Série TD 04 : Signature électronique

Questions générales :

1. Sur quelle technique cryptographique est basée la signature numérique ? Expliquez ?
2. Est-ce que la technique cryptographique est appliquée directement sur le message ? Pourquoi ?
3. Quels objectifs de sécurité offre la signature numérique ?
4. Expliquer le principe de déroulement de la signature d'un document.
5. Que doit-on posséder pour signer un document électronique ? et pourquoi ?

Série TD 05 : Les Certificats Numériques

Exercice 1 : Voici deux cas pratiques

Cas 1 : Salma souhaite envoyer un courrier confidentiel à Mohamed, le scénario suivant va être exécuté:

- Elle va consulter un annuaire ou un serveur Web pour avoir la clé publique de Mohamed -
- Ensuite elle chiffrera le message en utilisant cette clé

Cas 2 : Mohamed envoie un document signé à Salma en utilisant sa clé privé (sans l'utilisation de certificat)

Questions :

1. 1. Quelle sont les risques de sécurité encourus dans les deux cas. Et comment y remédier ?
2. Qu'est-ce qu'un certificat électronique

Exercice 2 : Voici un exemple de certificat X509v3

1. Que représente chaque ligne de ce certificat ? La clé privée figure t'elle ?
2. Comment la signature de ce certificat est-elle calculée ?
3. Comment peut-on vérifier la validité de ce certificat ? Expliquer avec un schéma
4. Qu'est-ce qu'une autorité de certification ?

Certificate:

1. Data:
2. **Version:** 1.3
3. **Serial Number:** 234-A12
4. **Signature Algorithm:** md5withRSAEncryption
5. **Issuer:** C=ZA, SP=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services, CN=www.thawte.com, Email=webmaster@thawte.com
6. **Validity**
7. Not Before: Nov 14 17:15:25 1999 GMT
8. Not After : Dec 14 17:15:25 2016 GMT
9. **Subject:** C=CH, SP=NE, L=Neuchâtel, O=Assoc. ABORD,
10. OU=Ermitage project, CN=projet-ermitage.org,
11. Email=admin@projet.ermitage.org
12. **Subject Public Key Info:**
13. **Public Key Algorithm:** rsaEncryption
14. **Modulus:**

00:9a:92:25:ed:a4:77:69:23:d4:53:05:2b:1f:3a:55:32:bb:27:de:0a:48
:d8:fc:c8:c0:c8:77:f6:5d:61:fd:1b:33:23:4f:f4:a8:2d:96:44:c9:5f:c
2:6e:45:6a:9a:21:a3:28:d3:27:a6:72:19:45:1e:9c:80:a5:94:ac:8a:67

15. **Exponent:** 65537 (0x10001)
16. **Signature Algorithm:** md5withRSAEncryption

7c:8e:7b:58:b9:0e:28:4c:90:ab:20:83:61:9e:ab:78:2b:a4:54:39:80:7b
:b9:d9:49:b2:b3:2a:fe:8a:52:f4:c2:89:0e:5c:7b:92:f8:cb:77:3f:56:2
2:9d:96:8b:b9:05:c4:18:01:bc:40: ee:bc:0e:fe:fc:f8:9b:9d:70:e3

TD 04

Signature électronique

Questions générales :

1. Sur quelle technique cryptographique est basée la signature numérique ? Expliquez ?

La signature électronique repose sur le principe de la cryptographie asymétrique.

Pour signer électroniquement un document le signataire utilise son certificat, qui constitue sa carte d'identité numérique. Ce certificat contient des informations sur son possesseur, ainsi que deux clés : une clé publique et une clé privée. La clé privée est utilisée pour signer le document, la clé publique est utilisée pour vérifier cette signature. Cela signifie que seul le possesseur du certificat (qui connait la clé privée) peut signer un document, mais que n'importe qui est en mesure de vérifier cette signature.

2. Est-ce que la technique cryptographique est appliquée directement sur le message ? Pourquoi ?

- Le condensat permet de vérifier l'intégrité des données
- On n'applique pas l'algorithme au message lui-même, mais à son condensat, obtenu à l'aide d'une fonction de hachage. La taille du condensat étant fixe et indépendante de la taille du message lui-même, cela permet de réduire la bande passante utilisée pour transmettre le message en plus la plupart des mécanismes de signatures numériques sont basé sur la cryptographie asymétrique. Cette dernière est coûteuse en calculs. L'appliquer sur des messages de taille arbitraire entraînerait une dégradation des performances du système

3. Quels objectifs de sécurité offre la signature numérique ?

- **Authentification** : Cela garantit l'identité de la personne qui a signé les données : l'origine du message, du document ou de la transaction est incontestable.
- **Intégrité des données** : La signature électronique protège l'intégrité des données. Cela signifie que le document reçu n'a pas été altéré, volontairement ou involontairement
- **non-répudiation** : L'auteur (la personne qui signe) d'un document prouve son identité. La non-répudiation établit, plus tard, qui a participé à une transaction. L'expéditeur ne peut nier avoir envoyé le message et le destinataire ne peut nier l'avoir reçu. Simplement, la non-répudiation signifie qu'une information ne peut être rejetée, tout comme avec les signatures manuscrites

4. Expliquer le principe de déroulement de la signature d'un document.

La signature d'un document se déroule comme suit :

a. Signature

Le signataire calcule le condensat du document à signer, puis il encrypte ce condensat à l'aide de sa clé privée. Il crée ensuite la signature, qui peut-être intégrée au document original ou enregistrée dans un fichier séparé. Cette signature est composée de l'empreinte signée (le condensat encrypté) et de son certificat.

b. Vérification

Le destinataire calcule le condensat du document reçu (en omettant la signature, si celle-ci est intégrée au document), et décrypte l'empreinte signée, à l'aide de la clé publique contenue dans le certificat du signataire. Il compare ces deux valeurs, si elles sont identiques, alors la signature est authentique, et l'identité du signataire est bien celle qui est décrite par le certificat. En vérifiant la validité de ce certificat, le destinataire est assuré de la validité de cette signature.

5. Que doit-on posséder pour signer un document électronique ? et pourquoi ?

On doit posséder un certificat numérique. Pour s'assurer que la clé publique que notre correspondant nous a communiqué est bien celle de la personne physique ou morale qu'il prétend être.

TD05

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