

Université de Guelma
Département Informatique

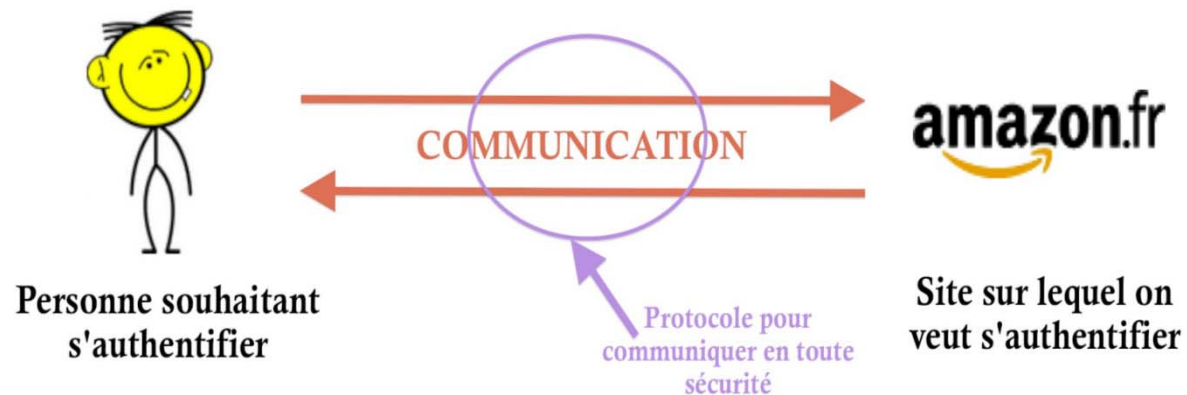
Chapitre 2 : Les protocoles de sécurité

Cours - Sécurité Informatique
3 année LMD Système d'Information

Par : Dr. M. A. Ferrag

Qu'est-ce qu'un protocole de sécurité ?

- Ensemble de règles régissant le comportement d'individus pour répondre aux besoins d'une application (paiement en ligne, vote électronique, authentification d'individus, etc)

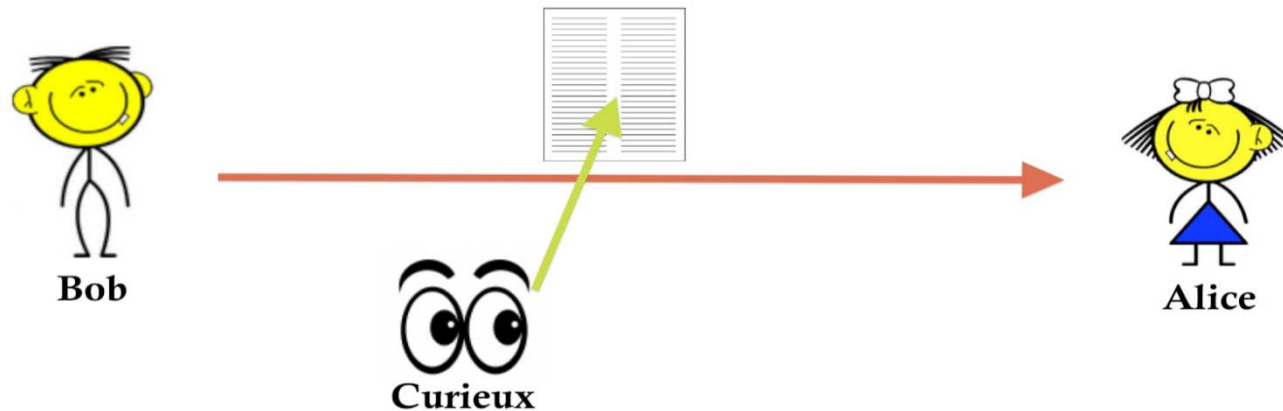


L'utilisation des protocoles est transparente pour l'utilisateur

Sécuriser les messages

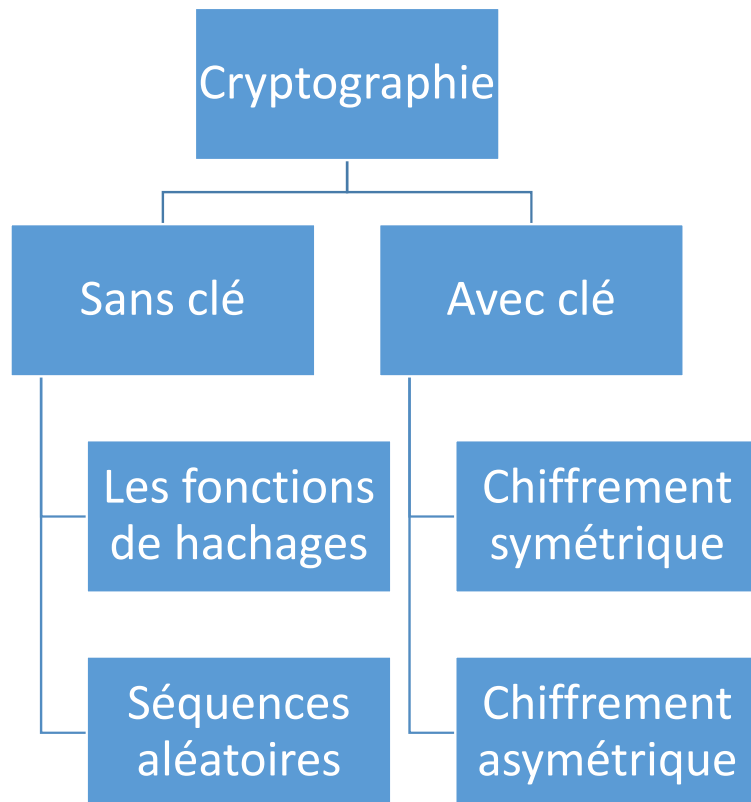
- Communication entre 2 individus A et B --- **échange de messages**Besoin que ces messages soient chiffrés pour garantir leur confidentialité
- Exemple : Durant leurs cours, Alice et Bob, qui ne sont pas côte à côte dans la classe, communiquent en se faisant passer des petits mots.

Problème : n'importe qui peut lire le mot...






Utilisation de la cryptographie

La cryptographie



- **Chiffrement symétrique** : chiffrement plus rapide, mais nécessite de se "rencontrer" pour pouvoir s'échanger la clé commune.
- **Chiffrement asymétrique** : algorithmes de cryptages plus complexes, donc plus lent, mais communication sans échange préalable de clé.
- Les fonctions de hachage sont généralement utilisées pour garantir l'intégrité.

Garantir son identité

- Authentification de Bob : $\{\text{Bob.MotdePasse}\}_{K_{BA}}$,
avec K_{BA} la **clé partagée** par Bob et .
- Ils doivent donc d'abord **s'échanger** cette clé partagée.
- Pour cela, on doit commencer par un chiffrement **asymétrique**.
⇒ Bob doit donc connaître la clé publique d' .
- **Problème** : comment obtenir cette clé et être sûr que c'est la bonne ?
⇒ Bob doit être sûr qu'il communique bien avec .

On connaît donc la clé publique du serveur de certificat (K_S), et on lui demande de nous donner la clé publique d'Amazon (K_A).

Protocole AAA

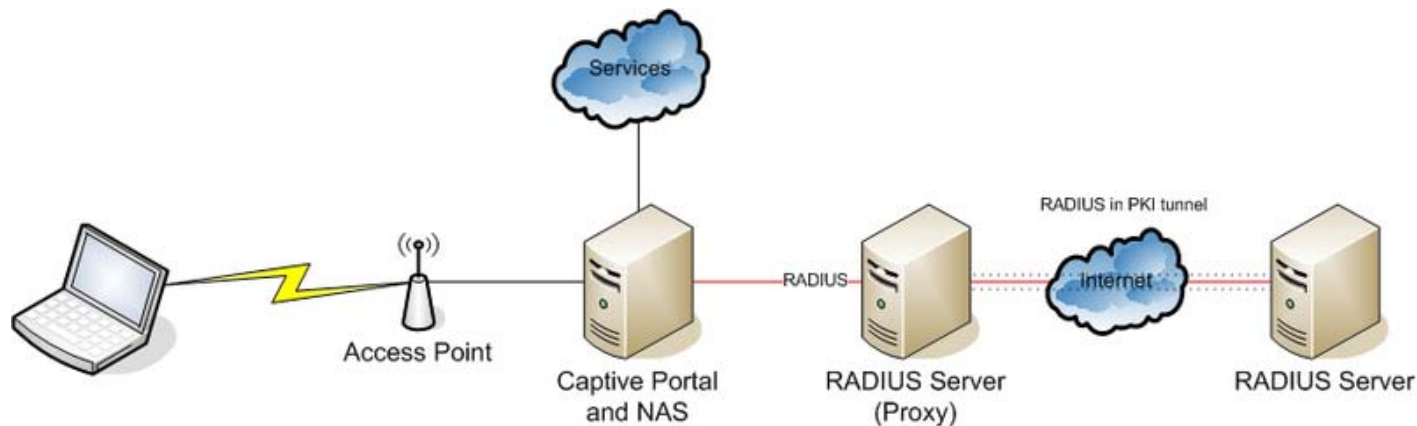
- En sécurité informatique, **AAA** correspond à un protocole qui réalise trois fonctions : l'authentification, l'autorisation, et la traçabilité.
- AAA est un modèle de sécurité implémenté dans certains routeurs Cisco mais que l'on peut également utiliser sur toute machine qui peut servir de NAS (Network Access Server), ou certains switches Alcatel.
- AAA est la base des protocoles de télécommunication Radius et Diameter qui sont notamment utilisés dans les réseaux mobiles UMTS et LTE pour authentifier et autoriser l'accès des terminaux mobiles au réseau.

Liste de protocoles AAA

- **RADIUS**
- **Diameter**
- **TACACS**
- **TACACS+**

RADIUS

- RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification. Le protocole RADIUS a été inventé et développé en 1991 par la société Livingston, qui fabriquait des serveurs d'accès au réseau pour du matériel uniquement équipé d'interfaces série ; il a fait ultérieurement l'objet d'une normalisation par l'IETF.

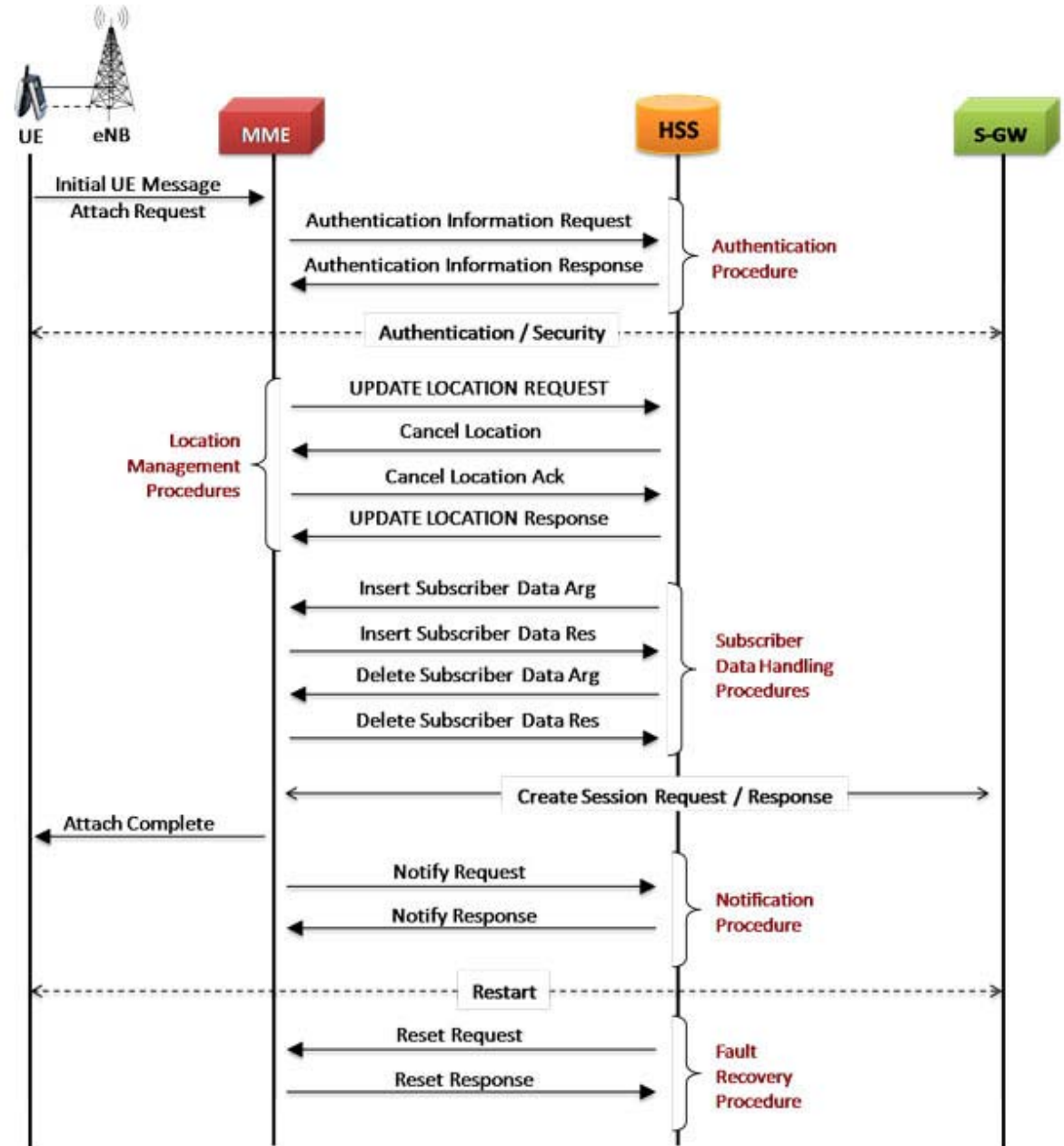


Diameter (1)

- Diameter est un protocole d'authentification, successeur du protocole RADIUS.
- Ce protocole est défini par la RFC 35881, et définit les pré-requis minimums nécessaire pour un protocole AAA.
- Il est notamment utilisé dans le cœur des réseaux de téléphonie mobile pour accéder aux bases de données HLR et HSS permettant d'identifier, d'authentifier et de localiser les abonnés mobiles 3G et LTE /4G.

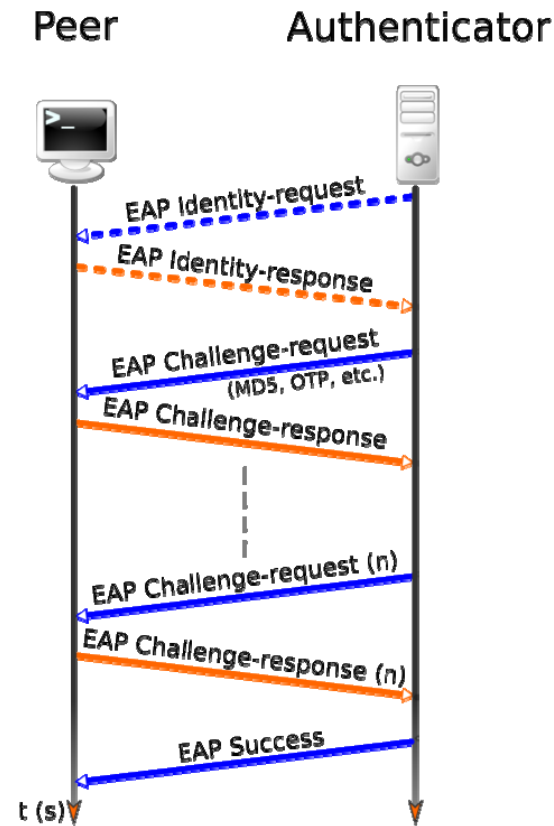
Diameter (2)

- MME (Mobility management entity)
- HSS (Home Subscriber Server)
- S-GW (Gateway)



Le Protocol EAP

- Extensible Authentication Protocol ou EAP est un protocole de communication réseau embarquant de multiples méthodes d'authentification, pouvant être utilisé sur les liaisons point à point (RFC 22841), les réseaux filaires et les réseaux sans fil (RFC 37482, RFC 52473) tel que les réseaux Wi-Fi.
- Plusieurs méthodes d'authentification sont prédéfinies (MD5, OTP, Generic Token Card, etc.) mais il est possible d'en rajouter sans qu'il soit nécessaire de changer ou de créer un nouveau protocole réseau.

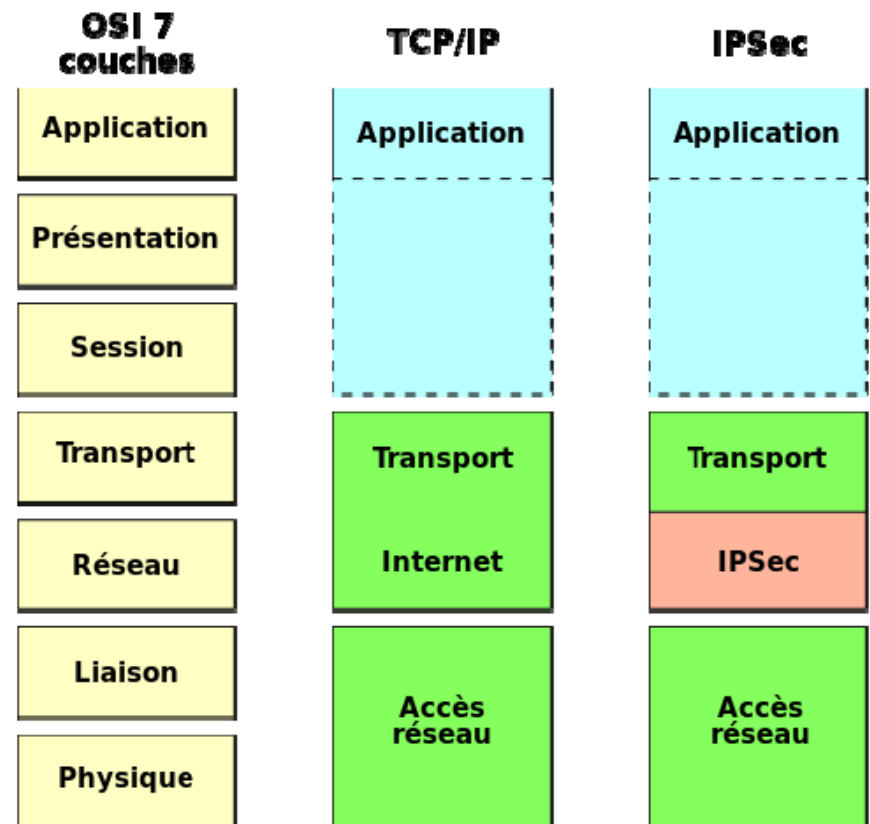


Internet Protocol Security (IPSec) (1)

- IPsec (Internet Protocol Security), défini par l'IETF comme un cadre de standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques
- IPsec se différencie des standards de sécurité antérieurs en n'étant pas limité à une seule méthode d'authentification ou d'algorithme et c'est la raison pour laquelle il est considéré comme un cadre de standards ouverts

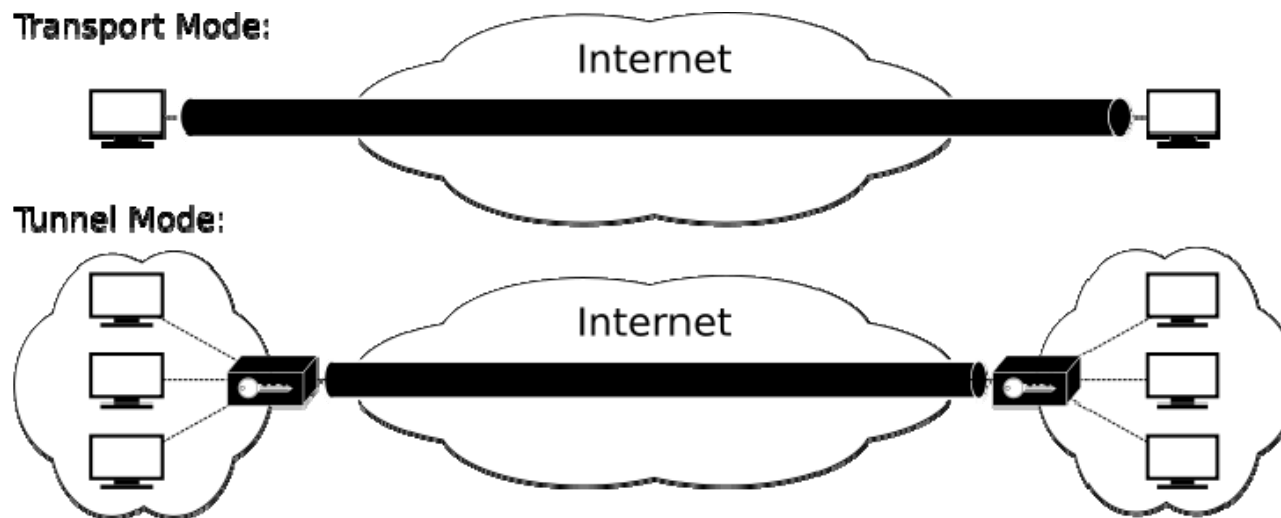
Internet Protocol Security (IPSec) (2)

- IPsec opère à la couche réseau (couche 3 du modèle OSI) contrairement aux standards antérieurs qui opéraient à la couche application (couche 7 du modèle OSI), ce qui le rend indépendant des applications, et veut dire que les utilisateurs n'ont pas besoin de configurer chaque application aux standards IPsec.



IPSec - Modes de fonctionnement

- **Mode transport** : Dans le mode transport, ce sont uniquement les données transférées (la partie payload du paquet IP) qui sont chiffrées et/ou authentifiées.
- **Mode tunnel** : En mode tunnel, c'est la totalité du paquet IP qui est chiffré et/ou authentifié.



Le protocole SSL/TLS (1)

- Secure Socket Layer est un protocole légèrement supérieur à la couche 4 du modèle OSI. Il a pour objectif, tel qu'il est défini dans la RFC 2246, de fournir la confidentialité et l'intégrité des données entre deux applications en communication.
- La version actuelle de SSL est la 3.1, connue sous le nom de TLS (Transport Layer Security). Ce changement de nom marque le rachat du brevet SSL par l'IETF, appartenant initialement à Netscape. Nous parlerons donc plutôt de TLS que de SSL, cette nouvelle appellation risquant fort de supplanter la première dans les années qui viennent.

Le protocole SSL/TLS (2)

En pratique, le SSL devrait être utilisé dans les cas suivants :

- Pour sécuriser les transactions bancaires en ligne.
- Pour sécuriser les connexions et tout échange d'information confidentielle .
- Pour sécuriser les applications et les messageries web, telles que Outlook Web Access, Exchange et Office Communications Server.
- Pour sécuriser les flux de production et les applications de virtualisation tels que Citrix Delivery Platforms et les plates-formes sur le Cloud.
- Pour sécuriser les connexions entre un client de messagerie, tel que Microsoft Outlook et un serveur mail, tel que Microsoft Exchange.
- Pour sécuriser le transfert de fichiers au travers de services « https » et FTP, dans les cas de mise à jour de sites Internet par exemple.
- Pour sécuriser les connexions aux panneaux de contrôle et les activités d'hébergement, telles que Parallels, cPanel, et bien d'autres encore.
- Pour sécuriser les traffics intranet.
- Pour sécuriser les connexions aux réseaux et aux traffics de réseaux utilisant les VPNs SSL, tels que VPN Access Servers, et les applications, telles que Citrix Access Gateway.

Le protocole SSL/TLS (3)

```
+-----+
|      |< - - - - - - - - - - -CLIENT HELLO-|1      |
|      | -SERVER HELLO - - - - - - - - - - >|2      |
|      | -CERTIFICATE - - - - - - - - - - >|3      |
|  S    | -CERTIFICATE REQUEST - - - - - - - >|4      |
|  E    | -SERVER KEY EXCHANGE - - - - - - ->|5      | C
|  R    | -SERVER HELLO DONE- - - - - - - ->|6      | L
|  V    |<- - - - - - - - - - - -CERTIFICATE-|7      | I
|  E    |<- - - - - - - - - - - -CLIENT KEY EXCHANGE-|8    | E
|  U    |<- - - - - - - - - - - -CERTIFICATE VERIFY-|9    | N
|  R    |<- - - - - - - - - - - -CHANGE CIPHER SPEC-|10   | T
|      |<- - - - - - - - - - - -CLIENT FINISHED-|11   |
|      | -CHANGE CIPHER SPEC- - - - - - - ->|12   |
|      | -SERVER FINISHED - - - - - - - - ->|13   |
|      |<- - - - - - - - - - - -ENCRYPTED DATA - - - ->|14   |
+-----+
```

La session SSL est établie en suivant une séquence d'échanges d'informations entre client et serveur, comme le montre la Figure . Cette séquence peut varier, selon que le serveur est configuré pour fournir un certificat de serveur ou réclame un certificat client.

Le protocole SSL/TLS (3)

- SSL utilise le chiffrement symétrique conventionnel pour chiffrer les messages au cours d'une session. Il existe neuf choix possibles pour le chiffrement, y compris l'option du transfert non chiffré :
 - Pas de chiffrement
 - Chiffrement en continu (Stream Ciphers)
 - RC4 avec clés de 40 bits
 - RC4 avec clés de 128 bits
 - Chiffrement par blocs CBC (CBC Block Ciphers)
 - RC2 avec clé de 40 bits
 - DES avec clé de 40 bits
 - DES avec clé de 56 bits
 - Triple-DES avec clé de 168 bits
 - Idea (clé de 128 bits)
 - Fortezza (clé de 96 bits)

Certificat numérique X.509

- Un certificat numérique est une sorte de “carte d'identité” d'une entité informatique.

1.Version la version de X.509

2.Serial Number un numéro de série

3.Signature Algorithm les algos qui ont signés le certificat

4.Issuer l'autorité qui a signé le certificat

5.Validity la période de validité

6.Subject le propriétaire du certificat

7.Subject Public Key Info des infos concernant la clé publique

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 3 (0x3)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=FR, ST=Indre-et-Loire, L=Tours, O=Resgate Security
  Department, CN=authority.microgate.fr/emailAddress=security@microgate.fr
  Validity
    Not Before: May 13 15:33:45 2005 GMT
    Not After : May 11 15:33:45 2015 GMT
  Subject: C=FR, ST=Indre-et-Loire, L=Tours, O=Resgate Security
  Department, CN=webmail.microgate.fr/emailAddress=security@microgate.fr
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
    Modulus (2048 bit):
      00:b4:bf:b6:d0:e6:af:30:5e:5f:a4:b8:6c:01:37:
      0e:81:e4:c5:11:6e:08:e8:05:24:0d:30:ef:94:35:
```