Chapitre II. Principes généraux de la cryptographie

Auteur: Omar.cheikhrouhou@isetsf.rnu.tn

Dans ce chapitre, nous allons passé un bref aperçu sur les principes de base de la cryptographie (cryptographie à clé secrète et à clé publique), ainsi que les différents services de sécurité que procure la cryptographie. Nous allons définir ensuite les certifictas numériques, et les Infrastructures de gestion de clés où PKI, qui établissent un environnement sûre dans le quel sont utilisés les certificats. On va décrire les différents composants d'une PKI, ainsi que la structure d'un certificat conforme au standard X.509. On cloturera ce chapitre par la gestion en cours des certificats numérique, en l'occurence, la révocation, le renouvellement et la mise à jour.

I.1 Définition des principes de base en sécurité

Il existe quatre principaux services de sécurité [5,4] :
Authentification : c'est l'assurance de l'identité d'un objet, généralement une personne, mais cela peut aussi s'appliquer à un serveur, une application (applet Java), etc.
Intégrité : l'intégrité d'un objet (document, fichier, message, ...) est la garantie que cet objet n'a pas été modifié par une autre personne que son auteur.
Confidentialité : c'est l'assurance qu'un document ne sera pas lu par un tiers qui n'en a pas le droit.
Non répudiation : le but est que l'émetteur d'un message ne puisse pas nier l'avoir envoyé et le récepteur l'avoir reçu. Les transactions commerciales (e-commerce et autres) ont absolument besoin de cette fonction.

Ces besoins ont toujours existé pour les documents papiers, mais le fait de les utiliser pour des documents électroniques, rend la situation plus délicate. Ces données circulent en clair sur les réseaux informatiques. Or il est techniquement possible, pour une personne mal intentionnée vis à vis d'une autre personne, d'accéder aux communications Internet ou Intranet, ... Si des protections n'ont pas été prévues et certaines précautions prises, ces attaques sont même simples à réaliser.

I.2 Mécanismes de chiffrement, empreinte, signature

Dans ce qui suit, nous expliquons les mécanismes permettant de réaliser les fonctions de sécurité décrites ci-dessus.

Chiffrement :
Pour assurer la confidentialité d'un document électronique, on chiffre le document ; c'est-à-dire, on lui applique une fonction mathématique ayant comme paramètre une clé de chiffrement (K1). Une clé de chiffrement est une suite de bits de différentes tailles (40 bits, 56 bits, etc.).
Une fois le texte chiffré, il n'est interprétable que par les détenteurs de la clé de déchiffrement (K2) correspondante.

Si K1 = K2, on parle de chiffrement symétrique (Figure.1).

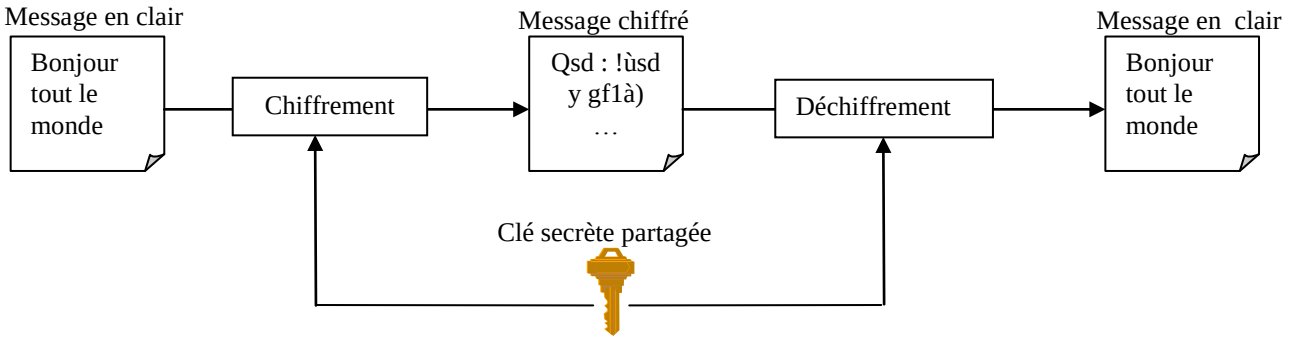

Figure.1 Chiffrement symétrique

Sinon, on parle de chiffrement asymétrique (Figure.2) ou de chiffrement à clé publique. Dans ce cas, chaque utilisateur possède une paire de clés privée/publique, telle que la clé privée est connue uniquement par son

propriétaire tandis que la clé publique peut être publiquement connue. La clé publique est dérivée de la clé privée, mais il est mathématiquement impossible de faire l'opération inverse. Chaque message chiffré par une clé ne peut être déchiffré que par l'autre clé.

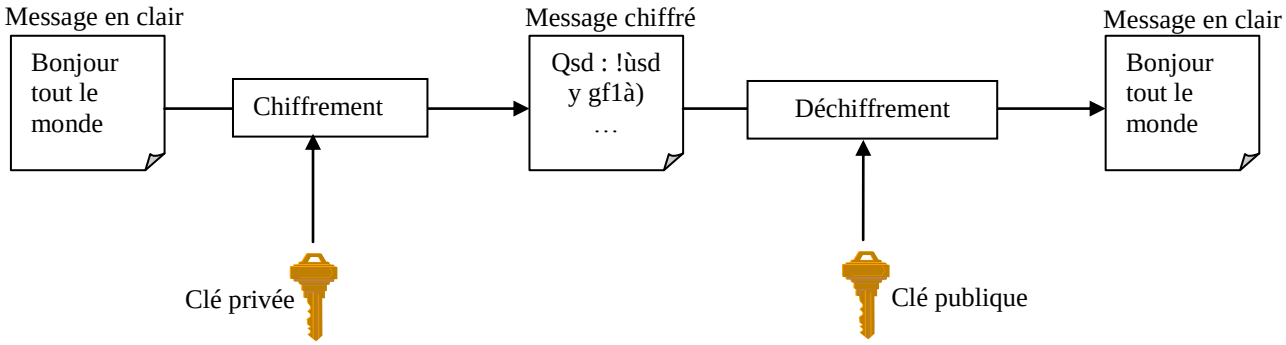

Figure.2 Chiffrement asymétrique

Signature électronique :

La signature électronique est l'un des mécanismes qui permet d'assurer les fonctions d'authentification, d'intégrité et de non répudiation.

Pour générer une signature numérique (Figure.3), il faut dans un premier temps utiliser une fonction de hachage. C'est une fonction mathématique qui, à partir d'un texte de n'importe quelle longueur , génère un nombre de taille fixe bien inférieur à la taille du texte. Ce nombre est appelé condensé ou empreinte. *MD5* (*Message Digest*) est une fonction de hachage très répandue, qui calcule une empreinte sur 128 bits.

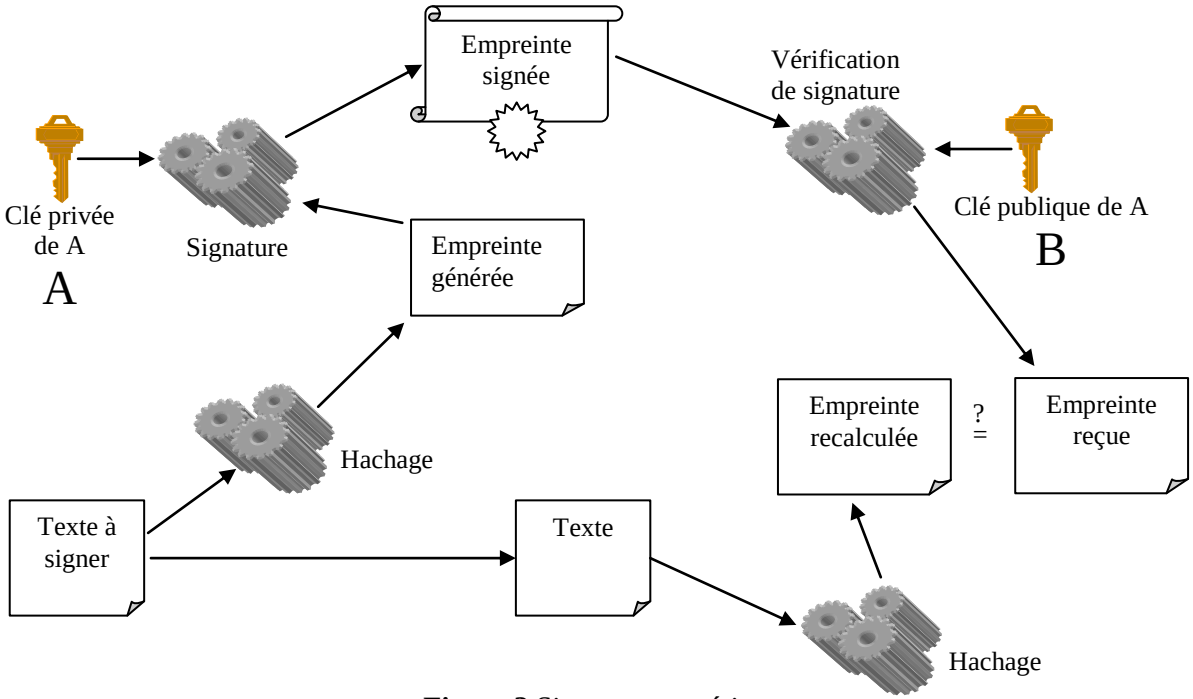

Figure.3 Signature numérique

Avant d'envoyer le message, l'outil logiciel émetteur calcule l'empreinte du message, puis chiffre cette empreinte avec sa clé privée (chiffrement asymétrique). Le résultat obtenu est appelé signature numérique. Avant l'envoi, cette signature est ajoutée au message (concaténation), qui devient un message signé.

Le logiciel du destinataire qui reçoit l'ensemble déchiffre cette empreinte avec la clé publique de l'émetteur. Puis il recalcule localement l'empreinte du message reçu à l'aide de la même fonction de hachage et compare

le résultat avec l'empreinte déchiffrée (Figure.3). Si les deux sont égales, cela veut dire que le message n'a pas été modifié durant le transfert et que l'émetteur de ce message est authentifié. Du même coup, l'émetteur

ne peut nier l'envoi du message vu qu'il est le seul détenteur de la clé privée ayant servi à signer le message.
La signature numérique possède plusieurs propriétés rendant son utilisation incontournable [9] :

- Une signature ne peut être falsifiée.
- Une signature donnée n'est pas réutilisable pour un autre document.
- La modification d'un document signé altère la signature de ce document.
- Une signature ne peut être niée.

A travers ce qui précède on a pu voir l'utilisation de la cryptographie pour mettre en œuvre différents services de sécurité. Cependant l'utilisation des clés de chiffrement, et en l'occurrence la paire de clés publique/privée pose quelques problèmes [9] :

- La protection des clés privées.
- La garantie quant à l'appartenance d'une clé publique à une entité.
- La publication des clés publiques pour qu'elles puissent être facilement accessibles.

La validité d'une clé publique, etc.

I.3 Certificats électroniques

Nous avons décrit les mécanismes qui permettent d'assurer les fonctions de base de sécurité avec le couple de clés privée/publique, mais il y a une lacune dans le raisonnement précédent. On a considéré qu'un utilisateur connaissait la clé publique d'une personne simplement en consultant un serveur web ou un serveur *LDAP* (***L**ightweight **D**irectory **A**ccess **P**rotocol*)... et qu'il considérait cette clé publique comme valide.

Qu'est ce qui garantit que la clé publique de X qu'un utilisateur Y a récupéré est correcte ? Une personne P1 pourrait publier une clé publique en faisant croire qu'elle appartient à une autre personne P2.

Il a donc fallu créer un mécanisme supplémentaire, le ‘certificat électronique’, pour assurer la validité de la clé publique.

Un certificat est un document électronique, résultat d'un traitement fixant les relations qui existent entre une clef publique, son propriétaire (une personne, une machine, une application) et l'application pour laquelle il est émis :

- pour une personne, il prouve l'identité de la personne.
- pour une application, il assure que celle-ci n'a pas été détournée de ses fonctions.
- pour un site, il offre la garantie lors d'un accès vers celui-ci que l'on est bien sur le site auquel on veut accéder.

I.4 Infrastructure de Gestion de Clés

Comme il existe un circuit de procédures et de vérifications, des personnes habilitées, ... pour délivrer des carte d'identité, il faut mettre l'équivalent en place pour les certificats. Il faut ainsi décider qui va recueillir et vérifier les informations données par une personne lorsqu'elle va demander un certificat, qui va créer le certificat, qui va le lui délivrer, pour quelle durée, où va-t-il être stocké, où va-t-on pouvoir récupérer les certificats d'autres personnes, comment retirer un certificat suite à son expiration ou à sa compromision, ... Il faut définir ce que l'on appelle une architecture de gestion des certificats. IGC (Infrastructure de Gestion de clés) ou *PKI* (*Public Key Infrastructure*) sont les deux sigles les plus connus pour la désigner.

«Une IGC offre un environnement de confiance, ainsi qu'un ensemble de garanties relatif aux certificats de clés publiques» .

Les normes internationales décrivent les différents éléments fonctionnels d'une IGC. En simplifiant, l'architecture est constituée de :

- Objets :
  - Bi-clés (clé privée/clé publique), certificats
- Eléments :

- Autorité de certification,

- Autorité d'enregistrement,
- Système de publication/distribution de certificats (annuaire),
- Applications compatibles avec la *PKI*.

Bi-clés :
Couple composé d'une clé privée et d'une clé publique correspondante, permettant la mise en oeuvre d'algorithme de chiffrement asymétrique.
On distingue classiquement quatre bi-clés:

- Bi-clés de confidentialité
  Utilisées pour chiffrer des messages de petites tailles.

- Bi-clés de signature
  La clé privée est utilisée pour signer des messages.
  La clé publique est utilisée pour vérifier les signatures.

- Bi-clés de certification
  Utilisées par l'autorité de certification pour signer des certificats ou des messages de révocation.

- Bi-clés d'échange/transport de clés
  Permet le transport des clés symétriques utilisées pour sécuriser les communications.

I.4.1 **Autorité d'Enregistrement** (AE)

L'AE vérifie l'identité du demandeur de certificat, s'assure que celui-ci possède bien un couple de clés privée/publique (on suppose que c'est l'utilisateur qui les crée) et récupère la clé publique du demandeur. Elle transmet ensuite cette information (information d'identité du demandeur ainsi que sa clé publique) à l'autorité de certification.

La transmission des demandes doit se faire de manière sécurisée, personne ne doit pouvoir modifier la demande durant le transport par exemple. Pour ce faire, l'autorité d'enregistrement ainsi que l'autorité de certification ont des certificats et utilisent les mécanismes d'authentification, d'intégrité et de confidentialité pour communiquer entre eux.

I.4.2 **Autorité de Certification** (AC)

Comme vu précédemment, un certificat électronique est délivré par une autorité de certification. Une Autorité de Certification (ou AC) est un organisme qui délivre des certificats électroniques. Une AC possède aussi son propre certificat qui peut être soit un certificat autosigné (créé par elle-même) ou créé par une autre autorité de certification . L'AC utilise sa clé privée pour signer les certificats qu'elle délivre.

En délivrant un certificat, l'AC se portera garante de l'identité de l'entité (personne, application, serveur, etc.) possédant le certificat (le propriétaire). Donc l'AC joue le rôle d'un tiers partie de confiance par rapport aux différentes entités utilisant les certificats.

La confiance que l'on accordera à un certificat va dépendre du sérieux de l'autorité qui l'aura délivré. Si une AC n'est pas 'reconnue' comme digne de confiance, les utilisateurs se verront peut être dans l'obligation de rejeter les certificats délivrés par cette AC. Une AC *reconnue* est n'importe quelle autorité de certification dont le ou les certificats Root CA sont contenus (préconfigurés) dans au moins un des navigateurs web : *Internet Explorer, Opera, Mozilla* ou *Netscape* [1]. Le Root CA est l'autorité de certification racine dans la chaîne de certificats (Figure.5). Le Root CA, est l'unique AC de la hiérarchie possèdant un certificat autosigné.

I.4..3 Service de Publication

Celui-ci rend disponibles les certificats émis par l'autorité de certification. Il publie aussi la liste des certificats valides et des certificats révoqués (les certificats hors d'usage pour différentes raisons). Concrètement ce service peut être rendu possible par un annuaire *LDAP* ou un serveur Web accessible depuis Internet.

Le schéma suivant (Figure.4), récapitule les différents composants d'une IGC, ainsi que les différentes intéractions entre ces composants.

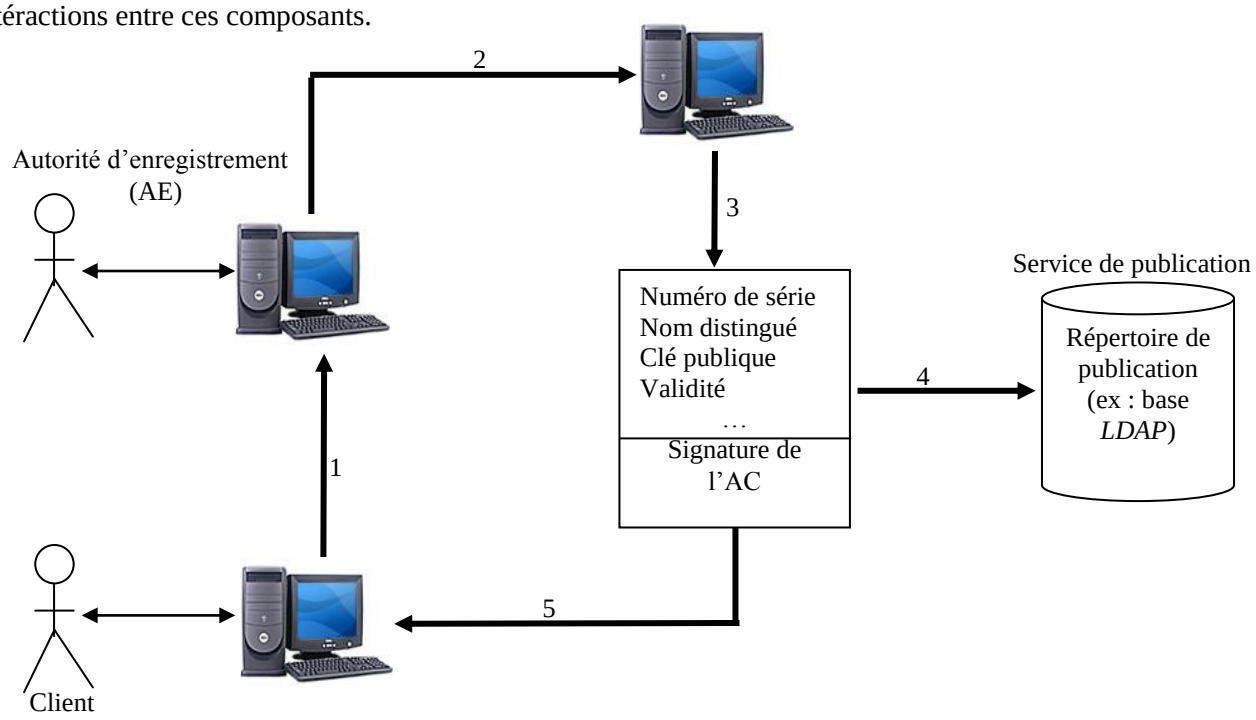

Figure.4 Principales composantes d'une PKI (IGC).

La délivrance d'un certificat utilisateur (client) passe par les étapes décrites dans la Figure.4 :
1- Demande de délivrance de certificat par le client.
2- Vérification de l'identité du client par l'AE.
3- Génération de certificat par l'AC.
4- Envoi du certificat par l'AC pour publication dans le répertoire de publication.
5- Envoi du certificat par l'AC au client.

I.4.4 Révocation de certificat

Lorsqu' une AC délivre un certificat, celui-ci contient sa date de création et une date de fin de validité . Généralement, comme de nombreuses cartes professionnelles, un certificat de personne dans une entreprise a une durée de vie fixe par défaut, un an par exemple. Mais cette durée n'est pas suffisante pour invalider un certificat dans certains cas. En effet, une personne peut quitter une entreprise ou changer de service ou se faire dérober sa clé privée. Dans ce cas il faut invalider son certificat courant.

Plusieurs méthodes de révocation et sont sécrites dans le chapitre 2.

I.5 Structure des PKIs

Il existe plusieurs structures de *PKIs*. Dans ce qui suit, nous allons décrire les structures existantes les plus connues.

I.5.1 Structure hiérarchique

Une structure hiérarchique, comme montrée à la Figure.5, est une structure dans laquelle toutes les entités (utilisateurs finaux et autres) ont confiance en une seule entité centrale : l'autorité de certification racine (AC0 dans la Figure.5).

Dans la Figure.5, AC0 représente le Root CA (AC racine), AC1 une AC intermédiare, AC 3/4/2 sont des ACs feuilles et U 1/2/3 sont des entités (utilisateur, application, serveur, etc.)

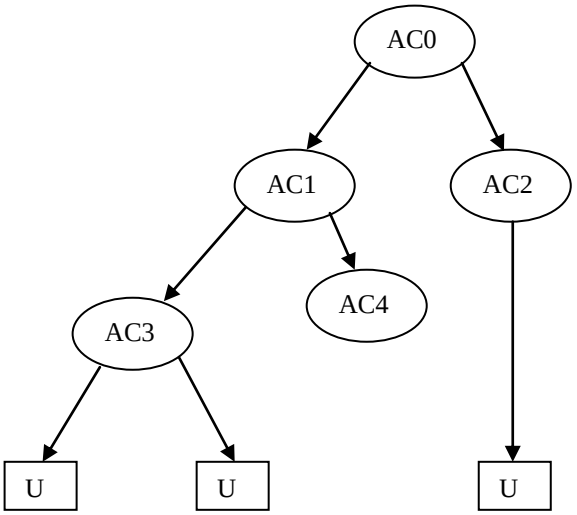

Figure.5 Certification hiérarchique à une seule racine

Chaque AC délivre des certificats aux ACs filles et éventuellement à des utilisateurs [2]. En général, les ACs feuilles délivrent uniquement des certificats à des utilisateurs. On peut ainsi établir des relations de confiance hiérarchiques [2, 9].

Cette architecture hiérarchique évite qu'une seule entité soit responsable des certificats, et donc augmente la fiabilité et réduit le risque de compromision des clés privées des ACs.

Dans la Figure.5, pour valider le certificat de U1, il faut les certificats de AC3, AC1 et AC0. On appelle cela la chaîne de certificats.

Une chaîne de certificats d'une entité X est l'ensemble des certificats des ACs contenus dans le chemin reliant le Root CA à l'entité X incluse (la généalogie du certificat de X) [2].

Dans ce schéma, la confiance accordée à une AC, est héritée par toutes ces AC filles, et ainsi de suite jusqu'aux feuilles [2, 9].

La certification hiérarchique peut être utilisée, par exemple, dans les entreprises de grande taille pour distribuer des certificats qui donneront accès à l'Intranet de l'entreprise. Dans ce cas, chaque certificat AC intermédiaire peut représenter une filiale ou un département de l'entreprise.

Une autre alternative de la structure hiérarchique à une seule entité de confiance (Root CA) est la structure hiérarchique à multiple entités de confiance [12] (Figure.6).

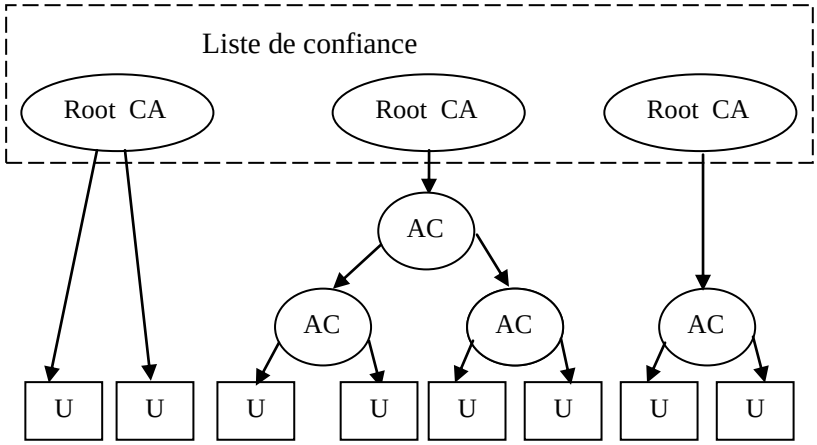

Figure.6 Certification hiérarchique à multiples racines

Dans cette approche, les certificats des utilisateurs sont validés de la même façon que précédemment, à une différence près : un certificat est valide si la chaîne de certificats construite lui correspondant contient l'une des ACs de la liste de confiance.

Les navigateurs webs les plus populaires utilisent cette approche, et sont livrés avec une liste d'ACs de confiance contenant une centaine de certificats d'autorités de certification de confiance [12].

Il existe encore d'autres structures de PKIs, comme les PKI à structure croisée (Figure.7) et les PKI à structure de pont (Figure.8). Faute de place, nous ne pouvons décrire ces deux type de PKI.

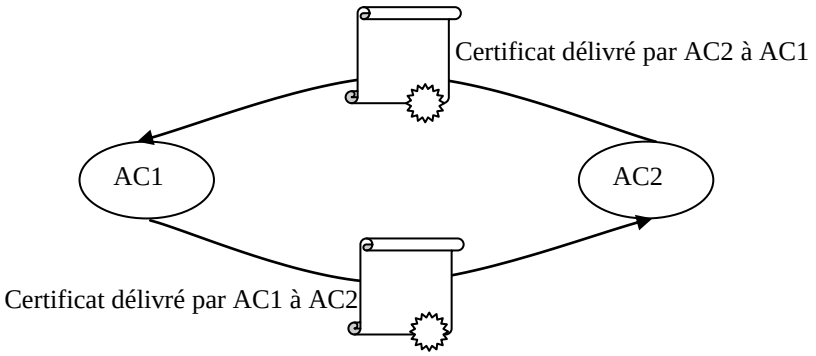

Figure.7 Certification croisée (*cross certification*)

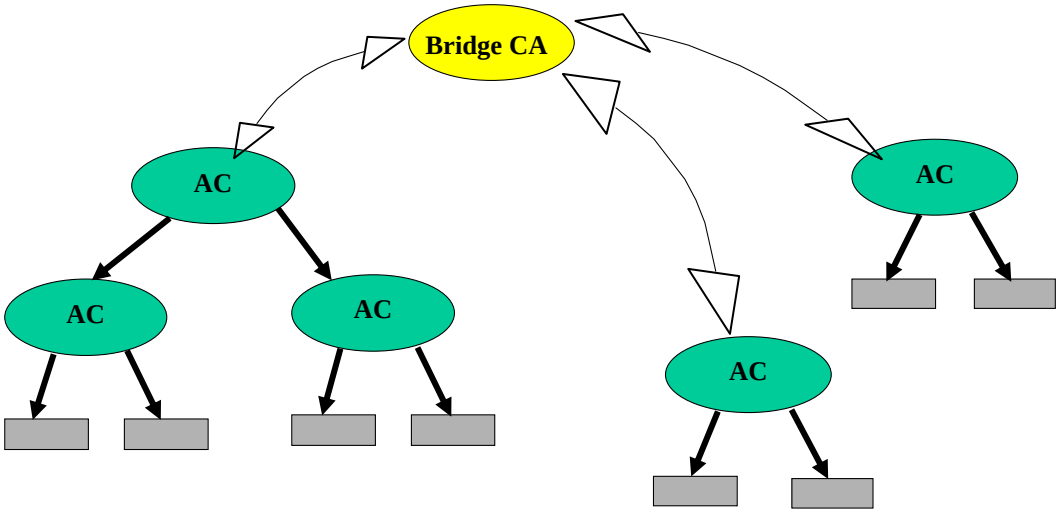

Figure.8 Certification à pont (*bridge certification*)

I.6 Format des certificats X.509

Un certificat conforme à la norme *X.509* [2, 7] (qui est le format standard des certificats de clé publique) peut contenir quelques 11 champs. Leur ordre dans le certificat correspond à la Figure.9.

Serial Number
Issuer
Period of Validity
Subject
Subject's Public Key
...
...
Extensions
Signature

Figure.9 Format d'un certificat *X.509 V.3*

Serial Number (*Numéro de série*) : C'est une valeur assignée par l'AC qui a émis le certificat. L'AC assure l'unicité de la valeur pour chaque certificat émis.
Issuer (*délivreur du certificat*) :
Identifie l'autorité de certification (l'AC) qui a délivré le certificat.
Period of Validity (*Période de validité*) :
Identifie la date de début et la date de fin de validité d'un certificat. En dehors de cet intervalle, le certificat n'est pas considéré comme valide.
Subject (*Sujet du certificat*) :
Identifie l'identité du propriétaire du couple clés privée/publique à certifier (certificat).
Subject's Public Key :
Ce champ contient la clé publique de l'entité à authentifier (*Subject*). Ce champ identifie aussi l'algorithme asymétrique à utiliser, ainsi que tout autre paramètre utile à cet algorithme.
Signature *(Signature numérique*) :
Ce champ contient l'identifiant de l'algorithme (fonction de hachage) utilisé par l'AC pour signer le certificat, ainsi que la valeur de la signature numérique.
Extensions *(Extensions du certificat*) :
Le champ extension fut introduit dans la version 3 de *X.509*. Il procure une place aux autorités de certification (ACs) pour ajouter leurs propres informations aux certificats qu'elle délivre.Ce champ permet à certaines communautés d'utilisateurs (organismes privés ou autres) de définir des extensions privées pour prendre en compte des informations qui leur sont propres.

Dans ce qui suit, une liste non exhaustive de ces extentions est donnée.

CRL Distribution Points (*Points de distribution de la CRL*) :
Cette extension indique comment obtenir les informations relatives à la *CRL*, à savoir : la localisation de la *CRL*, les raisons de révocation des certificats et l'AC qui a délivré la *CRL*.
Il existe plusieurs raisons de révocation de certificats prédéfinies [2, 3] ; parmi ces raisons :

- Compromision de la clé privée correspondant à la clé publique à certifier.
- Compromision de la clé privée d'une AC.
- Changement d'affiliation du sujet du certificat.
- Remplacement d'un certificat.

I.6 Gestion des certificats en cours (Mise à jour, renouvellement et révocation de certificat)

Un certificat peut être l'objet de plusieurs opérations [7] : mise à jour, renouvellement et révocation.

La révocation d'un certificat est la mise hors service de ce certificat avant qu'il ait atteint sa date

d’expiration. Plusieurs causes peuvent être à l’origine de la révocation du certificat notamment la compromission de la clé privée associée à la clé publique du certificat. Dans ce cas, le certificat révoqué est

publié afin que les autres utilisateurs en prennent connaissance lors de la validation de ce certificat.
La mise à jour d’un certificat est une autre forme de révocation, qui concerne la modification (ajout/suppression) de certains champs du certificat, y compris la clé publique du certificat, sans que le certificat soit arrivé à sa date d’expiration ou que le certificat soit révoqué suite à une compromission. Dans ce cas, l’AC ayant délivré le certificat va l’invalider en le révoquant, puis va générer un nouveau certificat contenant les modifications nécessaires, avec une nouvelle période de validité et une nouvelle signature.

Le renouvellement d’un certificat est la regénération d’un même certificat une fois sa date d’expiration atteinte. Donc seule la période de validité ainsi que la signature du certificat changent. Les autres informations contenues dans le certificat sont supposées rester inchangées.

Implicitement, la mise à jour ou le renouvellement d’un certificat sous-entend en premier lieu la *révocation* du certificat, puis la génération d’un nouveau certificat contenant les modifications nécessaires, avec le nouveau certificat contenant obligatoirement un numéro de série différent de celui du certificat révoqué.

I.7 Conclusion

L’utilisation des certificats numériques est devenue de plus en plus partie intégrante de notre vie quotidienne. Les cartes bancaires, les certificats logiciels sont tous des exemples courants de certificats de clé publique établissant un lien certifié entre une clé publique et son propriétaire.

Dans ce chapitre nous présentons la gestion des certificats telle qu'elle est effectuée aujourd'hui au sein des PKIs. Plusieurs opérations peuvent être appliquées à un certificat : révocation, mise à jour et renouvellement. La révocation consiste à mettre hors service un certificat avant même que sa date d'expiration ne soit atteinte; la mise à jour permet de modifier certains champs du certificat (y compris la clé publique) sans que la date d'expiration soit dépassée ou que le certificat soit révoqué; le renouvellement sert à regénérer un même certificat une fois sa date d'expiration atteinte.

La pièce maitresse de cette gestion est la révocation. En effet, une fois un certificat révoqué, son état doit être rendu publiquement connu, afin qu’un utilisateur voulant l’utiliser se rende compte de sa révocation. Prenons l’exemple d’une carte bancaire volée. Une fois que son propriétaire a fait opposition au près des autorités compétentes, toute utilisation future de la carte sera impossible, par conséquent aucune utilisation frauduleuse ne pourra avoir lieu.