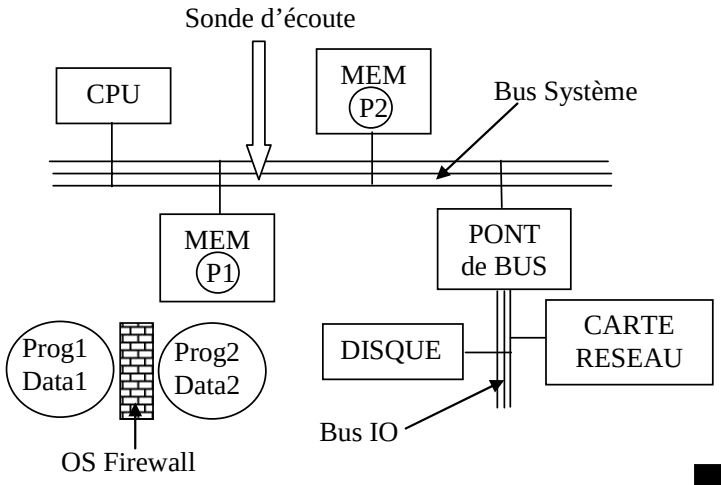
Notion de base de sécurité des réseaux

Applications distribuées

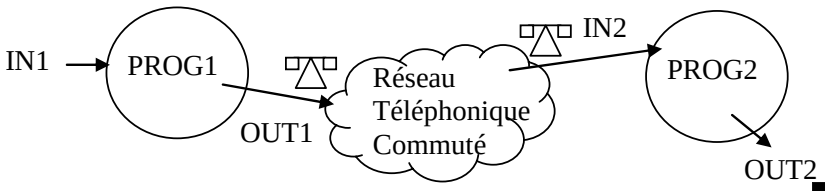
- **Une application distribuée est un ensemble d'entités logicielles, logiquement autonomes, qui produisent, consomment et échangent des informations**
  - OUTi = PROG(INi))
- **Dans un premier temps les composants logiciels des applications étaient logés dans un même système informatique, constituant de fait leur média de communication (parfois dénommé *gluware*).**
  - Le bus système permet le transfert des informations stockées en mémoire, les modules logiciels sont réalisés par des processus gérés par le système d'exploitation.
  - La sécurité est uniquement dépendante des caractéristiques du système d'exploitation, par exemple en terme de gestion des droits utilisateurs, ou d'isolement des processus.

GlueWare



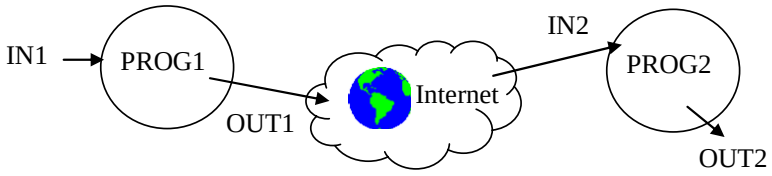
L'âge des MODEMs

- **Dans une deuxième période l'application distribuée est répartie entre plusieurs systèmes informatiques reliés entre eux par des liens de communications supposés sures (c'est à dire qu'il est difficile d'enregistrer ou de modifier l'information transmise) tels que modems ou liaisons spécialisées (X25, RNIS ...).**
- **Nous remarquerons à ce propos qu'il est possible de sécuriser une liaison de type point à point par un dispositif matériel de chiffrement.**



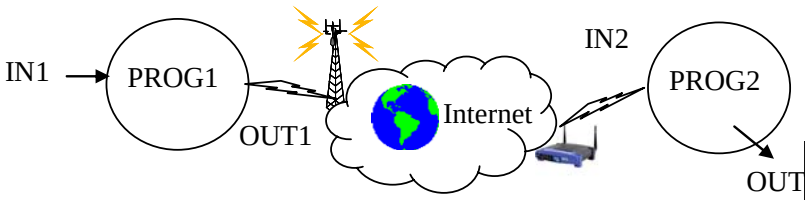
Internet Protocol

- Enfin l'émergence de la toile d'araignée mondiale a permis de concevoir des systèmes distribués à l'échelle planétaire, les composants logiciels sont répartis sur des systèmes informatiques hétéroclites, le réseau n'est pas sûr, le nombre d'utilisateurs est important.
- La sécurité devient un paramètre critique et tente de concilier des contraintes à priori antinomiques telles que, nécessité économique d'utiliser Internet, et impérative résistance à la piraterie informatique ou à l'espionnage.



Ubiguitous Networks

- La dernière révolution des communications s'appuie sur les technologies de réseaux IP sans fil, tels que Wi-Fi ou WiMAX.
- Les liens filaires symboles d'une connectivité volontaire et contrôlée s'estompent, l'infrastructure du réseau devient diffuse et invisible. Un nouveau besoin de sécurité s'affirme, le contrôle des accès réseaux.



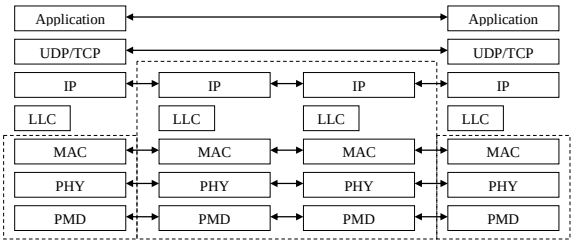
Principes de sécurité

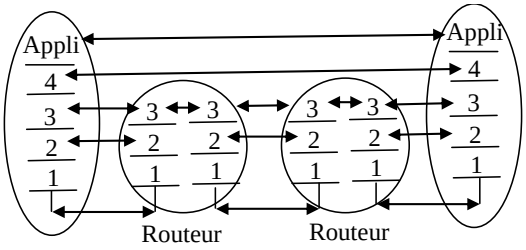
- L'identification (identity).
  - L'utilisateur d'un système ou de ressources diverses possède une identité (une sorte de clé primaire d'une base de données) qui détermine ses lettres de crédits (credential) et ses autorisations d'usage. Cette dernière peut être déclinée de multiples manières, compte utilisateur (login) d'un système d'exploitation ou techniques biométriques empreinte digitale, empreinte vocale, schéma rétinien…
- L'authentification (authentication).
  - Cette opération consiste à faire la preuve de son identité. Par exemple on peut utiliser un mot de passe, ou une méthode de défi basée sur une fonction cryptographique et un secret partagé. L'authentification est simple ou mutuelle selon les contraintes de l'environnement.
- La confidentialité (privacy).
  - C'est la garantie que les données échangées ne sont compréhensibles que pour les deux entités qui partagent un même secret souvent appelé association de sécurité (SA). Cette propriété implique la mise en oeuvre d'algorithmes de chiffrements soit en mode flux (octet par octet, comme par exemple dans RC4) soit en mode bloc (par exemple par série de 8 octets dans le cas du DES).
- L'intégrité des données (MAC, Message AuthentiCation).
  - Le chiffrement évite les écoutes indiscrètes, mais il ne protège pas contre la modification des informations par un intervenant mal intentionné. Des fonctions à sens unique (encore dénommées empreintes) telles que MD5 (16 octets) ou SHA1 (20 octets) réalisent ce service. Le MAC peut être associé à une clé secrète (HMAC(Message,clé), Keyed-Hashing for Message AuthentiCation).
- La non-répudiation.
  - Elle consiste à prouver l'origine des données. Généralement cette opération utilise une signature asymétrique en chiffrant l'empreinte du message avec la clé RSA privée de son auteur (RSA(Empreinte(Message))).
- On cite parfois un sixième attribut relatif à la sûreté de fonctionnement (disponibilité, résilience) du système.

De la confiance (TRUST)

- **La confiance est une relation sans propriétés particulières.**
  - *Réflexivité*, ai-je confiance en moi-même (pas dans tous domaines).
  - *Symétrie*, je fais confiance au pilote de l'avion ou au chirurgien, la réciproque n'est pas forcément vraie.
  - *Transitivité*, j'ai confiance dans le président, le président a confiance en la présidente, je n'ai pas obligatoirement confiance dans la présidente.
- **Les infrastructures PKI supposent une transitivité de la relation de confiance. Le client du réseau et un serveur d'authentification partagent une même autorité de certification (CA), qui crée une classe de confiance basée sur une relation R (R signifiant= «fait confiance à»).**
  - (Client R CA) ET (Serveur R CA) => (Client R Serv

La sécurité appliquée aux réseaux





Comment sécuriser une pile réseau ?

- **PHY- Le chiffrement au niveau physique sur des liaisons point à point.**
  - Par exemple cryptographie quantique (PMD), saut de fréquences pseudo aléatoire, ou chiffrement 3xDES du flux octets (une méthode couramment déployée par les banques). Dans ces différentes procédures les clés sont distribuées manuellement.
- **MAC- Confidentialité, intégrité de données, signature de trames MAC.**
  - C'est la technique choisie par les réseaux sans fil 802.11. La distribution des clés est réalisée dans un plan particulier (décrit par la norme IEEE 802.1x). Dans ce cas on introduit la notion de contrôle d'accès au réseau LAN, c'est à dire à la porte de communication avec la toile d'araignée mondiale. C'est une notion juridique importante, le but est d'interdire le transport des informations à des individus non authentifiés (et donc potentiellement criminels…)
- **TCP/IP- Confidentialité, intégrité de données, signature des paquets IP et/ou TCP.**
  - C'est typiquement la technologie IPSEC en mode tunnel. Un paquet IP chiffré et signé est encapsulé dans un paquet IP non protégé. En effet le routage à travers l'Internet implique l'analyse de l'en tête IP, par les passerelles traversées. IPSEC crée un tunnel sécurisé entre le réseau d'accès et le domaine du fournisseur de service. On peut déployer une gestion manuelle des clés ou des protocoles de distribution automatisés tels que ISAKMP. La philosophie de ce protocole s'appuie sur la libre utilisation du réseau d'accès ce qui n'est pas sans soulever des problèmes juridiques. Par exemple des criminels protègent leurs échanges de données, il est impossible aux réseaux traversés de détecter leur complicité dans le transport d'informations illégales.
- **ADDON- Insertion d'une couche de sécurité additive assurant la protection d'application telles que navigateurs WEB ou messageries électroniques.**
  - Par exemple le protocole SSL basé sur la cryptographie asymétrique réalise cette fonction. Généralement ce dernier conduit une simple authentification entre serveur et client. Il utilise un secret partagé (Master Secret) à partir duquel on dérive des clés de chiffrements utilisées par l'algorithme négocié entre les deux parties. Par exemple dans le cas d'une session entre un navigateur et un serveur bancaire, le client authentifie son service bancaire. Une fois le tunnel sécurisé établit le client s'authentifie à l'aide d'un login et d'un mot de passe. Il obtient alors une identité temporaire associée à un simple cookie.
- **APPLICATION- Gestion de la sécurité par l'application elle même.**
  - Ainsi le protocole S-MIME réalise la confidentialité, l'intégrité et la signature des con[illegible] critiques d'un message électronique.

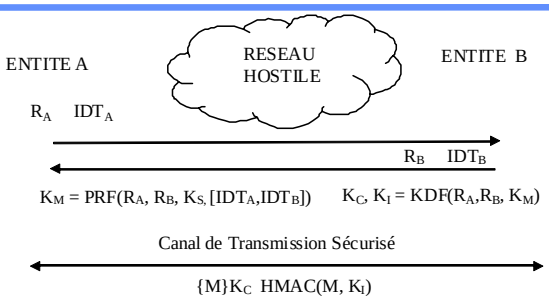
Quels objectifs ?

- **MAN – WAN**
  - Deux classes de réseaux selon que les bandes de fréquences soient soumises à licence ou non, par exemple Wi-Fi et WiMobile (IEEE 802.16e)
  - Contrôle des accès, généralement avec une infrastructure centralisée (AAA, Authentication Authorization Accounting)
  - Confidentialité, non répudiation (signature des trames)
  - **Assurer la rentabilité financière du service**
- **WLAN**
  - Réseaux privés ou d'entreprises
  - Contrôle des accès
  - Confidentialité, non répudiation
  - **Contrôler les accès aux réseau de l'entreprise, éviter la fuite d'information.**
- **WPAN**
  - Réseaux personnels.
  - Appairage entre terminaux et périphériques.
  - **Obtenir une architecture fonctionnelle, éviter la fuite d'information**

Quelles architectures ?

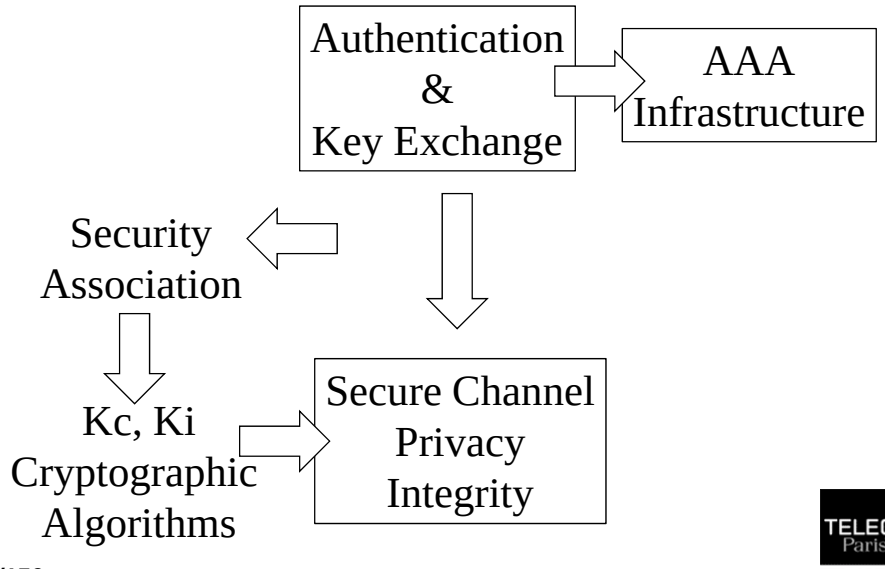
- **Clés symétriques distribuées manuellement**
  - Out Of Band
  - Pas de serveur d'authentification centralisé
- **Clés symétriques distribuées automatiquement**
  - Serveur d'authentification centralisé
- **Vecteurs d'authentification**
  - GSM, UMTS
  - Serveur d'authentification central ou réparti
- **Architecture basée sur des clés asymétriques**
  - Distribution de certificats et de clés RSA privées
  - Architecture répartie ou centralisée
  - Problème de la révocation

Création d'un canal sécurisé



- La procédure d'authentification d'une paire d'entités informatiques, parfois dénommée phase d'autorisation, consiste typiquement à échanger les identités (IDTA et IDTB) d'un couple d'interlocuteurs (appelés client/serveur ou initiateur/répondeur), deux nombres aléatoires (RA, RB) formant un identifiant unique de la session, puis d'effectuer un calcul.
- Ce dernier produit, à l'aide d'une valeur secrète (KS) un secret maître (KM), à partir duquel on déduit des clés de chiffrement (KC) et d'intégrité (KI) permettant de créer un canal sécurisé.
- Dans un contexte de cryptographie symétrique la clé KS est distribuée manuellement ; dans un contexte de cryptographie asymétrique la clé KS sera par exemple générée par A, mais chiffrée par la clé publique (e,n) de B (Ks^e mod n).
- La protection de l'identité est une préoccupation croissante avec l'émergence des technologies sans fil. Il existe divers mécanismes permettant d'obtenir cette propriété avec des degrés de confiance divers, par exemple grâce à la mise en œuvre de pseudonymes (tel que le TIMSI du GSM), du protocole de Diffie-Hellman, ou du chiffrement de certificats par la clé publique du serveur.

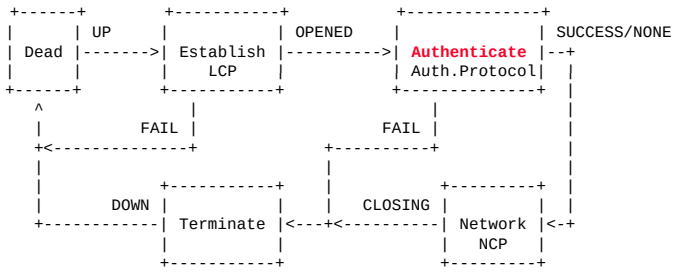
Mécanismes de base



About the Point To Point Protocol

ABOUT PPP

- **PPP (RFC 1661, 1994) was widely used for MODEM access control.**
- **It is still widely used for high speed link (DSL) access control.**
- **In PPP Authentication occurred *before* IP address allocation**



Flag 0x7E	Address 0xFF	Control 03	Protocol 2 bytes	information 1500 octets max	CRC 2 bytes	Flag 0x7E

- **Protocol Field Value**
  - 0x0021 : IP
  - 0xC021 : Link Control Protocol (LCP)
  - 0x8021 : Network Control Protocol (NCP)
  - 0xC023 : Password Authentication Protocol (PAP)
  - 0xC025 : Link Quality Report (LQR)
  - 0xC223 : Challenge Handshake Authentication Protocol (CHAP)

A PPP Authentication example 1/2

LCP Coding

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Data ...
+-+-+-+-+
LCP (code), 1-Request 2-Ack C-IDENTITY
```

LCP Option=3, Authentication Request

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type=3    |    Length=5   | Authentication-Protocol= c223 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Algorithm=5 MD5|
+-+-+-+-+-+-+-+-+
```

CHAP coding

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Data ...
+-+-+-+-+
```

Code

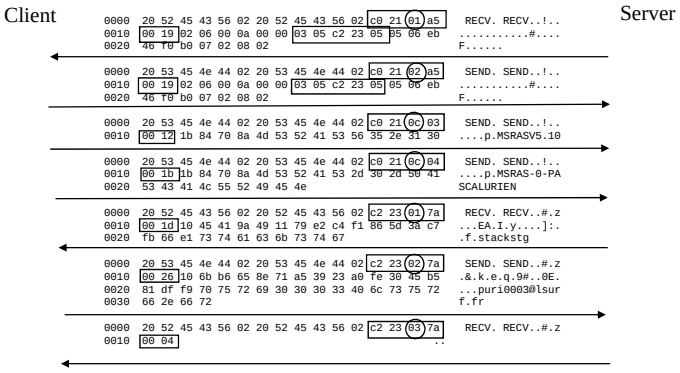
1- Challenge, 2-Response

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Code      |  Identifier   |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Value-Size   |  Value ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Name ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

3-Success, 4-Failure

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Code      |  Identifier   |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Message  ...
   +-+-+-+-+-+-+-+-+-+-+-+-
```


A PPP Authentication example 1/2

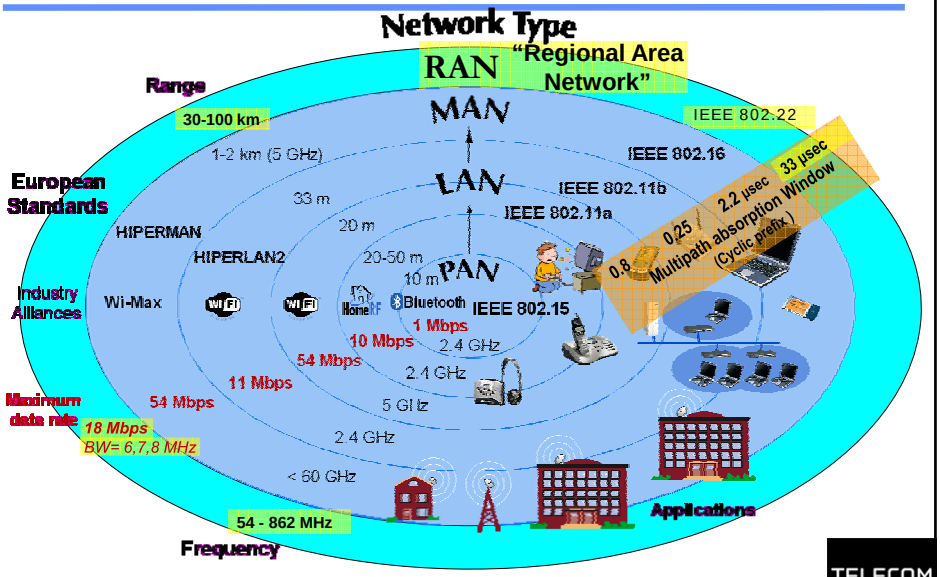


Evolution des Réseaux sans fil

Evolution des réseaux sans fil.

- **2G Global System for Mobile Communication.**
  - Voix 13 Kbit/s - Short Message SMS 160 octets.
- **2,5G General Packet Radio Service.**
  - Mode paquet - Débit < 32 Kbit/s
- **3G Universal Mobile Telecommunication System.**
  - Mode Paquet - Débit < 2 Mbits.
- **4G Wireless Local Area Network**
  - Ethernet sans fil 802.11 – Wi-Fi
    - 802.11b, 11 Mbits/s Portée 25/100 m.
    - 802.11a, 54 Mbits/s **incompatible** 802.11b.
    - 802.11g, 54 Mbits/s **compatible** 802.11b
  - Piconet Bluetooth.
    - Portée 10 m, débit < 1 Mbit/s
- **Ultra Wide Band.**
  - Wireless USB
- **IEEE 802.16, WiMax**
  - Quelques kilomètres, débit 15 Mbits/s

Standards IEEE



En 2008, les réseaux sans fil sont déjà partout !

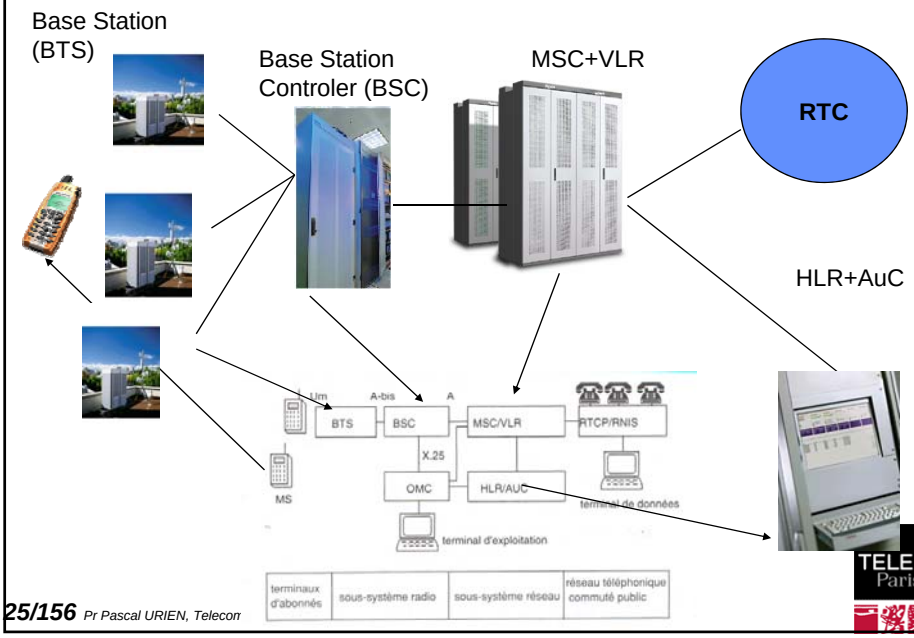
Les défis de la sécurité dans les réseaux sans fil

- **Sécurité des liens radios,** *Network Access*
  - Wi-Fi, IEEE 802.11, IEEE 802.1x, IEEE 802.11i
  - Wi-Max fixe, IEEE 802.16-2004
  - Wi-Mobile, IEEE 802.16e
  - BlueTooth, ZigBee, Wireless USB…
- **Sécurité du *Roaming*: atteindre son réseau mère (Home Network)**
  - Technologies VPN pour le déploiement de tunnel sécurisé
    - IPSEC and IKEv2
    - L2TP, PPTP
- **Sécurité des *Applications***
  - SSL/TLS
    - Messenger
  - SSH
    - Remote SHELL
  - P2P
    - SKYPE

La sécurité du GSM

Provisionning + Simple Authentification

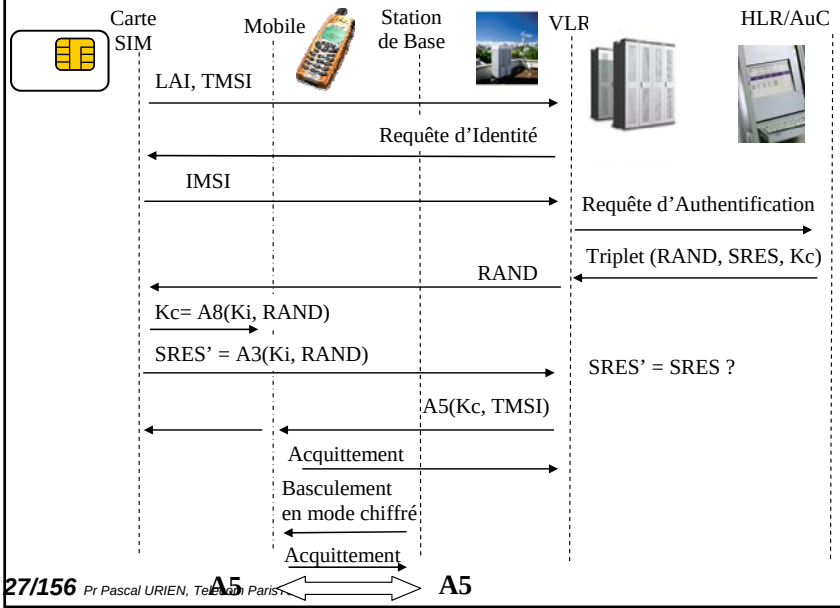
Architecture



Principes 1/2

- **Mécanisme de type provisionning**
  - Vecteurs d'authentification (triplet du GSM)
  - RAND (64 bits), SRES (32 bits), Kc (64 bits, dont 10 sont forcés à zéro)
- **Algorithmes**
  - Clé Ki de 128 bits
  - $A3_{Ki}$(RAND), calcul de la signature SRES
  - $A8_{Ki}$(RAND), calcul de Kc
  - A3/A8 est en fait un algorithme unique, le COMP-128
    - COMP128-1, craqué en 1998, 2^{19} vecteurs
    - COMP128-2, version améliorée de COMP128-2
    - COMP 128-3, basé sur AES
  - A5(Kc), chiffrement de paquets données (voix)
    - Mode bloc de 112 bits
    - A5/1, version forte, craquée en 99
    - A5/2, version faible, craquée en 99
    - A5/3, nouvelle version (MILENAGE-2G)

Principes 2/2



Eléments d'identifications

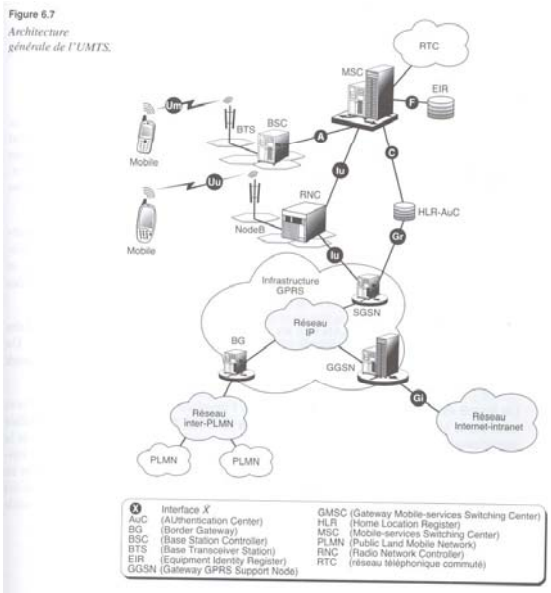
- **Mobile Equipment (ME)**
  - IMEI, International Mobile Equipment Identity
- **Subscriber Identity Module (SIM)**
  - K_i – Subscriber Authentication Key
    - RUN_GSM_ALGO
  - IMSI – International Mobile Subscriber Identity
    - DF_GSM/EF_IMSI
  - TMSI – Temporary Mobile Subscriber Identity
  - PIN – Personal Identity Number protecting a SIM
  - LAI – Location Area Identity
    - DF_GSM/EF_LOCI

Sécurité de l'UMTS

Provisionning + Authentification Mutuelle

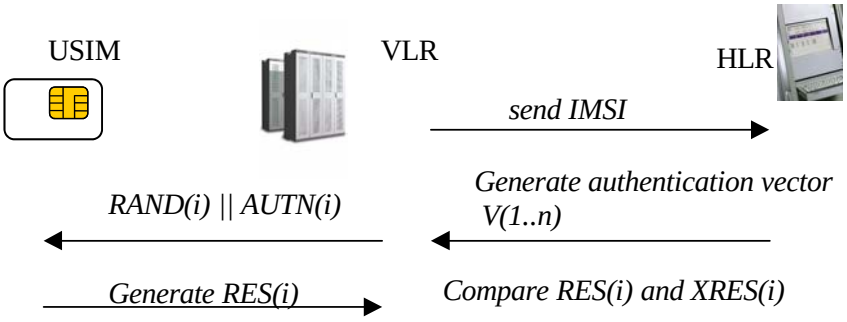
UMTS

Figure 6.7
Architecture générale de l'UMTS.

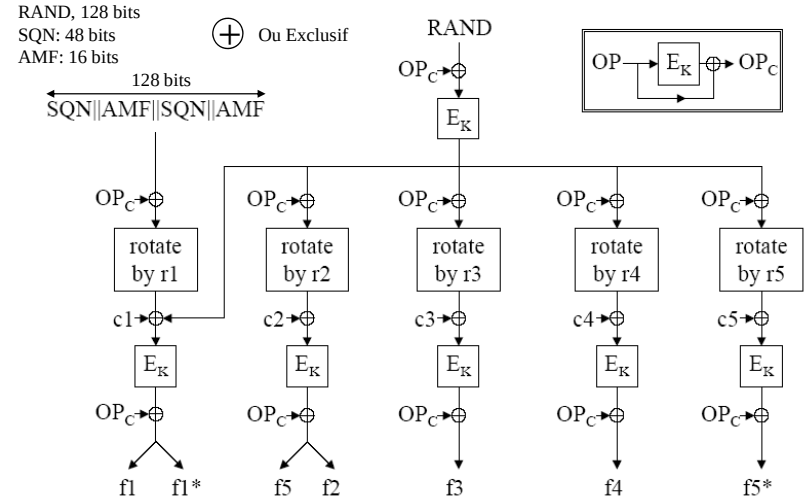


Principes

- **Mutuelle Authentification**
  - Authentication and Key Agreement (AKA)
  - Cipher key (CK) and Integrity key (IK)



MILENAGE

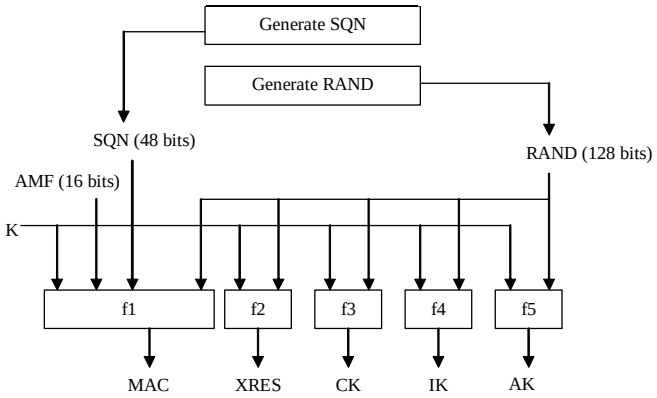


ri= 64,0,32,64,96 (rotation gauche)

ci= 0,1,2,4,8

OP: clé OPérateur (128 bits) Ek: AES + clé 128bits

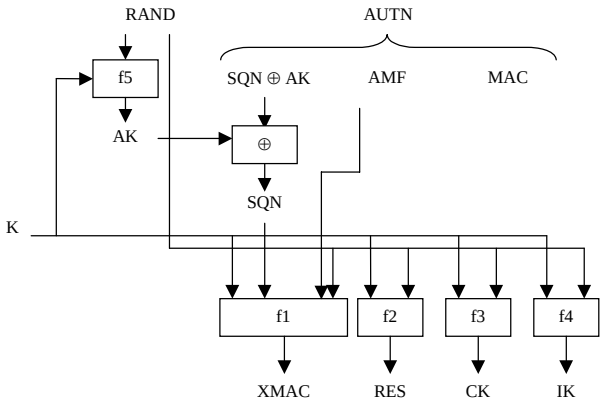
AUTN: Authentication Vector



AUTN := SQN ⊕ AK || AMF || MAC

AV := RAND || XRES || CK || IK || AUTN

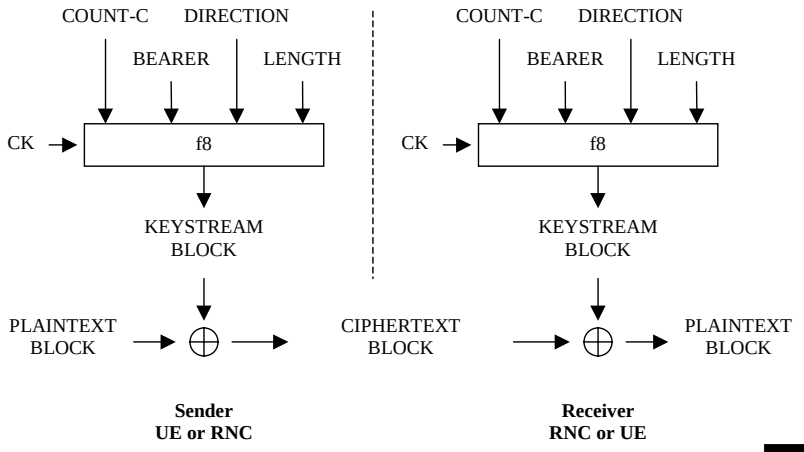
CARTE USIM



Verify MAC = XMAC

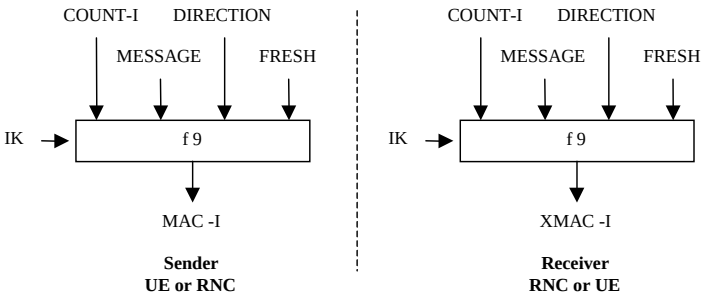
Verify that SQN is in the correct range

Chiffrement



Intégrité

MESSAGE	MAC

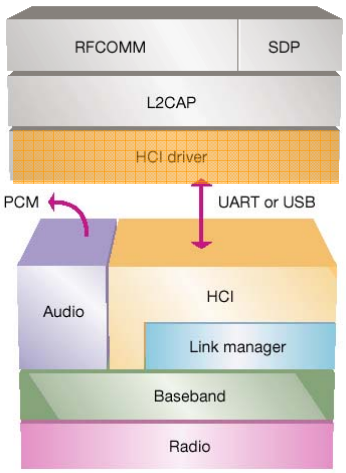


FRESH, valeur aléatoire

Sécurité Bluetooth

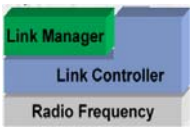
Aperçu de Bluetooth 1/3

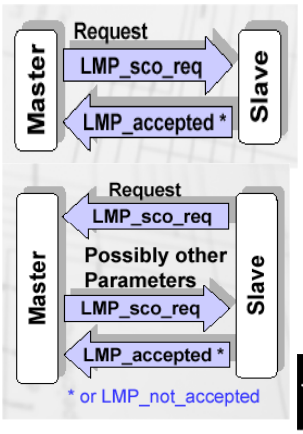
- **Réseau Maître-Esclaves.Portée # 10 m.**
- **Remplacement des liaisons filaires par des liens radio (2,4 Ghz).**
  - 1600 sauts de fréquence (hops) par seconde.
  - Slots de 0,625 ms (1/1600)
  - Deux modes de transfert de données
    - SCO (synchronous connection oriented), voix (64 Kbit/s)
    - ACL (Asynchronous connection link), données (433-433 Kbit/s, 732,2-57,6 Kbit/s)
- **Au plus 7 noeuds esclaves actifs**
- **Un esclave peut être inactif (« parked »), jusqu'à 255 nœuds.**
- **Adaptation au bus hôte (PCMCIA, USB…) via le protocole HCI (*Host Controler Interface*)**
- **Définition de services et profiles**
  - Audio
  - Port Série (RFCOMM)
  - …



Composants BlueTooth 1/3

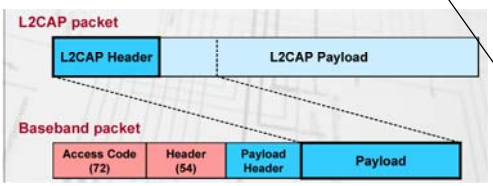
- **Niveau physique**
  - Radio.
  - Baseband, gestion des trames, time slots,…
- **Link Controller**
  - Gestion des slots
  - Gestion de canaux logiques
- **Link Manager**
  - Gestion de liens virtuels
  - Attachement/De-attachements des nœuds esclaves
  - Négociation de la qualité de ligne (QoS)
  - Sécurité, authentification et chiffrement.

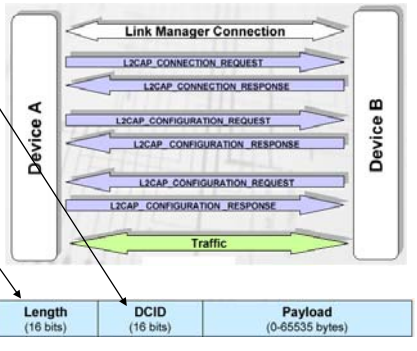




Composants BlueTooth 2/3

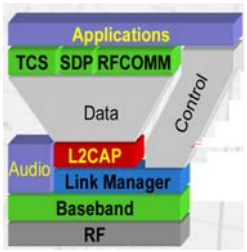
- **L2CAP, Logical Link Control and adaptation Protocol**
  - Multiplexage de canaux logiques (associées à différentes applications).
  - Segmentation / Re-assemblage.



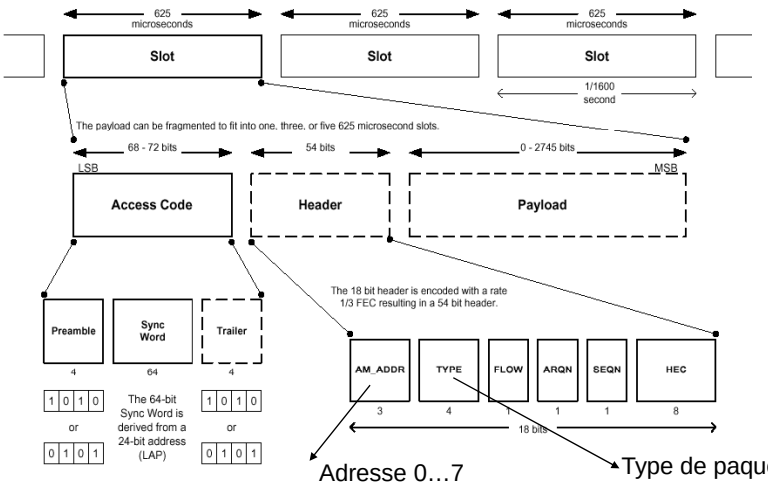


Composants BlueTooth 3/3

- **SDP,** Service **Discovery Protocol**
  - Découverte des services tels que
    - RFCOMM (émulation de port série)
    - Telephony Control Protocol (TCS), émulation de ligne téléphonique
- **Profiles**
  - CTP, Cordless Telephony Profiles
  - HP, Headset Profile
  - SPP, Serial Port Profile
  - PPP, point to point protocol
  - OBEX, Object Exchange Protocol



Format des paquets BlueTooth



Format of an over-the-air payload bearing Bluetooth WPAN packet

Notion de Canaux Logiques

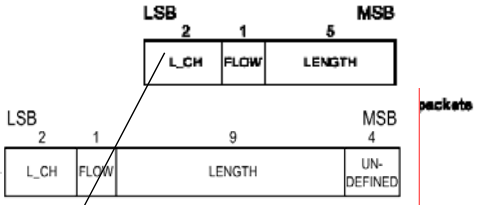


Figure 23—Payload header format for multislot packets

Table 18— Logical channel L_CH field contents

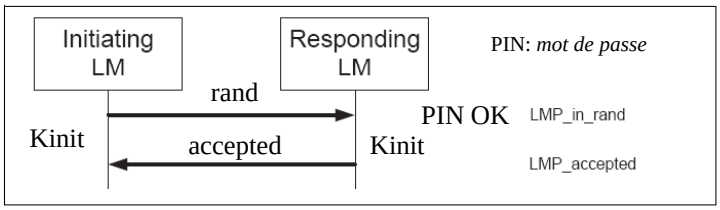
L_CH code b_1b_0	Logical Channel	Information
00	NA	undefined
01	UA/UI	Continuation fragment of an L2CAP message
10	UA/UI	Start of an L2CAP message or no fragmentation
11	LM	LMP message

Eléments de sécurité de BlueTooth

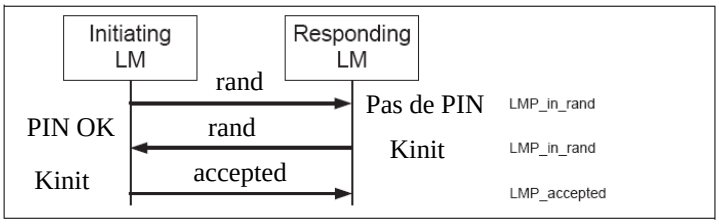
- **Un secret partagé entre les dispositifs maître et esclave: le PIN**
- **Procédure de "pairage" en quatre phases**
  - Création d'une clé d'initialisation, Kinit
  - Création d'une clé de lien, Link_Key
  - Authentification
  - Demande de chiffrement

Création d'une clé Kinit à l'aide d'un PIN

K_init = F(PIN, rand)



Sequence 3: Pairing accepted. Responder has a variable PIN. Initiator has a variable or fixed PIN.

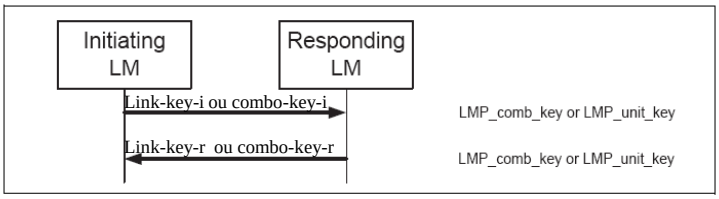


Sequence 4: Responder has a fixed PIN and initiator has a variable PIN.

Création d'une clé de lien KAB

- **Création de KAB**

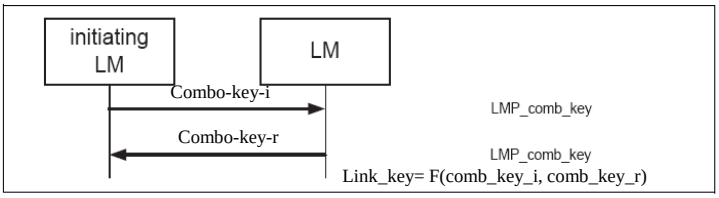
unit-key = link_key exor Kinit
combo_key = aléa



Sequence 7: Creation of the link key.

Link_key = F(unit_key_i , unit_key_r)
Link_key = F(comb_key_i, comb_key_r)

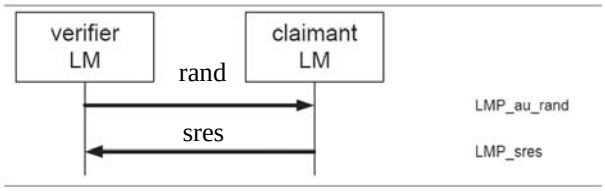
- **Modification de KAB**



Sequence 8: Successful change of the link key.

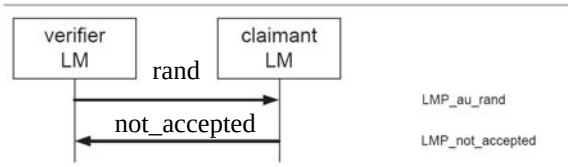
Mécanisme d'Authentification

- **Une clé de ligne (Link Key) est disponible**



Sequence 1: Authentication. Claimant has link key.

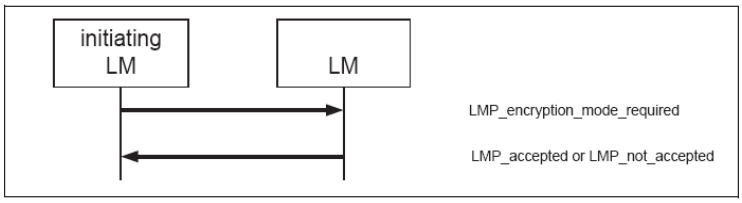
- **Echec, du à la non existence d'une clé de ligne**



Sequence 2: Authentication fails. Claimant has no link key.

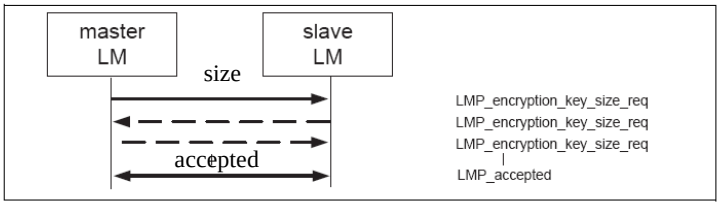
Chiffrement

- **Demande de mode chiffré**



Sequence 12: Negotiation for encryption mode.

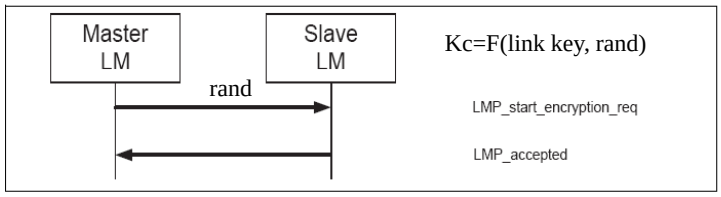
- **Négociation da la taille d'une clé de chiffrement**



Sequence 13: Encryption key size negotiation successful.

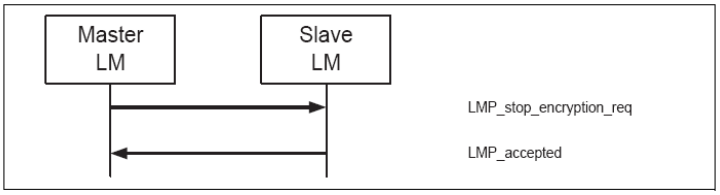
Chiffrement

- **Start Encryption: création de la clé de chiffrement**



Sequence 15: Start of encryption.

- **Stop Encryption**



Sequence 16: Stop of encryption.

SSL - TLS

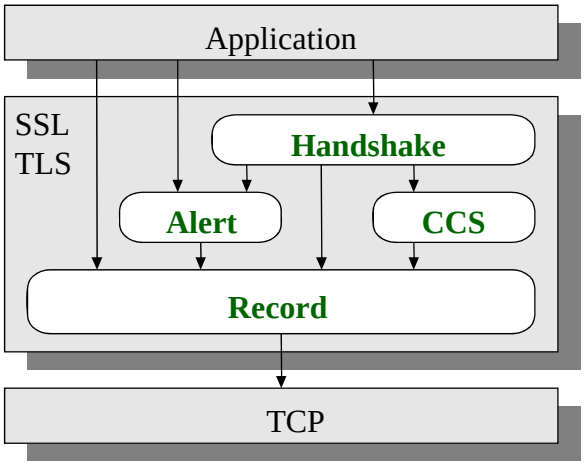
Historique

- **SSL défini par *netscape* et intégré au browser**
  - Première version de SSL testé en interne
  - Première version de SSL diffusé : V2 (1994)
  - Version actuelle V3
- **Standard à l 'IETF au sein du groupe Transport Layer Security (TLS)**

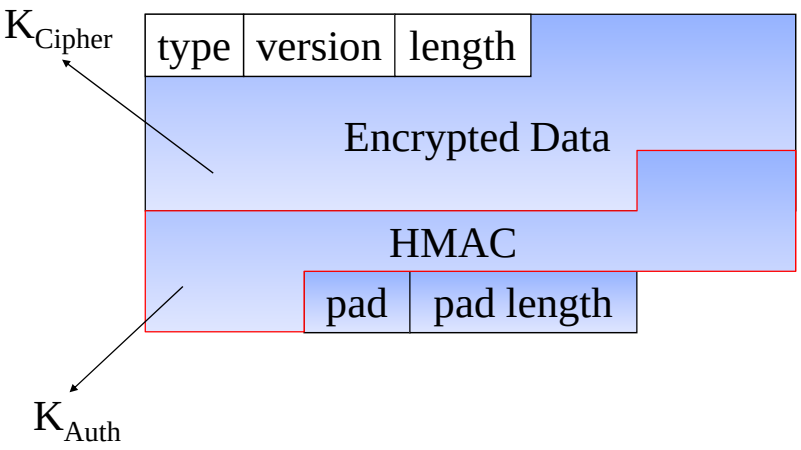
SSL : Services

- **Authentification**
  - Serveur (obligatoire), client (optionnel)
  - Utilisation de certificat X509 V3
  - A l'établissement de la session.
- **Confidentialité**
  - Algorithme de chiffrement symétrique négocié, clé généré à l'établissement de la session.
- **Intégrité**
  - Fonction de hachage avec clé secrète : HMAC(clé secrète,Message)
- **Non Rejeu**
  - Numéro de séquence

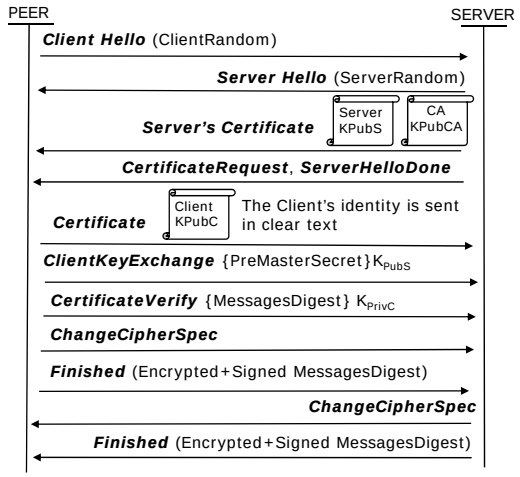
SSL/TLS : Protocoles



Record Layer



SSL/TLS, Dialogue de base



MasterSecret= PRF(ClientRandom, ServerRandom, PreMasterSecret,...)

Keys = PRF(ClientRandom, ServerRandom, MasterSecret,...)

IPSEC

ISAKMP - IKEv1

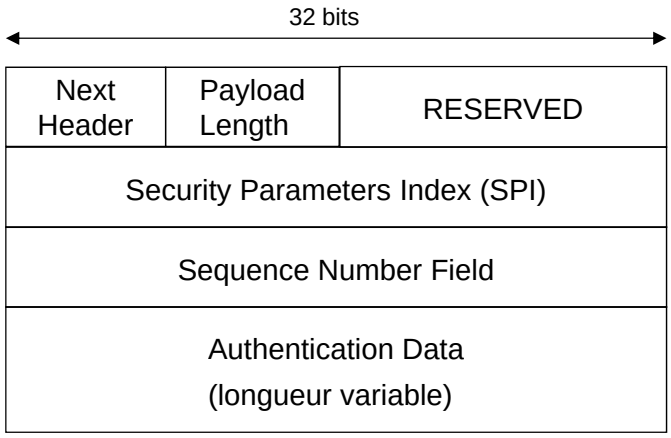
IPSEC: AH et ESP

- **Deux en têtes spécifiques sont utilisés, AH (IP Authentification Header) et ESP (IP Encapsulating Security Payload).**
- **AH garantit l'intégrité et l'authentification des datagrammes IP, mais n'assure pas la confidentialité des données.**
- **ESP est utilisé pour fournir l'intégrité, l'authentification et la confidentialité des datagrammes IP.**

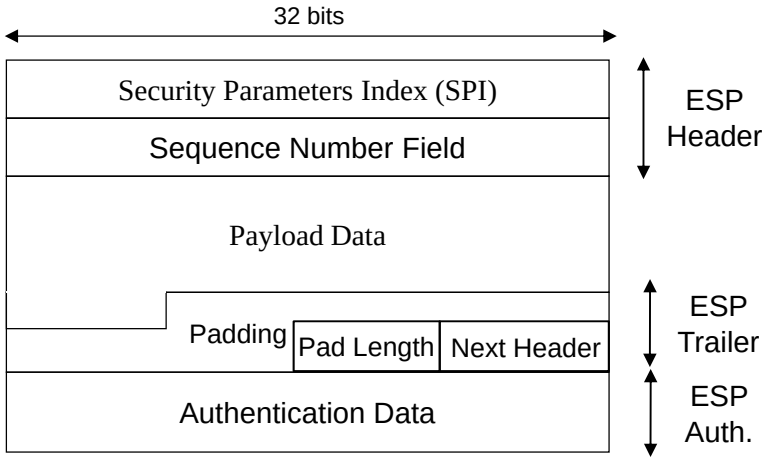
Security Association

- **Ce concept est fondamental à la fois pour AH et ESP. La combinaison d'un SPI (*Security Parameter Index*) et d'une adresse de destination identifie de manière unique un SA particulier.**
- **Une association de sécurité inclue usuellement les paramètres suivant :**
  - Un algorithme d'authentification (utilisé pour AH).
  - La (les) clé(s) utilisée(s) par l'algorithme d'authentification.
  - L'algorithme de chiffrement utilisé par ESP.
  - La (les) clé(s) utilisée(s) par l'algorithme de chiffrement.
  - Divers paramètres utiles à l'algorithme de chiffrement.
  - L'algorithme d'authentification utilisé avec ESP (s'il existe)
  - Les clés utilisées avec l'algorithme d'authentification d'ESP (si nécessaire).
  - La durée de vie de la clé.
  - La durée de vie du SA.
  - La ou les adresses de source du SA
  - Le niveau de sécurité (Secret, non classé …)
- **Le système hôte qui émet l'information sélectionne un SA en fonction du destinataire. L'association de sécurité est de manière générale *mono directionnelle*.**

Authentication Header

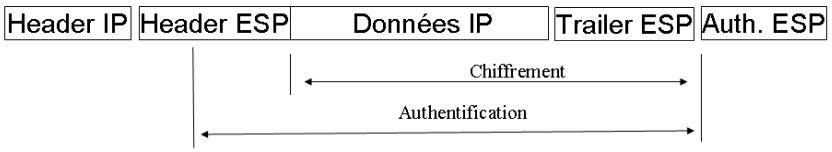


Encapsulating Security Payload

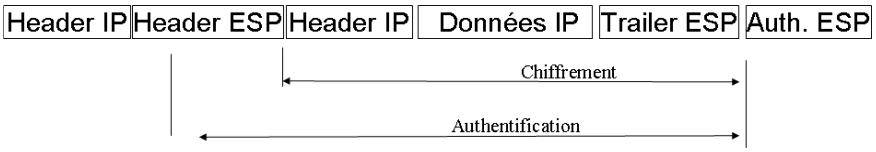


IPSEC: Mode Transport et Mode Tunnel

Mode transport



Mode tunnel

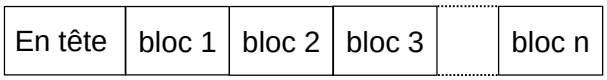


ISAKMP

- Internet Security Association and Key Management Protocol
- Ce protocole sert à :
  - **l'établissement**
  - **la modification**
  - **la suppression**
  - **des Associations de Sécurité**
- ISAKMP comprend deux phases :
  - l'établissement d'une SA ISAKMP
    - **authentification des tiers, génération des clefs,**
    - **échanges ISAKMP**
  - la négociation des paramètres d'une SA pour un mécanisme donné (par exemple AH ou ESP)
    - **le trafic de cette phase est sécurisé par la SA ISAKMP**
  - NB : Une SA ISAKMP est bidirectionnelle

Messages et Blocs

- Il existe 13 types de blocs :
  - SA *Security Association*
  - P *Proposal*
  - T *Transform*
  - KE *Key Exchange*
  - ID *Identification*
  - CERT *Certificate*
  - CR *Certificate Request*
  - HASH *Hash*
  - SIG *Signature*
  - NONCE *Nonce*
  - N *Notification*
  - D *Delete*
  - VID *Vendor ID*



ISAKMP

- **SA (*Security Association*) : ce bloc contient des champs qui indiquent le contexte de la négociation. :**
  - 0 pour ISAKMP
  - 1 pour IPSec
- **P (*Proposal*) : ce bloc indique le mécanisme de sécurité de l'on désire utiliser (AH, ESP) et le SPI associé à la SA.**
  - Chaque bloc est numéroté. S'il y a plusieurs mécanismes pour une même SA, les blocs portent le même numéro.
- **T (*Transform*) : ce bloc indique une transformation (algorithme de chiffrement, fonction de hachage, ...).**
  - Ces blocs sont également numérotés

ISAKMP

- **KE (*Key Exchange*) : ce bloc sert au transport des données nécessaires à la génération de la clef de session.**
- **ID (*Identification*) : ce bloc est utilisé pour l'identification des parties. Un des champs de ce bloc est le champ *ID Type*. Pour ISAKMP, cela peut être par exemple une adresse IP.**
- **CERT (*Certificate*) : ce bloc permet de transporter des certificats, ou toute information s'y rattachant.**
- **CR (*Certificate Request*) : ce bloc est utiliser pour réclamer un certificat à son interlocuteur.**
- **HASH (*Hash*) : ce bloc contient le résultat de l'application d'une fonction de hachage.**

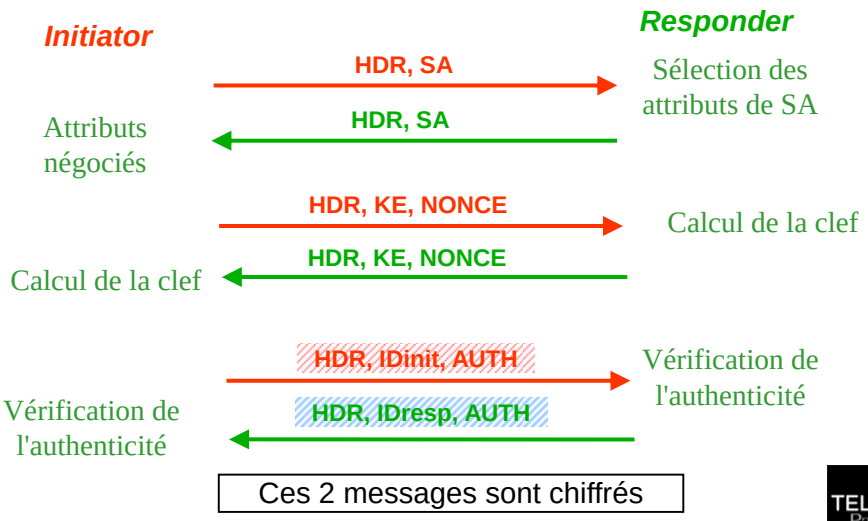
ISAKMP

- **SIG (*Signature*) : ce bloc a le même rôle que le bloc *HASH*, mais il est utilisé dans le cas d'une signature.**
- **NONCE (*Nonce*) : ce bloc est utilisé pour transporter de l'aléa.**
- **N (*Notification*) : ce bloc est utilisé pour transmettre les messages d'erreur ou d'informations sur les négociations en cours.**
  - Il existe 2 champ : *Notify Message Type* et *Notify Data*.
- **D (*Delete*) : ce bloc permet de supprimer une SA et indiquer qu'elle n'est plus valable.**
- **VID (*Vendor ID*) : ce bloc est réservé aux programmateurs pour distinguer 2 instances de son implémentation.**

ISAKMP

- A partir des blocs précédents, le protocole ISAKMP définit des types d'échanges (E*xchange Types*).
- Il y a 5 types d'échanges par défaut :
  - Base Exchange
  - Identity Protection Exchange
  - Authentication Only Exchange
  - Aggressive Exchange
  - Informational Exchange
- **Notation**
  - **HDR = entête du paquet ISAKMP**
  - **SA = blocs SA + P + T**

ISAKMP: Identity Protection Exchange



Au sujet de IKEv1

- **Internet Key Exchange**
- **RFC 2409, 1998**
- **IKE PHASE 1 réalise une association de sécurité ISAKMP entre deux systèmes, qui protège les échanges de IKE phase 2**
  - 4 modes, Main Mode, Agressive Mode, Quick Mode, New Group Mode
  - Plusieurs protocoles d'échanges de clés
    - Asymétriques, OAKLEY et SKEME
    - Symétrique (Pre-Shared-Key)
- **IKE PHASE 2 réalise une association de sécurité pour des sessions IPSEC**

IKEv1, Pre-Shared-Keys, Main Mode

```
        Initiator                          Responder
       -----------                        -----------       Echange
       HDR, SA                    -->                       Chiffré
                                  <--     HDR, SA
       HDR, KE, Ni                -->
                                  <--     HDR, KE, Nr
       HDR*, IDii, [ CERT, ] SIG_I -->
                                  <--     HDR*, IDir, [ CERT, ] SIG_R
```

For pre-shared keys:

SKEYID = prf(pre-shared-key, Ni_b | Nr_b)

The result of either Main Mode or Aggressive Mode is three groups of authenticated keying material:

```
SKEYID_d = prf(SKEYID, g^xy | CKY-I | CKY-R | 0)
SKEYID_a = prf(SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1)
SKEYID_e = prf(SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2)
```

and agreed upon policy to protect further communications. The values of 0, 1, and 2 above are represented by a single octet. The key used for encryption is derived from SKEYID_e in an algorithm-specific manner.

To authenticate either exchange the initiator of the protocol generates HASH_I(SIG_I) and the responder generates HASH_R(SIG_R)

where:

```
HASH_I = prf(SKEYID, g^xi | g^xr | CKY-I | CKY-R | SAi_b | IDii_b )
HASH_R = prf(SKEYID, g^xr | g^xi | CKY-R | CKY-I | SAi_b | IDir_b )
```

SAi_b is the entire body of the SA payload (minus the ISAKMP generic header), all proposals and all transforms offered by the Initiator.
CKY-I and CKY-R are the Initiator's cookie and the Responder's cookie, respectively, from the ISAKMP header.
g^xi and g^xr are the Diffie-Hellman public values of the initiator and responder respectively.

IKeV1, Phase II, Pre-Shared-Key, Quick Mode

```
Initiator                                                    Responder
-----------                                                  -----------
HDR*, HASH(1), SA, Ni [, KE ] [, IDci, IDcr ] -->
                                        <-- HDR*, HASH(2), SA, Nr [, KE ] [, IDci, IDcr]
HDR*, HASH(3) -->
```

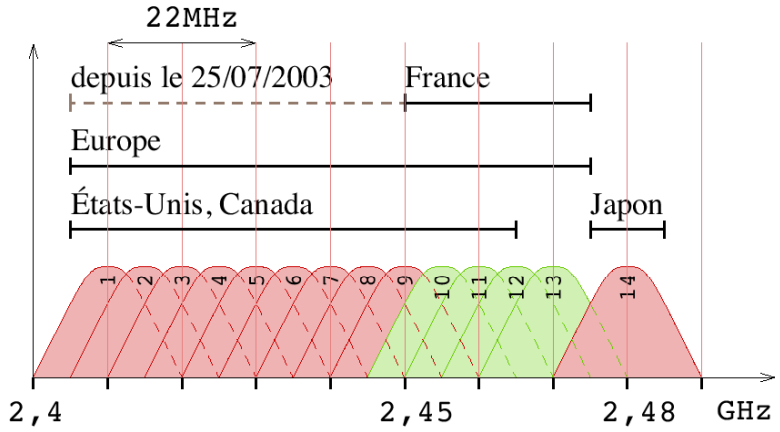
```
HASH(1) = prf(SKEYID_a, M-ID | SA | Ni [ | KE ] [ | IDci | IDcr ] )
HASH(2) = prf(SKEYID_a, M-ID | Ni_b | SA | Nr [ | KE ] [ | IDci | IDcr ] )
HASH(3) = prf(SKEYID_a, 0 | M-ID | Ni_b | Nr_b)
```

```
KEYMAT = prf(SKEYID_d, protocol | SPI | Ni_b | Nr_b)
```

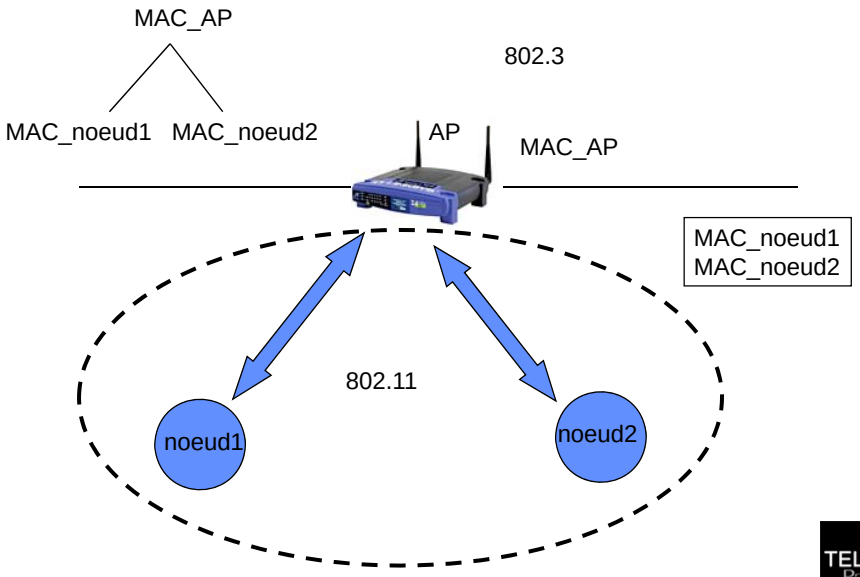

La sécurité du Wi-Fi

Pascal Urien

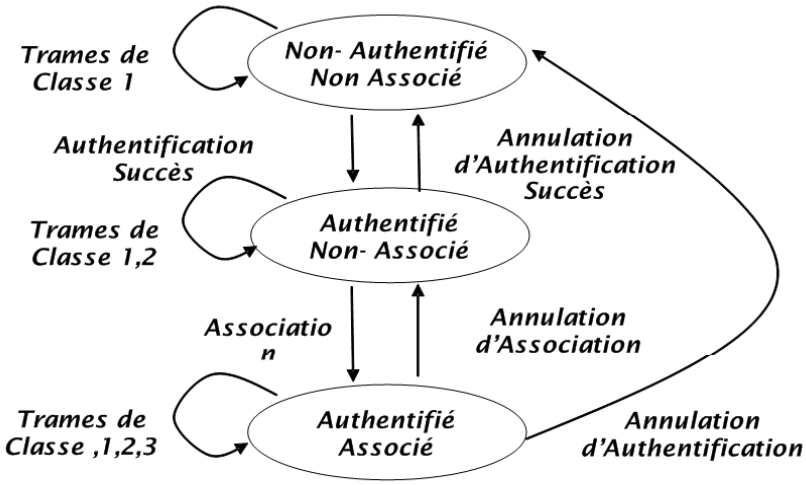
802.11b, 14 canaux de 22 Mhz



Association



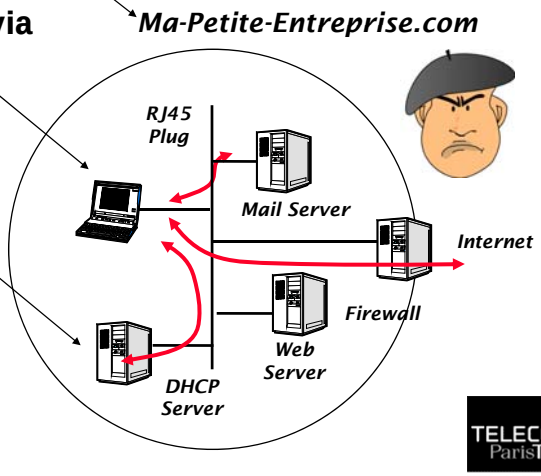
Authentification



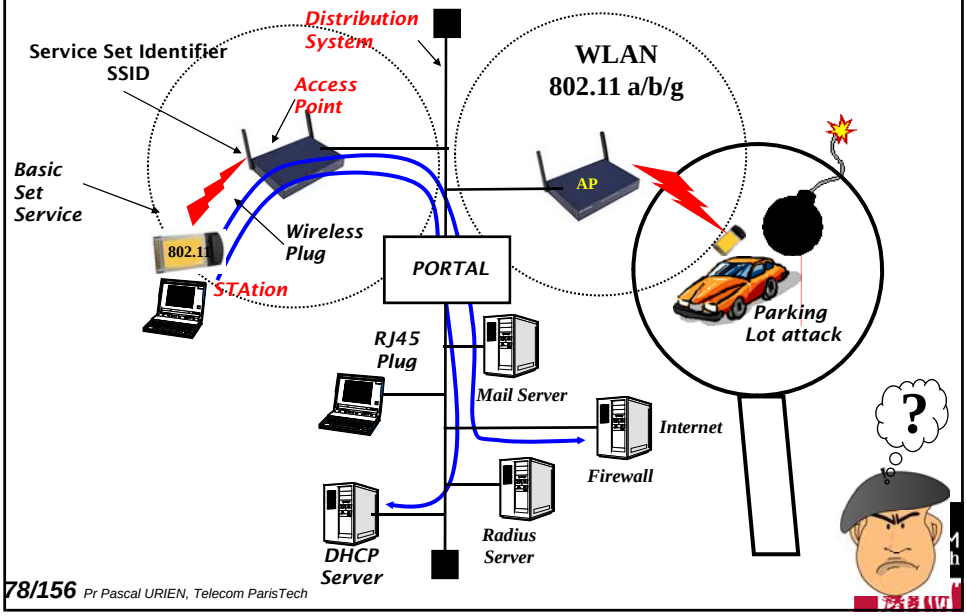
Wi-Fi, introduction à la Sécurité

Intranet Câblé Classique

- Les accès aux locaux sont contrôlés.
- Connexion des PCs via une prise RJ45.
- Serveur DHCP non sécurisé.



L' Architecture 802.11.



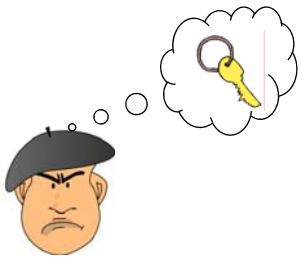
La Nécessaire Sécurité des Accès Sans Fil.

- **Authentification des accès.**
  - *Simple*, identification du nomade (prévention du *spoofing*) et de ses droits (*credentials*).
  - *Mutuelle*, protection contre des AP indésirables (*rogue access point*).
  - Contrôle d'accès au réseau, protection du réseau = qui utilise le réseau.
- **Confidentialité (chiffrement) des trames.**
  - Protection du transport de l'information
  - Prévention des écoutes des canaux radio, au niveau 2 (MAC)
  - Mais d'autres méthodes sont disponibles IPSEC (3) SSL/TLS (application), SSH (application).
- **Intégrité des trames.**
  - Prévention des attaques par corruption de données (*bit flipping attack*)
- **Signature des trames.**
  - Non répudiation. Nécessaire à l 'obtention de services.
- **Fourniture/Facturation des services.**
  - Roaming, Voice Over IP (VoIP), Qualité de services (QoS).

AAA *Authentication, Authorization, Accounting*.

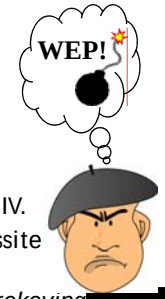
- Groupe de travail IETF RFC *2904*

WEP



Sécurité Wi-Fi - WEP

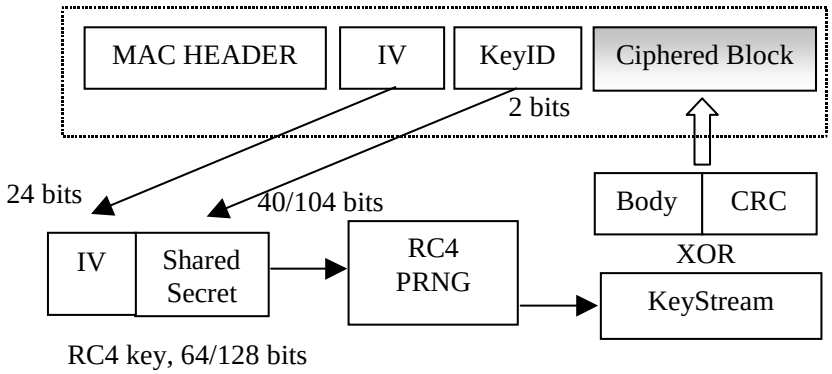
- **Open Authentication, c'est à dire pas d'authentification**
  - Utilise le SSID comme mot de passe, peu sûre.
- **Filtrage des adresses MAC**
  - *Address Control List,* peu sûre.
- **Clés RC4 fixes (64 ou 128 bits), partagées entre stations et points d 'accès.**
  - Authentification re-jouable.
  - Intégrité des données non garantie.
  - Pas de signature
  - Confidentialité des données, *sous réserves*.
    - Attaque par enregistrement des 16 millions de vecteurs IV.
    - Attaque RC4 *Fluhrer, Mantin, Shamir (août 2001*), nécessite l 'enregistrement d'environ de 1 million de trames.
    - Implique un rafraîchissement périodique des clés WEP (*rekeying*, exemple changement de clés toutes les 10,000 trames (1 million le seuil citrique de sécurité).



Wireless Equivalent Privacy. 1/5

- **Station et AP partagent 4 secrets de 40 bits.**
- **Une trame WEP transporte des données chiffrées par une clé RC4 de 64 bits déduite d 'un secret partagé (40 b) et d 'une valeur IV (24b) fixée par l 'émetteur de l 'information.**
  - Le chiffrement RC4 (Ci) est réalisé par le ou exclusif (*code de Vernam*) du message (Mi) en clair avec suite d 'octets pseudo aléatoire Xsi déduit de la clé.
  - On peut déduire la valeur de la clé Xsi connaissant la valeur en clair Ci.
    - **Ci = Mi ⊕Xsi, Ci ⊕Mi = Xsi**
  - Une clé RC4 ne doit pas être réutilisée (2^{24} = 16 millions de trames chiffrées par clé)

La trame WEP 2/5.



m ParisTech

Lacunes du protocole WEP. 3/5

- **Association**
  - Le BSS est identifié par le paramètre SSID présent dans les trames fanion (Beacon) émises périodiquement.
  - Une station s'associe volontairement à un AP.
- **Authentification**
  - AP émet un challenge en clair. La station chiffre cet aléa avec un IV (24 b) et une clé RC4 (1 parmi 4).
    - On en déduit la suite aléatoire de chiffrement Xsi.
  - La procédure d authentification peut être rejouée.

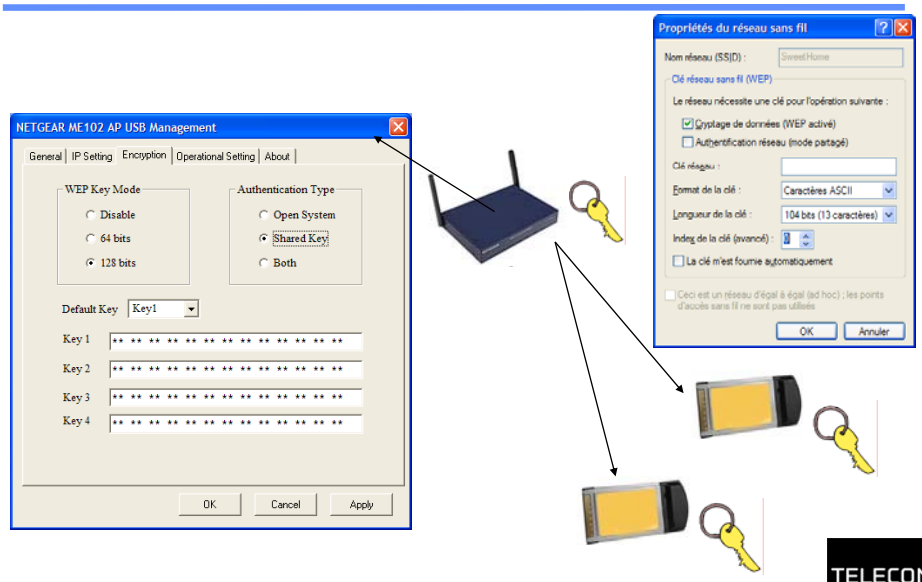
Lacunes du protocole WEP. 4/5

- **Confidentialité.**
  - Seulement 2^{24} valeurs IV.
  - 50 % de chances de réutiliser une valeur IV au bout de 4823 trames.
  - Les suites de chiffrement Xsi se déduisent des valeurs en clair.
  - 2^{40} essais (1million/s .12 jours) permettent de trouver les secrets partagés de 40 bits.
- **WEP est cassable en quelques heures.**
  - Des logiciels sont disponibles sur le WEB
  - Attaque de Fluhrer par des valeurs dites *résolvantes, IV=(B+3,255,x)* $x \in [0,255]$. Environ 60 valeurs sont nécessaires pour obtenir l'octet de la clé de rang B.

Lacunes du protocole WEP. 5/5

- **Intégrité des données.**
  - Dans une trame WEP le CRC est chiffré.
  - Le CRC est une fonction linéaire du ou exclusif, le CRC du ou exclusif (octet à octets) de deux trames de même longueurs est le ou exclusif de leur CRC respectif.
  - Le ou exclusif (octets à octets) d 'une trame WEP (chiffrée) et d 'une trame en clair fournit un CRC correcte.
  - WEP n 'assure pas l 'intégrité des données.

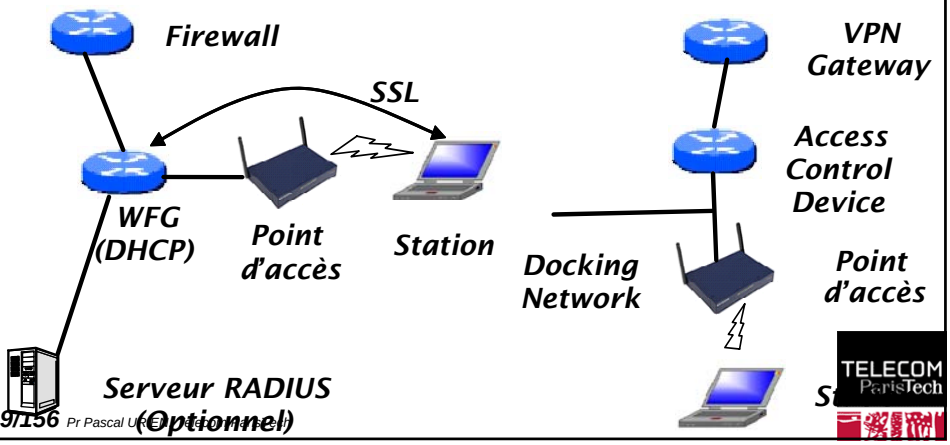
WEP + Windows



Architectures Alternatives

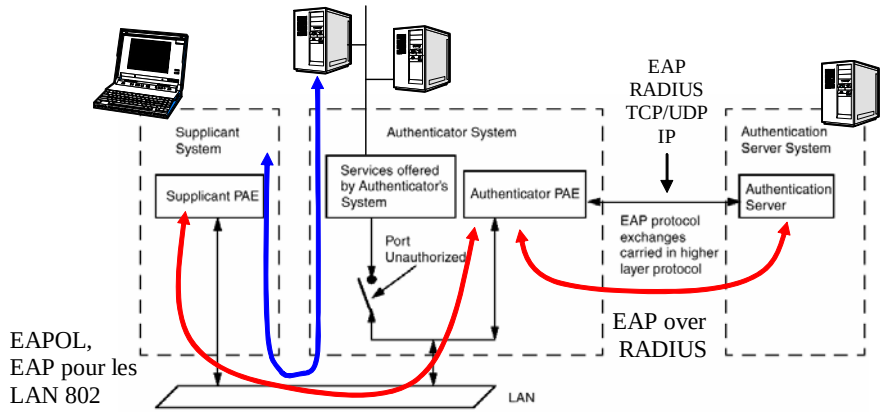
Architectures Alternatives

- **Tunnels VPN**
  - IPSEC
- **Les portails captifs**
  - WFG – *Wireless Firewall Gateway*
- *Access Control List*
  - Switch Mobile (2004)



Le modèle 802.1x

Architecture d 'authentification 802.1x. 2/2



Network Port Authentication - 802.1x. 1/2

- **Les trames émises par une station non authentifiée sont filtrées par le système d 'authentification.**
- **Les éléments de la procédure d 'authentification sont échangés via par le protocole EAP (*Extended Authentication Protocol*) .**
- **EAP est transporté par des trames 802 (EAP encapsulation over LAN) entre station et système d 'authentification.**
- **Le processus d 'authentification est conduit avec un serveur distant (et non par un AP).**
  - Architecture centralisée.
- **EAP est transporté par le protocole RADIUS (*Remote Access Dialing User Service*) entre système d 'authentification et serveur d 'authentification distant.**

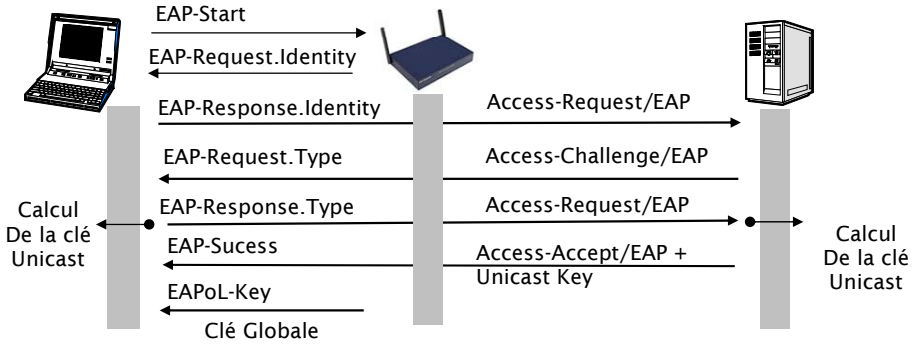
Le modèle 802.1x

- **1. L'identité du client (EAP_ID) détermine un serveur d'authentification (RADIUS). Elle est transmise au serveur RADIUS (RS), via le point d 'accès (AP).**
- **2. Le processus d 'authentification se déroule entre le client (*supplicant*) et le serveur radius (RS). Le point d 'accès (*Authenticator*) se comporte comme un relais entre ces deux entités.**
- **3. A la fin du processus d'authentification une clé unicast (ou clé maître MSK) est calculée par le client et le RS.**
- **4. La clé MSK est transmise (chiffrée) par RS vers AP, à l 'aide du protocole RADIUS.**
- **5. AP calcule alors une clé globale (WEP), il chiffre cette valeur par la clé SK, et la transmet au client (via trame EAPOL-Key).**

EAPoL key Descriptor

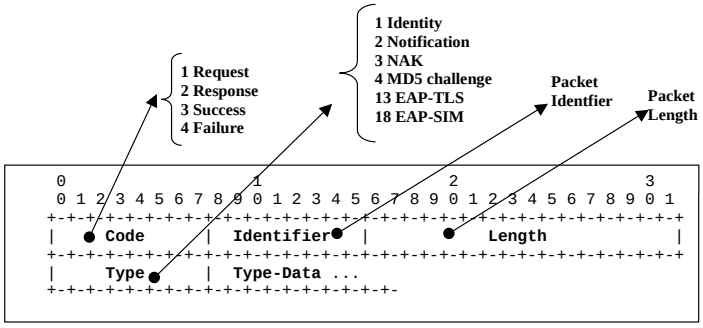
Descriptor Type – 1 octet	
Key Information – 2 octets	Key Length – 2 octets
Key Replay Counter – 8 octets	
Key Nonce – 32 octets	
EAPOL-Key IV – 16 octets	
Key RSC – 8 octets	
STA MAC Address – 6 octets	
GTK Length -2 octets	
Key MIC – 16 octets	
Key Data Length – 2 octets	Key Data – n octets

802.1x



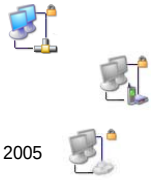
Le protocole EAP.

- **EAP est conçu pour transporter des scénarios d authentification.**
- **Quatre types de messages, requêtes, réponses, succès, échec**



EAP, what else ?

- **The Extensible Authentication Protocol (EAP) was introduced in 1999, in order to define a flexible authentication framework.**
  - EAP, RFC 3748, "Extensible Authentication Protocol, (EAP)", June 2004.
    - *EAP-TLS*, RFC 2716, "PPP EAP TLS Authentication Protocol", 1999.
    - *EAP-SIM*, RFC 4186, " Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) ", 2006
    - *EAP-AKA*, RFC 4187, " Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) ", 2006
- **EAP Applications.**
  - Wireless LAN
    - Wi-Fi, IEEE 802.1x, 2001
    - WiMAX mobile, IEEE 802.16e , PKM-EAP, 2006
  - Wired LANs
    - ETHERNET, IEEE 802.3
    - PPP, RFC 1661, "The Point-to-Point Protocol (PPP)", 1994
  - VPN (Virtual Private Network) technologies
    - PPTP, Point-to-Point Tunneling Protocol (PPTP), RFC 2637
    - L2TP, Layer Two Tunneling Protocol (L2TP), RFC 2661
    - IKEv2, RFC 4306, "Internet Key Exchange (IKEv2) Protocol", 2005
  - Authentication Server
    - RADIUS, RFC 3559, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", 2003
    - DIAMETER, RFC 4072, "Diameter Extensible Authentication Protocol Application", 2005
  - Voice Over IP
    - UMA, Unlicensed Mobile Access, http://www.umatechnology.org



Exemple 1/2

PSWD: 5678

Exemple 2/2

EAP-Start
00 30 ab 14 68 ef 00 30 ab 1a 07 8f 88 8e **01 01 00 00**

Identity-Request
00 30 ab 1a 07 8f 00 30 ab 14 68 ef 88 8e **01 00 00 05 01 a7 00 05 01**

Identity-Response
00 30 ab 14 68 ef 00 30 ab 1a 07 8f 88 8e **01 00 00 0e 02 a7 00 0e 01 41 42 43 44 5c 31 32 33 34**

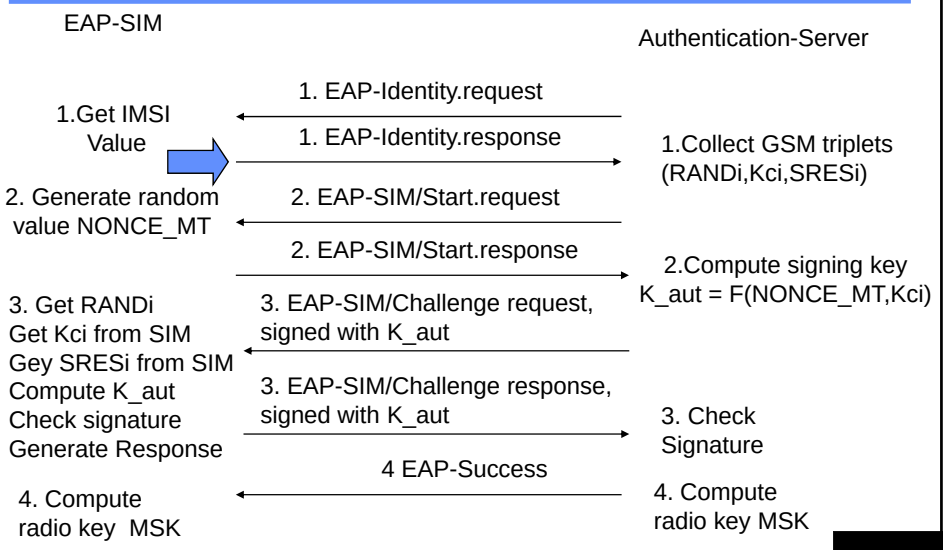
MD5-Request
00 30 ab 1a 07 8f 00 30 ab 14 68 ef 88 8e **01 00 00 06 01 a8 00 06 04 00**

MD5-Response
00 30 ab 14 68 ef 00 30 ab 1a 07 8f 88 8e **01 00 00 1f 02 a8 00 1f 04 10 3d 92 48 f4 2b be 0f 81 05 4e d4 39 87 77 a3 82 41 42 43 44 5c 31 32 33 34**

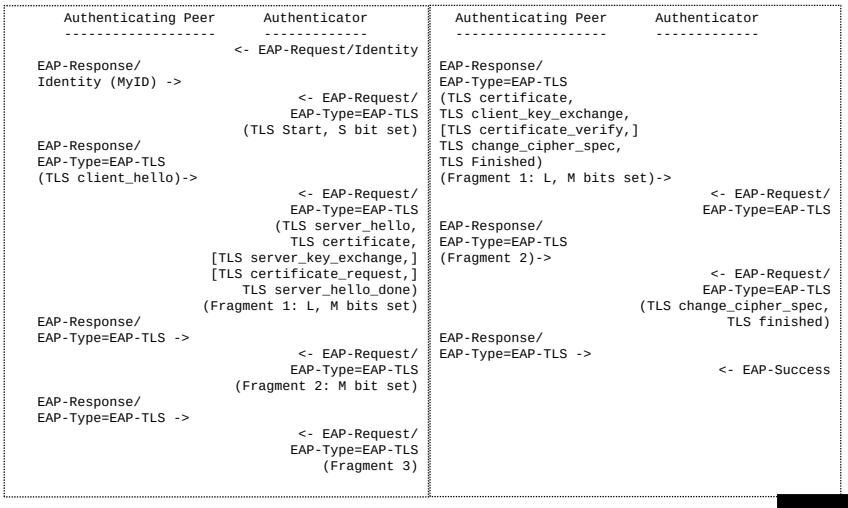
EAP-Success
00 30 ab 1a 07 8f 00 30 ab 14 68 ef 88 8e **01 00 00 05 03 a9 00 05 02**

Exemples EAP

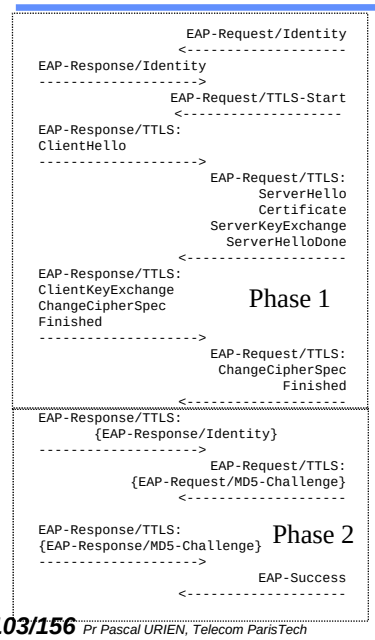
EAP-SIM



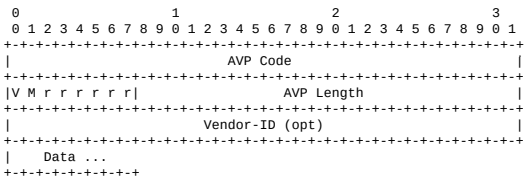
EAP-TLS



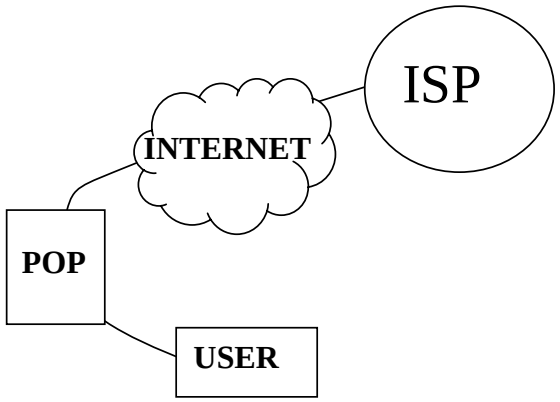
EAP-TTLS



- **TTLS works in two phases**
  - Phase 1.
    - A EAP-TTLS session open a secure TLS tunnel
    - EAP-TTLS phase 1 is very similar to EAP-TLS
  - Phase 2.
    - Multiple protocols (EAP and other) are transported and protected by the previously opened TLS tunnel.
    - Protocols are transported in AVP



RADIUS



RADIUS

- **Le protocole *Remote Authentication Dial In User Service* est spécifié par la RFC 2865. La RFC 2866 (*RADIUS accounting*) définit les attributs utiles à la facturation. Les messages sont transportés par des paquets UDP, utilisant les ports 1812 (*radius*) et 1813 (*radacct*).**
- **Un fournisseur de service Internet (ISP) réalise/vend un lien entre un terminal (PC) et son réseau IP. De manière logique le client est connecté via une liaison point à point (PPP, ADSL…) à un intranet (domaine) géré par l'ISP, qui loge les serveurs abritant les services (messagerie, site WEB, …) et offre généralement des éléments de sécurité (pare-feu, protection contre les virus …).**

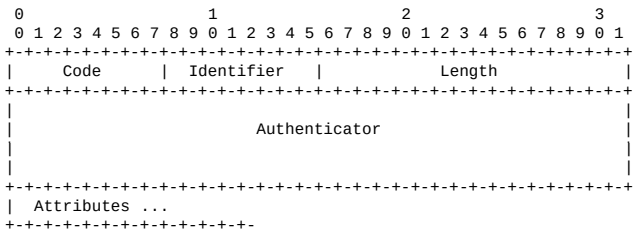
Le protocole RADIUS

- **Permet d 'échanger des services entre fournisseurs de service.**
- **Network Access Server (NAS), est un serveur réalisant l 'authentification d 'un utilisateur désirant accéder au réseau (connexion PPP, accès sans fils…).**
- **NAS se comporte comme le client d 'un serveur d 'authentification RADIUS qui stocke les paramètres d 'authentification de l'utilisateur et ses droits.**
- **Les messages entre NAS et serveur RADIUS sont signés à l 'aide d 'un secret partagé et d 'une empreinte MD5.**
- **Le protocole RADIUS est également utilisé pour la facturation.**

Sécurité Radius

- **Le NAS génère des requêtes *Access-Request*, associées à un nombre aléatoire de 16 octets (le champ *Authenticator*). La réponse du serveur d'authentification est l'un des trois messages suivants**
  - *Access-Challenge*
  - *Access-Reject*
  - *Access-Success.*
- **Elle est signée par un nombre *Response Authenticator* (16 octets), une empreinte MD5 calculée à partir des données de la réponse, du champ *Authenticator* importé de la requête, et d'un *secret partagé* .**
- **De surcroît un paquet RADIUS comporte un attribut de signature (le *Message-Authenticator* #80), qui conformément à la RFC 2104, est déduit du secret partagé et du contenu du message.**

Format des paquets RADIUS

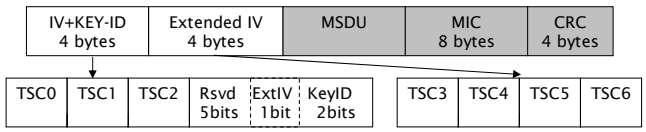


- *Code*
  - 1 Access-Request
  - 2 Access-Accept
  - 3 Access-Reject
  - 4 Accounting-Request
  - 5 Accounting-Response
  - 11 Access-Challenge
- *Identifier*
  - Identifiant d'une requête et de la réponse associée.
- *Length*
  - Longueur totale du paquet en tête incluse (à partir du champ code).
- *Authenticator*
  - Un champ de 16 octets. C'est un nombre aléatoire dans de la cas d'un message access-request.
  - Pour les paquets access-accept, access-reject, accept-challenge, accounting-response c'est l'empreinte MD5 du message (en tête incluse, à partir de code) concaténé aux valeurs RequestAuthenticator et secret partagé.
  - ResponseAuth = MD5(Code||ID||Length||RequestAuth||Attributes||Secret)
- *Attributes*
  - Type, un octet, , l'identifiant d'un attribut (0..255)
  - Length, un octet, la longueur, champ type inclus (2,...255)
  - Value, la valeur de l'attribut

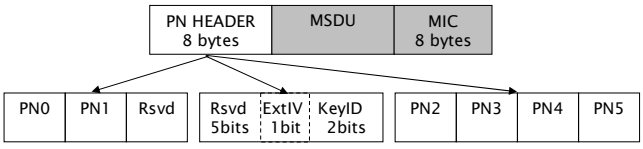
IEEE 802.11i

Ce qui est nouveau

- **Définition des** *Information Elements IE.*
- *Distribution des clés globales à l'aide d'un protocole à quatre passe.*
- *Gestion de plusieurs protocoles radio*
  - *TKIP (RC4)*
  - *CCMP (AES)*



Trame TKIP



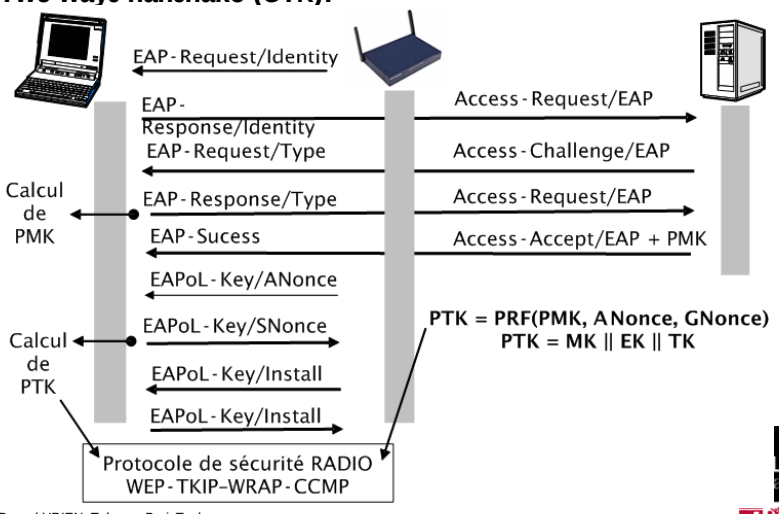
Trame CCMP

802.11i

- **Eléments d'information IE**
  - Un point d'accès diffuse dans ses trames *Beacon* ou *Probe* des éléments d'information afin de notifier aux nœuds sans fil les informations suivantes,
    - La liste des infrastructures d'authentification supportées (typiquement 802.1X)
    - La liste des protocoles de sécurité disponibles (TKIP, CCMP,…)
    - La méthode de chiffrement pour la distribution d'une clé de groupe (GTK).
  - Une station 802.11 notifie son choix par un élément d'information transmis lors de sa demande d'association.
- **Distribution de clés avec mutuelle authentification entre AP et Supplicant.**

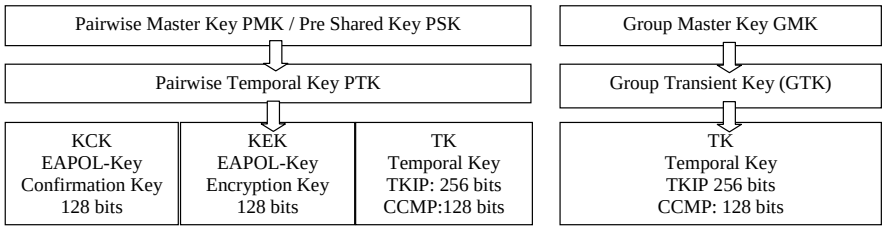
Distribution des clés

- **Four ways handshake (PTK).**
- **Two ways hanshake (GTK).**



802.11 i: Hiérarchie des clés

- PMK est déduite de l'authentification EAP.
- PSK est une alternative à PMK.
- GMK est une clé maître de groupe.



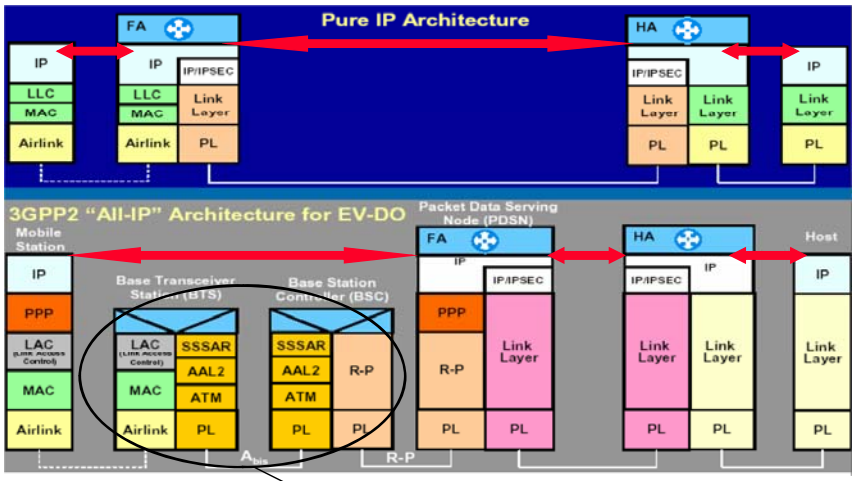
Sécurité du WiMax

« *The last mile* »

Introduction

Comparaison IEEE 802.16e - 3GPP2

Wi-Technologies



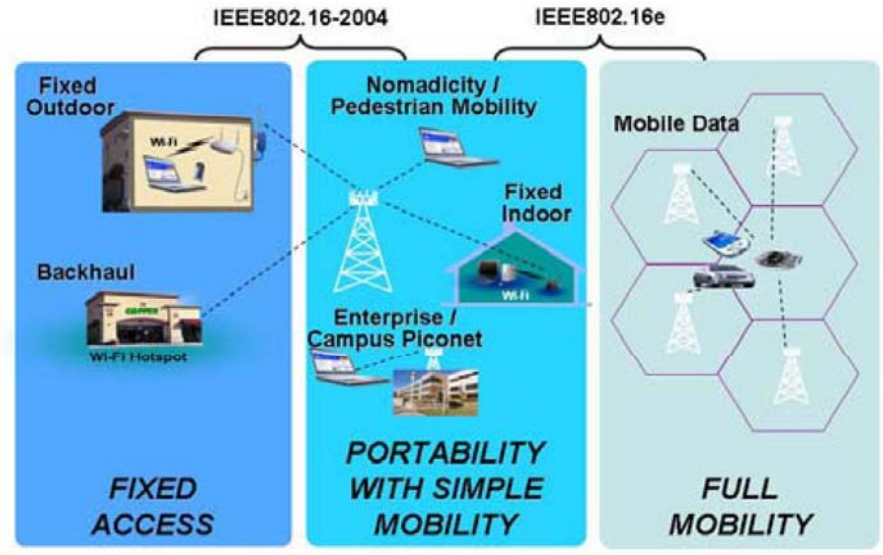
3GPP-Technologies

Non IP segment

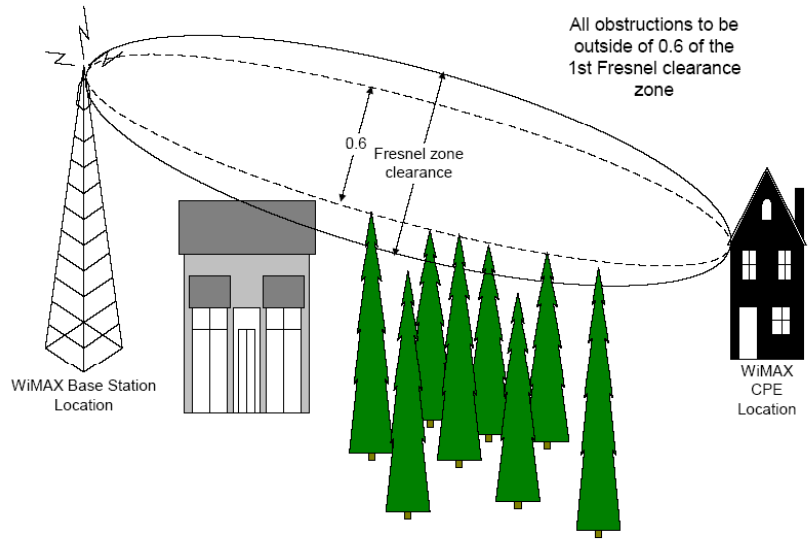
IEEE 802.16 standards 1/2

	802.16-2001 (1)	802.16a (2)	802.16-2004 (1)+(2)	802.16e
Completed	December 2001	January 2003	October 2004	December 2005
Spectrum	10 - 66 GHz	2 - 11 GHz	(1)+(2)	< 6 GHz
Bit Rate	32 – 134 Mbps in 28MHz channel bandwidth	Up to 75 Mbps in 20MHz channel bandwidth	(1)+(2)	Up to 15 Mbps in 5MHz channel bandwidth
Modulation	QPSK, 16QAM and 64QAM	OFDM 256 sub-carriers QPSK, 16QAM, 64QAM	(1)+(2)	Same as 802.16a
Mobility	Fixed	Fixed, Portable	Fixed, Portable	Nomadic/High Mobility
Channel Bandwidths	20, 25 and 28 MHz	Scalable 1.5 to 20 MHz	(1)+(2)	Same as 802.16a with UL sub-channels
Typical Cell Radius	2-5 km	7 to 10 km Max range 50 km	(1)+(2)	2-5 km

IEEE 802.16 standards 2/2

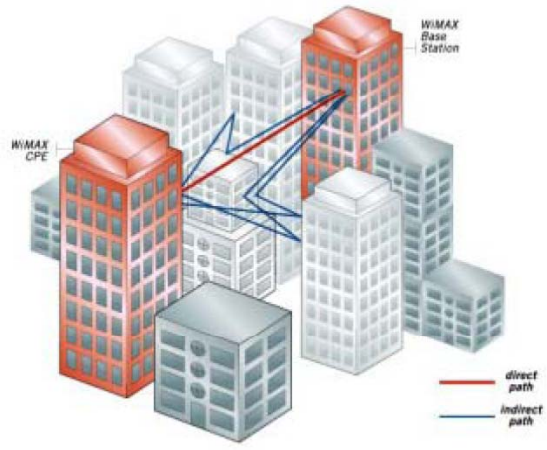


IEEE 802.16-2001, Line Of Sight



119/15 LOS Fresnel zone

IEEE 802.16-2004, Non Line Of Sight

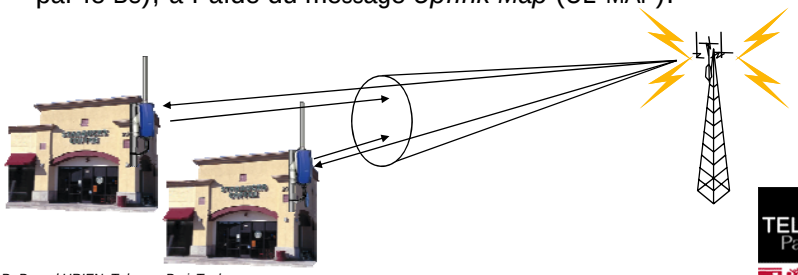


NLOS propagation

120/156 Pr Pascal URIEN, Telecom ParisTech

Le PMP

- **L'architecture du WiMAX comporte des stations de base BS** *(Base Station)* **munies de plusieurs antennes directionnelles, gérant des** *secteurs*, **et établissant des liens de type PMP** *(Point to Multi Point)*. **Dans un secteur donné, les voies descendantes (émission d'information vers les clients) et montantes (réception des données émises par les clients) sont gérées par une station de base unique.**
- **La station de base émet périodiquement des trames** *(management frames)* **décrivant la structure :**
  - des voies descendantes (*downlink frames*, données émises par le BS), à l'aide du message *Downlink Map* (DL-MAP) ;
  - des voies montantes (*upstream frames*, pour les données reçues par le BS), à l'aide du message *Uplink Map* (UL-MAP).



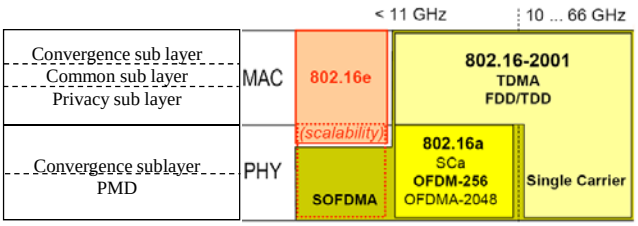
Méthodes d'Accès Radio

- **Une voie est organisée en une série de rafales** *(bursts)*, **chacune d'entre elle étant identifiée par un code DIUC** *(Downlink Interval Usage Code)* **ou UIUC** *(Uplink Interval Usage Code)*, **et caractérisée par des paramètres de modulation et de codage radio spécifiques, permettant d'obtenir des débits adaptés aux niveaux de signal et de bruit présents entre un client et une station de base. Un canal de transmission est associé à un ou plusieurs** *bursts*, **lesquels sont organisés en plusieurs canaux logiques.**
- **Le récepteur,** *Subscriber Station* **(SS) dans 802.16 ou** *Mobile Station* **(MS) dans 802.16e, analyse les trames reçues et utilise les canaux (montants) de communication pour différentes classes de service telles que administration du système (demande de connexion, allocation de qualité de service,…) ou transmission de données (en mode** *Best effort* **par exemple). La gestion des collisions d'accès aux canaux montants, est réalisée par plusieurs types d'algorithmes.**

Modèle en couches du WiMAX

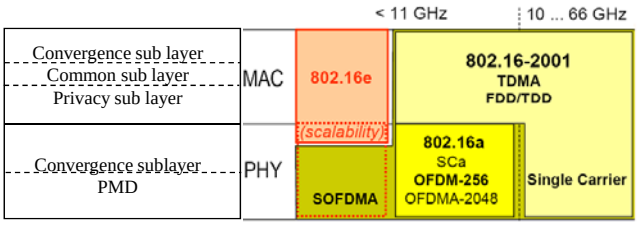
Modèle en couche du WiMAX 1/2

- La couche MAC se divise en trois éléments, une couche de convergence, une couche dite commune, et une couche de sécurité.
  - La couche de convergence (CS - *Convergence Sublayer*) réalise l'interface entre un réseau extérieur (ATM, Ethernet…) et les unités de service (MAC-SDU) échangées avec le réseau radio local (MAC-CPS, *Common Part Sublayer*). Elle gère un mécanisme de *classification*, en charge de la qualité de service, en associant à chaque identifiant de connexion 802.16 local (le *Connection IDentifier* ou CID, un nombre de 16 bits), un flux de données vers le réseau extérieur (identifié par un *Service Flow IDentifier*, SFID, un nombre de 32 bits).
  - La couche commune (CPS, *Common Part Sublayer*) est liée aux ressources physiques. Elle administre les connexions locales, applique les mécanismes de qualité de service et gère les accès (émission/réception) au niveau physique. Elle échange des SDUs avec plusieurs classes de CSs.
  - La couche de sécurité, (PS, *Privacy Sublayer*) est en charge des mécanismes d'authentification et d'échange de clés, elle assure également le chiffrement et l'intégrité des trames.



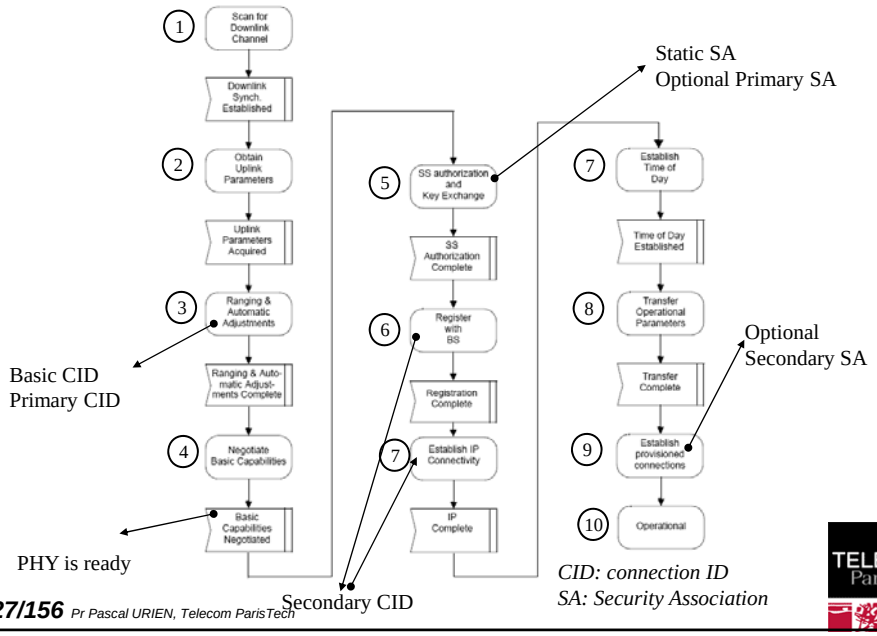
Modèle en couche du WiMAX 2/2

- La couche physique (PHY) se divise en deux parties, une couche de convergence (*Convergence Sublayer*, CS) et une couche gérant la radio (*Physical Medium Dependant*, PMD). Cependant lorsque le PMD réalise tous les services nécessaires à l'entité MAC-CPS, la couche de convergence est vide.



Procédure d'insertion d'une station WiMAX

Insertion d'une station 1/3



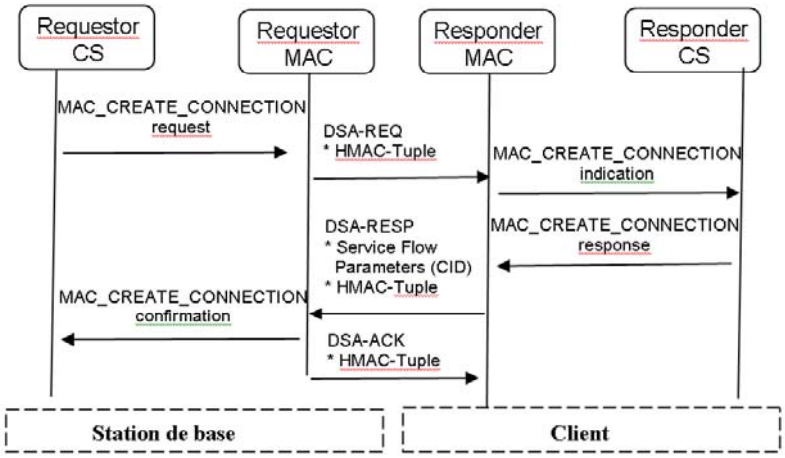
Insertion d'une station 2/3

- 1- Recherche et synchronisation avec la voie descendante. Le module de réception PHY du client analyse le signal descendant et se synchronise avec ce dernier. C'est possible en analysant les caractéristiques de la voie descendante fournies périodiquement par la station de base par le biais des messages d'administration DL-MAP. Le module MAC du client déduit grâce à DL-MAP le nombre de *bursts* de la voie descendante, puis obtient la structure des canaux, renseignée dans le message DCD (*DownLink Channel Descriptor)* ;
- 2- Acquisition des paramètres de la voie montante. Le client déduit des messages UL-MAP et UCD (*Uplink Channel Descriptor*,) l'organisation des canaux de transmission ;
- 3- Étalonnage et ajustement de la puissance d'émission. À l'aide des messages *Ranging Request* (RNG-REQ) et *Ranging Response* (RNG-RSP), le client ajuste sa puissance d'émission et obtient diverses informations de la station de base. En particulier, les paramètres *Basic Connection ID* et le *Primary Management CID* sont affectés au client par la station de base et notifiés dans la réponse RNG-RSP ;Basic CID
- 4- Négociation des paramètres de transmission. Au terme de la procédure d'étalonnage le client informe la station de base de ses capacités à l'aide du message d'administration SBC-REQ *(SS Basic Capability Request)* acquitté par un SBC-RESP *(SS Basic Capability Response)* ;
- 5- Autorisation et échange de clés. Le client et la station de base réalisent une séquence d'authentification et d'échange de clés à l'aide des messages d'administration PKM-REQ (*Privacy Key Management Request*) et PKM-RESP *(Privacy Key Management Response)*. Ce protocole utilise le *Primary Management CID* ;

Insertion d'une station 3/3

- 6- Enregistrement. Grâce à cette procédure le client devient un membre actif du réseau. Les messages *Registration Request* (REG-REQ) et *Registration Response* (REG-RSP), authentifiés par un *HMAC-tuple* (un couple valeur HMAC, index d'une clé HMAC) lui permettent d'obtenir un *Secondary Management CID*, utilisé en particulier pour des services IP tels que DHCP ;
- 7- Etablissement de la connectivité IP. La version IP utilisée par le client est indiquée dans le message REG-REQ. Le client obtient une adresse IP à l'aide du classique protocole DHCP (décrit par la RFC 2131) ;
- 8- Acquisition de la date et de l'heure. Le client obtient ces paramètres grâce au protocole défini par la RFC 868 ;
- 9- Téléchargement des paramètres de configuration. Le client obtient un fichier de configuration à l'aide du protocole TFTP (Trivial FTP, RFCs 1123 et 2349) ;
- 10- Activation des services prépayés. La station de base délivre des messages DSA-REQ *(Dynamic Service Additional Request)* au client afin d'établir les connexions nécessaires à l'activation des services. Ces messages sont acquittés par le client à l'aide de réponses DSA-RESP *(Dynamic Service Additional Response)*.

Obtention de services prépayés



Origines du protocole PKM-EAP

Data-Over-Cable Service Interface Specifications
"DOCSIS"

ETSI TR 102 469
Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Architecture

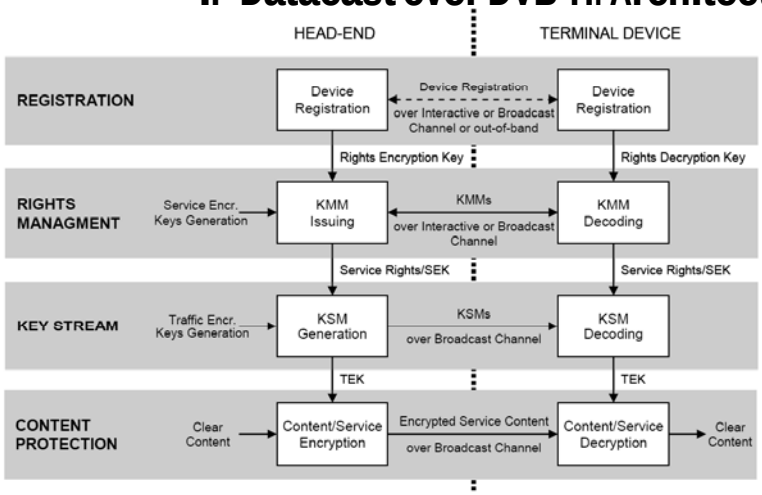
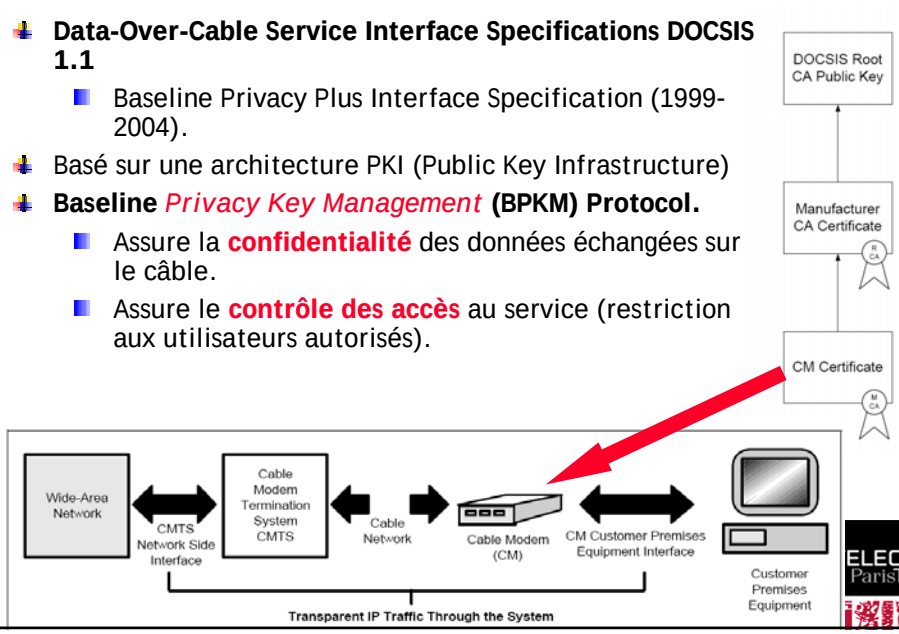


Figure 13: Hierarchical Model for Service Protection

DOCSIS: BPKM

- **Data-Over-Cable Service Interface Specifications DOCSIS 1.1**
  - Baseline Privacy Plus Interface Specification (1999-2004).
- Basé sur une architecture PKI (Public Key Infrastructure)
- **Baseline** *Privacy Key Management* **(BPKM) Protocol.**
  - Assure la **confidentialité** des données échangées sur le câble.
  - Assure le **contrôle des accès** au service (restriction aux utilisateurs autorisés).



La sécurité du WiMAX

Le modèle de sécurité 802.16-2001 & IEEE 802.16-2004

- Les fonctions de sécurité sont assurées par deux entités fonctionnelles, la première réalise le protocole PKM qui permet l'authentification d'un client et la sélection d'une suite d'algorithmes cryptographiques et de clés associées, la deuxième gère le chiffrement des trames MAC.
- Le protocole PKM est un héritage des normes IEEE 802.14 (*Cable-TV access method and physical layer specification*) puis DOCSIS (*Data-Over-Cable Service Interface Specifications*).
- Il est transporté dans des messages MAC d'administration de type PKM-REQ ou PKM-RESP (respectivement des requêtes et des réponses). Les fonctions de sécurité, c'est à dire l'authentification des messages d'administration et le chiffrement des trames d'information, s'appuient sur un jeu de trois types de clés
  - 1- Une clé d'autorisation (en abrégé AK, *Authorization Key*), à partir de laquelle sont déduites les clés d'authentification (HMAC) des messages d'administration.
  - 2- Une clé de chiffrement de clé (en abrégé KEK, *Key Encryption Key*); elle est directement calculée à partir de la valeur AK.
  - 3- Des clés de chiffrement de trames de données (en abrégé TEK, *Trafic Encryption Key*). Elles sont transmises chiffrées à l'aide de la clé KEK et d'un algorithme cryptographique négocié lors de la phase d'authentification du client.
- Les procédures d'authentification et de distribution de clés cryptographiques sont gérées par deux machines d'état distinctes, la machine d'état d'autorisation et la machine d'état de distribution de TEK.

Transport des messages PKM 1/4

Generic MAC header format

HT=0 (1)	EC (1)	Type (6)	ESF (1)	CI (1)	EKS (2)	Rsv (1)	LEN MSB (3)
LEN LSB (8)			CID MSB (8)				
CID LSB (8)			HCS (8)				

msb → lsb

MAC Header	Payload (optional)	CRC (optional)

MAC Management message format

Management Message Type	Management Message Payload

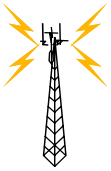
9	PKM-REQ	Privacy Key Management Request	Primary Management
10	PKM-RSP	Privacy Key Management Response	Primary Management or Broadcast ~~(optional)~~[a]

Structure des messages PKM 2/4

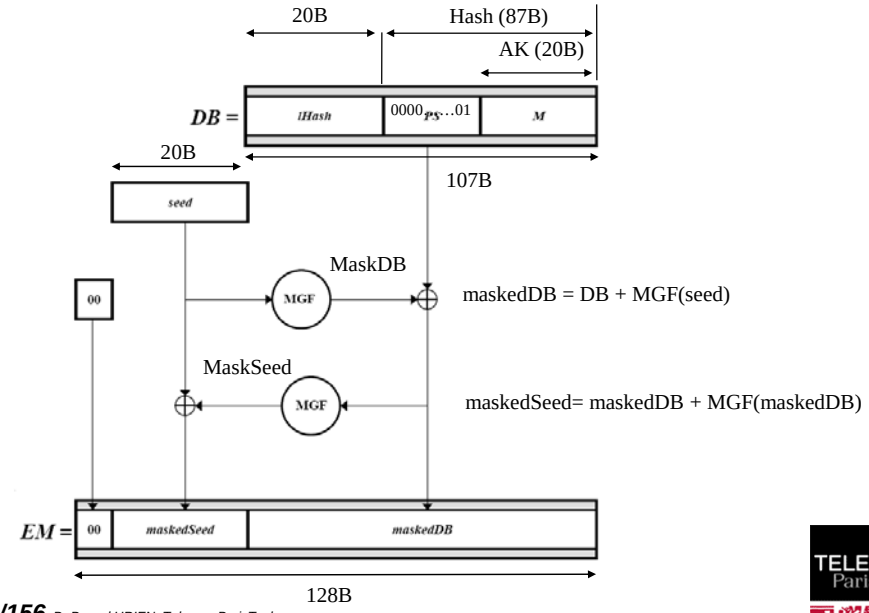
- Les messages PKM sont insérés dans des trames MAC d'administration (*management frames*) PKM-REQ et PKM-RESP.
- Ils comportent:
  - un entête indiquant un code du message (1 octet)
  - une étiquette (*identifier*, 1 octet) telle que la valeur incluse dans la réponse soit égale à celle de la requête correspondante.
  - Une liste d'attributs

```
PKM-REQ_Message_Format()
{
Management Message Type (1 octet) = 9 (requête) ou 10 (réponse)
Code (1 octet)
PKM identifier (1 octet)
Attributs encodés sous forme TLV (Type Longueur Valeur)
}
```

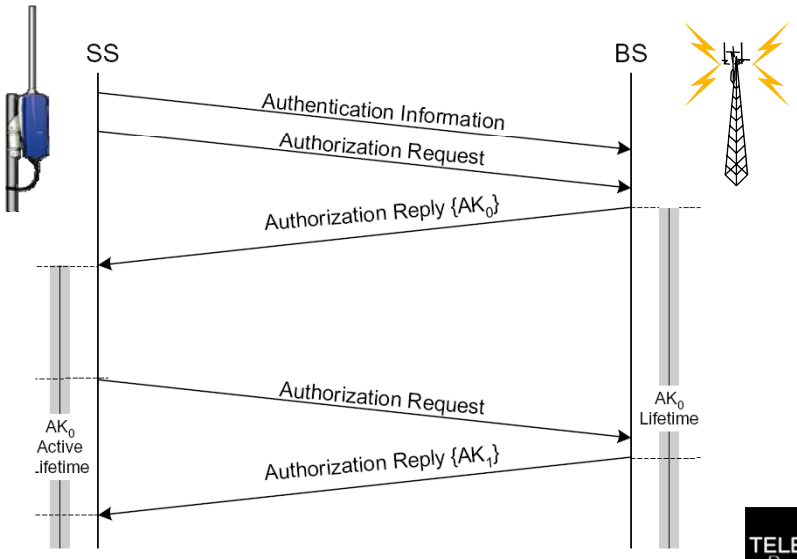

Procédure d'autorisation dans IEEE 802.16-2004



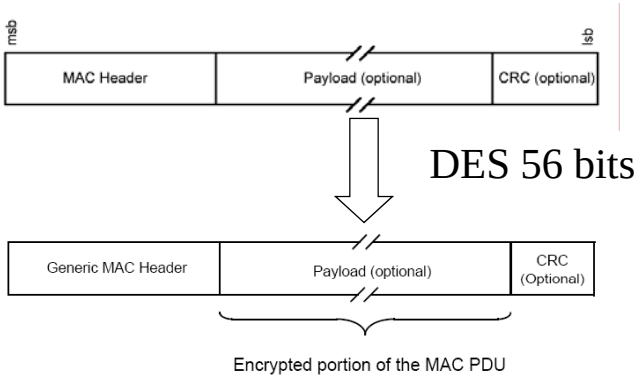
RSAES-OAEP



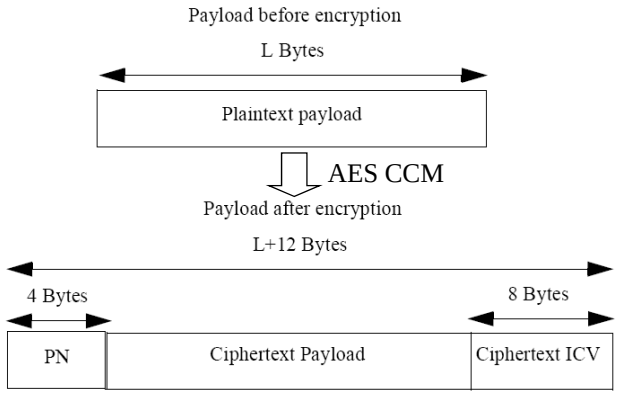
La distribution des clés TEKs (Traffic Encryption Key)



Chiffrement des données (IEEE 802.16-2001)



Chiffrement des données 802.16-2004, AES-CCM



PN: Packet Number

ICV: Integrity Check Value

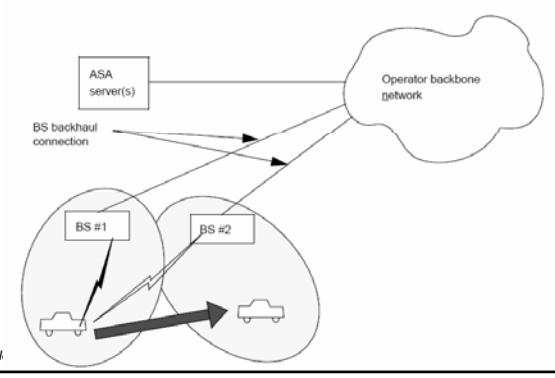
Associations de sécurité

- **Autorisation**
  - le certificat X.509 du client ;
  - une clé AK de 160 bits ;
  - un index de 4 bits de la clé AK, le *Key-Sequence-Number* ;
  - la durée de vie de la clé AK (70 jours par défaut) ;
  - une clé de chiffrement KEK associée à un algorithme de transport de clé TEK (par exemple 3-DES) ;
    - KEK=Truncate(SHA1(K_PAD_KEK | AK),128)
    - K_PAD_KEK=0x53 repeated 64 times, i.e., a 512 bit string.
  - deux clés de signature de 160 bits pour les liaisons descendantes et montantes, associées à un algorithme HMAC ;
    - HMAC_KEY_D=SHA1(H_PAD_D|AK), H_PAD_D=0x3A repeated 64 times
    - HMAC_KEY_U=SHA1(H_PAD_U|AK), H_PAD_U=0x5C repeated 64 times
  - une clé de signature de 160 bits pour les infrastructures MESH.
    - HMAC_KEY_G
- **Données**
  - un identifiant de 16 bits (SAID) ;
  - un algorithme de chiffrement, par exemple DES-CBC est l'unique alternative offerte par la version 802.16-2001 ;
  - deux clés de chiffrement TEK, une pour chaque sens de communication ;
  - deux index de 2 bits pour les TEKs ;
  - la durée de vie des clés TEK (30 minutes par défaut) ;
  - un vecteur d'initialisation IV (64 bits) associée à une TEK puisque les algor utilisés sont de type chaîné ;
  - le type de l'association de sécurité : primaire, statique ou dynamique

IEEE 802.16e

IEEE 802.16e

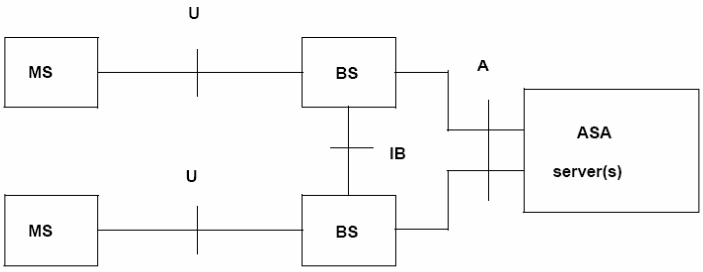
- **Le standard IEEE 802.16e apporte des améliorations de sécurité à la précédente version 802.16-2004, et s'adapte à des stations clientes se déplaçant à des vitesses automobiles usuelles; il introduit des accès réseaux hauts débits destinés à des applications fixes ou mobiles. Il intègre également des recommandations permettant de gérer des mécanismes de handover, c'est-à-dire le changement rapide de stations de base. Cette norme utilise des bandes de fréquences inférieures à 6 GHz, dont l'usage est soumis à l'obtention d'une licence.**



La sécurité IEEE 802.16e

- **L'architecture du réseau comporte des stations mobiles (*mobile station*, MS), communiquant avec des stations de base** *(Base Station BS)*.
- **Ces dernières sont reliées à un réseau d'opérateur** *(Operator Backbone Network)* **qui possède généralement un centre d'authentification et d'autorisation** *(Authentication and Service Authorization Server, ASA)*, **c'est-à-dire une base de données qui centralise toutes les informations des comptes clients ainsi que les paramètres utilisés pour leur identification.**

- L'interface U gère les services entre mobile et station de base.
- L'interface IB transporte des messages entre stations de base destinés à gérer les procédures de handover.
- L'interface A achemine des paquets d'authentification entre stations de base et serveurs ASAs.



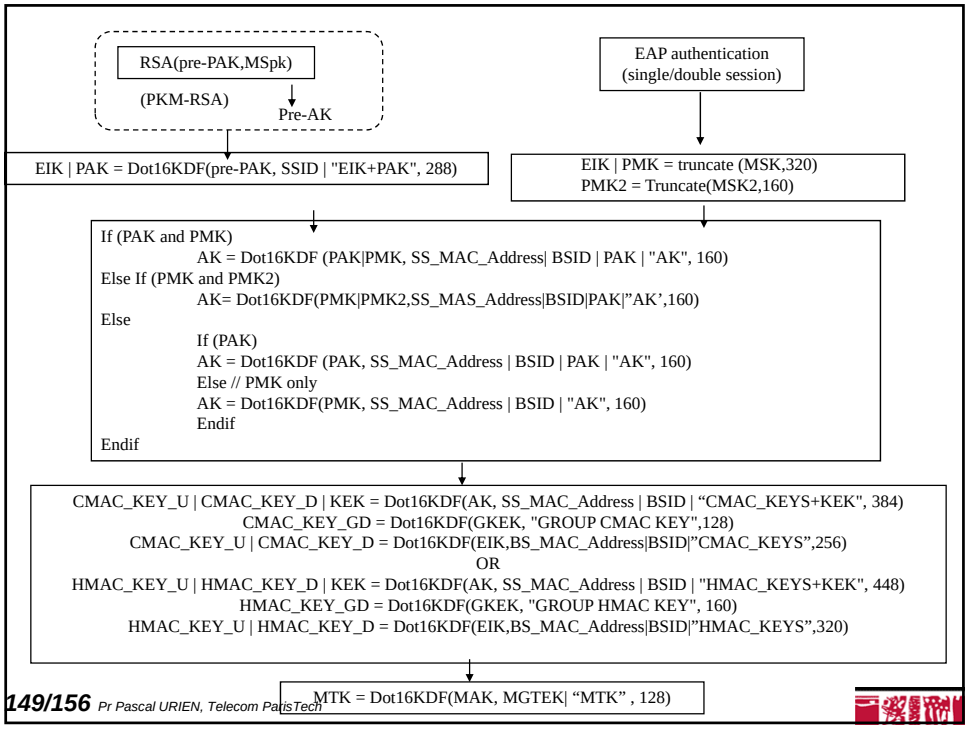
La sécurité IEEE 802.16e

- La norme identifie deux classes d'infrastructures, la première n'est pas liée à un opérateur ; la deuxième est typiquement gérée par un opérateur de téléphonie mobile. En fonction de ces contraintes, mais également pour des raisons de compatibilité avec les versions antérieures, deux types de mécanismes d'authentification sont définis, PKM-RSA importé de IEEE 802.16-2004 et PKM-EAP permettant la réutilisation du protocole EAP (Extensible Authentication Protocol, RFC 3748).
- Deux versions du protocole de gestion de clés PKM sont proposées ; la première PKMv1 est compatible avec des environnements conformes à l'IEEE 802.16-2004 ; la deuxième PKMv2 intègre de nouveaux éléments tels que :
  - Une authentification mutuelle entre station de base et mobile ;
  - L'usage de mécanismes basés sur RSA et/ou sur le protocole EAP ;
  - Une hiérarchie de clés modifiée ;
  - Le remplacement de la procédure HMAC-SHA1, basée sur une empreinte SHA1 (dont la solidité cryptographique est incertaine) par l'algorithme AES-CMAC;
  - Une nouvelle méthode de chiffrement, AES-key-wrap pour le transport des clés TEK. Cet algorithme, qui fait l'objet d'une recommandation NIST, réalise un chiffrement AES avec une clé de 128 bits et intègre de surcroît une valeur d'intégrité (ICV, Integrity Check Value), ce qui renforce la sécurité du procédé de distribution des clés TEK ;
  - La notion de pré authentification, c'est à dire un protocole permettant à un mobile et une station de base de partager une clé d'authentification sans procédure d'authentification mutuelle. Le standard 802.16e ne définit pas de méthode particulière pour le calcul de AK, mais nous remarquerons qu'il pourrait être basé sur les valeurs de l'adresse MAC du client et de l'identifiant de la station de base ;
  - Le service MBS (Multicast Broadband Service). Comme son nom l'indique, il est destiné à la diffusion d'informations, typiquement multimédia. Les mécan de sécurité permettent par exemple de déployer efficacement des infrast de type Pay TV (télévision payante).

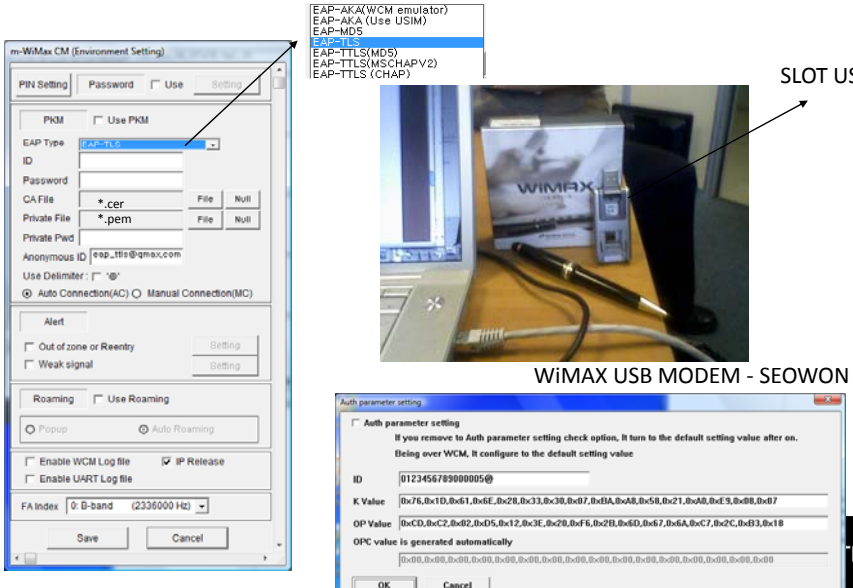
Hiérarchie des clés

Clés	Caractéristiques
Pre Primary AK Pre-PAK	Cette clé est gérée par la station de base et transmise chiffrée par la clé RSA publique du client lors d'une phase optionnelle PKM-RSA
Primary AK PAK	La clé PAK est déduite de la clé pre-PAK à l'aide d'une fonction Dot16KDF et de paramètres d'entrée tels que l'adresse MAC du client et l'identifiant de la station de base. Cette valeur intervient dans le calcul de la clé d'authentification AK
Master Session Key MSK	Cette clé est obtenue au terme d'une première session d'authentification EAP. Elle intervient dans le calcul des clés EIK et PMK
EAP Integrity Key EIK	Cette clé est calculée à partir de la clé pre-PAK ou à partir d'une clé MSK. Elle est utilisée pour authentifier les messages EAP lors d'une première occurrence (EIK=f(pre-PAK)), ou d'une deuxième occurrence (EIK=f(MSK)) d'une session d'authentification .
Master Session Key 2 MSK2	Cette clé est obtenue au terme d'une deuxième session d'authentification EAP. Elle intervient dans le calcul de la clé PMK2
Pairwise Master Key PMK	Cette clé est déduite de MSK. Elle intervient dans le calcul de la clé d'autorisation AK
Pairwise Master Key 2 PMK2	Cette clé est déduite de MSK2. Elle intervient dans le calcul de la clé d'authentification AK
Authorization Key AK	La clé AK est obtenue à l'aide d'une fonction Dot16KDF et de paramètres additionnels tels que les clés PAK, PMK, PMK2, l'adresse MAC du client et l'identifiant de la station de base

Clés	Caractéristiques
Key Encryption Key KEK	La clé de chiffrement de clé KEK est déduite de la valeur AK. Elle est utilisée pour le chiffrement des clés TEK
Traffic Encryption Key TEK	La clé de chiffrement de trafic TEK est générée par la station de base et transmise chiffrée au client au moyen de la clé KEK. Elle est utilisée pour le cryptage des trames de données
Clé CMAC ou HMAC de la voie montante C/HMAC_Key_U	Cette clé est en règle générale déduite de AK, de l'adresse MAC du client et de l'identifiant de la station de base. Elle authentifie les messages de la voie montante
Clé CMAC ou HMAC de la voie descendante C/HMAC_Key_D	Cette clé est en règle générale déduite de AK, de l'adresse MAC du client et de l'identifiant de la station de base. Elle authentifie les messages de la voie descendante
Group Key Encryption Key GKEK	Cette clé est générée par la station de base et transmise chiffrée au client, à l'aide de la clé TEK. Elle est utilisée pour le chiffrement d'une clé de groupe GTEK (*Group Traffic Encryption Key*)
Clé de groupe de la voie descendante C/HMAC_Key_GD	Cette clé est obtenue à partir de la valeur GKEK. Elle est utilisée par certains messages du protocole PKMv2
Group Traffic Encryption Key GTEK	La clé GTEK est produite de manière aléatoire par la station de base et diffusée aux clients chiffrée par la clé GKEK. Elle est utilisée pour transmettre des informations aux membres d'un groupe
MBS Transport Key MTK	La clé MTK est déduite d'une clé GTEK et d'une clé secrète MAK (MBS AK) dont le mode de distribution n'est pas précisé pa Cette valeur peut être utilisée pc de diffusion, telle que télévis



Un exemple de modem WiMAX



Dot16KDF (*Key Derivation Function*)

```
Dot16KDF(key, astring, keylength)
{
        result = null;
        Kin = Truncate (key, 128);
        for (i = 0;i <= int((keylength-1)/128); i++)
                { result <= result | Truncate (CMAC(Kin, i | astring | keylength), 128); }
        return Truncate (result, keylength);
}
```

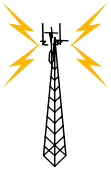
OR

```
Dot16KDF(key, astring, keylength)
{
        result = null;
        Kin = Truncate (key, 160);
        for (i = 0;i <= int((keylength-1)/160); i++)
                { result <=  result | SHA-1( i | astring | keylength | Kin);} }
        return Truncate (result, keylength);
}
```


PKMv2 - RSA

MS

BS



PKMv2 RSA-Request
(*MS_Random, MS_Certificate, SAID, SigSS*

Signature du mobile

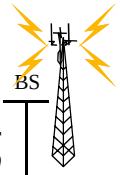
PKMv2 RSA-Reply
(*MS_Random, BS_Random, Encrypted pre-PAK,*
Key-Lifetime, Key-Sequence-Number, BS_Certificate, SigBS)

Signature de la station de base

PKMv2 RSA-Acknowledgement
(*BS_Random, Auth Result Code, Display-String, SigSS,*)

PKMv2 – EAP (Simple)

MS



BS

PKMv2 Authenticated-EAP-Transfer
(*EAP_Payload, C/HMAC Digest{EIK}*)
ou PKMv2 EAP-Transfer
(*EAP_Payload*)

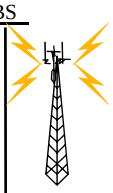
PKMv2 Authenticated-EAP-Transfer
(*EAP_Payload, C/HMAC Digest{EIK}*)
ou PKMv2 EAP-Transfer
(*EAP_Payload*)

PKMv2 Authenticated-EAP-Complete
(*EAP_Payload, C/HMAC Digest{EIK}*)

PKMv2-EAP (Double)

MS

BS



PKMv2 EAP-Start
(MS-Random, *Key-Sequence-Number, C/HMAC Digest{AK}*)

PKMv2 EAP-Transfer
(*EAP_Payload*)

PKMv2 EAP-Transfer
(*EAP_Payload*)

PKMv2 Authenticated-EAP-Complete
(*EAP_Payload, Key-Sequence-Number, C/HMAC Digest{AK}*)

PKMv2 EAP-Start
(MS-Random, *Key-Sequence-Number, C/HMAC Digest{AK}*)

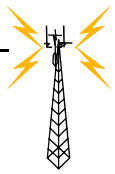
PKMv2 Authenticated-EAP-Transfer
(*EAP_Payload, Key-Sequence-Number, C/HMAC Digest{AK}*)

PKMv2 Authenticated-EAP-Transfer
(*EAP_Payload, Key-Sequence-Number, C/HMAC Digest{AK}*)

PKMv2 Authenticated-EAP-Transfer
(*EAP_Payload, C/HMAC Digest{AK}*)

PKMv2 - SA-TEK 3-ways handshake

MS



BS

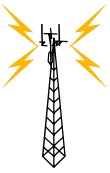
PKMv2 SA-TEK-Challenge
(BS_Random, Key-Sequence-Number, **AKID**, Key-Lifetime, HMAC/CMAC-Digest

PKMv2 SA-TEK-Request
(MS_Random, BS_Random, Key-Sequence-Number, AKID, Security-Capabilities, Security-Negociation-Parameters, PKMv2-Configuration-Settings, HMAC/CMAC-Digest)

PKMv2 SA-TEK-Response
(MS_Random, BS_Random, Key-Sequence-Number, AKID, SA_TEK_Update, Frame-Number, SA-Descriptor(s), Security-Negociation-Parameters, HMAC/CMAC-Digest)

PKMV2 – Distribution des clés TEK

MS



BS

PKMv2 Key-Request
(Key-Sequence-Number, SAID, Nonce, HMAC/CMAC-Digest

PKMv2 Key-Reply
(Key-Sequence-Number, SAID, TEK-Parameters, TEK-Parameters, GKEK-Parameters, GKEK-Parameters, Nonce, HMAC/CMAC-Digest)

PKMv2 Group-Key-Update
(Key-Sequence-Number, GSAID, Key-Push-Modes, Key-Push-Counter, GTEK-Parameters, GTEK-Parameters, HMAC/CMAC-Digest)