TD4

Certificats Numériques

Exercice 1 :

1. Il existe un risque d'usurpation d'identité :

Cas 1 : Dans le premier cas la confidentialité est compromise. Supposant, un pirate « Aissa » , a pu modifier l'annuaire ou le serveur Web qui contient la clé publique de « Salma ». Il a pu par exemple remplacer la clé publique de « Mohamed » par la sienne. Si « Salma », croit détenir la clé publique de « Mohamed » alors que c'est celle de « Aissa », elle envoie un message chiffré à « Mohamed » en le chiffrant avec la clé publique de « Mohamed ». Si celle-ci est en fait la clé publique de « Aissa », alors « Aissa » pourra déchiffrer ce message destiné à « Mohamed » avec sa clé privée. « Aissa » pourra donc lire le courrier confidentiel de « Mohamed ».

Cas 2 : « Aissa » pourra envoyer un message signé à « Salma » avec une signature générée avec sa clé privée et en se faisant passer pour « Mohamed ». « Salma » qui recevra le message vérifiera la signature du message avec ce qu'elle croit être la clé publique de « Mohamed ». La vérification sera correcte, donc « Salma » pensera que le message vient de « Mohamed ».

- Pour remédier à ce genre de problème on doit assurer la validité de la clé publique en utilisant le certificat numérique

2. Un certificat numérique : est un document électronique utilisé pour identifier un individu, un serveur, une entreprise ou toute autre entité et pour associer une clef publique à cette identité. Un certificat fournit généralement une preuve reconnue de l'identité de la personne. La cryptographie à clef publique utilise les certificats pour éviter les problèmes d'usurpation d'identité. Les certificats aident à prévenir l'utilisation de fausses clefs publiques.

Exercice 2 :

1. Chaque ligne représente :

Ligne 2 : version

Ligne 3 : Numéro de série unique, dans le domaine de confiance auquel appartient le certificat, qui l'identifie de façon unique. C'est ce numéro de série qui sera posté dans la liste de révocation en cas de révocation

Ligne 4 : Désigne le procédé utilisé par l'AC pour signer le certificat : (norme ISO). Il s'agit d'un algorithme asymétrique et d'une fonction de condensation.

Ligne 5 : Spécifie le DN (Distinguished Name) de l'AC qui a généré le certificat.

Ligne 6 : période de validité du certificat (les dates de début et de fin de validité du certificat).

Ligne 9 : Spécifie le DN de l'utilisateur possédant la partie privée de la clé publique contenue dans le certificat.

Ligne 12 : C'est le cœur du certificat. Ce champ contient la valeur de la clé publique du détenteur du certificat et les algorithmes avec lesquels elle doit être utilisée RSA with MD5 par exemple

Ligne 16 : Algorithme de signature + la Signature du certificat

2. Non la clé privée ne figure pas dans le certificat : Le certificat émis par l'AC lie une clef publique particulière au nom de l'entité qu'il identifie (tel qu'un nom d'employé ou de serveur). Seule la clef publique certifiée dans le certificat fonctionnera avec la clef privée correspondante possédée par l'entité identifiée par le certificat

3. Comment la signature de ce certificat est-elle calculée ?: 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.

4. Comment peut-on vérifier la validité de ce certificat ?: La validité du certificat peut être vérifiée en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats. Evidemment, les dates de validité du certificat sont aussi vérifiées avant de le déclarer valide.

5. 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. Autant dire que son rôle et ses responsabilités sont importantes