



Les 17,18,19,20 novembre 2008
Yamoussoukro – CÔTE D'IVOIRE

ATELIER : INFRASTRUCTURES A CLES PUBLIQUES (ICP/PKI)

YAO Éric Armand



Infrastructure à clé publique (ICP/PKI)

◆ Agenda

- Introduction
- Certificats numériques
- Infrastructure à clé publique
- Composantes d'une PKI
- Gestion des certificats
- Modèle de Confiance

Introduction (1/3)

- ◆ L'évolution des technologies de l'information ont changé la gestion des clés cryptographiques.
- ◆ Historiquement, les infrastructures de gestion des clés (IGC) étaient une partie intégrante :
 - Des équipements,
 - Des réseaux spécifiques à une communauté fermé d'utilisateurs (militaires, diplomates, banquiers, etc.)
- ◆ Aujourd'hui, l'IGC doit répondre à une communauté de plus en plus ouvertes d'utilisateurs ayant :
 - Des besoins multiples,
 - Des matériels hétérogènes.

Introduction (2/3)

- ◆ Dans le cadre du développement des échanges électroniques :
 - comment reconnaître les interlocuteurs et leur faire confiance s'il n'est pas possible :
 - ◆ De les voir,
 - ◆ De les entendre,
 - ◆ Ni même de recevoir leurs signatures ?
 - Comment préserver le secret des échanges sans recourir à :
 - ◆ Des enveloppes fermées,
 - ◆ Des appels téléphoniques chiffrés ?
 - Comment être assuré que le destinataire a reçu le message intact et soit sûr de son origine ?

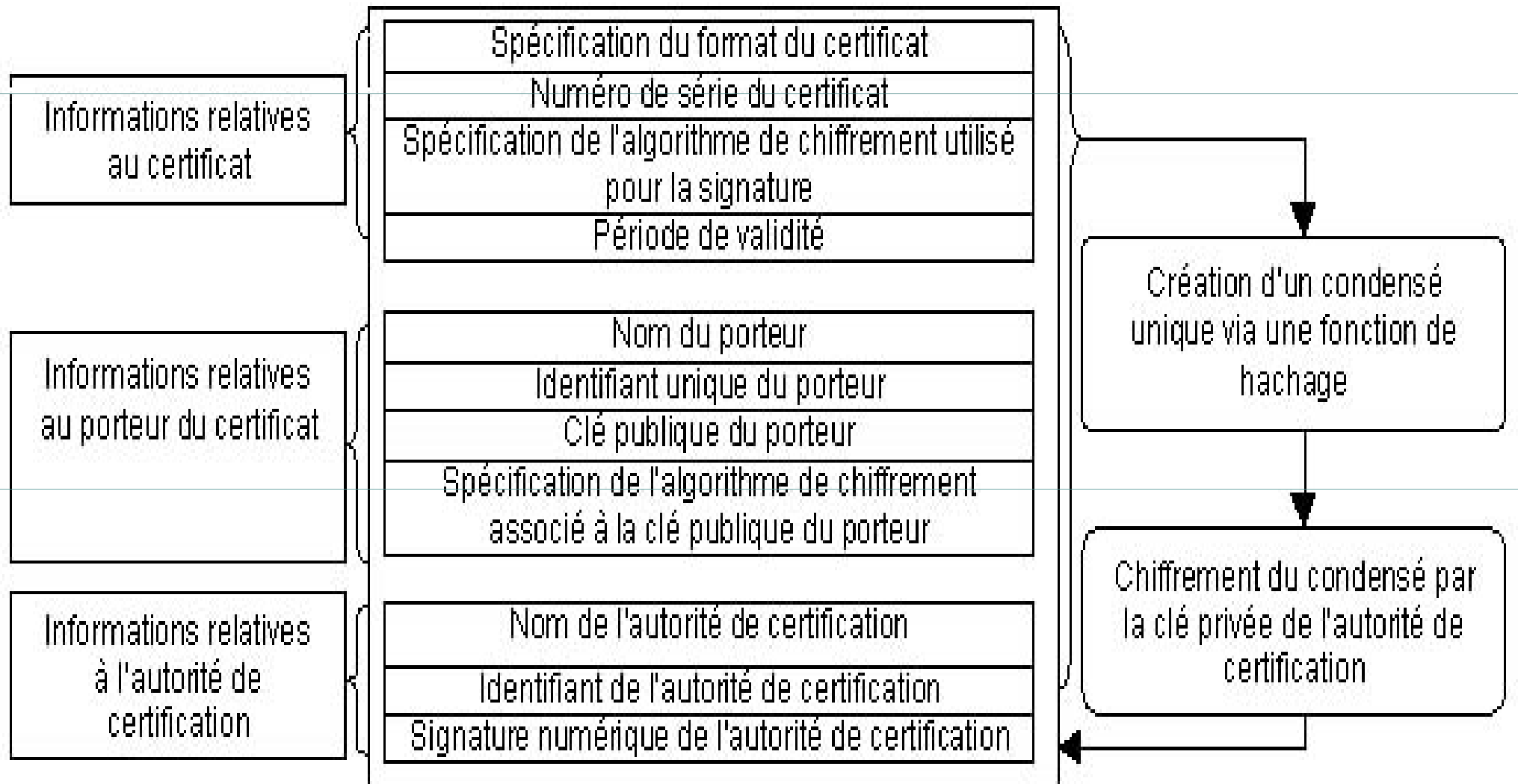
Introduction (3/3)

- ◆ Les infrastructures à clé publique nous offre un environnement de confiance pour garantir aux transactions électronique :
 - La confidentialité : seul le destinataire peut connaître le contenu des messages qui lui sont transmis.
 - L'authentification : le destinataire d'un message doit pouvoir s'assurer de son origine.
 - L'intégrité : le destinataire doit pouvoir s'assurer que le message n'a pas été modifié.
 - La non répudiation : L'émetteur et le destinataire ne peuvent nier avoir respectivement envoyé et reçu le message.

Le certificat numérique

- ◆ Un certificat numérique est une pièce d'identité électronique.
- ◆ Il est l'une des mises en œuvre de la signature électronique.
- ◆ Il permet d'authentifier l'émetteur d'un document, d'un message ou d'une transaction électronique.
- ◆ La forme standard d'un certificat est définie selon la norme X.509.

CONTENU D 'UN CERTIFICAT (X.509)



Les usages des certificats

- ◆ Authentifier les utilisateurs dans certaines applications (accès aux ressources Internet, Intranet, Extranet),
- ◆ Authentifier les serveurs,
- ◆ Vérifier les signatures numériques,
- ◆ Sécuriser des messages électroniques.

Les usages des certificats

- ◆ SSL(Secure Socket Layer - connexion):
 - certificat client et serveur
- ◆ S/MIME(Secure Multipurpose Internet Mail Extensions)
 - certificat client
- ◆ SET et 3D-Secure (Visa, MasterCard, etc.)
 - certificats marchand
 - certificats porteur de la carte de crédit
 - certificats passerelle de paiement
- ◆ SSH (Secure Shell)
- ◆ IPsec (réseau)

Infrastructure à clé publique (PKI/ICP)

- ◆ Un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques ou HSM, des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques.
- ◆ Son but est de répondre aux besoins de confidentialité, d'authentification, du contrôle d'accès, de non répudiation et d'intégrité.
- ◆ Elle Contribue à l'authentification des détenteurs de clés en émettant des certificats confirmant la validité des clés et l'identité des détenteurs.

Fonctions réalisées par une ICP

- ◆ Gérer le cycle de vie complet des clés et des certificats ;
- ◆ Fournir Un système de recouvrement de clé ;
- ◆ Mettre à jour les pairs de clés et les certificats;
- ◆ Gérer l'historique des clés ;
- ◆ Fournir une possibilité de certification croisée;

Les éléments nécessaires pour une PKI utilisable

- ◆ Une Autorité de Certification ;
- ◆ Un dépôt de certificats ;
- ◆ Un système de révocation de certificat ;
- ◆ Un système de recouvrement de certificat ;
- ◆ Un support de non-repudiation des signatures numériques ;
- ◆ Une mise à jour des certificats ;
- ◆ Une gestion de l'historique des clés ;
- ◆ Un support pour la certification croisée;

Composantes d'une PKI

La RFC 4210, indique qu'il y a quatre(4) entités impliquées dans la gestion d'une ICP, se sont :

1. L'utilisateur de l'ICP (EE – Entité d'Extrémité),
2. L'Autorité d'Enregistrement (AE/RA),
3. L'Autorité de Certification (AC/CA),
4. Le site de dépôt.

L'Entité d'Extrémité (EE)

- ◆ L'utilisateur ou le système qui est le sujet d'un certificat.
- ◆ Selon la RFC 3647, l'Entité d'Extrémité a les obligations suivantes :
 - La protection de la clé privé de l'entité ;
 - La restriction de l'utilisation de la clé privé et du certificat ;
 - La notification dès que la clé privé est compromise.

Autorité de d'Enregistrement (AE/RA)

- ◆ Interface entre l'utilisateur et l'autorité de certification
- ◆ Rôle :
 - ◆ Authentifie les demandeurs ou porteurs de certificats
 - ◆ Applique la politique de certification vis-à-vis des requêtes des utilisateurs
 - ◆ Récupère la clé publique du demandeur
 - ◆ Soumet les demandes de certificats à l'autorité de certification

Autorité de Certification (AC/CA)

- ◆ Une entité de confiance (gouvernementale ou privée) qui délivre les certificats numériques, qui est responsable de tout le cycle de vie des certificats et qui offre:
 - une combinaison de technologies: protocoles et standards de sécurité (PKI, SSL, SET...).
 - une infrastructure de services hautement sécurisés incluant des systèmes redondants.
 - un recueil de procédures et des engagements de responsabilités qui établissent sa capacité à agir en tant que tiers partie de confiance.
 - ◆ Politique de certification
 - ◆ Déclaration des pratiques de certification
 - Un cadre légal permettant de régler les litiges.

Politique de certification (PC)

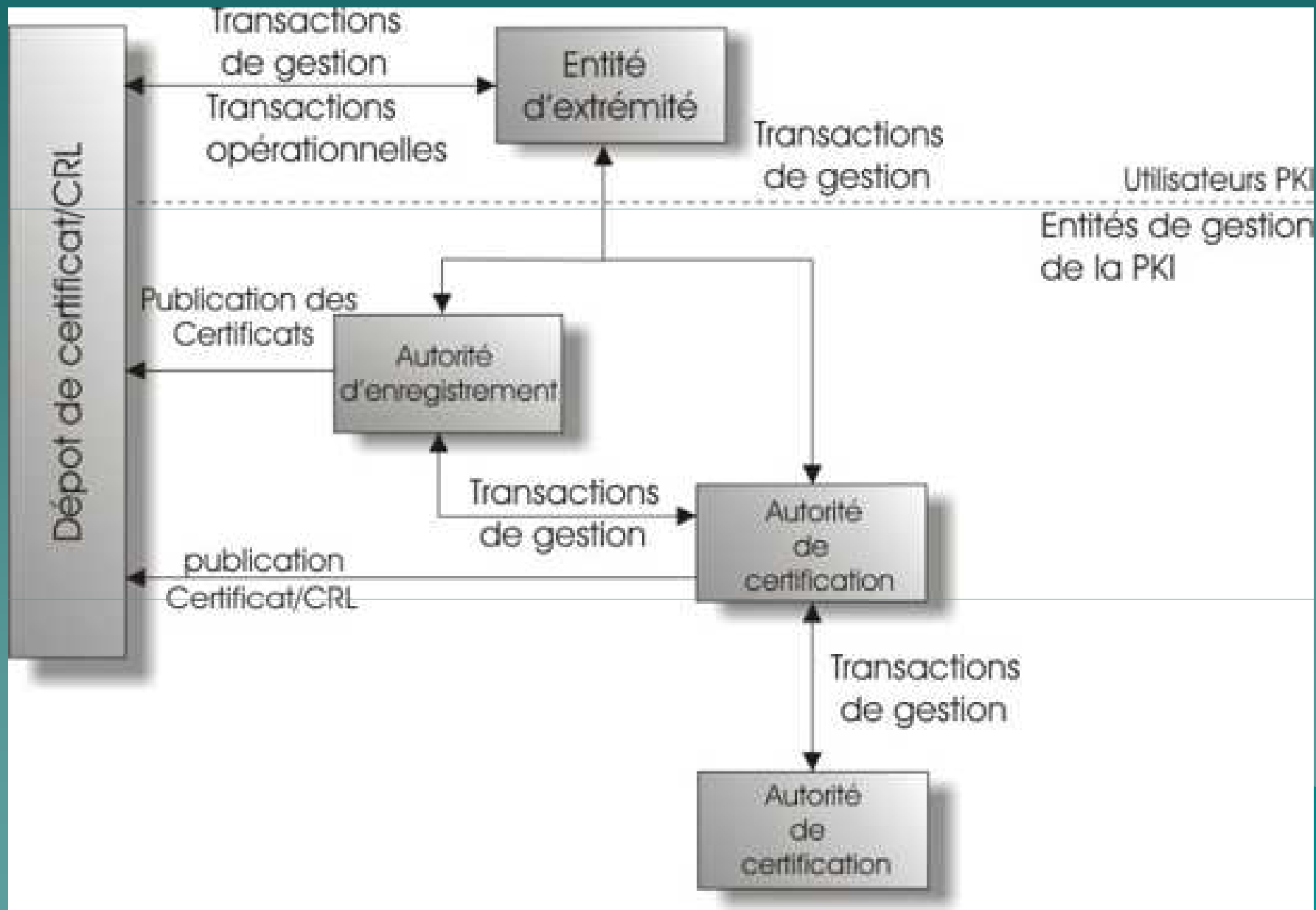
- ◆ La politique de certification représente un document important dans l'activité de certification qui décrit la politique de sécurité adoptée pour la génération de certificats et la publication de leur état.
- ◆ Cette politique de sécurité décrit le fonctionnement de l'autorité de certification ainsi que les responsabilités des utilisateurs lors de la demande et l'utilisation des certificats et des clés.

=> La politique de certification est un document stable (pouvant être utilisé pendant une longue durée).

Déclaration des pratiques de certification (DPC)

- ◆ La DPC est un document détaillé qui décrit comment une autorité de certification implémente une politique de certification spécifique.
- ◆ Une DPC a pour objet de décrire les moyens (techniques et juridiques), les méthodes et les procédures mis en oeuvre afin de garantir que les objectifs de sécurité spécifiés dans la Politique de certification seront effectivement atteints.
- ◆ Chaque DPC est appliquée à une seule politique de certification.
- ◆ La DPC n'est pas un document publique. Il est confidentiel.

Interaction des composantes d'une ICP/PKI



Gestion des certificats

- ◆ Elle doit se faire de façon rigoureuse et sécurisée.
- ◆ La gestion des certificats se compose des opérations suivantes :
 - La génération
 - La révocation
 - La publication
 - L'archivage

Génération de certificat

- ◆ Une AC affirme que l'entité dont l'identité est associée au certificat est le détenteur de la clé publique.
- ◆ Une AC insère son nom dans les certificats et les LCRs qu'elle génère.
- ◆ La clé privée d'une AC doit être hautement sécurisée.
- ◆ Le module cryptographique utilisée pour la génération et la sauvegarde de la clé privée de l'AC doit avoir au minimum les exigences de FIPS 140 level 2.

Génération de certificat

- ◆ L'enregistrement (AE-AC),
- ◆ La génération de la pair de clé (EE-AE-AC),
- ◆ La création du certificat (AC),
- ◆ La distribution de la pair de clé et du certificat (AE-AC)

Révocation de certificats

- ◆ Une révocation correspond à la cessation du fonctionnement d'un certificat avant l'expiration de sa durée de validité.
- ◆ Plusieurs raisons peuvent causer une révocation:
 - ◆ Changement de la valeur d'un champ dans le certificat.
 - ◆ La clé privée du sujet est compromise,...
- ◆ Suite à une révocation, une AC génère une liste (LCR) contenant les numéros de séries des certificats révoqués
- ◆ Une LCR est signée par l'AC pour garantir l'authentification et l'intégrité de son contenu.
- ◆ Les AC peuvent utiliser un mécanisme de notification en ligne tel que OCSP (Online Certificate Status Protocol) pour réduire le temps de latence entre la révocation et la notification.

Publication

- ◆ Les certificats et les LCRs doivent être publiés pour tous les utilisateurs d'une PKI.
- ◆ Plusieurs techniques de publication peuvent être utilisées par une PKI: FTP, Web, annuaire LDAP.
- ◆ Ces techniques doivent être disponibles d'une manière continue pour permettre le bon déroulement des opérations de vérification.

Archivage

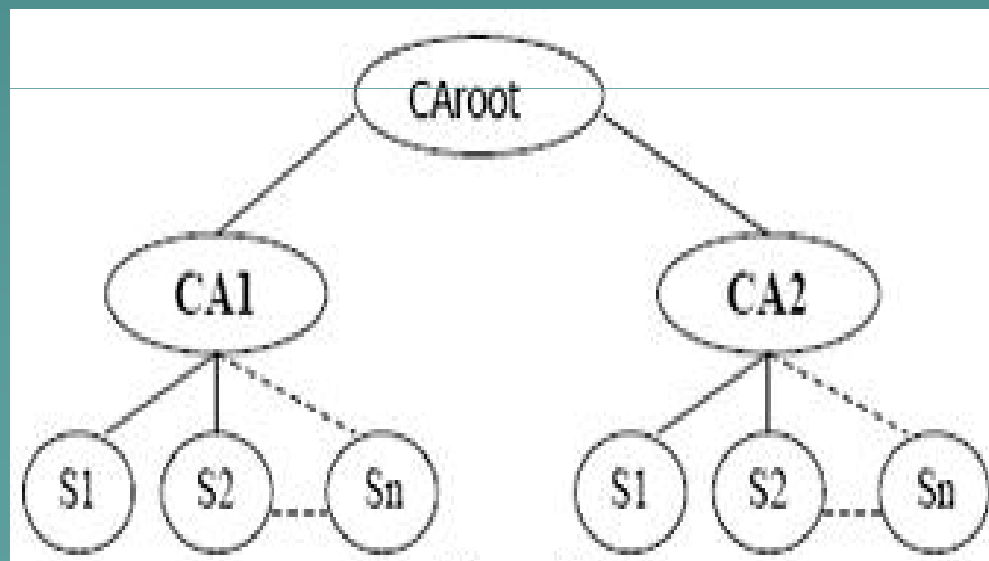
- ◆ Une AC a besoin d'archiver les certificats qu'elle émet pour une longue durée pour permettre les opérations de vérification des documents signés lorsque le certificat associé à la clé privée de signature n'est plus valide.
- ◆ Une AC peut déléguer l'opération d'archivage à une entité externe: archiveur.
- ◆ Un archiveur doit garantir la sécurité des données qu'il archive : contrôle d'accès aux locaux et mécanismes de sécurité logique (signature numérique, cryptage et horodatage)

Modèle de confiance

- ◆ Hiérarchique (une racine AC),
- ◆ En maille (pas de racine),
- ◆ En pont (une autorité de co-certification),
- ◆ Etc.

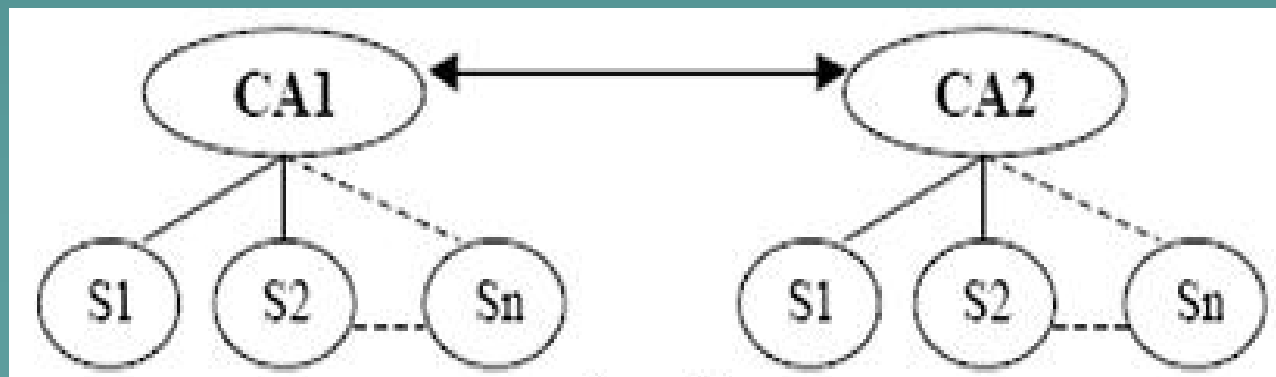
Modèle de Confiance hiérarchique

- ◆ Plusieurs autorités fournissent les services de PKI, qui sont liées par des relations de type « supérieur-subordonné ».
- ◆ Tous les utilisateurs ont confiance dans l'autorité racine de toute la hiérarchie. C'est le seul composant qui a un certificat auto-signé.
- ◆ Une nouvelle autorité doit faire générer son certificat par une des autorités déjà existantes.



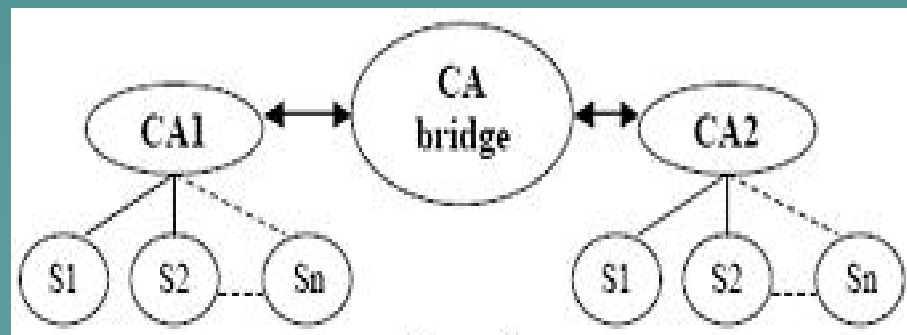
Modèle de Confiance en maille

- ◆ Plusieurs autorités fournissent les services de PKI. Ces autorités sont liées par des relations de confiance d'égal à égal.
- ◆ Les autorités de certification génèrent des certificats entre elles. Elles sont responsables mutuellement des certificats de leur homologue.
- ◆ Une nouvelle autorité échange des certificats avec au moins une autorité de la maille.



Modèle de Confiance en pont

- ◆ L'autorité de certification pont joue le rôle d'un médiateur de confiance.
- ◆ Cette autorité ne génère pas des certificats pour des utilisateurs finaux.
- ◆ Elle permet de limiter les échanges entre les autorités. Le nombre d'échange entre les autorités est réduit car il ne faut plus échanger la clef publique avec toutes les autres autorités mais uniquement avec l'autorité pont.



Conclusion

- ◆ L'usage de certificats numériques permet de répondre aux 4 besoins de sécurité pour l'échange d'informations qui sont :
 - l'intégrité : les données n'ont pas été modifiées
 - la non-répudiation : l'expéditeur d'un message ne peut pas nier son envoi et son contenu
 - la confidentialité
 - l'authentification
- ◆ Les certificats associés à une infrastructure à clé publique permettent d'instaurer des relations de confiance et ainsi favoriser le développement du commerce électronique et de façon générale toute transaction électronique.