Université Batna 2

Infrastructure à clé publique (PKI)

Chapter 6

Préambule

Outre la mise en place de

- pare-feu et
- système de détection d’intrusion

Il est de nos jours **nécessaire de mettre en place un système d’authentification** afin de s'assurer de l'identité des interlocuteurs, de protéger les données et d'autoriser l'accès qu'aux personnes ayant le droit de les manipuler.

Préambule

Risques liés aux réseaux : malgré les bienfaits des réseaux informatiques, ceux-ci présentent **d'énormes risques**.

Parmi ceux-là on peut citer

- Interception de messages
  - Prise de connaissance des mots de passe
  - Vol d'information
  - Perte d'intégrité du système et du réseau
- Intrusion des systèmes
  - Vol ou compromission des informations
  - Destruction des informations
  - Virus
  - Détournement de biens
- Perte d'accessibilité au système ou au réseau
- Faux clients, marchands escrocs

Préambule

Objectifs de la cryptographie

Parmi les objectifs de la cryptographie

- Garantir la confidentialité
- Vérifier l'intégrité des données
- Gérer l'authentification
- Assurer la non-répudiation

Préambule

Rappel de quelques notions

Chiffrement / déchiffrement

- **Chiffrement** consiste à transformer un message clair en un message non compréhensible, on parle d'un message chiffré, afin de cacher la signification aux personnes n'ayant pas le droit à le lire ou à l'utiliser.
- **Déchiffrement** est l'opération inverse permettant de récupérer le message original à partir d'un message chiffré.

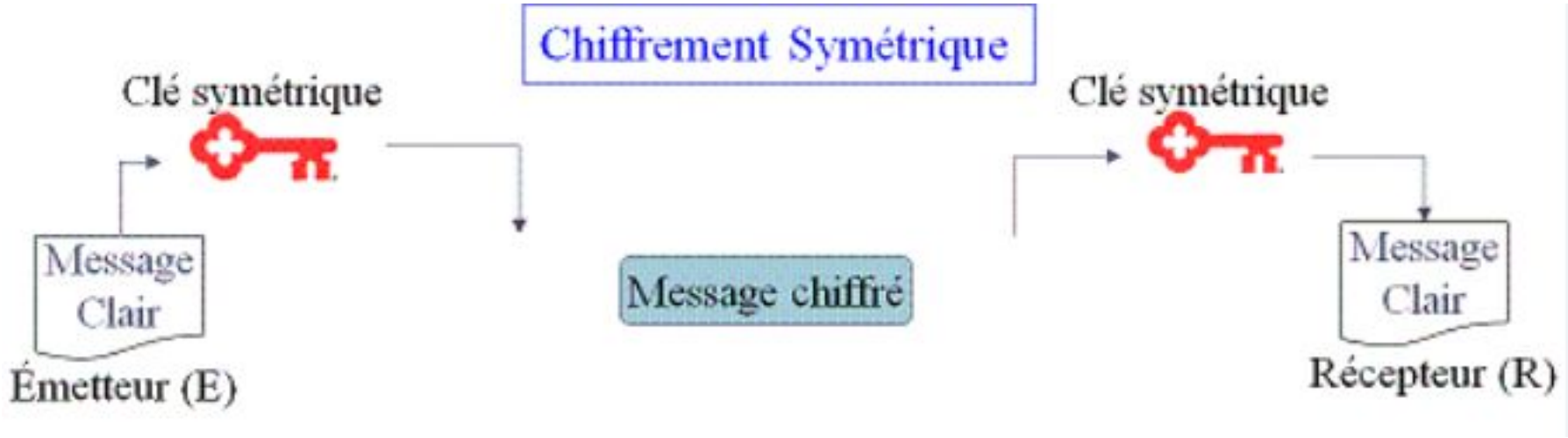
Clé de chiffrement

- Le message peut être chiffré ou déchiffré à l'aide d'une clé de chiffrement ou de déchiffrement, respectivement.
- La clé de **chiffrement peut être la même que la clé de déchiffrement ou pas**.
- Si c'est la même clé on parle de système **cryptographique symétrique** sinon on parle ou de système **cryptographique asymétrique**.

Préambule

Chiffrement symétrique

- Dans le chiffrement symétrique, **la même clé est partagée secrètement** entre l'expéditeur et le destinataire.
- L'expéditeur l'utilise pour chiffrer son message et le destinataire pour le déchiffrer en utilisant un algorithme de chiffrement symétrique.



Préambule

Chiffrement asymétrique

- Dans le chiffrement asymétrique, chaque nœud du réseau génère une paire de clés asymétriques : **une clé publique diffusée à tout le monde** et **une clé privée maintenue secrète** au niveau du nœud.
- Si une machine A veut envoyer un message à la machine B, A chiffre le message avec la clé publique de la machine B qui seule peut la déchiffrer avec sa clé privée.

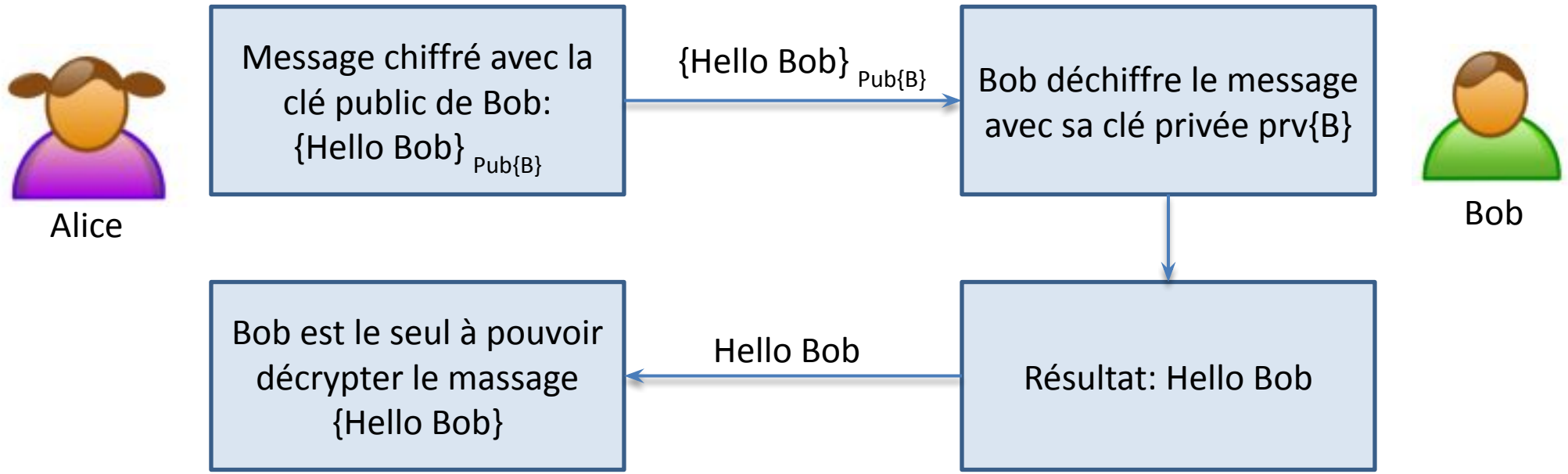
Tout message chiffré avec la clé publique ne peut être déchiffré qu'avec la clé privée correspondante et la clé privée ne peut pas être calculée à partir de la clé publique correspondante.

Préambule

Utilité d'un système asymétrique dans l'authentification

L'usage d'un système **asymétrique** est également utile pour l'identification.

Dans le scénario dans la figure ci-dessous Alice veut s'assurer de l'identité de Bob. Elle ne connaît de Bob que sa clé publique. Pour s'assurer de l'identité de Bob, Alice lui envoie un défi (un message "Hello Bob") chiffré par la clé publique de Bob. Ensuite, pour prouver son identité à Alice, Bob déchiffre le message avec sa clé privée et renvoie le message en clair à Alice. A la réception du message en clair, Alice le compare avec son défi et s'assure de l'identité ou pas de Bob, car seul Bob pourra déchiffrer le message.



Préambule

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

Préambule

Jusque là, nous avions toujours supposé que la clé publique est distribuée d'une manière sécurisée. Si cette hypothèse n'est pas vérifiée, un schéma asymétrique peut subir une attaque de type Man in the Middle.

Une telle attaque est illustrée dans le scénario ci-après.

Préambule

Jusque là, nous avions toujours supposé que la clé publique est distribuée d'une manière sécurisée. Si cette hypothèse n'est pas vérifiée, un schéma asymétrique peut subir une attaque de type Man in the Middle.

Une telle attaque est illustrée dans le scénario ci-après.

La solution au problème dit Man in the Middle est l'usage d'un **certificat numérique** qui assure la **liaison entre l'identité et la clé publique** correspondante dans un document numérique signé par une tierce partie de confiance dite **autorité de certification**.

PKI : Infrastructure à clés publiques

L'infrastructure à clé public peut être défini par **un ensemble de composants** (ordinateurs, équipements cryptographiques, systèmes, applications, procédures, fonctions, etc.) basés sur la cryptographie **à clé publique** afin de **gérer les clés** et de **délivrer les certificats numériques** utilisés par les services de sécurité.

- **Un certificat numérique** (appelé également certificat à clé publique) est utilisé pour **authentifier une entité** et de **chiffrer les échanges**. Ce certificat est signé par un **tiers de confiance**.
- **La gestion des clés** consiste à la génération, la maintenance, la révocation et la distribution des clés cryptographique.
- Elle doit aussi assurer le stockage sécurisé des clés de déchiffrement et mettre en place un mécanise permettant l'association identité/clé.

PKI : Infrastructure à clés publiques

Services fournis par l'infrastructure à clé public (PKI)?

La PKI permet de

- vérifier l'identité des différents entités communicantes
- créer les certificats
- faire des tests d'appartenance de certificats
- gérer la révocation des clés et le recouvrement des clés de déchiffrement
- Renouveler et publier les certificats

PKI : Infrastructure à clés publiques

Les différents acteurs pour une PKI

- **Autorité de certification (CA)**: signe les demandes de certificat (Certificate Signing Request => CRS) et les révocations de ces derniers (Certificate Revocation List => CRL). C'est l'autorité décisionnelle et de confiance dans le processus de certification faisant d'elle **l'entité le plus critique**.

- **Autorité d'enregistrement (RA):** Cette entité vérifie l'identité du demandeur de certificat et s'assure qu'il ne s'agit pas d'une usurpation d'identité. Elle **constitue l'interface entre l'utilisateur et la CA**.

- **Autorité de dépôt (Repository):** stocke l'ensemble des certificats valides et révoqués. l'ensemble des certificats des clés publiques émis par la CA est **mis à disposition des utilisateurs** par l'autorité de dépôt.

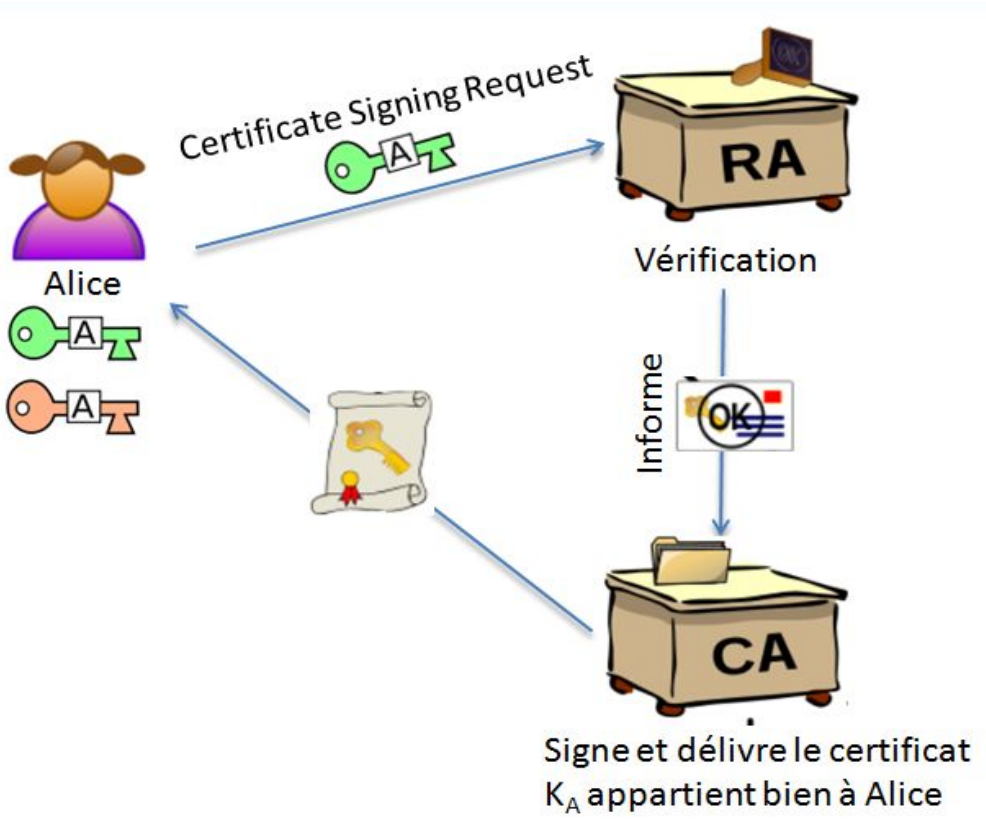
- **Autorité de recouvrement ou autorité de séquestre**: cette entité s'occupe de protéger des clés privées et assure une récupération de clé(s) ultérieure(s). La **perte d'une clé privée par son propriétaire** ne doit pas être définitive.

PKI : Infrastructure à clés publiques

Exemple:

Actions à entreprendre par Alice pour joindre la PKI :

- Alice commence par générer sa paire de clé privée/clé publique. Envoie par la suite sa clé publique à la RA via le CRS (Certificate Signing Request).
- La RA vérifie qu'Alice est bien celle qui prétend l'être et informe la CA qui va délivrer le certificat stipulant "K_A appartient bien à Alice".
- Le Repository récupère et stocke ce certificat, et le met à disposition pour tout le monde.
- Si **Bob** veut vérifier l'authenticité d'Alice, il peut récupérer (depuis le Repository) le certificat d'Alice.
- Si Bob fait confiance à la CA, il peut accepter comme valide le certificat, et authentifier diverses conversations avec Alice. Cela implique bien sûr la possession de la clé publique de la CA, pour bien vérifier la signature digitale sur le certificat.



Exemples de CAs

1. **DigiCert** : Connu pour ses certificats SSL/TLS et ses solutions de sécurité.
2. **GlobalSign** : Fournit des certificats numériques pour la sécurité des sites Web et l'authentification.
3. **Let's Encrypt** : Une autorité de certification gratuite qui fournit des certificats SSL/TLS pour sécuriser les sites Web.
4. **Comodo** (maintenant Sectigo) : Propose une gamme de certificats SSL/TLS et de services de sécurité.
5. **Entrust Datacard** : Fournit des certificats numériques pour la sécurité des transactions en ligne.
6. **GoDaddy** : Connu pour l'enregistrement de domaines, il propose également des certificats SSL.
7. **VeriSign** : Une des premières autorités de certification, maintenant une partie de DigiCert.

PKI : Infrastructure à clés publiques

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 **CAs** 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 CAs. Le navigateur fera confiance à tout certificat signé par l'une de ces CAs dans sa liste.
- Modèle anarchique: **Chaque utilisateur** établit la liste des entités à qui il fait confiance.

Certificats Numériques

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.

Pourquoi une infrastructure à clé public (PKI):
Ci dessous quelques cas d'usage d'un certificat PKI:

- Assure une **communication réseau sécurisé** grâce au chiffrement de données et ainsi elle assure la confidentialité.
- Permet de **signer un code ou un document**, ainsi elle assure l'authenticité.
- Permet de **signer un mail**, ainsi elle assure l'authenticité.
- Permet **une authentification personnelle**, ainsi elle assure l'authenticité et la non répudiation.
- Permet de **signer et de certifier les IoT**, ainsi, elle assure l'authenticité.
- etc.

Certificats Numériques

Types de certificats numériques ou électroniques:
Nous distinguons deux types de certificats électroniques, les certificats de signature et les certificats de chiffrement.

Les certificats de signature sont utilisés, comme leurs nom l'indique, pour **signer les documents** ou pour **s'authentifier sur un site web**. Dans ce type de certificat, il est nécessaire de s'assurer que la clé privée n'est possédé que par une seule entité.

Les certificats de chiffrement, sont utilisés pour chiffrer **les données envoyées sur le réseau**. Exemple: Si Alice veut envoyer un mail à Bob, elle va chiffrer le contenu du mail avec la clé publique de Bob (c'est à dire, la partie publique du certificat de Bob) et s'assure ainsi que seul Bob pourra déchiffrer le mail. Dans ce type de certificat, **il peut y'avoir nécessité de recouvrer les informations chiffrées** en cas de perte de la clé privée par le destinataire.

Certificats Numériques

Mode de création des certificats électroniques:
La création de certification peut se faire de deux façons: la création en mode centralisé et la création en mode décentralisé.

Dans la **création en mode décentralisé**, les deux clé publique et privée sont **crées par l'utilisateur**. Ensuite, uniquement la clé publique et mise dans la demande de création de signature (CSR : Certificate Signing Request). En revanche, la clé privée reste secrète et archivée dans le poste de travail de l'utilisateur.

Ce mode de création est **le plus utilisé** car il est plus simple de refaire un certificat en décentralisé qu'à recouvrer une clé.

Outre, il est **préconisé pour les certificats de signature** ou d'authentification. Le **recouvrement** de la clé privée est **impossible** avec ce mode de création.

Certificats Numériques

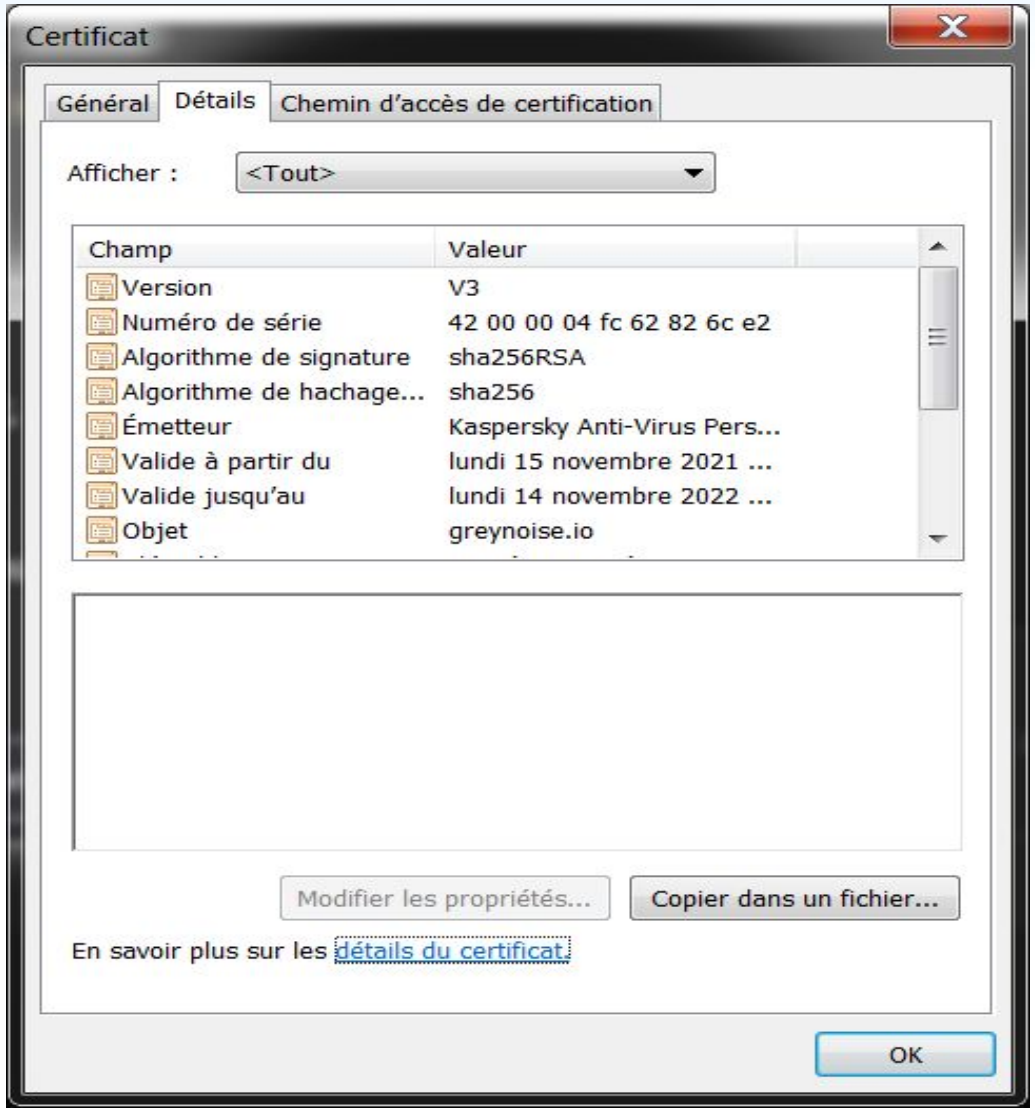
Mode de création des certificats électroniques:
La création de certification peut se faire de deux façons: la création en mode centralisé et la création en mode décentralisé.

Dans la **création en mode centralisé**, les deux clé publique et privée sont crées par l'autorité de certification (CA). Cela signifie que, quand l'utilisateur envoie sa demande de création de signature (CSR : Certificate Signing Request), cette dernière ne contient aucune clé. Une fois le CA produit les deux clés, il envoie à l'utilisateur le certificat avec uniquement la clé publique, ensuite la clé privée à part (dans un fichier sous le format PKCS#12). L'acheminement de la clé privée vers l'utilisateur final (le demandeur de certificat) doit être sécurisé.

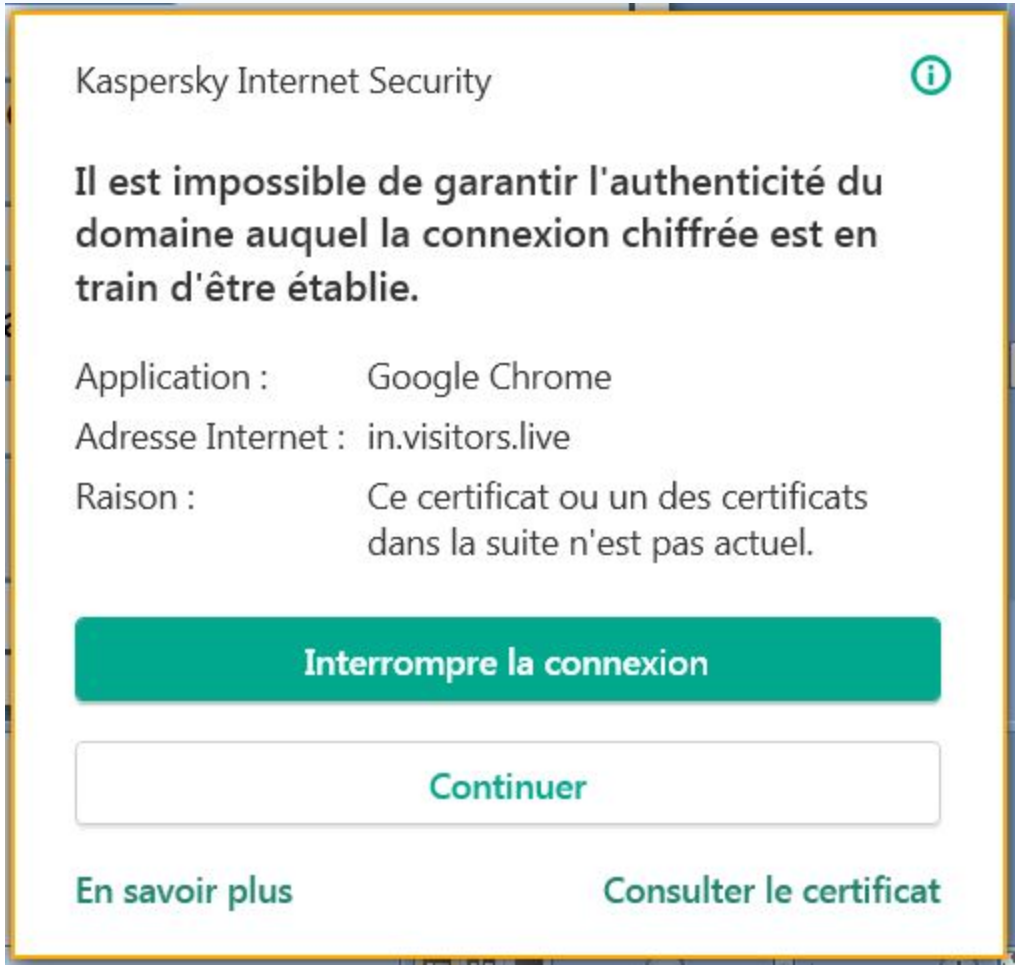
Ce mode de création est préconisé pour les certificats de chiffrement. Le fait que le CA détient une copie de la clé privée rend **le recouvrement de la clé privée possible** lorsque l'utilisateur perd sa clé privée.

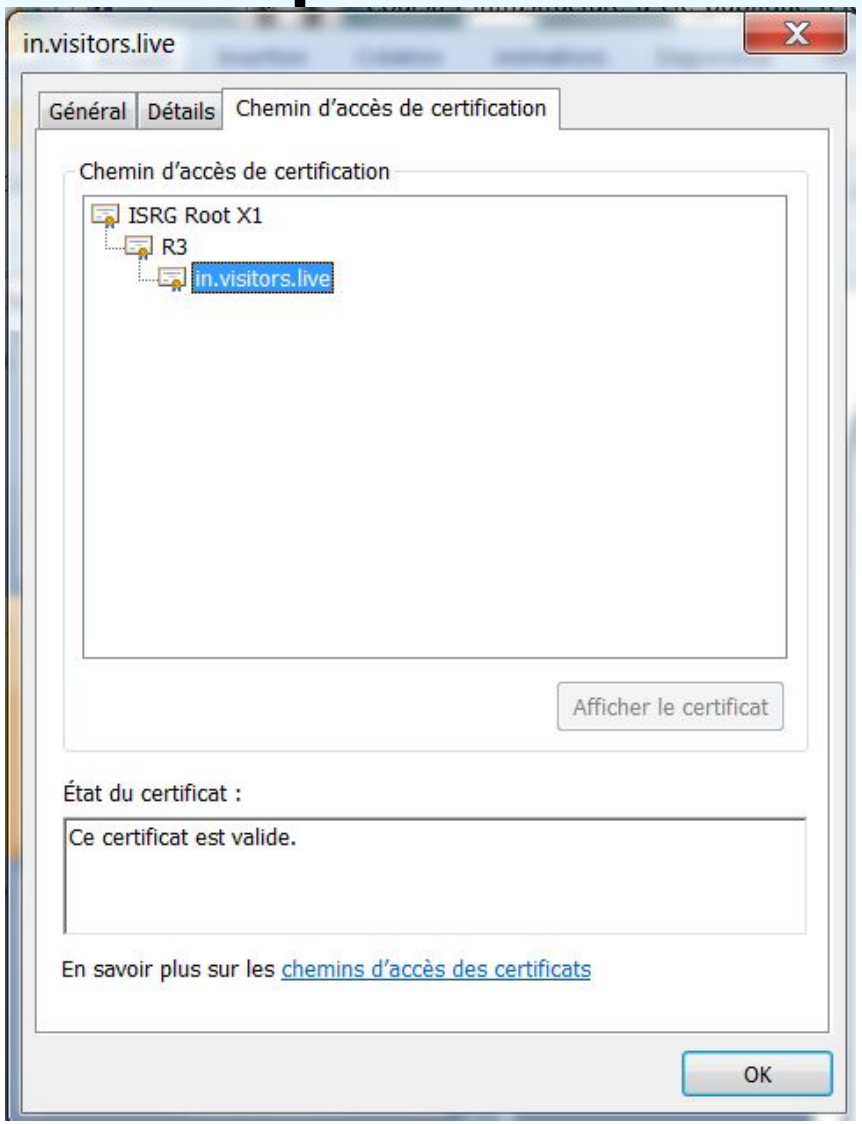
Certificats Numériques

Structure d'un certificat X.509:

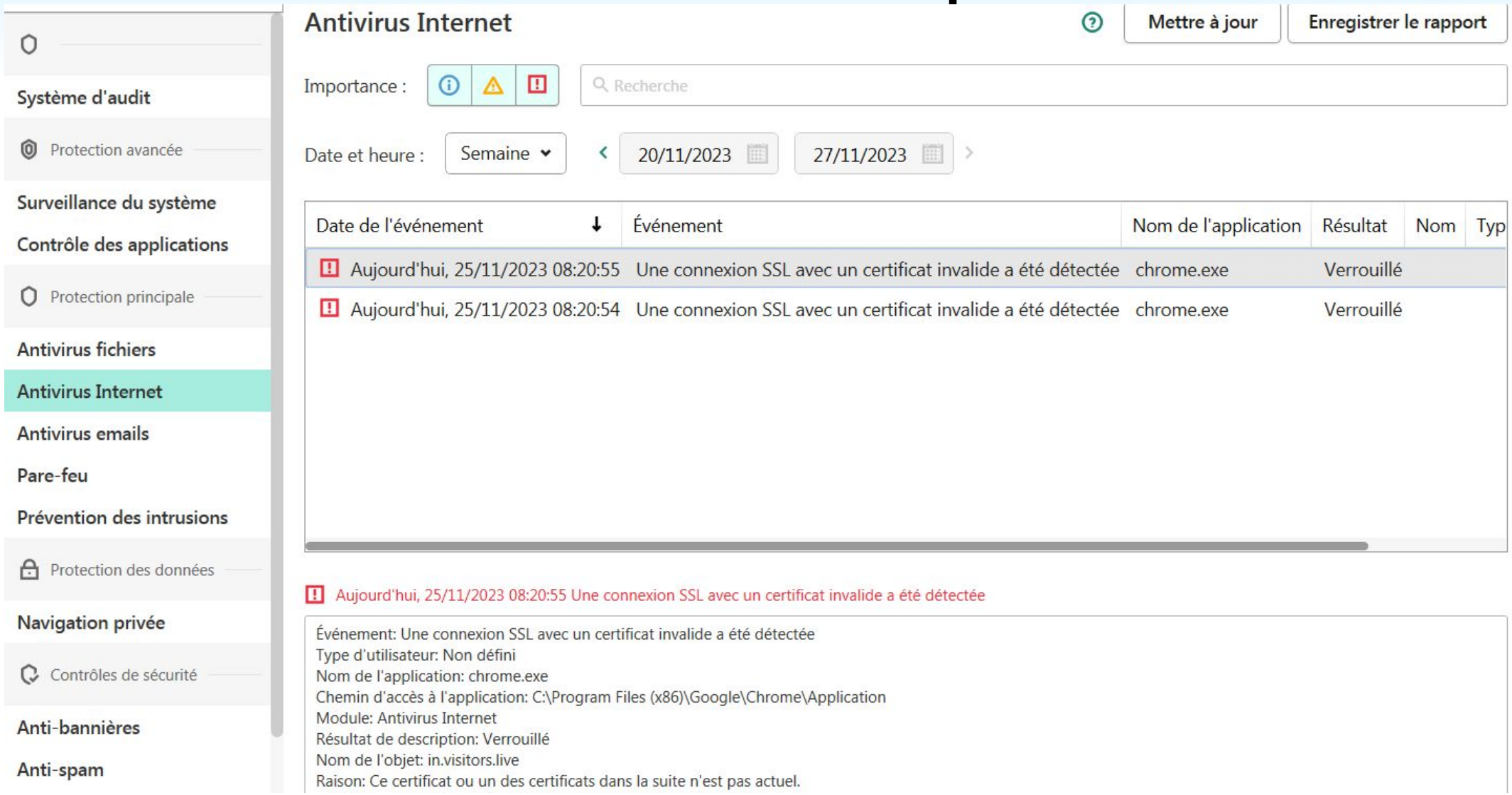


Certificats Numériques



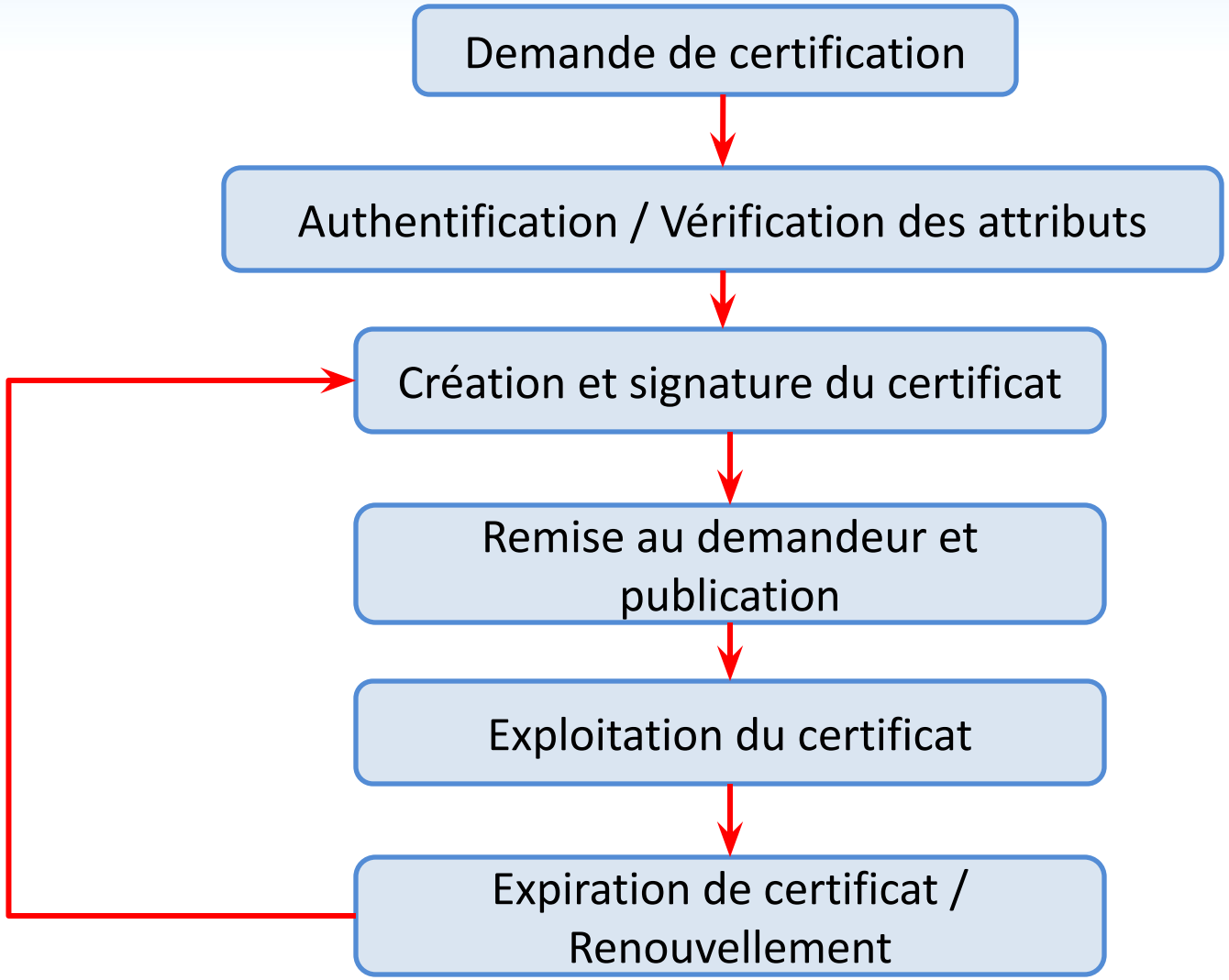


Certificats Numériques



PKI : Infrastructure à clés publiques

Cycle de vie d'un certificat numérique



Certificats Numériques

Révocation et expiration de certificats:

Il faut faire la différence entre l'**expiration** d'un certificat et la **révocation** d'un certificat. l'expiration d'un certificat numérique signifie que sa date de validité est atteinte et qu'il faut renouveler le certificat. Tandis que la révocation d'un certification signifie que le certificat numérique n'est plus valide alors que la date de validation n'est pas encore atteinte.

Certificats Numériques

Révocation et expiration de certificats:

Les causes de la révocation sont nombreuses, nous citons:

- **Compromission** réelle ou suspectée de la **clé privée**.
- **Modification d'un au moins un attribut** certifiés.
- **Perte de la clé** privée (effacement d'un disque dur, perte ou détérioration d'une carte à puce, oubli du code PIN, etc.).
- **Perte de confiance vis-à-vis d'un acteur** ou d'un composant de la PKI (e.g., symantec).
- **La perte ou la compromission** de la clé privée **de l'autorité de certification** ayant signé le certificat en question.
- etc.

Une fois un certificat révoqué ou invalide suite à son expiration, ce dernier est ajouté dans une liste appelée CRL (**Certificate Revocation List**) afin d'informer les applications qu'elles ne doivent plus faire confiance à ce certificat.

Certificats Numériques

Certificats Numériques dans une PKI:

Comme vu précédemment, chaque certificat possède **deux clés**, une clé privée et une clé publique. La clé **privée** doit rester **secrète**. Tandis que la clé **publique** est **publiquement** partagée sur le certificat numérique.

L'autorité de certification **est un tiers de confiance** permettant de signer l'ensemble des informations et certifier l'exactitude des informations portées par le certificat (identification, appartenance, etc.).

Le CA doit aussi s'assurer **que le certificat est utilisé par un seul besoin** (exemple: un site web doit posséder un seul certificat et ce certificat ne peut pas être utilisé par un autre site web).

Les entreprises utilisent les PKI afin de non seulement assurer de façon électronique leur identité mais aussi l'identité des autres entités avec lesquelles elles communiquent.
-> VPN or Kerberos vs PKI