CHAPITRE 7

INFRASTRUCTURES À CLÉ PUBLIQUE

7.1 Définition

Une Infrastructure à clés publiques "PKI: Public Key Infrastructure" est définie comme étant la mise en commun d'un ensemble de ressources, matérielles et humaines, alliée à la mise en place de règles régissant l'utilisation de certificats issus de la cryptographie asymétrique. Elle procure des certificats **attestant de la relation existante entre une clé publique et son détenteur**. Elle s'occupe de la gestion des paires de clés asymétriques dans un climat de confiance et assure lors des échanges entre des parties, les principaux points suivants:

- Protéger les données et les identités de toute fuite éventuelle ;
- Assurer l'identification de l'utilisateur ;
- Procéder à une vérification des entités présentes lors des échanges ;
- Protéger les données de toute modification ou altération.

La PKI assure cette sécurité à travers un ensemble de services parmi lesquels nous citons :

- L'enregistrement des ressources (humaines ou informatisées) ;
- La gestion des certificats, la liste de révocation et les utilisateurs

7.2 Les composants de l'infrastructure

L'infrastructure de gestion des clés est basée sur plusieurs composants qui sont indispensables à son fonctionnement. Parmi ces composants, nous répertorions comme principaux, les suivants:

7.2.1 Certificats

Ils assurent la sécurité d'une clé publique afin d'éviter les failles de sécurité liées à l'usurpation d'identité et à la modification écrite.

7.2.2 utilisateurs

Ce sont les personnes ou entités organisationnelles ayant émis ou émettant des demandes de certificat, ou souhaitant simplement vérifier la validité et les informations sur l'identité d'un certificat préalablement reçu. En plus des principaux composants que nous venons de voir, nous avons aussi quelques-uns dits complémentaires, à savoir : les bases de données, le serveur d'horodatage, les serveurs HTTP, SMTP, POP.

7.2.3 Autorité de certification (AC)

On peut dire que c'est le composant le plus important de l'infrastructure PKI du fait de son rôle central dans les différentes cinématiques d'échanges à l'intérieur d'une PKI.

L'autorité de certification est chargée de:

- Reçevoir les demandes de création de certificats venant des autorités d'enregistrement.
- Vérifier la validité de la signature des messages reçus,
- garantir de l'intégrité de la demande et de l'authentification des émetteurs.
- délivrer et gérer les certificats et signe ces certificats en utilisant sa clé privée.
- Envoyer les certificats aux utilisateurs et en parallèle les transmettre au service de publication.

7.2.4 Autorité d'enregistrement (RA)

Elle joue le rôle d'intermédiaire entre l'utilisateur et l'autrité de certification "AC" et dépend de cette dernière. Elle a comme responsabilité de:

- Vérifie l'identité présentée par le demandeur;
- Créer un couple de clés privée-publique pour l'utilisateur Ceci est réalisé avec un logiciel spécifique sur un ordinateur dédié et déconnecté du réseau);
- Garder la clé publique du demandeur;
- Remettre à l'utilisateur la clé privée générée;
- Transmettre avec un message électronique signé une demande de certificat (contenant les informations d'identité et la clé publique du demandeur) à l'autorité de certification. Cette transmission doit se faire de manière sécurisée.

En résumé, cette autorité a pour tâche de gérer les requêtes de certificat qu'elle reçoit des différentes entités et de concevoir les paires de clés qui leur sont spécifiques.

7.2.5 Services d'archivage et de publication

L'archivage est un service qui permet le stockage des paires de clés pour une restitution en cas de perte de la clé privée. En effet, il a pour mission de stocker en toute sécurité les clés de chiffrement émis au sein de l'infrastructure. La publication est un service qui répertorie les différents certificats à clés publiques émis par la CA afin de les rendre disponibles aux éventuels futurs utilisateurs, c'est pourquoi on se réfère communément à lui par le terme de dépôt. Ainsi, un annuaire peut être utilisé (LDAP ou X500 par exemple), un serveur Web ou encore un outil de messagerie, etc. Ce service est contraint par plusieurs exigences telles que, par exemple, le délai de mise à jour des listes de révocation ou la disponibilité de ces listes.

7.3 Principe de fonctionnement des infrastructures de gestion de clés publiques

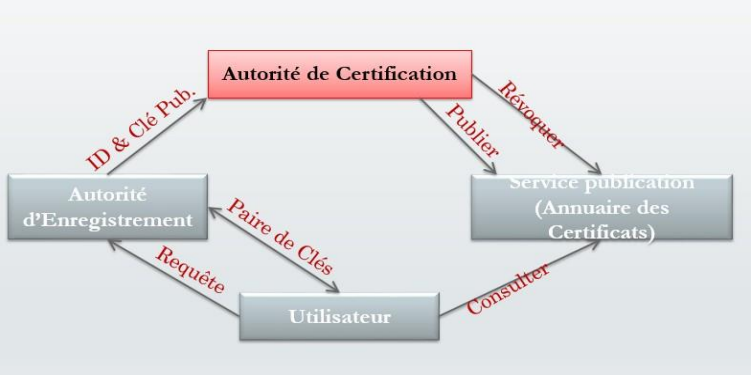
Le principe de fonctionnement des infrastructures de gestion de clés repose essentiellement sur les services précédemment cités. Le fonctionnement d'une PKI se compose de plusieurs étapes :

1. Générer les clés, qui se fait aléatoirement de sorte à garantir leur non prédictibilité ;
2. Enregistrer les clés, permettant de garder toute leur intégrité et cela de manière confidentielle ;
3. Générer les certificats ;
4. Révoquer un certificat, en cas de corruption de ce dernier. Une fois révoqué celui-ci est consigné dans une CRL (Liste de Révocation de Certificat) ;
5. Supprimer une clé, lorsque celle-ci est expirée ou pose un problème de sécurité.
6. Archiver une clé, afin de garder une trace de celle-ci même après une mise au rencart, afin d'assurer la continuité du travail achevé avec cette dernière.

7.4 Procédure de certification

La procédure de certification se fait principalement en trois étapes :

- L'utilisateur s'enregistre auprès de l'autorité d'enregistrement en donnant des justifications concrètes vis-à-vis son identité.
- L'autorité d'enregistrement génère la paire de clés de l'utilisateur et envoie une requête de certification à l'autorité de certification.
- L'autorité de certification génère un certificat pour l'utilisateur et publie ce dernier sur l'annuaire.



7.5 Domaines d'application des PKI

De nombreuses applications profitent de la sécurité fournie à travers l'utilisation des infrastructures à clés publiques. Parmi elles, nous avons retenu :

- L'accès à Internet À travers les navigateurs et serveurs Web qui utilisent le chiffrement pour l'authentification et la confidentialité, mais surtout au niveau du e-commerce qui incite à des transactions financières : ceci implique l'utilisation de protocoles tels que SSL (Secure Sockets Layer), qui permet d'effectuer des échanges sécurisés sur Internet.
- La messagerie Afin de sécuriser la messagerie, l'utilisation des paires de clés est nécessaire pour la sécurisation des messages, fichiers et signatures. Le protocole utilisé est le S/MIME (Secure Multipurpose Internet Mail Extensions), ce protocole gère la confidentialité des courriels.
- Le réseau privé virtuel Le chiffrement des données et l'authentification sont les deux principales fonctions utilisées pour gérer les liens entre les différentes parties au sein d'un réseau privé virtuel (Virtual Private Network (VPN)). Afin d'assurer la confidentialité entre les paires ou équipements (site-to-site, router-to-router) et pour sécuriser les connexions à distance (client-To serveur). Cependant, l'IETF a intégré ces services dans le protocole IPSec afin de la sécuriser les tunnels VPN.

7.6 Les modèles et les architectures PKI

Les relations entre les composants de l'infrastructure à clé publique sont catégorisées en modèle et architecture selon la situation dans laquelle l'infrastructure PKI est mise en place. Chaque autorité de certification à un nombre d'entités avec lesquelles elle communique, qui permet le contrôle plus ou moins aisé des échanges.

Les autorités de certification (AC) sont des entités qui valident l'identité et l'émission des certificats. Elles peuvent être des organismes indépendants ou des entreprises qui utilisent leur propre logiciel d'émission de certificats (tel que Red Hat Certificate System). Tout logiciel client ou serveur qui supporte les certificats maintient une liste des certificats d'AC de confiance. Ces certificats d'AC déterminent quels autres certificats le logiciel peut valider - en d'autres mots, dans quels émetteurs de certificats le logiciel peut avoir confiance. Dans le cas le plus simple, le logiciel ne peut valider que les certificats émis par une des AC pour lesquelles il possède le certificat. Il est également possible pour un certificat d'une AC de confiance de faire partie d'une chaîne de certificats d'AC, chacun émis par l'AC parente dans la hiérarchie de certificat

7.6.1 Hiérarchies d'AC

Dans les grandes organisations, il peut être judicieux de déléguer la responsabilité de l'émission des certificats à plusieurs autorités de certification. Par exemple, quand le nombre de certificats requis peut être trop important à maintenir par une seule AC, il est possible de déléguer la responsabilité de l'émission de certificats à des AC subordonnées. Le standard X.509 inclus un modèle de paramétrage d'une hiérarchie d'AC comme celle montrée dans la Figure.

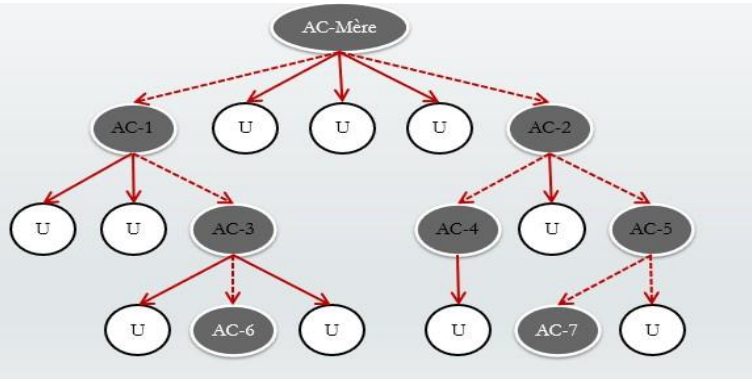


Figure 7.1: hiérarchie d'AC

Dans ce modèle, l'AC mère est au sommet de la hiérarchie. Le certificat de l'AC mère est un « certificat auto-signé » : c'est-à-dire que le certificat est signé numériquement par la même entité « L'AC mère ». Les AC directement subordonnées à l'AC mère on des certificats d'AC signés par l'AC racine. Les AC se trouvant sous les AC subordonnées dans la hiérarchie ont leurs certificats signés par les plus hautes AC subordonnées.

7.6.1.1 Certificat d'attribut

Un certificat d'attribut a la même structure d'un certificat d'identité à la différence qu'il: Donne des informations sur les privilèges d'un utilisateur. Ces informations sont liées aux droits que possède un utilisateur dans une application donnée, qui lui permet de procéder à certaines opérations techniques ou accéder à certains services ou ressources. Ne contient pas forcement la clé publique de l'utilisateur. Le possesseur d'un certificat d'attribut doit avoir un certificat d'identité.

7.6.1.2 Chaînes de certificat

Les hiérarchies d'AC se reflètent dans les chaînes de certificats. Une chaîne de certificats est une série de certificats émis par des AC successives. Une chaîne de certificats trace le chemin des certificats d'une branche de la hiérarchie jusqu'à la racine. Dans une chaîne de certificats, on a donc :

- Chaque certificat est suivi par le certificat de son émetteur.
- Chaque certificat contient le nom (DN) de l'émetteur du certificat, qui est identique à celui du nom du sujet du certificat suivant dans la chaîne.
- Chaque certificat est signé avec la clé privée de son émetteur. La signature peut être vérifiée avec la clef publique du certificat de l'émetteur, qui est le prochain certificat dans la chaîne.

7.6.1.3 Vérification d'une chaîne de certificat

La vérification de la chaîne de certificats est le processus permettant de s'assurer qu'une chaîne de certificats donnée est bien formée, proprement signée et sécurisée. Les logiciels Red Hat utilisent la procédure suivante pour former et vérifier une chaîne de certificats, en commençant par le certificat présenté pour l'authentification :

- La période de validité du certificat est vérifiée par rapport à la date actuelle fournie par l'horloge système du vérificateur.
- Le certificat de l'émetteur est localisé. La source peut être une base de certificats locale du

vérificateur (du client ou du serveur) ou une chaîne de certificats fournit par le sujet (par exemple, par une connexion SSL).

- La signature du certificat est vérifiée à l'aide de la clef publique du certificat de l'émetteur.
- Si le certificat de l'émetteur est présent dans les certificats de confiance du vérificateur, la vérification s'arrête avec succès à cette étape. Autrement, le certificat de l'émetteur est vérifié pour être certain qu'il contient les indications appropriées concernant les AC subordonnées dans l'extension du type de certificat de Red Hat, et la chaîne de vérification recommence depuis l'étape 1, mais avec le nouveau certificat.

7.6.2 Modèle croisé

Les relations croisées servent à relier deux hiérarchies d'autorités de certification de deux organisations différentes. L'autorité de certification racine de chaque organisation signe pour l'autre un certificat d'identité. Ainsi, n'importe quel utilisateur de la première hiérarchie peut vérifier la clé publique de n'importe quel autre utilisateur de la deuxième.

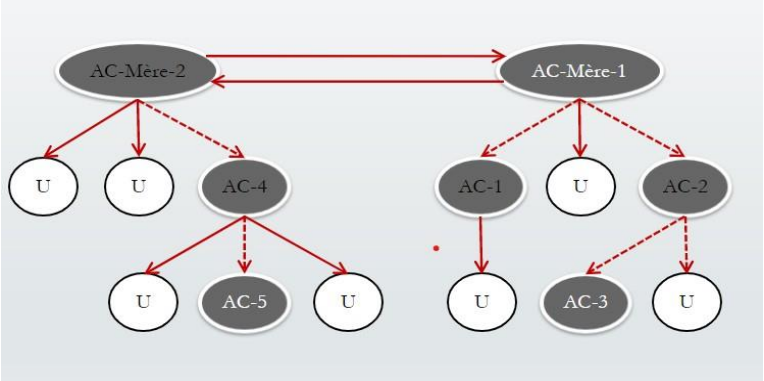


Figure 7.2: Modèle de certification croisé

7.6.3 Modèle complètement distribué

Dans ce modèle, il n'y a pas la notion d'autorité de certification. Chaque utilisateur se considère comme étant une autorité de certification, où il peut signer et délivrer des certificats pour les utilisateurs. Ce système permet la création d'un graphe de confiance entre l'ensemble des utilisateurs.

La vérification de la validité d'un certificat se fait à travers la vérification de toute la chaîne de certificats qui relie les deux utilisateurs en se basant sur le principe : « **Si A fait confiance à B, et ce dernier fait confiance à C, alors A peut faire confiance à C** ».

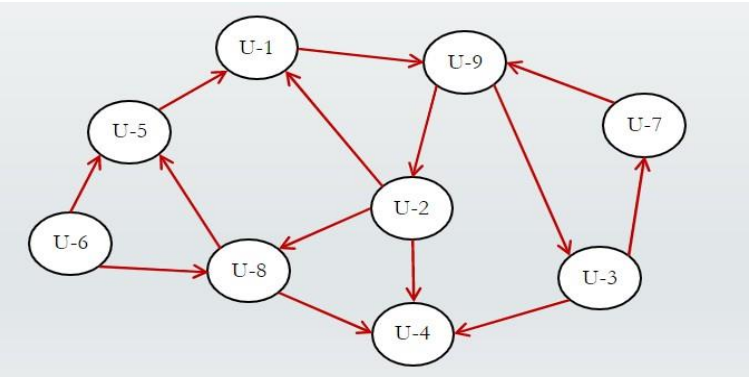


Figure 7.3: Modèle de certification croisé

7.7 Le partage du pouvoir de certification

7.7.1 La cryptographie à seuil

Le partage de secret repose sur le concept de d'détention d'une portion d'une information secrète par plusieurs entités. La cryptographie `a seuil permet le partage d'une valeur secrète S à un ensemble de n serveurs, sans que chacun d'eux connaisse sa valeur. A partir d'au moins k serveurs on peut reconstruire le secret (k _ n). Si le nombre de serveurs est inférieur à k, aucune information n'est obtenue sur le secret S. La cryptographie `a seuil s'exécute en deux étapes :

1. ***Le partage du secret :*** Cette étape permet de mettre en commun un secret S entre n serveurs. On crée un polynôme $F(x)$ de degré $k - 1$ avec des coefficients arbitraires en mettant $a_0 = S$. On choisit ensuite publiquement n points distincts xi, et on distribue secrètement à chaque serveur une part privée (x_i, $F(x_i)$). Le point xi pourrait être n'importe quelle valeur publique qui identifie le serveur si d'une manière unique. Pour simplifier la notation, on met $x_i = i$, par conséquent les parts privées sont d´entrées par $F(1)$, $F(2)$, ..., $F(n)$.

2. ***La reconstruction du secret :*** Cette étape permet de reconstruire le secret S à partir d'un sous-ensemble de k parts : {$F(1)$, $F(2)$, ..., $F(k)$}. Etant donné k points distincts (i, $F(i)$), il existe un polynôme unique $F(x)$ de degré k – 1 passant par tous les points. Ce polynôme peut être calculé à partir des points (i, $F(i)$) en utilisant l'interpolation de Lagrange.

7.7.2 Certification avec la cryptographie à seuil à base de RSA

La certification s'exécute comme suit :

(1) Générer les paramètres d'une paire de clés RSA : e, d, n, $\Phi(n)$.
(2) Définir un polynôme $F(x) = d + a_1x + ... + a_{k-1}x^{k-1}$, ensuite calculer pour chaque serveur si sa part privée : $S_i = F(i) \bmod \_(n)$.
(3) Chaque serveur si génère une signature partielle SP_i du certificat comme suit : $SP_i = C^{Si} \bmod n$.
(4) Pour combiner l'ensemble des signatures partielles, calculer l'interpolation de Lagrange de chaque serveur : $\mathcal{L}_i = \prod_{j=1, j\neq i}^{j=k} \frac{j}{j-i} \bmod \phi(n)$. Ensuite, calculer la signature complète SC du certificat : $\mathcal{SC} = \prod_{i=1}^{i=k} \mathcal{SP}_i^{\mathcal{L}_i} \bmod n$.
(5) Si l'égalité $C = SC^e \bmod n$ est vérifiée, alors la signature est valide.

Exemple

- $e = 11$, $d = 131$, $n = 527$, $\Phi(n) = 480$.
- $F(x) = 131 + x + x^2$. S1 = F(1) mod 480 = 133, S_2 = F(2) mod 480 = 137, et S_3 = F(3) mod 480 = 143.
- Pour C = 6 : $SP_1 = 6^{133} \bmod 527 = 347$, $SP_2 = 6^{137} \bmod 527 = 181$, et $SP_3 = 6^{143} \bmod 527 = 88$.
- $L_1 = 3$, $L_2 = 477$, et $L_3 = 1$. SC = 3473 × 181477 × 881 mod 527 = 522.
- $522^{11} \bmod 527 = 6$.