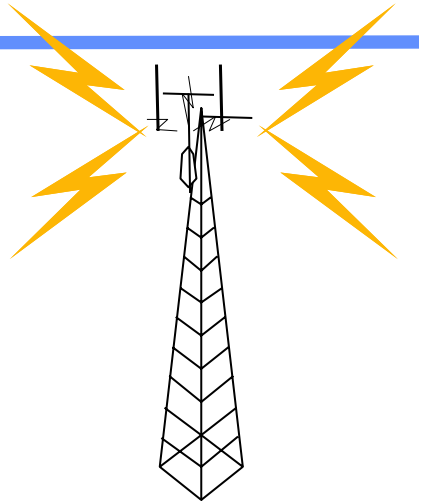
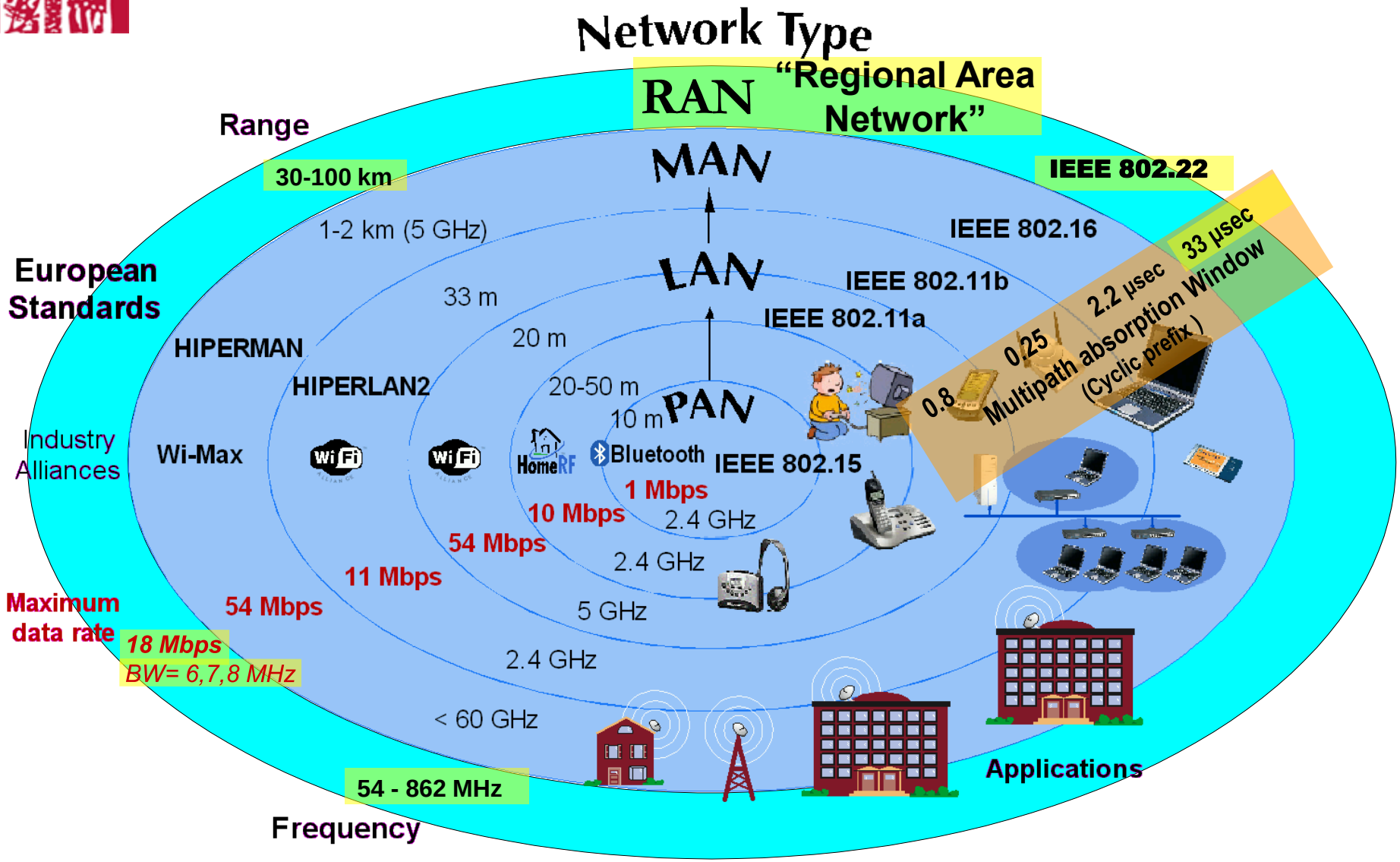


Sécurité du WiMax

« *The last mile* »

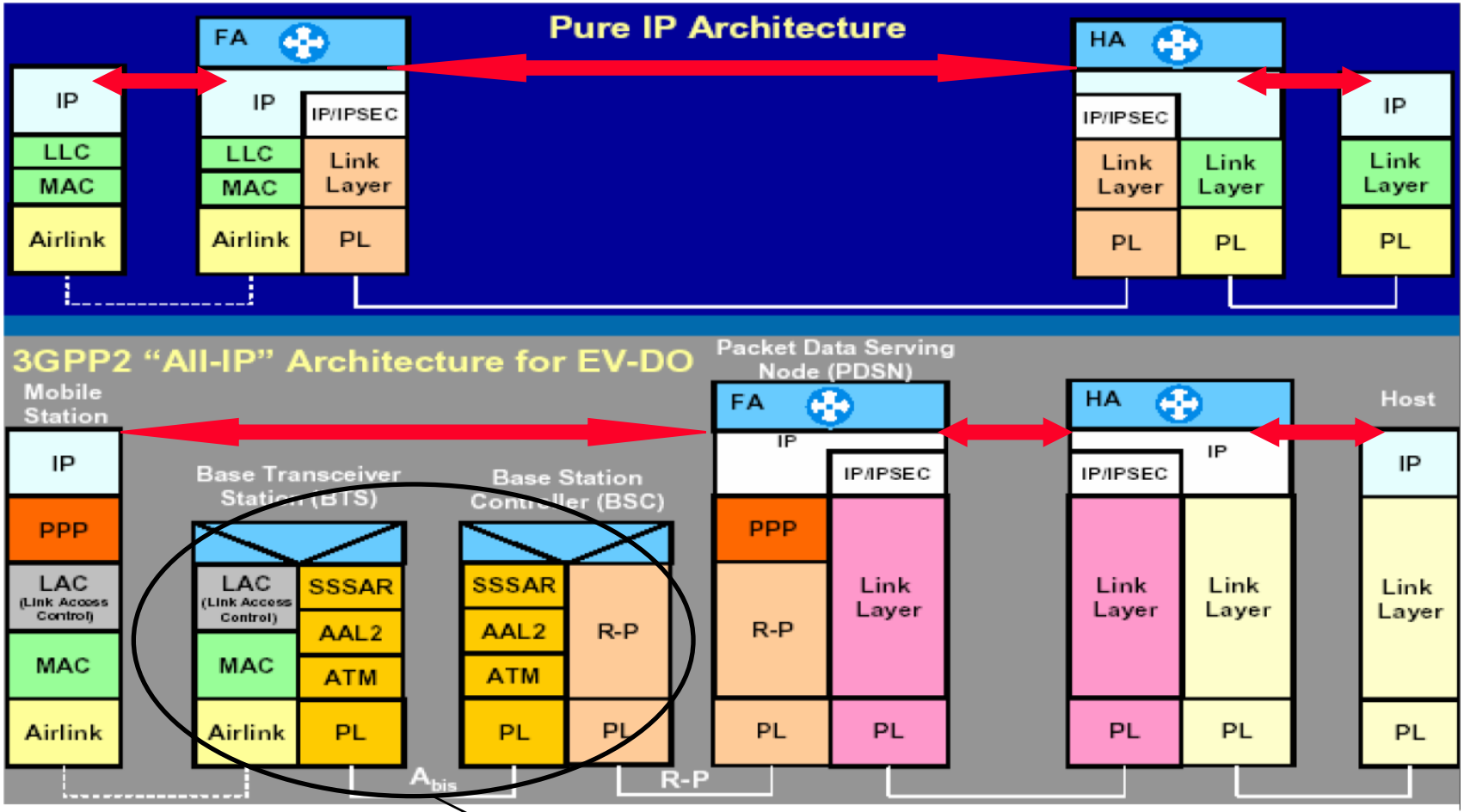
Introduction

Le WiMAX dans la famille des standards IEEE



Comparaison IEEE 802.16e - 3GPP2

Wi-Technologies



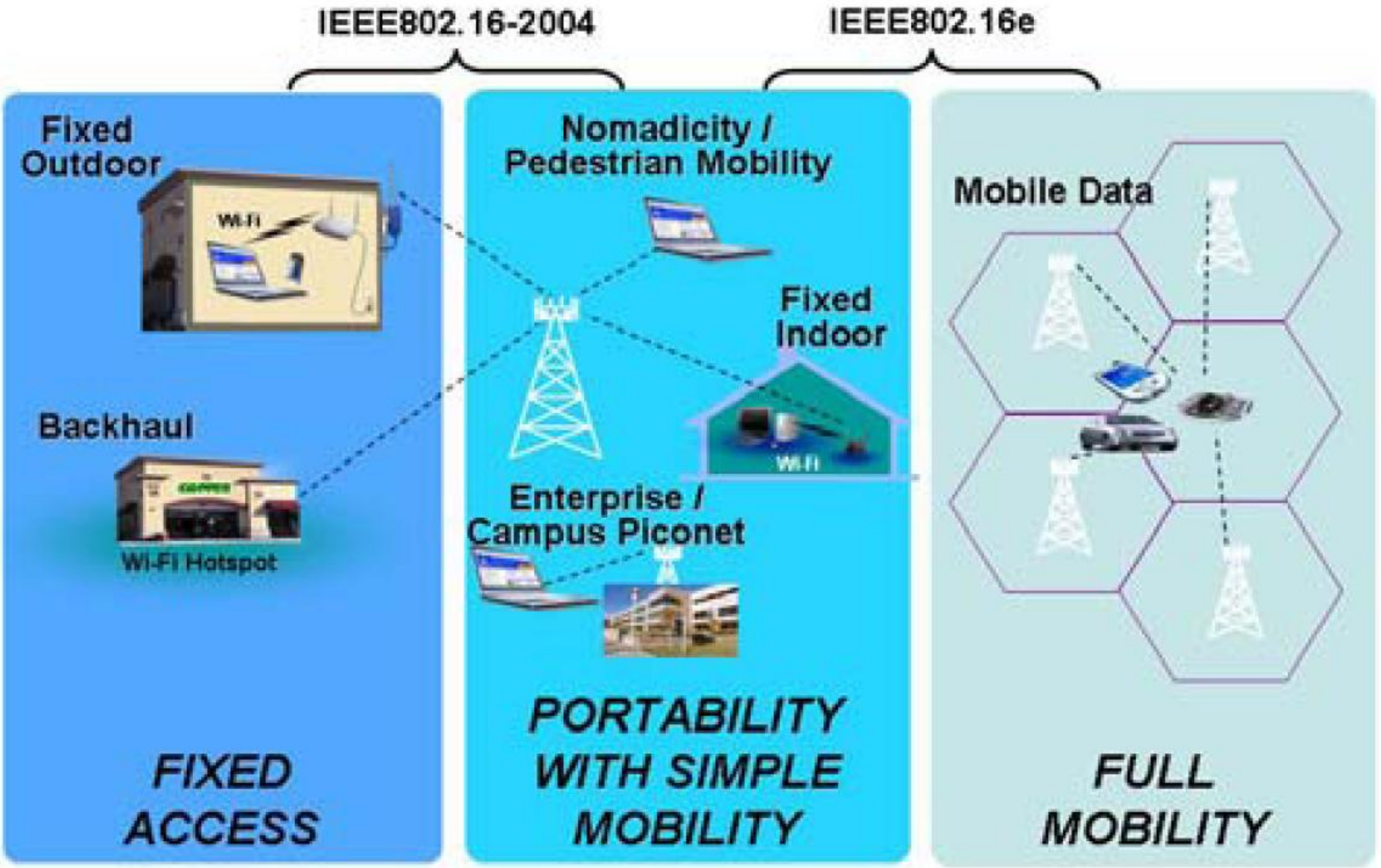
3GPP-Technologies

Non IP segment

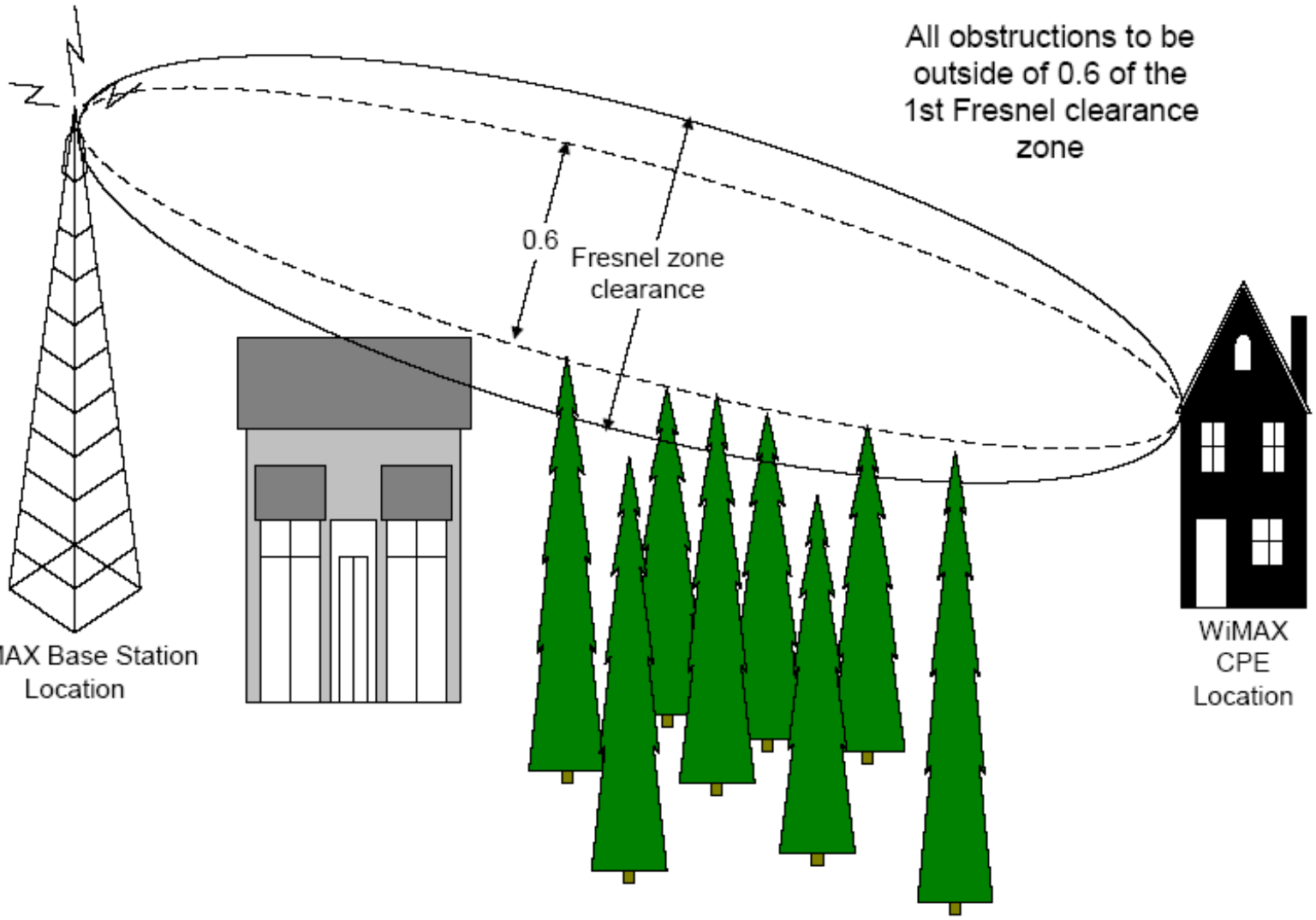
IEEE 802.16 standards 1/2

	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

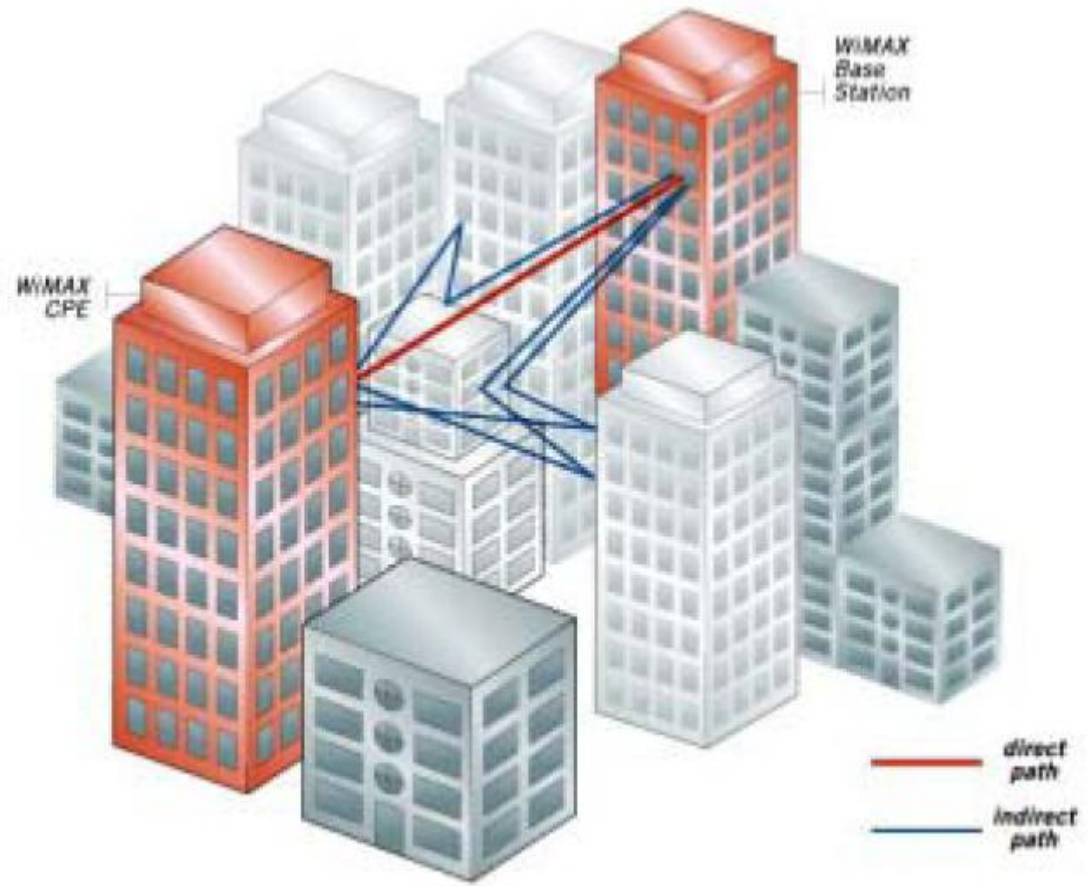


IEEE 802.16-2001, Line Of Sight



LOS Fresnel zone

IEEE 802.16-2004, Non Line Of Sight



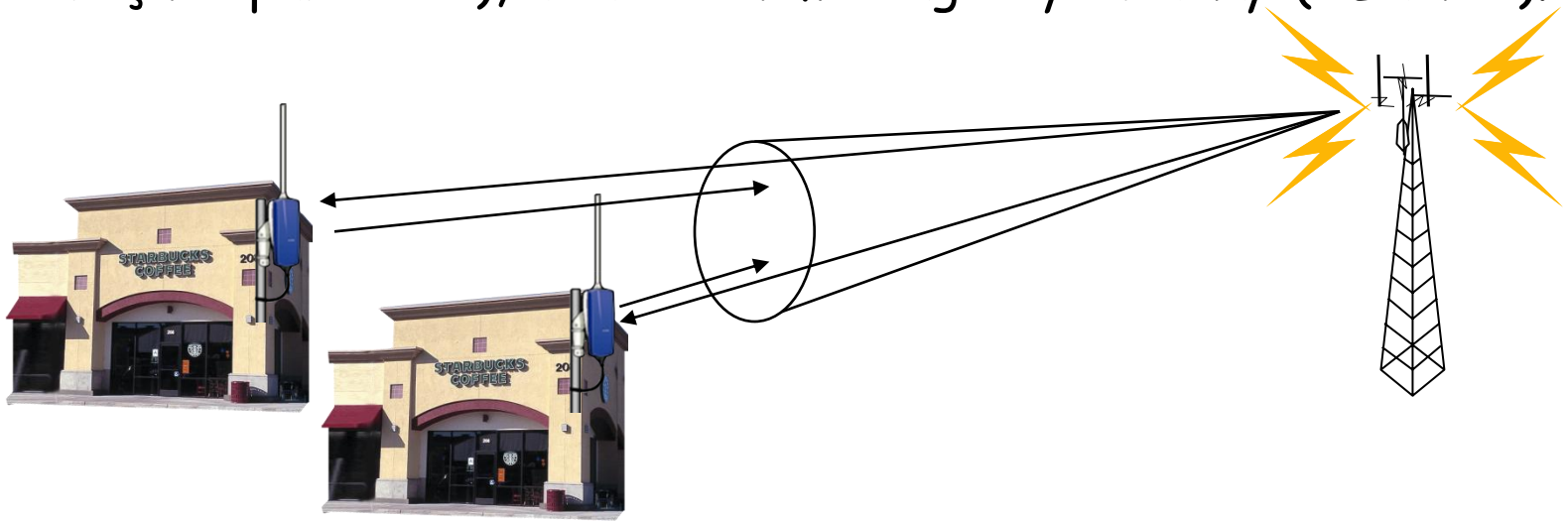
NLOS propagation

Marchés

- En premier lieu la fourniture de services de téléphonie en mode sans fil tels que T1 en Europe (2,048 Mbits/s) ou E1 (2,000 Mbits/s) aux Etats-Unis ; c'est une opportunité de prestations alternatives aux offres des opérateurs téléphoniques classiques, utilisant une infrastructure câblée.
- Le haut débit à la demande (ou *broadband on demand*) permet à une entreprise d'établir des connexions performantes entre ses agences, pour organiser par exemple des vidéoconférences.
- Cette technologie fournit également aux zones mal desservies des accès internet haut débits, analogues aux modems ADSL mais basés sur des liens hertziens.
- De même des sites géographiques isolés, pour lesquels les coûts de câblage sont importants, peuvent bénéficier de cette technique, qualifiée dans ce cas de boucle locale radio (BLR), délivrant des services de type voix ou données.
- Enfin le réseau WiMAX est un complément naturel aux *hotspots* Wi-Fi, il assure la continuité des connexions IP pour un utilisateur nomade ou un automobiliste. Un abonné peut être géré par un unique fournisseur de services IP sans fil (*Wireless Internet Service Provider*, WISP) ou bénéficier d'accords entre différents WISPs afin de conserver de manière transparente ses services (c'est le mécanisme de *roaming*)

Le PMP

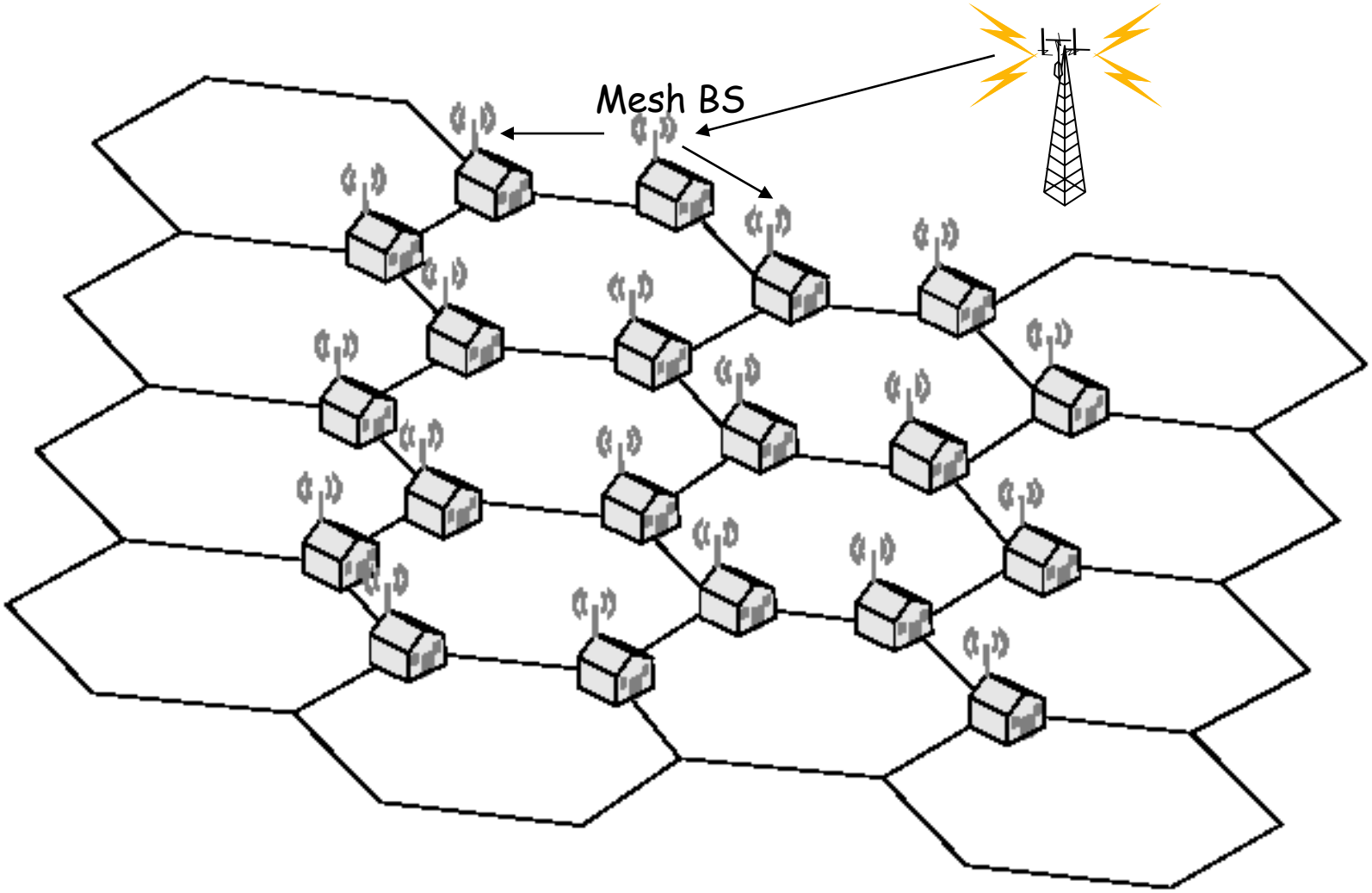
- **L'architecture du WiMAX comporte des stations de base BS *(Base Station)* munies de plusieurs antennes directionnelles, gérant des *secteurs*, et établissant des liens de type PMP *(Point to Multi Point)*. Dans un secteur donné, les voies descendantes (émission d'information vers les clients) et 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.

IEEE 802.16a (2003): MESH network

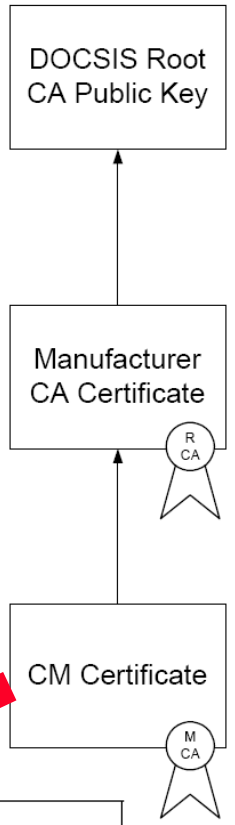


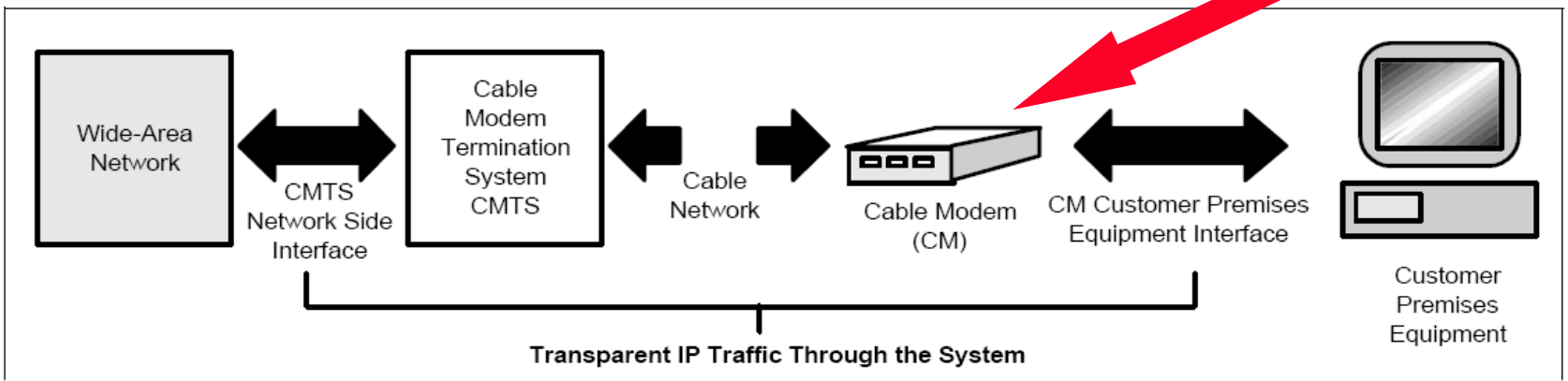
Origines du protocole PKM-EAP

Data-Over-Cable Service Interface Specifications
"DOCSIS"

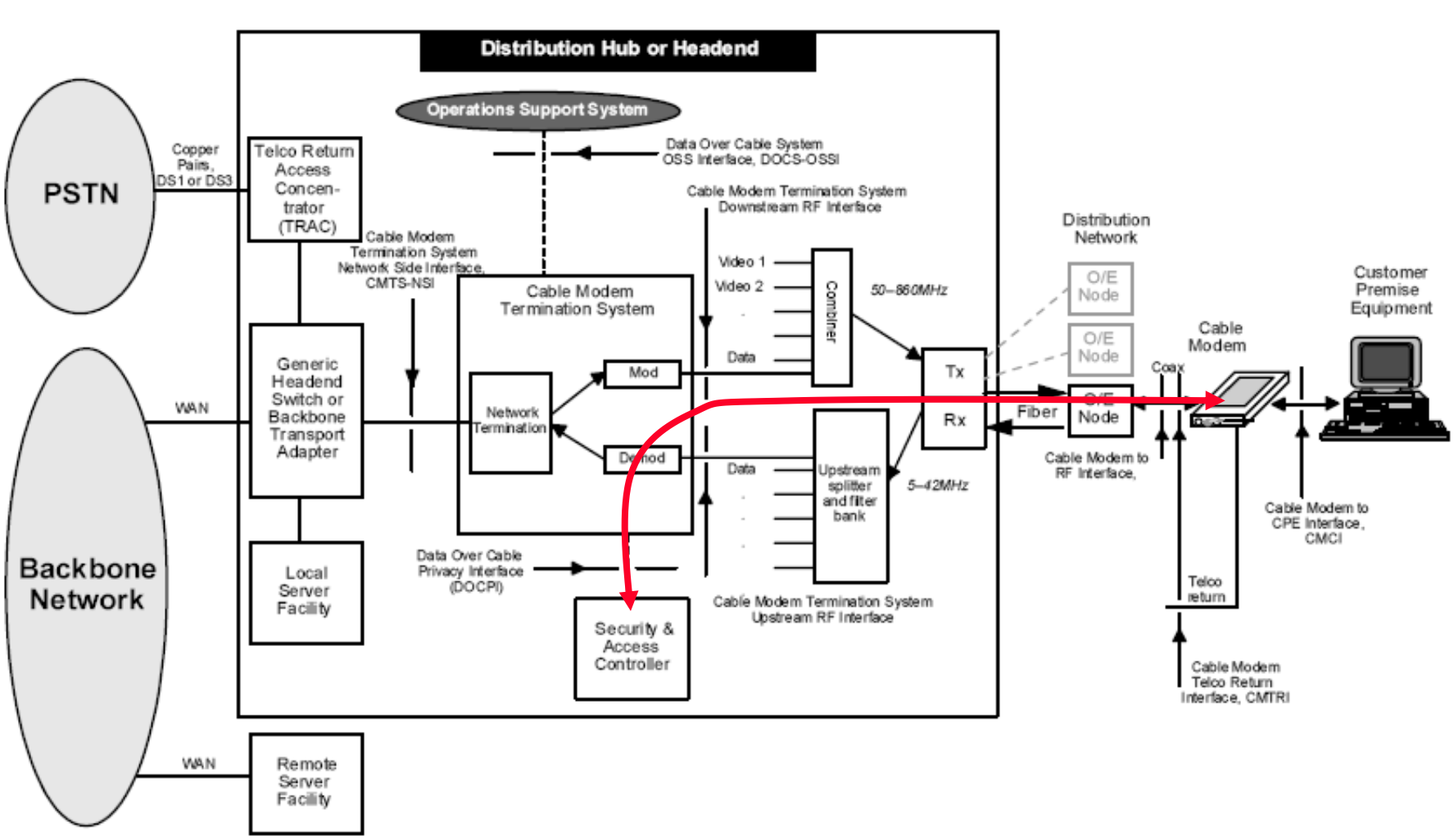
DOCSIS 1/2: BPKM

- **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).





DOCSIS 2/2: Functional architecture



DOCSIS et IEEE 802.16-2004

DOCSIS 1.1-2004

Table 4-17. BPKM Attribute Types

Type	BPKM Attribute
0	Reserved
1	Serial-Number
2	Manufacturer-ID
3	MAC-Address
4	RSA-Public-Key
5	CM-Identification
6	Display-String
7	AUTH-KEY
8	TEK
9	Key-Lifetime
10	Key-Sequence-Number
11	HMAC-Digest
12	SAID
13	TEK-Parameters
14	~~SA-Flag~~ OBSOLETED
15	CBC-IV
16	Error-Code
17	CA-Certificate
18	CM-Certificate
19	Security-Capabilities
20	Cryptographic-Suite
21	Cryptographic-Suite-List
22	BPI-Version
23	SA-Descriptor
24	SA-Type
25	SA-Query
26	SA-Query-Type
27	IP-Address
28-126	Reserved
127	Vendor-Defined
128-255	Vendor-assigned attribute types

802.16-2004

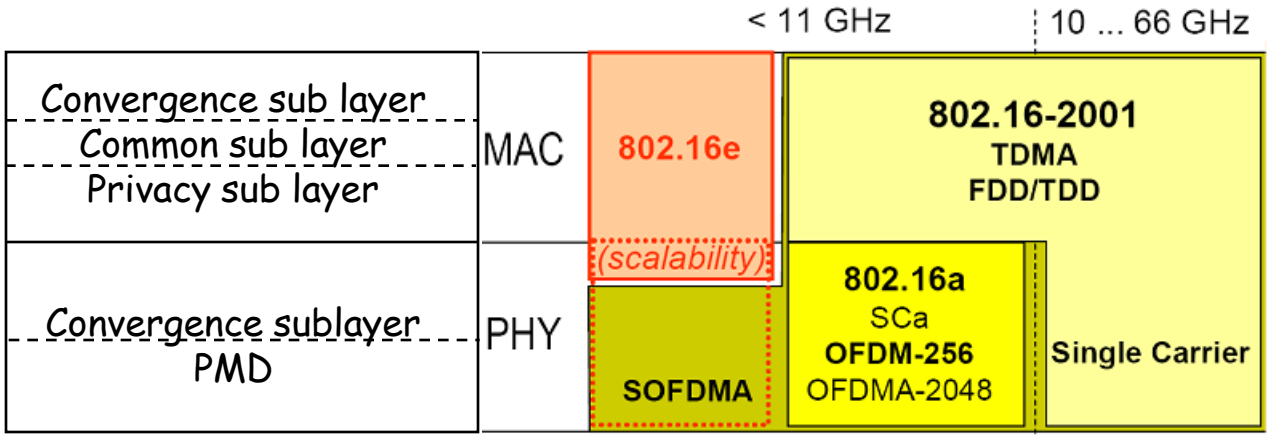
Type	PKM attribute
0–5	*reserved*
6	Display-String
7	AUTH-Key
8	TEK
9	Key-Lifetime
10	Key-Sequence-Number
11	HMAC-Digest
12	SAID
13	TEK-Parameters
14	*reserved*
15	CBC-IV
16	Error-Code
17	CA-Certificate
18	SS-Certificate
19	Security-Capabilities
20	Cryptographic-Suite
21	Cryptographic-Suite-List
22	Version
23	SA-Descriptor
24	SA-Type
25	*reserved*
26	*reserved*
27	PKM Configuration Settings
28–255	*reserved*

Modèle en couches du WiMAX

Modèle en couche du WiMAX 1/2

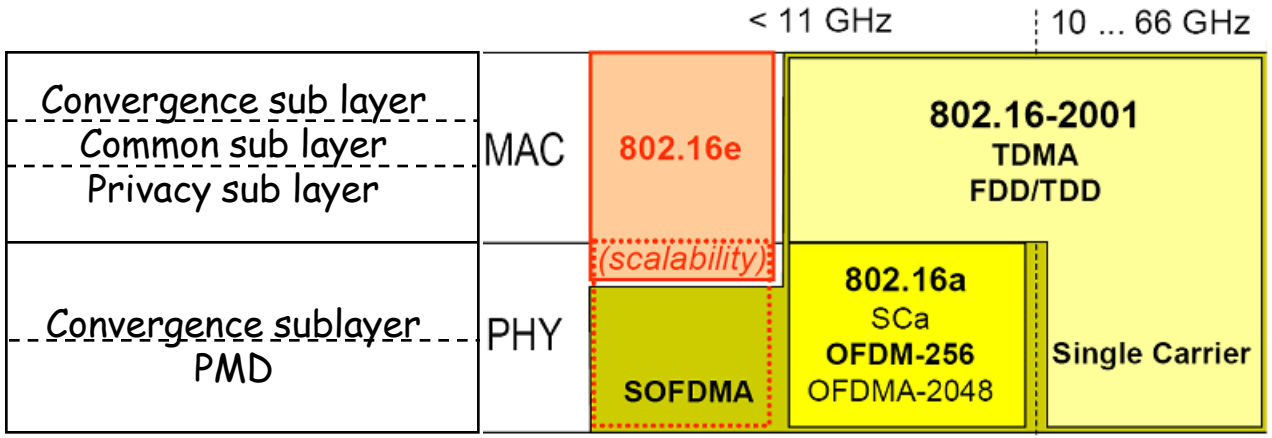
La couche MAC se divise en trois éléments, une couche de convergence, une couche dite commune, et une couche de sécurité.

- 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.

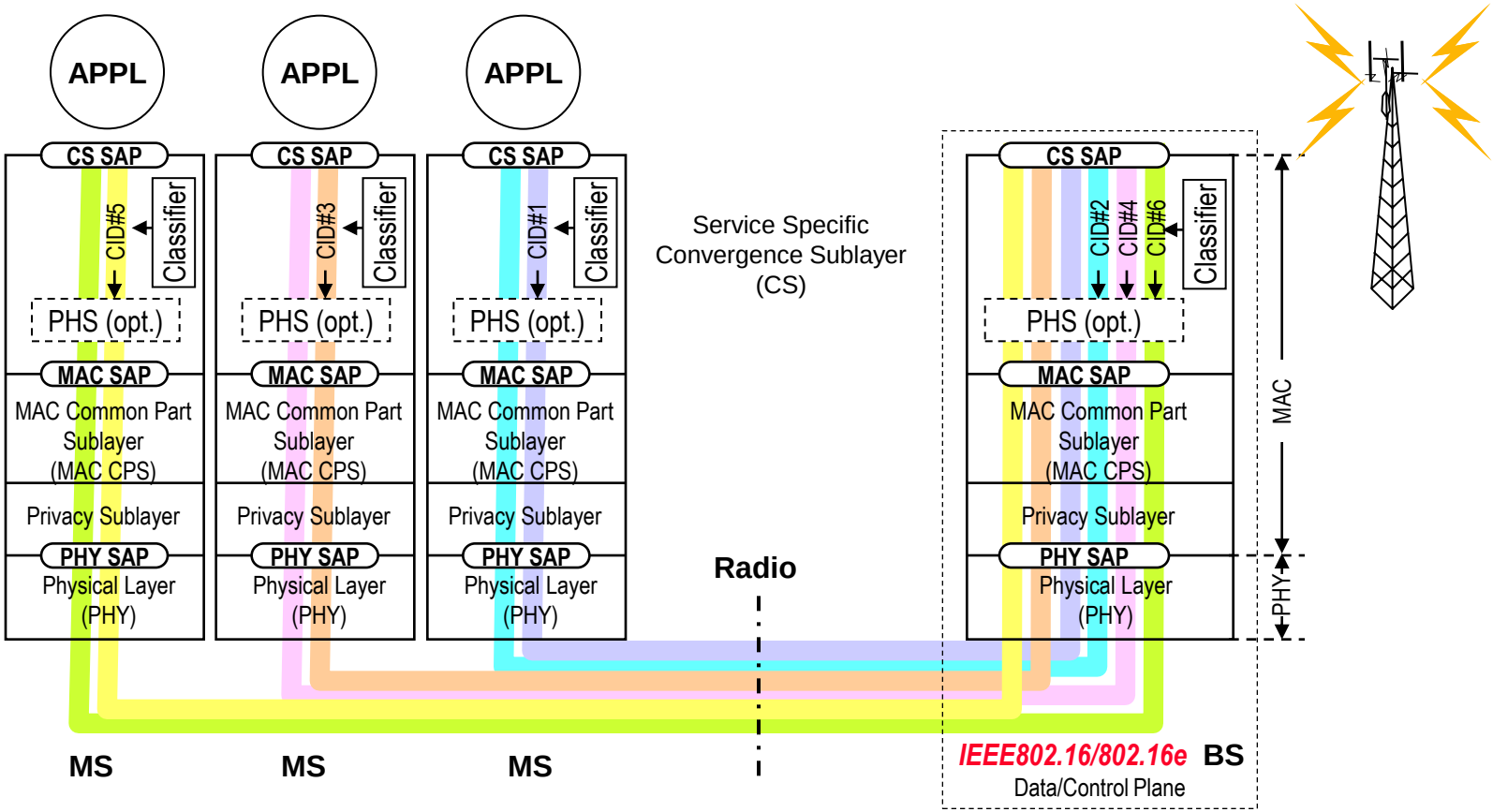


Modèle en couche du WiMAX 2/2

- 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.



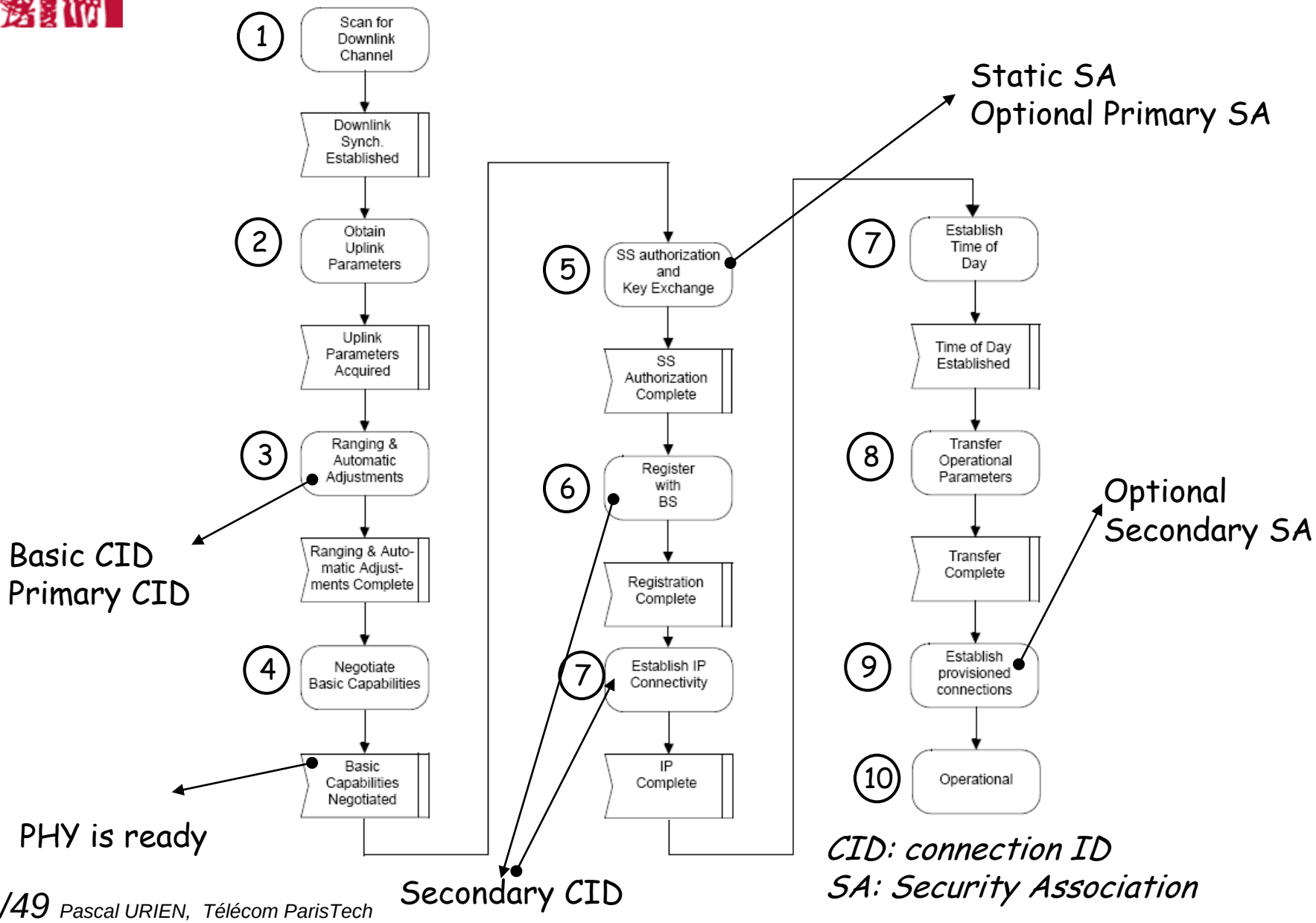
Concept de classification



Classification des PDUs applicatives dans les connexions (CID) adéquates
Transfert des CS-PDU au MAC-SAP associé au SFID
Réception des CS –PDU par le MAC-SAP

Procédure d'insertion d'une station WiMAX

Insertion d'une station 1/3



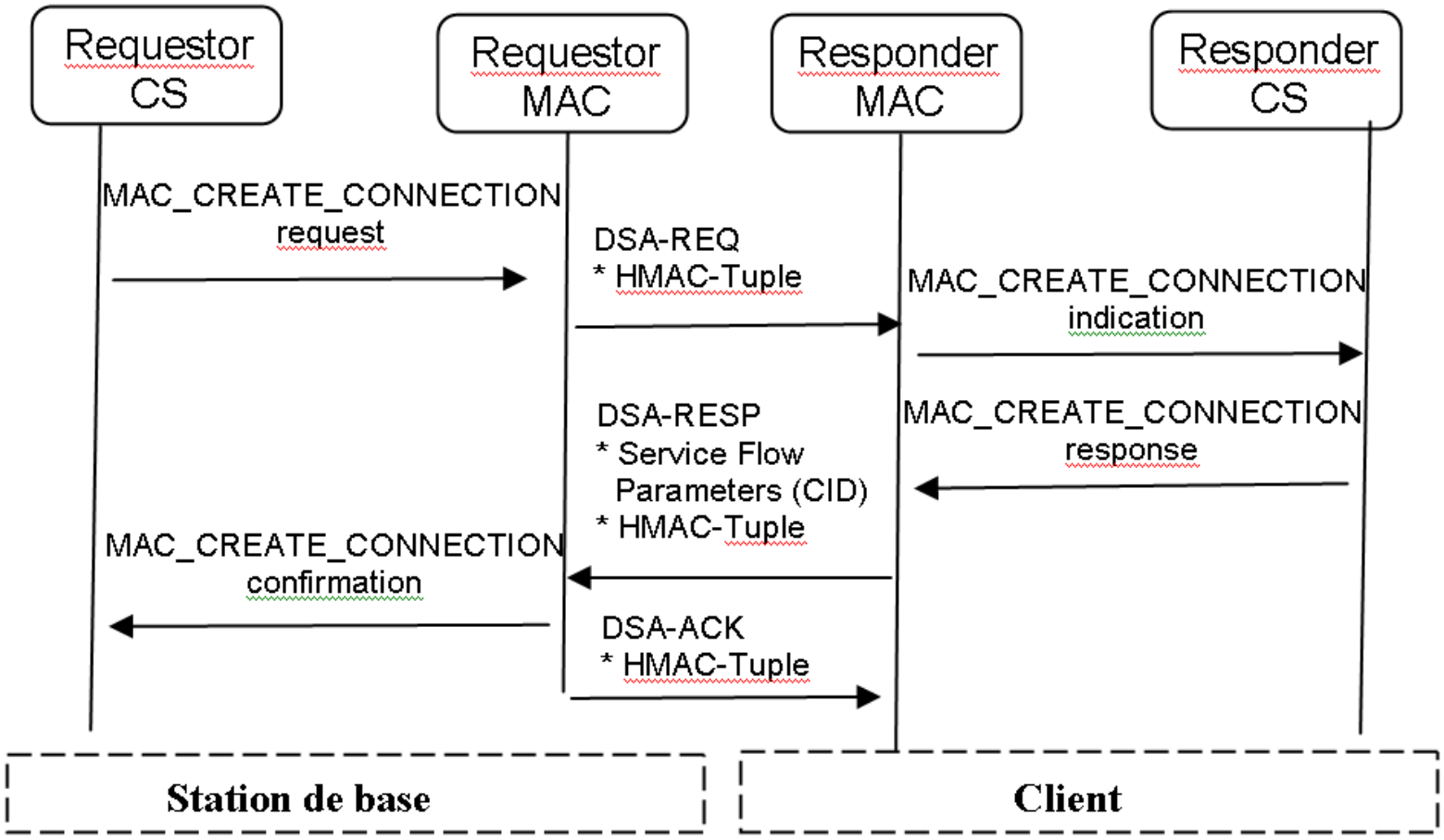
Insertion d'une station 2/3

- 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



La sécurité du WiMAX

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

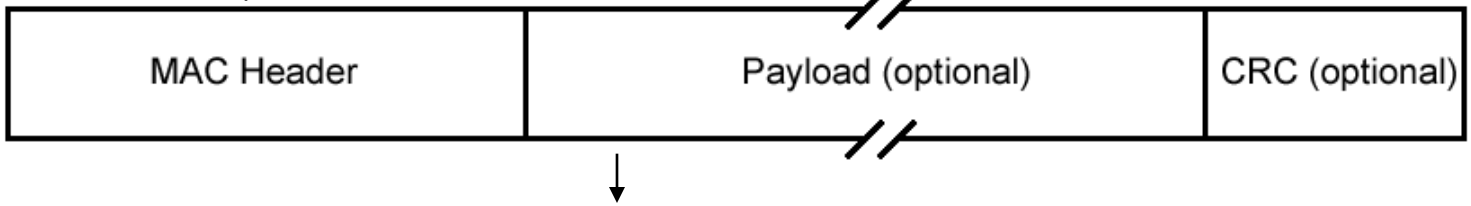
- Les fonctions de sécurité sont assurées par deux entités fonctionnelles, la première réalise le protocole PKM qui permet l'authentification d'un client et la sélection d'une suite d'algorithmes cryptographiques et de clés associées, la deuxième gère le chiffrement des trames MAC.
- Le protocole PKM 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 des clés TEK.

Transport des messages PKM 1/4

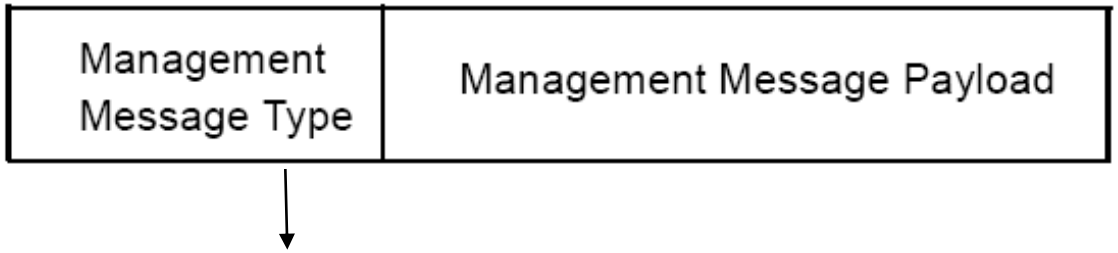
Generic MAC header format

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 Management message format



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)
}
```

Codes des messages PKM 3/4

Code	PKM message type	MAC Management message name
0-2	*reserved*	—
3	SA Add	PKM-RSP
4	Auth Request	PKM-REQ
5	Auth Reply	PKM-RSP
6	Auth Reject	PKM-RSP
7	Key Request	PKM-REQ
8	Key Reply	PKM-RSP
9	Key Reject	PKM-RSP
10	Auth Invalid	PKM-RSP
11	TEK Invalid	PKM-RSP
12	Auth Info	PKM-REQ
13	EAP Transfer	PKM-REQ/PKM-RSP
14	Pre-Auth-Request	PKM-REQ
15	Pre-Auth-Reply	PKM-RSP
16	Pre-Auth-Reject	PKM-RSP
17	PKMv2 Auth-Request	PKM-REQ
18	PKMv2 Auth-Reply	PKM-RSP
19	Key Update Command	PKM-RSP
20	~~Protected~~ Authenticated EAP	PKM-REQ/PKM-RSP
21	SA-TEK-Challenge	PKM-RSP
22	SA-TEK-Request	PKM-REQ
23	SA-TEK-Response	PKM-RSP
24~~13~~–255	~~*reserved*~~*Reserved*	—

Exemples d'attributs des messages PKM 4/4

Type	Length	Value
1 byte	*variable*	Length bytes

Type	PKM attribute
0–5	*reserved*
6	Display-String
7	AUTH-Key
8	TEK
9	Key-Lifetime
10	Key-Sequence-Number
11	HMAC-Digest
12	SAID
13	TEK-Parameters
14	*reserved*
15	CBC-IV

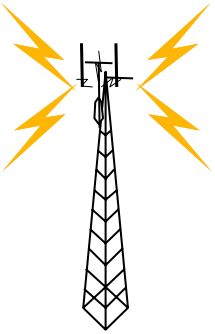
16	Error-Code
17	CA-Certificate
18	SS-Certificate
19	Security-Capabilities
20	Cryptographic-Suite
21	Cryptographic-Suite-List
22	Version
23	SA-Descriptor
24	SA-Type
25	*reserved*
26	*reserved*
27	PKM Configuration Settings
28–255	*reserved*

Type	PKM attribute
22	~~Version~~ *Reserved*
28	EAP-Master-Key-Id
29	Nonce
30	Target BSID
31	AA-Descriptor
32	AA-Type
33	SS_RANDOM
34	BS_RANDOM
35	PAK
36	PAK/AK Sequence Number
37	BS-Certificate
38	SigBS
39	MS-MAC Address
40	OMAC-Digest
41	Key Push Modes
42	Key Push Counter
43	GKEK
~~28~~41-255	reserved

Procédure d'autorisation dans IEEE 802.16-2004

SS

BS



auth_info(SS_cert)

auth_req(SS_cert, list of crypto suites, basic CID)

auth_reply(RSA(AK,SSpk), key_seq_num, key_lifetime, list of SAIDs & their properties)

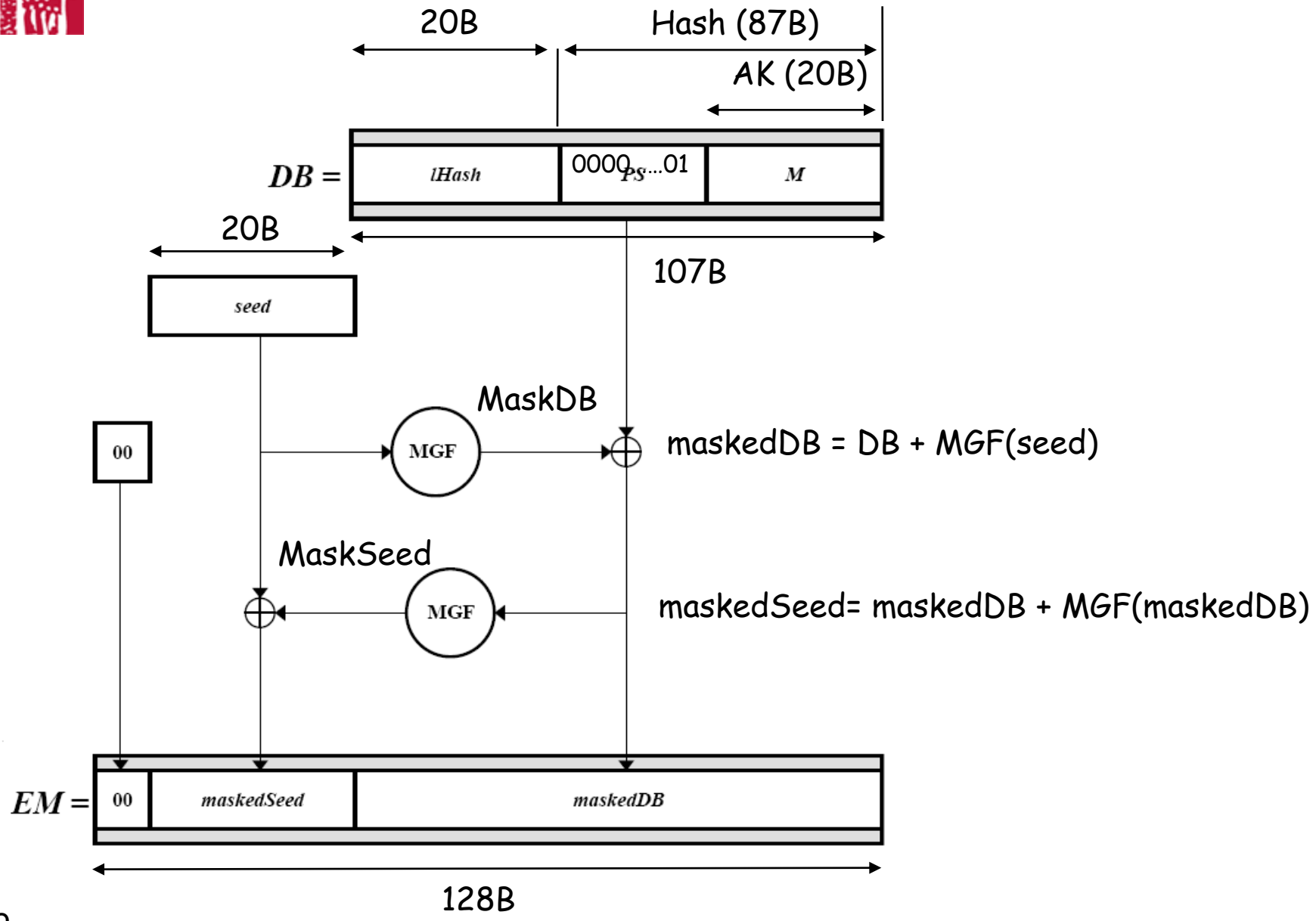
KEK
HMAC_KEY_D
HMAC_KEY_U

KEK
HMAC_KEY_D
HMAC_KEY_U

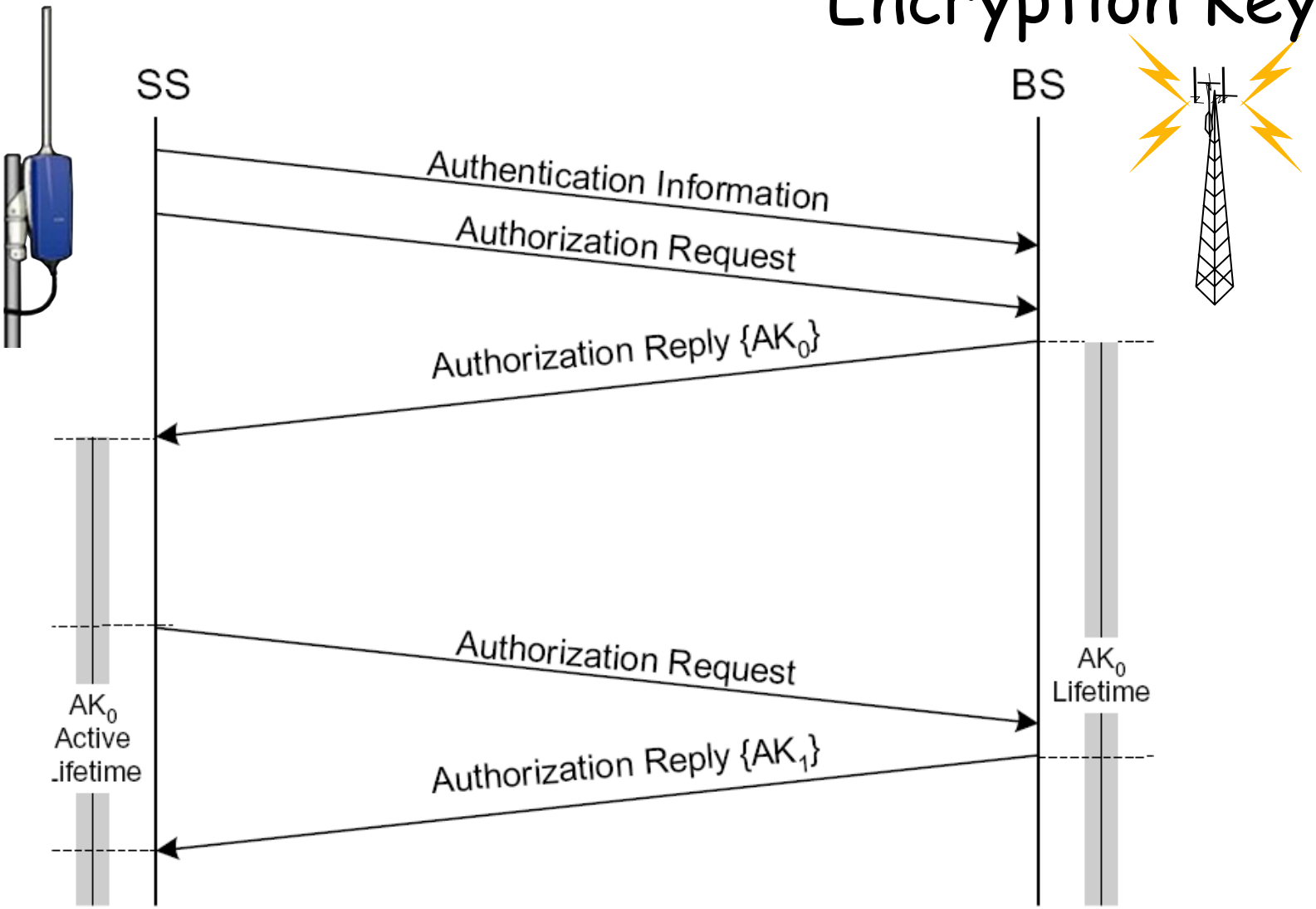
TEK_key_req(SAID)

TEK_key_reply(3DES-EDE(TEK0,KEK), 3DES-EDE(TEK1,KEK),CBC-IV, Lifetime)

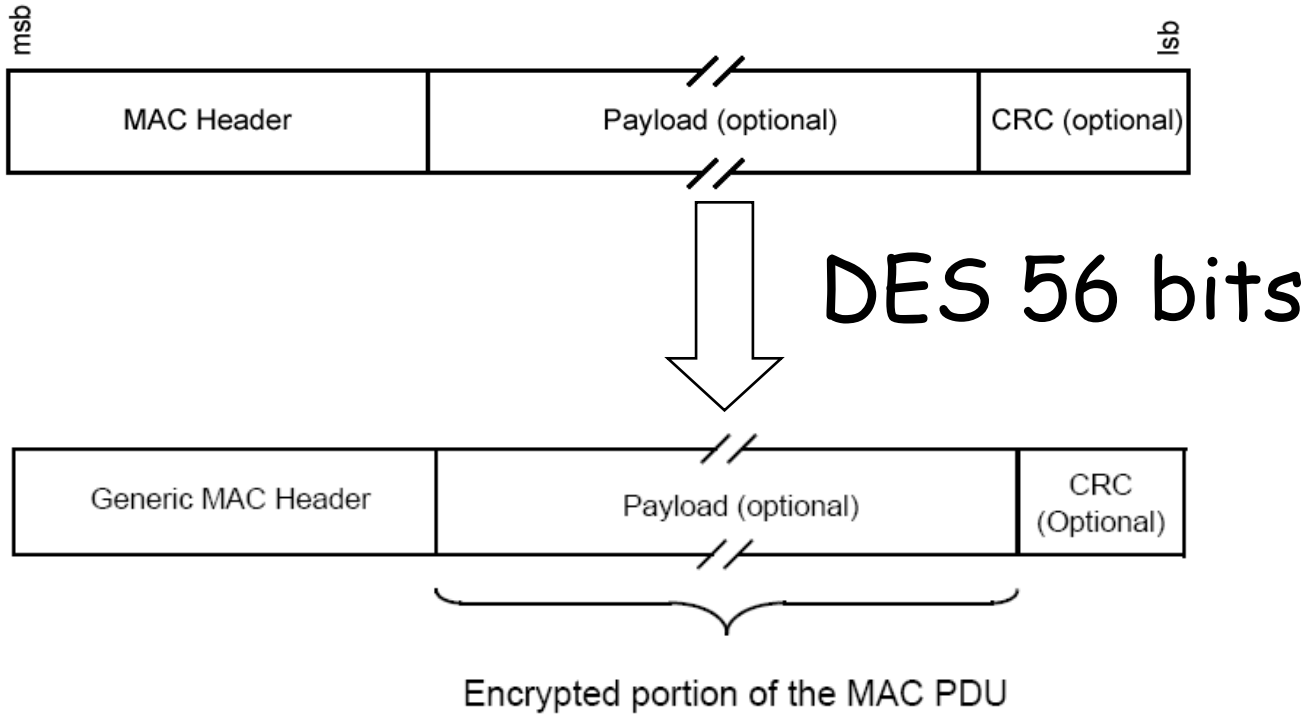
RSAES-OAEP


20B
Hash (87B)
AK (20B)
DB =
lHash
0000...01
PS
M
20B
107B
seed
MaskDB
00
MGF
maskedDB = DB + MGF(seed)
MaskSeed
MGF
maskedSeed= maskedDB + MGF(maskedDB)
EM =
00
maskedSeed
maskedDB
128B

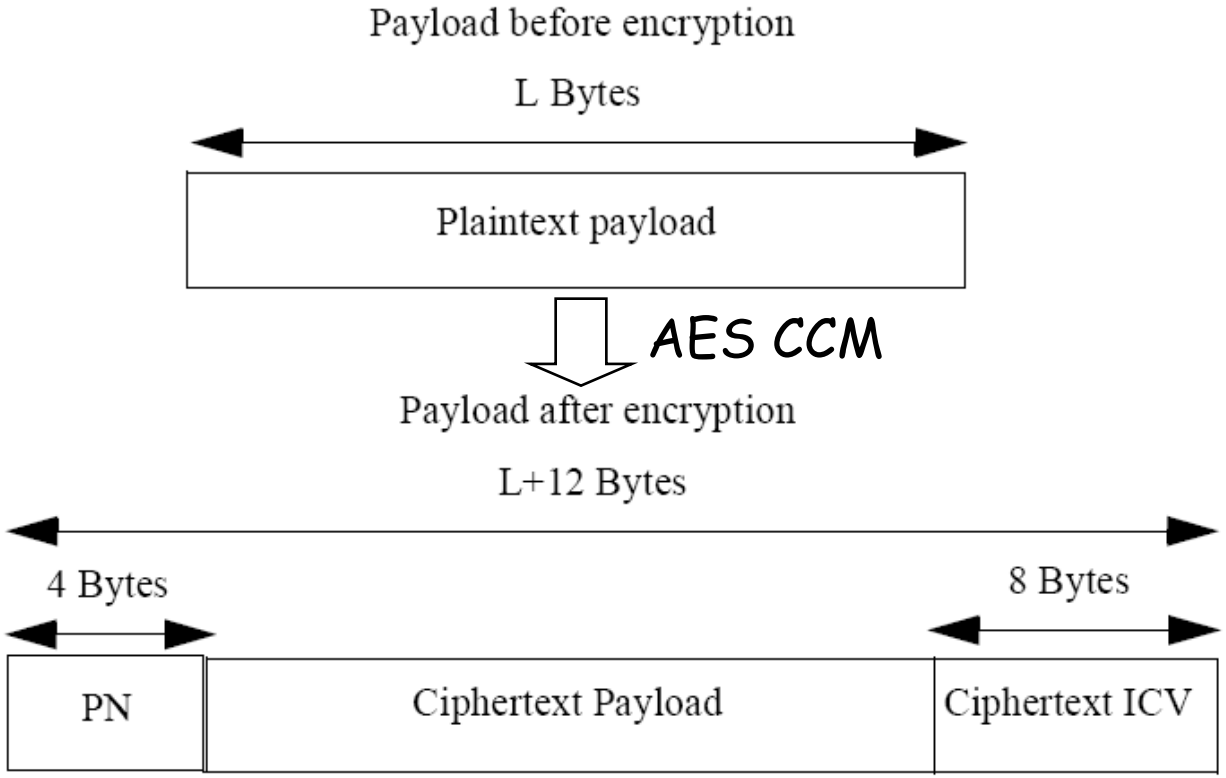
La distribution des clés TEKs (Traffic Encryption Key)



Chiffrement des données (IEEE 802.16-2001)



Chiffrement des données 802.16-2004, AES-CCM



PN: Packet Number

ICV: Integrity Check Value

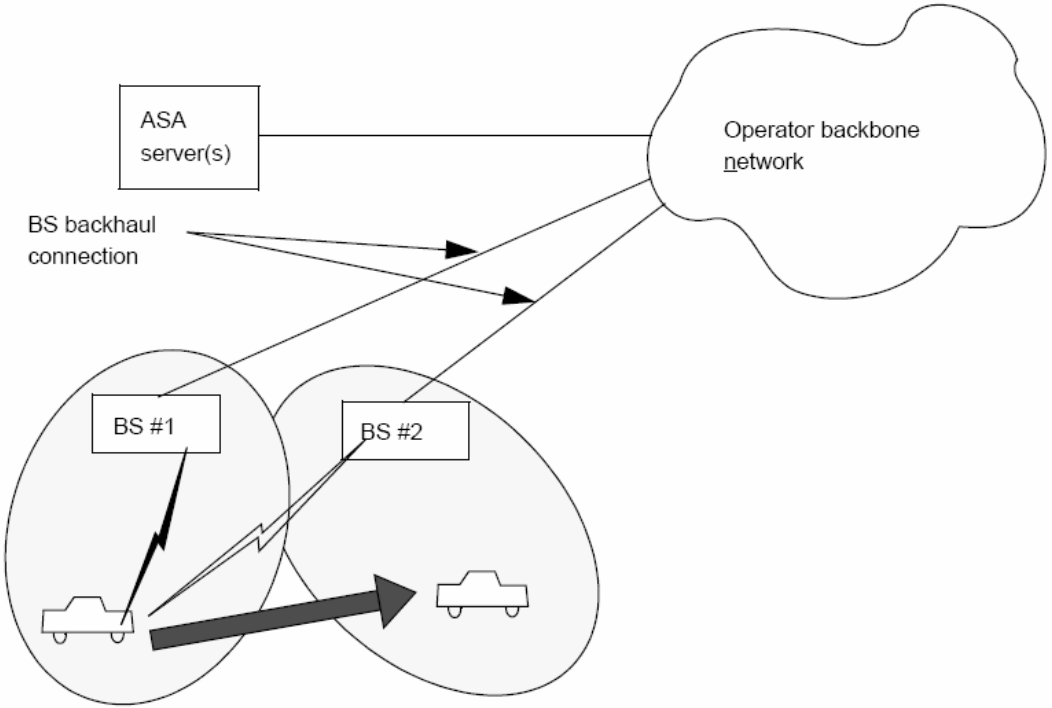
Associations de sécurité

- **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 algorithmes utilisés sont de type chaîné ;
  - le type de l'association de sécurité : primaire, statique ou dynamique

IEEE 802.16e

IEEE 802.16e

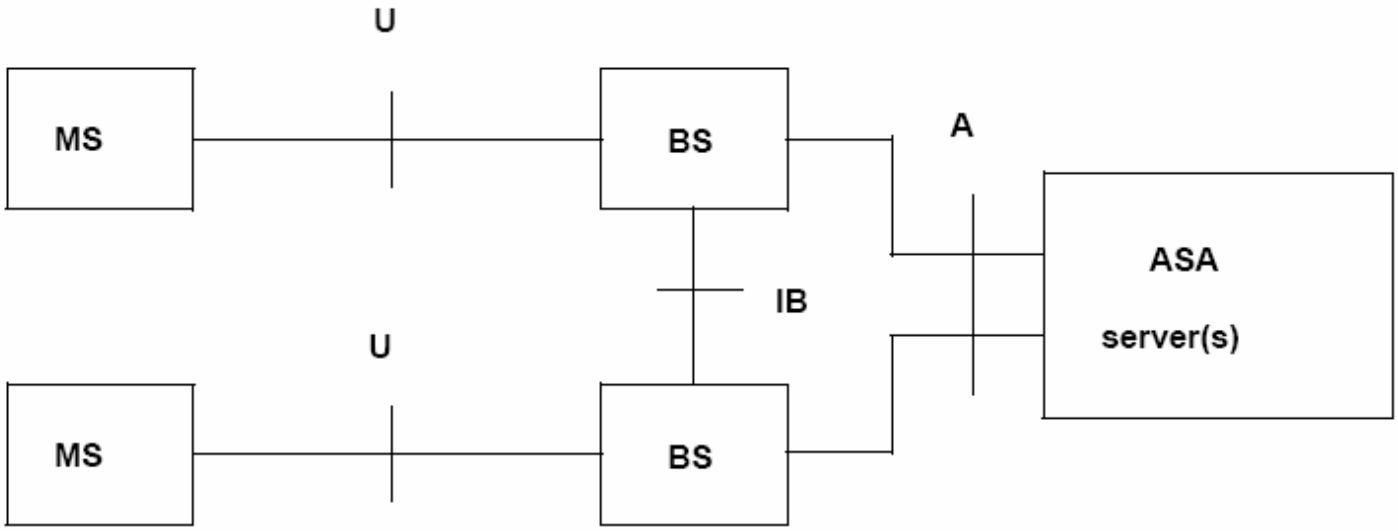
- Le standard IEEE 802.16e apporte des améliorations de sécurité à la précédente version 802.16-2004, et s'adapte à des stations clientes se déplaçant à des vitesses automobiles usuelles; il introduit des accès réseaux hauts débits destinés à des applications fixes ou mobiles. Il intègre également des 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.



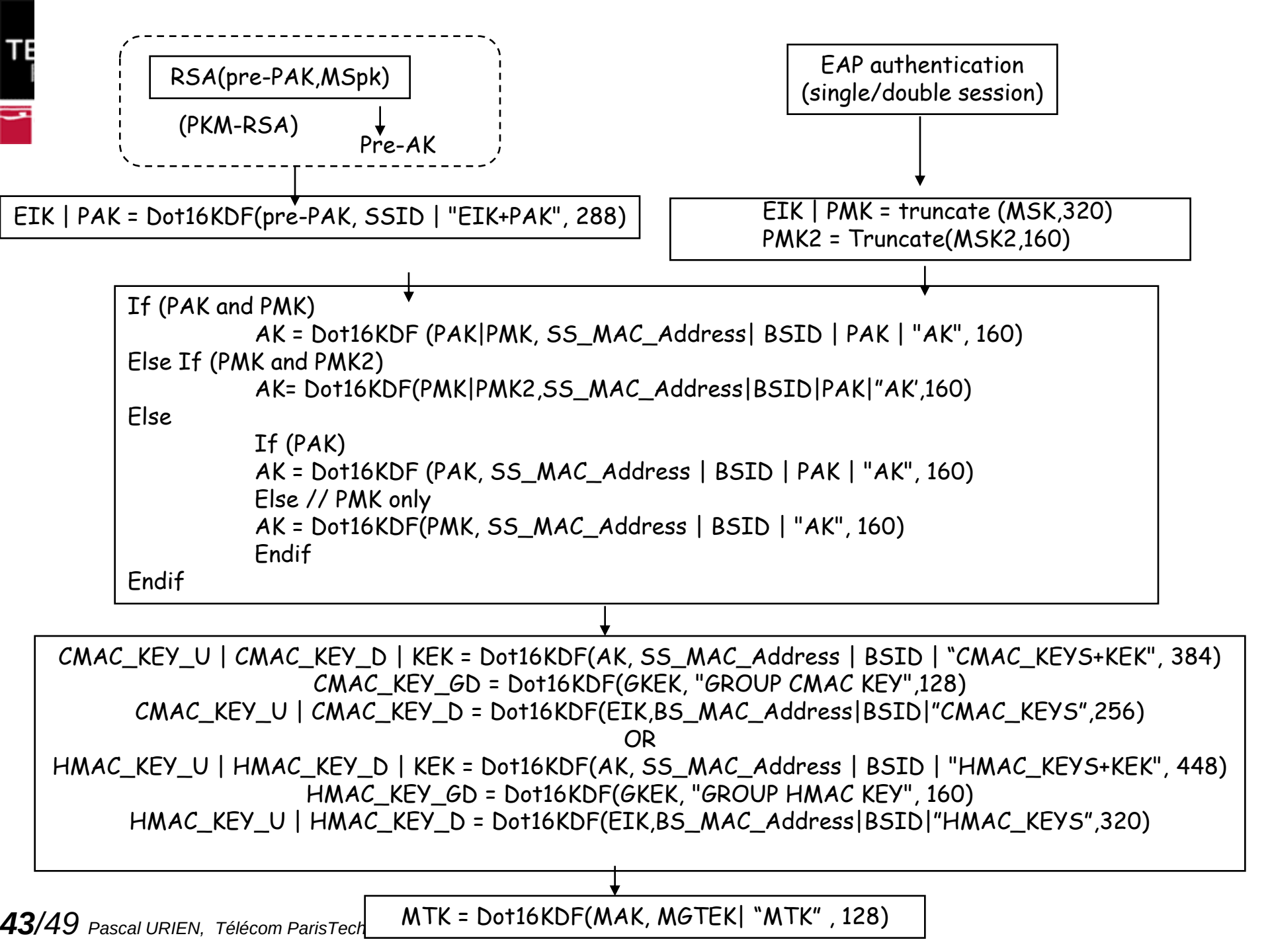
La sécurité IEEE 802.16e

- 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 mécanismes de sécurité permettent par exemple de déployer efficacement des infrastructures 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 par le standard. Cette valeur peut être utilisée pour des services de diffusion, telle que télévision à péage


RSA(pre-PAK,MSpk)
(PKM-RSA)
Pre-AK
EAP authentication
(single/double session)
EIK | PAK = Dot16KDF(pre-PAK, SSID | "EIK+PAK", 288)
EIK | PMK = truncate (MSK,320)
PMK2 = Truncate(MSK2,160)
If (PAK and PMK)
AK = Dot16KDF (PAK|PMK, SS_MAC_Address| BSID | PAK | "AK", 160)
Else If (PMK and PMK2)
AK= Dot16KDF(PMK|PMK2,SS_MAC_Address|BSID|PAK|"AK',160)
Else
If (PAK)
AK = Dot16KDF (PAK, SS_MAC_Address | BSID | PAK | "AK", 160)
Else // PMK only
AK = Dot16KDF(PMK, SS_MAC_Address | BSID | "AK", 160)
Endif
Endif
CMAC_KEY_U | CMAC_KEY_D | KEK = Dot16KDF(AK, SS_MAC_Address | BSID | "CMAC_KEYS+KEK", 384)
CMAC_KEY_GD = Dot16KDF(GKEK, "GROUP CMAC KEY",128)
CMAC_KEY_U | CMAC_KEY_D = Dot16KDF(EIK,BS_MAC_Address|BSID|"CMAC_KEYS",256)
OR
HMAC_KEY_U | HMAC_KEY_D | KEK = Dot16KDF(AK, SS_MAC_Address | BSID | "HMAC_KEYS+KEK", 448)
HMAC_KEY_GD = Dot16KDF(GKEK, "GROUP HMAC KEY", 160)
HMAC_KEY_U | HMAC_KEY_D = Dot16KDF(EIK,BS_MAC_Address|BSID|"HMAC_KEYS",320)
MTK = Dot16KDF(MAK, MGTEK| "MTK" , 128)

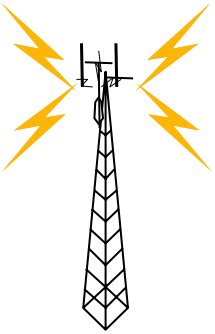
Dot16KDF (*Key Derivation Function*)

```
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

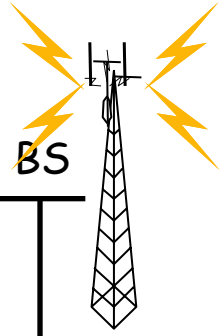
PKMv2 RSA-Reply
(*MS_Random, BS_Random, Encrypted pre-PAK, Key-Lifetime, Key-Sequence-Number, BS_Certificate, SigBS)*

Signature de la station de base

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

PKMv2 – EAP (Simple)

MS



BS

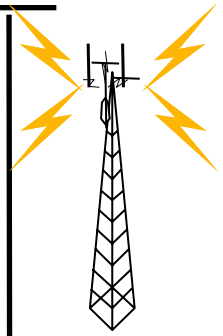
PKMv2 Authenticated-EAP-Transfer
(EAP_Payload, C/HMAC Digest{EIK})
ou PKMv2 EAP-Transfer
(EAP_Payload)

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}*)

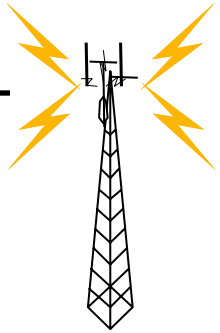
PKMv2 Authenticated-EAP-Transfer
(*EAP_Payload, Key-Sequence-Number, C/HMAC Digest{AK}*)

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

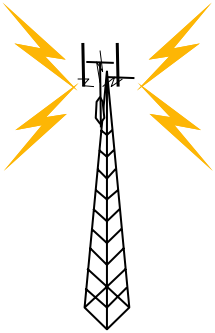
PKMv2 SA-TEK-Request
(MS_Random, BS_Random, Key-Sequence-Number, AKID, Security-Capabilities, Security-Negociation-Parameters, PKMv2-Configuration-Settings, HMAC/CMAC-Digest)

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)