Infrastructure de gestion de clés publiques(PKI)

Introduction :

La PKI peut etre definie comme un dispositif technologique qui permet de créer des Autorités de Certifications (AC) pour identifier les entités. L'autorité de certification a donc pour rôle de délivrer les certificats numériques. Ces derniers permettent d'entreprendre des opérations cryptographiques telles que le chiffrement (ou cryptage), l'authentification et la signature numérique. Ces opérations servent à garantir la confidentialité, l'intégrité et la non-répudiation lors des transactions électroniques.

Dans ce chapitre, nous allons définir l'infrastructure de gestion de clés publiques ainsi que ses composants, le processus et la politique de certification, les différents protocoles d'une PKI et enfin le processus de publication.

2.1 Notion de PKI

Une PKI assure la sécurité des transactions électroniques et l'échange de renseignements sensibles grâce à des clefs cryptographiques et à des certificats. Une PKI offre divers services : confidentialité, contrôle d'accès, intégrité, authentification, services de non-répudiation pour les transactions commerciales électroniques et les applications informatiques connexes.[**W3**]

En outre, elle gère la production et la distribution des paires de clefs publique et privée, et diffuse la clef publique (ainsi que l'identification de l'utilisateur) sous forme de « certificat » sur des babillards électroniques publics.

Une PKI comprend ce qui suit :

— Autorité de certification ;
— Annuaire de certificats ;
— Autorité Système de révocation de certificats ;
— Système de sauvegarde et de récupération de clefs ;
— Autorité Soutien à la non-répudiation ;
— Mise à jour automatique des clefs ;
— Autorité Gestion de l'historique des clefs ;
— Horodatage ;

— Logiciel client interagissant de manière fiable et continue avec tout ce qui est énuméré ci-dessus.

2.2 Les composants d'une PKI

L'infrastructure à clé publique est construite autour d'un ensemble de composants et de procédures de gestion des paires de clés publiques et privées.

Une PKI typique comprend les fonctions suivantes. Ceux-ci peuvent être remplis par une procédure ou un composant technologique et, dans certains cas, par un mélange des deux.

— Autorité de certification (CA) : émet le certificat d'une entité et agit comme un composant de confiance au sein d'une PKI privée. Tout certificat émis par l'autorité de certification est approuvé par toutes les entités qui font confiance à l'autorité de certification. Le rôle exact d'une autorité de certification dépendra de sa position au sein d'une hiérarchie de l'autorité de certification .**[W2]**

— Certificat : Un document numérique, signé par une autorité de certification, et utilisé pour prouver le propriétaire d'une clé publique, dans une PKI. Le certificat a un certain nombre d'attributs, tels que l'utilisation de la clé, l'authentification du client, l'authentification du serveur ou la signature numérique et la clé publique. Le certificat contient également le nom du sujet qui est une information identifiant le propriétaire. Cela peut être, par exemple, un nom DNS ou une adresse IP.

— Autorité d'enregistrement (RA) : Reçoit les demandes de signature de certificat et vérifie l'identité d'une entité finale. L'AE approuvera une demande avant que le certificat ne puisse être émis par l'AC. Il s'agit d'une étape très importante du processus et elle implique souvent une procédure d'inscription des entités finales dans l'ICP.

— Autorité de validation (VA) : Une VA permet à une entité de vérifier qu'un certificat n'a pas été révoqué. Le rôle d'AV est souvent effectué par une installation en ligne hébergée par une organisation qui gère l'ICP. Une autorité de validation utilisera souvent OCSP ou CRL pour annoncer les certificats révoqués.

— Stockage sécurisé : Une méthode de stockage sécurisé d'une clé privée est requise à la fois pour l'autorité de certification (CA) et l'entité finale, afin de protéger la clé contre toute compromission.

— Paire de clés publique / privée - Une clé privée et la clé publique associée sont mathématiquement liées l'une à l'autre. La clé publique peut être largement partagée. La clé privée prouve la propriété de l'identité et doit être gardée secrète.

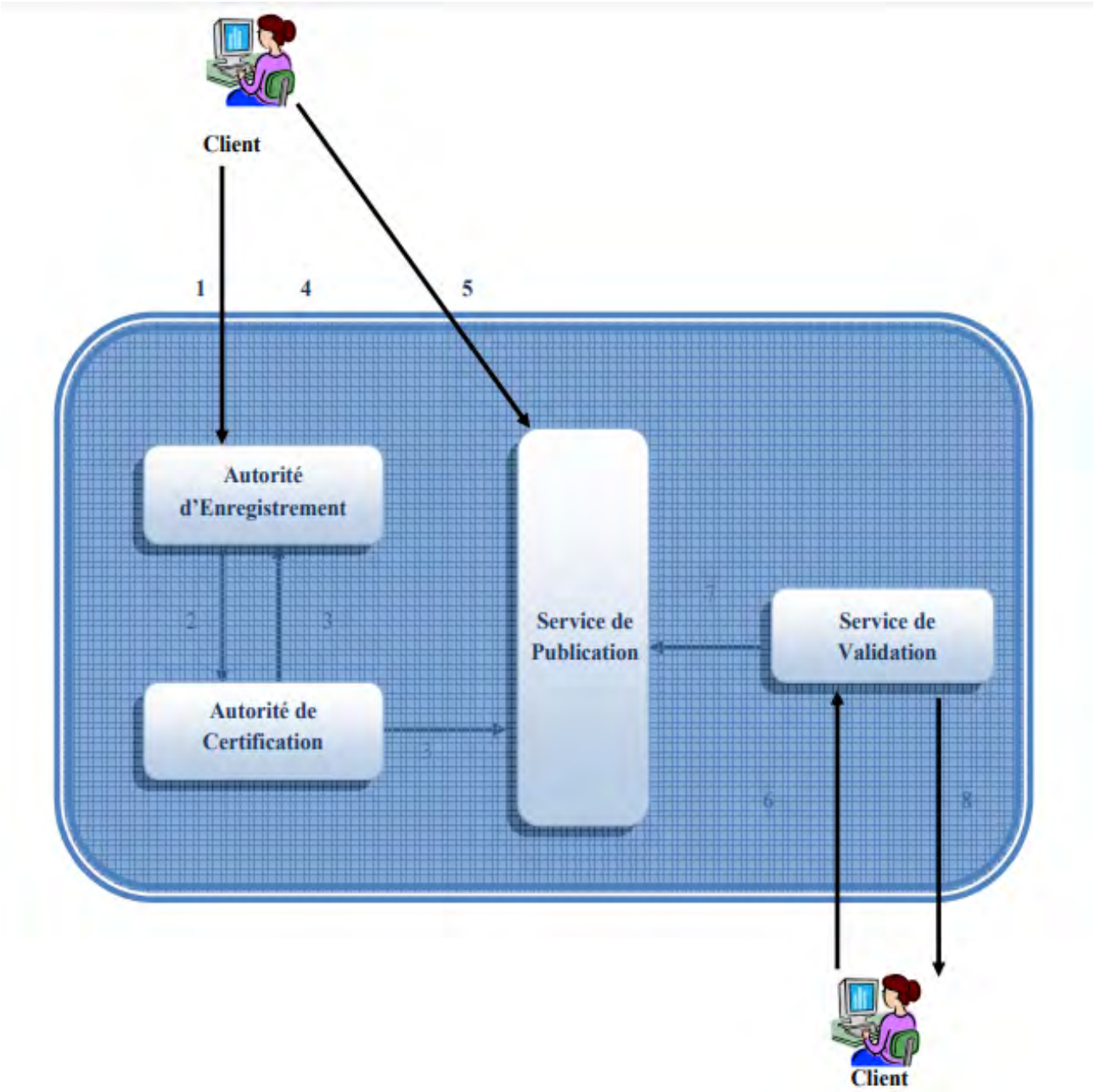

Figure 9 – Composants et principe de fonctionnement des PKIS

1. L'utilisateur fait sa demande à l'autorité d'enregistrement
2. L'autorité d'enregistrement vérifie les données d'identification, la possession de

la clé privée et valide la requête qui est transférée à l'autorité de certification

3. L'autorité de certification vérifie la validité de la requête et génère le certificat. Le certificat est publié dans l'annuaire et transmis à L'autorité d'enregistrement
4. L'autorité d'enregistrement avertit l'utilisateur que son certificat est disponible
5. L'utilisateur récupère le certificat dans l'annuaire
6. L'utilisateur envoie au répondeur OCSP une requête pour vérifier l'état du certificat.
7. Le répondeur OCSP récupère la liste des certificats révoqués à partir du service de publication
8. Le répondeur OCSP envoie la réponse à l'utilisateur.

Il existe d'autres composantes non mentionnées dans les documents de l'IETF, mais qui peuvent être nécessaires dans certains cas :

— **Autorité de certification ;**
— **Annuaire de certificats ;**
— **Autorité Système de révocation de certificats ;**
— **Système de sauvegarde et de récupération de clefs ;**
— **Autorité Soutien à la non-répudiation ;**
— **Mise à jour automatique des clefs ;**
— **Autorité Gestion de l'historique des clefs ;**
— **Horodatage ;**
— **Logiciel client interagissant de manière fiable et continue avec tout ce qui est énuméré ci-dessus.**

2.3 Répartition des AC

les autorités de certifications fonctionnent par une chaîne de confiance. Quelles seraient donc les conséquences si une chaîne venait à se briser.

Toutes les autorités de certifications certifiées par l'autorité de certification supérieure seront donc remises en cause car elles n'auraient plus aucun moyen de prouver ses certificats car la communication entre elles serait brisée (figure 1).

Pour parer à ce problème, il existe plusieurs modèles pour structurer les autorités de certifications :[**W8**]

2.3.1 Modèle hiérarchique

Modèle hiérarchique : Les autorités CA1 et CA2 ont soumis leurs clefs publiques à un CARoot qui leur a généré un certificat. L'autorité CARoot peut être défini comme le plus haut niveau d'autorité. C'est le seul composant qui ait un certificat auto-signé.

Un certificat auto-signé est le seul certificat qui permette d'assurer l'intégrité et non l'authenticité, d'où la chaîne de confiance. Par conséquence, CA1 et CA2 deviennent des CA subordonnées de CARoot .

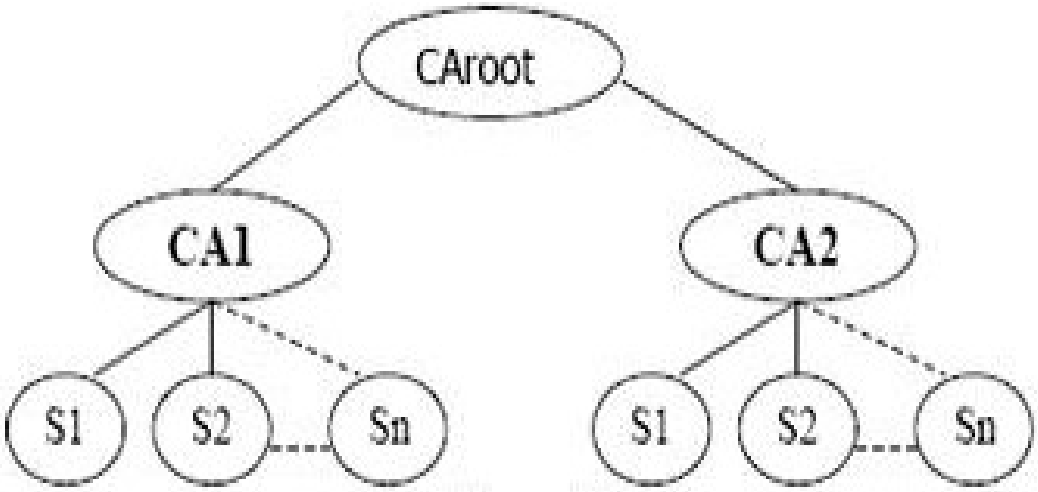

Figure 10 – Modele hierarchique

2.3.2 Modèle croisé (Peer-to-Peer)

Modèle Peer-to-Peer : Le modèle hiérarchique ne règle pas notre problème, c'est pourquoi, il existe le modèle Peer-to-Peer qui permet que différentes autorités de certification soient au même niveau. Si des autorités de certifications sont au même niveau, les certificats qu'elles génèrent sont co-signé, autrement dit, que CA1 peut signer des certificats pour CA2 et vice-versa. Ils sont responsables mutuellement des certificats de leur homologue (figure 3).

Le problème de ce modèle est que toutes les autorités de certifications de même niveau doivent s'échanger leur clef publique pour pouvoir générer des certificats pour leur homologue, de ce fait, plus il y a d'autorités de certification, plus il y aura d'échange de clef publique (pour N autorités de certification il faut générer N^2-N/2 certificats pour certifier toutes les autorités).

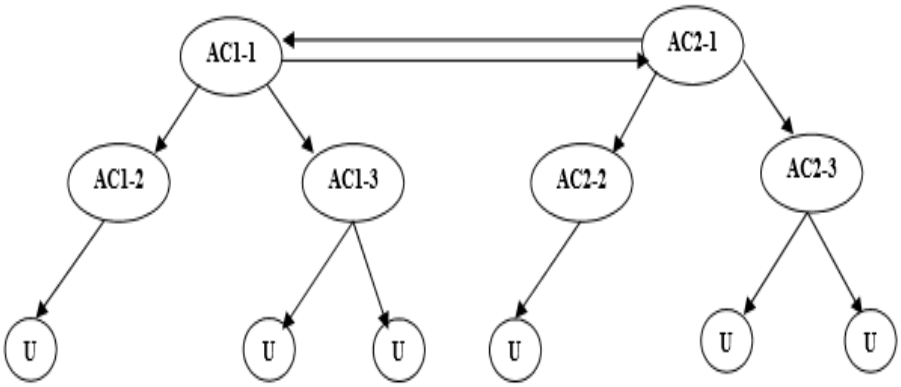

Figure 11 – Modèle Croisé(Peer-to-Peer)

2.3.3 Modèle Bridge

Modèle Bridge : Le modèle en pont ou Bridge est une alternative aux deux autres modèles. En effet, le modèle hiérarchique ne permet pas d'avoir une structure stable et le modèle Peer-to-Peer nécessite un nombre important d'échange entre les autorités. Le modèle en pont ressemble fortement au modèle Peer-to-Peer sauf qu'il permet de limiter les échanges entres 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 .

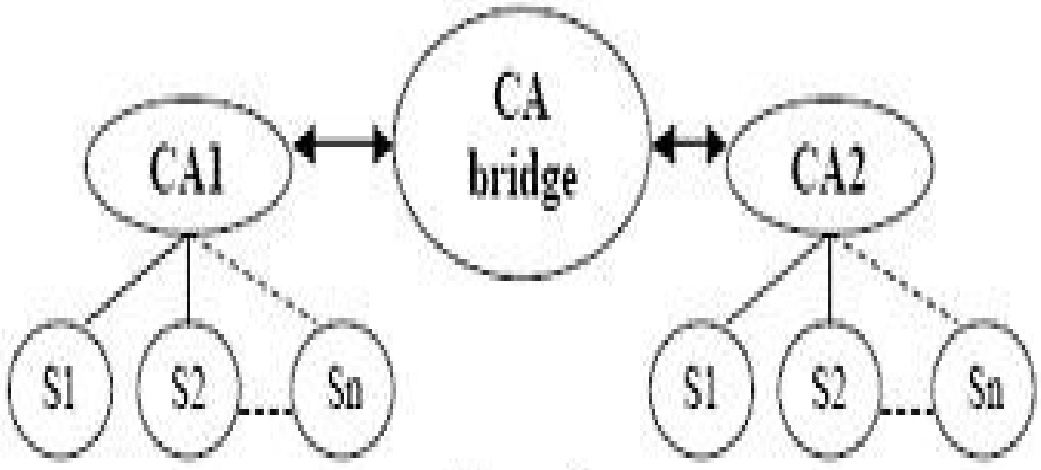

Figure 12 – Modele bridge

2.4 Cycle de vie des clés et des certificats

Sans une gestion de leur cycle de vie, les certificats peuvent se perdre, expirer et entraîner toutes sortes de perturbations imprévues. Les certificats constituent le socle de la sécurité réseau et jouent un rôle clé sur la confiance en ligne et sur les réseaux internes. Il semblerait par conséquent logique de les gérer efficacement, non ?

Pour une bonne gestion de l'ensemble de vos certificats et de leur cycle de vie, le mieux est d'éviter les contrôles manuels. L'utilisation d'un service de gestion du cycle de vie des certificats permet aux administrateurs de surveiller en continu leurs systèmes et certificats numériques, et de pouvoir lancer des audits permettant d'anticiper les expirations et les renouvellements afin d'éviter toute interruption de service.

De nombreuses entreprises font aujourd'hui appel aux fournisseurs de solutions d'infrastructures à clés publiques (PKI) leaders pour gérer leurs certificats tout au long de leur cycle de vie.

2.5 La politique d'une PKI

La politique d'une PKI se définit à deux niveaux :

— **La politique de certification** :

Une politique de certification est un ensemble de règles, qui fournit un renseignement sur la possibilité d'utiliser un certificat pour une communauté particulière ou des applications ayant des besoins de sécurité communs. Elle spécifie entre autre les conditions et les caractéristiques de délivrance du certificat. Dans le cas général, un certificat est utilisable par n'importe quelle application pour autant que ces conditions et ces caractéristiques sont jugées satisfaisantes. Cependant, une politique de certification peut éventuellement restreindre l'usage du certificat à un ensemble données d'applications, voir même à une seule application.

— **La politique de sécurité** :

La politique de sécurité est la partie juridique de la PKI. En effet, lorsqu'on met en place une PKI, il faut fournir trois documents :

Rapport pratique de certification : qui spécifie les critères de certification et la politique de révocation des certificats,

Politique du certificat : qui explique et limite l'utilisation du certificat numérique,

Considérations légales : qui permet de responsabiliser les utilisateurs en cas de perte ou de fraude à l'intérieur même de la PKI.

2.6 Les protocoles d'une PKI

Dans cette partie, nous allons décrire les principaux protocoles supportés par les différentes composantes d'une PKI. Ces protocoles permettent aux utilisateurs de faire appel aux différents services offerts par la PKI.

2.6.1 CRL

Une liste de révocation de certificats (CRL) est une liste de certificats numériques qui ont été révoqués par l' autorité de certification (CA) émettrice avant leur date d'expiration prévue et qui ne devraient plus être approuvés. Les CRL sont un type de liste noire et sont utilisées par divers points de terminaison, y compris les navigateurs Web , pour vérifier si un certificat est valide et digne de confiance. Un certificat est révoqué de manière irréversible si, par exemple, il est découvert que l'autorité de certification (CA) a émis un certificat de manière incorrecte, ou si une clé privée est supposée avoir été compromise. Les certificats peuvent également être révoqués en cas de non-respect par l'entité identifiée des exigences de la politique, telles que la publication de faux documents, la fausse déclaration du comportement du logiciel ou la violation de toute autre politique spécifiée par l'opérateur CA ou son client. La raison la plus courante de révocation est que l'utilisateur n'est plus en possession exclusive de la clé privée (par exemple, le jeton contenant la clé privée a été perdu ou volé).

Un protocole permet d'interroger ces listes en temps réel, OCSP (Online Certificate Status Protocol). Il est déjà standardisé et implémenté dans certains produits. » .

2.6.2 OCSP

Online Certificate Status Protocol (OCSP, en français « protocole de vérification de certificat en ligne ») est un protocole Internet utilisé pour valider un certificat numérique X.509. OCSP est standardisé par l'IETF dans la RFC 69601.

Ce protocole est une alternative réglant certains des problèmes posés par les listes de révocation de certificats (CRL) dans une infrastructure à clés publiques (PKI). Les messages OCSP sont codés en ASN.1 et peuvent être transportés par différents

protocoles applicatifs (SMTP, LDAP, HTTP, etc.). Les communications OCSP étant de la forme « requête/réponse », les serveurs OCSP sont appelés répondeurs OCSP.

— **Avantage par rapport aux CRL :** Plusieurs raisons peuvent amener à préférer le protocole OCSP aux traditionnelles CRL :

OCSP fournit des informations sur le statut du certificat plus à jour ;

avec OCSP, le client n'a plus besoin de récupérer lui-même la CRL. Vu la taille parfois importante de cette CRL, cela allège le trafic réseau ;

le client n'a plus à traiter lui-même la CRL. Cela permet l'économie d'un traitement relativement complexe ; le répondeur OCSP permet de proposer des mécanismes de facturation au vendeur, et non pas à l'acheteur ;

les CRL peuvent être comparées à une « liste de mauvais clients » d'une banque. Cela constitue une fuite d'information non souhaitable.

— **Composition d'une requête OCSP :** Les communications OCSP sont de la forme « requête/réponse » et les serveurs OCSP sont appelés répondeurs OCSP. Dans le protocole OCSP, le serveur demande l'état d'un ou de plusieurs certificats à la fois, au répondeur OCSP. Ce dernier vérifie l'état du certificat demandé et retourne une réponse à l'entité de fin.

Définie dans la RFC 2560, une requête OCSP se compose des éléments suivants :

une version du protocole ;

une demande de service ;

certaines informations sur le certificat cible.

des extensions optionnelles qui peuvent être traités par le répondeur OCSP.

La figure suivante illustre comment la requête OCSP est formée et envoyée vers le serveur OCSP.

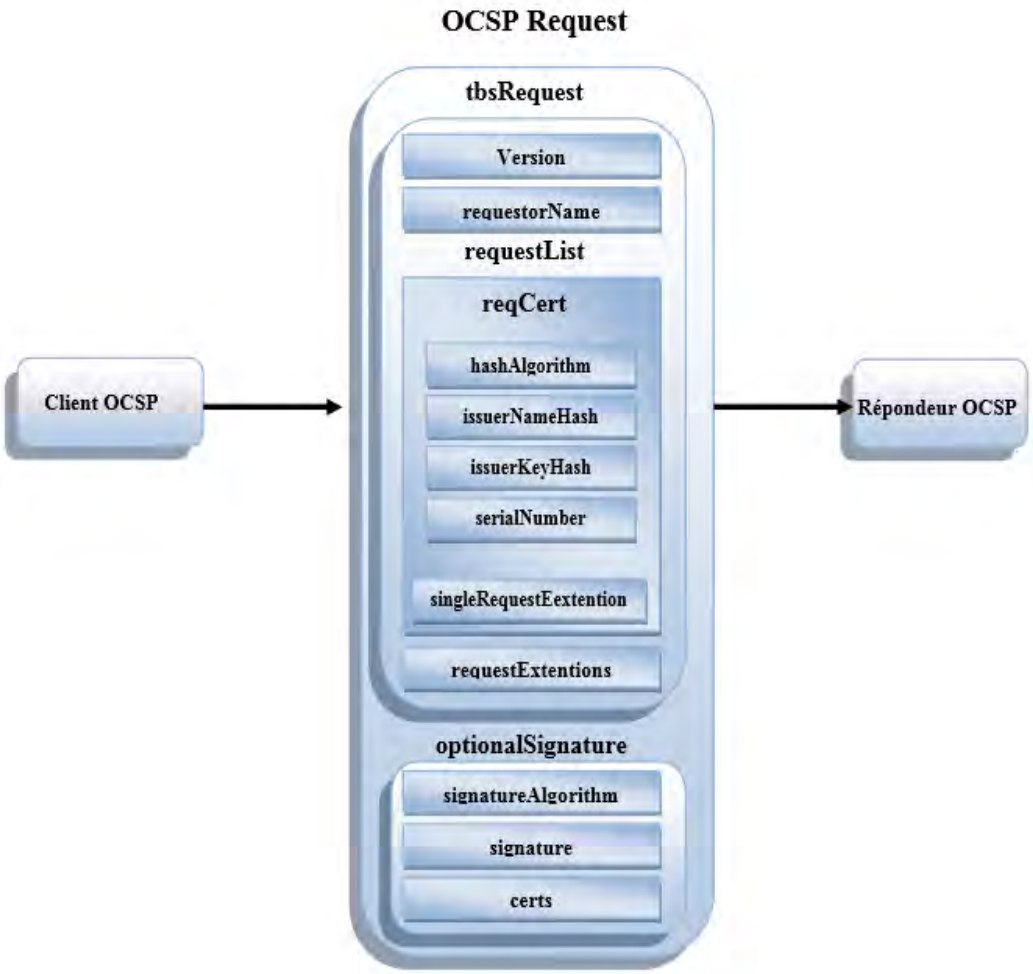

Figure 13 – Composition d'une requête OCSP

À la réception de cette requête, le répondeur OCSP vérifie si :

le message est bien formé ;

il est configuré pour fournir le service demandé ;

la requête contient les informations requises pour être traitée.

Si l'une des trois conditions précédentes n'est pas respectée, le répondeur OCSP produit un message d'erreur, sinon il renvoie une réponse définitive.

Les réponses OCSP peuvent être de divers types :

Bon (good) : cela veut dire que la réponse à la requête émit par le serveur est positive et que le certificat est valide (n'est pas révoqué).

Révoqué (revoked) : cela veut dire que le certificat sollicité n'est plus valide, c'est-àdire qu'il est révoqué temporairement ou définitivement.

Inconnu (unknown) : cela veut dire que le répondeur OCSP n'a pas trouvé d'information sur le certificat demandé.

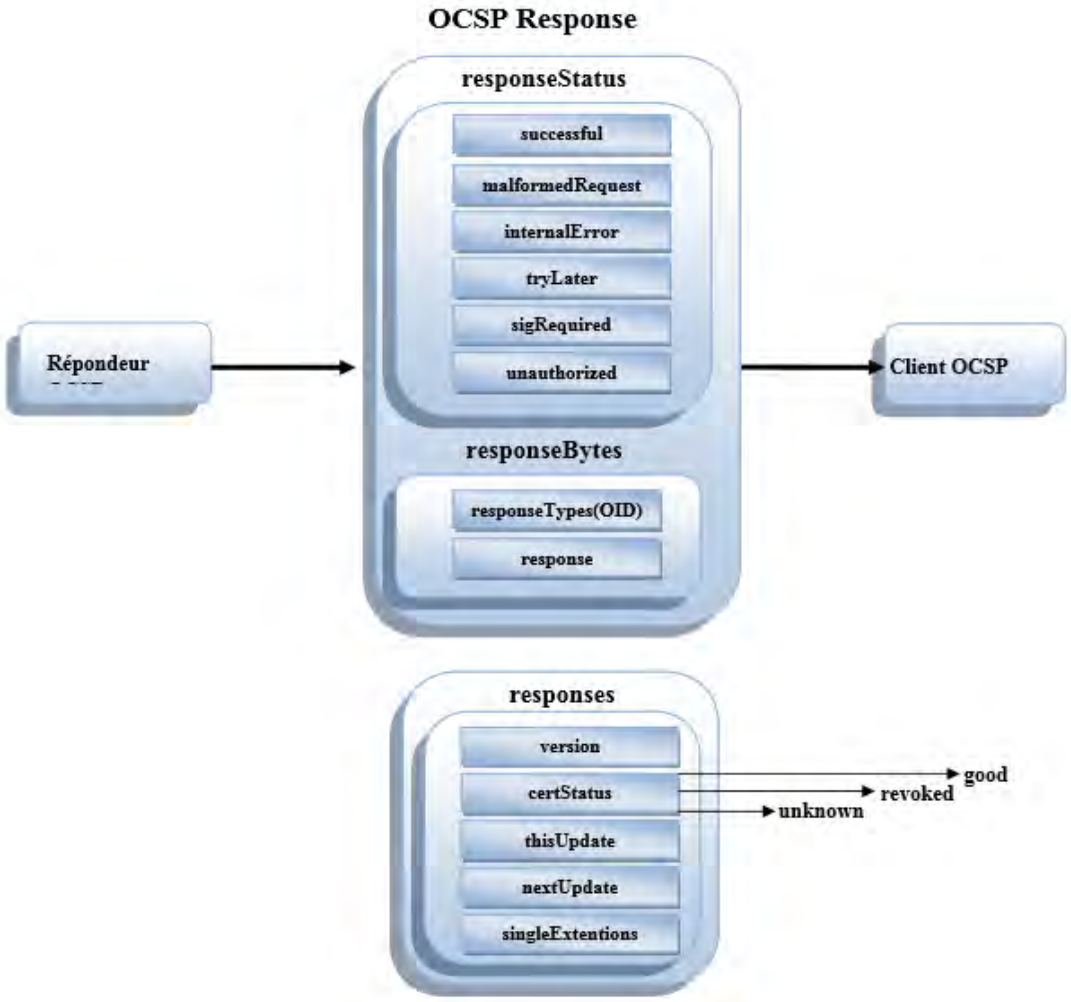

Figure 14 – Composition d'une réponse OCSP

— **Délégation d'Autorité de Signature OCSP** La clé qui signe l'information d'état d'un certificat et la clé qui a signé le certificat ne doit pas être la même. L'émetteur du certificat délègue explicitement son autorité de signature au répondeur OCSP. L'émetteur publie un certificat contenant une valeur unique «extendKeyUsage» dans la signature des certificats OCSP. Ce certificat doit être délivré directement au répondeur par l'AC informée [RFC 2560].

2.6.3 CMP

Le certificat de gestion de protocole (CMP) est un protocole Internet utilisé pour l'obtention des certificats numériques X.509 dans une infrastructure de gestion de clés.

Il est décrit dans [RFC 4210] en développant un protocole compréhensible supportant une grande variété de modèles. Le protocole CMP permet aux utilisateurs d'une PKI de réaliser à distance certaines opérations de gestion des certificats à clé publique :

— s'enregistrer auprès de la PKI et recevoir son certificat ;
— recouvrer ses clés ;
— effectuer la mise à jour de ses clés ;
— renouveler son certificat ;
— effectuer une demande de révocation.

2.7 Annuaire

2.7.1 Définition

Les certificats émis par une ICP doivent être rendus publiques afin que les différents partenaires qui les utilisent puissent s'échanger leur clé publique. Pour cela, les certificats sont publiés dans un annuaire d'accès libre.

Cet annuaire peut également contenir le certificat de l'AC et les CRLs. Des annuaires LDAP sont généralement utilisés pour cette fonction.

Il constitue en quelque sorte une base de données centrale accessible en mode de lecture, en mode d'ajout (nouveau certificat) et en mode de suppression (révocation d'un certificat). Il contient également une liste de révocation de certificats(CRL) qui comporte la liste de l'ensemble des certificats révoqués depuis la création de l'annuaire, datés et signés par les autorités de certification.

2.7.2 Annuaire et PKI

L'annuaire est indépendant de la PKI cependant la PKI en a besoin. Les seules contraintes de l'annuaire sont qu'il doit accepter le protocole X.509 pour le stockage des certificats révoqués et le protocole LDAP .

Son rôle est comme dit précédemment de stocker les certificats révoqués et par la même occasion, les certificats en cours de validité afin d'avoir un accès rapide à ces certificats. De plus, l'annuaire peut stocker les clefs privées des utilisateurs dans le cadre du recouvrement de clef. Sachant que les certificats sont largement distribués, l'annuaire est une solution pour les mettre à disposition.

2.7.3 Protocole d'accès au répertoire

Pour comprendre mieux le service d'annuaire, il est nécessaire de bien connaître les bases sur les protocoles d'accès à l'annuaire que sont X .500 et LDAP.

1. X.500, Dans le cadre de l'authentification avec les annuaires, la norme X.509 fait partie du standard OSI X.500 pour les annuaires. Il définit le modèle des données d'un certificat (c'est-à-dire les attributs userCertificate, caCertificate, crossCertificatePair, certificateRevocationList...). Il définit des mécanismes pour l'authentification. Le certificat inclut le DN de l'utilisateur et le DN du CA qui a signé le certificat. Les évolution de la norme X.509 pour satisfaire les exigences de PKIX sont les suivantes : X.509v3(1997)

   Nouveau mécanisme d'extension

   Extensions prédéfinies :

   Des informations sur les clés : ID, utilisation...

   Des informations de politique : certificate policy,...

   Des extensions sur l'utilisateur et la CA : nom alternatif,...

   Des contraintes de chemin de certification X.509v4(2000)

   Vérification des chaînes de certificats avec des CAs de différents domaines et hiérarchies.

   Amélioration dans le domaine des révocations de certificat

   Nouvelles caractéristiques dans les certificats en attribut

   Définition de l'usage des certificats en attribut pour le contrôle d'accès et l'autorisation d'accès

2. LDAP (Lightweight Directory Access Protocol) Lightweight Directory Access Protocol (LDAP) est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire (il est une évolution du protocole DAP). Ce protocole repose sur TCP/IP. Il a cependant évolué pour représenter une norme pour les systèmes d'annuaires, incluant un modèle de données, un modèle de nommage, un modèle fonctionnel basé sur le protocole LDAP, un modèle de sécurité et un modèle de réplication. C'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs. LDAP est moins complexe que le modèle X.500 édicté par l'UIT-T.

LDAP a été initialement conçu pour accéder de manière légère aux annuaires X.500. Ces annuaires étaient traditionnellement interrogés à travers le protocole X.500 Directory Access Protocol (DAP) qui nécessitait l'utilisation de la pile de protocoles du modèle OSI. L'utilisation d'une passerelle LDAP/DAP permettait d'accéder à un serveur DAP en étant sur un réseau TCP/IP. Ce modèle d'annuaire est dérivé de DIXIE et de Directory Assistance Service. Plus précisément, la structure d'un annuaire est comme suit :

Un annuaire est un arbre d'entrée.

Une entrée est constituée d'un ensemble d'attributs.

Un attribut possède un nom, un type et une ou plusieurs valeurs.

Les attributs sont définis dans des schémas. Le fait que les attributs puissent être multivalués est une différence majeure entre les annuaires LDAP et les SGBDR. De plus, si un attribut n'a pas de valeur, il est purement et simplement absent de l'entrée.

Chaque entrée a un identifiant unique, le Distinguished Name (DN). Il est constitué à partir de son Relative Distinguished Name (RDN) suivi du DN de son parent. C'est une définition récursive. On peut faire l'analogie avec une autre structure arborescente, les systèmes de fichiers ; le DN étant le chemin absolu et le RDN le chemin relatif à un répertoire. En règle générale le RDN d'une entrée représentant une personne est l'attribut uid.

La communication LDAP s'appuie sur le protocole TCP, et de manière optionnelle sur TLS

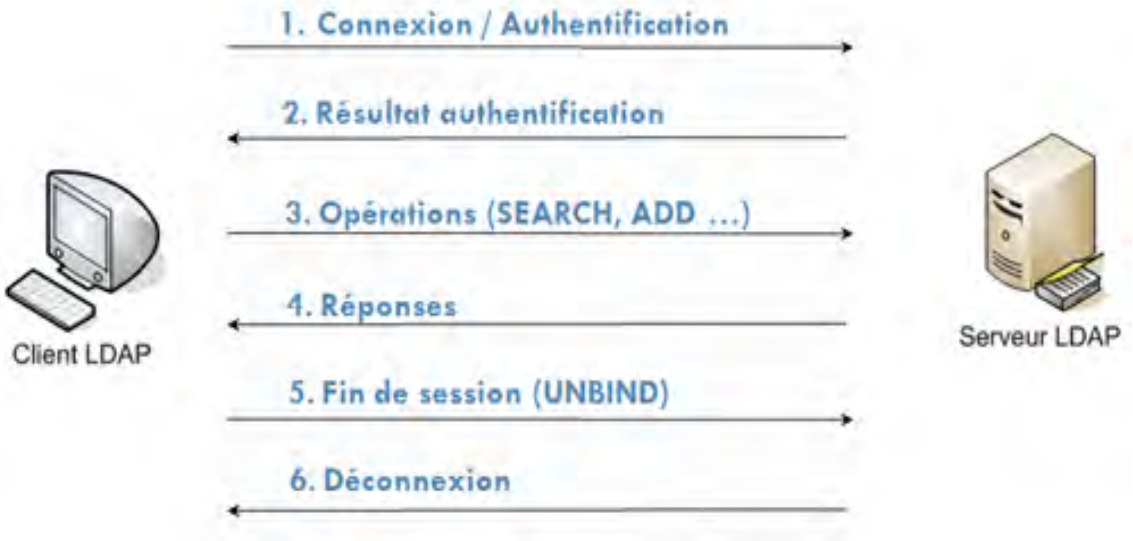

Figure 15 – Fonctionnement du protocole LDAP

Conclusion :

Nous avons vu qu'une infrastructure de gestion de clés publiques se construit, c'est donc une structure à la fois technique et administrative. Le domaine des PKI est intéressant : il est possible de les utiliser pour diverses applications telles que le mail chiffré, le web sécurisé, le commerce électronique ... Comme les PKI intègrent la cryptographie à clé publique et certificat numérique, elles peuvent se confier à des tierces parties de confiance et échanger des données en toute sécurité. Il existe plusieurs solutions ou produits qui implémentent une PKI et qui offrent la possibilité de sécuriser les données. Le chapitre suivant sera consacré à la mise en place de l'un de ces produits.