ICP/PKI: Infrastructures à Clés Publiques

Aspects Techniques et organisationnels

Dr. Y. Challal
Maître de conférences
Université de Technologie de Compiègne
Heudiasyc UMR CNRS 6599
France

Plan

- **Rappels**
- **Infrastructure à clés publiques (PKI)**
- **Cycle de vie d'un certificat**
- **Schéma fonctionnel simplifié d'une PKI**
- **Démo: déploiement d'une PKI**

Confiance et Internet

Dans la vie courante la plupart des transactions reposent sur une « confiance » acquise par un contact physique

Dans le cybermonde cette relation de proximité est rompue

Comment garantir la sécurité des transactions?

- **Sécurité juridique**: valeur probante d'un acte effectué sur Internet
- **Sécurité des échanges** vis à vis des tentatives frauduleuses des tiers ou de l'une des parties

Menaces et services de sécurité (1)

- **Votre correspondant est-il ce qu'il prétend être?**
  - Usurpation d'identité
- **Vos échanges n'ont-ils pas été altérés?**
  - Altération de contenu
- **Vos échanges n'ont-ils pas été écoutés?**
  - Écoute
- **Votre correspondant ne va-t-il pas contester la valeur de l'acte établi à distance?**
  - Répudiation

Menaces et services de sécurité (2)

- **La cryptographie moderne apporte des réponses à ces menaces:**
  - Identification
  - Authentification de l'origine de données
  - Confidentialité
  - Intégrité
  - Non répudiation

- **Systèmes symétriques vs. asymétriques**
  - Symétriques: souples, petites clés, gestion de clés complexe
  - Asymétriques: lents, clés plus larges, gestion de clés plus simple, garantie du service de non-répudiation

- **En pratique: on utilise les deux (ex. SSL/TLS)**

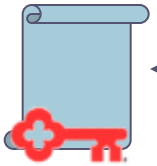
Atouts et Limites de la cryptographie à clé publique

- **Cryptographie à clés publiques**
  - Gestion de clés plus simple
  - Authentification forte
  - Non répudiation, signature numérique ➔ Sécurité juridique
  - …

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

Attaque « man in the middle »

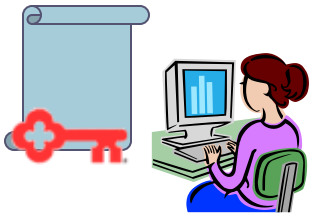
5. Le message est lisible par Intrus !!



4. Alice chiffre un message pour Bob avec la clé publique de Intrus qu'elle croie appartenir à Bob.

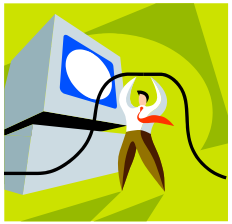
1. Envoie à Alice

3. Intrus envoie sa propre clé publique en se faisant passé pour Bob



Clé publique de Bob

2. Interception par Intrus



Clé publique de l'Intrus

Solution: usage de certificats à clé publique

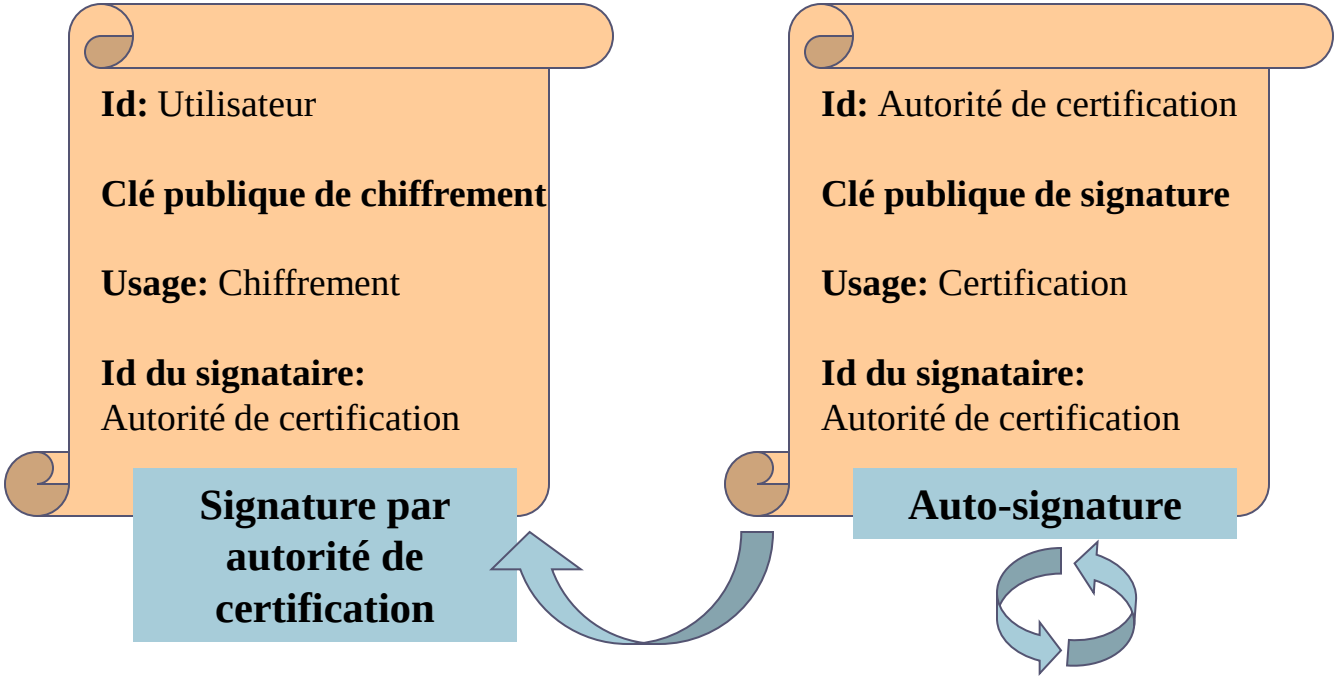
- **Un certificat à clé publique est un certificat numérique qui lie l'identité d'un système à une clé publique, et éventuellement à d'autres informations;**
- **C'est une structure de donnée signée numériquement qui atteste sur l'identité du possesseur de la clé privée correspondante à une clé publique.**
- **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
- **Id unique du signataire (Facultatif)**
- **Id unique du détenteur du certificat (Facultatif)**
- **Extensions (Facultatif)**
  - Liste des extensions...

Autorité de certification

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



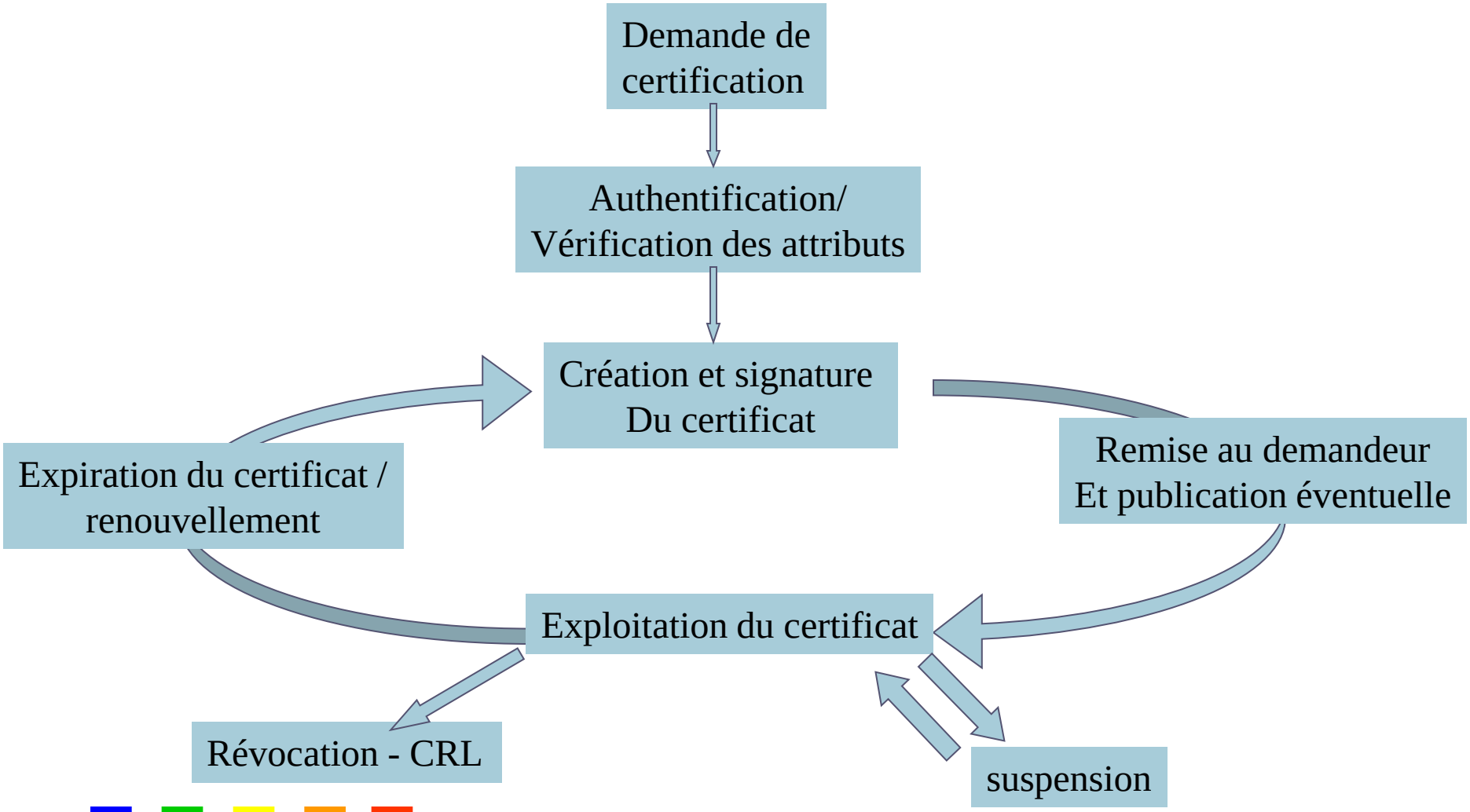
PKI: Infrastructure à clé publique

Définition d'une infrastructure à clé publique :

- **« Ensemble de composants, fonctions et procédures dédiés 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]

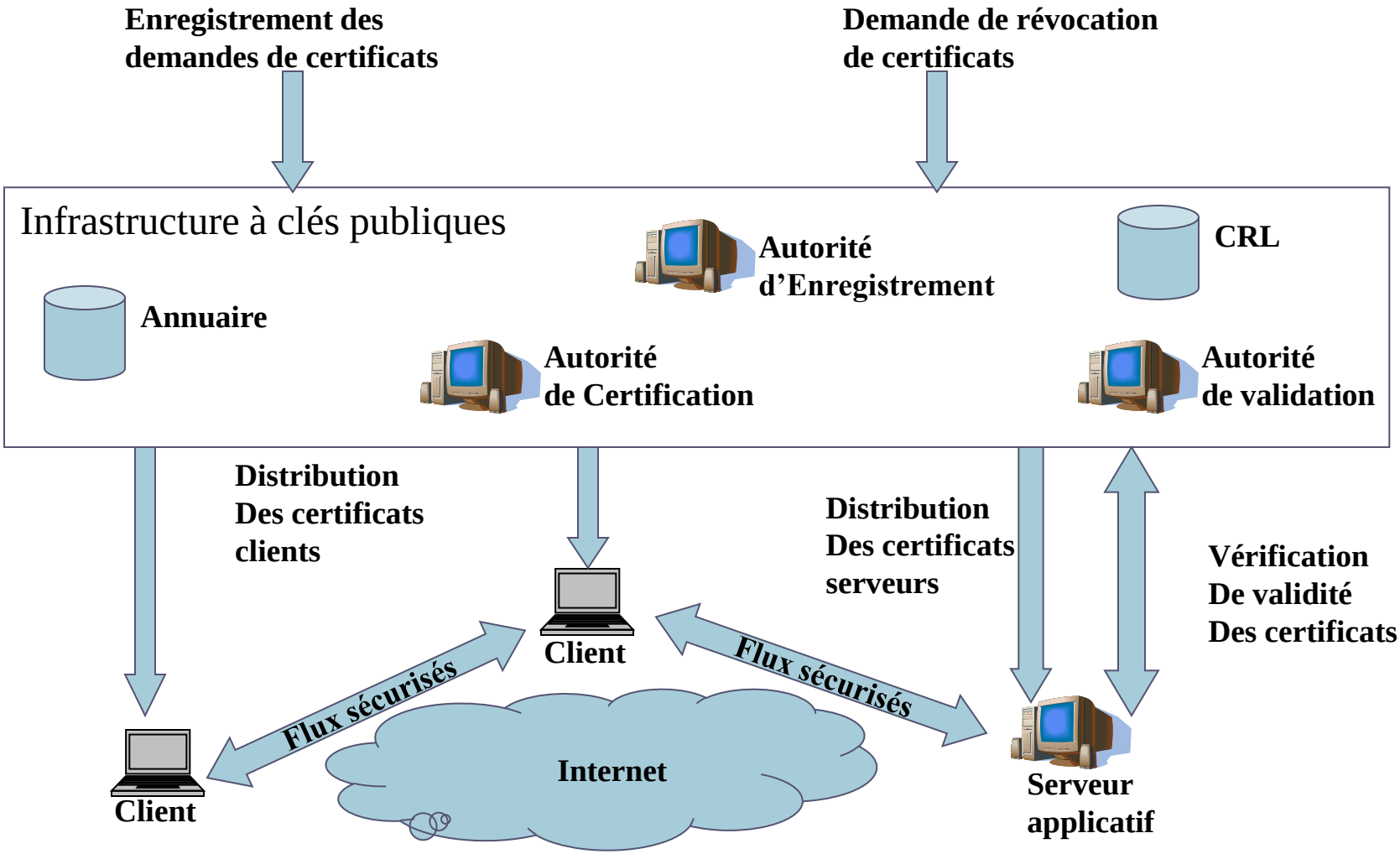
PKI: Cycle de vie de certificats



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)

Schéma fonctionnel simplifié d'une PKI

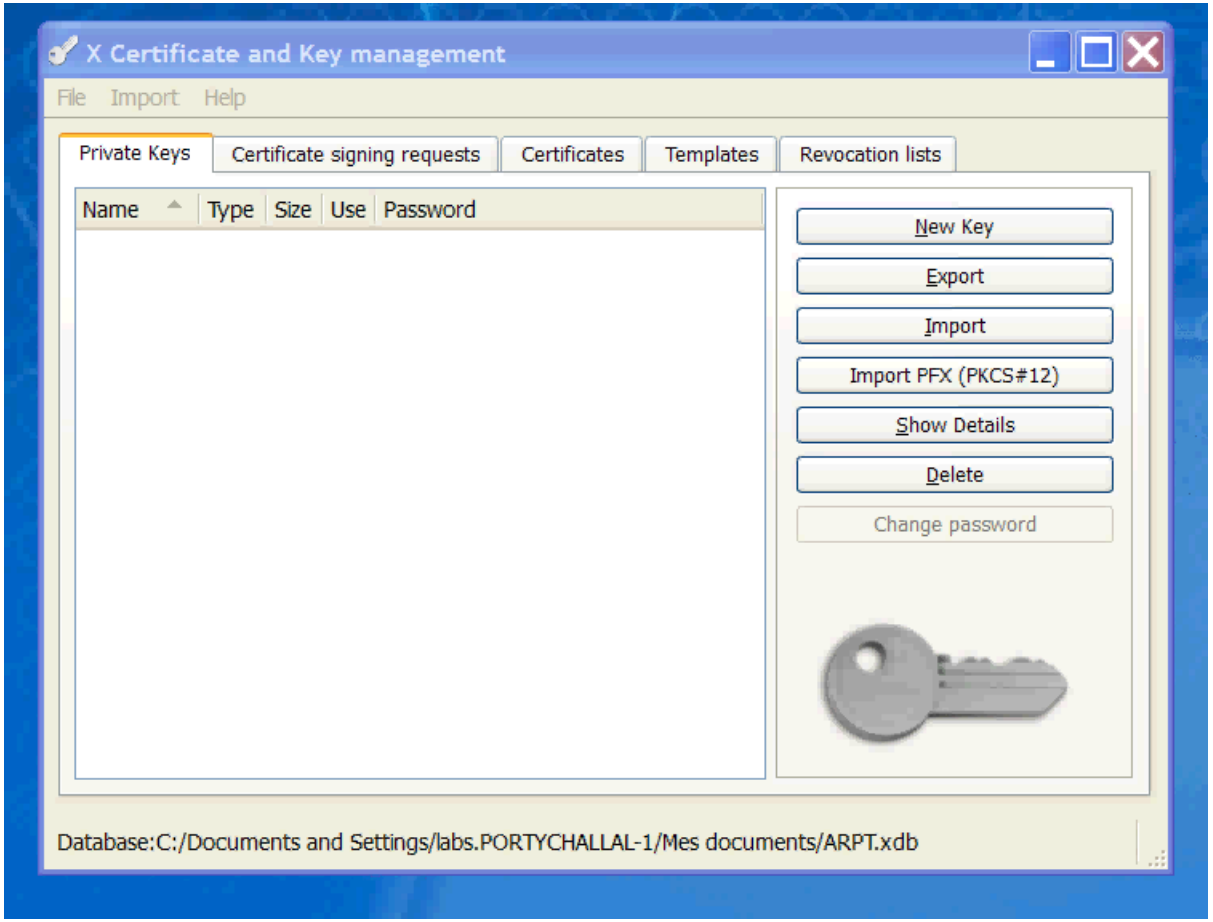


Modèles de confiance dans les PKI

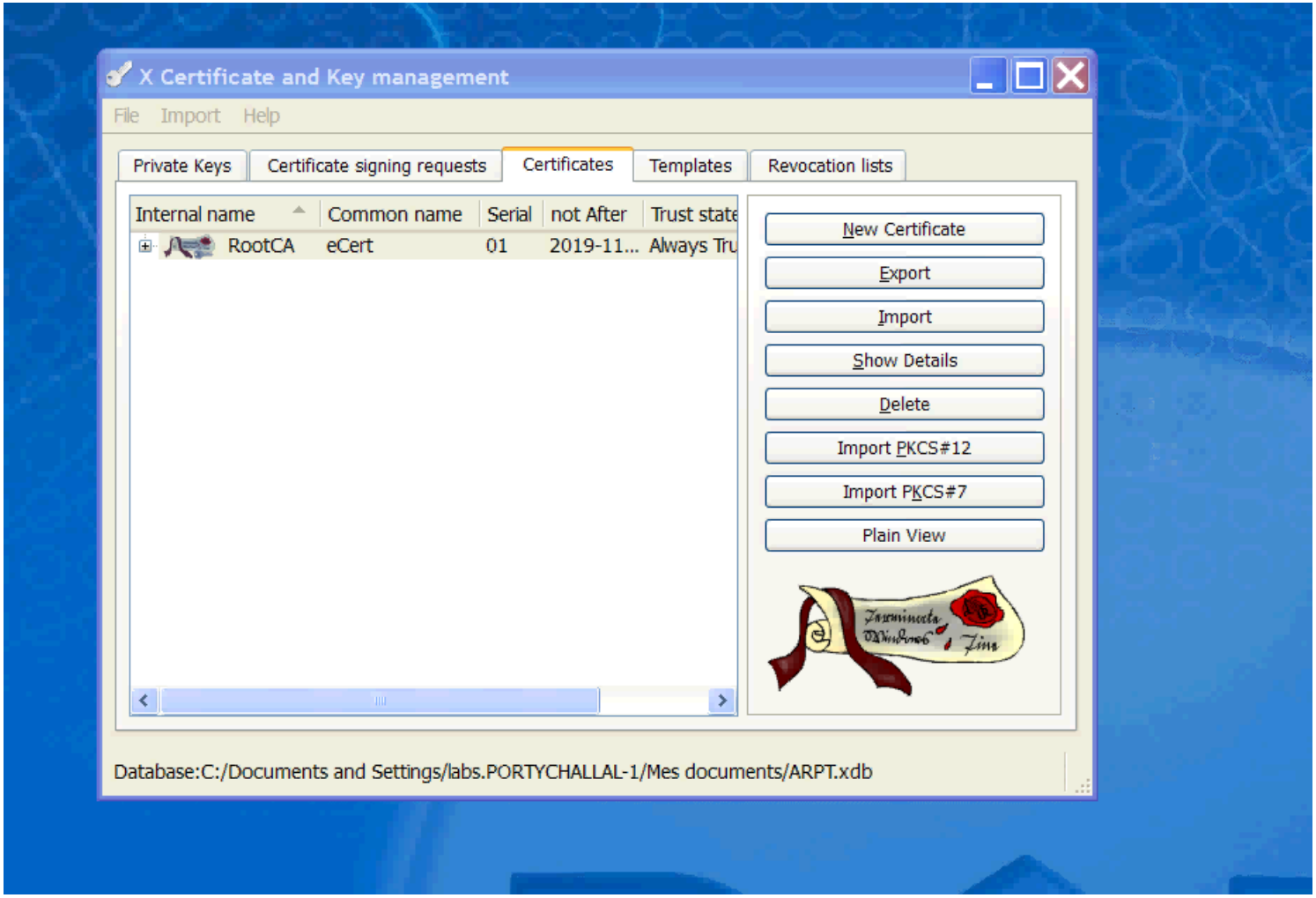
- **Modèle monopoliste**
  - Une CA pour tout le monde
- **Délégation de pouvoir de certification**
  - Une CA délègue le pouvoir de certification à d'autres entités qui deviennent CA à leur tour, en leur fournissant un certificat qui certifie leur capacité d'être CA.
- **Modèle oligarchique**
  - Déploiement 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

Démo: Création d'une PKI

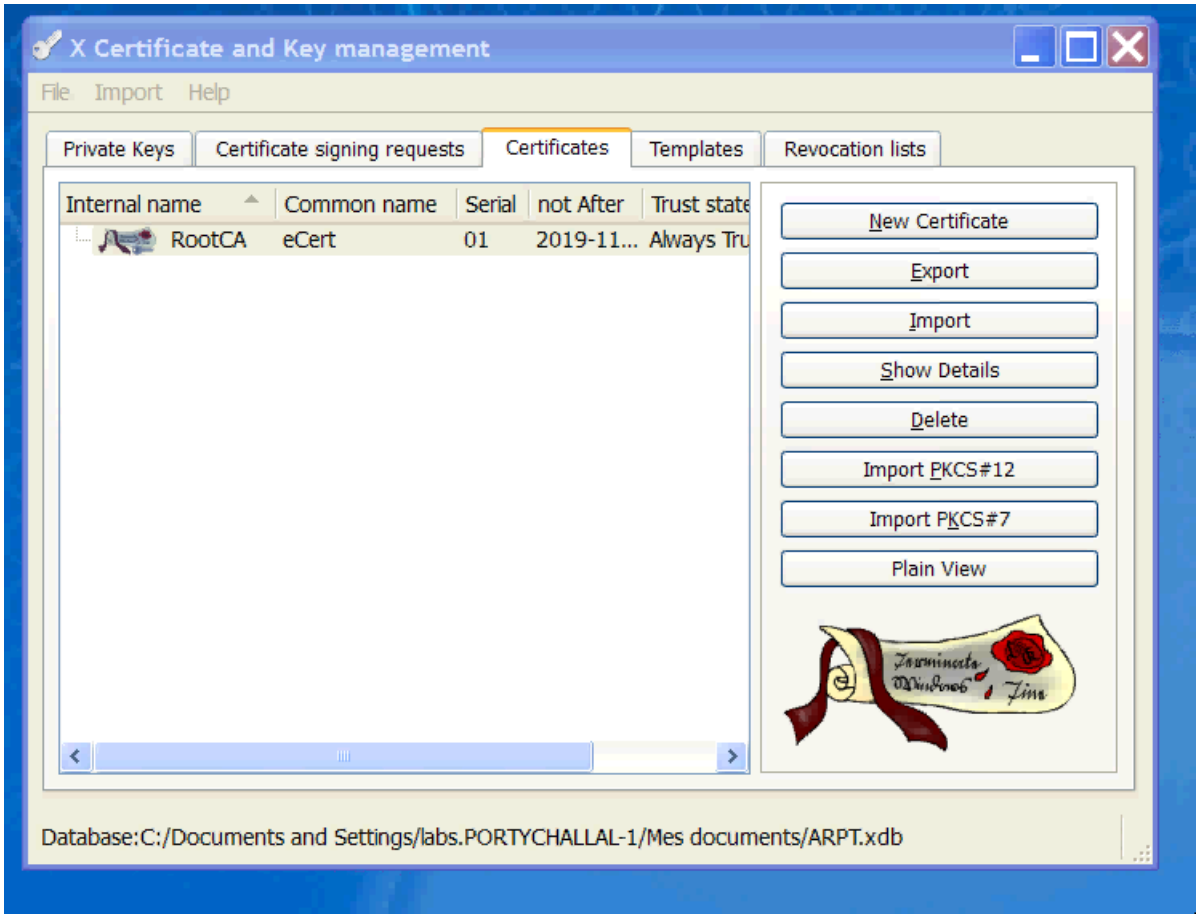
Création d'une Autorité de Certification Racine



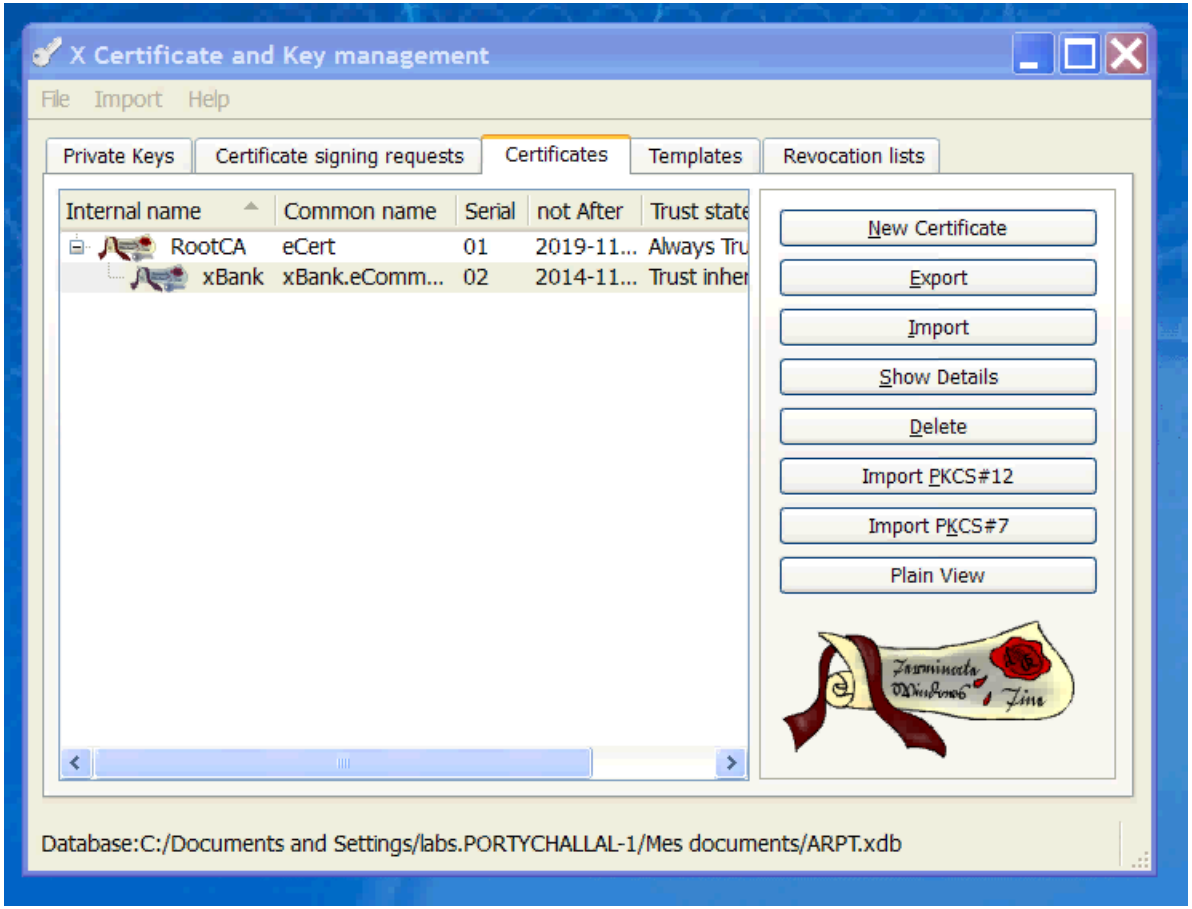
Intégration d'un certificat racine dans un navigateur web



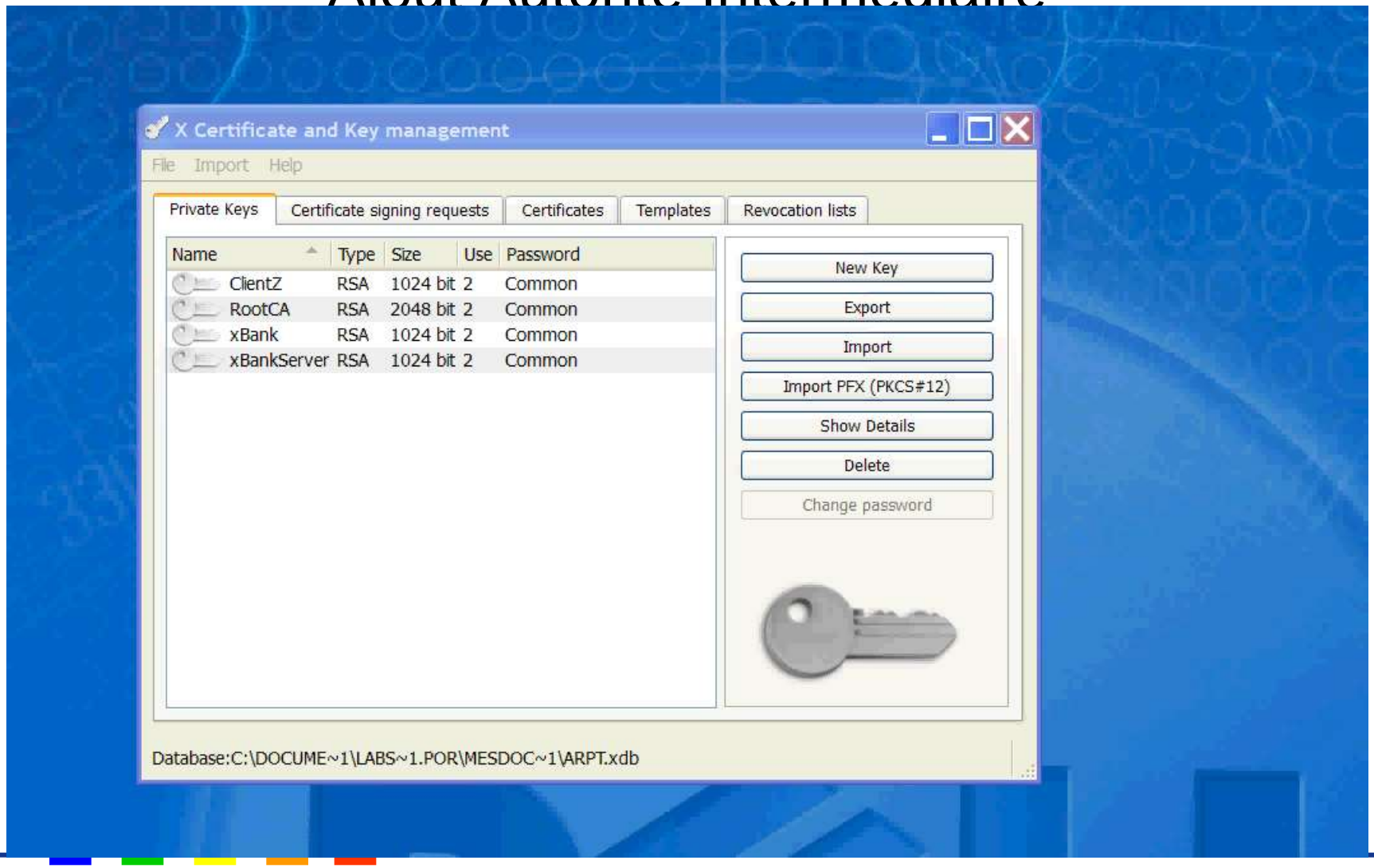
Création d'une Autorité de Certification Fille



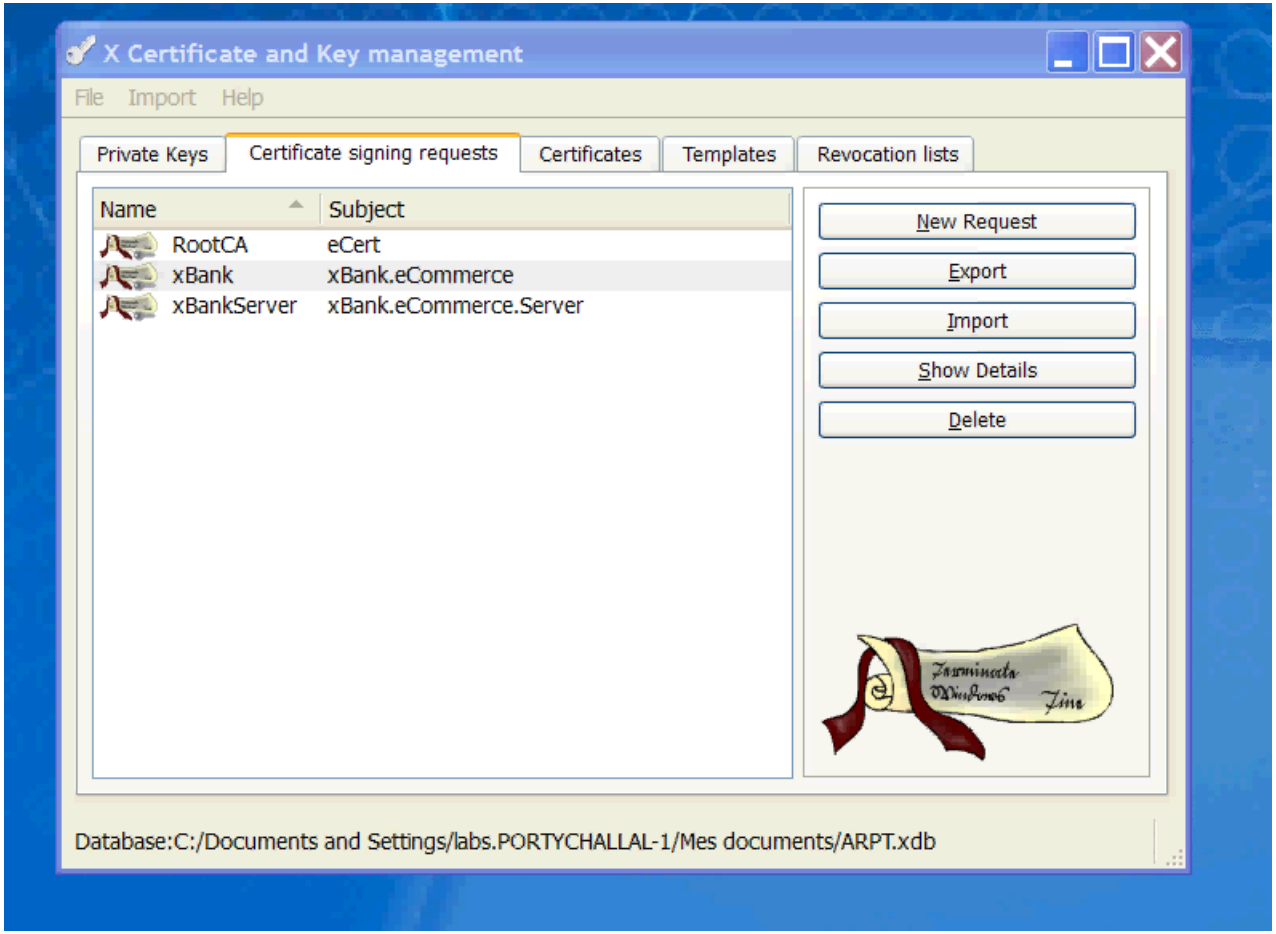
Création d'un Certificat pour un Serveur Web



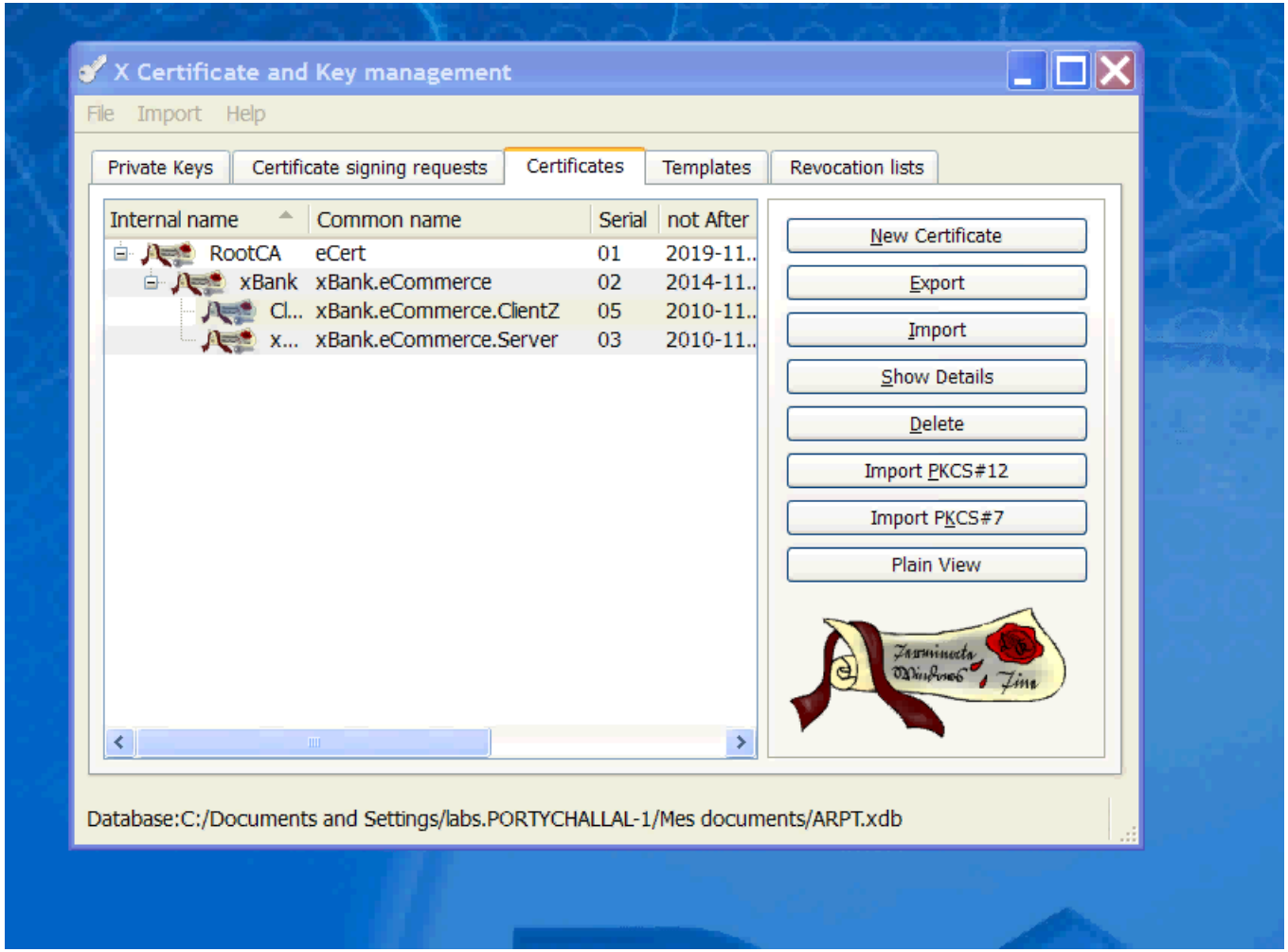
Ajout Autorité Intermédiaire



Création Certificat Client

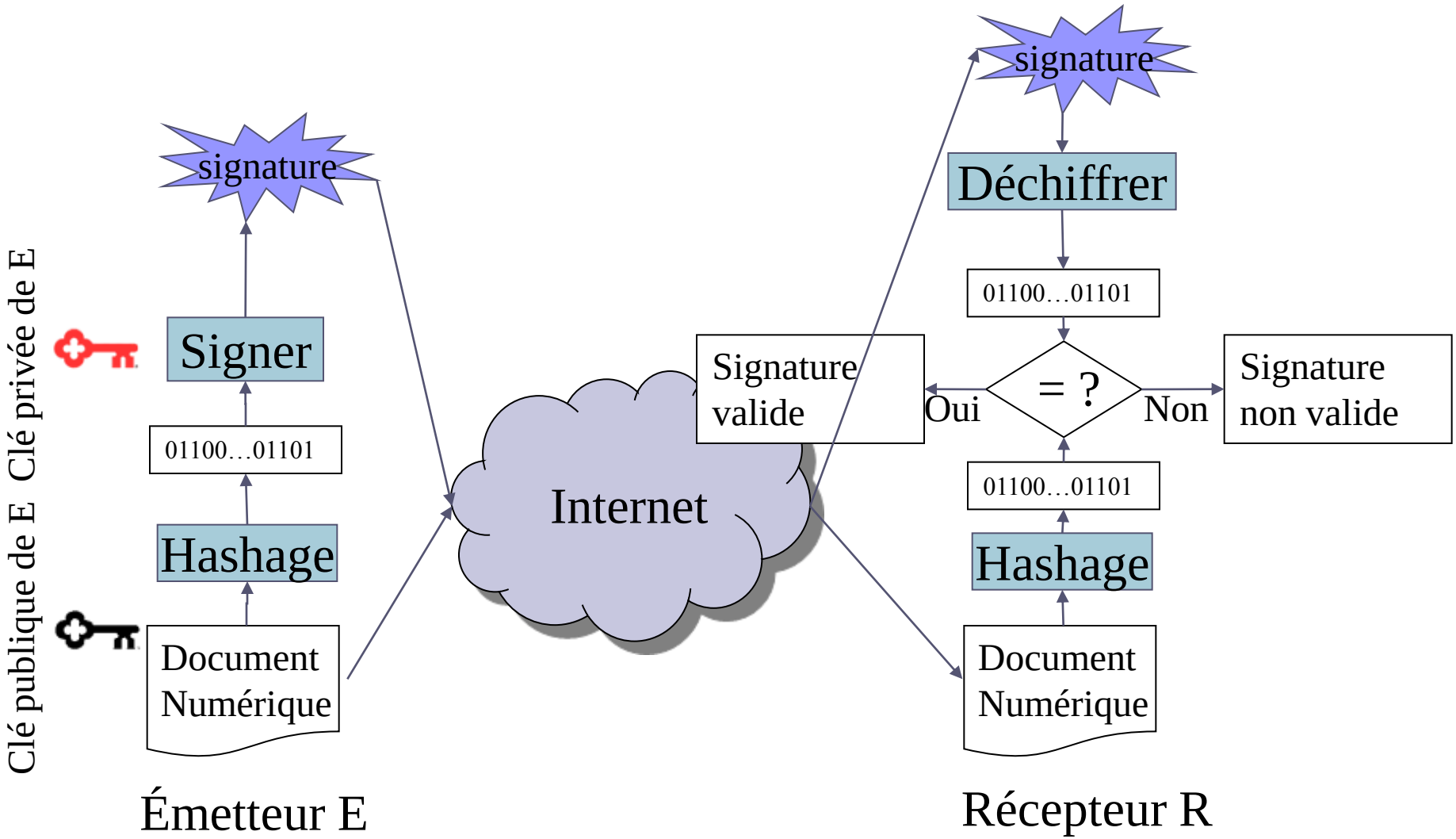


Révocation d'un Certificat



Merci

Signature digitale: Non répudiation



Cryptographie à clé publique: Authentification

Défi

Hashage

Condensat

Clé privée

Chiffrement

B

Réponse

Défi

Hashage

Condensat

= ?

Condensat

Clé publique

Déchiffrement

B

Réponse

Validation de certificat

- **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)

Révocation de certificats

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

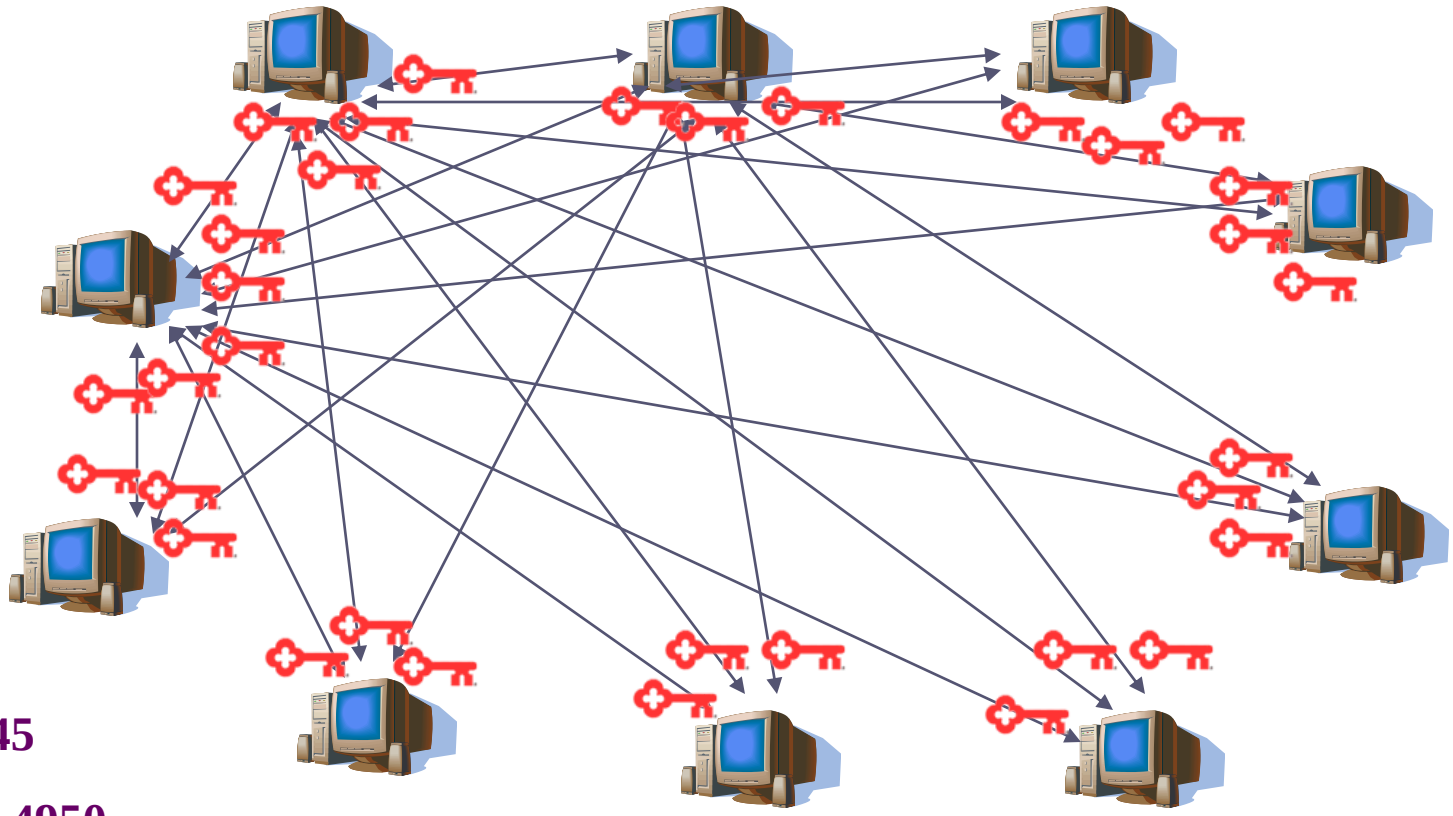
- **Motifs de révocation**
  - Compromission réelle ou suspectée de la clé privée
  - Modification d'un au moins des attributs certifiés
  - Perte de la clé privée (effacement d'un disque dur, perte ou détérioration d'une carte à puce, oubli du code PIN, …)
  - Évolution de l'état de l'art cryptographique (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
- **Méthode de révocation : CRL**

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
- **Id unique du signataire (Facultatif)**
- **Id unique du détenteur du certificat (Fa**
- **Extensions (Facultatif)**
  - Liste des extensions...

Signature de l'autorité

Limite du chiffrement symétrique: gestion de clés complexe



10 → 45

100 → 4950

5000 → 12.497.500

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 la correspondance entre l'identité de B et sa clé publique

Cryptographie à clé publique

- **Chaque utilisateur aura besoin d'une paire de clés: (clé privée, clé publique)**
- **Il suffit d'une paire de clés par utilisateur pour sécuriser les communications d'une communauté ➔ Gestion de clés plus simple**
- **Service de Non répudiation / Signature numérique ➔ sécurité juridique**