CHAPITRE 6

CERTIFICATS NUMÉRIQUES

6.1 Introduction

Nous avons décrit dans le premiers chapitre les mécanismes qui permettent d'assurer les 3 fonctions de base de sécurité avec le couple de clés privée-publique et les algorithmes de chiffrement asymétriques. Mais il y a **une énorme lacune** dans les raisonnements précédents. On a considéré qu'un utilisateur connaissait la clé publique d'une personne simplement en consultant un annuaire ou un serveur Web et ainsi il la considérait comme vraie. Mais **qu'estce qui garantit que la clé publique qu'un utilisateur a ainsi récupérée est la bonne ?** Il ne faut pas oublier que tout ceci fonctionne de manière électronique, sur Internet, sans contact direct donc sans moyen visuel de reconnaissance d'une personne. **C'est le rôle des certificats**.

6.2 Qu'est ce qu'un certificat numérique?

Un certificat est l'équivalent d'une carte d'identité ou d'un passeport. Un passeport contient des informations concernant son propriétaire (nom, prénom, adresse, etc.), la signature manuscrite, la date de validité, ainsi qu'un tampon et une présentation (forme, couleur, papier) qui permettent de reconnaître que ce passeport n'est pas un faux, qu'il a été délivré par une autorité bien connue. Le certificat numérique ou électronique, résultat d'un traitement fixant les relations qui existent entre une clé publique, son propriétaire et l'application pour laquelle il est émis.

- Pour une personne il assure son identité
- Pour une application, il assure que celle-ci n'as 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

Un certificat numérique est un **document électronique permettant l'association entre une clé publique et une entité** (personne, équipement (dans le cas du réseau V2G), entreprise. . .) afin d'assurer sa validité. On peut donc établir de façon triviale que le certificat est le lien entre une entité physique et une entité numérique, certifié par l'autorité de certification.

6.3 Le standard X509

Le standard régissant les certificats numériques est le X.509. Il définit un certificat en plusieurs champs. Le format reconnu actuellement est le format **X509V3**. C'est un petit fichier, qui contient au moins les informations suivantes:

- Version du standard.
- Numéro de série du certificat.
- Le nom de l'autorité (de certification) qui a créé le certificat
- L'identité de l'utilisateur .
- La clé publique de l'utilisateur.
- Des informations optionnelles
- L'identité du signataire.
- Algorithme de signature utilisé.
- Fonction de hachage utilisée.
- Les dates de validité du certificat.
- Signature numérique de l'autorité de certification

Cette signature électronique est calculée sur les informations contenues dans le certificat comme dans le cas d'un message électronique. La signature est l'empreinte de ces informations chiffrée avec la clé privée de l'autorité de certification qui a délivré ce certificat.

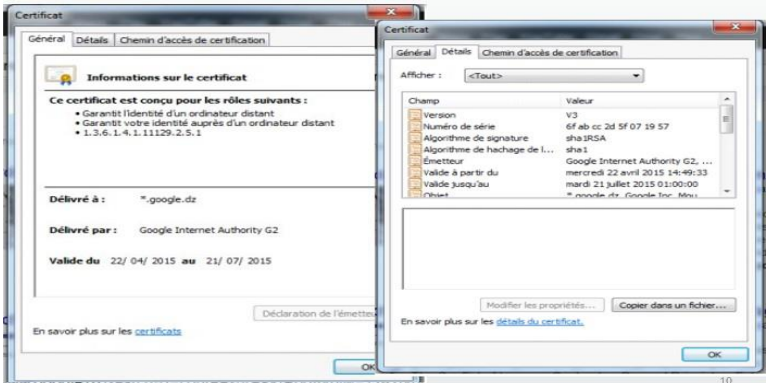

Figure 6.1: Exemple de certificat numérique

6.4 cycle de vie

Comme présenté dans la figure, les certificats ont un cycle de vie composé des phases suivantes:

- Demande de certification ;

- Vérification des attributs ;
- Création et signature du certificat ;
- Remise au demandeur (publication) ;
- Utilisation du certificat ;
- Suspension ou révocation du certificat ;
- Expiration du certificat (possible renouvellement).

Figure 6.2: Cycle de vie d'un certificat

6.5 Utilité et Caractère des certificats numériques

Les certificats électroniques sont utilisés dans différentes informatiques pour garantir:

- la non-répuduation et l'intégrité des données avec la signature numérique;
- la confidentialité des données grâce au chiffrement des données;
- L'authentification forte d'un individu ou d'une identité numérique.

Un certificat est:

- Infalsifiable : il est chiffré pour empêcher toute modification.
- Nominatif: il est délivré à une entité (comme la carte d'identité est délivrée à une personne et une seule).
- Certifié: il y a le «tampon» de l'autorité qui l'a délivré

6.6 Types de certificats

Le type de certificats électroniques dépend du support qui l'héberge. Ainsi, nous pouvons distinguer trois (03) types de certificats : le certificat serveur, le certificat personnel ou client et le certificat IP SEC (Internet Protocol Security) ou VPN

6.6.1 Le certificat serveur

Ce type de certificat est installé sur un serveur. Il est le garant de l'identité du serveur et la sécurité de la session établie par un utilisateur. Le certificat serveur le plus répandu actuellement est le certificat SSL ou « Security Socket Layer ». Il permet d'assurer l'authenticité d'une URL et de garantir la sécurité des transactions effectuées par les internautes.

6.6.2 Le certificat personnel ou certificat client

Le certificat client est enregistré sur un ordinateur ou sur un conteneur, comme les clés USB ou carte à puce, appartenant à une personne physique. En analogie avec la carte d'identité d'une personne physique, il sert à identifier l'utilisateur et définir ses droits d'accès aux différentes informations partagées sur le réseau.

6.6.3 Le certificat IP SEC (Internet Protocol Security) ou VPN

Le certificat IPSEC est quant à lui hébergé sur un équipement réseau. Il a pour but de chiffrer l'ensemble des informations transmises sur les réseaux usant des protocoles internet. Comme les deux précédents certificats, il sert également d'identifiant pour le composant de réseau. Il permet ainsi de rendre privé l'ensemble des flux transitant entre deux équipements réseaux.

6.7 Autorité de certification et infrastructure de gestion de clés

6.7.1 Définition d'une autorité de certification

Une autorité de certification (AC) est un organisme **reconnu** comme étant **compétent** pour **délivrer** des certificats à une population auprès de laquelle elle a toute confiance et en assurer la validité. Elle s'engage sur l'identité d'une personne au travers du certificat électronique qu'elle lui remet. Une autorité de certification est responsable (vis-à-vis de ses clients, mais aussi de toute personne se fiant à un certificat électronique qu'elle a émis) de l'ensemble du processus de certification et, par voie de conséquence, de la validité des certificats qu'elle émet. Par ailleurs, c'est elle qui définit la politique de certification et la fait appliquer. La confiance que l'on accordera à un certificat va dépendre du sérieux de l'autorité qui l'aura délivré. De plus, on voit très bien le risque encouru par une entreprise ou un organisme dont la carte d'identité des employés aurait été créé par une autorité ni habilitée, ni contrôlée par ellemême. Le choix de l'autorité de certification dans une organisation ou une entreprise est une décision stratégique.

6.7.1.1 Types d'autorités de certification

Les principales autorités de certification américaines et européennes sont divisées en deux catégories:

- Les autorités de certification reconnues:VeriSign, thawte, Entrust, Baltimore
- Les autorités de certification non reconnue: Certinomis, ChamberSign, E-Trust, E-Certify.

6.7.2 Infrastructure de gestion de clé

Quelle que soit l'autorité de certification choisie, il faut faire d'autres choix. Comme il existe un circuit de procédures et de vérifications, des personnes habilitées, etc., pour délivrer les cartes d'identité, il faut mettre l'équivalent en place. Il faut ainsi décider qui va recueillir et vérifier les informations données par

une personne lorsqu'elle va demander un certificat, suivant quelles procédures, 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, etc. Il faut définir ce que l'on appelle une architecture de gestion des certificats. IGC (Infrastructure de Gestion de Clés), et PKI (Public Key Infrastructure) sont les deux sigles les plus connus pour la désigner. Les normes internationales décrivent les différents éléments fonctionnels d'une IGC. En simplifiant, l'architecture est constituée de :

6.8 Les classes de certificats

Il est courant de catégoriser les certificats par leurs classes. Cette classe permet de connaître quel niveau de validation (et donc de sécurité) qu'on peut attendre des certificats.

- Classe 1 : Un certificat électronique de classe 1 ne garantit que l'existence de l'adresse e-mail de son titulaire. Il n'assure donc pas l'identité du détenteur du certificat et par ailleurs, n'effectue aucun contrôle à ce sujet.
- Classe 2 : preuve de l'identité requise (photocopie de carte d'identité par exemple ou bien numéro SIRET/SIREN et nom de domaine). Le contrôle se fait à distance sur remise de justificatif.
- Classe 3 : un certificat ne peut être délivré que dans le cadre d'une présentation physique du demandeur (contrôle face à face du client).
- Classe 3+ : la même chose que la classe 3 avec en plus la délivrance de la clef privée et du certificat associé sur support physique.

6.9 Forme de certificats électronique

6.9.1 La solution logicielle

Le certificat est téléchargé et stocké sur le disque dur de l'ordinateur. Ce n'est pas la solution la plus sécurisée car le certificat peut être copié ou supprimé par une personne mal intentionnée. Le certificat logiciel est donc fortement déconseillé.

6.9.2 La solution matérielle

6.9.2.1 Le certificat sur clé USB

la clé se connecte directement sur le port USB du PC. Par contre, sur PC station, si le port USB est à l'arrière de votre machine, vous aurez des difficultés à connecter votre clé USB à chaque utilisation. Si le port USB est en face avant, vous risquez de casser la clé USB qui dépasse de votre poste. De plus, ce n'est pas un support personnalisable.

6.9.2.2 Le certificat sur carte à puce

Un lecteur de cartes est nécessaire. Sur un ordinateur portable, il est souvent inclus, par contre sur PC station, il faudra s'en procurer un. La carte à puce est personnalisée au nom du bénéficiaire et de l'organisme auquel il est rattaché. Ce qui est très utile lorsque vous êtes plusieurs à posséder des certificats électroniques au sein de votre entreprise ou si vous êtes porteur de plusieurs certificats, pour le compte de plusieurs entités. Parce que le certificat est logé sur carte à puce ou sur clé USB, il vous apporte un niveau de sécurité plus élevé que le certificat logiciel et répond à vos besoins de souplesse et de mobilité :

- Votre certificat et les éléments secrets associés sont stockés sur une puce (carte ou clé), hors de votre poste de travail ;
- Ils sont protégés par un code confidentiel connu de vous seul (et personnalisable) ;
- Ils vous accompagnent sur vos différents lieux de travail.

6.10 Utilisation des certificats

L'utilisation de la cryptographie à clé publique ou à clé symétrique est très répandue. Cette utilisation est faite à travers les certificats pour les raisons citées ci-dessus. Parmi les applications et protocoles utilisant les certificats, nous pouvons citer :

- Le courrier électronique sécurisé (S/MIME).
- Les protocoles SSL/TLS
- Réseaux virtuels privés : IPsec.
- Niveau applicatifs (en remplacement d'une authentification par mot de passe de l'utilisateur).

6.11 Gestion des certificats

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

6.11.1 Révocation d'un certificat

La révocation est la mise hors service d'un 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.

6.11.2 Mise à jour d'un 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'autorité de certification ayant délivré le certificat, va 18 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.

6.11.3 Renouvellement d'un certificat

Le renouvellement d'un certificat est la régénération 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.