Sécurité Applicative

3A - SSI

Pr. El Bakkali Hanane

Sommaire du cours

I. Introduction

1. Pourquoi sécuriser?
2. Où et quoi sécuriser?
3. Comment sécuriser?
4. Politique de sécurité :

I.1. Pourquoi sécuriser ?

- Les SI sont de plus en plus considérés comme les centres névralgiques des organismes;
- Parfois, le SI est au cœur de l'activité de l'organisme;
- Les SI sont de plus en plus connectés à Internet;
- Il existe différentes motivations pour attaquer un SI, dont :
  - Bénéfices financiers (vol de n° de carte de crédit, espionnage industriel, nuisance à l'image de marque profitant aux concurrents, ..);
  - Satisfaction personnelle (plaisir/jeu, fierté maladive, concurrence entre Hackers, etc);
  - Vengeance (salarié licencié et/ou sous estimé, ...)
  - Convictions politiques et/ou idéologiques (partisans d'un parti, terroristes, ...);
  - Espionnage d'état.

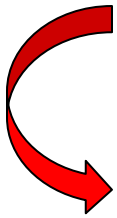
I.1. Pourquoi sécuriser ?

- Suivre les tendances: la sécurité est à la mode !
  - Le marché de la sécurité est en pleine croissance;
  - **Sécurité Web : un marché de 1 milliard de dollars en 2009 (**Radicati Group)
- Les statistiques montrent que les attaques (déclarées ou découvertes) ont tendance à la fois à croître et à devenir plus efficaces et qu'elles touchent même les grandes sociétés des TIC;
- Toutes les attaques exploitent des faiblesses de sécurité au niveau du SI (notamment au niveau des **applications** et réseaux sous-jacents);
- Les pertes dues à une attaque peuvent être très graves (rien qu'en termes de temps perdu, elles peuvent être considérables)
- Enfin, la cybercriminalité n'est pas encore bien cernée par les instances judiciaires, ce qui rend le recours à la justice peu fructueux.

I.2. Où et quoi sécuriser ?

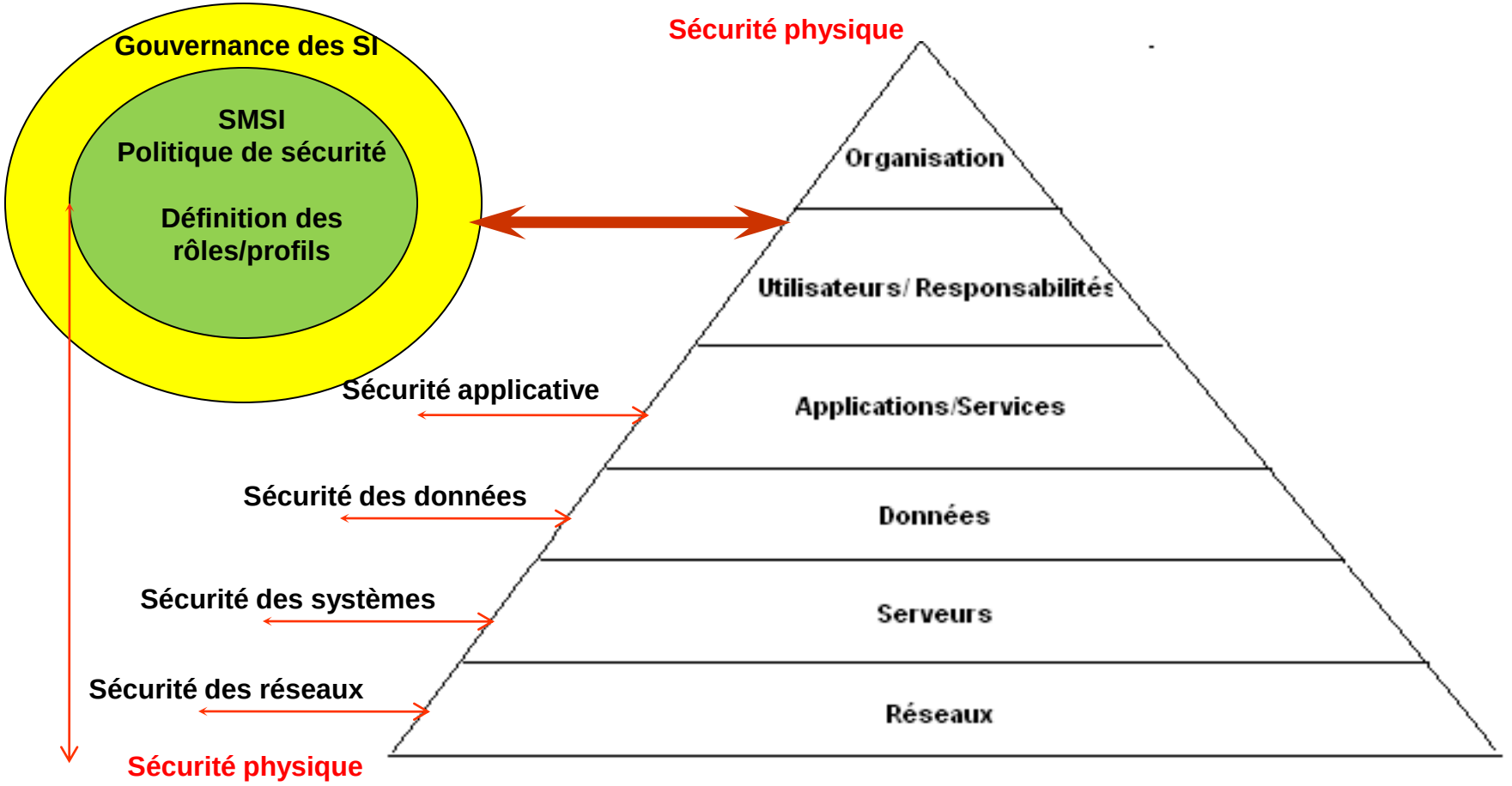
☞Les Besoins en termes de sécurité se situent à plusieurs niveaux (cela dit, les frontières entres ces différents niveaux sont loin d'être bien nettes) :

- Sécurité des locaux, des infrastructures et des équipements (physique);
- Sécurité des réseaux;
- Sécurité des **applications** et des systèmes d'exploitation;
- Sécurité des données (exp. BD, Datawarehouses, …).



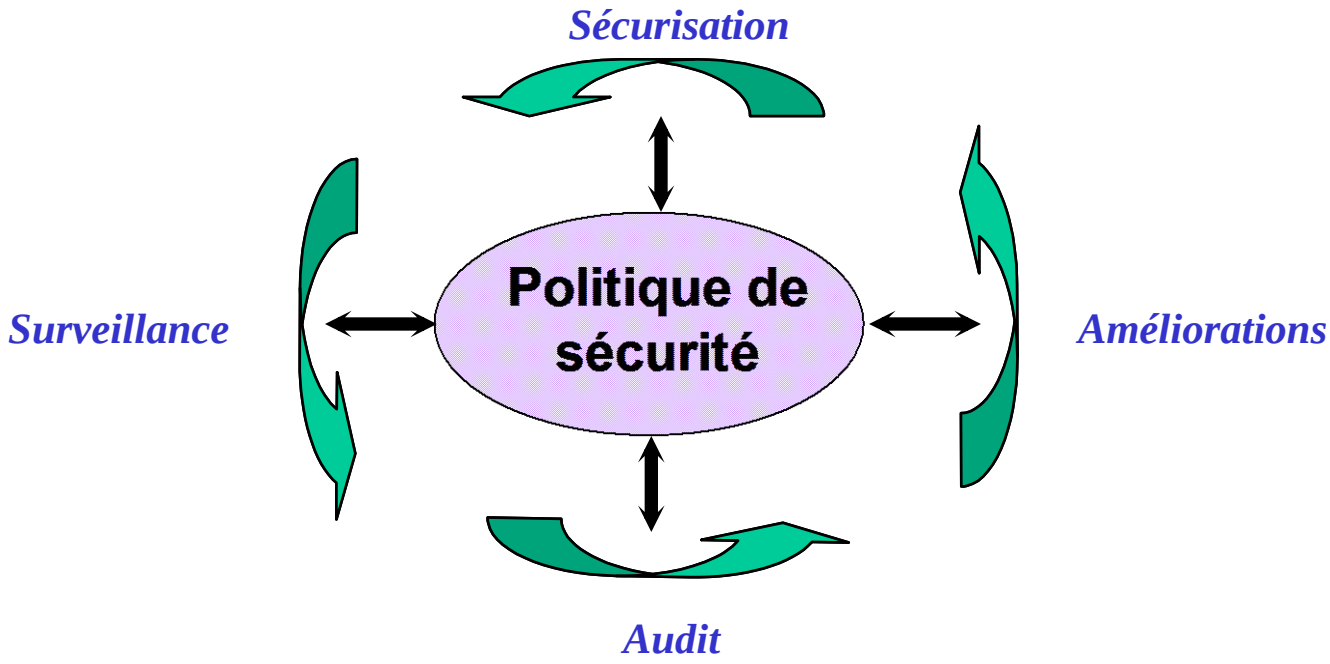
Il faut donc utiliser des mesures et des outils de sécurité distincts pour assurer la sécurité à chaque niveau, en vue de sécuriser globalement tout le SI.

I.2. Où et quoi sécuriser ?



I.3. Comment sécuriser ?

➔ *Cycle de la sécurité:*



I.4. Politique de sécurité

- Elle doit être la base, le point de départ de tout projet de sécurité;

- L'implication des hauts responsables dans l'élaboration d'une PS est plus que souhaitable; elle est indispensable pour la réussite du projet;

- Une PS est une structure autour de laquelle un organisme construit tous les aspects de sécurisation de son SI;

- Elle doit définir les règles représentant les accès acceptables aux ressources du SI : politique de contrôle d'accès;

- Il existe diverses méthodes (bonnes pratiques) qui peuvent servir de guide à l'élaboration d'une politique de sécurité (exp: Marion, Méhari pour l'analyse des risques).

- Différents modèles formels de politique de sécurité (surtout de contrôle d'accès) existent dans la littérature (exp. Bell-Lapadula, Clark et wilson, RBAC, …)

I.4. Politique de sécurité :

☞Il est recommandé qu'elle traite d'abord les points suivants:

- **Diagnostic de l'existant**:
  - Recensement et classification des ressources à protéger;
  - Identification de l'infrastructure Réseau;
  - Inventaire des outils de sécurité existants;
  - Aspects organisationnels.
- **Analyse des risques** :
  - Estimation des vulnérabilités;
  - Identification des menaces éventuelles;
  - Estimation des pertes directes et indirectes pouvant être causées par chaque menace;
  - Définition des priorités concernant les ressources à protéger.

I.4. Politique de sécurité :

- **Définition des rôles (qui est responsable de quoi):**
  - Existence ou non d'un RSSI;
  - Externalisation ou non de la sécurité (si oui: totale ou partielle);
  - Hiérarchie de la sécurité:

    Par exemple: - RSSI à DSI à DG
    - RSSI à DG
    - RSSI à Direction métier
  - Chaînage des responsabilités au sein de l'équipe Sécurité;
  - Rôle (en termes de sécurité) de l'utilisateur final (salarié, client ou fournisseur).

Importance de la sensibilisation à la 'culture' de la sécurité !

I.4. Politique de sécurité :

- **Estimation du coût/ budget de la sécurité**:
  - Le coût de démarrage doit être raisonnable par rapport aux pertes possibles à moyen terme;
  - Le budget annuel de la sécurité (parfois difficile à séparer du budget informatique) doit être inférieur aux pertes probables pendant un an;
  - Choix du niveau de sécurité à atteindre(en termes OSI: classe de sécurité) dépend du budget alloué;
  - Choix fonctionnels et techniques, après:
    - ✓ Comparaison (technique et financière) entre différents outils et technologies disponibles sur le marché;
    - ✓ Formation éventuelle du personnel (du DG à l'utilisateur final);
    - ✓ Sollicitation éventuelle de prestataires de service externes.

I.4. Politique de sécurité :

☞ Elle doit offrir -en réponse aux points précités- une sorte de plan directeur de sécurité qui contient le détail des procédures suivantes:

- **Procédures de protection**, dont:
  - Politique de contrôle d'accès qui comprend les procédures d'accès aux différentes ressources (système, réseau, données, etc);
  - Mécanismes de contrôle et de neutralisation des virus;
  - Mécanismes de protection des informations confidentielles;
  - Procédures de sauvegarde;
  - Procédures de configuration et de mise à jour des outils installés et des correctifs correspondants.

I.4. Politique de sécurité :

- **Procédures de détection**, dont:
  - Mécanismes de surveillance des serveurs (données, messagerie, Web, etc.) ;
  - Mécanismes de surveillance des activités réseaux;
  - Procédures de 'lecture' et d'analyse des activités journalières (Exps: rapports de certains outils, messages d'alertes, tableaux de bord, etc).
- **Procédures de réaction** (juste après la détection de l'incident), dont:
  - Procédures de réaction à une attaque par pirate (différents scénarios);
  - Procédures de réaction à une attaque virale;
  - Procédures de réaction à des incidents de force majeure.

I.4. Politique de sécurité :

- **Procédures de redressement** (réaction à court et moyen terme), dont:
  - Plan de gestion de crise ;
  - Plan de continuité des activités.
  - Contrats d'assurances;
  - Contrats de maintenance;
  - Procédures judiciaires.

Conclusion : Importance d'une bonne politique de sécurité !

I.4. Politique de sécurité :

- **Qlqs Normes et méthodes utilisés comme 'guides' pour l'élaboration d'une PS (ou d'une partie d'une PS)**:
  - Normes ISO 27001 (ex ISO 17799) :
    - ✓ Depuis 2005, elle offre un cadre de bonnes pratiques à suivre, et une démarche visant à la mise en place d'un « Système de management de la sécurité de l'information » (SMSI) qui permet d'établir une **politique de sécurité**, et de renseigner sur les moyens à mettre en œuvre pour l'appliquer (en s'appuyant sur le guide ISO 27002).
  - Méthodes d'Analyse des risques : Marion, Mehari, Ebios, Octave, etc. et norme ISO 27005.

Sommaire du cours

Sommaire

1. Risques de sécurité au niveau applicatif
2. Besoins de sécurité applicative
3. Moyens de sécurité actuels
4. Pourquoi une PKI ?

II.1. Risques au niveau applicatif

- **Applications à risque :**
  - Applications incontournables :
    - ✓ Messagerie électronique, DNS, etc.
    - ✓ Applications Web ‘locales’ et ‘Publiques’
    - ✓ Progiciels,…
  - Applications en plein essor :
    - ✓ E-commerce
    - ✓ E-gouvernement
- **Menaces contre la sécurité des SI, ont tendance à migrer du niveau réseau au niveau applicatif (surtout les applications Web et les Web services).**

II.1. Risques au niveau applicatif

Principales attaques applicatives:

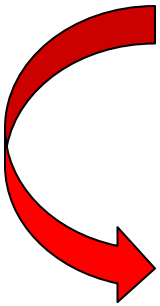
- Attaques contre les serveurs DNS
- Spam, Spam et encore du Spam
- Attaques contre les applications Web
- *Ingénierie sociale (pas vraiment une attaque applicative mais ..) et risques liés aux réseaux sociaux (Facebook, Twitter, …)*
- Attaques au niveau des sites Web
  - ✓ Au second semestre 2008, 61 des 100 sites les plus populaires, contenaient du contenu malicieux ou des redirections cachées (Réf: une étude publiée en octobre 2009 par WebSense).
  - ✓ Le nombre de sites légitimes compromis dépasserait le nombre de sites créés par des cybercriminels.
  - ✓ Les sites de réseaux sociaux sont un trésor d'information pour les attaquants et un moyen d'acheminer les attaques (vol d'identité, phishing, distribution de vers, …).

II.2. Besoins de sécurité applicative

- **Besoins de sécurité:**
  - **Contrôle d'accès** aux applications et gestion des **autorisations**;
  - **Authentification** des utilisateurs & serveurs (exp: sites Web) ;
  - **Non-répudiation** des transactions par les utilisateurs;
  - **Traçabilité** des actions des utilisateurs et des processus;
  - **Intégrité** des données et **confidentialité** des données 'critiques' ;
  - **Disponibilité** des applications/services/données;
  - Résistance aux attaques applicatives (réduction des vulnérabilités).
- **Besoins annexes:**
  - Convivialité ;
  - Performance (temps de réponse ↘).

II.3. Moyens de sécurité actuels

- **Cryptographie à clé publiques/ à clés secrètes**
- **Signature électronique**
- **Certificats de clés publiques**
- **Protocoles sécuritaires : SSL/TLS, IP-Sec, 3D-Secure, …**
- **Réseaux privés virtuels : VPN**



Infrastructure de clé publique ou PKI

plus qu'une solution technique

Signature électronique:

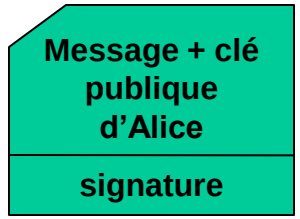
- **Fonctions d'une signature :**
  - Authentification du signataire
  - Acceptation présumée des termes du 'document' signé
  - Preuve en cas de litiges
- **Définitions :**
  - Électronique : Une donnée sous forme électronique qui est jointe ou liée logiquement à une unité de données et qui sert de méthode **d'authentification**. Elle peut être utilisée pour identifier le(s) signataire(s) d'un acte **juridique** accompli par voie électronique.
  - Numérique : données ajoutées à l'unité de données, ou une transformation cryptographique de cette unité permettant à un destinataire de prouver la source et l'intégrité de l'unité.

Signature électronique:

➢ Définitions (suite):

- Sécurisée (adoptée par le conseil des ministres du 13/4/06): une signature électronique qui doit :
  - ✓ être liée uniquement au signataire;
  - ✓ permettre d'identifier le signataire;
  - ✓ être créée par des moyens que le signataire puisse garder sous son contrôle exclusif;
  - ✓ être liée aux données auxquelles elle se rapporte, de telle sorte que toute modification ultérieure de ces données soit détectable.
- Sécurisée présumée fiable : Une signature sécurisée utilisant des moyens certifiés et des **certificats** qualifiés (Décret français du 30 mars 2001).

Signature électronique:



- **Problématique :**
  - Une signature valide n'implique pas forcément que le message est bien signé par 'Alice', pour la simple raison qu'il se peut que **la clé publique** utilisée pour la vérification de la signature ne soit pas réellement la clé publique d'Alice mais celle d'une autre entité qui veut être prise pour Alice.
  - Le vérificateur de la signature doit avoir la ***certitude*** que la clé publique est bien celle de Alice. Il lui faut donc un mécanisme permettant d'affirmer qu'une clé publique correspond ou non à une entité.

    → Si la *confidentialité* d'une clé publique n'est pas requise (au contraire, il faut la publier), son ***intégrité et son authenticité*** sont à préserver.

Certificat numérique :

- **Rôle/ utilisation :**
  - Un certificat de clé publique est un ensemble de données numériques dont le rôle est de lier une clé publique à son propriétaire pour qu'un utilisateur du certificat puisse croire à l'authenticité de la clé publique certifiée et donc à celle d'un document signé moyennant la clé privée associée.
  - Ce rôle ne peut être rempli que si :
    - ✓ le certificat est émis et signé par une tierce partie considérée 'de confiance' par le vérificateur du certificat et qui -par le biais de cette signature- affirme qu'elle est convaincue de l'authenticité de la clé publique qu'elle a certifiée.
    - ✓ Le vérificateur connaît de *manière sûre* la clé publique de la tierce partie afin de pouvoir vérifier sa signature apposée au certificat.

Certificat numérique :

- **Problématique :**
  - Si le vérificateur n'a pas pu obtenir 'directement' la clé publique de la tierce partie, il doit vérifier son authenticité, elle aussi, grâce à un autre certificat (de cette clé) signé par une autre tierce partie de confiance, et ainsi de suite.
  - On dit, dans ce cas, qu'il procède à la validation d'un chemin de certification.
    - → Pour que ce chemin *aboutit*, il faut au moins que parmi ces tierces parties, il y en a une dont le vérificateur connaît, de manière sûre, la clé publique et ce, sans biais de certificat (on parle de 'Trust Anchor').

Certificat numérique :

- **Description :**
  - En général, un certificat contient les informations suivantes :
    - ✓ Identifiant de l'émetteur du certificat (la tierce partie de confiance qui a signé le certificat) ;
    - ✓ Identifiant et/ou autre information de l'entité qui possède la clé publique à certifier (sujet du certificat) ;
    - ✓ La clé publique objet de certification ;
    - ✓ Autres informations (exp : date d'expiration).
    - ✓ **Signature** de l'émetteur du certificat
- **Formats les plus utilisés : X.509 V3, PGP**

Certificat numérique :

➢ Certificat X.509 V3 (1/3):

- Il est le format le plus utilisé; il est défini par l'ISO/IEC JTC1 SC21 comme faisant partie des spécifications X.509 V3. :
  - ✓ Cette 3ème version (datant de 1995) est la plus flexible grâce au champ **d'extensions** qui peuvent être définies, par une communauté d'utilisateurs, dans le but de contenir des informations qui lui sont spécifiques et utiles.
  - ✓ Chaque extension est caractérisée par trois informations :
    - l'identifiant de l'extension considérée,
    - le fait qu'elle soit critique ou non,
    - la valeur de l'extension, propre à un certificat.
  - ✓ Le champ d'extension(s) peut ne contenir aucune extension.

Certificat numérique :

- **Certificat X.509 V3 (2/3):**

CERTIFICAT

Contenu du certificat (Données certifiées)

Version 3
Numéro de série du certificat
Informations sur la signature du certificat par l'AC (algorithmes et paramètres)
Nom du fournisseur du certificat
Période de validité du certificat
Nom du porteur de certificat
Informations sur la clé publique (valeur de la clé publique, algorithme et paramètres)
Extensions du Certificat

Identifiant du type de l'extension	Criticité (oui / non)	Valeur
Identifiant du type de l'extension	Criticité (oui / non)	Valeur
Identifiant du type de l'extension	Criticité (oui / non)	Valeur
…		

Algorithme de signature du certificat par l'AC

Algorithmes
Paramètres

Signature numérique du contenu du certificat

Valeur de la signature numérique du certificat par l'AC

Certificat numérique :

➢ Certificat X.509 V3 (3/3):

- Des extensions sont standardisées , comme :
  - ✓ SubjectAlternativeName :
  - ✓ IssuerAlternativeName :
  - ✓ KeyUsage : usage de la clé certifiée (signature, chiffrement de clé, signature de certificat, …)
  - ✓ CertificatePolicies : indique les **politiques de certificat** supportées par l'émetteur;
  - ✓ PolicyMappings : indique l''équivalence' entre politiques de domaines différents;
  - ✓ PolicyConstraints :permet à l'émetteur d'appliquer des contraintes concernant les politiques de certificats sur les autres émetteurs dans un chemin de certification.;
  - ✓ Etc.

Certificat numérique :

- **Autorités de certification :**
  - Les émetteurs de certificats sont –à priori- des tierces parties de confiance qui ont donc pour rôle d'émettre des certificats qui permettent à des entités communicantes de s'authentifier en prouvant l'authenticité de leurs clés publiques et donc de leur signature.
  - Ces émetteurs sont appelés des autorités de certification ou 'CAs'.
  - Une **CA** est généralement un organisme, publique ou privé, qui jouit d'une notoriété au sein d'une communauté (qui peut être restreinte ou large) de telle sorte que cette dernière croit à l'authenticité des certificats qu'elle émis.

Certificat numérique :

- **Politique de certificat :**
  - Dans X.509, elle est définie comme étant « Un ensemble nommé de règles qui indiquent l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes ». Elle détermine :
    - ✓ le niveau d'assurance attribué au certificat ;
    - ✓ le mode de vérification de l'identité des titulaires ;
    - ✓ la durée de validité des certificats ;
    - ✓ La révocation (utilisation des CRL)
    - ✓ Les limites de responsabilité
    - ✓ Le niveau des contrôle de sécurité et des audits, etc.

Certificat numérique :

- **Politique de certificat (2/2):**
  - Une CA pour montrer qu'elle est conforme à une politique de certificat, elle doit publier un CPS (Certificate Practice Statement) dont le rôle est de décrire de manière plus détaillée les pratiques d'émission et de gestion de certificats suivies par cette CA.
  - Le CPS représente donc la manière dont la politique de certificat est appliquée.
  - La confiance 'dans' un certificat émis par une CA dépend de sa politique de certificat et de son CPS.

Certificat numérique :

- **Types de certificat :**
  - Il existe principalement deux types de certificats :
    - ✓ Le certificat d'identité où la partie réservée à l'information concernant le propriétaire de la clé publique permet de l'identifier.
    - ✓ Le certificat d'autorisation ou d'attributs où on ne s'intéresse pas à l'identité de l'entité certifiée mais à un certain nombre de ses attributs (tranche d'âge, profession, possession d'une licence spéciale, etc.).
  - Ces deux types de certificats diffèrent aussi en termes de :
    - ✓ durée de vie (généralement plus courte pour un certificat d'attributs)
    - ✓ Portée d'application (généralement plus réduite pour un certificat d'attributs)
    - ✓ Autorité émettrice (AA vs CA)

Une CA ou une PKI?

- **Une CA est un composant d'une PKI parmi d'autres**
- **Une PKI peut contenir plusieurs CAs**
- **L'importance d'autres types d'entités que les CAs**
- **Une PKI est donc plus qu'une simple CA**

Sommaire du cours

III. Infrastructures de clés publiques PKI

Sommaire

III.1. PKI : Définitions, Rôle & Fonctionnement

➢ **Définition 1**

Un ensemble d'entités, communiquant par des protocoles et offrant des services pour la gestion (création, distribution, révocation, …) des clés publiques et de leur certificat (≈ IETF).

➢ **Définition 2**

Un système global d'authentification, de gestion des relations de confiance et de méthodes de protection de la confidentialité où les autorités de certification (CA) agissent comme des émetteurs de certificats

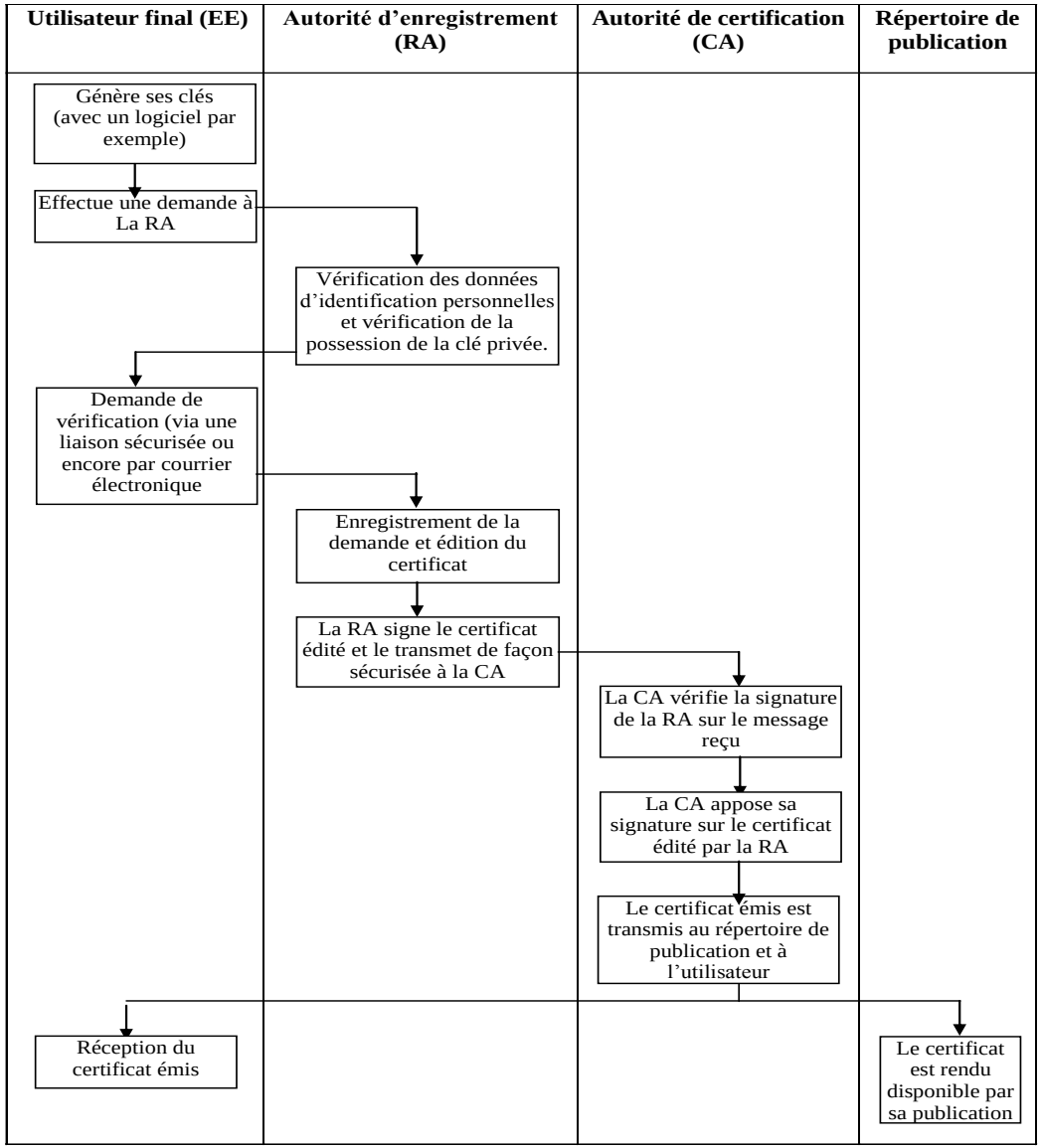
➢ Une PKI est généralement composée de plusieurs CAs afin de permettre l'utilisation des certificats dans un contexte large où une seule CA ne peut assurer à elle seule la gestion et la distribution de tous les certificats.

III.1. PKI : Définitions, Rôle & Fonctionnement

- **Entités** :
  - Entité finale (EE) : le titulaire d'un certificat et le vérificateur d'un certificat,
  - Autorité d'enregistrement(RA),
  - Autorité de certifications(CA)
  - Autorité de certification de politique (PCA et/ou PAA).
- **Méthode de révocation/validation** : liste de certificats révoqués (CRL) ou validation en ligne (exp. On-line Certificate Status Protocol :OCSP)
- **Politique de certificats** : un ensemble nommé de règles qui indiquent l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes .
- **Modèle de confiance** : architecture, relations de confiance, etc.
- **Les protocoles de gestion de certificats**

III.1. PKI : Définitions, Rôle & Fonctionnement

- **Emission d'un certificat** :



Rôle d'une PKI :

- Fournir les mécanismes nécessaires à établir des relations de confiance entre ses utilisateurs et leur offrir des services de sécurité tels que la confidentialité, l'intégrité, l'authentification et la non-répudiation et ce, essentiellement par le biais des certificats de clés publiques.
- Parmi les contextes où une PKI est très utile si ce n'est nécessaire, on trouve :
  - L'e-commerce ;
  - L'e-gouvernement ;
  - Le cas d'une grande entreprise possédant plusieurs applications qui nécessitent des services d'authentification et d'autorisation.

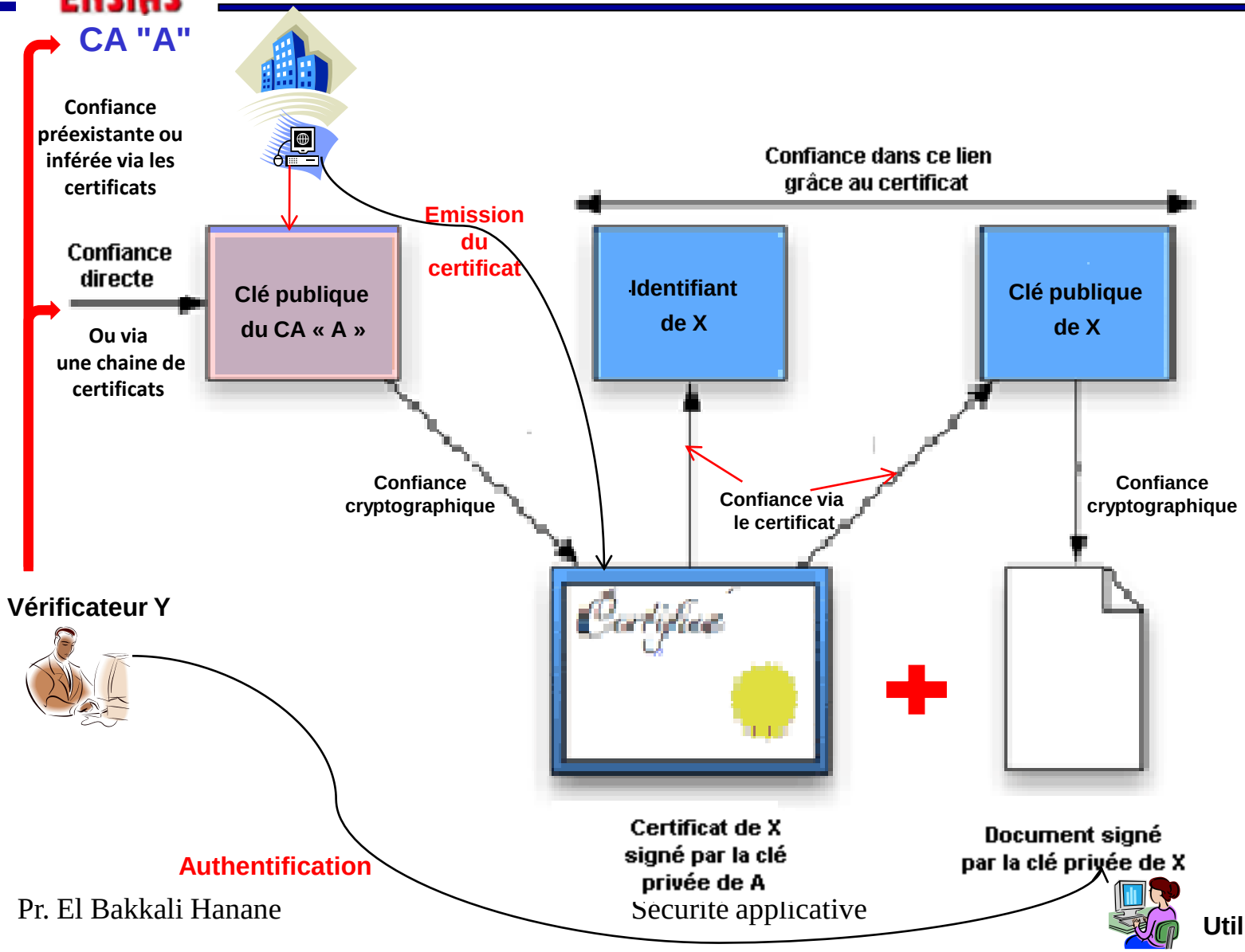
Confiance dans le 'contexte PKI'?

- Les relations de confiance entre entités d'une PKI se basent sur des relations préalables entre elles qui sont de deux sortes :
  - relations préexistantes en dehors de la PKI ;
  - relations nécessaires à l'adhésion à la PKI.
- Elles se basent aussi sur la confiance dans les techniques cryptographiques (algorithmes de cryptage & fonctions de hashage)
- La confiance n'est jamais totale ou absolue, elle est plutôt limitée par des contraintes et relative à un contexte donné.

Confiance 'inférée' suite à l'émission d'un certificat

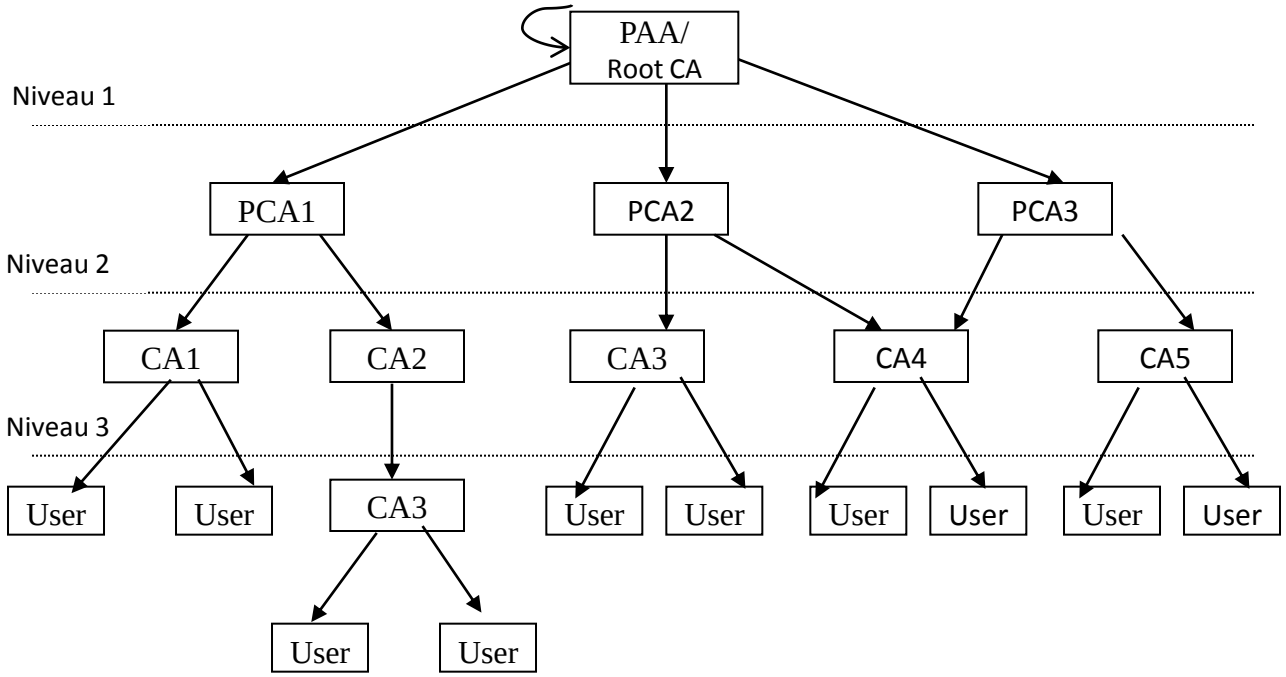
- Le vérificateur du certificat, dépendamment de sa confiance dans la CA émettrice et de sa politique de certification, peut 'inférer' les croyances suivantes :
  - La CA émettrice du certificat a été '*convaincue*' –suite à des procédures qui lui sont spécifiques - de l'authenticité du lien entre la clé certifiée et le sujet du certificat au moment de son émission. Ce lien peut concerner :
    - ✓ l'identité du sujet (certificat d'identité);
    - ✓ des attributs du sujets (certificat d'attributs ou d'autorisation).
  - Il est confiant - à un certain degré - de l'authenticité du dit lien.
- Confiance dans une CA : Compétence vs Honnêteté.

III.3. Modèle de confiance d'une PKI



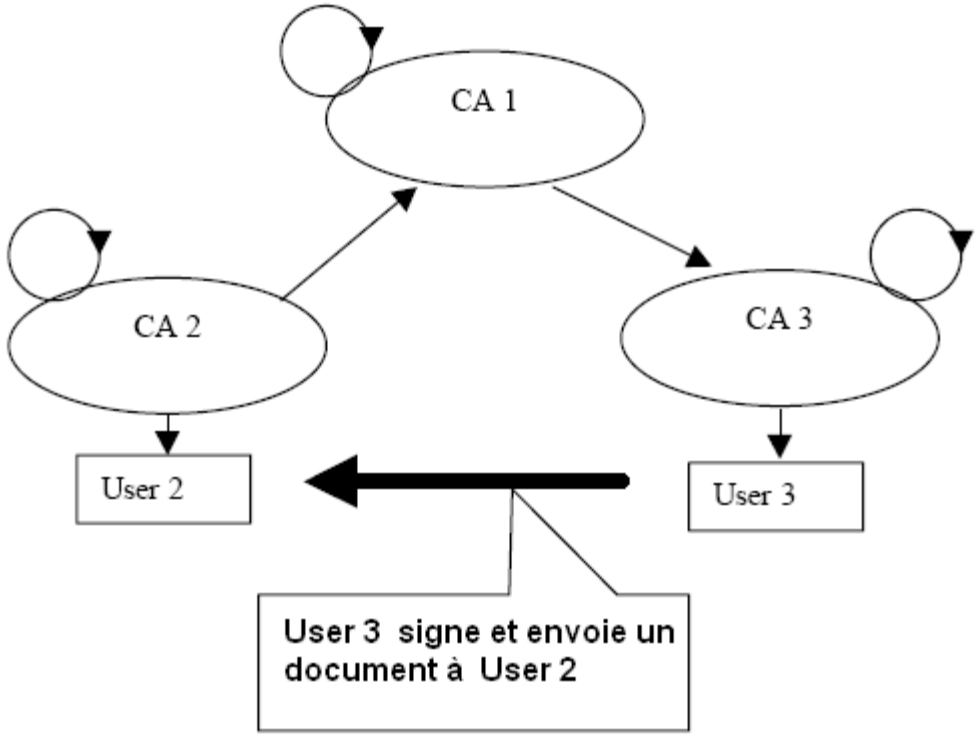
III.3. Modèle de confiance d'une PKI

➢ **Exemple d'un modèle hiérarchique** :



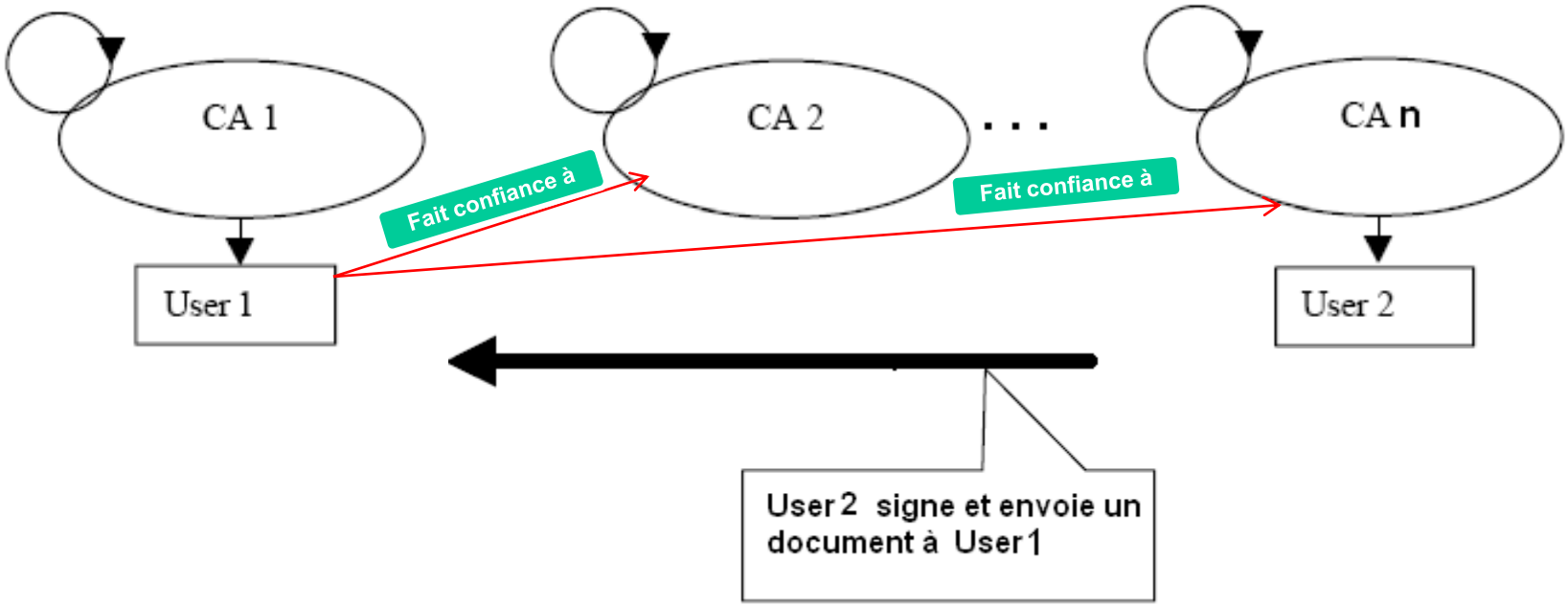
III.3. Modèle de confiance d'une PKI

- **Exemple d'un modèle 'réseau' avec des cross-certifications** :



III.3. Modèle de confiance d'une PKI

➢ **Exemple du modèle 'Liste de confiance'** :



III.4. Types d'une PKI

- PKI globales vs fermées :
  - Globales : PKI préconisée par les normes X500/X509 ou la PKI de PGP (web of trust).
  - 'Fermées' ou 'autonomes' d'entreprise :
    - ✓ En général, une seule autorité de certification suffit.
    - ✓ Achat de solution 'clé en main' parfois open source (exp : NewPKI, IDX-PKI de IDEALX, …)
    - ✓ Marché de plus en plus florissant des vendeurs de solutions PKI.
- PKI gouvernementales vs privées :
  - Gouvernementales: PKI du Canada, PKI fédérale des U.S.A, L'IGC/A (Infrastructure de Gestion de la Confiance de l'Administration) de la DCSSI française , CertEurope, …
  - Privées (prestataires de service de certification): Verisign devenu External Certificate Authority en 2005 (agréé par les agences fédérales des U.S.A), Entrust, KEYNECTIS, etc.

III.5. Limitations d'une PKI

- Problème de déploiement et de gestion
- Problème d'interopérabilité
- Coût élevé
- Non comprise ou non appréciée par les utilisateurs
- Politiques de certificats très 'légères' ou ignorées
- Problèmes techniques (révocation, protection des clés privés, veille technologique, …)
- PKI globale difficile à atteindre
- Complexe et fait appel généralement à d'autres infrastructures complémentaires (Horodatage, archivage, notarisation, …)
- etc.

III.6. PKI : Conclusion

- La confiance dans la sécurité offerte par les solutions PKI ne peut être vraiment légitime que si les problèmes –techniques, organisationnelles et juridiques- posés par les technologies cryptographiques et autres moyens qu'elles utilisent soient résolues de manière satisfaisante.
- Satisfaisantes dans le sens où l'objectif visé n'est pas une sécurité absolue –qui n'est qu'une chimère- mais une sécurité comparable à celle offerte dans le monde conventionnelle.
- Le challenge concerne plutôt les PKI globales et beaucoup moins les PKI fermées
- Mais, les applications de type e/m- commerce ou e/m-gov ont plutôt besoin d'une large PKI.
- Tous les gouvernements du monde y travaillent dans ce sens.

Sommaire du cours

Autorité d'horodatage :

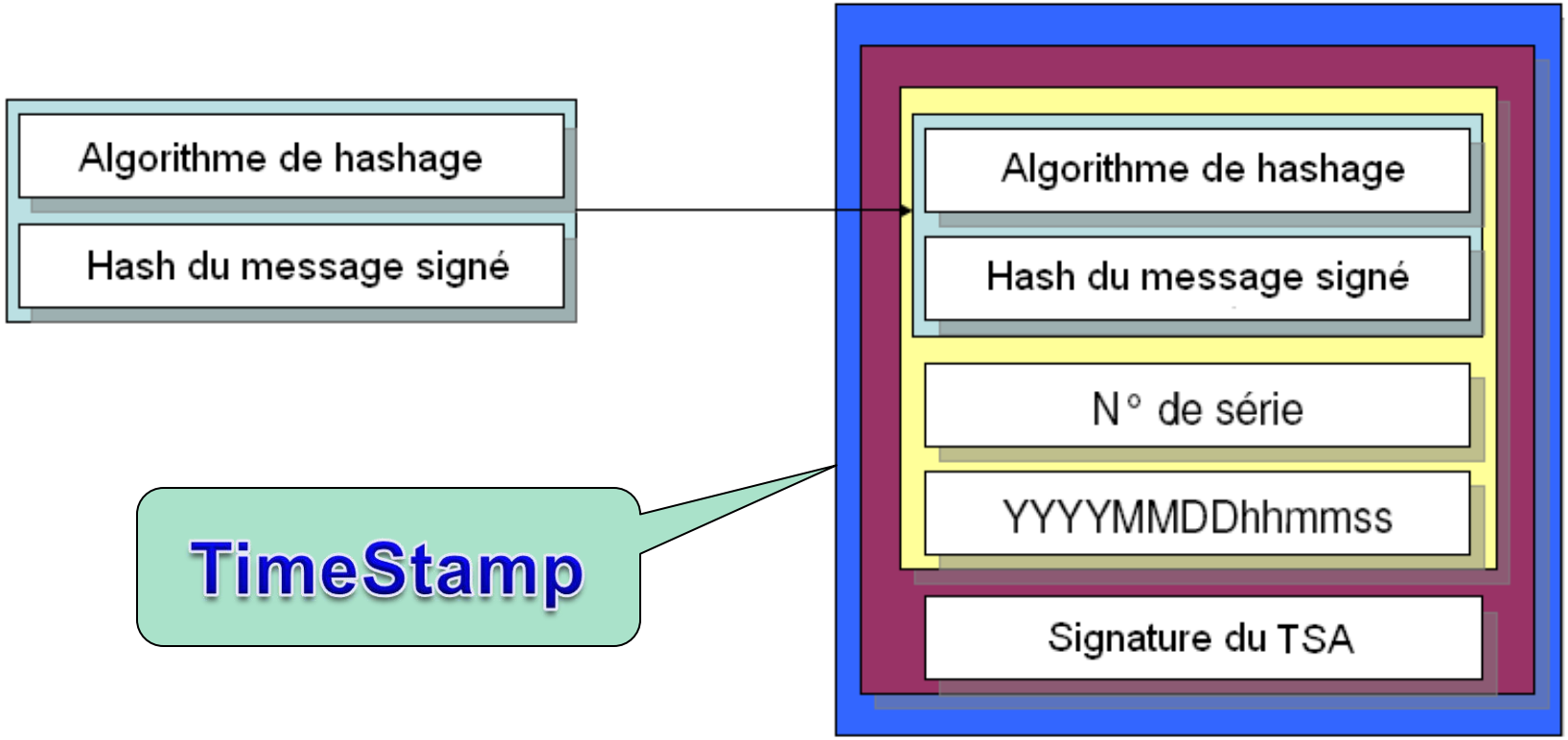
- **Définition :**
  - Une Autorité d'Horodatage ou Time Stamp Authority (TSA) peut être définie comme une tierce partie de confiance dont le rôle est de certifier des heures et des dates.
  - Une TSA est généralement associée à une PKI et permet de renforcer les services de sécurité offerts par la PKI (surtout la non-répudiation).
- **Buts de l'horodatage :**
  - Prolonger la durée de vie d'une preuve signée au-delà de la durée de vie de la signature (ou du certificat correspondant) en apportant la preuve d'antériorité ;
  - Éviter le renvoi à une date ultérieure d'un message par une entité qui a pu se le procurer (protection anti-rejeu ou replay).

Autorité d'horodatage:

- **Principe :**
  - **Compléter** la signature électronique d'un document par la date de signature ➔ signature électronique de la date connue sous le nom de contremarque ou jeton de temps (Time Stamp).
  - Un horodatage sécurisé doit se baser sur une source de temps sécurisée et reconnue fiable.
  - Si les certificats sont utilisés (ce qui est souvent le cas), il faut prolonger la durée de conservation des certificats et des listes de certificats révoqués (CRL).
  - La RFC 3161 définit le format des Time Stamps et le protocole TSP (Time Stamp Protocol).

Autorité d'horodatage:

- **Jeton d'horodatage (TimeStamp):**



Autorité d'horodatage:

- **Services offerts :**
  - Garantie de date de signature,
  - Preuves de possession,
  - Preuves d'existence et d'antériorité,
  - **Renforcement de la non-répudiation,**
  - Garantie de l'heure d'une transaction (commerciale ou administrative),
  - Garantie des heures et des dates des listes de certificats révoqués (CRL),
  - Messages avec accusés de réception,
  - **Notarisation et archivage sécurisés**,
  - …

Autorité d'horodatage:

- **Quelques questions importantes :**
  - Valeur légale du TimeStamp émis par une TSA ?
  - Durée de validité du TimeStamp (5 ans, 30 ans, …) ?
  - Validité du TimeStamp dans le cas où la TSA a arrêté ses activités ?
  - Exigences pour une TSA de confiance ?
  - Combinaison d'une signature non certifiée (non présumée fiable) et un TimeStamp qualifié ?
  - Taille de clé de l'algorithme de cryptage ou la sécurité de la fonction de hashage ne sont plus suffisants ?

Archivage sécurisé:

- **But :**
  - Conserver « en l'état » les contenus qui lui sont confiés tout en assurant de les restituer à l'identique ultérieurement.
- **Utilisation avec une PKI :**
  - L'archivage sécurisé des document signés, des certificats et toutes informations utiles relatives à la certification vise à se préparer aux éventuels besoins de restitution (par exemple, suite à des litiges) qui peuvent avoir lieu après l'expiration ou la révocation d'un certificat ou l'arrêt de service d'une CA.
  - L'archivage peut être interne ou via un tiers archiveur externe et indépendant jouant le rôle d'une **autorité d'archivage** de confiance (TAA: Trusted Archive Authority).

Autorité d'archivage:

- **Services offerts :**
  - Sauvegarde sécurisée (intégrité préservée) des documents électroniques qui lui sont confiés (exp, certificats, CRL, politiques de certificats, …) ;
  - Conservation active **sur le long terme** en prenant en charge **l'évolution des supports de stockage** (changement des mediums de sauvegarde lorsque cela s'impose) et des technologies cryptographiques ;
  - Mise à disposition des documents archivés aux personnes **autorisées** ou administrations mandatées ;

Sommaire du cours