

Université de Guelma
Département Informatique

Chapitre 2 : Les protocoles de sécurité (Partie 1)

Cours - Sécurité Informatique
3 année LMD Système d'Information

Par : Dr. M. A. Ferrag

Plan du cours

- **RADIUS**
- **Diameter**
- **EAP**

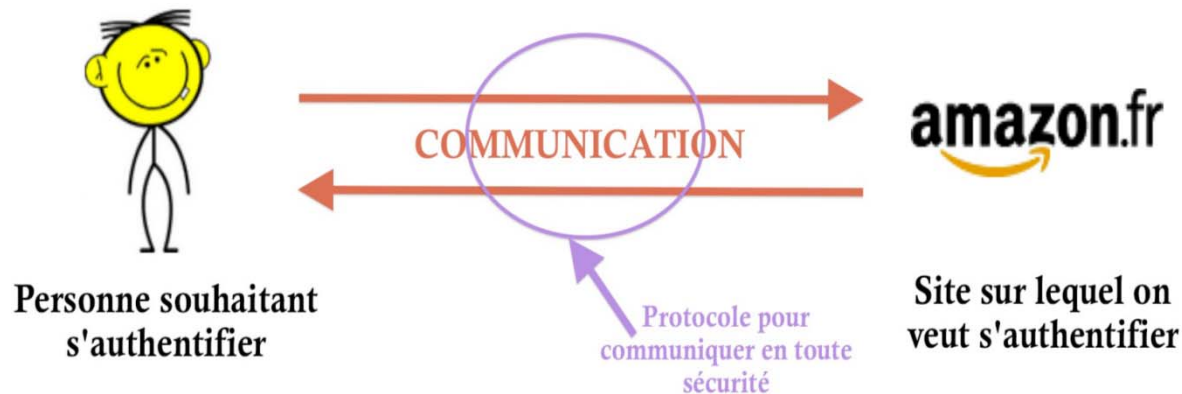
Pourquoi les protocoles de sécurité ?

- Sur internet (paiement en ligne, envoi de mots de passe, ...), ou encore quand on utilise une carte bancaire, on a besoin de :
 - Établir une communication sécurisée entre 2 individus - **Sécurité**
 - Être sûr de communiquer avec la bonne personne, et pas un intrus voulant voler des informations (comme le mot de passe) - **Authentification**
 - Être sûr que les données ne sont pas modifiées en cours de route - **Intégrité**



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)

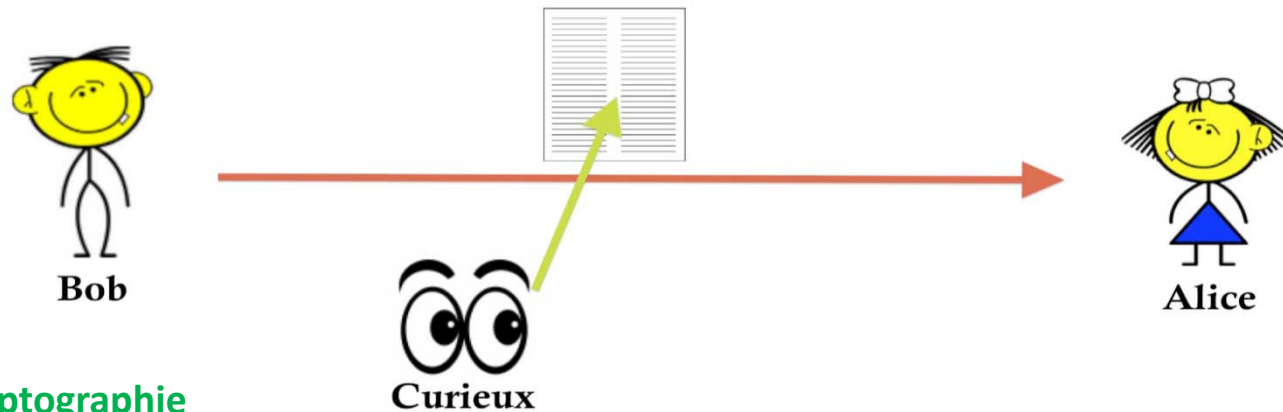


L'utilisation des protocoles est transparente pour l'utilisateur

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

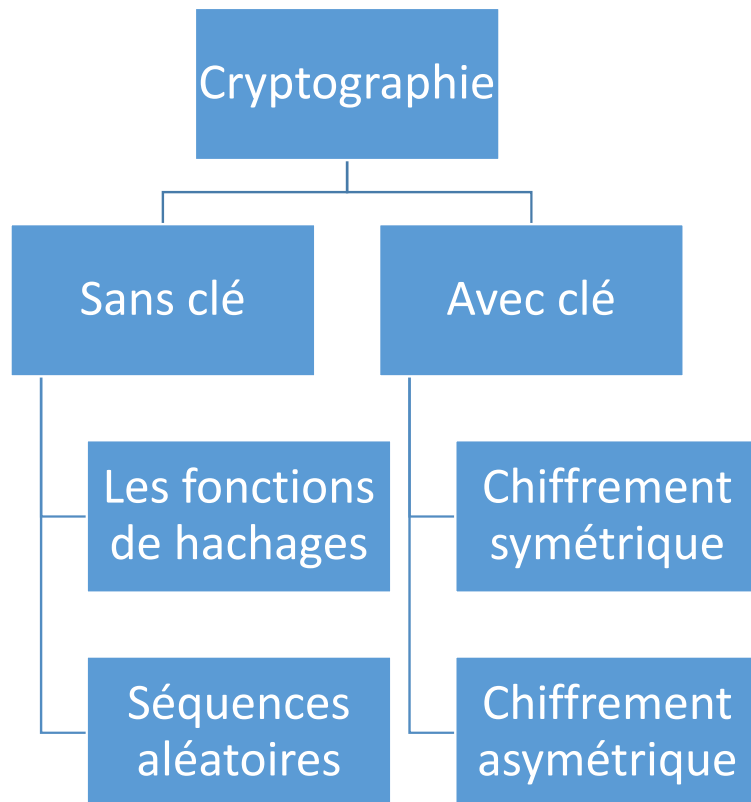
La cryptographie (1)

- Qu'est-ce que la cryptographie ? Un ensemble de méthodes permettant de chiffrer un message numérique, grâce à une clé.

Rend le message incompréhensible pour quiconque ne possédant pas la clé.

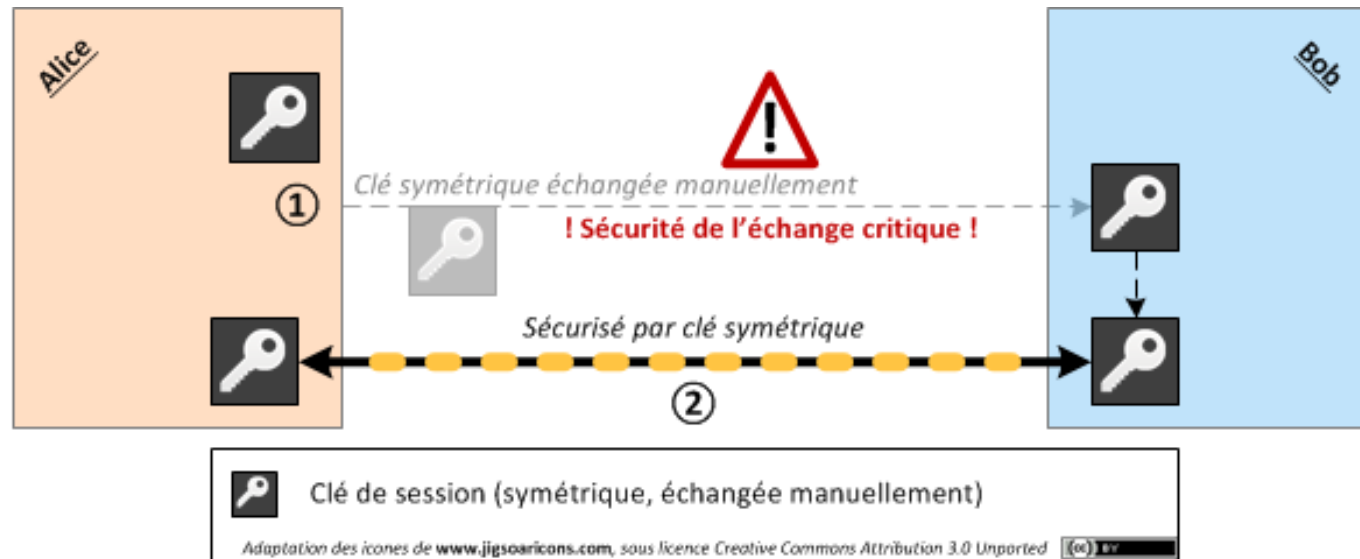
- Chiffrement **symétrique** : une seule clé partagée pour chiffrer et déchiffrer
- Chiffrement **asymétrique** : une clé pour chiffrer, une autre pour déchiffrer

La cryptographie (2)



- **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.

Chiffrement symétrique

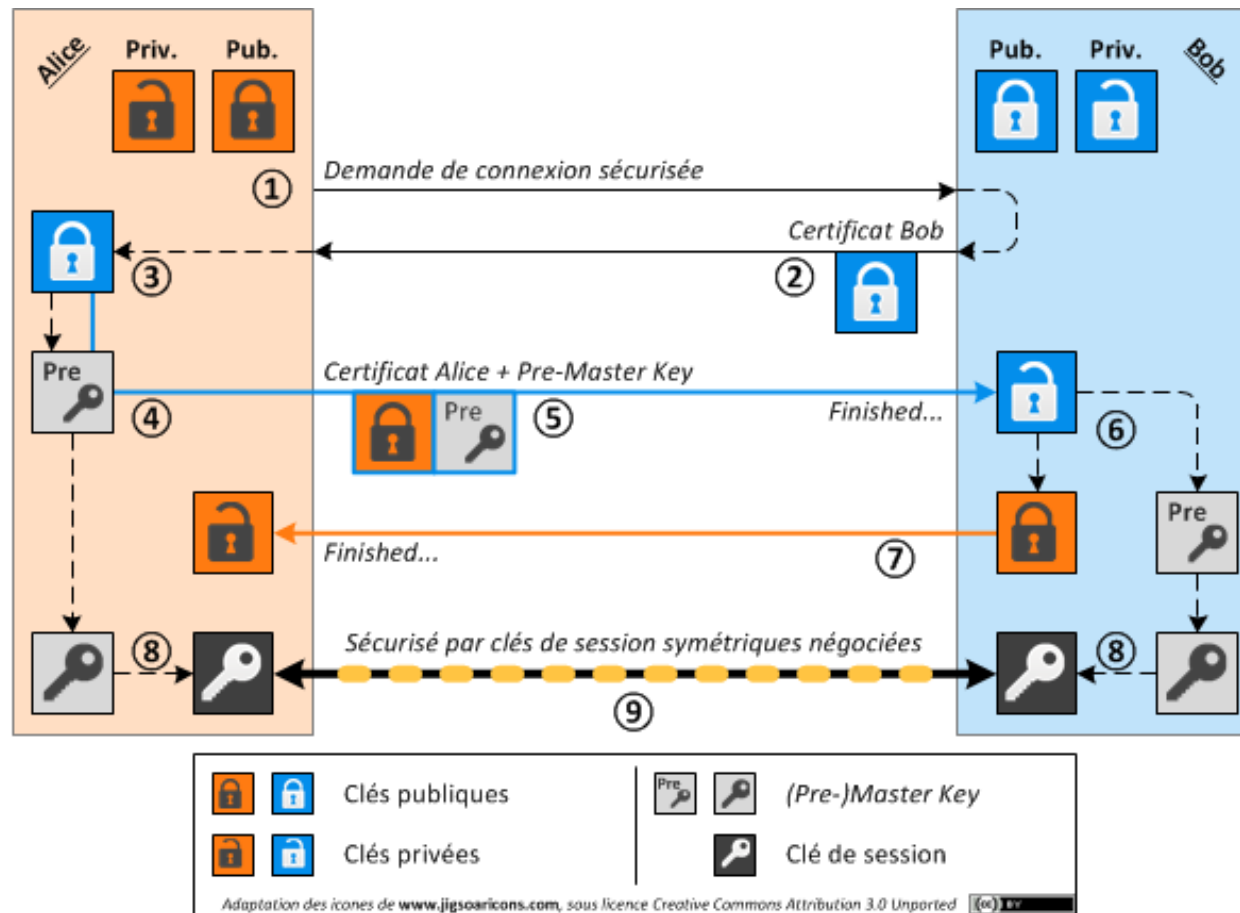


La clé doit être échangée à un moment donné. Et cet échange peut être intercepté, rendant le chiffrement inutile...

La clé est définie par un des participants, et n'est pas renouvelée automatiquement, la rendant plus vulnérable à des attaques par dictionnaire, par exemple.

Source : <https://www.nexcom.fr/>

Chiffrement asymétrique et hybride



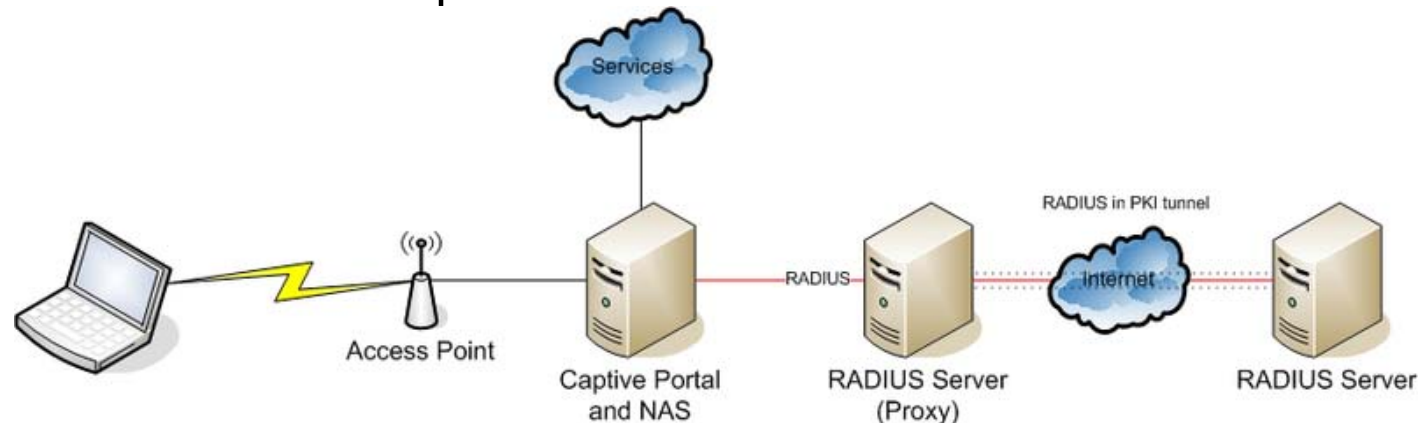
- 1- Alice demande une connexion sécurisée avec Bob.
- 2- Bob transmet, de manière non sécurisée, son certificat, à savoir sa clé publique.
- 3- Alice récupère la clé publique de Bob et authentifie celui-ci. La connexion est refusée si cette identité ne peut être vérifiée.
- 4- Alice génère une Pre-Master Key. Cette clé ainsi que la clé publique d'Alice sont transmises à Bob. Le secret de la Pre-Master Key doit être préservé pour assurer l'efficacité de la méthode.
- 5- Alice possédant la clé publique de Bob, elle l'utilise pour chiffrer son message.
- 6- A la réception du message chiffré, Bob utilise sa clé privée pour déchiffrer le message, chiffré avec sa clé publique par Alice. Il en extrait deux éléments : la clé publique d'Alice et, encore plus important, la Pre-Master Key.
- 7- Bob authentifie Alice à l'aide de sa clé publique. Si l'identité est vérifiée correctement, la négociation est terminée. Ce message peut être transmis de manière sécurisée grâce à la clé publique d'Alice. Celle-ci utilise alors sa clé privée pour décoder le message.
- 8- Dans le même temps, les deux parties génèrent la même clé maître (Master Key) finale via des procédés cryptographiques. De cette clé, ils peuvent en déduire une clé de session identique (et donc symétrique). Cette clé est régénérée régulièrement afin d'éviter les problèmes inhérents aux clés symétriques.
- 9- Cette clé de session symétrique permet de chiffrer efficacement le trafic entre les deux entités, sans la surcharge imprimée par un chiffrement asymétrique.

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.

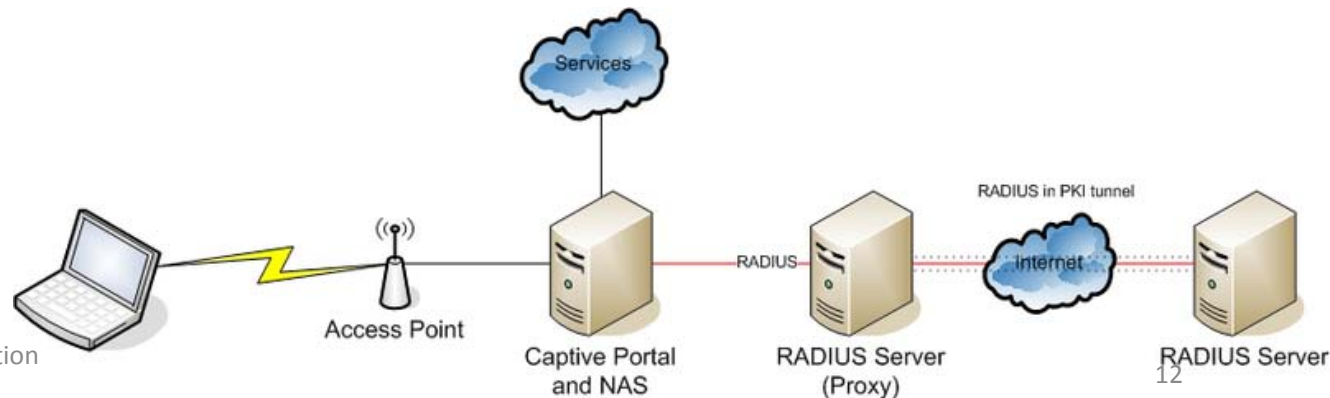
RADIUS - Principes généraux

- Protocole standard d'authentification, initialement mis au point par Livingston.
- Défini au sein des RFC 2865 et 2866.
- Fonctionnement basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau.
- Le protocole RADIUS permet de faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée.



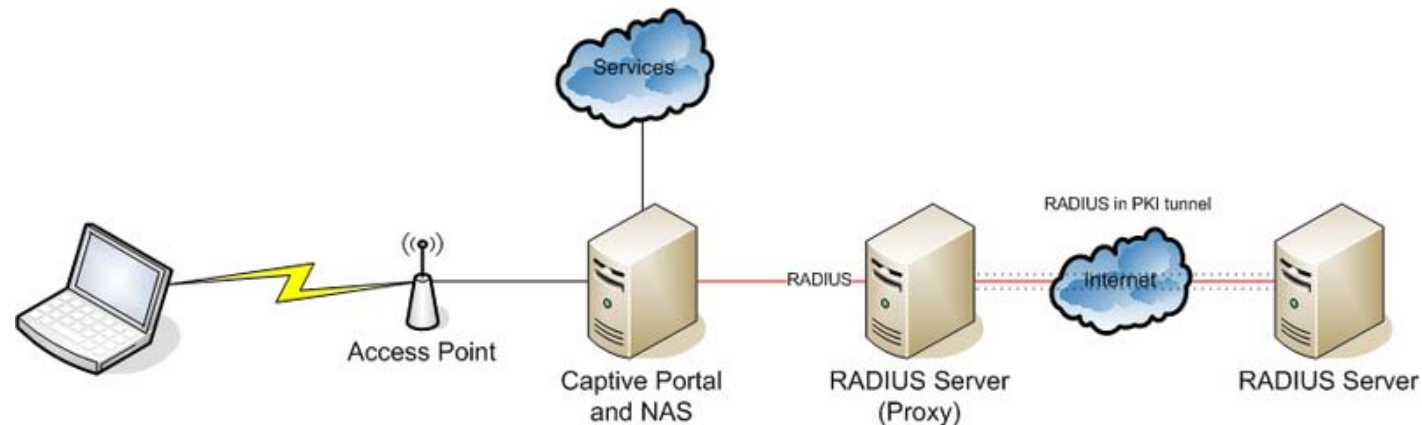
RADIUS - Scénario de fonctionnement (1/2)

- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance.
- Le NAS achemine la demande au serveur RADIUS.
- Le serveur RADIUS consulte sa base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur.
- Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :
 - **ACCEPT** : l'identification a réussi.
 - **REJECT** : l'identification a échoué.
 - **CHALLENGE** : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi ».



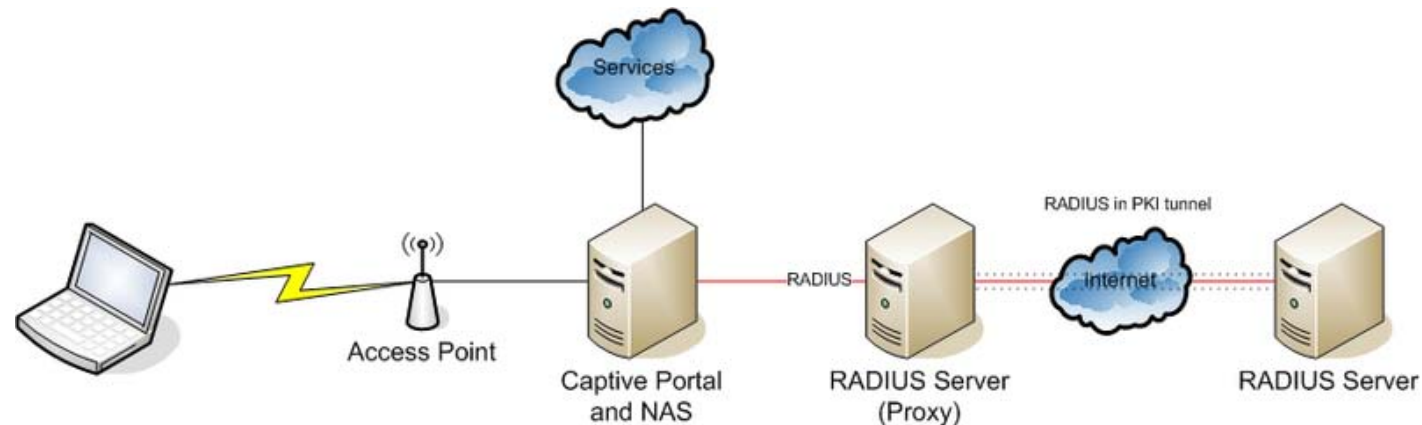
RADIUS - Scénario de fonctionnement (2/2)

- Une autre réponse est possible : **CHANGE PASSWORD** où le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.
- Change-password est un attribut VSA (Vendor-Specific Attributes), c'est-à-dire qu'il est spécifique à un fournisseur.
- Suite à cette phase dit d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.



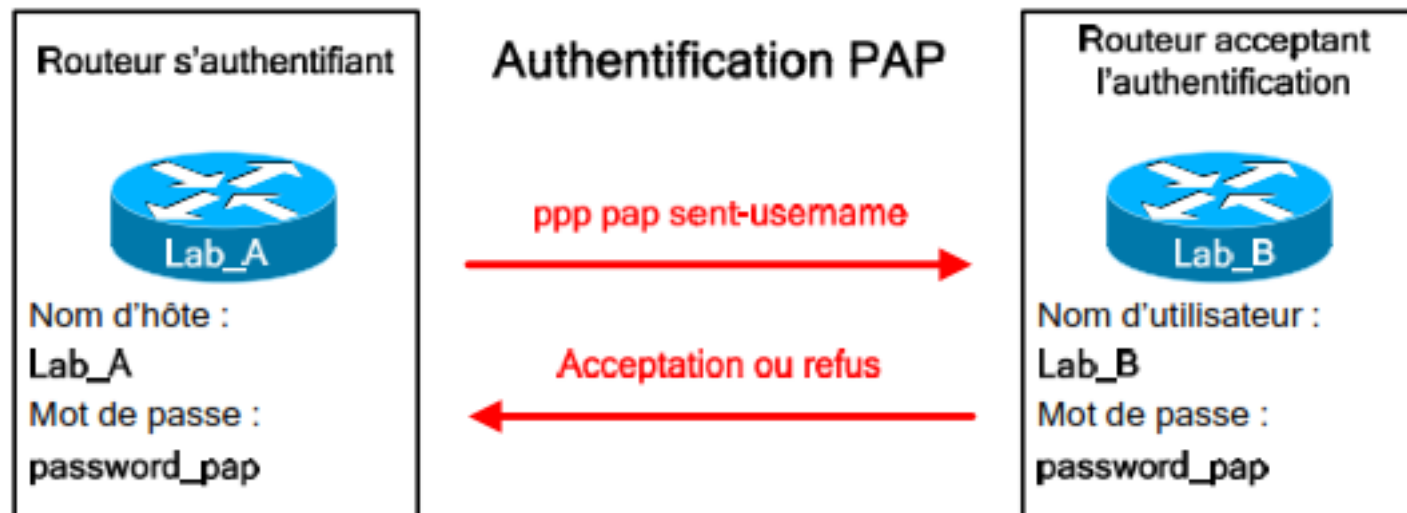
RADIUS - Protocoles de mots de passe

- RADIUS connaît nativement deux protocoles de mots de passe :
 - **PAP (échange en clair du nom et du mot de passe),**
 - **CHAP (échange basé sur un hachage de part et d'autre avec échange seulement du 'challenge').**
- Le protocole prévoit deux attributs séparés : User Password et CHAP-Password.



RADIUS - Protocoles de mots de passe

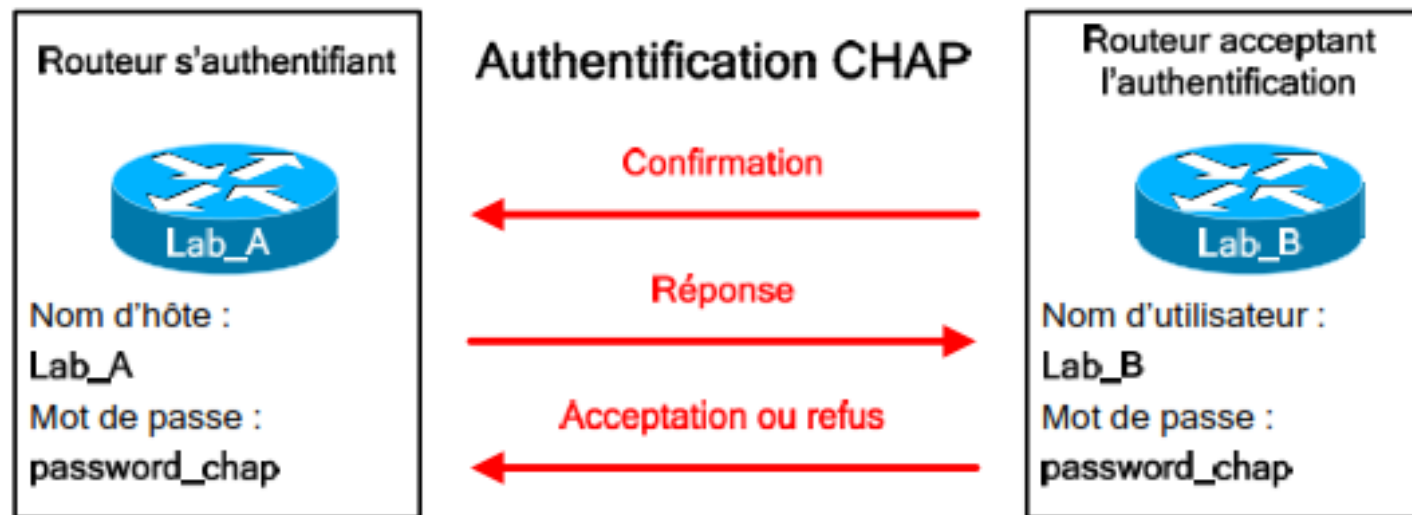
Password Authentication Protocol (PAP)



Point-to-Point Protocol (PPP)

RADIUS - Protocoles de mots de passe

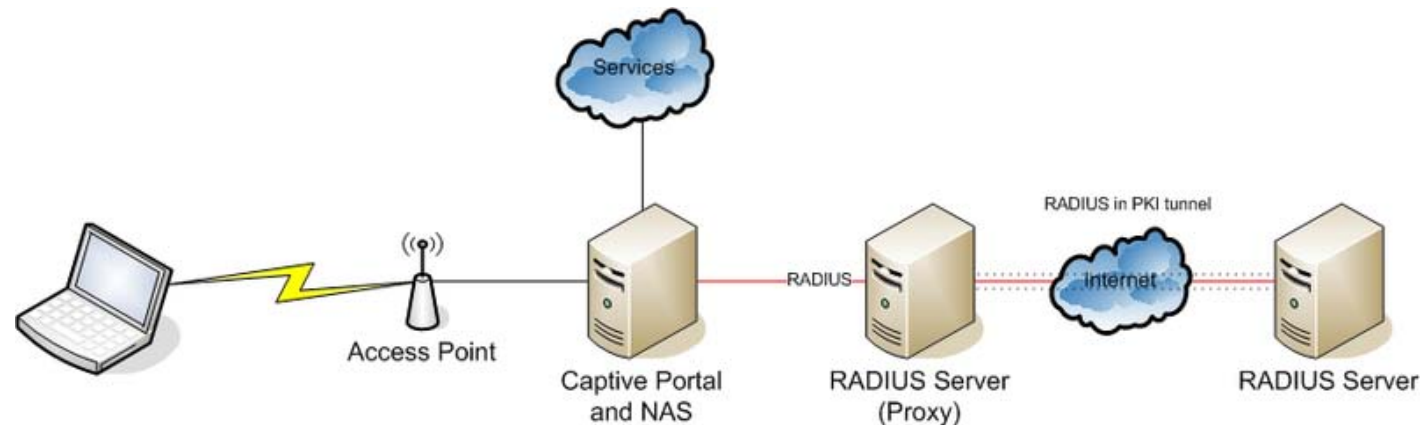
Challenge-Handshake Authentication Protocol



(CHAP) est un protocole d'authentification pour PPP à base de challenge

RADIUS - Protocoles de mots de passe

- RADIUS connaît nativement deux protocoles de mots de passe :
 - **PAP (échange en clair du nom et du mot de passe),**
 - **CHAP (échange basé sur un hachage de part et d'autre avec échange seulement du 'challenge').**
- Le protocole prévoit deux attributs séparés : User Password et CHAP-Password.



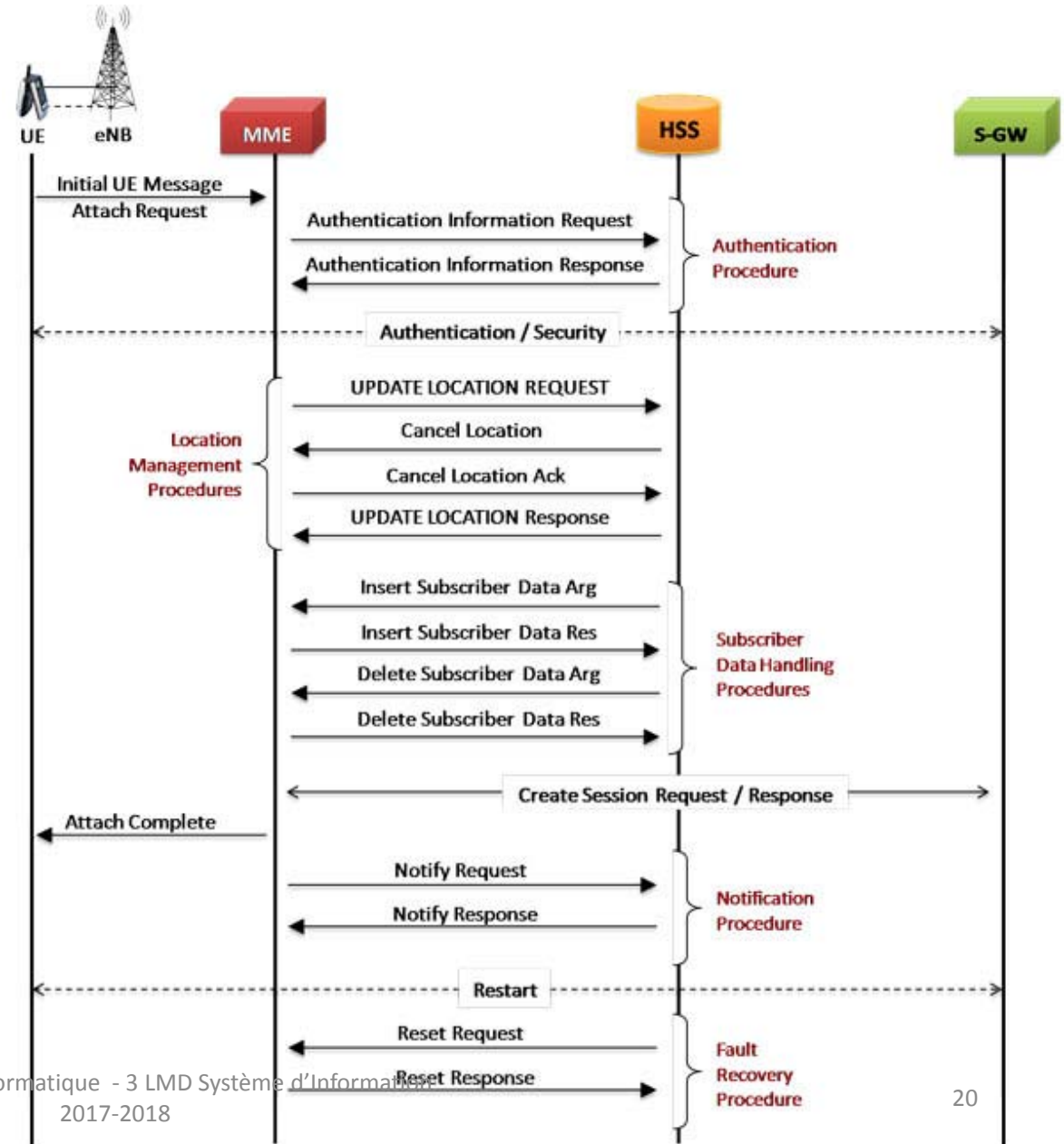
Diameter

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)

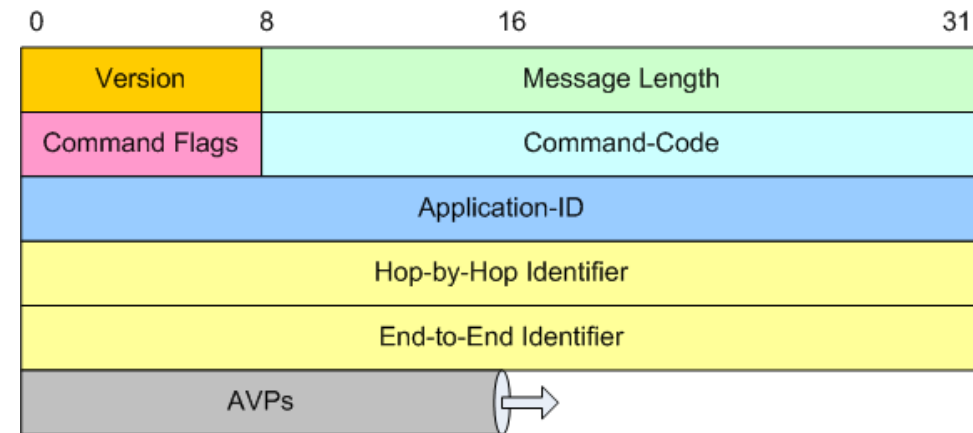
- MME (Mobility management entity)
- HSS (Home Subscriber Server)
- S-GW (Gateway)



Diameter (2) - Structure du message de Diameter

- Le Diameter est un protocole basé sur les messages (paquets). Il existe deux types de messages, à savoir, le message Request et le message Answer. La structure de ces deux messages est présentée dans la figure

- Version : Ce champ de version doit être réglé sur 1 pour indiquer la version 1.
- Longueur du message (Message Length) : Contient la longueur de Message Header + (Data) Avp.
- Drapeaux de commande (Command Flags) : Le champ drapeaux de commandes est de huit bits.
- ID d'application (ID d'application) : Pour identifier de manière unique chaque application.
- Hop-by-Hop Identifier : L'identificateur Hop-by-Hop est un champ entier non signé de 32 bits (en ordre d'octet réseau) et aide à faire correspondre les demandes et les réponses.
- Identificateur de bout en bout (End-to-End Identifier): L'identificateur de bout en bout est un champ entier non signé de 32 bits (en ordre d'octet de réseau) et sert à détecter des messages en double.

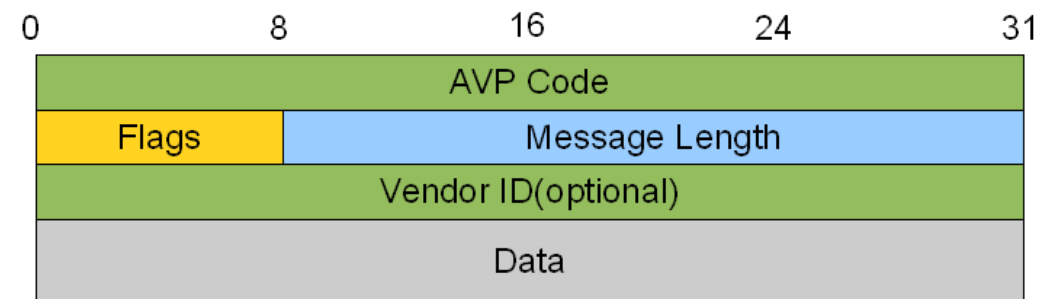


Structure du message de Diameter

Diameter (2) - Les AVP de Diameter

- Les AVP de Diameter sont l'unité de base dans le message Diameter qui contient les données (données d'authentification, données de sécurité, données relatives à l'application, etc.). Il doit y avoir au moins un AVP à l'intérieur du message Diameter. La structure de l'AVP Diameter est présentée dans la figure

- Code AVP (4 octets) : Le code AVP, combiné avec le champ Vendor-Id, identifie l'attribut uniquement. Les numéros AVP 256 et supérieurs sont utilisés pour le Diamètre.
- Drapeaux (Flags) : Indicateurs de bits qui spécifient comment chaque attribut doit être traité. Une description complète est disponible dans la section 4.1 de RFC 3588.
- AVP Longueur (AVP Length): Indique le nombre d'octets dans l'AVP, y compris les informations suivantes: Code AVP, AVP Longueur, Drapeaux AVP, Champ d'identification du fournisseur (s'il y a lieu) et Données AVP.
- Fournisseur ID (Vendor-ID): Un octet optionnel qui identifie l'AVP dans l'espace d'application. Le code AVP et AVP Vendor-ID créent un identifiant unique pour AVP.

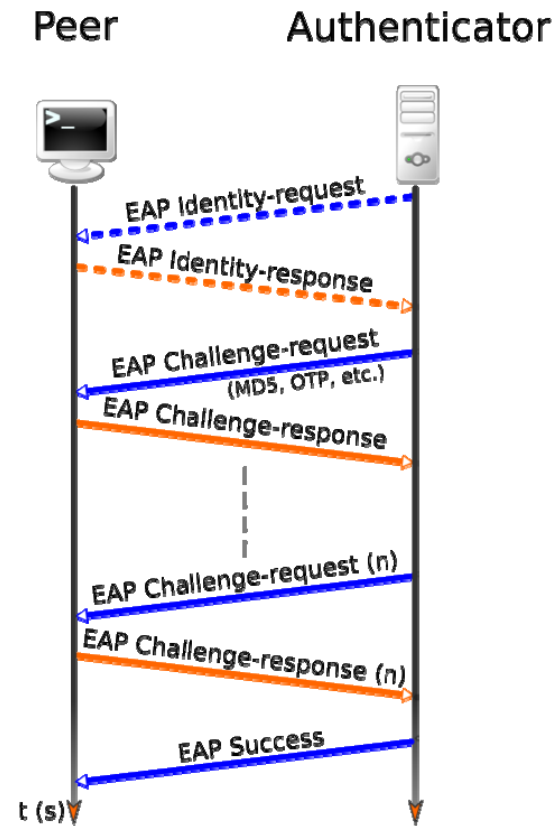


Structure de l'AVP Diameter

Le protocol EAP

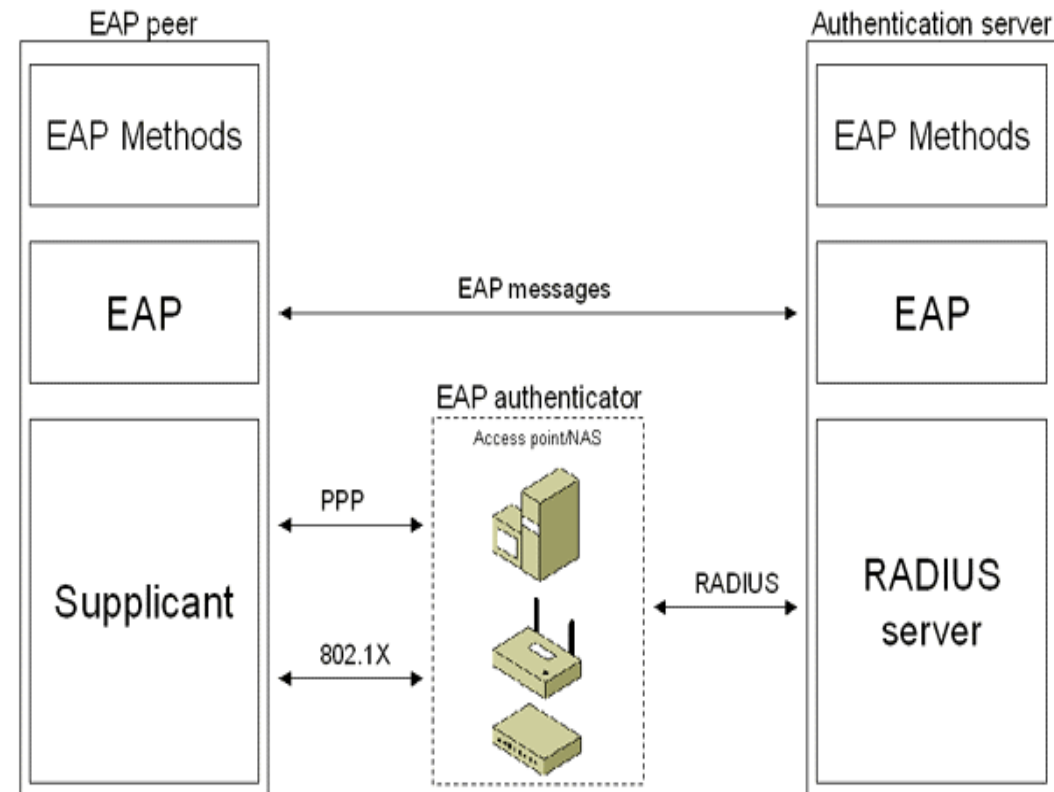
Le Protocol EAP

- 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.



Le Protocol EAP

- D'un point de vue architectural, une infrastructure EAP est constituée des éléments suivants, comme présenté dans la figure :
- *Homologue EAP* : Ordinateur qui tente d'accéder à un réseau, également appelé client d'accès.
- *Authentificateur EAP*: Point d'accès ou serveur d'accès réseau qui nécessite une authentification EAP avant d'accorder l'accès à un réseau.
- *Serveur d'authentification* : Ordinateur serveur qui négocie l'utilisation d'une méthode EAP spécifique avec un homologue EAP, qui valide les informations d'identification de l'homologue EAP et qui autorise l'accès au réseau. En général, le serveur d'authentification est un serveur RADIUS (Remote Authentication Dial-In User Service).



L'infrastructure EAP et le flux d'informations

EAP dans les différentes versions de Windows

La prise en charge EAP dans Microsoft Windows a débuté avec Windows 2000, qui prenait en charge les méthodes EAP suivantes :

- EAP-Message Digest 5 Challenge Handshake Authentication Protocol (EAP-MD5 CHAP)
- EAP-Transport Layer Security (EAP-TLS)
- Security Dynamics' ACE/Agent

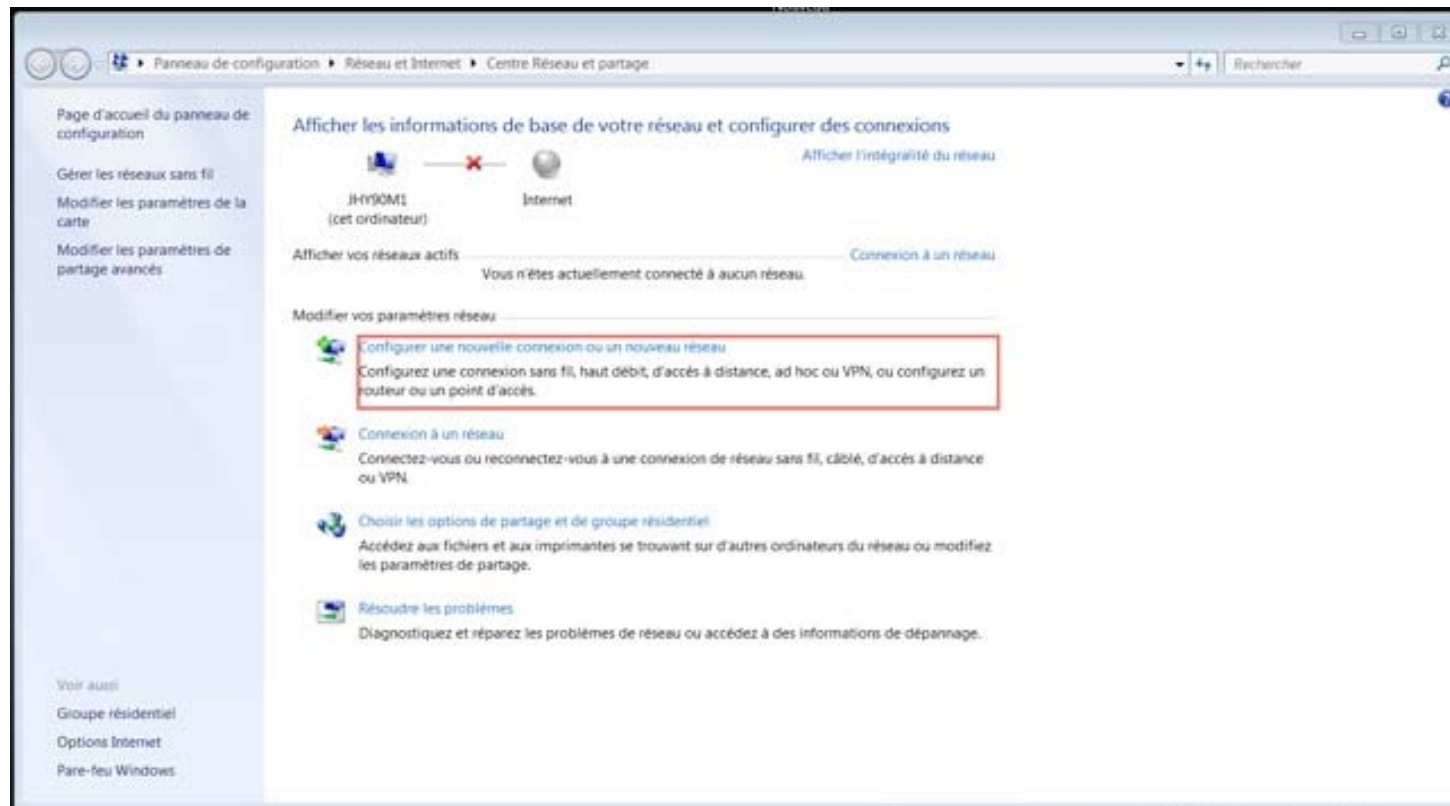
Windows XP Service Pack 1, Windows XP Service Pack 2, Windows Server 2003, et Windows 2000 Service Pack 4 supportent aussi les méthodes EAP suivantes:

- Protected EAP (PEAP)
- PEAP-MS-CHAP v2
- PEAP-TLS

Configuration du protocole EAP (1)

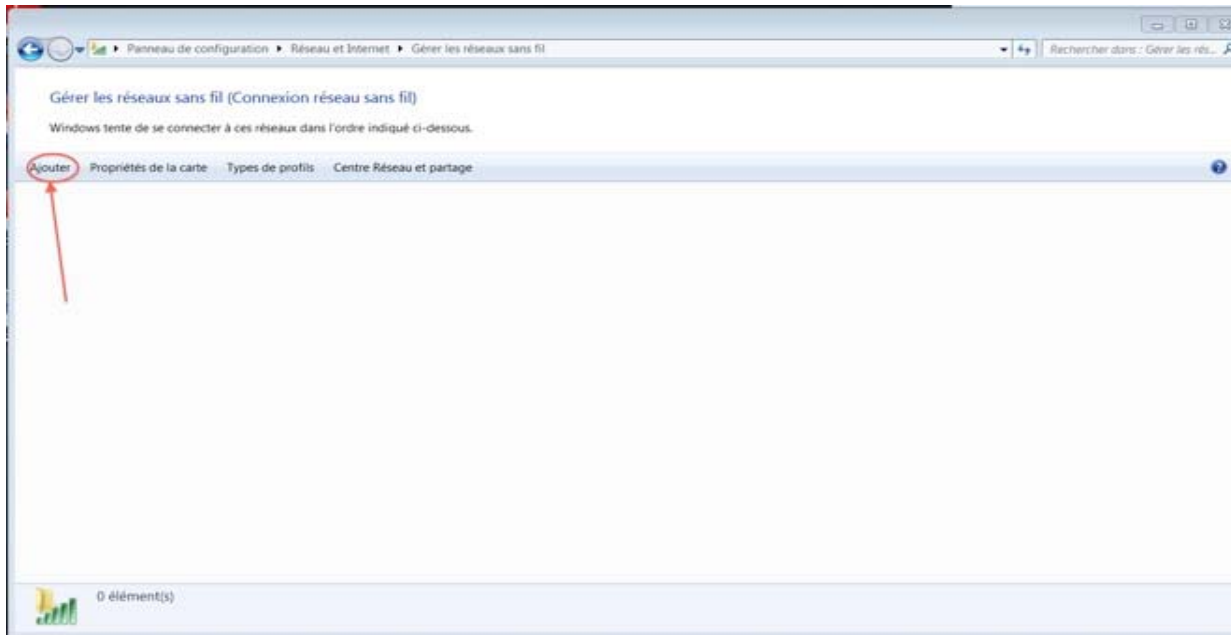
- Pour les ordinateurs exécutant Windows, le client EAP (client d'accès) est un ordinateur qui tente une connexion et le serveur d'authentification est un ordinateur exécutant Windows Server 2003 ou Windows 2000 Server et le service de routage d'authentification Internet (IAS) (pour tous les types de connexions). Dans le reste de cette sous-section, nous allons voir comment configurer du réseau wifi sous windows 7 utilisant le protocole EAP.
- Commencez par aller dans Panneau de configuration -> Réseaux et internet -> Centre réseau et Partage et sélectionnez 'Configurez une nouvelle connexion ou un nouveau réseau'

Configuration du protocole EAP (2)



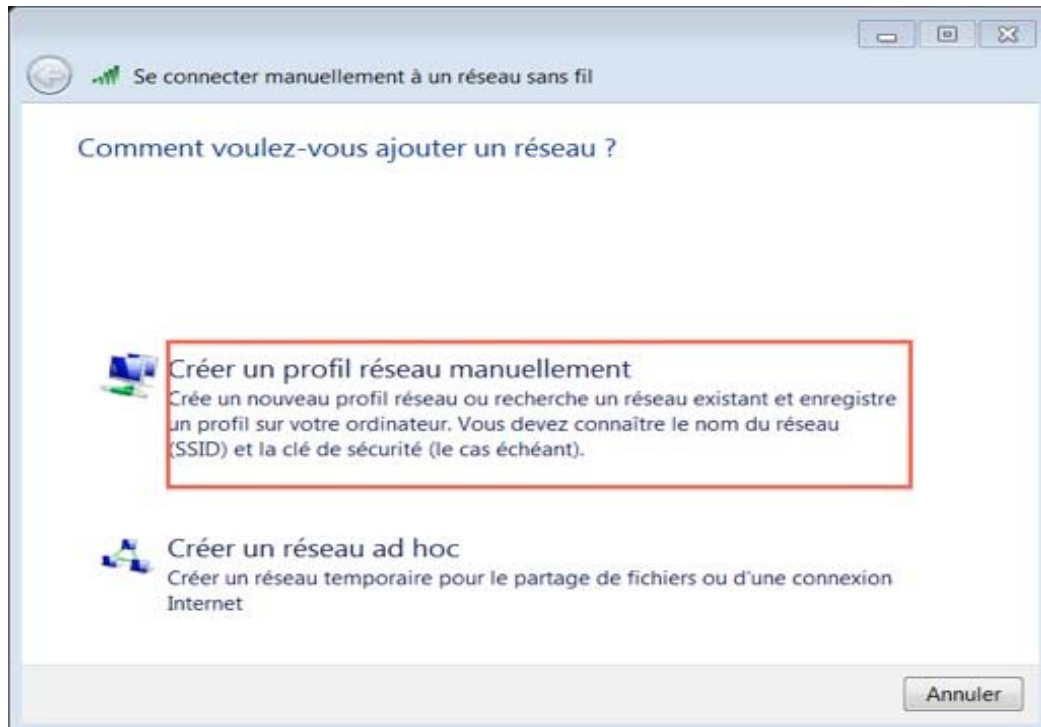
Configuration du protocole EAP (3)

- Cliquez sur le bouton 'Ajouter'



Configuration du protocole EAP (4)

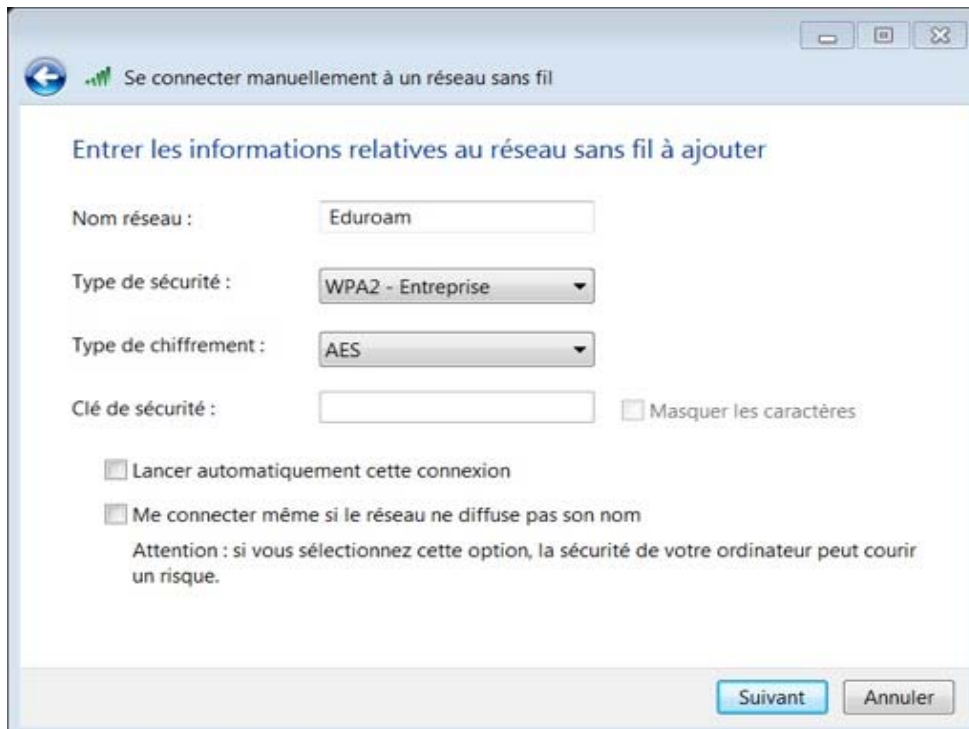
- Choisissez 'Créer un profil réseau manuellement'



- Renseignez les champs comme ci-dessous, puis cliquez sur 'Suivant'
Nom du réseau : Eduroam
Type de sécurité : WPA2 - Entreprise
Type de chiffrement : AES

Configuration du protocole EAP (5)

Le profil maintenant créé, il faut à présent configurer la connexion.
Donc cliquez sur 'Modifier les paramètres de connexion'



Se connecter manuellement à un réseau sans fil

Entrer les informations relatives au réseau sans fil à ajouter

Nom réseau :

Type de sécurité :

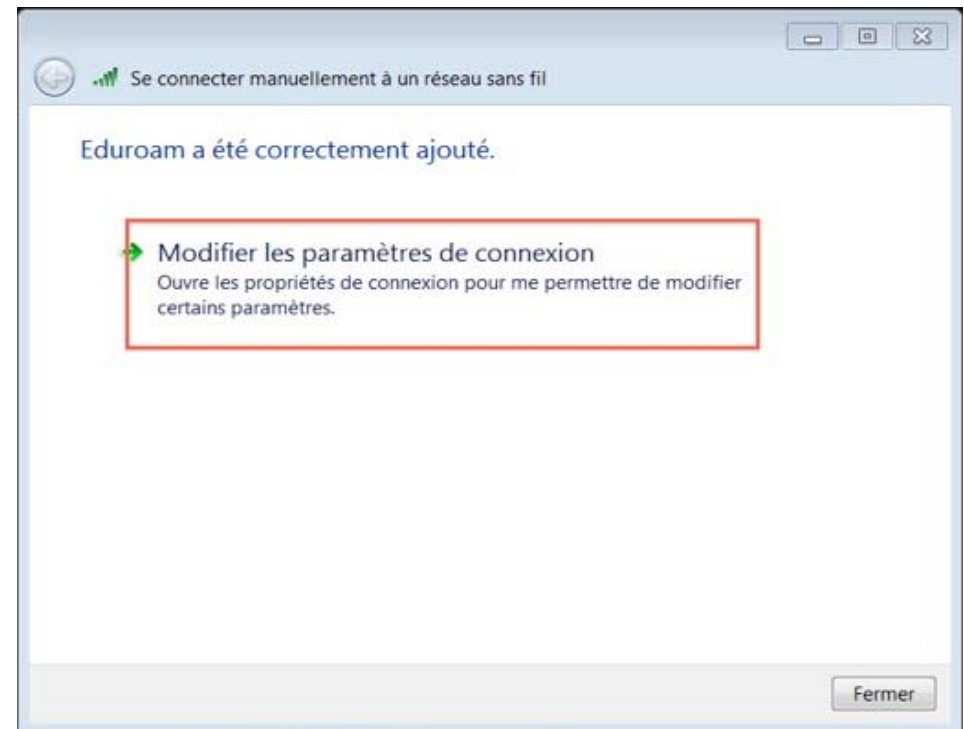
Type de chiffrement :

Clé de sécurité : ☐ Masquer les caractères

☐ Lancer automatiquement cette connexion

☐ Me connecter même si le réseau ne diffuse pas son nom

Attention : si vous sélectionnez cette option, la sécurité de votre ordinateur peut courir un risque.



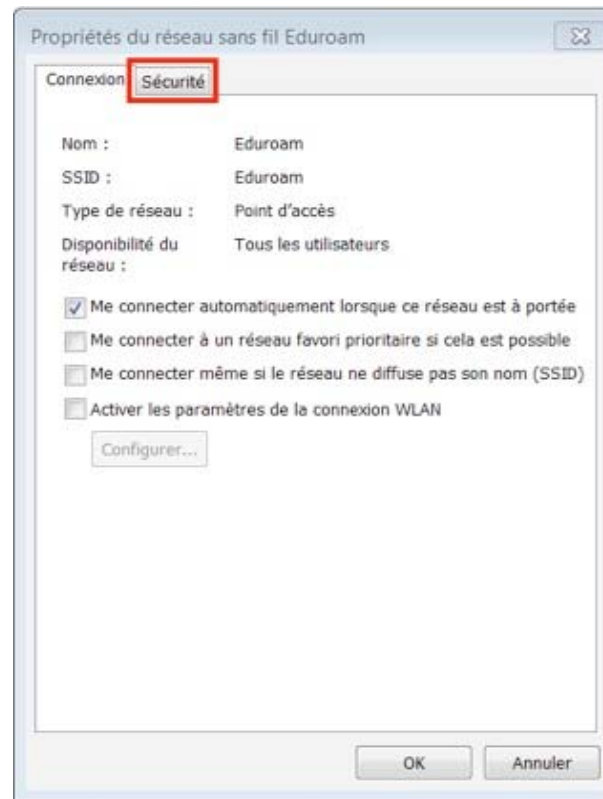
Se connecter manuellement à un réseau sans fil

Eduroam a été correctement ajouté.

Ouvre les propriétés de connexion pour me permettre de modifier certains paramètres.

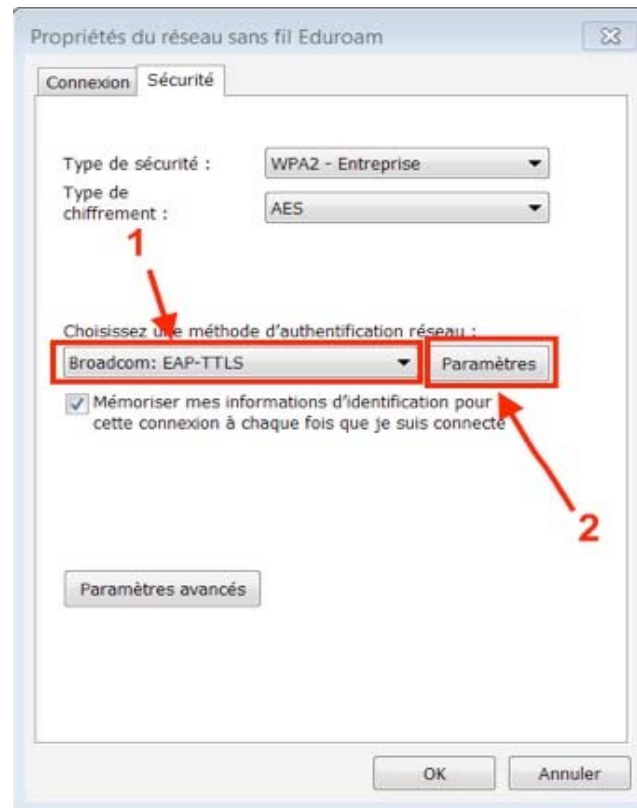
Configuration du protocole EAP (6)

- Allez dans 'Sécurité'



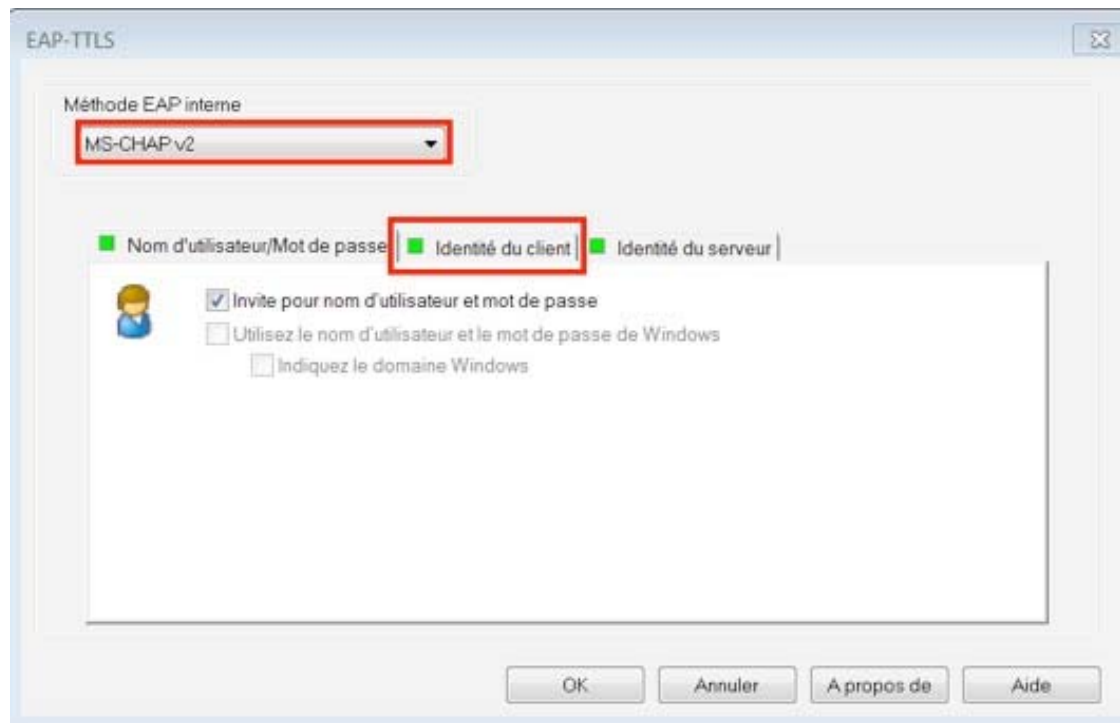
Configuration du protocole EAP (7)

Choisissez la méthode d'authentification réseaux 'Broadcom : EAP-TTLS' puis allez dans 'Paramètres'.



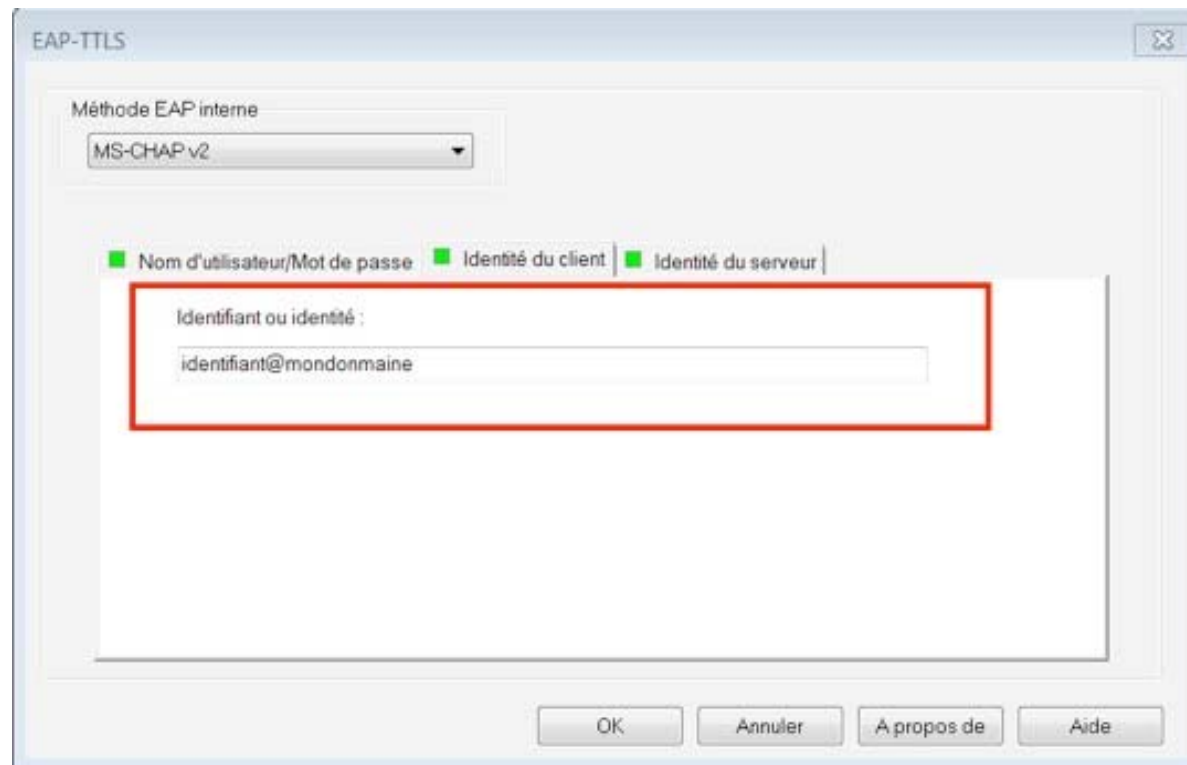
Configuration du protocole EAP (8)

Laissez les options par défaut et allez dans l'onglet 'Identité du client'.



Configuration du protocole EAP (9)

Renseignez le champs 'Identifiant ou identité' avec votre identifiant sous la forme 'identifiant@mondomaine'.



The screenshot shows the 'EAP-TTLS' configuration window. At the top, there is a dropdown menu for 'Méthode EAP interne' set to 'MS-CHAP v2'. Below this, there are three radio buttons: 'Nom d'utilisateur/Mot de passe' (selected), 'Identité du client', and 'Identité du serveur'. A red rectangular box highlights the 'Identifiant ou identité' text field, which contains the text 'identifiant@mondomaine'. At the bottom of the window, there are four buttons: 'OK', 'Annuler', 'À propos de', and 'Aide'.

Reference

- Dieter Gollmann "Computer Security" (3ème édition, mais 2ème est également bien)

[Http://www.amazon.com/Computer-Security-Dieter-Gollmann/dp/0470741155](http://www.amazon.com/Computer-Security-Dieter-Gollmann/dp/0470741155)

- Ross Anderson " Security Engineering "

[Http://www.amazon.com/Security-Engineering-Building-Dependable-Distributed/dp/0470068523/](http://www.amazon.com/Security-Engineering-Building-Dependable-Distributed/dp/0470068523/)

(Également disponible en ligne à: <http://www.cl.cam.ac.uk/~rja14/book.html>)

- Avoine, G., Junod, P., & Oechslin, P. (2015). Sécurité informatique-Cours et exercices corrigés. (3ème édition, mais 2ème est également bien)

Disponible à la bibliothèque de l'Université de Guelma