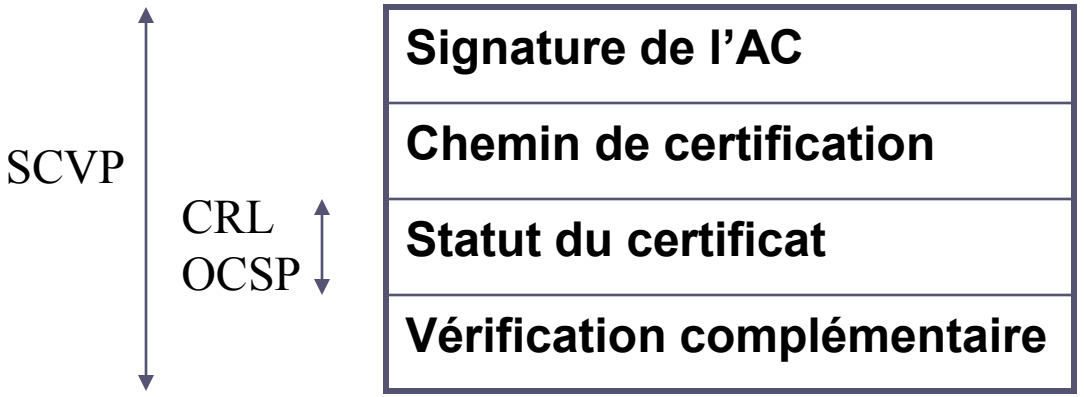
Validation de certificat (1)

- **Pour pouvoir se fier au contenu d'un certificat, il est nécessaire de réaliser les vérifications suivantes :**

Vérification	Commentaire
Signature de l'AC	L'application doit vérifier que le certificat est intègre et authentique
Chemin de certification	L'application doit vérifier qu'il existe une chaîne de certificats valide permettant de remonter à une AC de confiance
Période de validité	L'application doit vérifier que le certificat présenté n'est pas expiré
Statut du certificat	L'application doit vérifier que le certificat n'est pas révoqué (ni suspendu)

Validation de certificat (2)

- **Différents moyens et techniques standards pour offrir ce service**
  - Vérification du statut du certificat par récupération régulière de CRL
  - Vérification du statut du certificat en ligne : OCSP (On-line Certificate Status Protocol)
  - Vérification complète du certificat en ligne : SCVP (Simple Certificate Validation Protocol)



Révocation de certificats (1)

- **La révocation intervient quand la fin de validité réelle précède la fin de validité prévue**

- **Motifs de révocation**
  - Compromission réelle ou suspectée de la clé privée
  - Modification d'un au moins de attributs certifiés
  - Perte de la clé privée (effacement d'un disque dur, perte ou détérioration d'une carte à puce, oubli du code PIN, …)
  - Évolution de l'état de l'art cryptographique (la cryptanalyse de la clé privée entre dans le domaine du possible)
  - Perte de confiance vis-à-vis d'un acteur ou d'un composant de la PKI

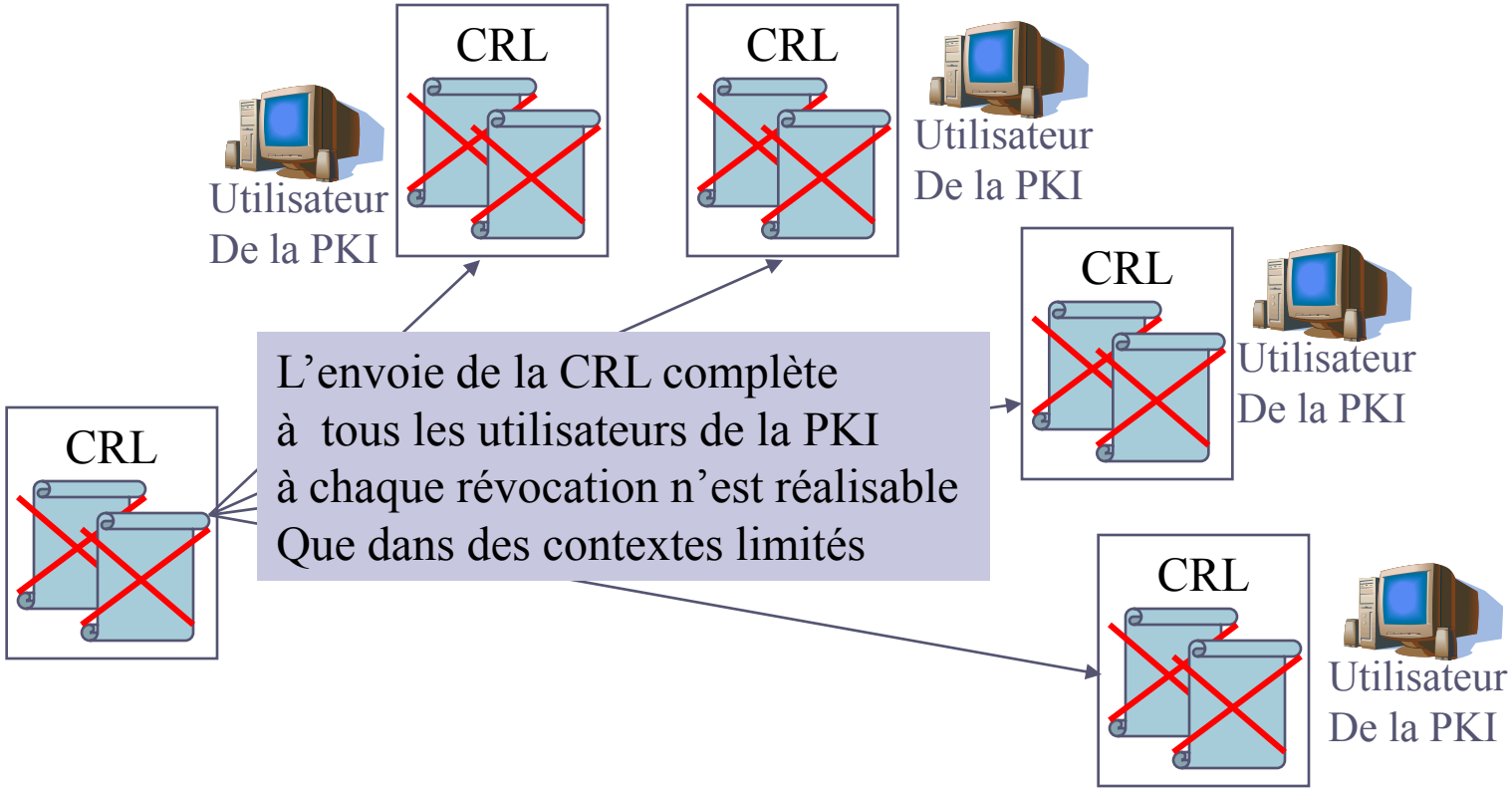
Révocation de certificats (2)

- **Le demandeur doit être habilité et authentifié**
  - Le propriétaire du certificat
  - Son supérieur hiérarchique
  - Le service de gestion du personnel
  - …

- **La méthode de révocation dépend de la méthode de validation**
  - Utilisation d'annuaire « positif »
    - ✓ La révocation consiste à enlever le certificat révoqué de l'annuaire
  - Utilisation d'un annuaire « négatif » ou CRL
    - ✓ inscription du certificat dans une liste de révocation de certificat

Gestion des CRL (1)

- **La gestion des CRL peut devenir complexe et lourde**



Gestion des CRL (2)

- **Les delta CRL ne contiennent que les changements depuis le dernière diffusion**

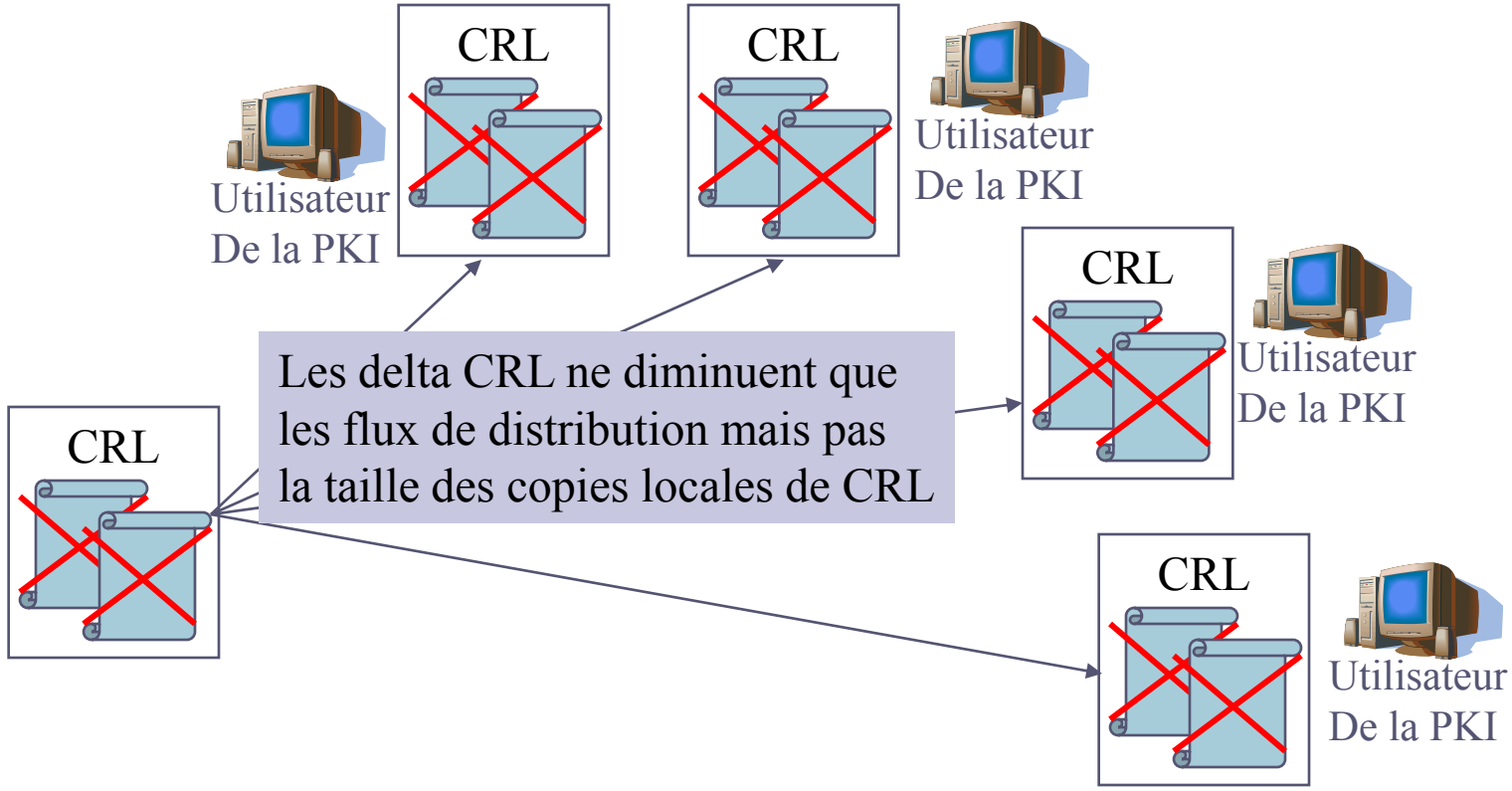
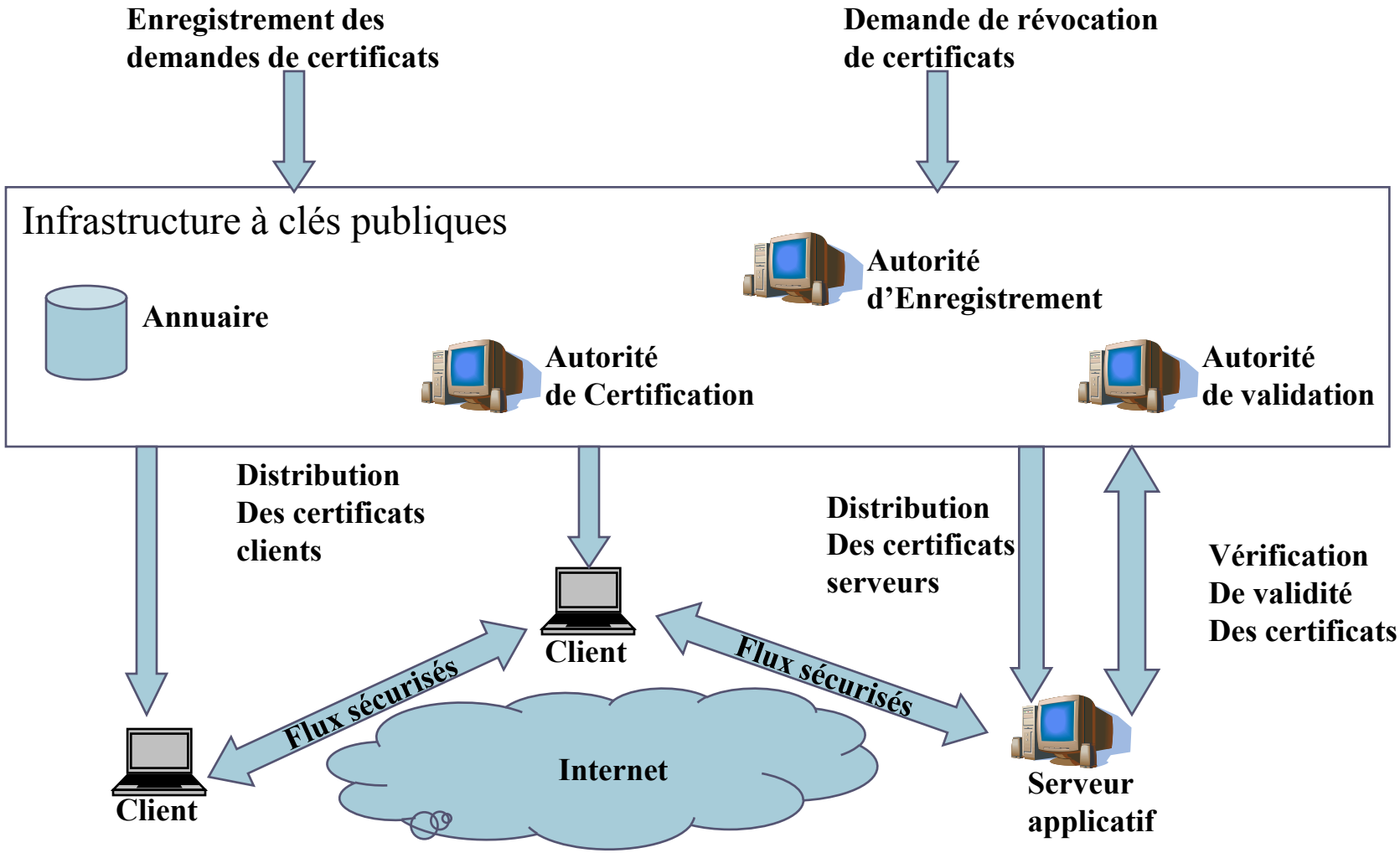


Schéma fonctionnel simplifié d'une PKI



Secure Socket Layer : SSL

Dr. Y. Challal

Secure Socket Layer : SSL

- **Un protocole de sécurisataion des échanges développé par Netscape**
- **Assurer les transactions Client / Serveur sur Internet**
- **Intégré dans les navigateurs web depuis 1994**
- **La vesrion 3.1 est baptisée Transport Layer Security TLS**
  - Standardisée à l'IETF: RFC 2246
- **Fonctionne au dessus de la couche TCP**

Services de sécurité assurés par SSL

- **Confidentialité**
  - Obtenue par chiffrement symétrique
- **Intégrité**
  - En utilisant des MAC : MD5(128 bits), SHA1(160 bits)
- **Authentification**
  - Identification des deux entités (client optionnel) basée sur les certificats X.509
  - Authentification de l'origine des données basée sur des MAC

Sous protocoles de SSL

- **SSL se déroule selon quatre sous protocoles**
  - Handshake
    - ✓ Authentification mutuelle
    - ✓ Négociation des algorithmes de chiffrement et de hachage
    - ✓ Échange des clés symétriques
  - Change Cipher Spec
    - ✓ Indiques la mise en place des algorithmes de chiffrement négocié
  - Record
    - ✓ Garantir la confidentialité à l'aide du chiffrement, et
    - ✓ L'authentification à l'aide de condensât
  - Alert
    - ✓ Émission de messages d'alertes suites aux erreurs que peuvent s'envoyer le client et le serveur

Déroulement de SSL

- **SSL se déroule en deux phases**
  - Phase 1: authentification du serveur
    - ✓ Requête client
    - ✓ Le serveur envoie son certificat et une liste d'algo de crypto à négocier
    - ✓ Le client vérifie le certificat du serveur à l'aide de la clé publique du CA contenu dans le navigateur
    - ✓ Le client génère un pré-master secret (PMS)(48 octets) qui sera utilisé pour générer le master-key (48 octets).
    - ✓ PMS est chiffré avec la clé publique du serveur
    - ✓ Les données échangées entre le client et le serveur seront chiffrées et authentifiées avec des clés dérivées du master-secret
  - Phase 2: authentification du client
    - ✓ Le serveur peut demander au client de s'authentifier en lui demandant son certificat
    - ✓ Le client répond en envoyant son certificat puis en signant un message avec sa clé privé (contient des info sur la session et le contenu des messages précédents)

Handshake SSL avec authentification mutuelle