Evolution des Réseaux sans fil

L'évolution des technologies réseaux

- **Réseaux analogiques ("L'âge de l'arbre")**
  - **1876**, Alexander Graham Bell invente le téléphone. L'architecture du réseau est basée sur des connections point à point, établies manuellement. Les compagnies téléphoniques construisent et contrôlent tous les composants du réseau.
- **Les réseaux numériques (première ébauche de grille dans l'arbre)**
  - **1948.** Claude Elwood Shannon invente le concept d'information numérique. L'architecture réseau est basé sur des commutateurs numériques, les "switchs".
- **Les réseaux IP (la grille envahit l'arbre)**
  - **1981**. Jon Postel, Steve Crocker, et Vint Cerf inventent le réseau Internet qui substitue les routeurs aux commutateurs. Le réseau est administré par de multiples organisations.
- **Réseaux Abstraits (L'âge du *Boogie Woogie*)**
  - L'IP sans fil (**1999**) et accès large bande (*Broadband Access*) (**2005**)
  - Le réseau devient abstrait. Les accès (technologies câblées, large bande, Wi-Fi, WiMax…), et les services (eMail, Skype, Messenger, UMA…) sont gérés par de multiples organisations.

Illustration of Network ages

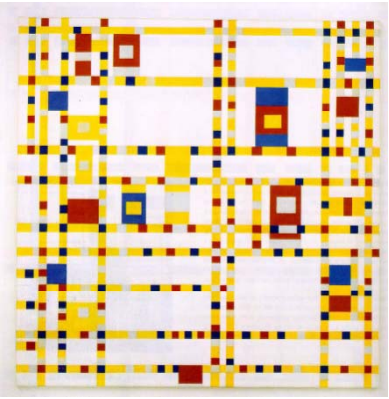
**Piet Mondrian*

"*Red tree"

"*Gray tree"

"*Apple tree"

"*Boogie Woogie"

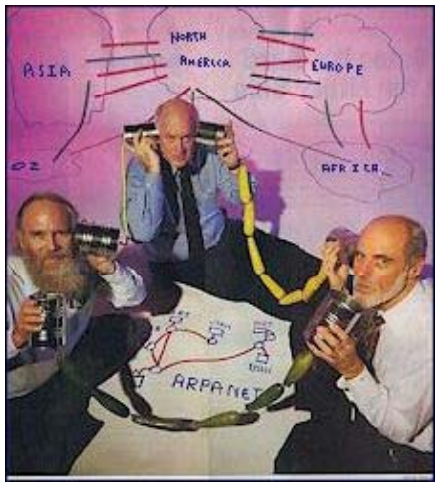


Alexander Graham Bell (1876).

Analog Networks

Claude Elwood Shannon (1948)

Digital Networks



Jon Postel, Steve Crocker Vint Cerf (1981)

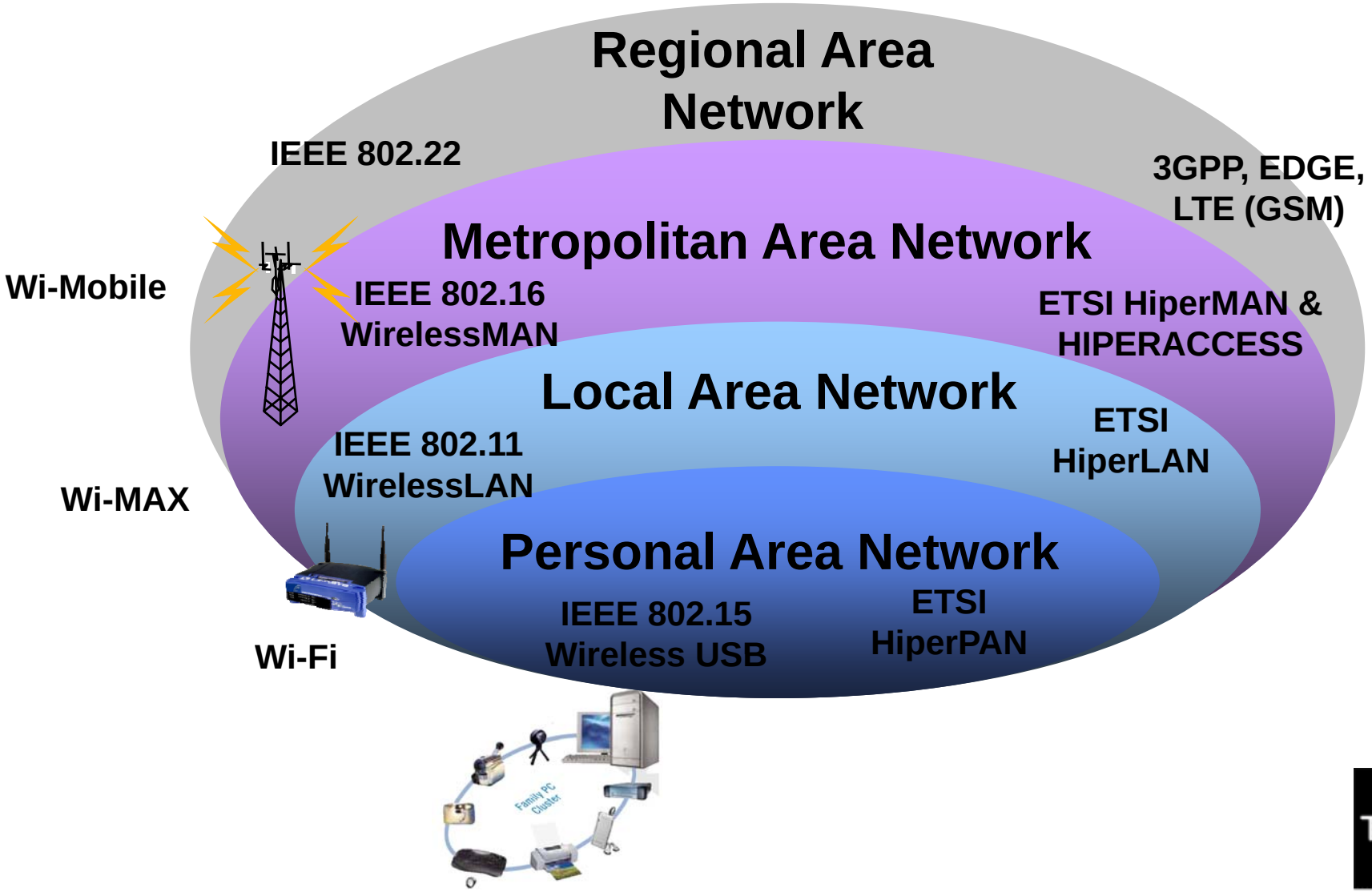
IP Networks

Wireless LAN (1999)
Broadband Access

Abstract Networks

ParisTech

Projets IP sans fil



Services sans fil.

UWB

802.15
BlueTooth

802.11

802.16
Wi-Max

802.16e

Réseau
de Transport
(IP, autre)

Core Network
(RTC,
GPRS,
UMTS,
802.20 …)

Réseau Mère
(HOME
NETWORK)

WEB

WEB

ADSL

Hotspot
(802.11
Wi-Fi)

Réseau Visité
Réseau d'Accès
(FOREIGN
NETWORK)

UMTS

GSM
GPRS

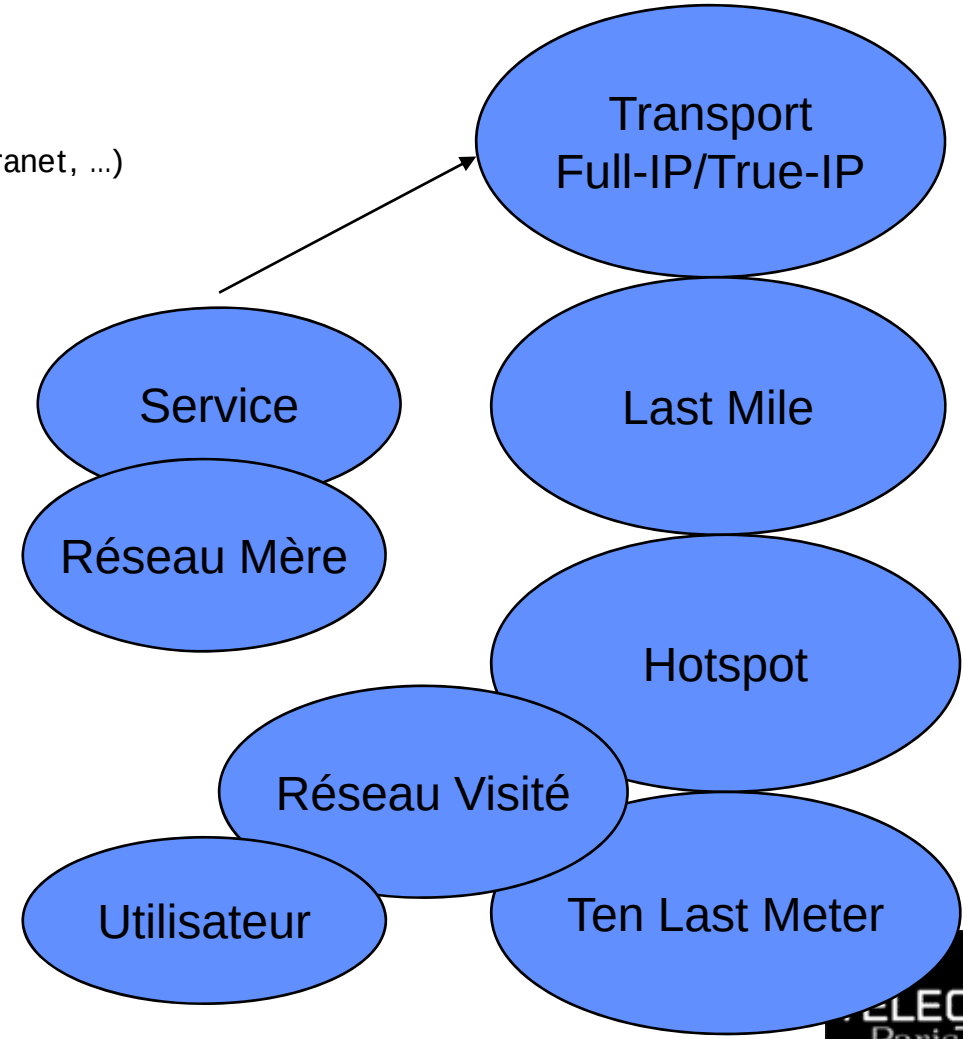
802.11

Wi-Fi

Wireless
USB

Services & infrastructures

- **Deux classes de services**
  - Multimédia
    - Voix
    - Images
  - Données
    - Accès au réseau mère (messagerie, intranet, …)
    - Accès au WEB
- **Infrastructure**
  - Réseau Mère
  - Réseau de transport
  - Réseau visité / Réseau d'accès
- **Distances.**
  - 1km – 10 km (GSM, GPRS, UMTS, LTE)
  - Last Mile (802.16) 2,5 km - 50 km
  - 100 m (Wi-Fi, UWB)
  - 10 m, Bluetooth, 802.15, UWB
- **Les débits**
  - 802.11 - Wi-Fi (11- 50 Mbit/s)
  - 802.16a – Wi-Max, jusqu'à 75 Mbit/s
  - 802.16e – Wi-Max , 5 Mbit/s
  - UMTS 2 Mbit/s
  - GPRS 32 Kbit/s
  - GSM donnés-9600 bit/s, voix-13Kbit/s
  - Bluetooth, < 1 Mbit/s

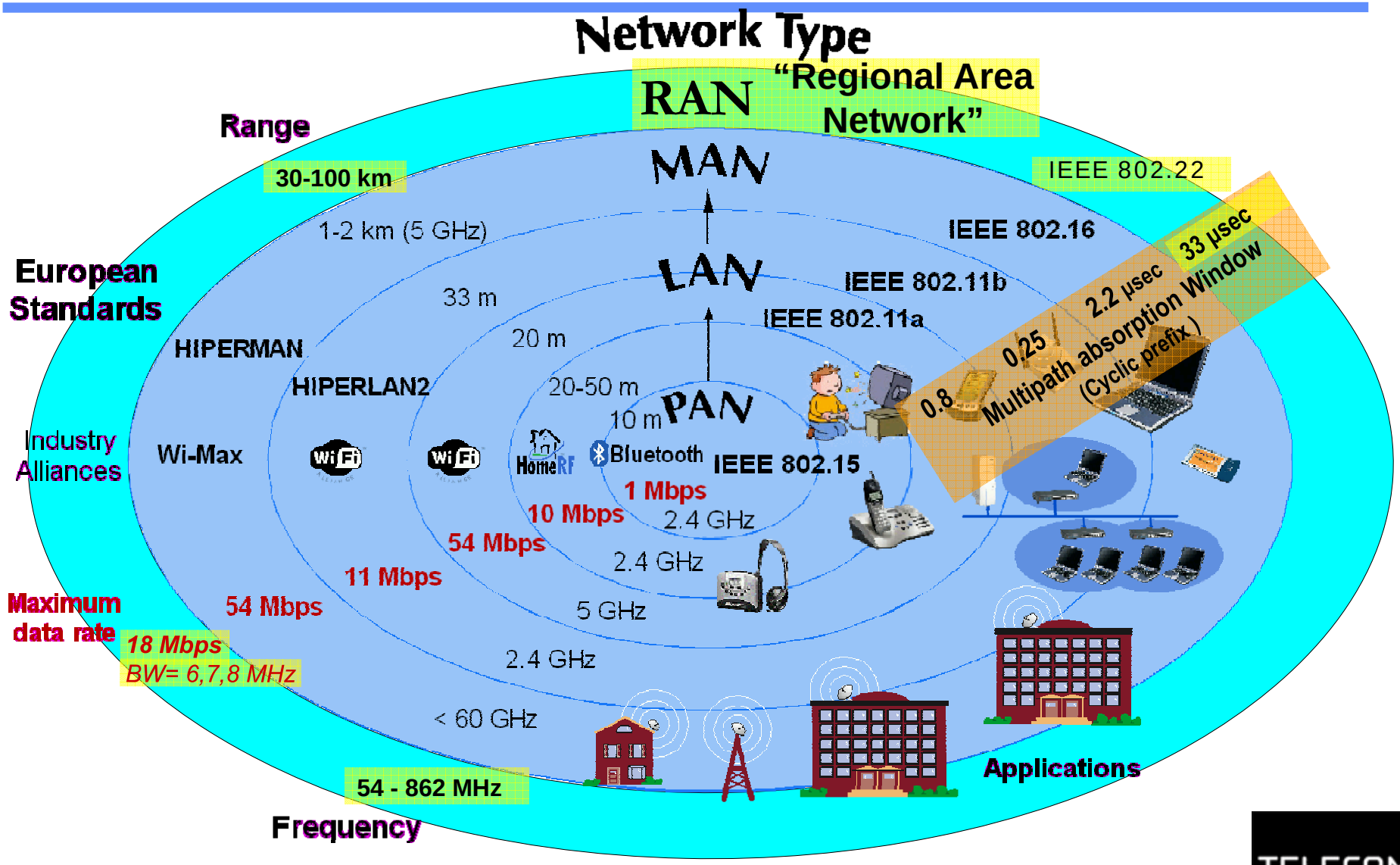


Evolution des réseaux sans fil.

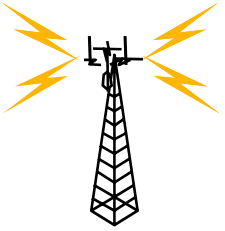
- **2G Global System for Mobile Communication.**
  - Voix 13 Kbit/s - Short Message SMS 160 octets.
- **2,5G General Packet Radio Service.**
  - Mode paquet - Débit < 32 Kbit/s
- **3G Universal Mobile Telecommunication System.**
  - Mode Paquet - Débit < 2 Mbits.
- **4G Wireless Local Area Network**
  - 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

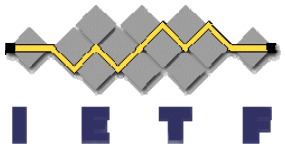
TELECOM ParisTech

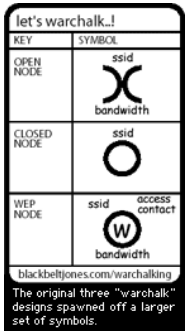
Standards IEEE

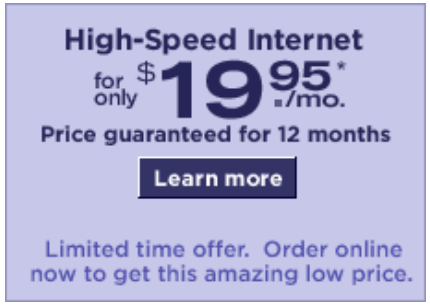


En 2009, les réseaux sans fil sont déjà partout !









TELECOM ParisTech

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

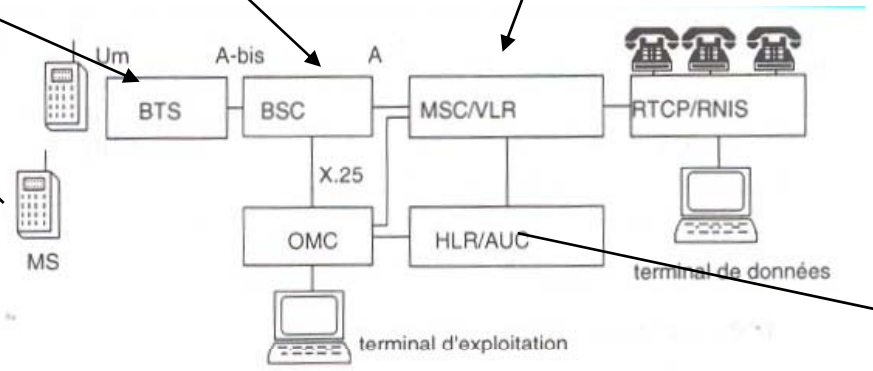
Base Station (BTS)

Base Station Controler (BSC)

MSC+VLR

RTC

HLR+AuC



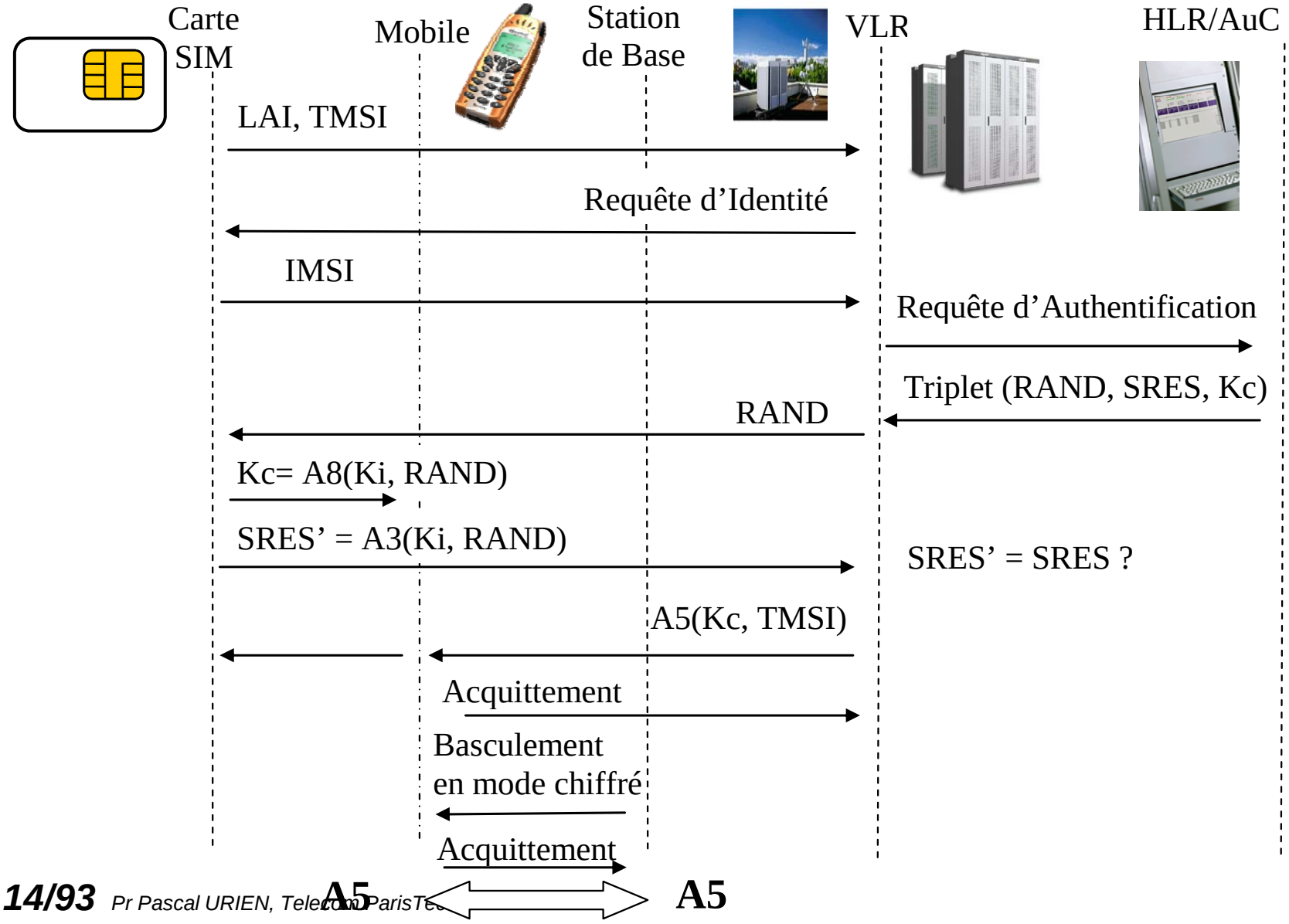
terminaux d'abonnés	sous-système radio	sous-système réseau	réseau téléphonique commuté public

TELECOM ParisTech

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



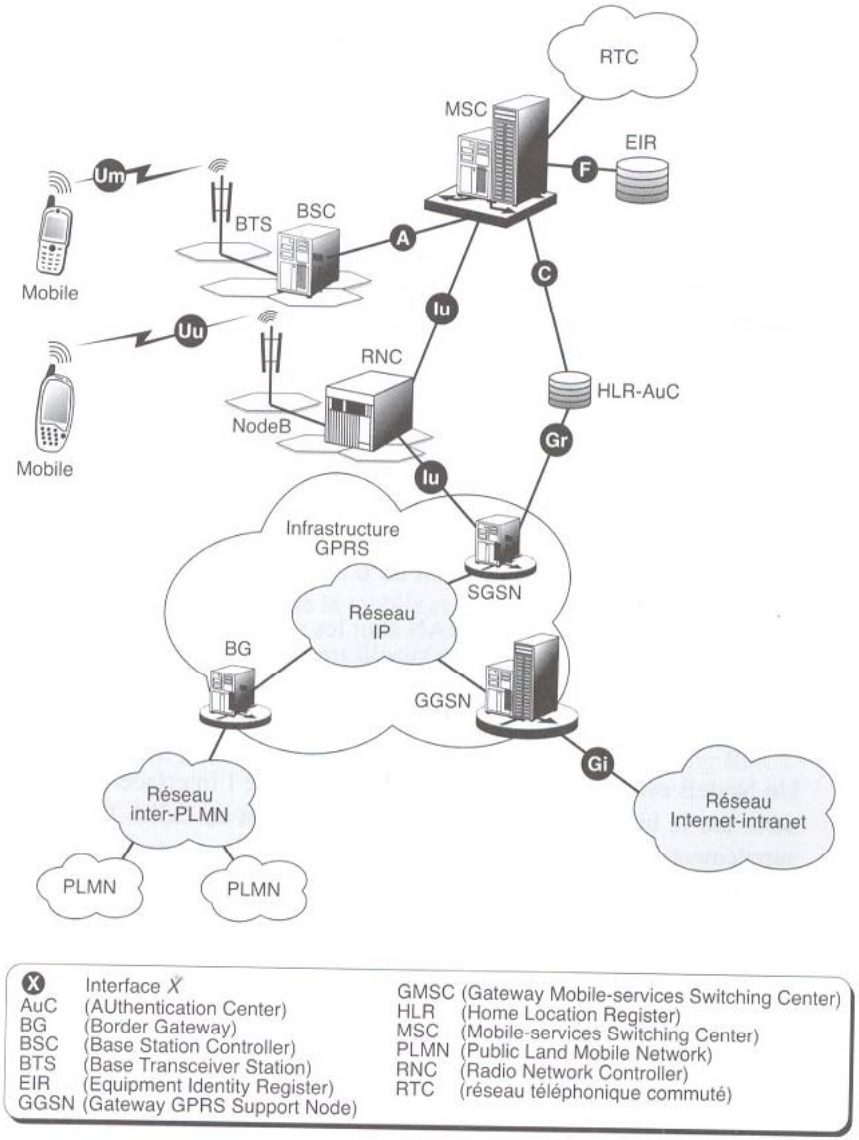
Eléments d'identifications

- **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

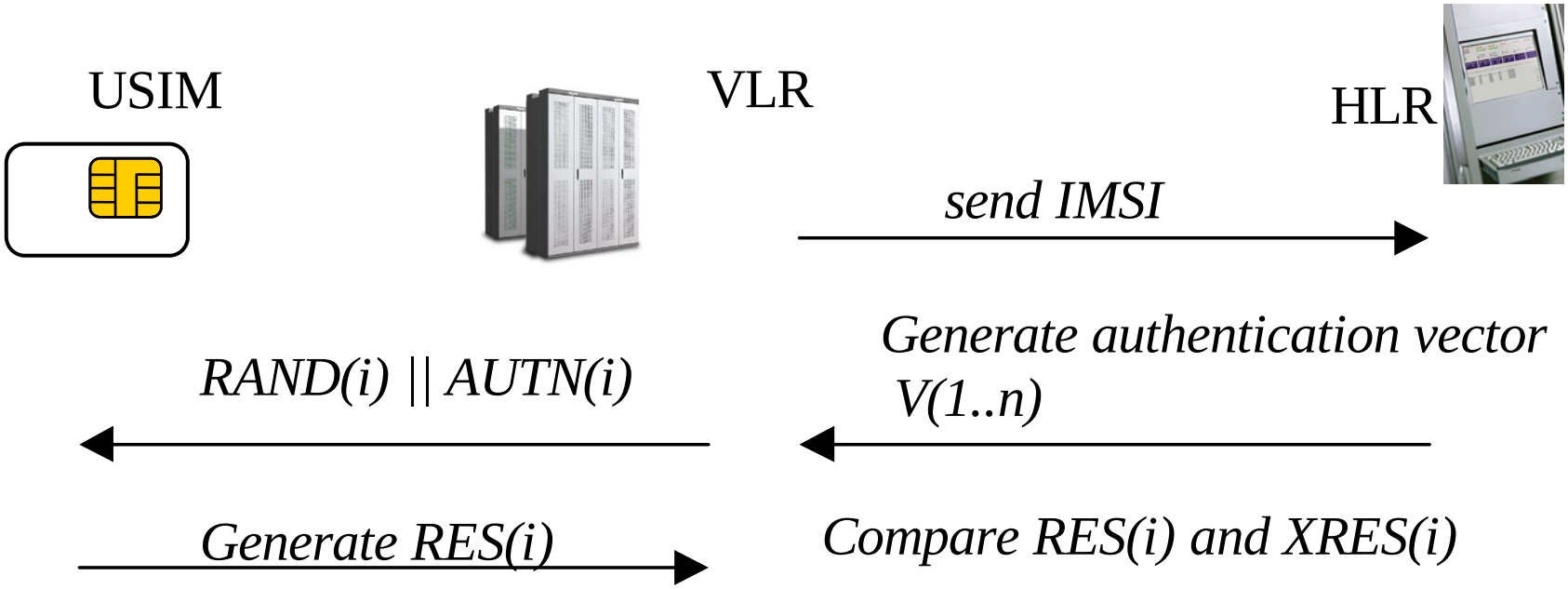
Provisionning + Authentification Mutuelle

Figure 6.7
Architecture générale de l'UMTS.



Mutuelle Authentification

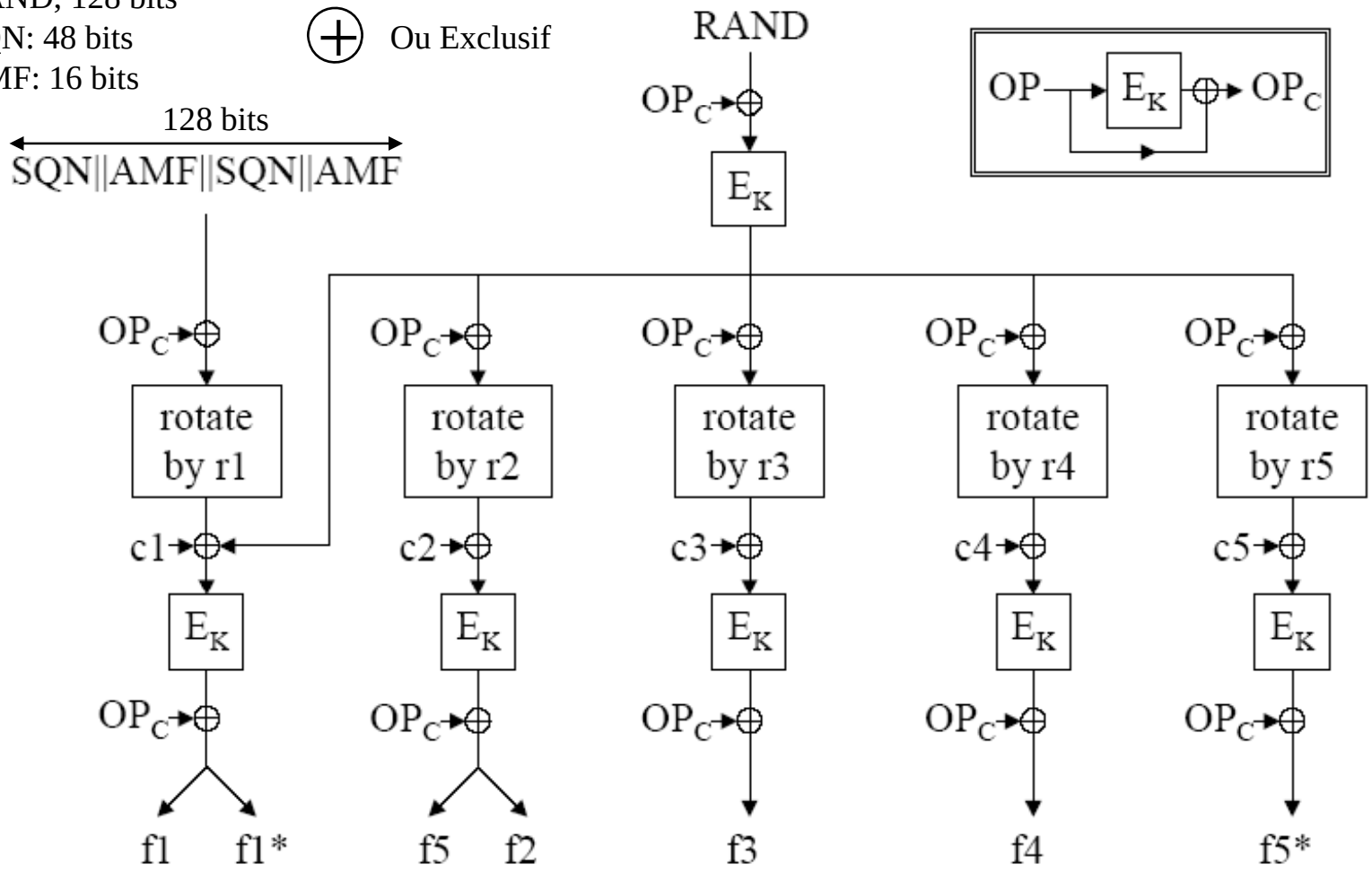
- Authentication and Key Agreement (AKA)
- Cipher key (CK) and Integrity key (IK)



MILENAGE

RAND, 128 bits
SQN: 48 bits
AMF: 16 bits

⊕ Ou Exclusif

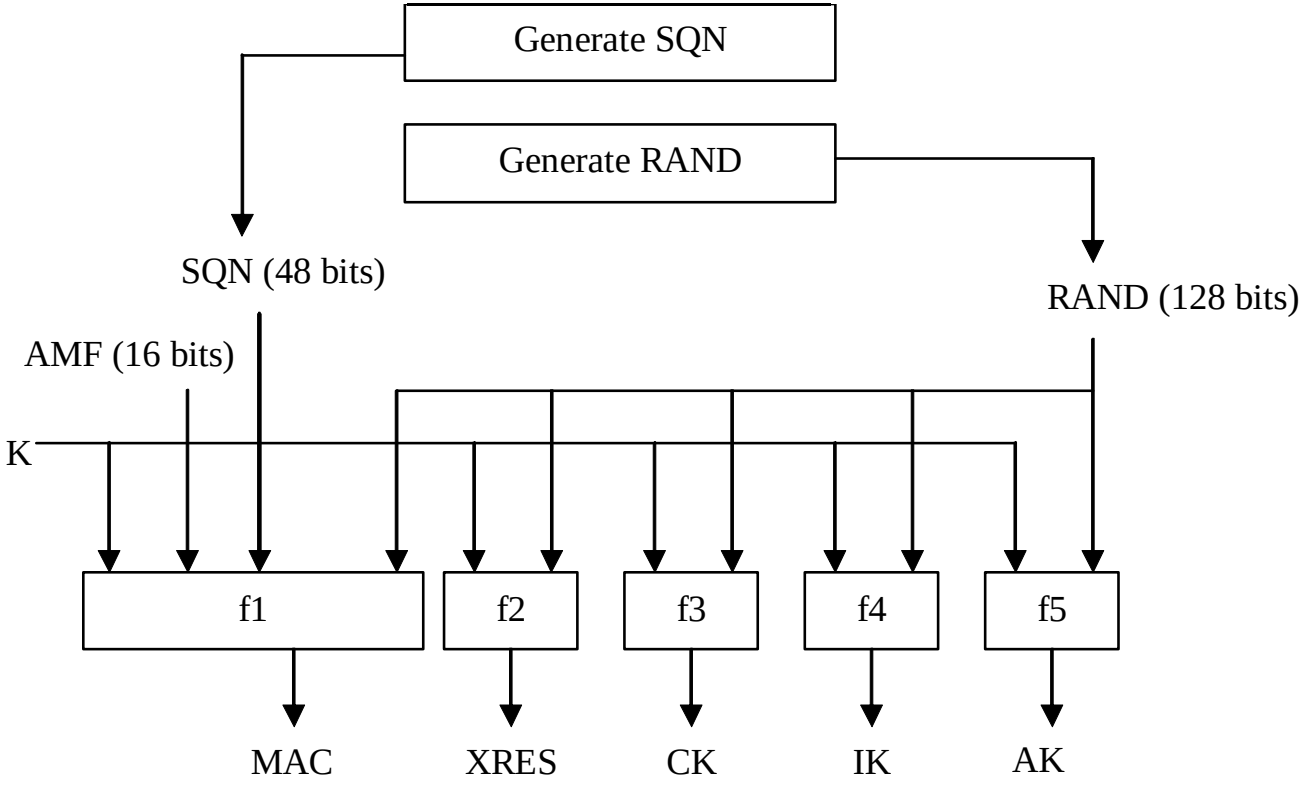


ri= 64,0,32,64,96 (rotation gauche)

ci= 0,1,2,4,8

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

AUTN: Authentication Vector

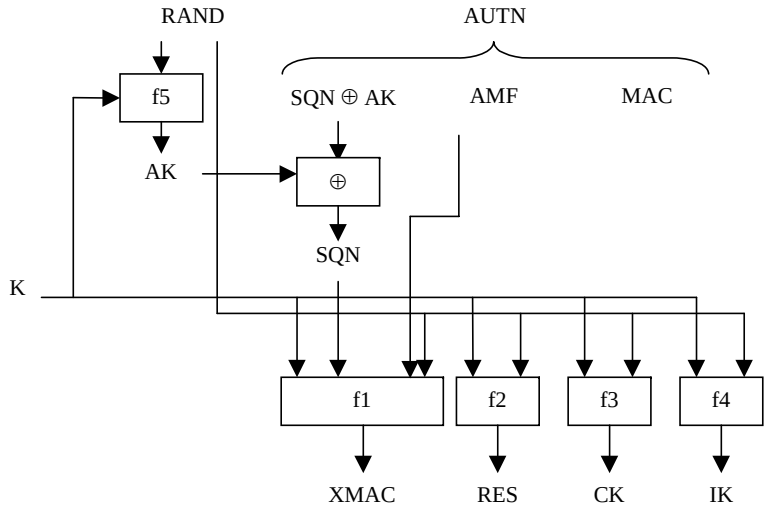


AUTN := SQN ⊕ AK || AMF || MAC

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

Carte USIM

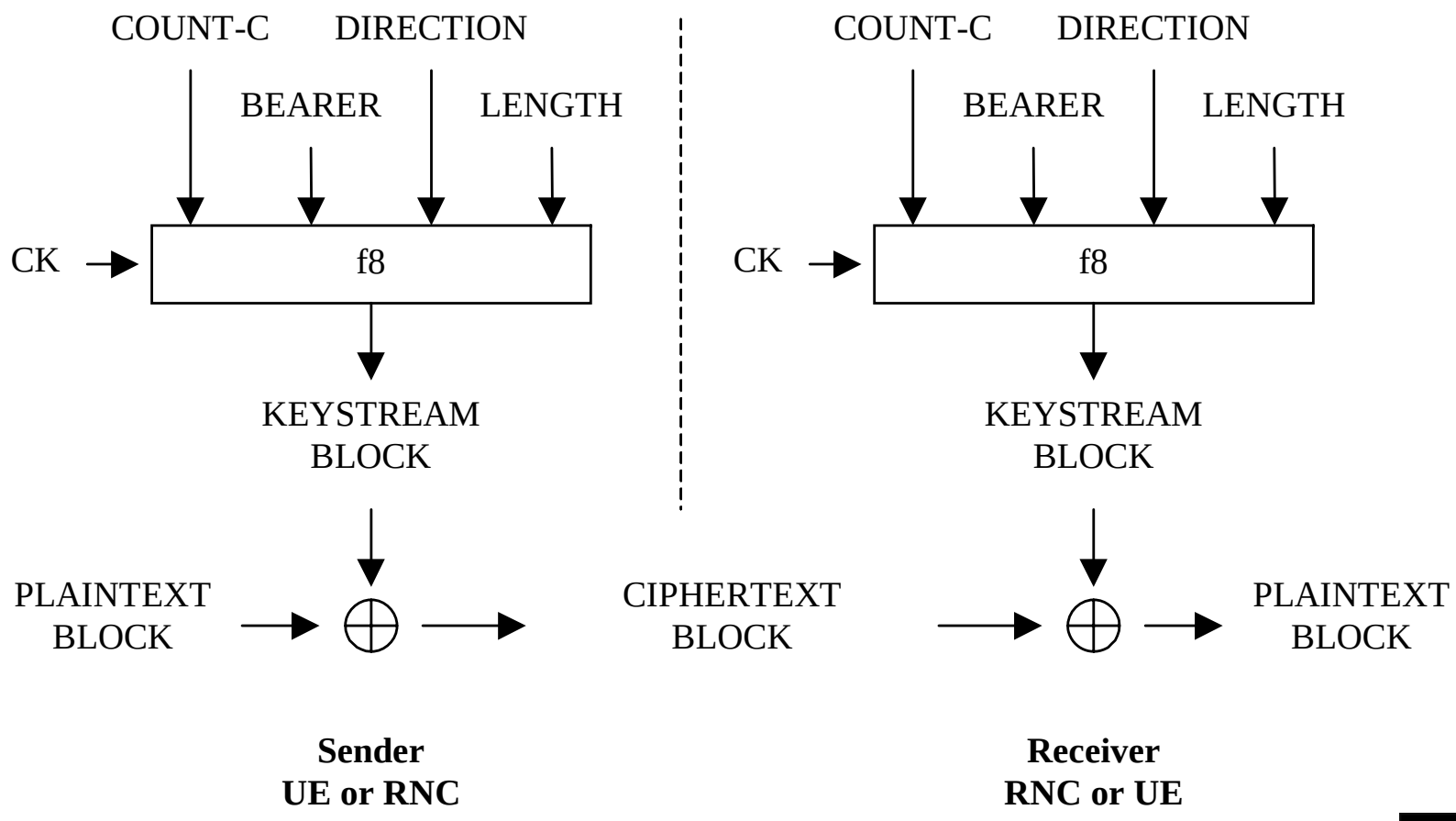
RAND: 23553cbe 9637a89d 218ae64d ae47bf35 AUTH: 55F328B43577 B9B9 4A9FFAC354DFAFB3

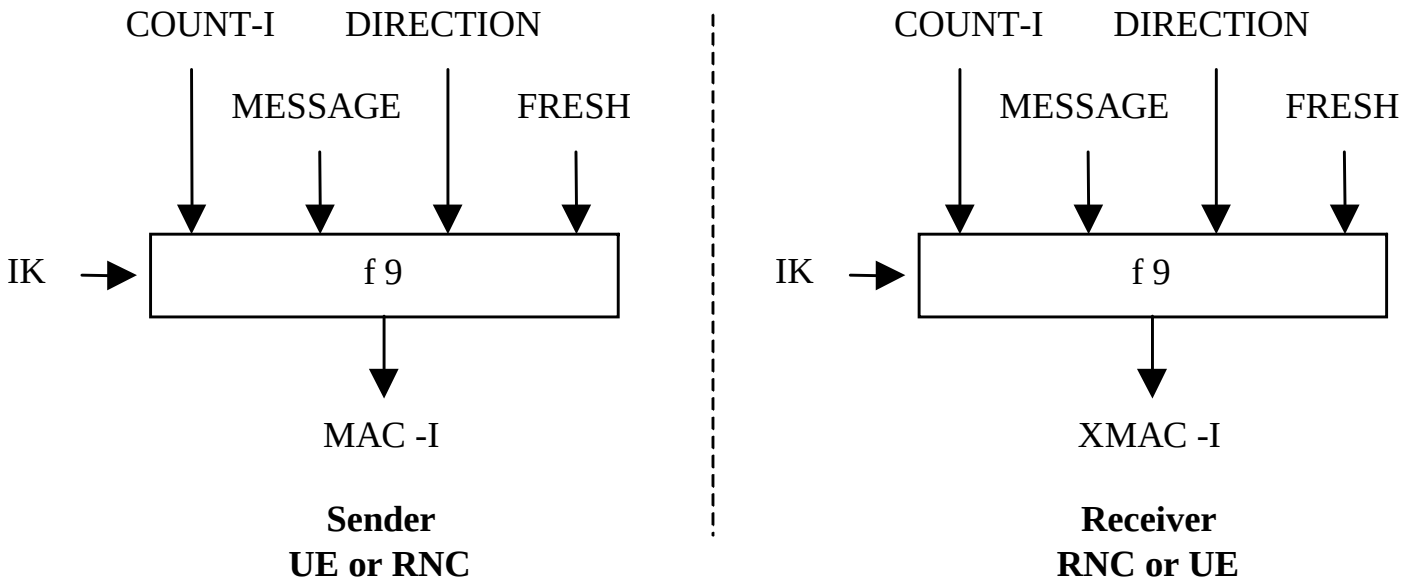



```
K:   465b5ce8 b199b49f aa5f0a2e e238a6bc
OP:  cdc202d5 123e20f6 2b6d676a c72cb318
SQN: ff9bb4d0b607
AMF: b9b9
RAND:23553cbe 9637a89d 218ae64d ae47bf35
4A 9F FA C3 54 DF AF B3                          f1/MAC
01 CF AF 9E C4 E8 71 E9                          f1*/AK2
A5 42 11 D5 E3 BA 50 BF                          f2/sres
B4 0B A9 A3 C5 8B 2A 05 BB F0 D9 87 B2 1B F8 CB  f3/ck
F7 69 BC D7 51 04 46 04 12 76 72 71 1C 6D 34 41  f4/ik
AA 68 9C 64 83 70                                f5/ak
45 1E 8B EC A4 3B                                f5*/ak2
```

```
Mécanisme de resynchronisation
AT_AUTS  = AK2 exor SQNms | MAC-S
AK2      = f5*(RAND)
MAC-S    = f1*(AMF,RAND,SQNms)
```

Chiffrement



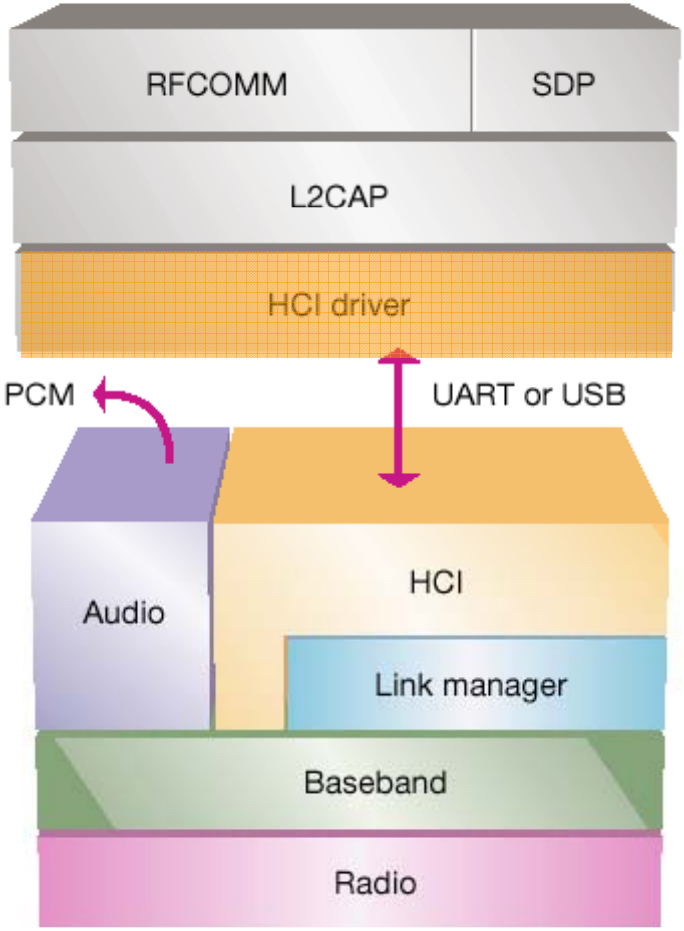


FRESH, valeur aléatoire

Sécurité Bluetooth

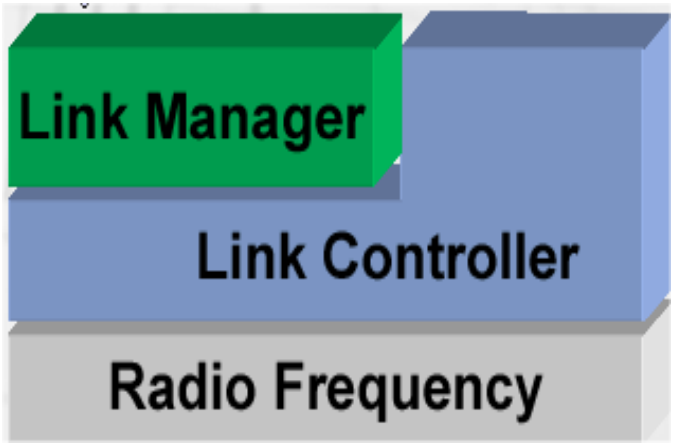
Aperçu de Bluetooth 1/3

- **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)
  - …



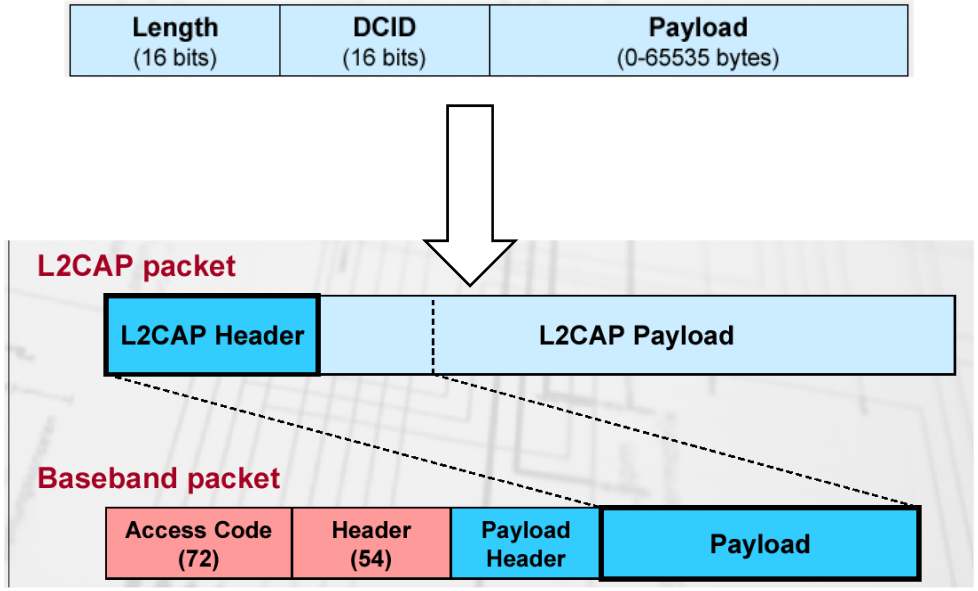
Composants BlueTooth 1/3

- **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.



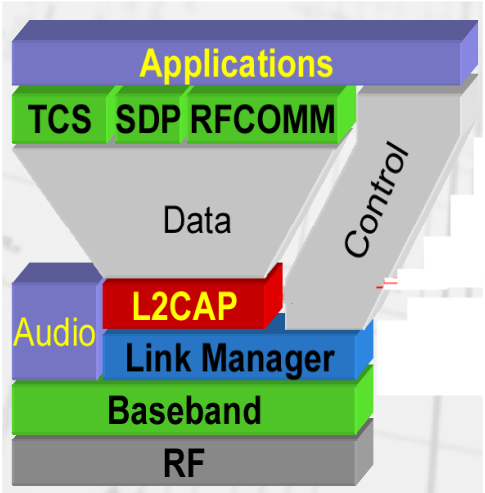
Composants BlueTooth 2/3

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

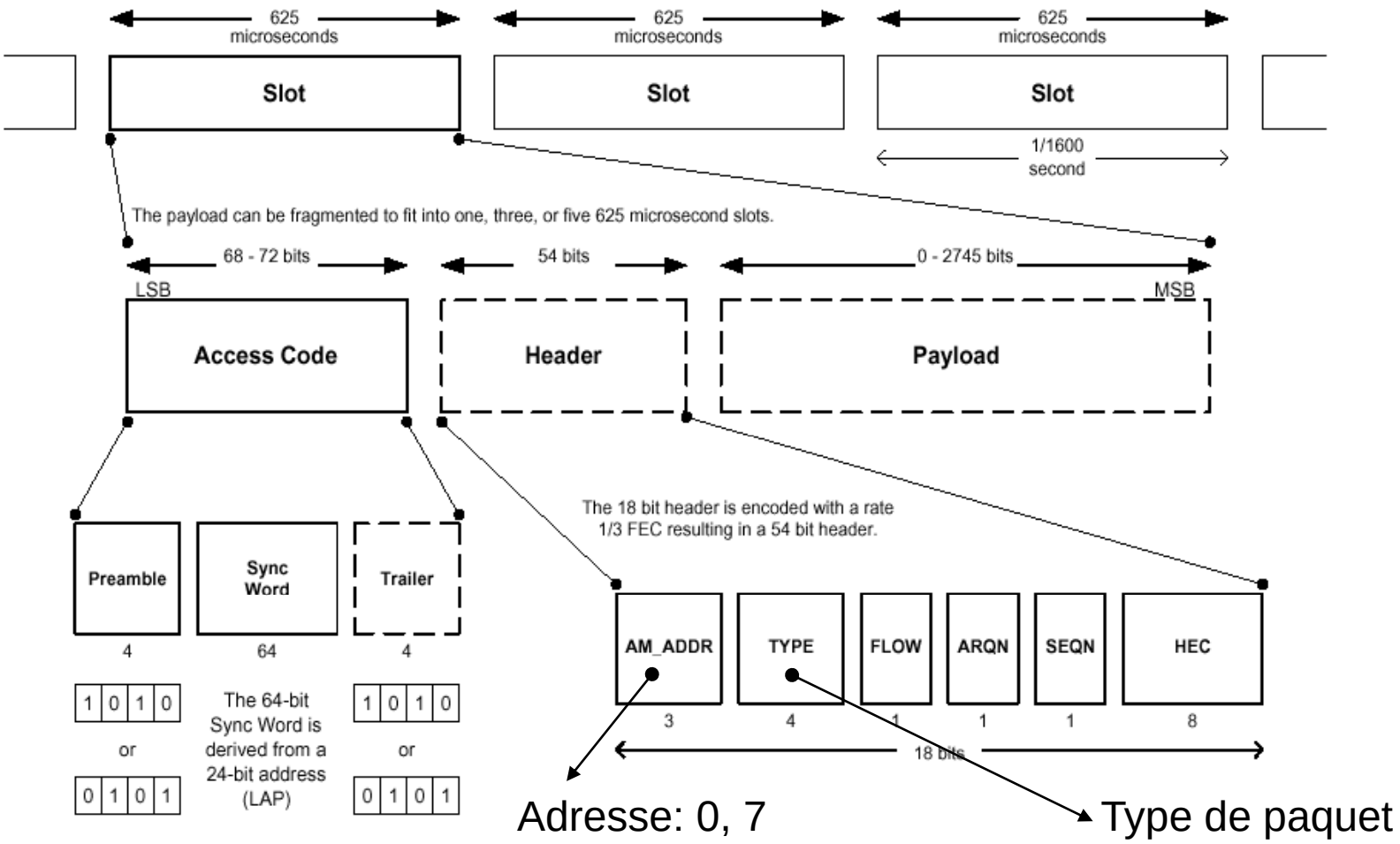


Composants BlueTooth 3/3

- **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

Type de paquet:

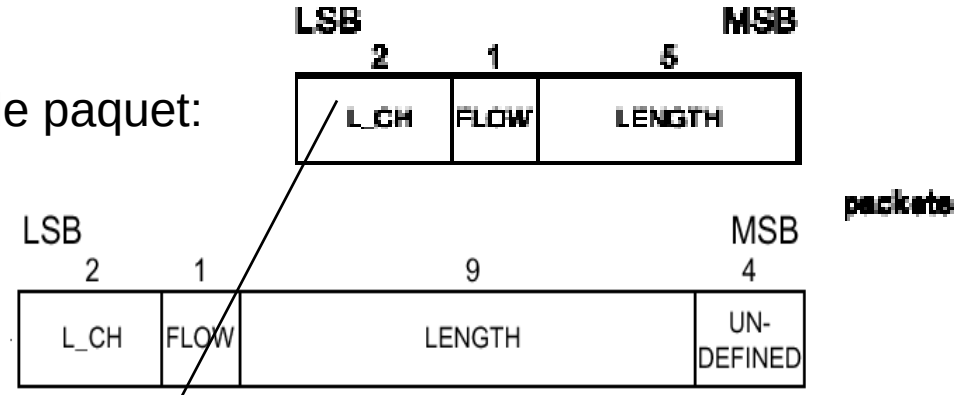


Figure 23—Payload header format for multislot packets

Table 18— Logical channel L_CH field contents

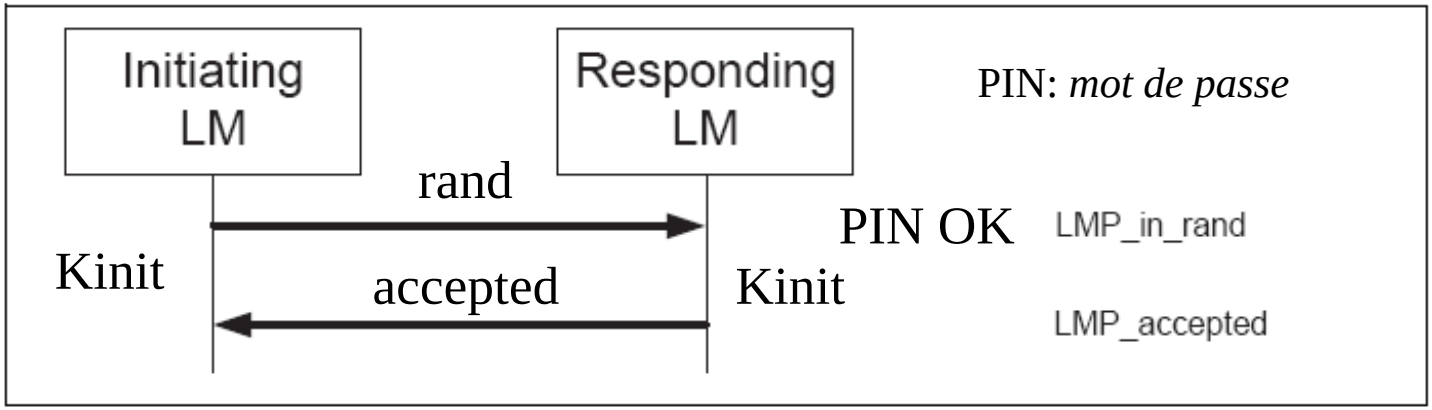
L_CH code b_1b_0	Logical Channel	Information
00	NA	undefined
01	UA/UI	Continuation fragment of an L2CAP message
10	UA/UI	Start of an L2CAP message or no fragmentation
11	LM	LMP message

Eléments de sécurité de BlueTooth

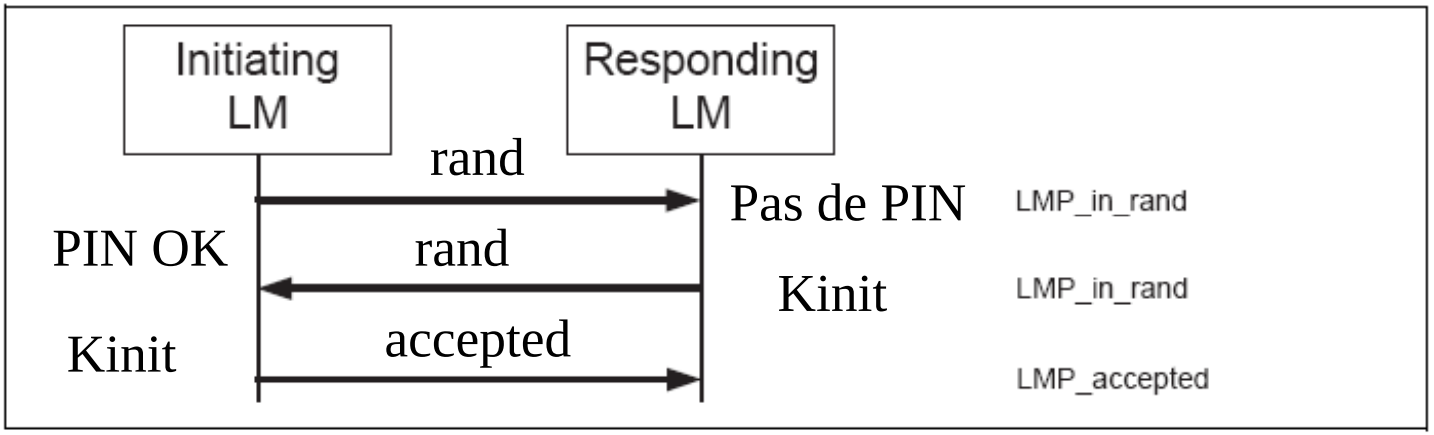
- **Un secret partagé entre les dispositifs maître et esclave: le PIN**
- **Procédure de “pairage” en quatre phases**
  - Création d’une clé d’initialisation, *Kinit*
  - Création d’une clé de lien, *Link_Key*
  - Authentification
  - Demande de chiffrement

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.

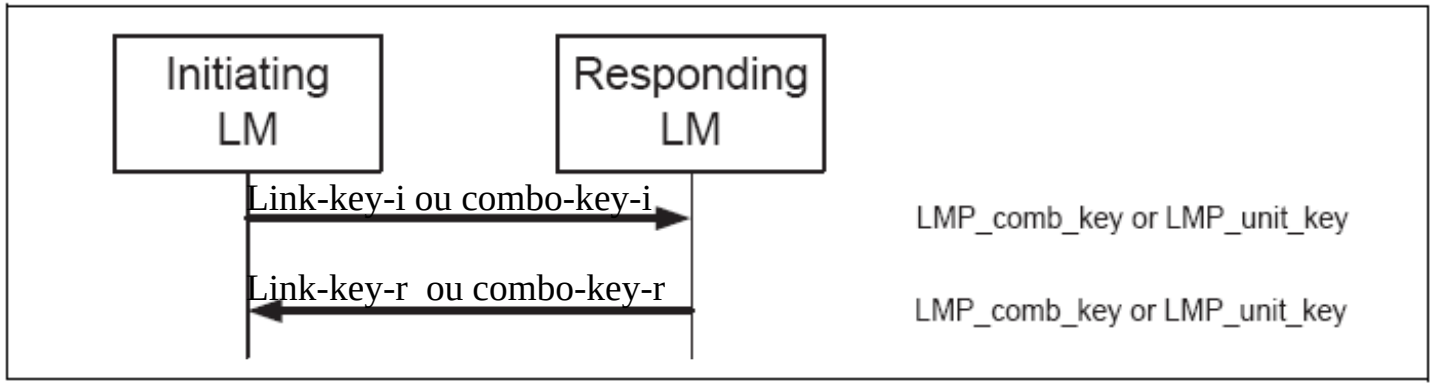


Sequence 4: Responder has a fixed PIN and initiator has a variable PIN.

Création d'une clé de lien KAB

Création de KAB

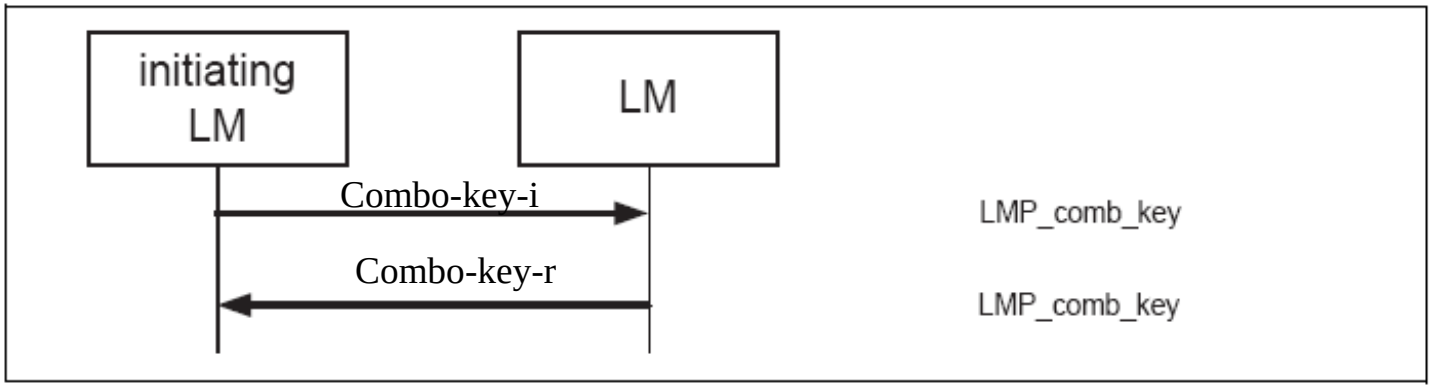
unit-key = link_key exor Kinit
combo_key = nombre aléatoire



Sequence 7: Creation of the link key.

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

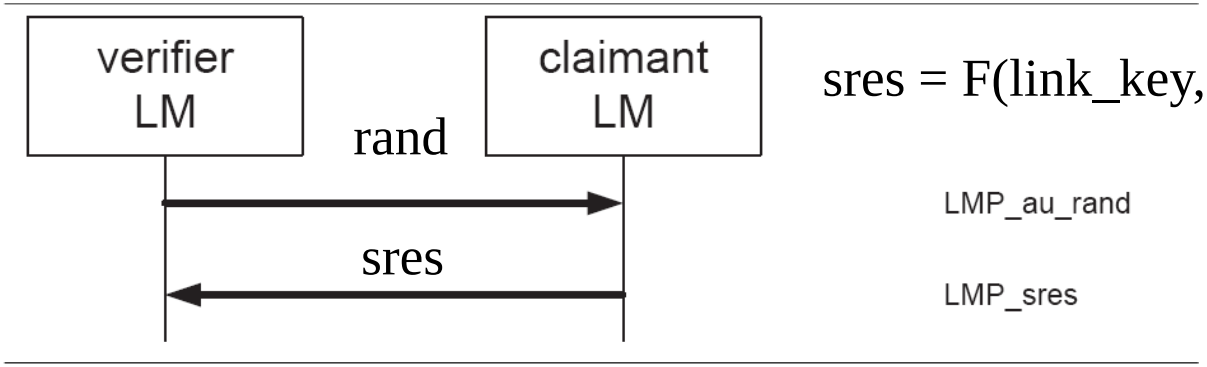
Modification de KAB



Sequence 8: Successful change of the link key.

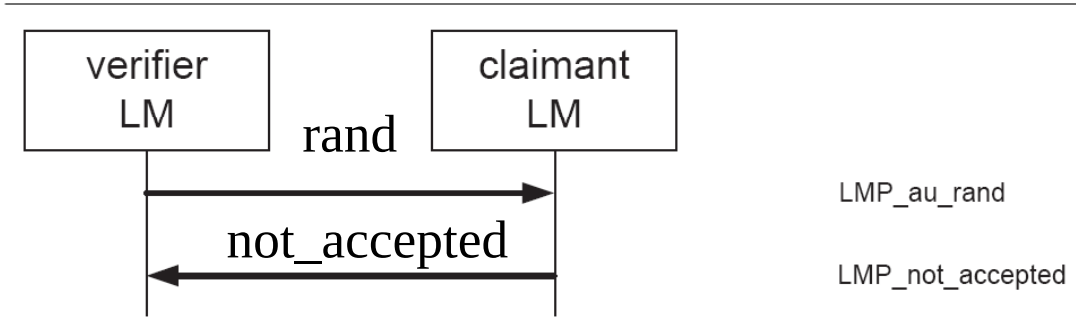
Link_key= F(KAB, comb_key_i, comb_key_r)

Une clé de ligne (Link Key) est disponible



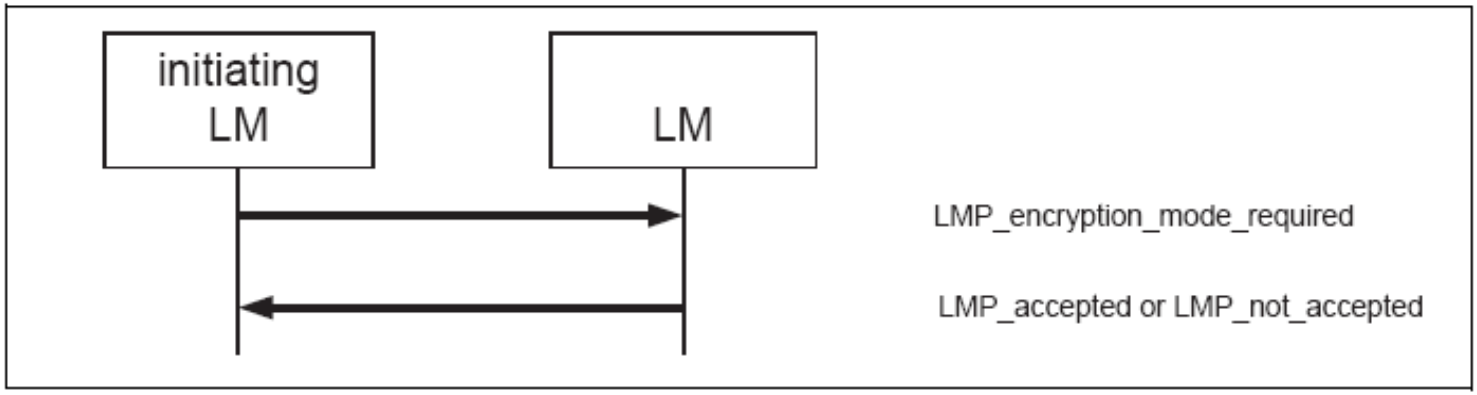
Sequence 1: Authentication. Claimant has link key.

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



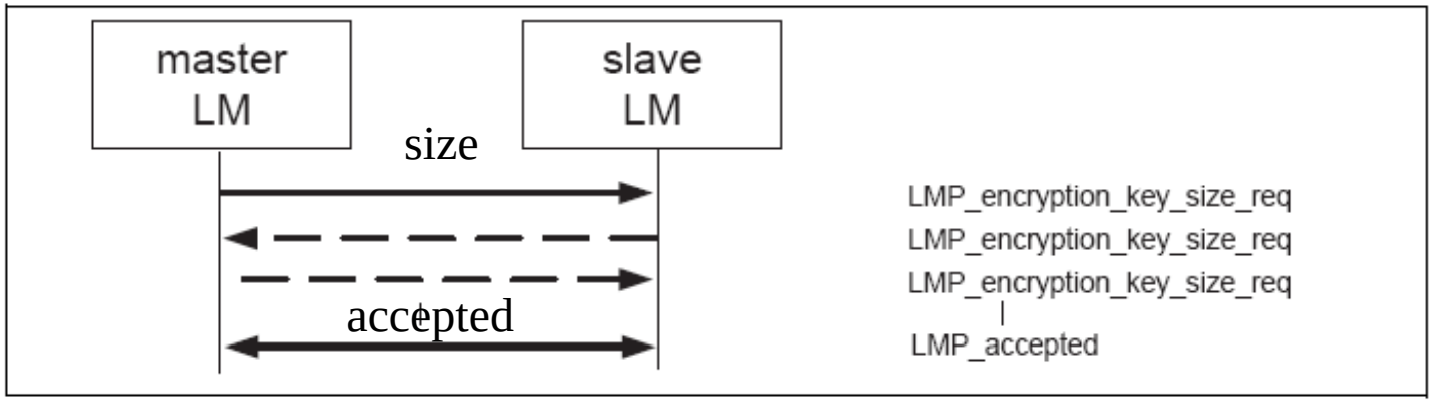
Sequence 2: Authentication fails. Claimant has no link key.

Demande de mode chiffré



Sequence 12: Negotiation for encryption mode.

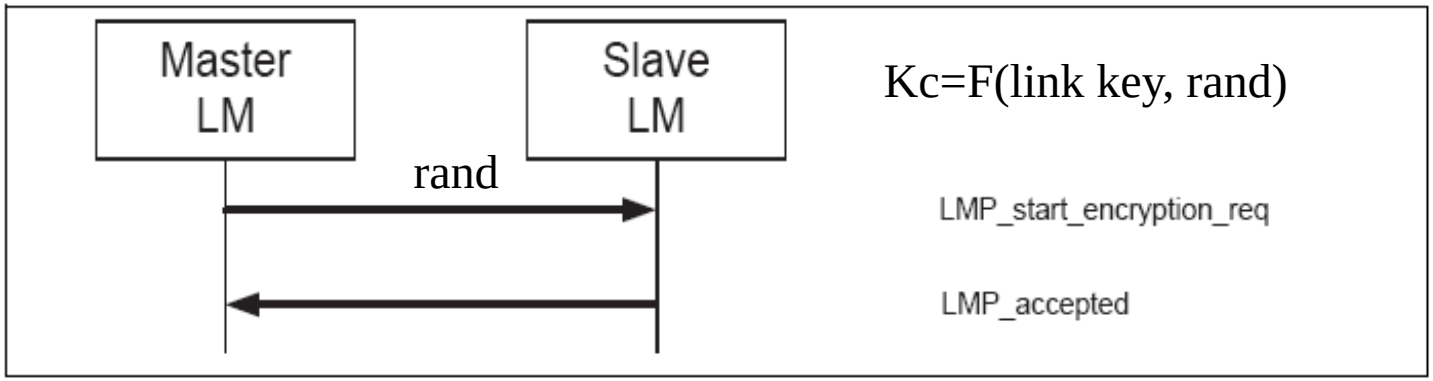
Négociation da la taille d'une clé de chiffrement



Sequence 13: Encryption key size negotiation successful.

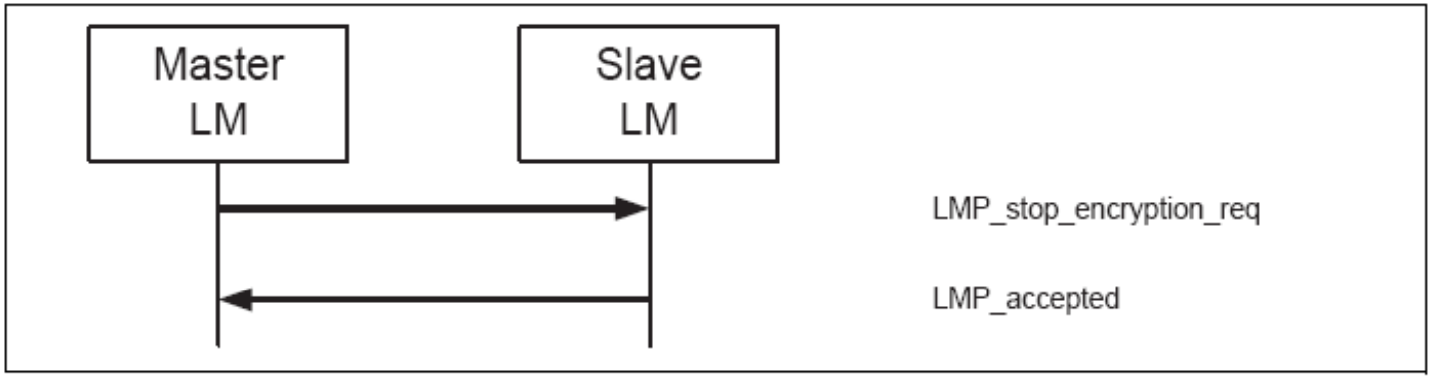
TELECOM ParisTech

Start Encryption: création de la clé de chiffrement (Kc)



Sequence 15: Start of encryption.

Stop Encryption

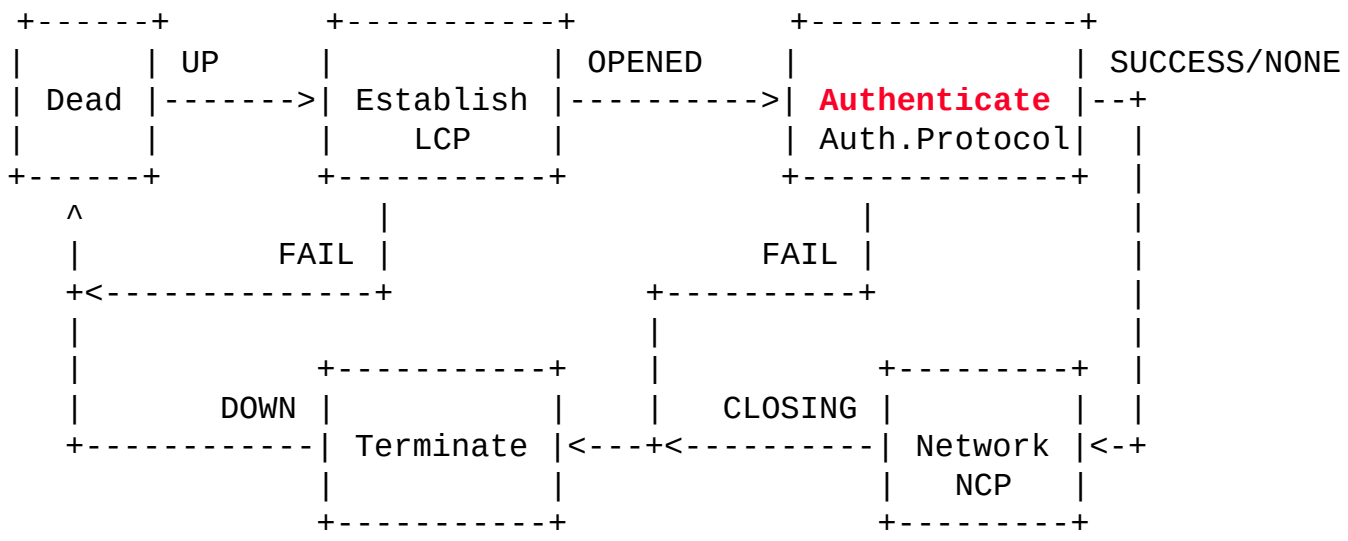


Sequence 16: Stop of encryption.

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**

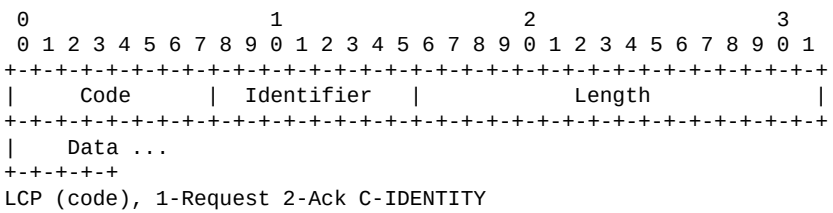


Flag 0x7E	Address 0xFF	Control 03	Protocol 2 bytes	information 1500 octets max	CRC 2 bytes	Flag 0x7E

- **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)

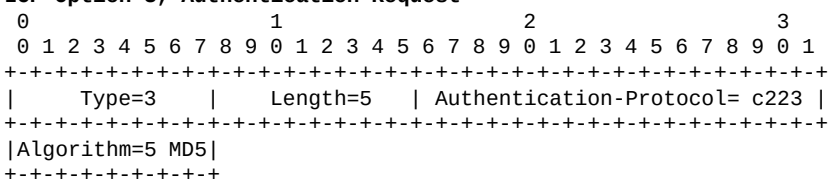
A PPP Authentication example 1/2

LCP Coding

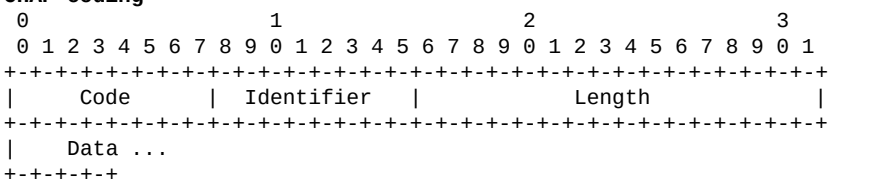


LCP (code), 1-Request 2-Ack C-IDENTITY

LCP Option=3, Authentication Request

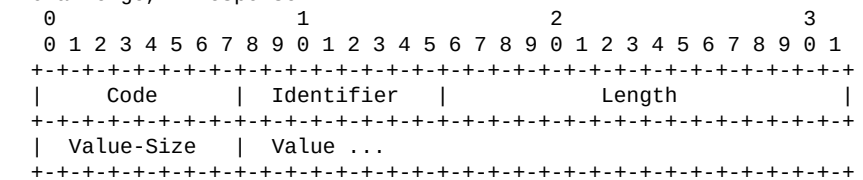


CHAP coding

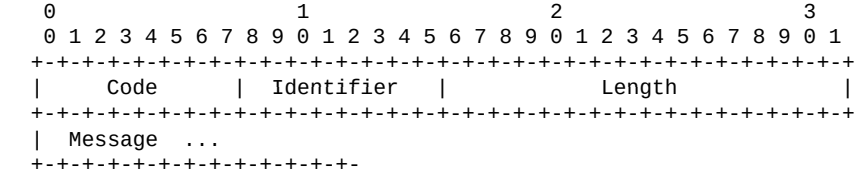


Code

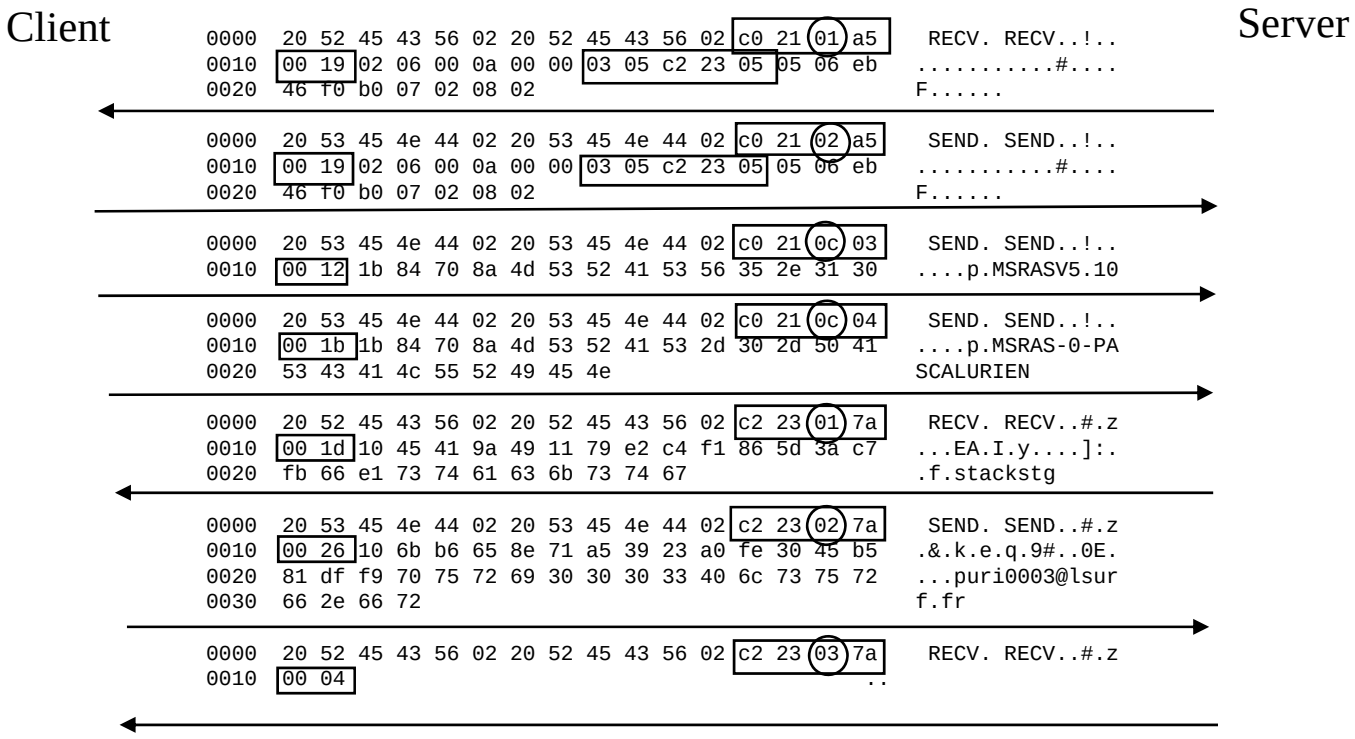
1- Challenge, 2-Response



3-Success, 4-Failure



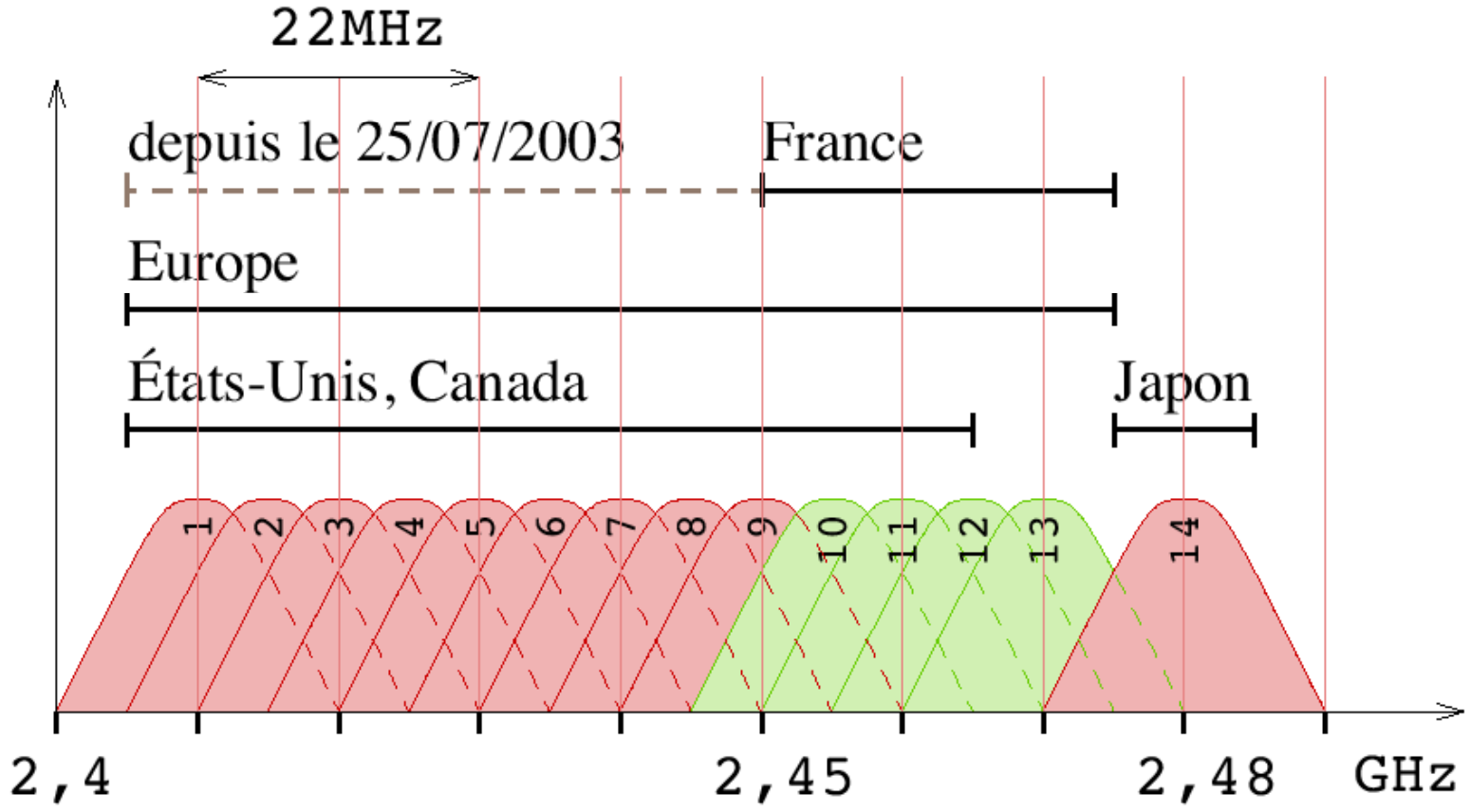
A PPP Authentication example 1/2



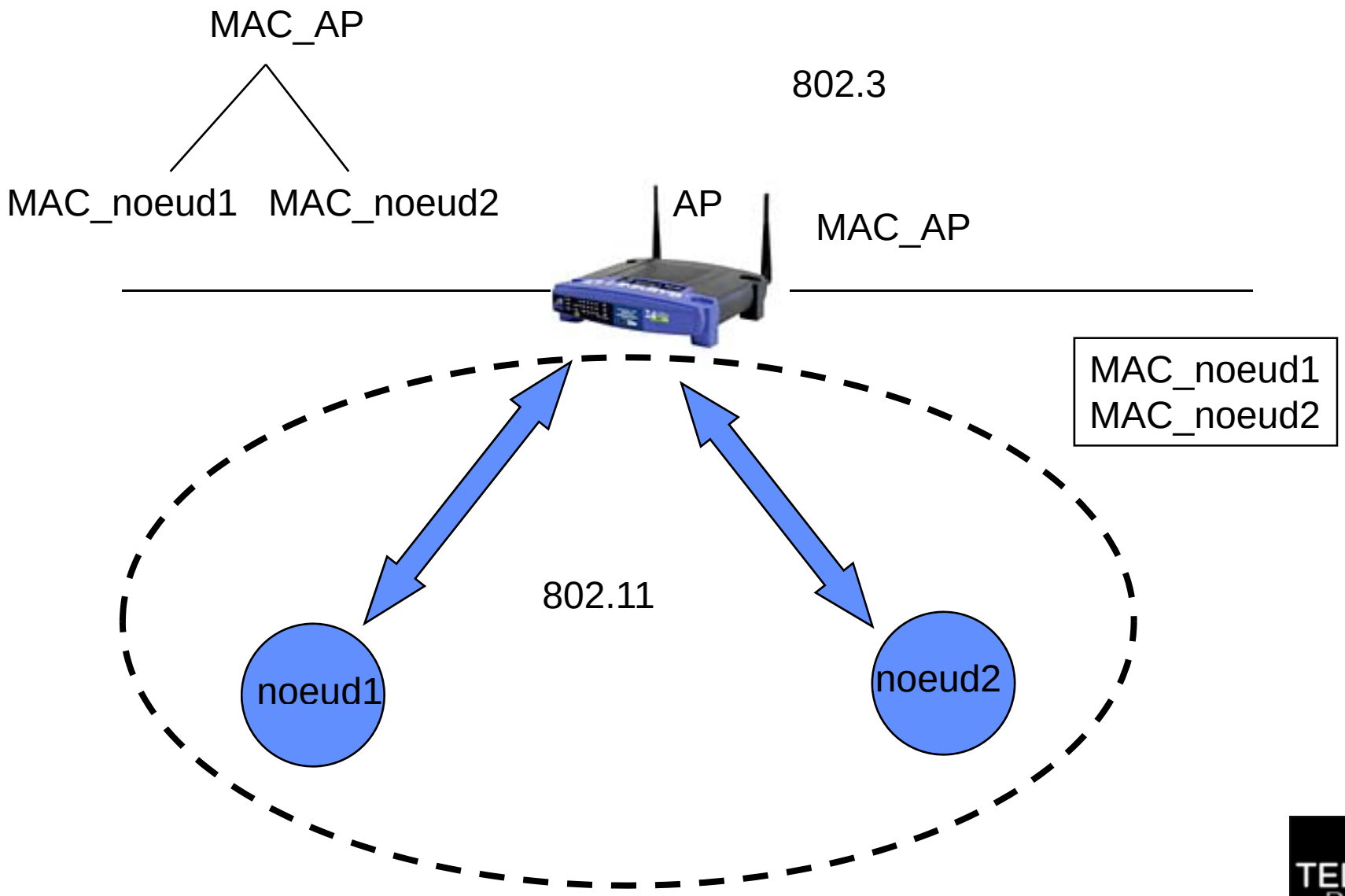
La sécurité du Wi-Fi

Pascal Urien

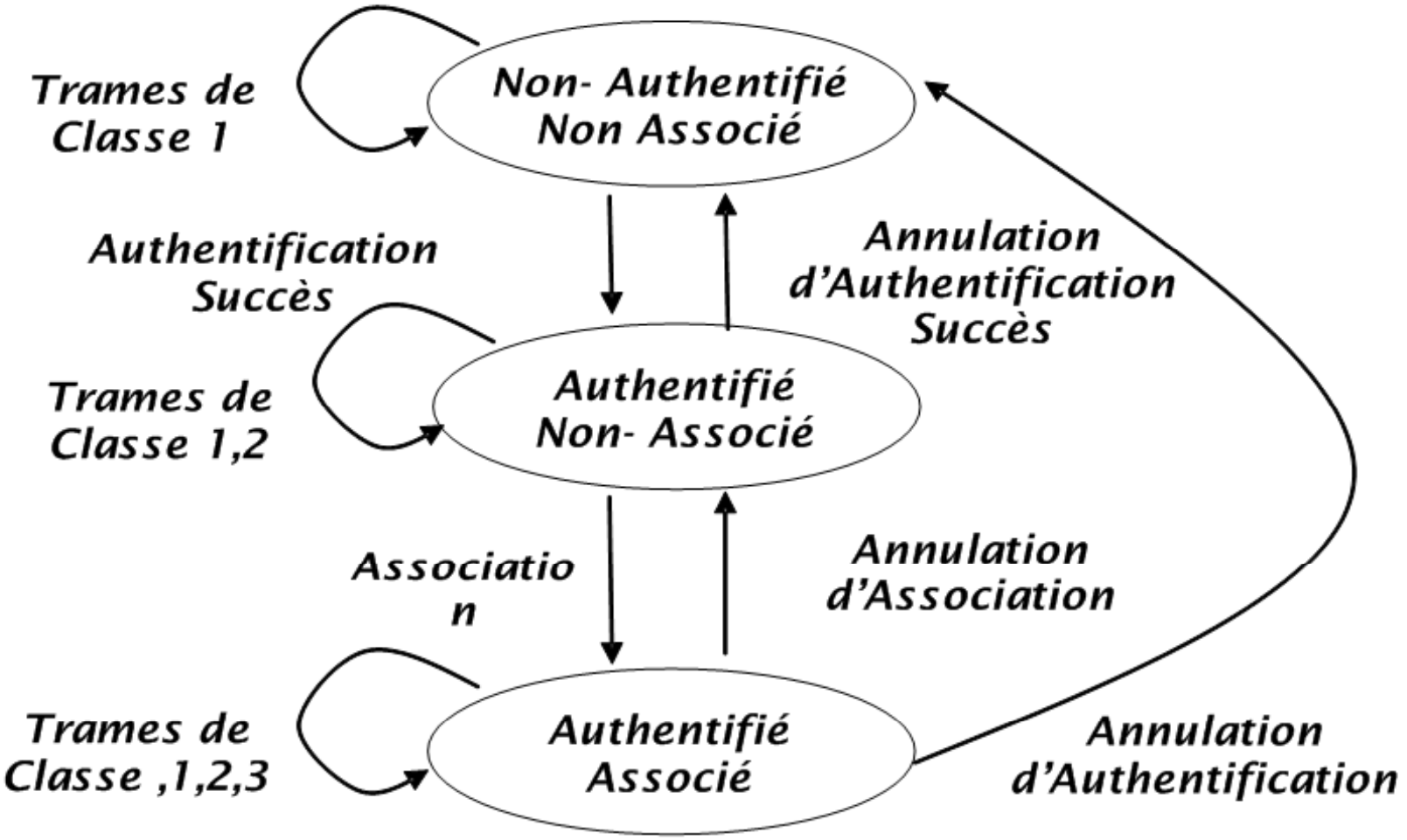
802.11b, 14 canaux de 22 Mhz



Association



Authentification



Wi-Fi, introduction à la Sécurité

Les enjeux du sans fil 1/4

- Le succès du réseau Internet, véritable moteur de la nouvelle économie de la dernière décennie, a imposé le protocole IP comme un standard de facto pour l'échange des données numériques. Surfant sur cette vague les entreprises ont adoptée cette technologie pour le stockage et la diffusion de leurs informations stratégiques ; intranet, courrier électronique, bases de données trois tiers, annuaires LDAP sont des services aujourd'hui indispensables à la compétitivité et la survie de toute activité économique.
- Si la prédominance des réseaux IP est actuellement incontestable, il convient également de remarquer que les technologies des réseaux locaux tendent également vers un standard de fait, le réseau Ethernet. Cette technologie, initialement basée sur le partage d'un guide d'onde (un câble en fait) a petit à petit migré vers une infrastructure basée sur des commutateurs de trames «*switchs*»).

Les enjeux du sans fil 2/4

- A la base les réseaux sans fil 802.11 ne sont que l'extension naturelle des réseaux Ethernet câblés. La croissance exponentielle de ce marché s'explique par un réel besoin des utilisateurs d'accéder au réseau de manière quasi transparente, sans l'obligation de connecter leur ordinateur personnel à une prise. Le réseau sans fil remplace le câble par un lien radio; cependant en raison des lois de propagation des ondes électromagnétiques cette prise virtuelle est utilisable dans un rayon de l'ordre de 100m, c'est-à-dire dans certain cas à l'extérieur des murs de l'entreprise. On introduit donc de nouveaux risques d'intrusion ou de fuite d'information, parfois qualifiés [Arbaugh *et al.*2001] d'attaque par le parking (*parking lot attack*).

Les enjeux du sans fil 3/4

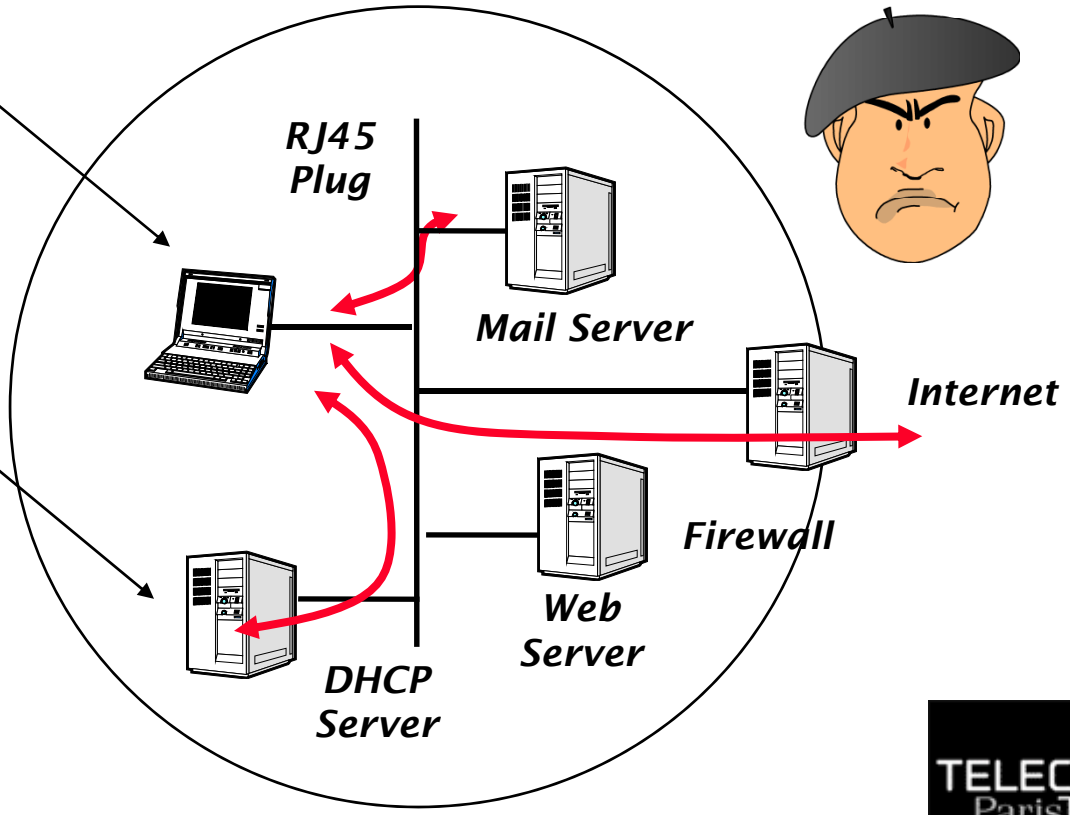
- L'apparition de l'IP sans fil dans des architectures câblées préexistantes implique donc la mise en place de nouvelles mesures de sécurité. Jusqu'à présent les entreprises ont déployés leurs réseaux locaux sans protection particulière des points d'accès. Typiquement le réseau est organisé autour d'un arbre de commutateur de paquets (HUB), auquel sont reliées des stations de travail, à l'aide de prises marquant les points d'accès au réseau (souvent dénommées *port d'accès*).
- L'entrée de l'établissement étant contrôlé et réservé au personnel autorisé, les ports d'accès ne sont pas usuellement sécurisés, en particulier pour permettre une libre connexion des ordinateurs portables. La mobilité des usagers s'appuie sur le protocole DHCP allouant dynamiquement une adresse, compatible avec l'organisation logique et géographique de l'intranet. Celui ci ne conduisant pas en règle générale une procédure d'authentification avant l'allocation des paramètres de configuration, il est très facile d'accéder à l'intranet d'une entreprise depuis un port d'accès.
- RFC 2131, Chapter 7 - Security Considerations, «*…Therefor… DHCP in its current form is quite insecure*».

Les enjeux du sans fil 4/4

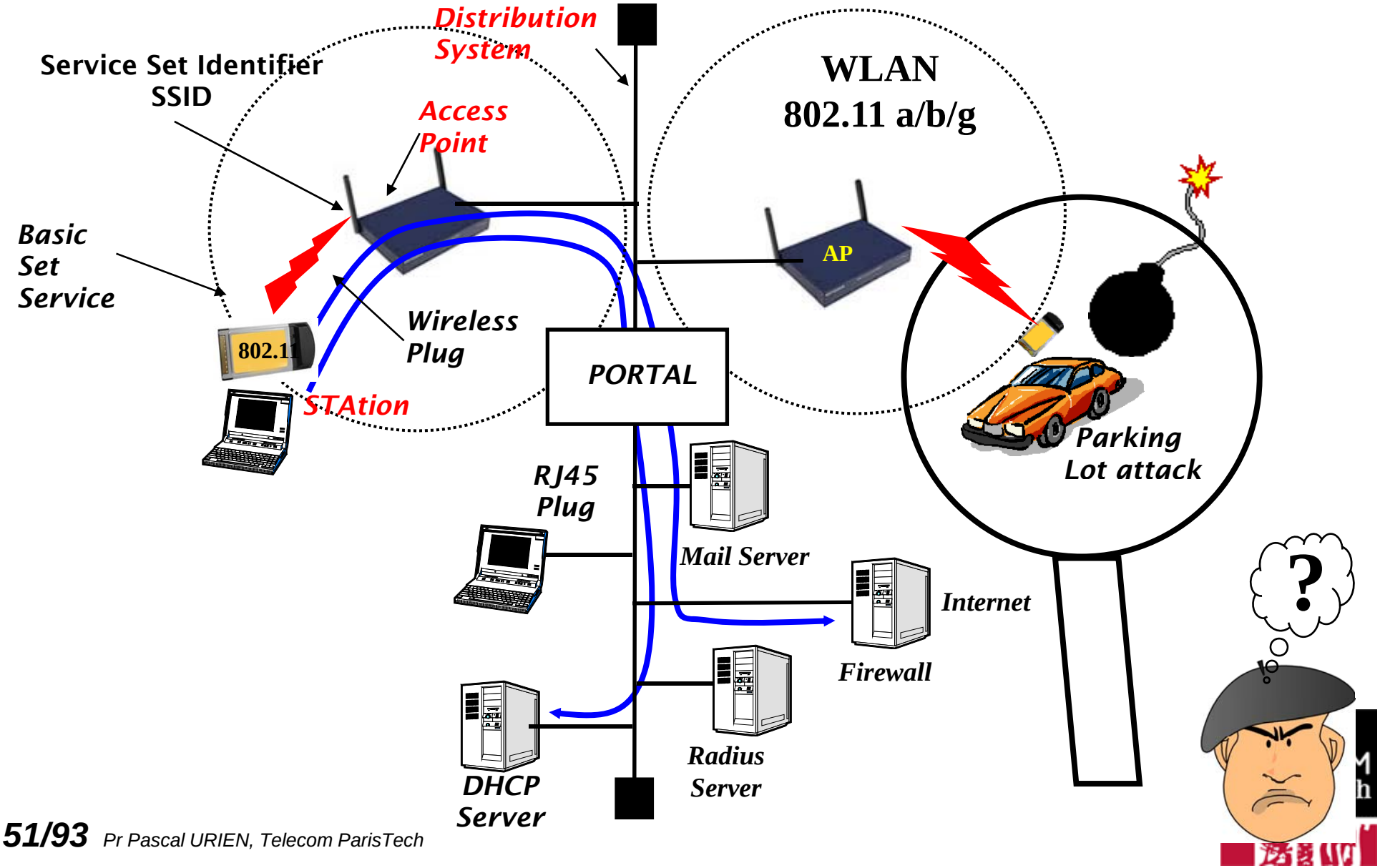
- En conséquence le contrôle des accès, quasi inexistant dans le cas des réseaux câblés, devient un pré requis pour le déploiement des réseaux 802.11. De même la signature des trames est également indispensable, en son absence, un pirate peut facilement usurper l'adresse MAC d'un utilisateur authentifié (*MAC spoofing*) et accéder aux ressources numériques disponibles. Le chiffrement des données transitant sur le lien radio est également souhaitable afin de garantir la confidentialité des échanges ; cependant de nombreuses méthodes (IPSEC, SSL, SSH ...) sont déjà en mesure d'assurer ce service.
- En résumé les services sécurisés indispensables aux extensions IP sans fil sont les suivants
  - - Identification et authentification des utilisateurs du réseau
  - - Signature des trames échangées (intégrité, authentification).
  - - Chiffrement des données (confidentialité)

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.

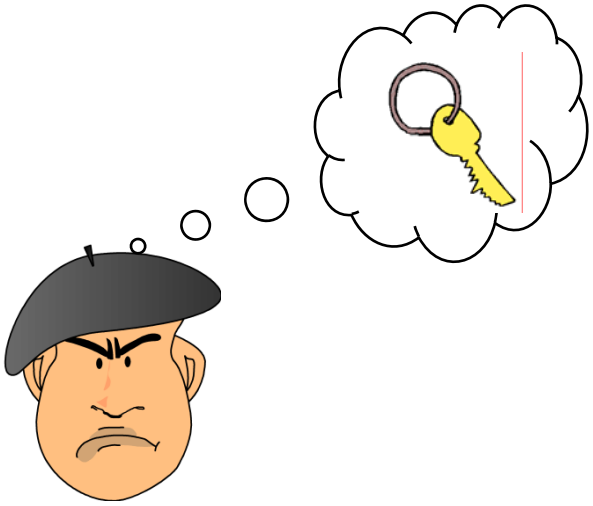
- **Authentification des accès.**
  - *Simple*, identification du nomade (prévention du *spoofing*) et de ses droits (*credentials*).
  - *Mutuelle*, protection contre des AP indésirables (*rogue access point*).
  - Contrôle d'accès au réseau, protection du réseau = qui utilise le réseau.
- **Confidentialité (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*

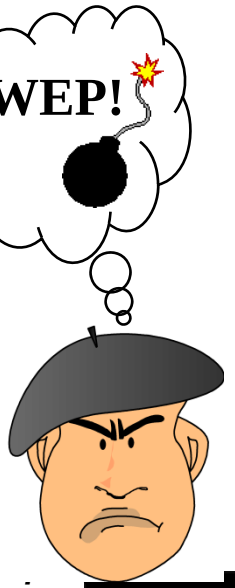
TELECOM ParisTech

WEP



Sécurité Wi-Fi - WEP

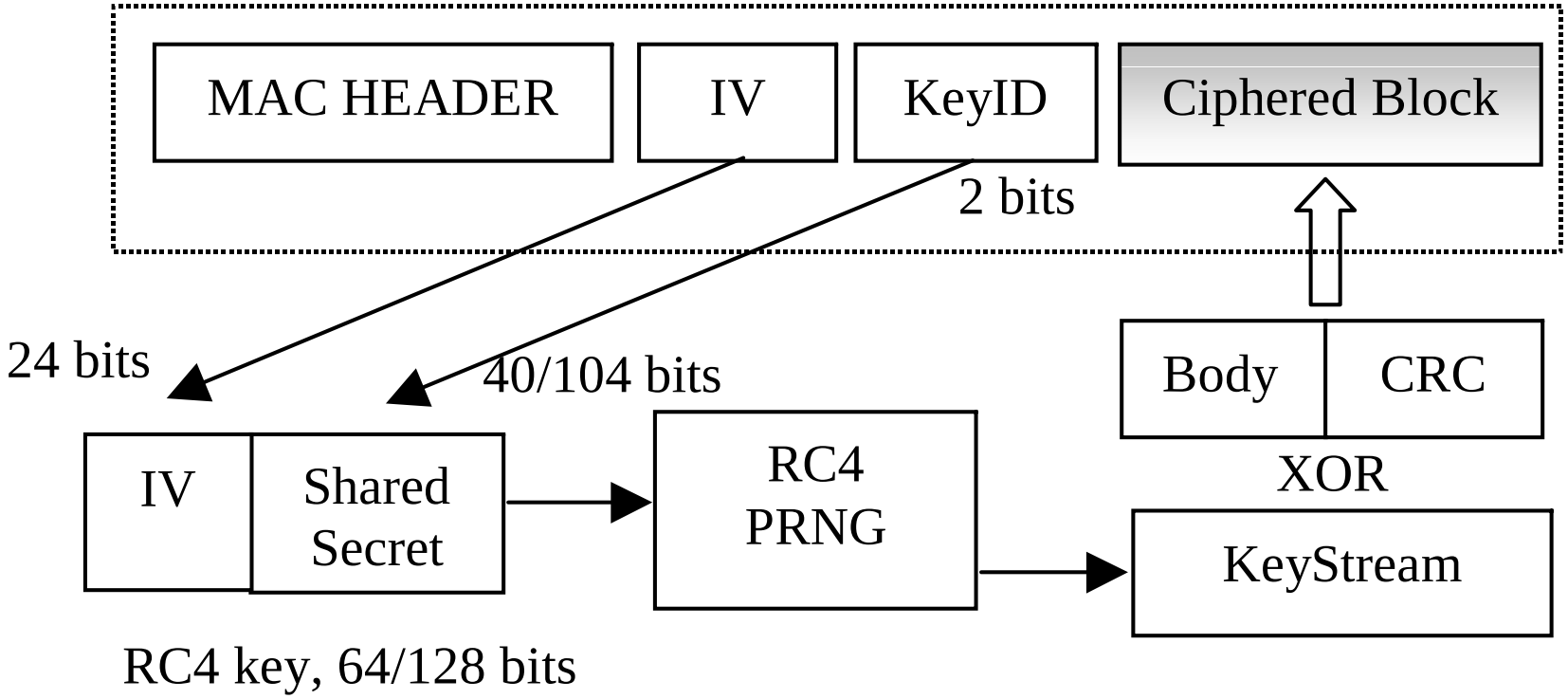
- **Open Authentication, c'est à dire pas d'authentification**
  - Utilise le SSID comme mot de passe, peu sûre.
- **Filtrage des adresses MAC**
  - *Address Control List*, peu sûre.
- **Clés RC4 fixes (64 ou 128 bits), partagées entre stations et points d 'accès.**
  - Authentification re-jouable.
  - 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.



TELECOM 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.

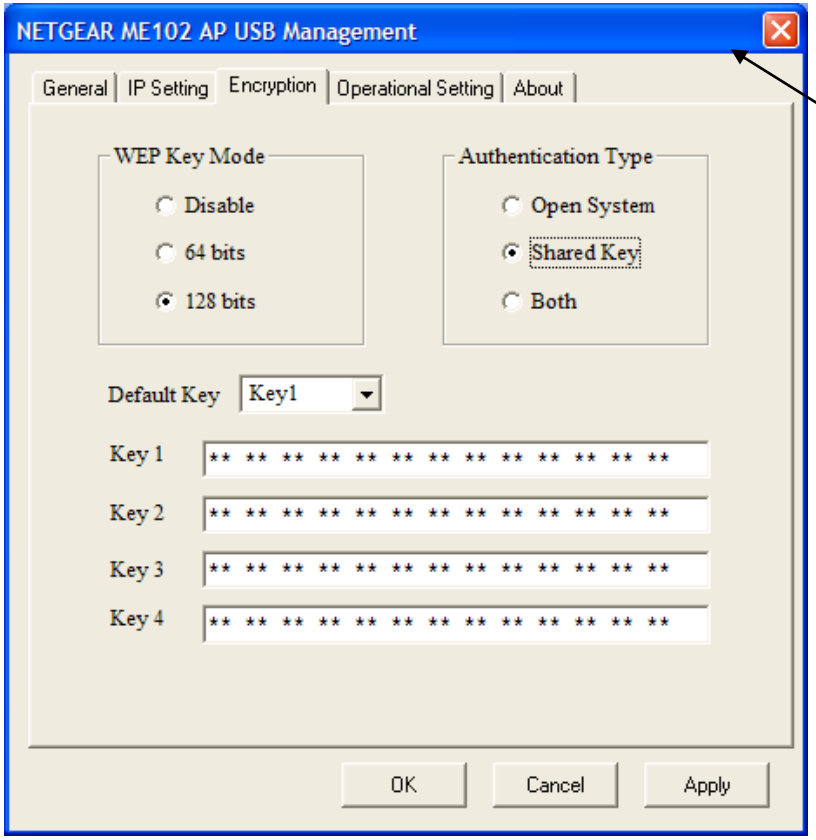
Lacunes du protocole WEP. 4/5

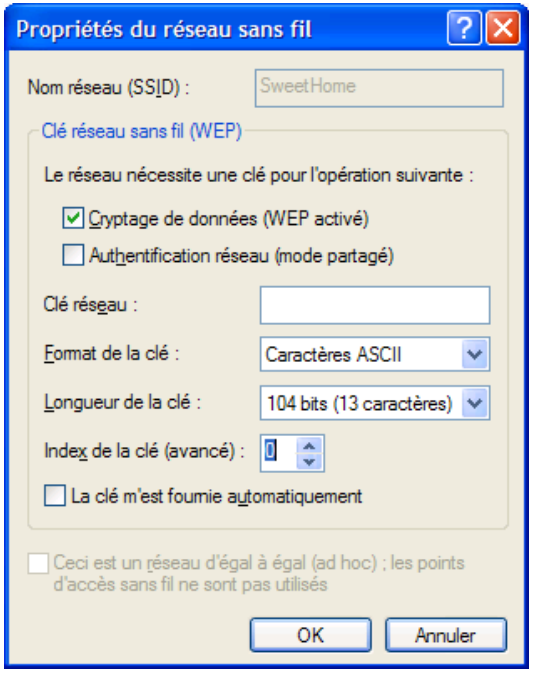
- **Confidentialité.**
  - Seulement 2^{24} valeurs IV.
  - 50 % de chances de réutiliser une valeur IV au bout de 4823 trames.
  - Les suites de chiffrement Xsi se déduisent des valeurs en clair.
  - 2^{40} essais (1million/s x 12 jours) permettent de trouver les secrets partagés de 40 bits.
- **WEP 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.

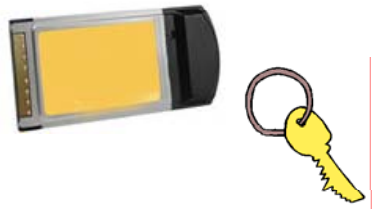
Lacunes du protocole WEP. 5/5

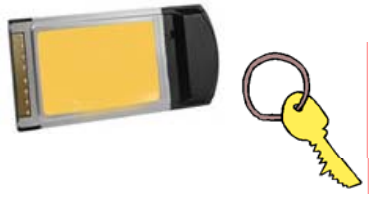
- **Intégrité des données.**
  - Dans une trame WEP le CRC est chiffré.
  - Le CRC est une fonction linéaire du ou exclusif, le CRC du ou exclusif (octet à octets) de deux trames de même longueurs est le ou exclusif de leur CRC respectif.
  - Le ou exclusif (octets à octets) d 'une trame WEP (chiffrée)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

WEP + Windows


NETGEAR ME102 AP USB Management
General
IP Setting
Encryption
Operational Setting
About
WEP Key Mode
Disable
64 bits
128 bits
Authentication Type
Open System
Shared Key
Both
Default Key
Key1
Key 1
Key 2
Key 3
Key 4
OK
Cancel
Apply


Propriétés du réseau sans fil
Nom réseau (SSID) :
SweetHome
Clé réseau sans fil (WEP)
Le réseau nécessite une clé pour l'opération suivante :
Cryptage de données (WEP activé)
Authentification réseau (mode partagé)
Clé réseau :
Format de la clé :
Caractères ASCII
Longueur de la clé :
104 bits (13 caractères)
Index de la clé (avancé) :
La clé m'est fournie automatiquement
Ceci est un réseau d'égal à égal (ad hoc) ; les points d'accès sans fil ne sont pas utilisés
OK
Annuler

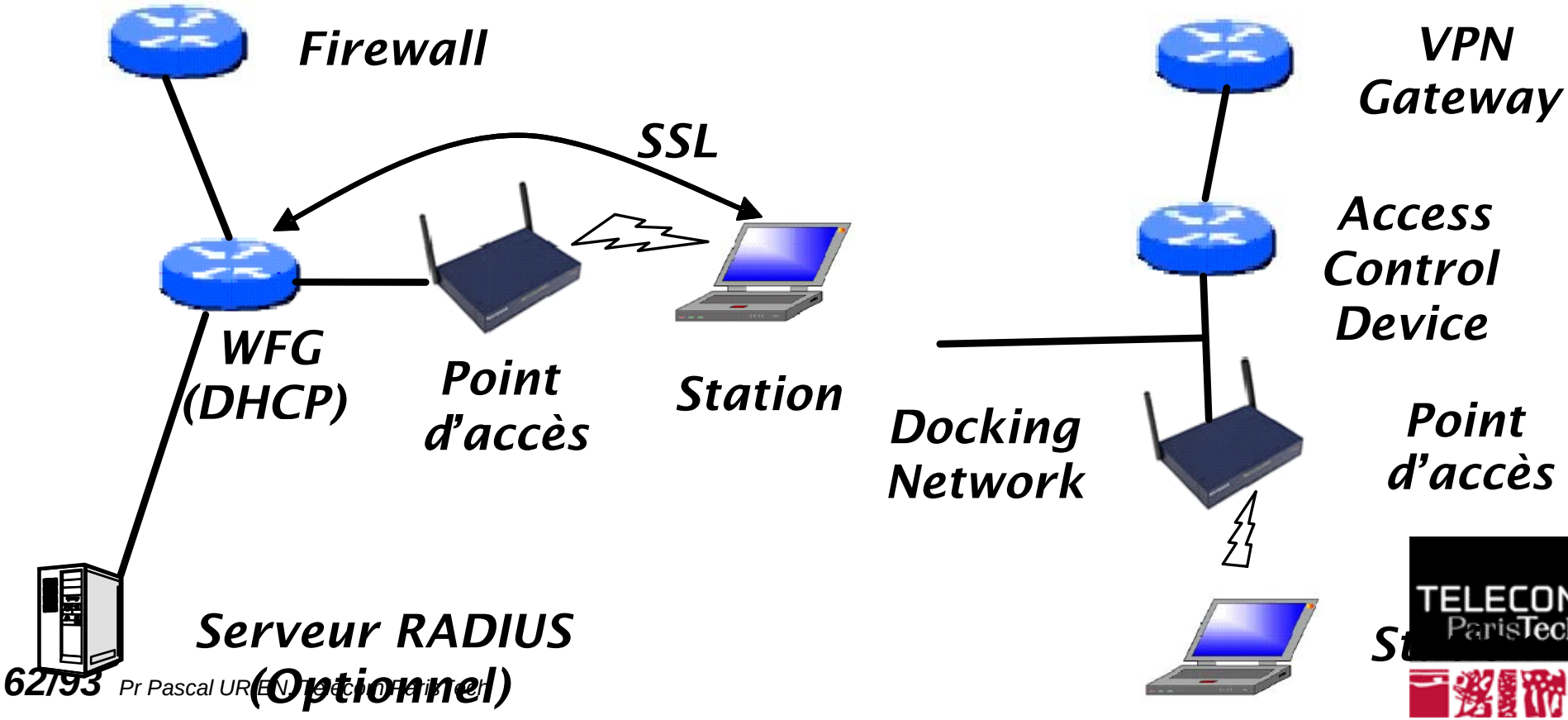




Architectures Alternatives

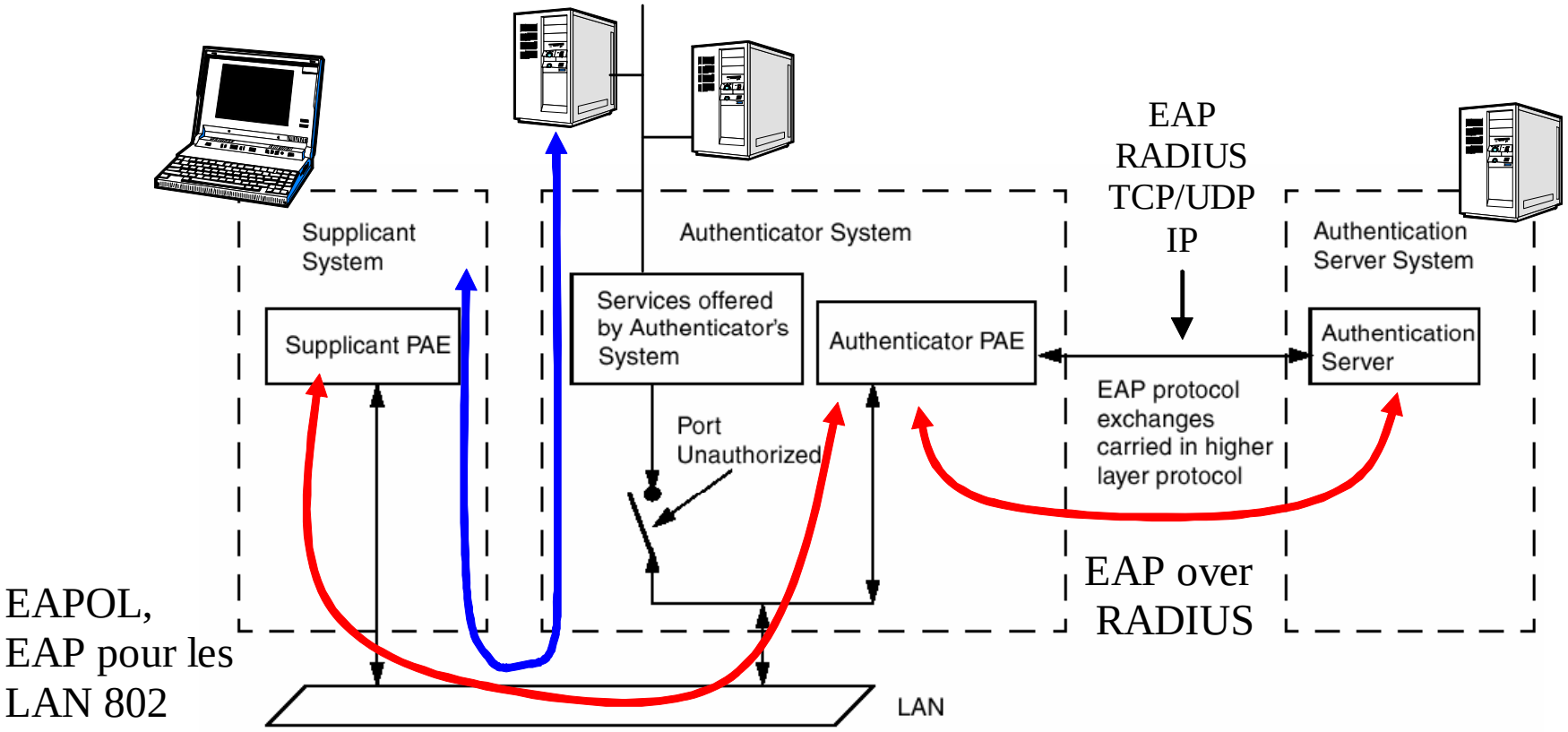
Architectures Alternatives

- **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

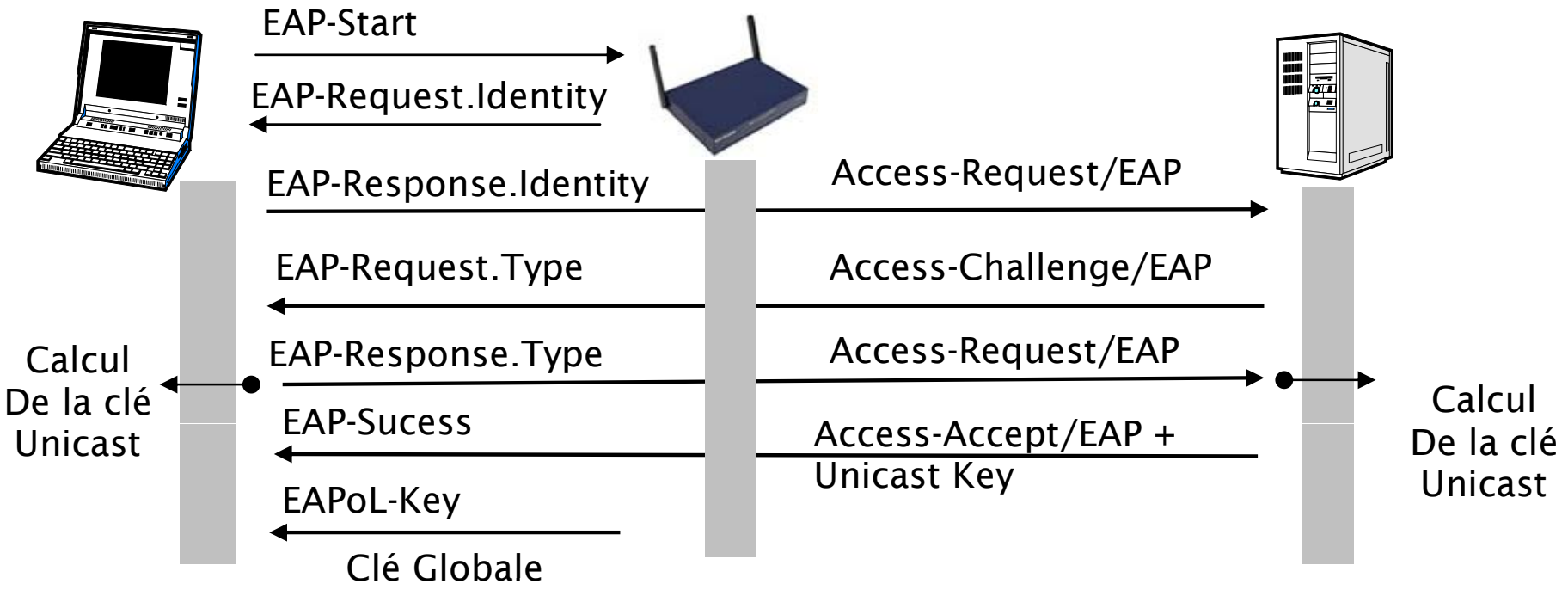
- **Les trames émises par une station non authentifiée sont filtrées par le système d 'authentification.**
- **Les éléments de la procédure d 'authentification sont échangés via par le protocole EAP (*Extended Authentication Protocol*) .**
- **EAP est transporté par des trames 802 (EAP encapsulation 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).**

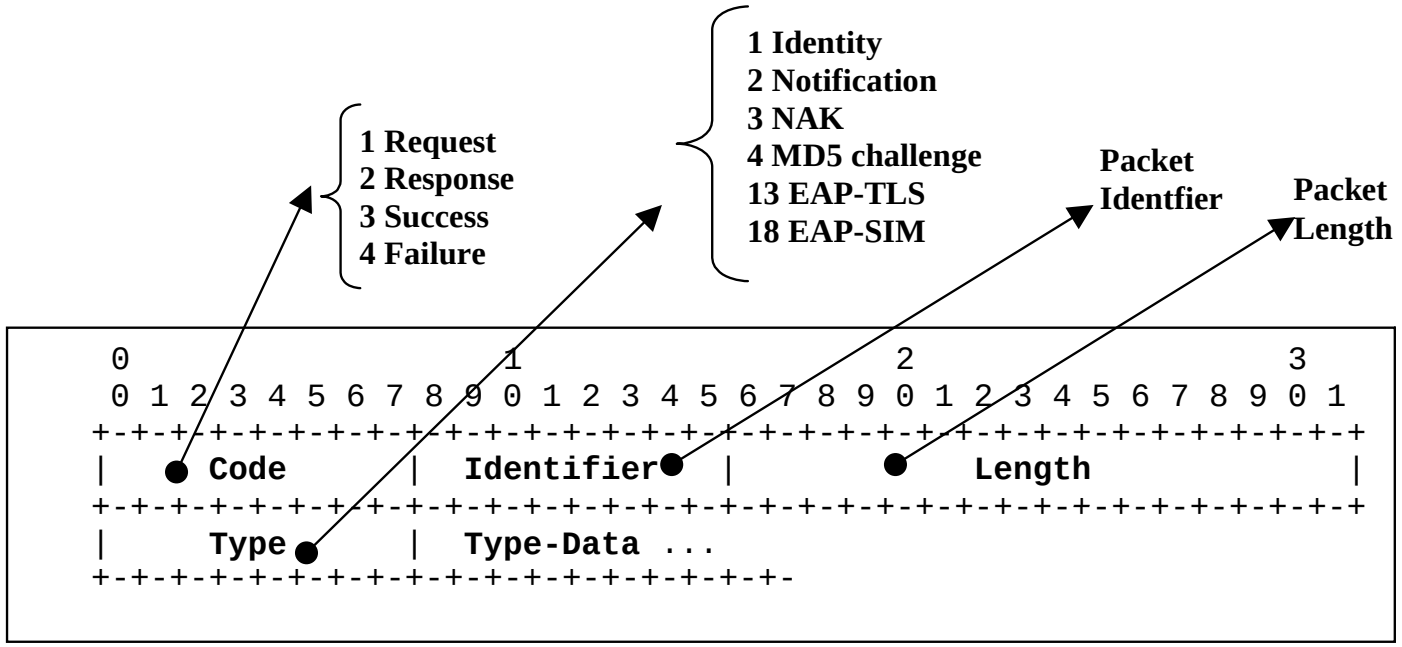
EAPoL key Descriptor

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


EAP-Start
EAP-Request.Identity
EAP-Response.Identity
Access-Request/EAP
EAP-Request.Type
Access-Challenge/EAP
Calcul
De la clé
Unicast
EAP-Response.Type
Access-Request/EAP
EAP-Sucess
Access-Accept/EAP +
Unicast Key
EAPoL-Key
Clé Globale
Calcul
De la clé
Unicast

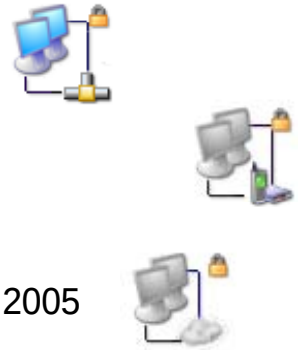
Le protocole EAP.

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

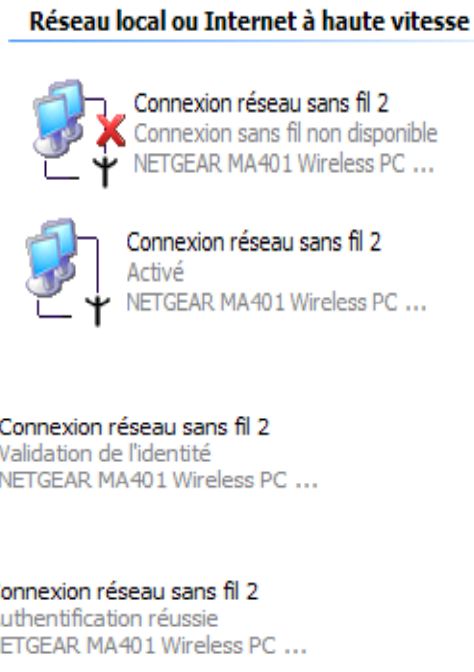


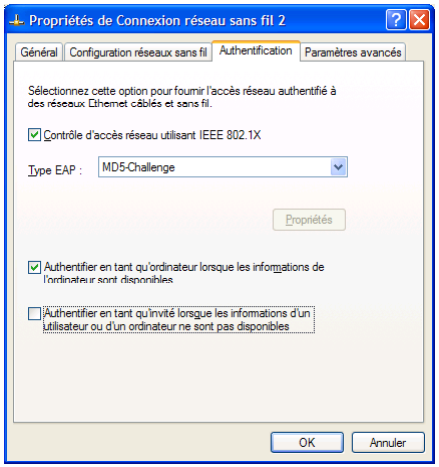
EAP, what else ?

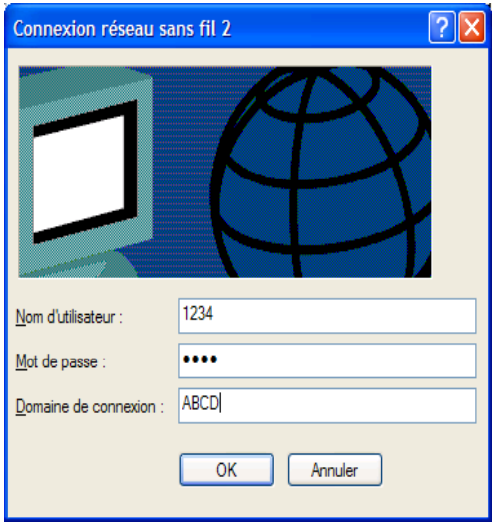
- **The Extensible Authentication Protocol (EAP) was introduced in 1999, in order to define a flexible authentication framework.**
  - EAP, RFC 3748, "Extensible Authentication Protocol, (EAP)", June 2004.
    - *EAP-TLS*, RFC 2716, "PPP EAP TLS Authentication Protocol", 1999.
    - *EAP-SIM*, RFC 4186, " 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

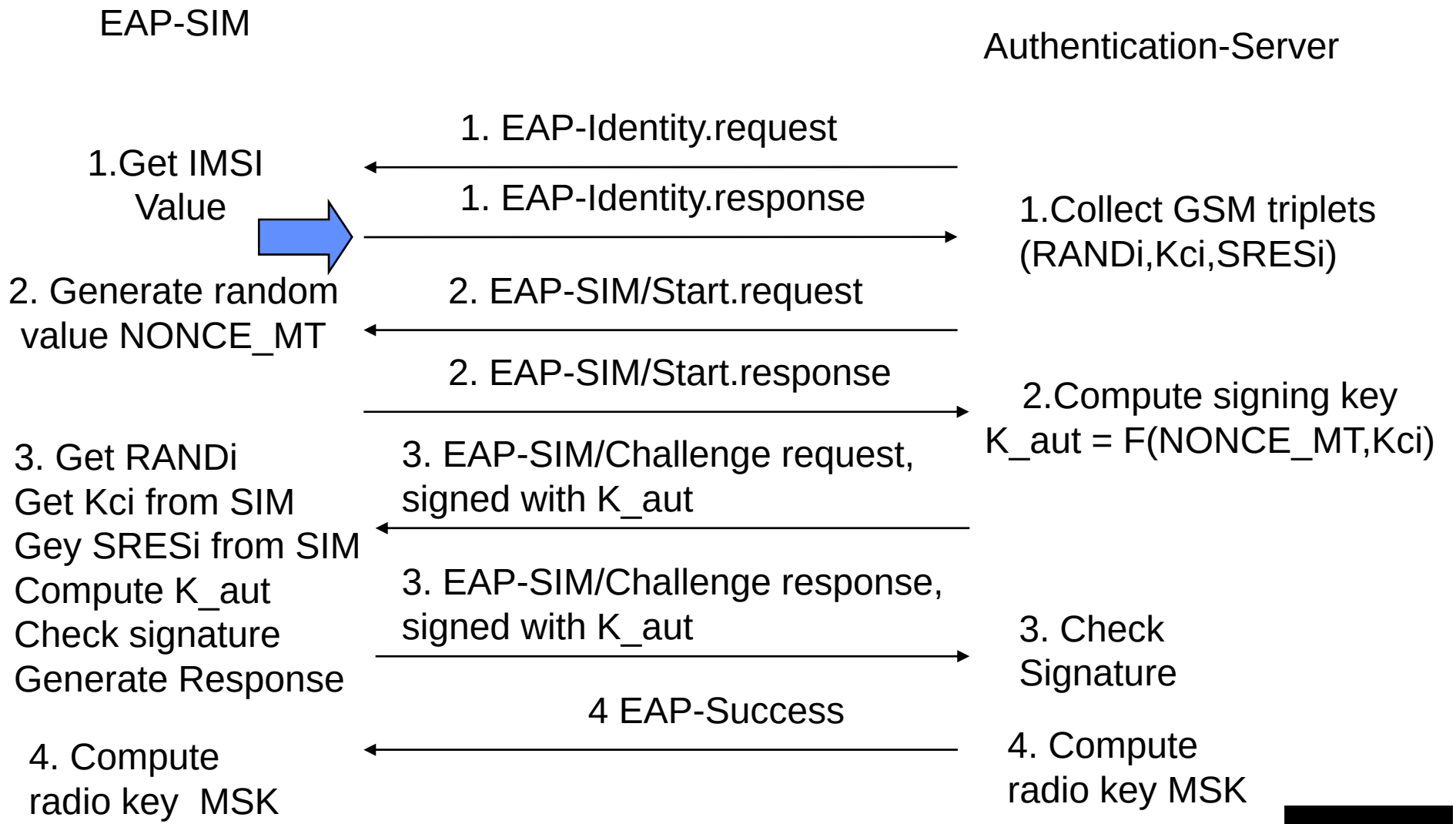
MD5-Request
00 30 ab 1a 07 8f 00 30 ab 14 68 ef 88 8e **01 00 00 06 01 a8 00 06 04 00**

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 1/8


EAP-SIM
Authentication-Server
1. EAP-Identity.request
1.Get IMSI Value
1. EAP-Identity.response
1.Collect GSM triplets (RANDi,Kci,SRESi)
2. Generate random value NONCE_MT
2. EAP-SIM/Start.request
2. EAP-SIM/Start.response
2.Compute signing key K_aut = F(NONCE_MT,Kci)
3. Get RANDi
Get Kci from SIM
Gey SRESi from SIM
Compute K_aut
Check signature
Generate Response
3. EAP-SIM/Challenge request, signed with K_aut
3. EAP-SIM/Challenge response, signed with K_aut
3. Check Signature
4 EAP-Success
4. Compute radio key MSK
4. Compute radio key MSK

EAP-Identity.request/response 2/8

```
01                      ; Code: Request
00                      ; Identifier: 0
00 05                   ; Length: 5 octets
01                      ; Type: Identity
```

```
02                      ; Code: Response
00                      ; Identifier: 0
00 20                   ; Length: 32 octets
01                      ; Type: Identity
   31 32 34 34          ; "124407010000000 1@eapsim.foo"
   30 37 30 31
   30 30 30 30
   30 30 30 31
   40 65 61 70
   73 69 6d 2e
   66 6f 6f
```

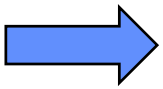
IMSI

EAP-ID may be null or only includes a NAI realm portion

EAP-SIM/Start 3/8

```
01                  ; Code: Request
01                  ; Identifier: 1
00 10               ; Length: 16 octets
12                  ; Type: EAP-SIM
   0a               ; EAP-SIM subtype: Start
   00 00            ; (reserved)
   0f               ; Attribute type: AT_VERSION_LIST
      02            ; Attribute length: 8 octets (2*4)
      00 02         ; Actual version list length: 2 octets
      00 01         ; Version: 1
      00 00         ; (attribute padding)
```

```
02                  ; Code: Response
01                  ; Identifier: 1
00 20               ; Length: 32 octets
12                  ; Type: EAP-SIM
   0a               ; EAP-SIM subtype: Start
   00 00            ; (reserved)
   07               ; Attribute type: AT_NONCE_MT
      05            ; Attribute length: 20 octets (5*4)
      00 00         ; (reserved)
      01 23 45 67   ; NONCE_MT 16 bytes value
      89 ab cd ef
      fe dc ba 98
      76 54 32 10
   10               ; Attribute type: AT_SELECTED_VERSION
      01            ; Attribute length: 4 octets (1*4)
      00 01         ; Version: 1
```



Random value 16 bytes generated by the client

Key Hierarchy & Derivation 4/8

```
(RAND1,SRES1,Kc1) = (10111213 14151617 18191a1b 1c1d1e1f, d1d2d3d4, a0a1a2a3,a4a5a6a7)
(RAND2,SRES2,Kc2) = (20212223 24252627 28292a2b 2c2d2e2f, e1e2e3e4, b0b1b2b3 b4b5b6b7)
(RAND3,SRES3,Kc3) = (30313233 34353637 38393a3b 3c3d3e3f, f1f2f3f4, c0c1c2c3 c4c5c6c7)
```

XKEY= SHA1(Identity | Kc1 | Kc2 | Kc3 | NONCE_MT | Version List | Selected Version)

XKEY = e576d5ca 332e9930 018bf1ba ee2763c7 95b3c712

And the other keys are derived using the **FIPS-186-2** PRF (Pseudo Random Function)

$$x\_j = PRF_{FIPS\text{-}186\text{-}2}(XKEY)$$

```
K_encr = 536e5ebc 4465582a a6a8ec99 86ebb620
```

Signing Key →

```
K_aut =  25af1942 efcbf4bc 72b39434 21f2a974
```

Radio Key →

```
MSK =    39d45aea f4e30601 983e972b 6cfd46d1
         c3637733 65690d09 cd44976b 525f47d3
         a60a985e 955c53b0 90b2e4b7 3719196a
         40254296 8fd14a88 8f46b9a7 886e4488
```

```
EMSK =   5949eab0 fff69d52 315c6c63 4fd14a7f
         0d52023d 56f79698 fa6596ab eed4f93f
         bb48eb53 4d985414 ceed0d9a 8ed33c38
         7c9dfdab 92ffbdf2 40fcecf6 5a2c93b9
```

EAP-SIM/Challenge request 5/8

```
01                  ; Code: Request
 02                 ; Identifier: 2
 01 18              ; Length: 280 octets
 12                 ; Type: EAP-SIM
    0b              ; EAP-SIM subtype: Challenge
    00 00           ; (reserved)
    01              ; Attribute type: AT_RAND
       0d           ; Attribute length: 52 octets (13*4)
       00 00        ; (reserved)
       10 11 12 13  ; first RAND
       14 15 16 17
       18 19 1a 1b
       1c 1d 1e 1f
       20 21 22 23  ; second RAND
       24 25 26 27
       28 29 2a 2b
       2c 2d 2e 2f
       30 31 32 33  ; third RAND
       34 35 36 37
       38 39 3a 3b
       3c 3d 3e 3f
```

```
   81               ; Attribute type: AT_IV
    05              ; Attribute length: 20 octets (5*4)
    00 00           ; (reserved)
    9e 18 b0 c2     ; IV value
    9a 65 22 63
    c0 6e fb 54
    dd 00 a8 95
82                  ; Attribute type: AT_ENCR_DATA (AES(K_encr) 128 bits)
    2d              ; Attribute length: 180 octets (45*4)
    00 00           ; (reserved)
    55 f2 93 9b bd b1 b1 9e a1 b4 7f c0 b3 e0 be 4c
    ab 2c f7 37 2d 98 e3 02 3c 6b b9 24 15 72 3d 58
    ba d6 6c e0 84 e1 01 b6 0f 53 58 35 4b d4 21 82
    78 ae a7 bf 2c ba ce 33 10 6a ed dc 62 5b 0c 1d
    5a a6 7a 41 73 9a e5 b5 79 50 97 3f c7 ff 83 01
    07 3c 6f 95 31 50 fc 30 3e a1 52 d1 e1 0a 2d 1f
    4f 52 26 da a1 ee 90 05 47 22 52 bd b3 b7 1d 6f
    0c 3a 34 90 31 6c 46 92 98 71 bd 45 cd fd bc a6
    11 2f 07 f8 be 71 79 90 d2 5f 6d d7 f2 b7 b3 20
    bf 4d 5a 99 2e 88 03 31 d7 29 94 5a ec 75 ae 5d
    43 c8 ed a5 fe 62 33 fc ac 49 4e e6 7a 0d 50 4d
0b                  ; Attribute type: AT_MAC
    05              ; Attribute length: 20 octets (5*4)
    00 00           ; (reserved)
    fe f3 24 ac     ; MAC value
    39 62 b5 9f
    3b d7 82 53
    ae 4d cb 6a
```

Signing Value

The MAC is calculated over the EAP packet above (with MAC value set to zero), followed by the NONCE_MT value (a total of 296 bytes).

MAC_Value = HMAC_SHA1(k_aut, message)

Decrypted Content of AT_ENCR 6/8

```
 84              ; Attribute type: AT_NEXT_PSEUDONYM
   13            ; Attribute length: 76 octets (19*4)
   00 46         ; Actual pseudonym length: 70 octets
   77 38 77 34 39 50 65 78 43 61 7a 57 4a 26 78 43
   49 41 52 6d 78 75 4d 4b 68 74 35 53 31 73 78 52
   44 71 58 53 45 46 42 45 67 33 44 63 5a 50 39 63
   49 78 54 65 35 4a 34 4f 79 49 77 4e 47 56 7a 78
   65 4a 4f 55 31 47
   00 00           ; (attribute padding)
85                 ; Attribute type: AT_NEXT_REAUTH_ID
   16              ; Attribute length: 88 octets (22*4)
   00 51           ; Actual re-auth identity length
                   ; 81 octets
   59 32 34 66 4e 53 72 7a 38 42 50 32 37 34 6a 4f
   4a 61 46 31 37 57 66 78 49 38 59 4f 37 51 58 30
   30 70 4d 58 6b 39 58 4d 4d 56 4f 77 37 62 72 6f
   61 4e 68 54 63 7a 75 46 71 35 33 61 45 70 4f 6b
   6b 33 4c 30 64 6d 40 65 61 70 73 69 6d 2e 66 6f
   6f
   00 00 00        ; (attribute padding)
06                 ; Attribute type: AT_PADDING
   03              ; Attribute length: 12 octets (3*4)
   00 00 00 00
   00 00 00 00
   00 00
```

AT_NEXT_PSEUDONYM
"w8w49PexCazWJ&xCIARmxuMKht5S1sxR DqXSEFBEg3DcZP9cIxTe5J4OyIwNGVzxeJOU1G"
AT_NEXT_REAUTH_ID
"Y24fNSrz8BP274jOJaF17WfxI8YO7QX00pMXk9XMMVOw7broaNhTczuFq53aEpOkk3L0dm@eap

EAP-SIM/Challenge Response 7/8

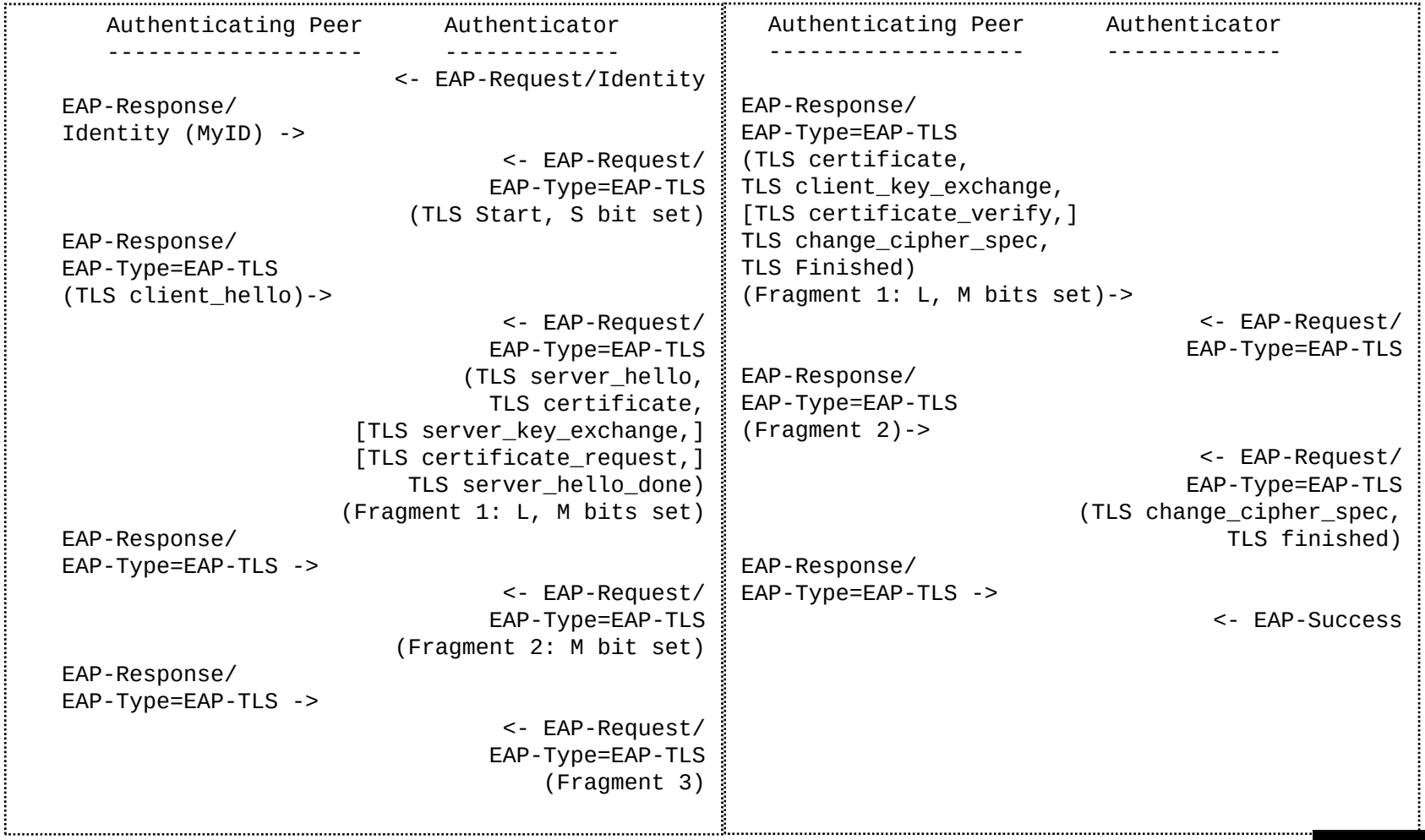
```
02                  ; Code: Response
02                  ; Identifier: 2
00 1c               ; Length: 28 octets
12                  ; Type: EAP-SIM
   0b               ; EAP-SIM subtype: Challenge
   00 00            ; (reserved)
   0b               ; Attribute type: AT_MAC
      05            ; Attribute length: 20 octets (5*4)
      00 00         ; (reserved)

      f5 6d 64 33   ; MAC value
      e6 8e d2 97
      6a c1 19 37
      fc 3d 11 54
```

The MAC is calculated over the EAP packet above (with MAC value set to zero), followed by the SRESi (SRES1| SRES2| SRES3) values (a total of 40 bytes).

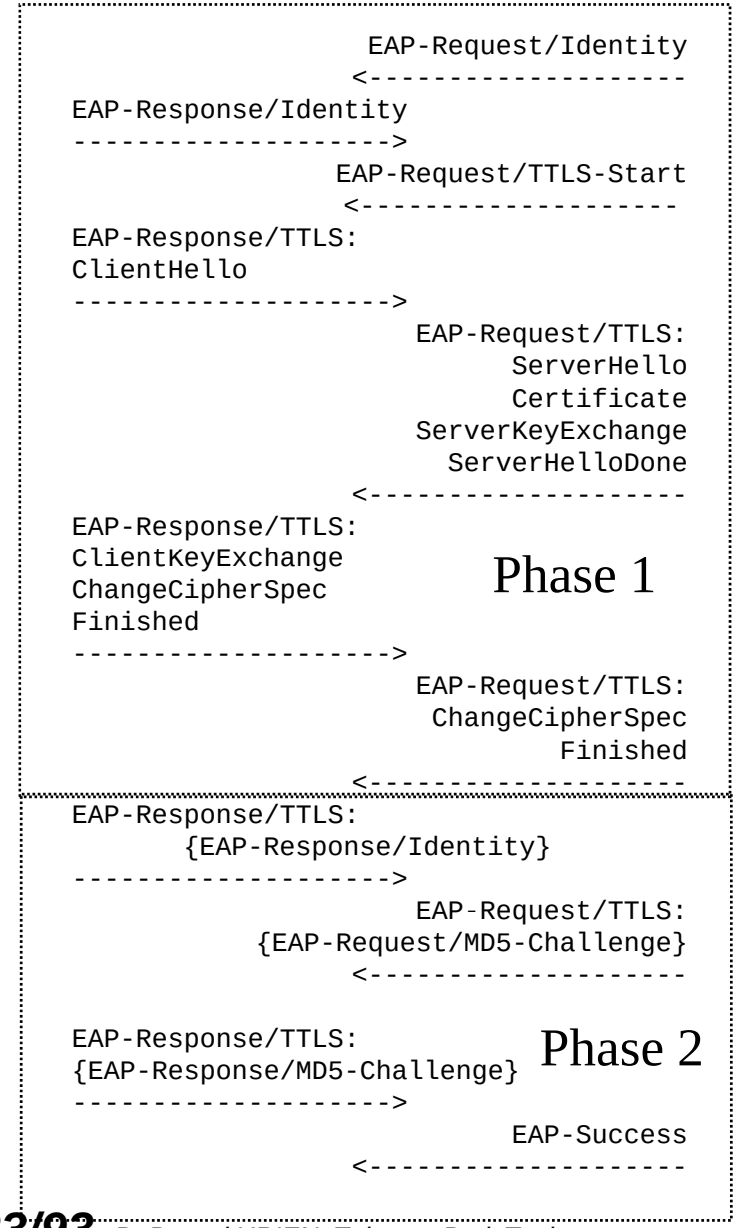
EAP-Success 8/8

```
03                      ; Code: Success
 03                     ; Identifier: 3
 00 04                  ; Length: 4 octets
```

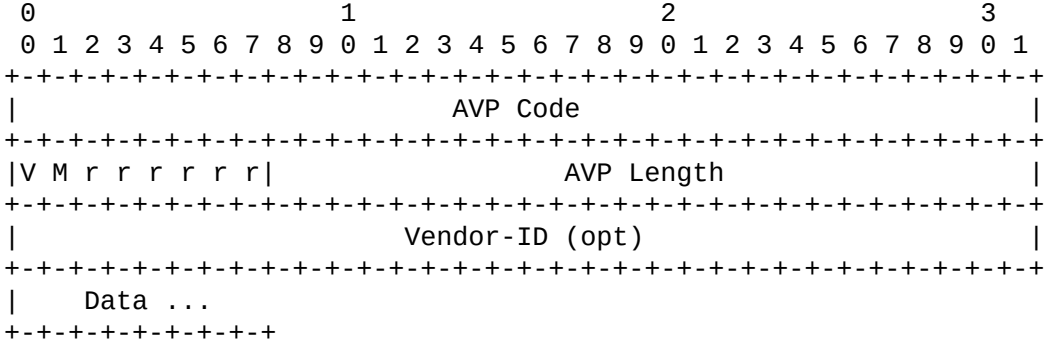
EAP-TLS

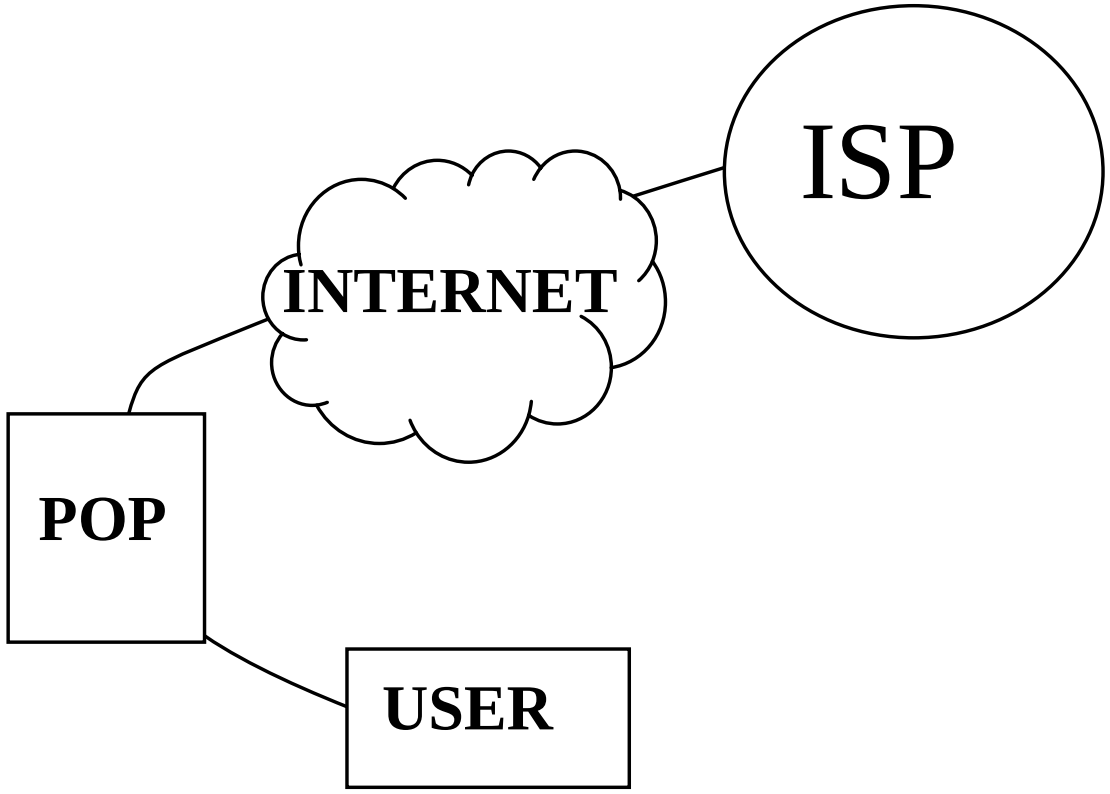

Authenticating Peer
Authenticator
<- EAP-Request/Identity
EAP-Response/
Identity (MyID) ->
<- EAP-Request/
EAP-Type=EAP-TLS
(TLS Start, S bit set)
EAP-Response/
EAP-Type=EAP-TLS
(TLS client_hello)->
<- EAP-Request/
EAP-Type=EAP-TLS
(TLS server_hello,
TLS certificate,
[TLS server_key_exchange,]
[TLS certificate_request,]
TLS server_hello_done)
(Fragment 1: L, M bits set)
EAP-Response/
EAP-Type=EAP-TLS ->
<- EAP-Request/
EAP-Type=EAP-TLS
(Fragment 2: M bit set)
EAP-Response/
EAP-Type=EAP-TLS ->
<- EAP-Request/
EAP-Type=EAP-TLS
(Fragment 3)
Authenticating Peer
Authenticator
EAP-Response/
EAP-Type=EAP-TLS
(TLS certificate,
TLS client_key_exchange,
[TLS certificate_verify,]
TLS change_cipher_spec,
TLS Finished)
(Fragment 1: L, M bits set)->
<- EAP-Request/
EAP-Type=EAP-TLS
EAP-Response/
EAP-Type=EAP-TLS
(Fragment 2)->
<- EAP-Request/
EAP-Type=EAP-TLS
(TLS change_cipher_spec,
TLS finished)
EAP-Response/
EAP-Type=EAP-TLS ->
<- EAP-Success

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

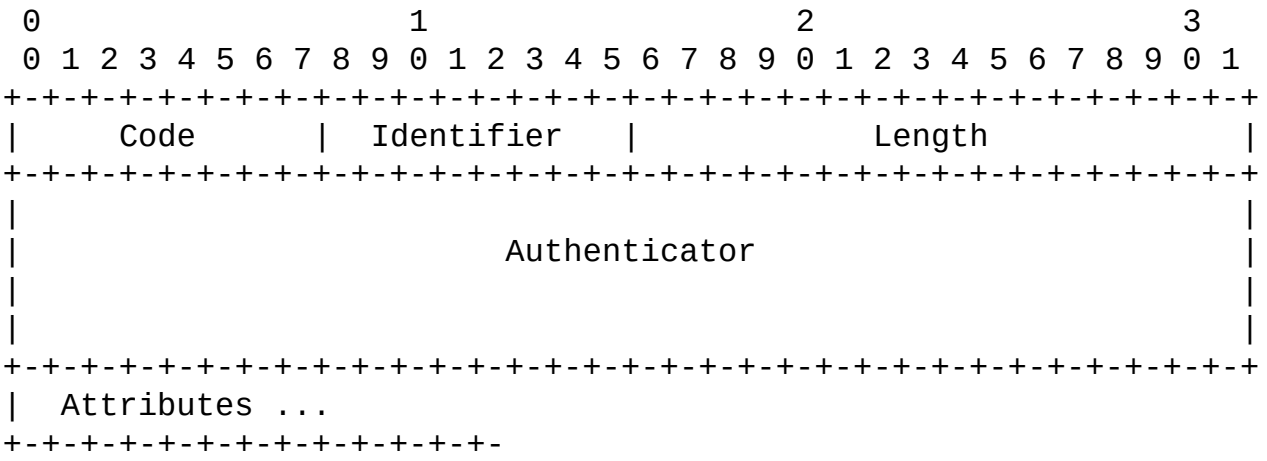
- **Le protocole** *Remote Authentication Dial In User Service* **est spécifié par la RFC 2865. La RFC 2866 (***RADIUS accounting***) définit les attributs utiles à la facturation. Les messages sont transportés par des paquets UDP, utilisant les ports 1812 (***radius***) et 1813 (***radacct***).**
- **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.

- **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

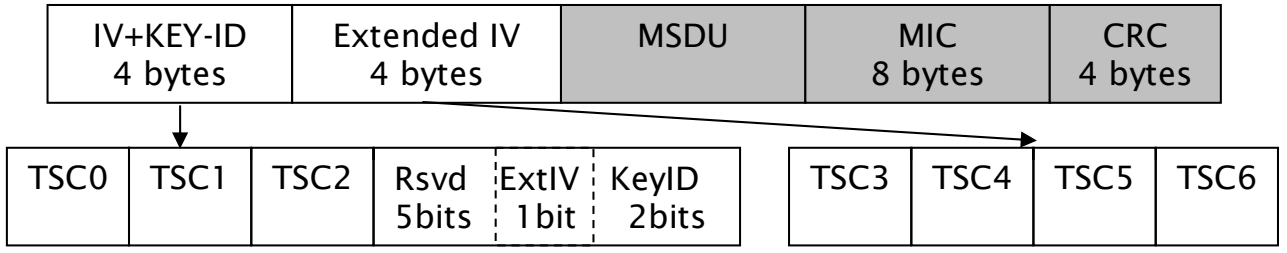


- *Code*
  - 1 Access-Request
  - 2 Access-Accept
  - 3 Access-Reject
  - 4 Accounting-Request
  - 5 Accounting-Response
  - 11 Access-Challenge
- *Identifier*
  - Identifiant d'une requête et de la réponse associée.
- *Length*
  - Longueur totale du paquet en tête incluse (à partir du champ code).
- *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

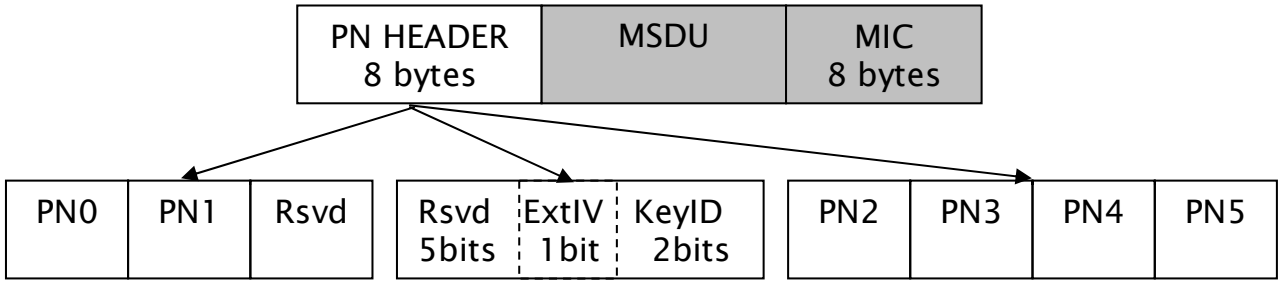
IEEE 802.11i

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

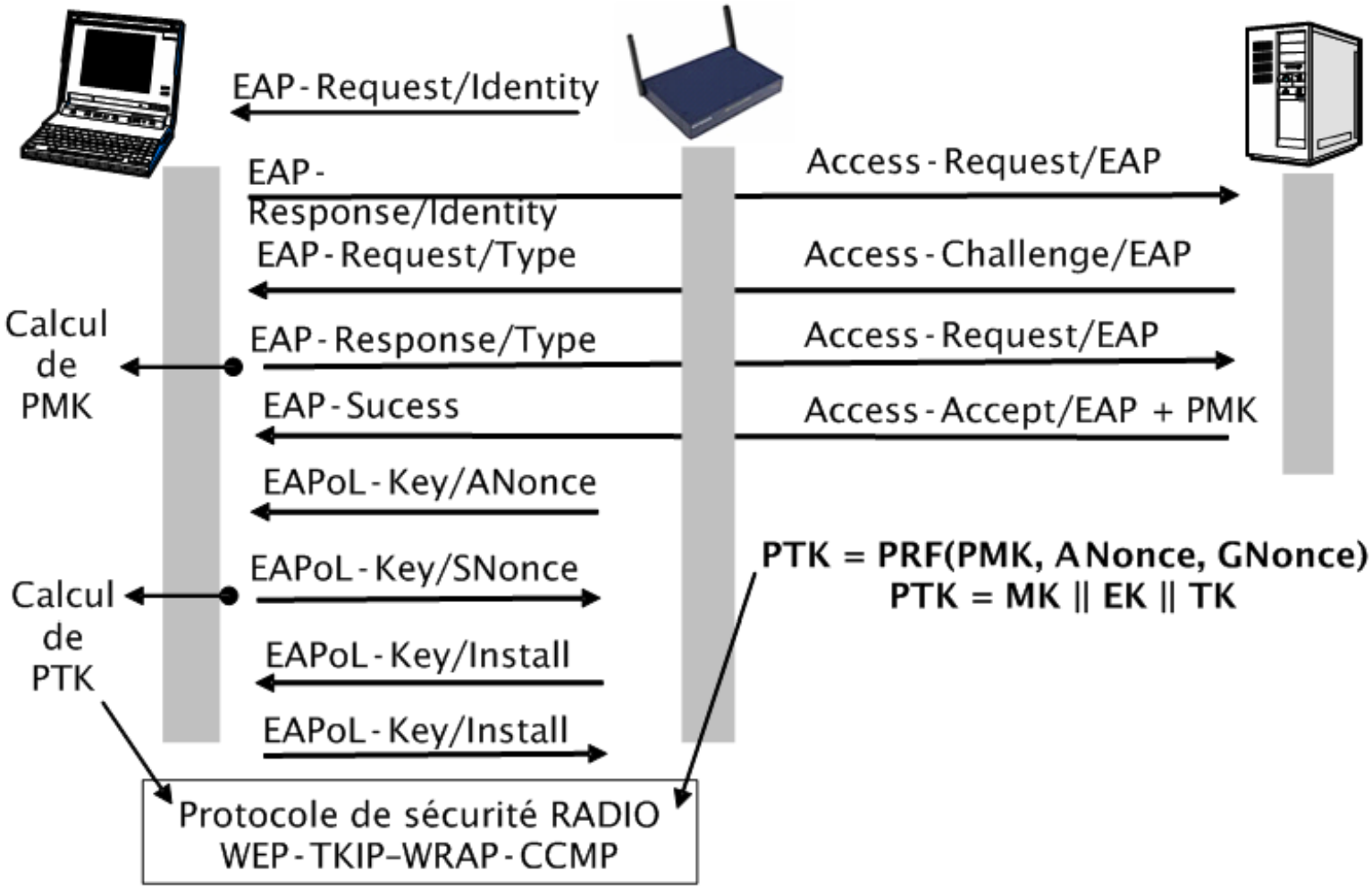


Trame CCMP

- **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.**