ITCE NFE 102
Année 2012-2013

La sécurité des transactions

F.-Y. Villemin (f-yv@cnam.fr)

http://dept25.cnam.fr/ITCE

Sécurité

La sécurité d'un système d'information comprend :

- la protection de la confidentialité de l'information
- le contrôle des accès
- l'authentification des intervenants
- l'intégrité du message et la non-répudiation du message

Sécurité

Le contrôle des accès permet de s'assurer que l'utilisateur a les droits et privilèges appropriés pour effectuer une opération (lire des données à caractère confidentiel, par exemple)

L'authentification permet de vérifier que l'utilisateur, la machine ou la compagnie à l'autre bout de la communication est bien celui qu'il se prétend être

L'intégrité du message assure que l'information reçue n'a pas été interceptée et altérée pendant son transfert

La non-répudiation du message fournit la preuve que la transaction a bel et bien eu lieu

Sécurité

Types d'attaques :

- Virus
- Pirates (Intrus criminels et crackers, hackers) :
- Installation de logiciels "sniffers"
- Capture de codes d'accès (Login/password) et autres informations
- Le courrier électronique peut être intercepté et lu
- Des informations stockées sur une machine peuvent être lues
- Les numéros des cartes de crédit des clients peuvent être volés…
- Arrêt du système ou altération des fichiers (perte de productivité)

Sécurité

Toute connexion réseau, même à un LAN, augmente la menace

Les données transitant sur le support physique peuvent être enregistrées

Toute connexion vers l'extérieur augmente encore davantage le risque

Les barrières physiques ont été rompues : il est possible d'accéder à votre réseau

Il faut remplacer les barrières physiques par leurs équivalents électroniques

Le mieux que puisse faire un système de sécurité c'est de rendre très cher et très difficile le piratage de votre système

Ne faites pas de publicité pour un système "inviolable"

=>Les "Hackers" considéreraient cela comme un défi

Sécurité

L'administrateur réseau doit intégrer un modèle de sécurité dans la mise en place de l'accès Internet fondé sur :

- **Authentification** : Autorise l'accès des seules personnes autorisées
- **Confidentialité** : L'information transmise n'est pas interceptée ni modifiée
- **Intégrité** : Ne pas modifier la propriété de l'information transmise
- **Disponibilité** : Systèmes opérationnels lorsque c'est nécessaire

Sécurité

Les serveurs WWW ont des faiblesses :

- Les scripts lancés par le serveur qui en étendent les fonctionnalités, par exemple :
  - ajouter des fonctionnalités de mail au logiciel du serveur
  - gérer des formulaires en entrée et retourner des informations depuis une base de donnée
- Les scripts activés par le client qui passe une information au serveur

=> Les scripts qui s'exécutent avec des privilèges sont dangereux

Un marché pour les serveurs sécurisés s'est développé :

- Sécurité importante coté serveur (S-HHTP et S-HTML)
- Transport crypté entre client et serveur (SSL)

Sécurité

Matériel et logiciel qui permettent aux seules données approuvées de passer au travers :

- Des mécanismes de sécurité de niveau réseau
- Logiciel de filtrage des routeurs
- Segmentation des réseaux IP

Des mécanismes de sécurité de niveau Application

Filtrage de niveau applicatif

Par exemple: n'autoriser seulement que le trafic e-mail de ou destiné à l'utilisateur X

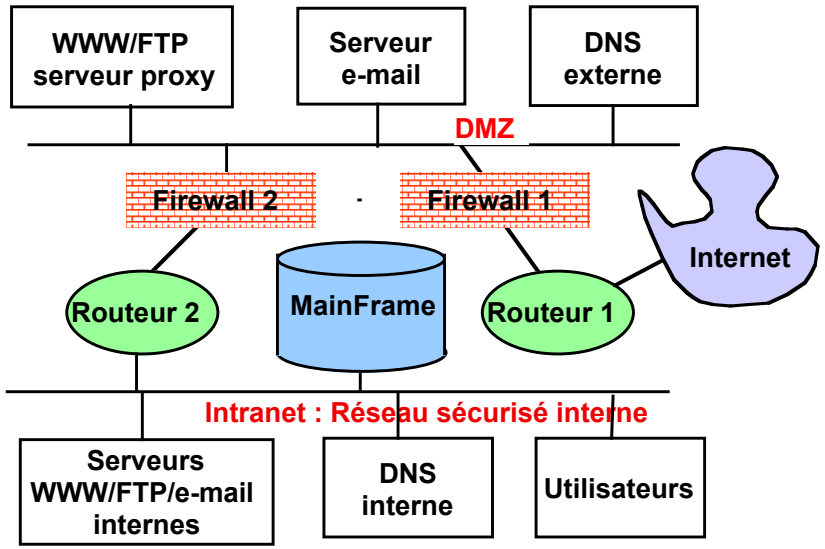
Audit intensif des transactions :

Les fichiers de traces nécessitent de l'attention et un archivage régulier

Un site Internet doit être construit avec beaucoup de soin et peut être compliqué

Il y a des logiciels du domaine public disponibles sur Internet

Sécurité



Confiance

Pour qu'un client puisse effectuer une transaction commerciale ou une entreprise une télédéclaration sur Internet en toute sécurité, il y est nécessaire que :

- celui qui se connecte soit assuré qu'il se connecte bien au serveur désiré et pas sur un autre
- celui qui s'identifie auprès du serveur soit la personne déclarée, évitant à la fois l'usurpation de son identité par un tiers mal intentionné et une contestation du déclarant
  => non-répudiation, authentification
- que les données échangées durant la connexion ne seront pas modifiés
  => intégrité des échanges

Confiance

Dans un certain nombre de cas, il est aussi nécessaire de garantir :

- que seul le destinataire puisse lire les données échangées
  => confidentialité
- La date et heure de la transmission
  => horodatage
- que le message a bien été reçu et lu
  => accusé d'échange

Le chiffrement, ou cryptographie, permet de satisfaire la majeur partie des besoins de confiance

Cryptographie

Les objectifs de la cryptographie sont :

1. La confidentialité, ou transmettre une information sur un canal non sécurisé de telle sorte qu'un tiers ne puisse pas la lire.
2. L'intégrité, ou assurer qu'une information n'a pas été altérée lors de sa transmission.
3. La non répudiation, ou empêcher qu'une personne nié avoir émis une information.
4. L'identification, ou prouver l'identité de l'émetteur.

Cryptographie

Le chiffrement garantit la confidentialité d'une information en lui appliquant une transformation pour assurer son secret.

La signature électronique garantit l'intégrité des informations transmises et la non répudiation.

Les protocoles d'authentification permettent d'empêcher un tiers d'usurper l'identité d'une autre personne.

La cryptographie à clé symétrique ou à clé secrète

La même clé qui sert à la fois à chiffrer et à déchiffrer un message :

- La difficulté est donc de transmettre cette clé secrète à la personne avec qui l'on veut établir des communications confidentielles
- Il faut détenir autant de clés secrètes que de personnes avec qui l'on dialogue, et conserver de façon très sécurisée toutes ces clés secrètes

La cryptographie à clé publique

La cryptographie à clé publique est une méthode utilisée pour transmettre et échanger des messages de façon sécurisée (authentification de l'émetteur, garantie d'intégrité et garantie de confidentialité) :

- Chaque personne engagée dans une transaction est munie d'une "clé secrète" ou "clé privée" et d'une "clé publique"
- La clé secrète ne doit être communiqué à personne, tandis que la clé publique est transmise à tous les interlocuteurs, sans aucune restriction

La cryptographie à clé publique

m = Message => m = Cpub(Cpriv (m)) et m = Cpriv(Cpub (m))

1) Un message codé avec une clé privée ne peut être décodé que par la clé publique associée

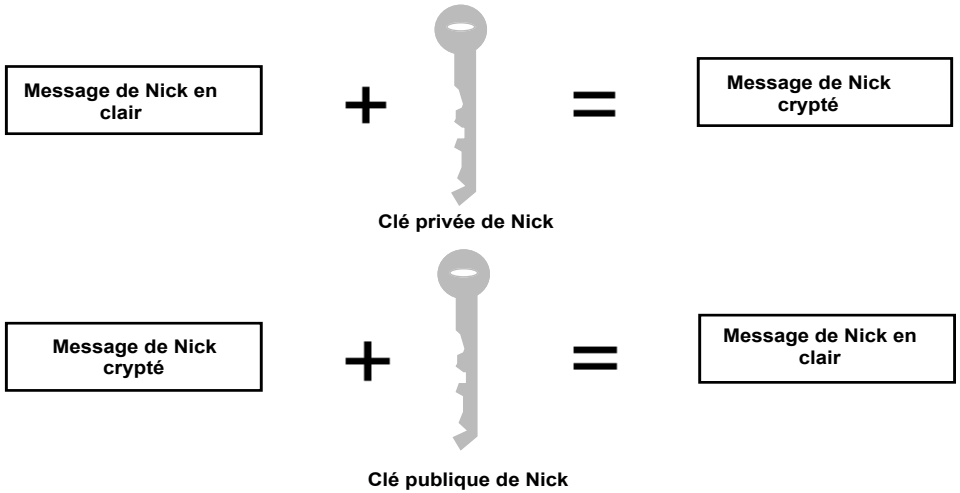
2) Un message codé avec une clé publique ne peut être décodé que par la clé privée associée

3) Une clé publique donnée ne peut être associée qu'à une seule clé privée

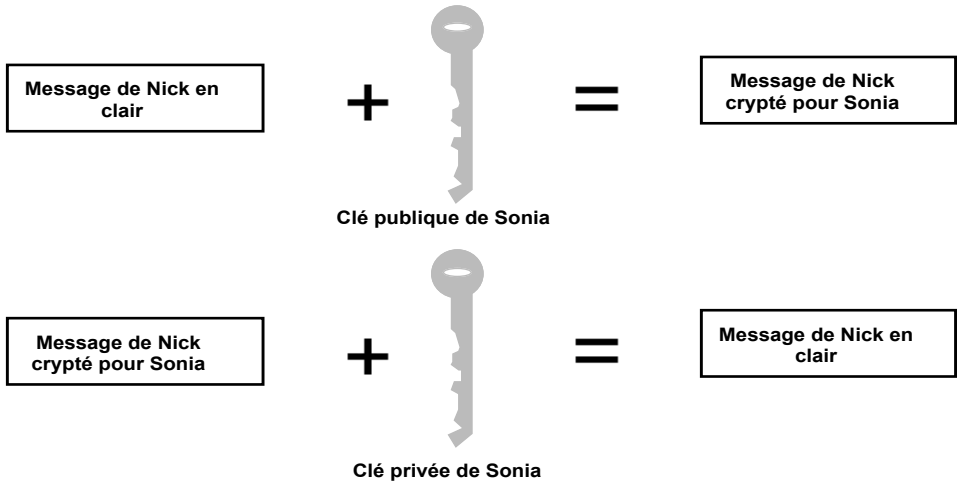
4) Seule la clé publique peut être utilisée pour chiffrer le message et seule la clé privée correspondante peut être utilisée pour le déchiffrer

5) Il est virtuellement impossible de déduire la clé privée si on ne connaît pas la clé publique

La cryptographie à clé publique



La cryptographie à clé publique



La cryptographie à clé publique

Algorithme RSA :

choisir p, q deux grands nombres premiers

calculer n = p*q

choisir e premier avec (p-1)(q-1)

La clé publique est (n, e)

calculer d tel que $e*d \equiv 1 \mod ((p-1)(q-1))$ ou

encore $d = e^{-1} \mod ((p-1)(q-1))$

La clé secrète est (d, n)

Chiffrement : $c_i = m_i^e \mod n$

Déchiffrement : $m_j = c_i^d \mod n$

Un exemple de clés

Soit 2 nombres premiers au hasard: p = 29, q = 37

- n = pq = 29 * 37 = 1073
- (p-1)(q-1) = (29-1)(37-1) = 1008
- e = 71, choisi au hasard tel que e n'ai aucun facteur en commun avec (p-1)(q-1)
- d = 1079, choisi tel que 71*d mod 1008 = 1

Jeux de clés :

- La clé publique est (e,n) = (71,1073) (=clé d'encryptage)
- La clé privée est (d,n) = (1079,1073) (=clé de décryptage)

Un exemple de codage

Crypter le message "HELLO" :
le message est transformé en la suite des codes ASCII de ses caractères de :

"HELLO" ⇒ m = 7269767679

Découpage de m en blocs comportant moins de chiffres que m (ici 4 chiffres), donc découpage de m en blocs de 3 chiffres (complété avec des zéros) :

m = 726 976 767 900

Chaque bloc est crypté :

726^71 mod 1073 = 436
976^71 mod 1073 = 822
767^71 mod 1073 = 825
900^71 mod 1073 = 552

Le message encrypté est :

m = 436 822 825 552

Un exemple de codage

Le message encrypté m = 436 822 825 552 est décrypté avec d:

436^1079 mod 1073 = 726
822^1079 mod 1073 = 976
825^1079 mod 1073 = 767
552^1079 mod 1073 = 900

Ce qui donne la suite de chiffre :

m = 726976767900

Les zéros terminaux sont supprimés :

m = 7269767679

ou :

m = 72 69 76 76 79

ce qui traduit en caractères donne le message "HELLO"

Exemples tirés du livre "Applied Cryptography" de Bruce Schneier (John Wiley & Sons)

Clés

Le nombre de bits d'une clé correspond à la taille de la clé, plus la taille d'une clé est importante, plus cette clé est inviolable

Lorsque l'on parle de clés de :

- 40 bits, 56 bits ou 128 bits, il s'agit de "clés de session", symétriques ("clé DES de 40 bits")
- 512 bits, 1024 ou 2048 bits, il s'agit de "clés de signature" ou de "clés de chiffrement de clés de session", utilisées par des algorithmes asymétriques ("clé RSA de 512 bits")

Il est plus rapide de chiffrer un message avec une clé symétrique qu'avec une clé asymétrique de résistance comparable : la clé de session (symétrique) est donc chiffrée avec la clé publique du destinataire et transmise au destinataire en toute confidentialité

Clés

Le nombre de clés nécessaires en fonction du nombre n d'utilisateurs est de :

- n(n-1)/2 pour les clés secrètes
- 2n pour les clés privées et publiques

La principale difficulté est la distribution des clés

Il y a un risque qu'une personne prétende être une autre personne lors de la génération des clés

Ce problème de distribution des clés a donné naissance aux certificats

Certificats

La problématique centrale de la cryptographie à clé publique (pour signer ou chiffrer un message) est la probité de la clé publique reçue de son interlocuteur, ou rapatriée depuis un annuaire partagé

Les certificats, aussi appelés identifications numériques, résolvent ce problème

Un certificat est un document électronique qui associe le nom d'une personne (personne physique, personne morale, site web, routeur) à une clé publique

Un tel certificat doit être émis par une institution reconnue

Certificats

Certificat Personnel	Certificat Serveur
Nom de son propriétaire : Jean Dupont (adresse e-mail : jdupont@societe.fr)	Nom de domaine du serveur: www.societe.fr
Adresse physique de la société, fonction de Jean Dupont, etc...	Nom et adresse physique de la société, etc...
La clé publique de Jean Dupont à certifier	La clé publique du serveur à certifier
La date d'expiration du certificat	La date d'expiration du certificat
Un numéro de série unique	Un numéro de série unique
Le nom de l'Autorité de Certification qui a délivré le certificat numérique	Le nom de l'Autorité de Certification qui a délivré le certificat numérique
La signature de l'Autorité de Certification (clé publique de l'Autorité de Certification)	La signature de l'Autorité de Certification (clé publique de l'Autorité de Certification)

Certification électronique

Autorité Administrative
Elle définit et fait appliquer la politique et les procédures de certification

Autorité d'enregistrement
Elle vérifie les validités des données du demandeur ainsi que les contraintes liées à l'usage de certificats conformément à la politique de certification
Elle peut demander la révocation d'un certificat

Autorité de certification
Elle valide les informations relatives à l'utilisateur fiable et rajoute des informations supplémentaires si nécessaires puis, construit le certificat suivant le format demandé et le signe avec sa clé privée
Elle peut également demander la révocation de certificats (publication de la liste)
Deux autorités de certification ont la possibilité de se certifier mutuellement (chacune signant le certificat de l'autre) ce qui permet d'introduire un lien de confiance fort entre les utilisateurs de ces deux autorités de certifications

Certification électronique

Autorité d'Horodatage
Elle délivre des contremarques de temps sur les données qui lui sont présentées et garantit ainsi la date qui est apposée sur tous les documents et les signatures issus de l'Autorité de certification

Service de publication
Il a pour fonction de publier des certificats validés ainsi que des listes de certificats révoqués (les certificats doivent être sauvegardés en dehors du service de publication)

Tiers de séquestre
Il s'agit d'un tiers de confiance, dont la fonction est d'offrir la possibilité aux utilisateurs ayant perdu leur clé privée de chiffrement (qui permet de rendre les données indéchiffrables pour tout autre utilisateur que le destinataire du message), de pouvoir déchiffrer les documents
La confiance est ici très importante, car cette entité est potentiellement capable de déchiffrer l'ensemble des messages d'un de ses utilisateurs

Certification électronique

Acteurs français

- Agence pour les technologies de l'information et de la communication dans l'administration (ATICA) qui est chargé de produire des référentiels communs aux administrations
- Direction Centrale de la sécurité des systèmes d'informations (DCSSI) qui est l'organisme national de certification
- Minefi qui est l'organisme gouvernemental chargé des orientations politiques dans le domaine des télécommunications et qui est un utilisateur des moyens nouveaux pour son fonctionnement propres est ses relations avec tous les assujettis à l'impôt,
- Comité français d'accréditation (COFRAC) est en charge de la procédure d'accréditation des CESTI (Centre d Evaluation de la Sécurité des Technologies de l'Information) avant un agreement par la DCSSSI. Il est le correspondant français de European Accreditation et International Accreditation Forum
- Le Groupement d'intérêt public "Modernisation des déclarations sociales" (GIP-MDS) a pour mission de créer les conditions permettant aux entreprises d'effectuer leurs déclarations sociales réglementaires et contractuelles à l'aide d'outils économiques, performants, simples d'installation et ergonomiques, en utilisant notamment les technologies de l'Internet. Net-entreprises est un service proposé aux entreprises pour leur permettre d'effectuer, par Internet, leurs déclarations sociales aux organismes de protection sociale

Certification électronique

Les IGC (infrastructures de gestion de clés ou PKI) sont des infrastructures techniques simples : annuaires, boite noire de fabrication de certificats et des interfaces d'accès à la boite noire

On distingue 4 grandes catégories de IGC :

- IGC attachées à un environnement bureautique
- IGC multi usages qui intègrent plus ou moins de fonctionnalités et proposent de mettre en œuvre du SSO (Single Sign On)
- Les logiciels Open Sources (logiciels libres) qui offrent une interface très rudimentaire mais incluent l'ensemble des fonctionnalités d une IGC
- Les IGC infogérées : le prestataire de services fournit une interface d'accès à l'autorité de certification pour la création de nouveaux certificats et leur révocation ainsi qu'une interface LDAP pour la publication des données publiques des certificats

L'utilisation des IGC est subordonnée à la confiance qu'y mettront les utilisateurs, d'où la nécessité du contrôle de la qualité des solutions de IGC

Créer un certificat

OpenSSL permet de créer une clé:

```
#openssl genrsa -des3 1024 >www.monsite.ext.key
#chmod 400 www.monsite.ext.key
```

Pour créer un certificat provisoire, il faire une requête de certification:

```
#openssl req -new -key www.monsite.ext.key -out www.monsite.ext.csr
```

Puis créer le certificat:

```
#openssl req -x509 www.monsite.ext.key -in www.monsite.ext.csr -out www.monsite.ext.crt
```


Obtenir un certificat

Pour obtenir un certificat "signé", il faut demander en faire la demande à un organisme de certification comme:

```
www.certplus.fr
www.verisign.com
www.certinomis.com…
```

qui réclamera des informations prouvant l'indentité (Kbis…) et la possession du nom de site, puis lui envoyer le fichier:

```
www.monsite.ext.csr
```

A l'issue de cet enregistrement, l'organisme est en mesure de "certifier" la clé publique du site (authentification)

Hachage

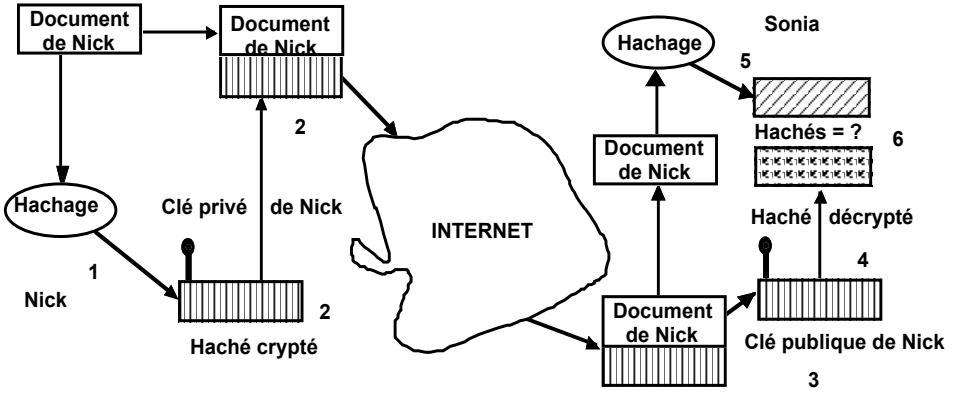
Une fonction de hachage permet la conversion d'une chaîne de caractères de longueur quelconque en une chaîne de caractères de taille inférieure et généralement fixe

Les propriétés des fonctions de hachage à sens unique sont telles que :

- il n'est pas possible de trouver un autre message ayant le même haché
- toute modification, même infime, entraîne la modification du haché

Les algorithmes de hachage les plus utilisé sont MD5, SHA-x (fonctions en PHP)

Signature électronique



Situation juridique

Une proposition de directive de la Commission européenne publiée le 23 octobre 1998 au Journal Officiel des Communautés Européennes, donne à la signature électronique la valeur de preuve jusqu'ici réservée uniquement à la version manuscrite

Le rapport du Conseil d'Etat propose une définition juridique de la signature, qui n'était pas encore inscrite dans le droit positif : "une signature identifie le signataire et manifeste son consentement au contenu de l'acte auquel elle est attachée, et aux obligations qui en découlent"

Situation juridique

La législation a été adaptée en tenir compte de ces remarques, en mars 1999 :

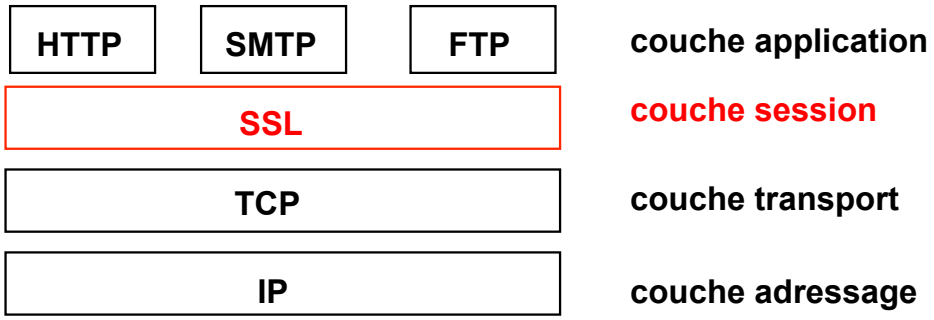
La taille des clés passe à 128 bits (chiffrement à clé publique)

Le 14 mars 2000, une loi adapte le droit de la preuve aux technologies de l'information :

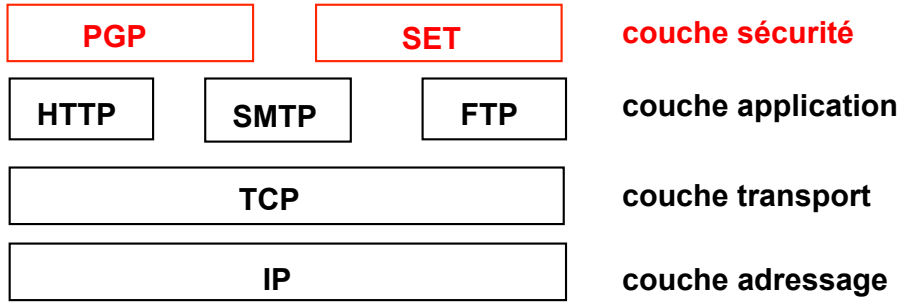
C'est la reconnaissance dans le droit positif Français de la signature électronique

Depuis 2000, en Europe, la signature électronique a valeur de preuve

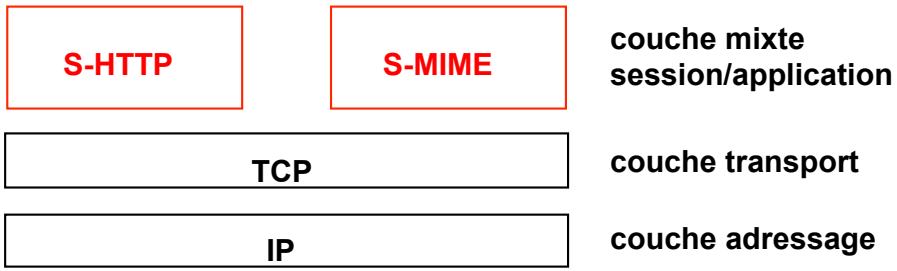
Protocoles de sécurité



Protocoles de sécurité



Protocoles de sécurité



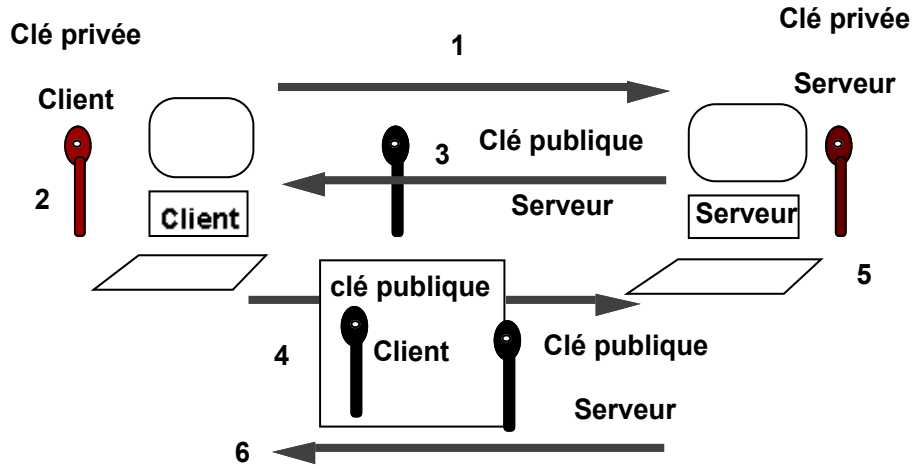
SSL

Le protocole SSL (Secure Socket Layer) a été inventé par Netscape et RSA labs et utilise la technologie de la cryptographie des clés publique/privée

SSL effectue la gestion des clés et l'authentification du serveur avant que les informations ne soient échangées

SSL correspond à une sorte de tuyau sécurisé dans lequel circule l'ensemble des échanges entre client et serveur

SSL



SSL

1. Un utilisateur quelconque utilise un navigateur et entre en communication avec un logiciel serveur. Le serveur possède déjà sa paire de clés publique/privée
2. Le logiciel client, une fois reconnu par le logiciel serveur, génère une paire de clés publique/privée
3. Le logiciel client demande au logiciel serveur de lui fournir sa clé publique (celle du serveur)
4. La clé publique du client est aussitôt chiffrée avec la clé publique de serveur et transmise au serveur
5. Le serveur décode le message avec sa clé privée serveur et authentifie la clé publique de l'utilisateur
6. Le serveur envoie ensuite au logiciel client une confirmation, chiffrée, du bon déroulement de l'opération

SSL

SSL est complètement transparent pour l'utilisateur

Toutes les informations transmises entre l'utilisateur et le serveur sont chiffrées

Seul ce serveur peut communiquer avec cet utilisateur puisqu'il est le seul à connaître la clé publique de cet utilisateur

Une nouvelle paire de clés étant générée à chaque établissement de communication, l'utilisateur et le serveur peuvent maintenant échanger des données de façon sûre

En aucun cas le serveur ne peut s'assurer de l'identité de l'utilisateur à l'autre extrémité sans un système de validation, comme le numéro d'identification personnel (NIP) obtenu par une inscription préalable

La version SSL v3.0 permet l'authentification du serveur et du client (si ce dernier est muni d'un Certificat Personnel)

SSL

En PHP, les fonctions de cryptage sont réunies dans 2 packages: mcrypt et mhash (cvs.php.net)

Le port standard de SSL est le port 443 et le préfixe: `https://`

Pour Apache, il existe un module "mod_ssl" (www.modssl.org) et une bibliothèque "OpenSSL" (www.openssl.org)

Configurer mod_ssl avec une zone sécurisée:

```
<directory /home/www/mesdocs/securise/>
SSLrequireSSL
</directory>
```

Les clés sont stockées dans : `/usr/local/apache/conf/ssl`