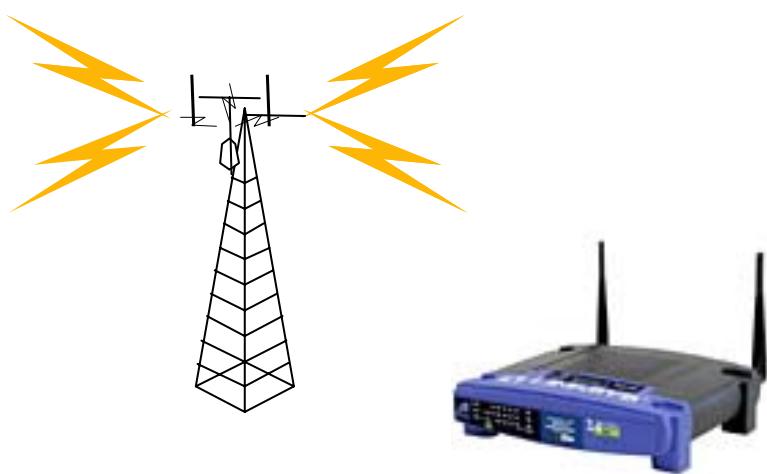




Sécurité des réseaux sans fil



Pascal Urien
Cours Master M2,
Octobre 2006



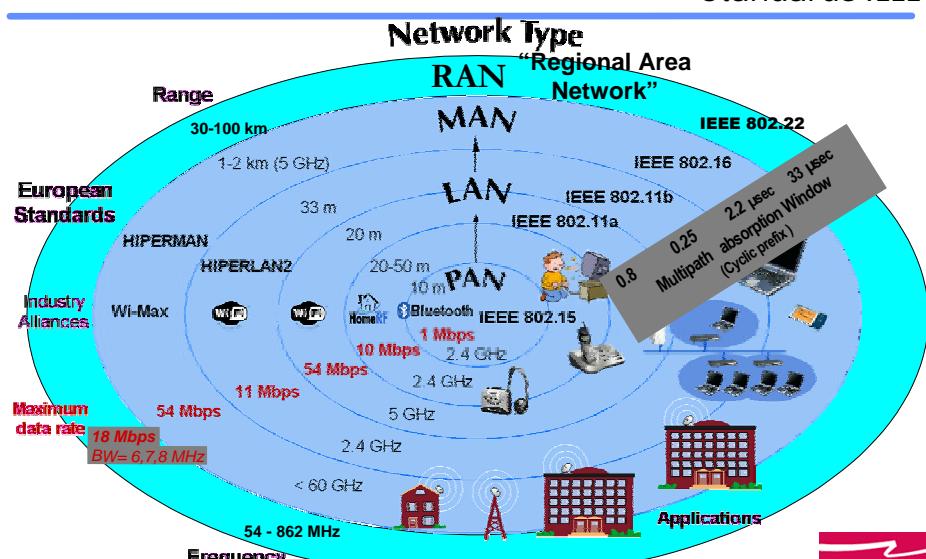
Sécurité des Réseaux sans Fil

Pascal Urien

1/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Standards IEEE



2/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



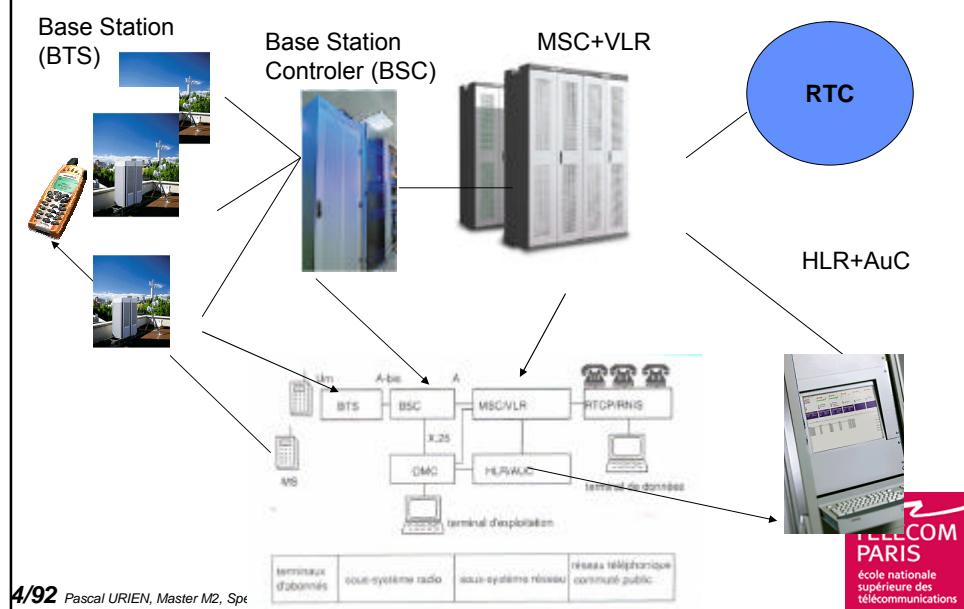
La sécurité du GSM

Provisionning + Simple Authentification

3/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Architecture



Principes

✚ 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, 2¹⁹ 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)

5/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



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

6/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



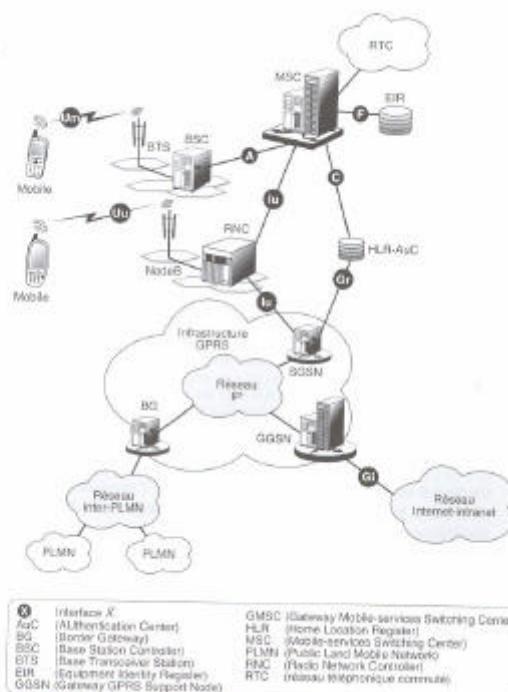
Sécurité de l'UMTS

Provisionning + Authentification Mutuelle

7/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Figure 6.7
Architecture générale de l'UMTS



UMTS

8/92 Pascal I

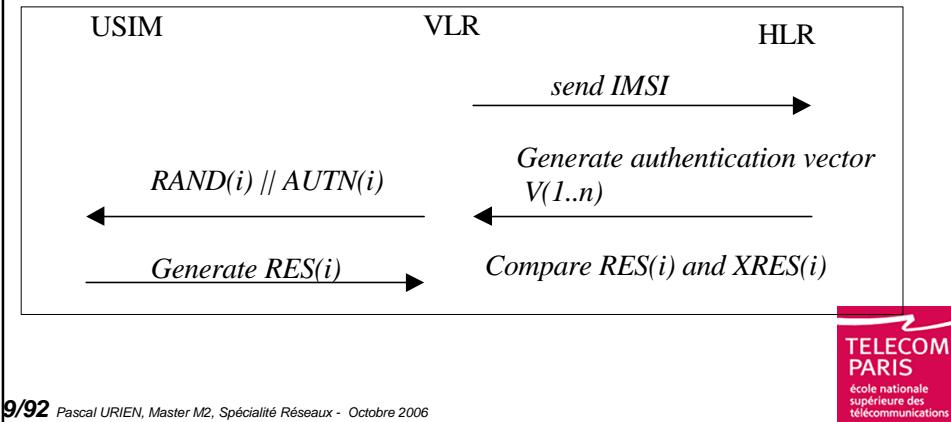
X	Interface X (Authentification Center)	GMSC (Gateway Mobile-services Switching Center)
S	Interface S	HLR (Home Location Register)
BSC	Base Station Controller	MSC (Mobile-services Switching Center)
BTS	Base Transceiver Station	PLMN (Public Land Mobile Network)
EIR	Equipment Identity Register	RNC (Radio Network Controller)
GGSN	Gateway GPRS Support Node	RTC (réseau téléphonique commun)



Principes

■ Mutuelle Authentification

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

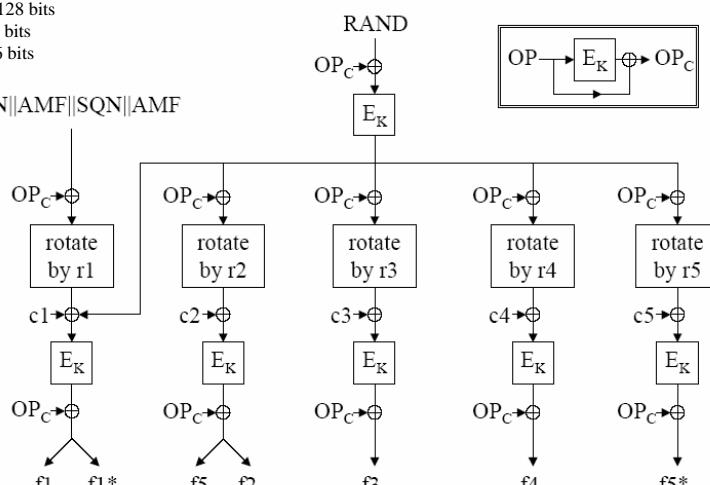


9/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

MILENAGE

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

SQN||AMF||SQN||AMF



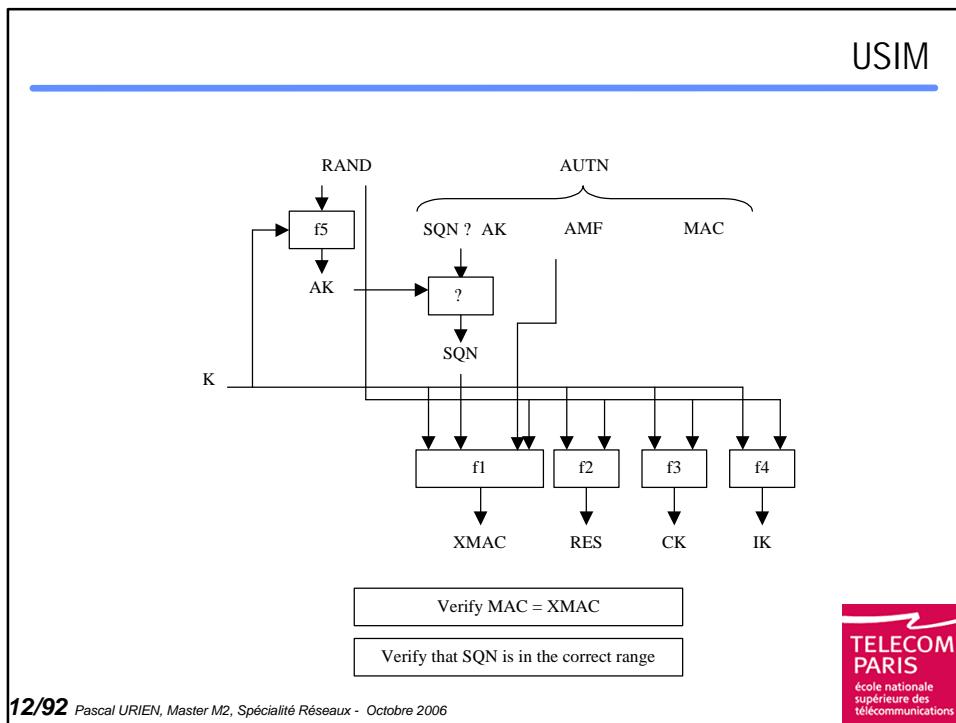
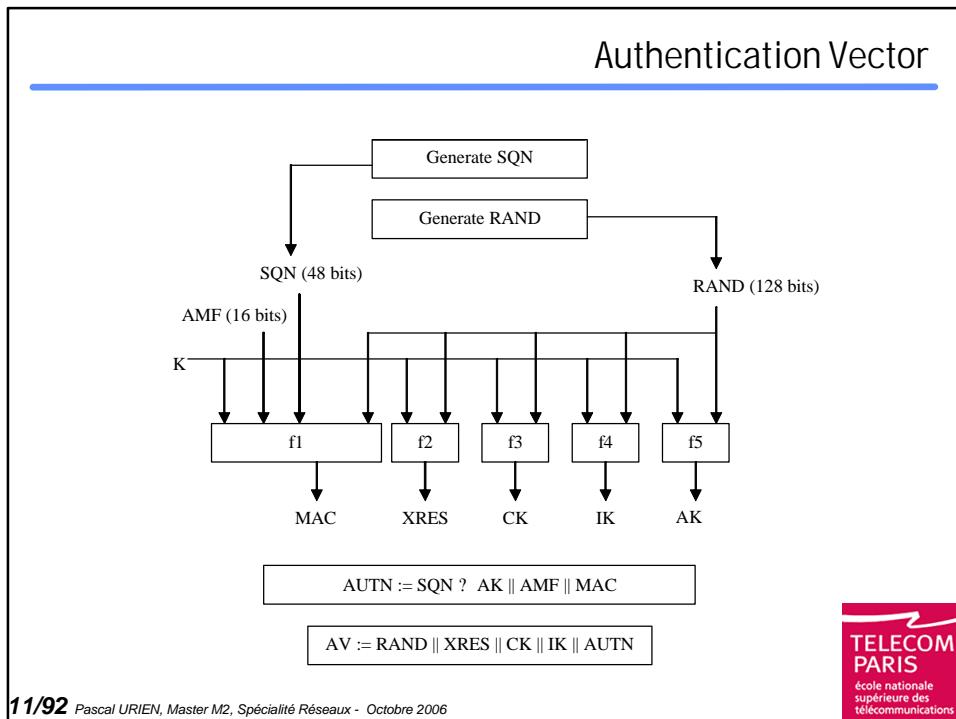
ri= 64,0,32,64,96 (rotation gauche)

ci= 0,1,2,4,8

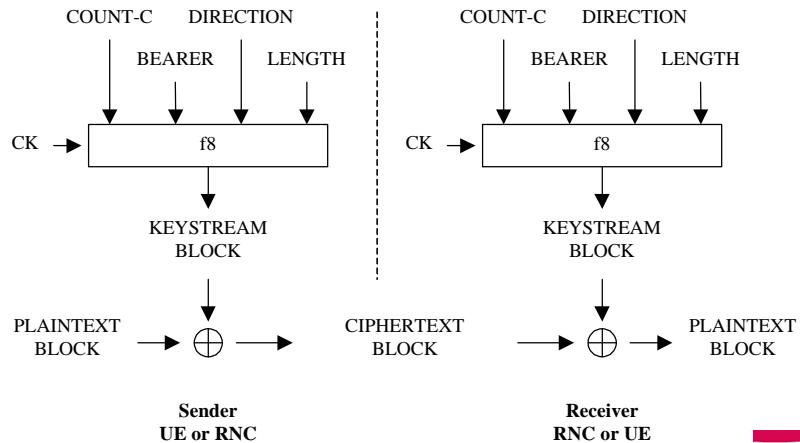
OP: clé OPérateur (128 bits) Ek: AES + clé 128bits

TELECOM PARIS
école nationale supérieure des télécommunications

10/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



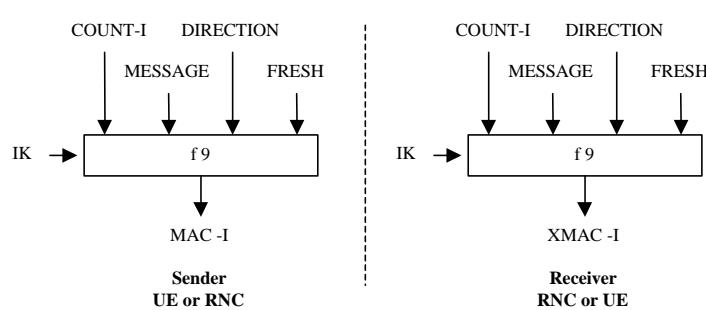
Chiffrement



13/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Intégrité



FRESH, valeur aléatoire

14/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Diameter Based Protocol

RFC 3588

15/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Topology

Client (NAS...)

Agents Diameter

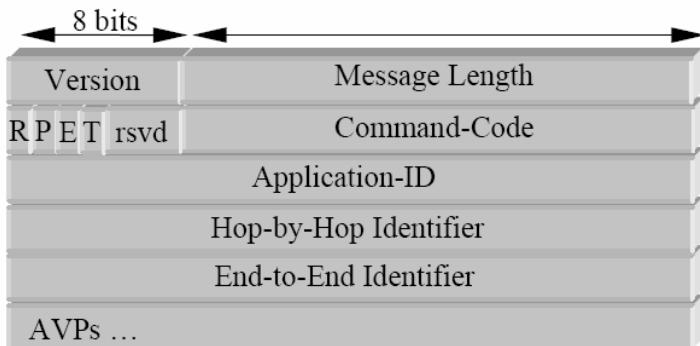
- Agent-relay, routage passif des messages, modification des informations de routage
- Agent-proxy, modification du contenu des messages, autre que des information de routages
- Agent de re-direction.
- Agent de translation (par exemple RADIUS-DIAMETER)

Home Diameter Server

16/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Format de l'en tête



17/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



En-Tête

- Version (un octet) doit être mise à 1. Il indique le numéro de version de Diameter.
- Message Length (3 octets) indique la longueur totale du message Diameter, en-tête incluse.
- Command flags (un octet) les 4 premiers bits sont R, P, T et E, les autres sont réservés pour un usage futur.
 - Si le bit 'Resquest' est mis à 1, le message est une requête, sinon le message est une réponse.
 - Si le bit 'Proxiable' est mis à 1, le message peut être 'relayé' ou redirigé sinon le message doit être traité localement.
 - Si le bit 'Error' est mis à 1, le message contient une erreur de protocole.
 - T, Potentially re-transmitted message, mis à un en cas de rétransmission
- Command-Code (3 octets), identifiant de la commande
- Application-ID, (4 octets) identifiant de l'application
- Hop-by-Hop, 4 octets, étiquette du message, modifié à chaque traversé d'un agent diamètre
- End-to-End Identifier, 4 octets étiquette du message de bout en bout.
- AVPs. Attribut Value Pair

18/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



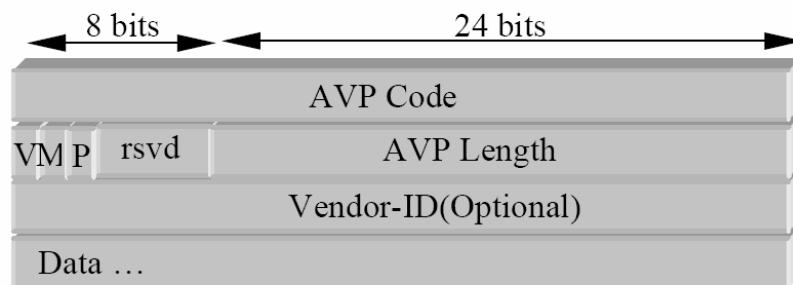
Exemple de commandes

Abort-Session-Request	ASR 274
Abort-Session-Answer	ASA 274
Accounting-Request	ACR 271
Accounting-Answer	ACA 271
Capabilities-Exchange-Request	CER 257
Capabilities-Exchange- Answer	CEA 257
Device-Watchdog-Request	DWR 280
Device-Watchdog-Answer	DWA 280
Disconnect-Peer-Request	DPR 282
Disconnect-Peer-Answer	DPA 282
Re-Auth-Request	RAR 258
Re-Auth-Answer	RAA 258
Session-Termination-Request	STR 275
Session-Termination-Answer	STR 275

19/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Format d'un AVP



20/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



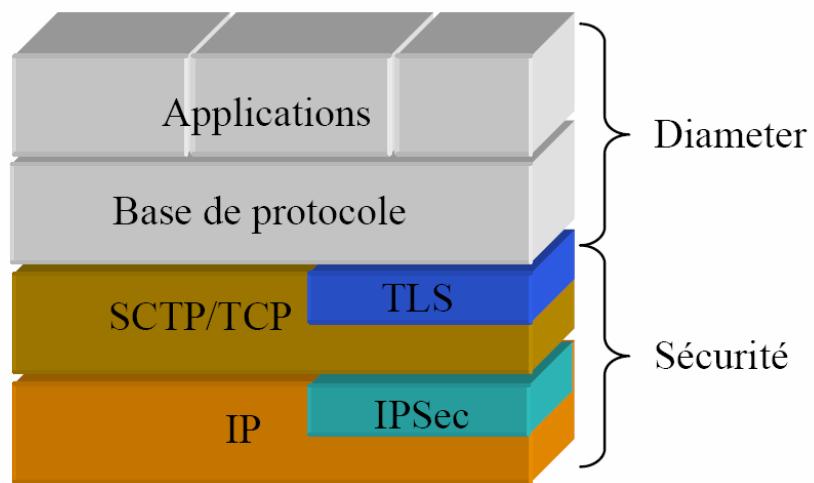
Structure d'un AVP

- ✚ AVP Code (4 octets)
 - Identifie l'AVP de manière unique. Les 256 premiers numéros sont réservés pour la compatibilité avec RADIUS. Les suivants sont utilisés par le protocole de base et ses extensions (numéros devant être alloués par l'IANA).
- ✚ AVP Length (3 octets) indique la longueur de cet AVP
- ✚ AVP Flags (un octet) indiquent à l'agent Diameter la manière de traitement de l'AVP.
 - Le bit 'M' indique si le support de cet AVP est obligatoire.
 - Le bit 'V', nommé Vendor-Specific bit, indique si le champ optionnel Vendor-ID est présent.
 - Le bit 'P' implique un chiffrement afin d'assurer la sécurité end-to-end.
- ✚ Vendor-ID (4octets) identifie le constructeur à l'origine de cet AVP propriétaire. La présence de ce champ est précisée par un bit 'V' du champ Flags.
- ✚ Data (longueur variable)



21/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

Transport et sécurité



22/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

supérieure des
télécommunications

SCTP et TCP

- ⊕ Diameter s'appuie sur les protocole SCTP (*Simple Control Transmission Protocol*) ou TCP.
- ⊕ Les caractéristiques du protocole SCTP sont :
 - **transport orienté connexion.**
 - **full duplex**
 - **transmission fiable des données dans l'ordre, sans perte et sans duplication.**
 - **un protocole de recouvrement de perte, basé sur des retransmissions et des horloges (timers.)**
 - **effectue du contrôle de flux grâce à un système de fenêtrage.**
 - **Le port 1812 avait été choisi pour SCTP**
 - **SCTP est orienté message alors que TCP est orienté octet.**

23/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Application Identifier

- ⊕ **Diameter Common Messages 0**
 - Application de base
- ⊕ **NASREQ 1 [NASREQ]**
 - Services AAA pour les NAS
- ⊕ **Mobile-IP 2 [DIAMMIP]**
 - Service AAA pour Mobile IPv4
- ⊕ **Diameter Base Accounting 3**
- ⊕ **Relay 0xffffffff**
- ⊕ **Diameter Credit-Control Application**
- ⊕ **Diameter Session Initiation Protocol (SIP) Application**
- ⊕ **Diameter Extensible Authentication Protocol (EAP) Application**
 - Diameter-EAP-Request DER 268
 - Diameter-EAP-Answer DEA 268

24/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Sécurité Bluetooth

25/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Standards

Specification of the Bluetooth System

Specification Volume 1

Wireless connections made easy

Specification of the Bluetooth System

Specification Volume 2

Wireless connections made easy

Core

Profiles



Bluetooth™

Version 1.1
February 22 2001

Bluetooth™

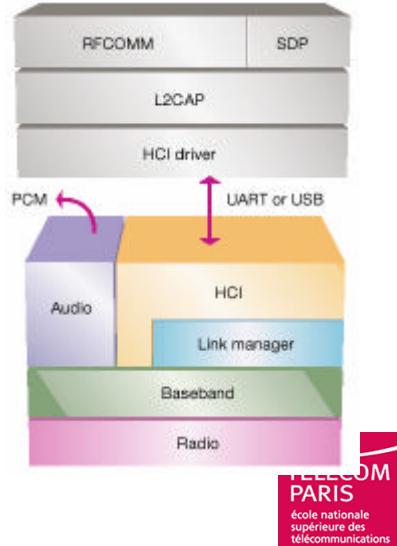
Version 1.1
February 22 2001

26/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Aperçu de Bluetooth 1/3

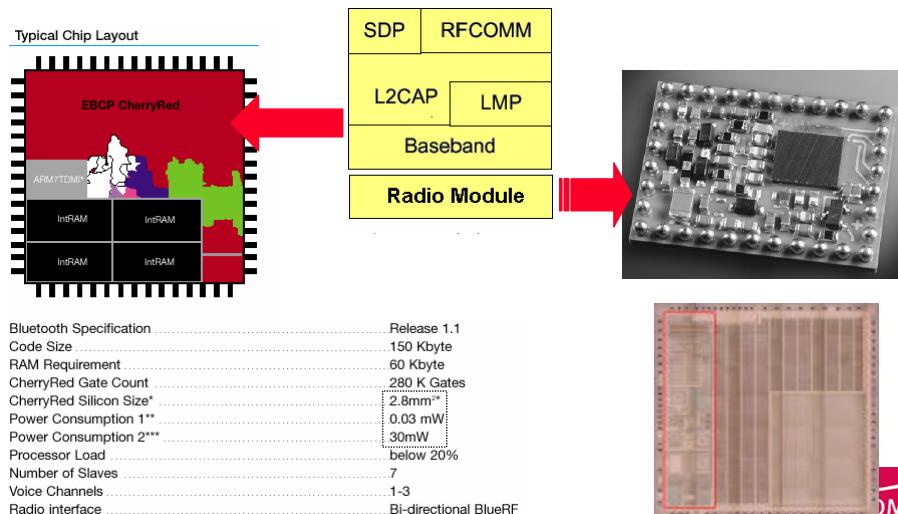
- Réseau Maître-Esclaves.
- Remplacement des liaisons filaires par des liens radio (2,4 Ghz).
 - Adaptation au bus hôte (PCMCIA, USB...) via le protocole HCI (*Host Controller Interface*)
- Définition de services et profiles
 - Audio
 - Port Série (RFCOMM)
 - ...



27/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

TELECOM PARIS
école nationale supérieure des télécommunications

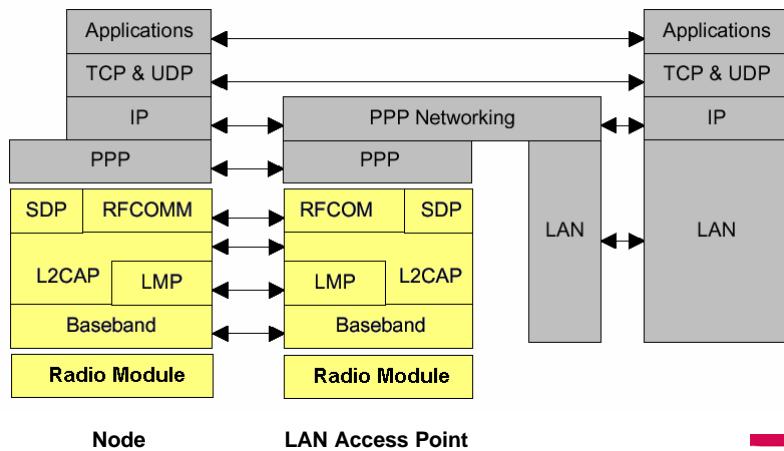
Intégration de Bluetooth 2/3



28/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

TELECOM PARIS
école nationale supérieure des télécommunications

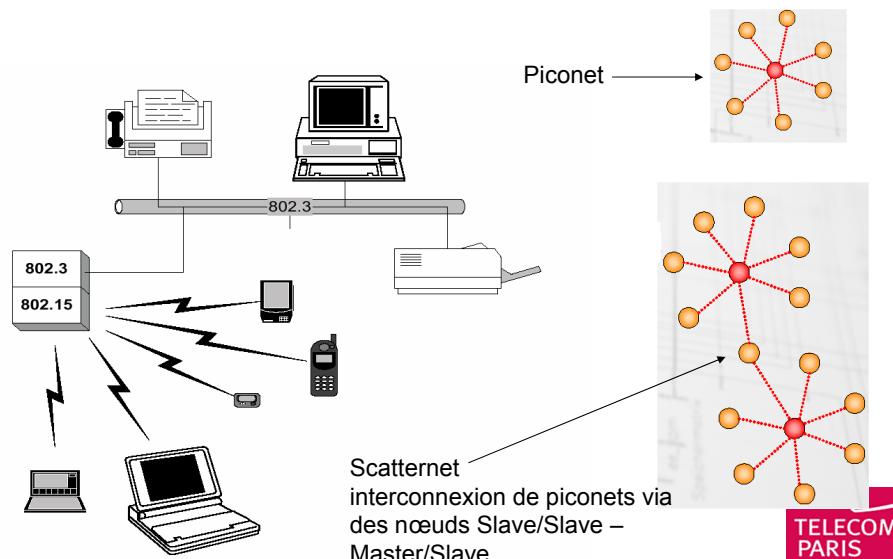
Le profile LAN de BlueTooth 3/3



29/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Wireless Personal Area Network WPAN



30/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Caractéristiques

- Portée # 10 m
- Modèle Maître-Esclave
- Au plus 7 noeuds esclaves actifs
- Un esclave peut être inactif (*parked*), jusqu'à 255 noeuds.
- Utilise la bande 2,4 Ghz, qui est la même que celle du Wi-Fi (802.11b), soit 79 canaux de 1 Mhz aux Etats Unis et 23 canaux en France.
- 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)

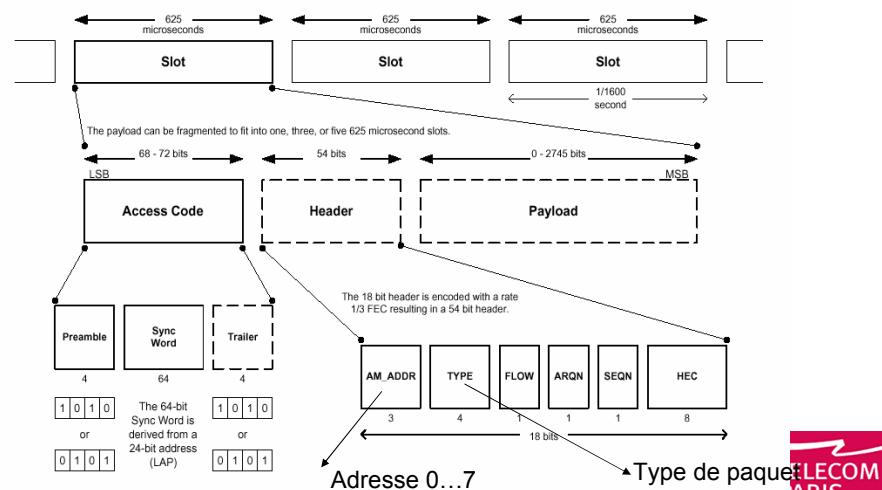
Operating frequency bands

Geography	Regulatory range (GHz)	RF channels
United States, Europe, and most other countries	2.400–2.4835	$f = 2402 + k \text{ MHz}, k = 0, \dots, 78$
France	2.4465–2.4835	$f = 2454 + k \text{ MHz}, k = 0, \dots, 22$

31/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

télécommunications

Format des paquets BlueTooth



32/

ÉCOLE NATIONALE
SUPÉRIEURE DES
TELECOMMUNICATIONS
PARIS

Notion de Canaux Logiques

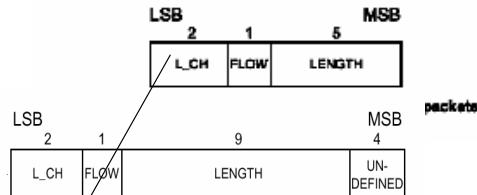


Figure 23—Payload header format for multislot packets

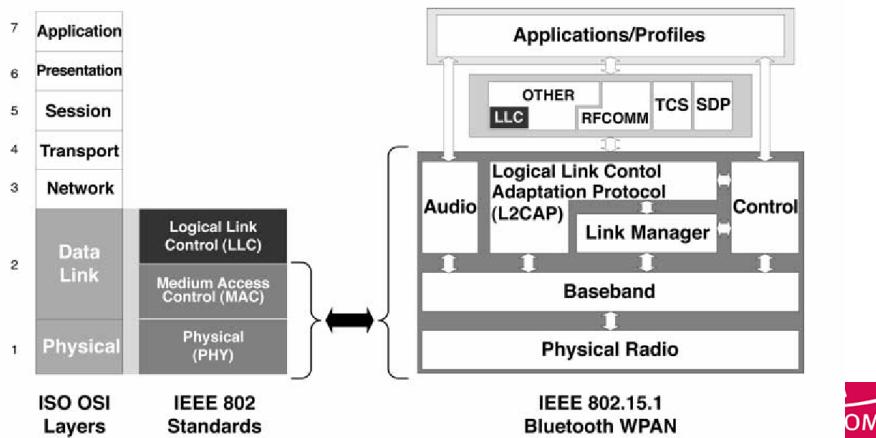
Table 18—Logical channel L_CH field contents

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

33/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Relations avec le modèle IEEE 802

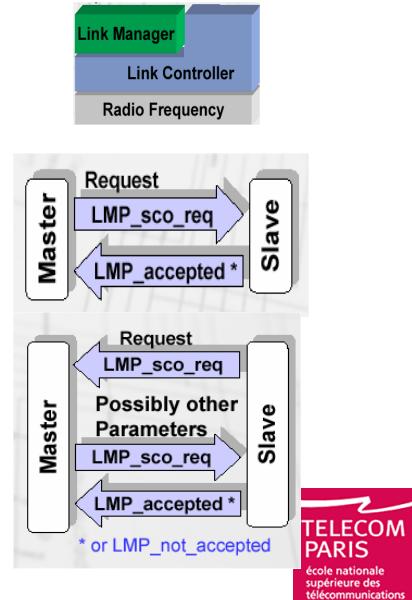


34/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



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 noeuds esclaves
 - Négociation de la qualité de ligne (QoS)
 - Sécurité, authentification et chiffrement.



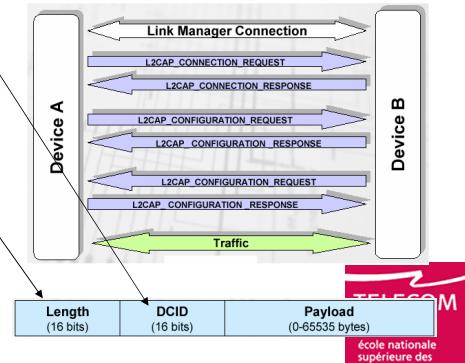
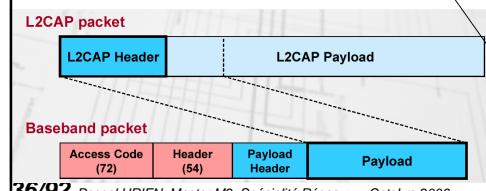
35/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

TELECOM PARIS
école nationale supérieure des télécommunications

Composants BlueTooth 2/3

■ L2CAP, Logical Link Control and adaptation Protocol

- Multiplexage de canaux logiques (associées à différentes applications).
- Segmentation / Re-assemblage.



36/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

TELECOM
école nationale supérieure des télécommunications

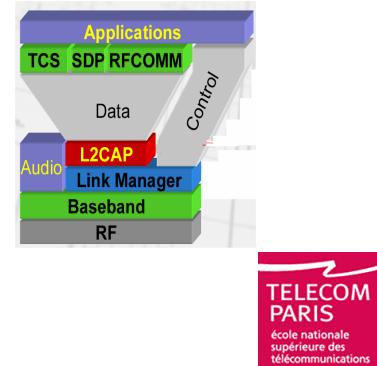
Composants BlueTooth 3/3

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

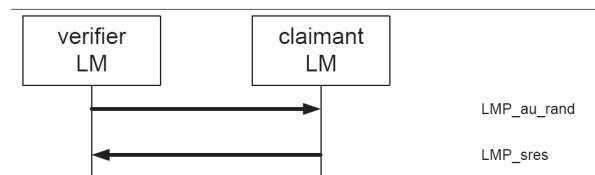


37/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

TELECOM PARIS
école nationale supérieure des télécommunications

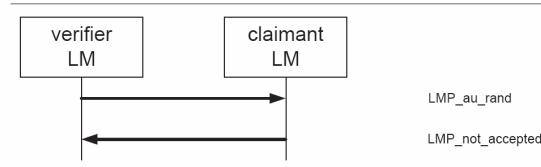
Authentification

Une clé de ligne (Link Key) est disponible



Sequence 1: Authentication. Claimant has link key.

Echec



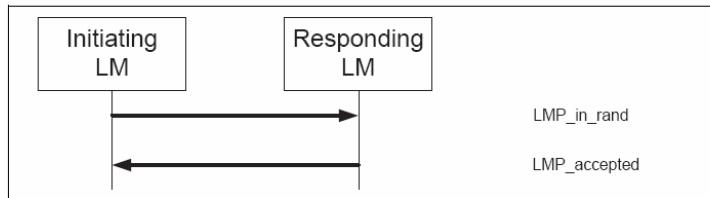
Sequence 2: Authentication fails. Claimant has no link key.

38/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

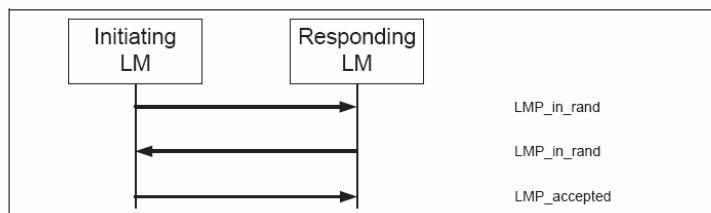
TELECOM PARIS
école nationale supérieure des télécommunications

Pairing

Creation d'une clé Kinit



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



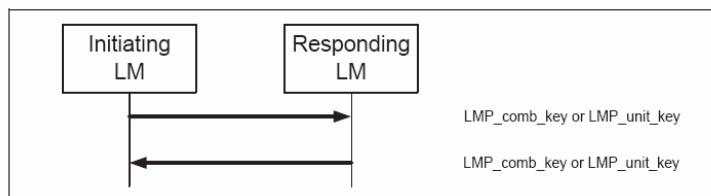
Sequence 4: Responder has a fixed PIN and initiator has a variable PIN.

39/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



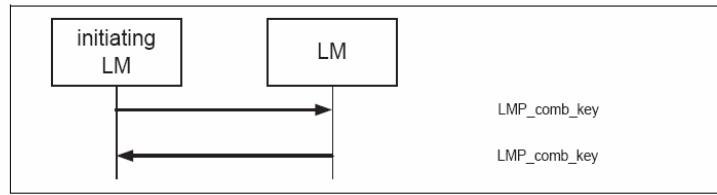
Pairing

Création d'une clé de ligne



Sequence 7: Creation of the link key.

Modification d'une clé de ligne



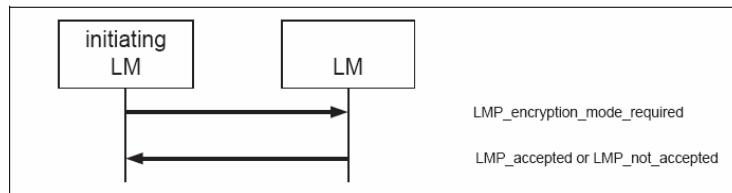
Sequence 8: Successful change of the link key.

40/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



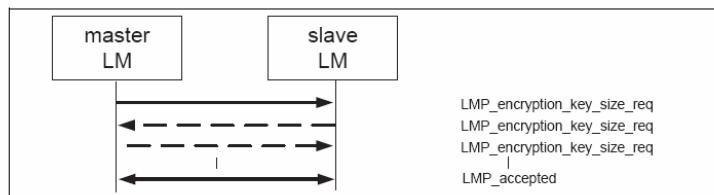
Chiffrement

■ Demande de chiffrement



Sequence 12: Negotiation for encryption mode.

■ Négociation d'une clé de chiffrement



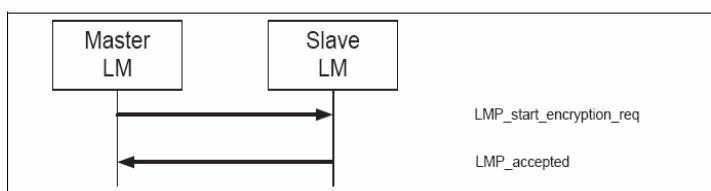
Sequence 13: Encryption key size negotiation successful.

41/92 Pascal Urien, master M2, Spécialité Réseaux - Octobre 2006



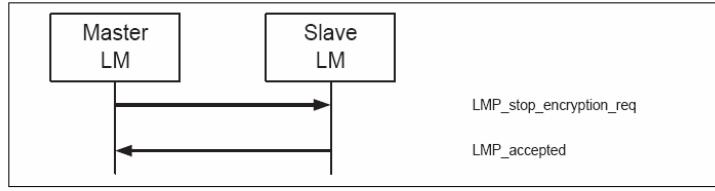
Chiffrement

■ Start Encryption



Sequence 15: Start of encryption.

■ Stop Encryption



42/92 Pascal Urien, master M2, Spécialité Réseaux - Octobre 2006



SSL - TLS

43/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Historique

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

44/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



SSL : Services

⊕ Authentification

- Serveur (obligatoire), client (optionnel)
- Utilisation de certificat X509 V3
- A l'établissement de la session.

⊕ Confidentialité

- Algorithme de chiffrement symétrique négocié, clé générée à l'établissement de la session.

⊕ Intégrité

- Fonction de hachage avec clé secrète : HMAC(clé secrète, Message)

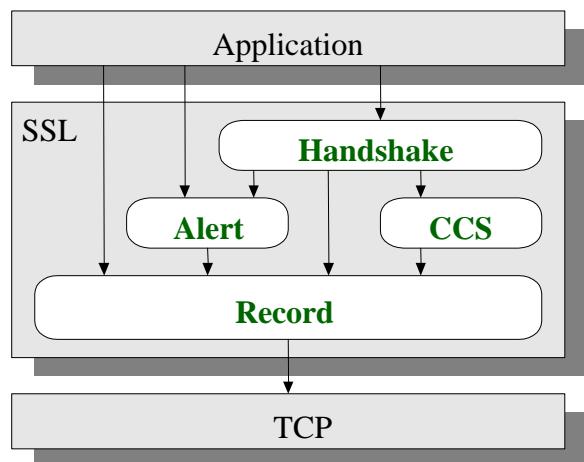
⊕ Non Rejet

- Numéro de séquence

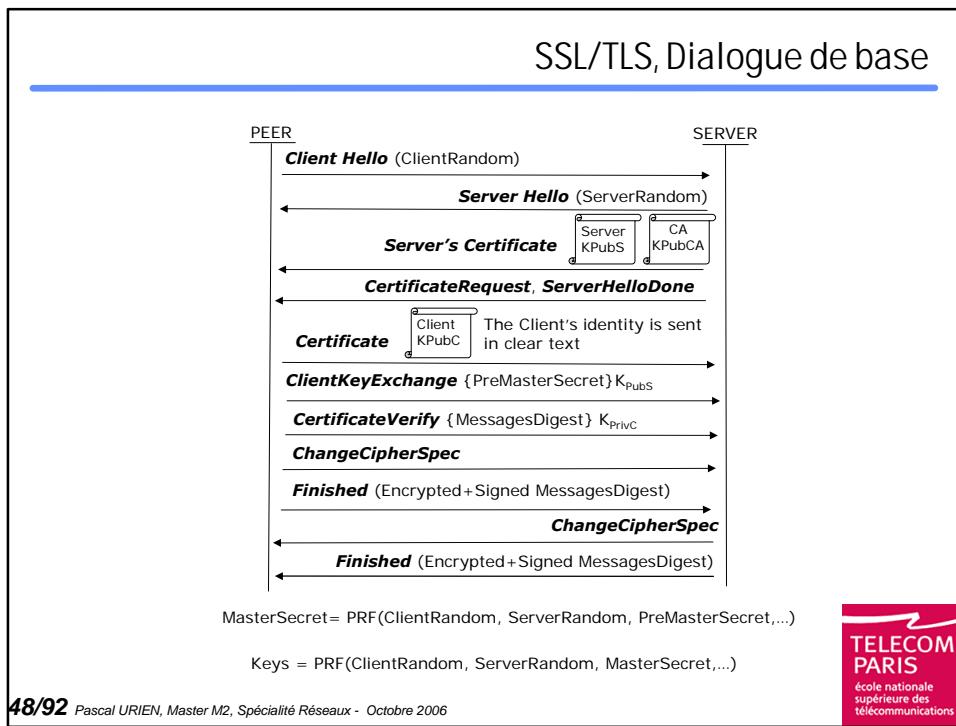
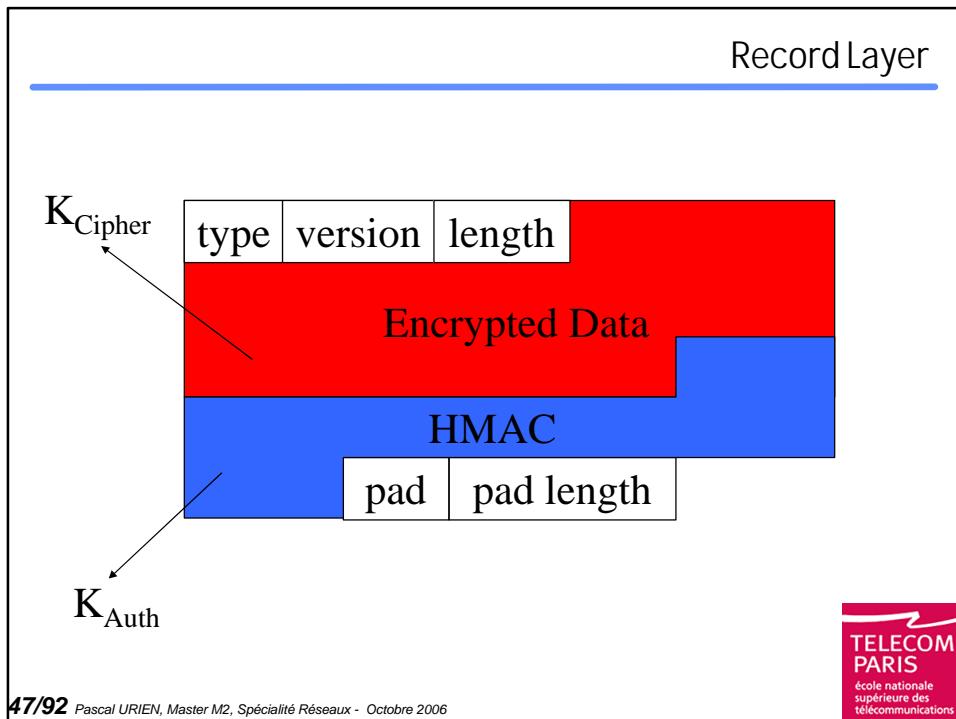


45/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

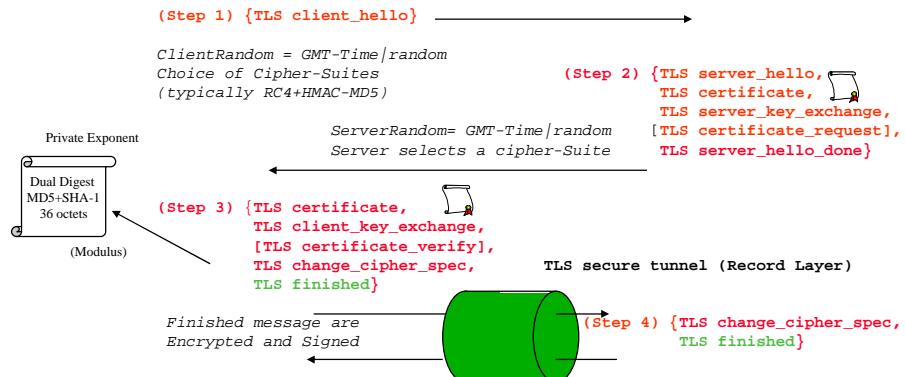
SSL/TLS : Protocoles



46/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



SSL - Négociation



49/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



IPSEC

50/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Définitions

- ✚ Authentification, la preuve que les données reçues sont identiques aux données émises, et que l'émetteur supposé est en fait l'émetteur réel.
- ✚ Intégrité, l'absence d'erreurs non détectées.
- ✚ La Confidentialité, seul le destinataire désigné de l'information est à même de comprendre cette information.
- ✚ Le chiffrement, le mécanisme utilisé pour assurer la confidentialité.
- ✚ La non répudiation (non rejet), le fait que le destinataire soit capable de prouver l'origine de l'information, même si son émetteur en nie en être la source.
- ✚ Security Association, l'ensemble des informations relatifs à une connexion ou à un ensemble de connexions.
- ✚ SPI, Security Parameter Index, un index utilisé en conjonction avec l'adresse de destination pour identifier une association de sécurité (*Security Association*).
- ✚ Traffic Analysis, des éléments du trafic réseau (taille des paquets, ...) utiles à un adversaire.

51/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



AH et ESP

- ✚ Deux en-têtes spécifiques sont utilisés, AH (IP Authentication Header) et ESP (IP Encapsulating Security Payload).
- ✚ AH garantit l'intégrité et l'authentification des datagrammes IP, mais n'assure pas la confidentialité des données. Cette absence de confidentialité permet une large utilisation de cet en-tête à travers Internet. Une *passerelle de sécurité* est un système qui sécurise des communications entre deux hôtes non sécurisés, elle est responsable de l'ajout de l'en-tête AH.
- ✚ ESP est utilisé pour fournir l'intégrité, l'authentification et la confidentialité des datagrammes IP. Le chiffrement de passerelle à passerelle est le mieux adapté pour la sécurité de réseaux privés, mais en tant que tel il ne substitue pas au chiffrement entre systèmes hôtes, et les deux procédés peuvent cohabiter.
- ✚ En l'absence de passerelles de sécurité les systèmes hôtes chiffrent uniquement les données utilisateurs (SSL...)

52/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Security Association

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

53/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

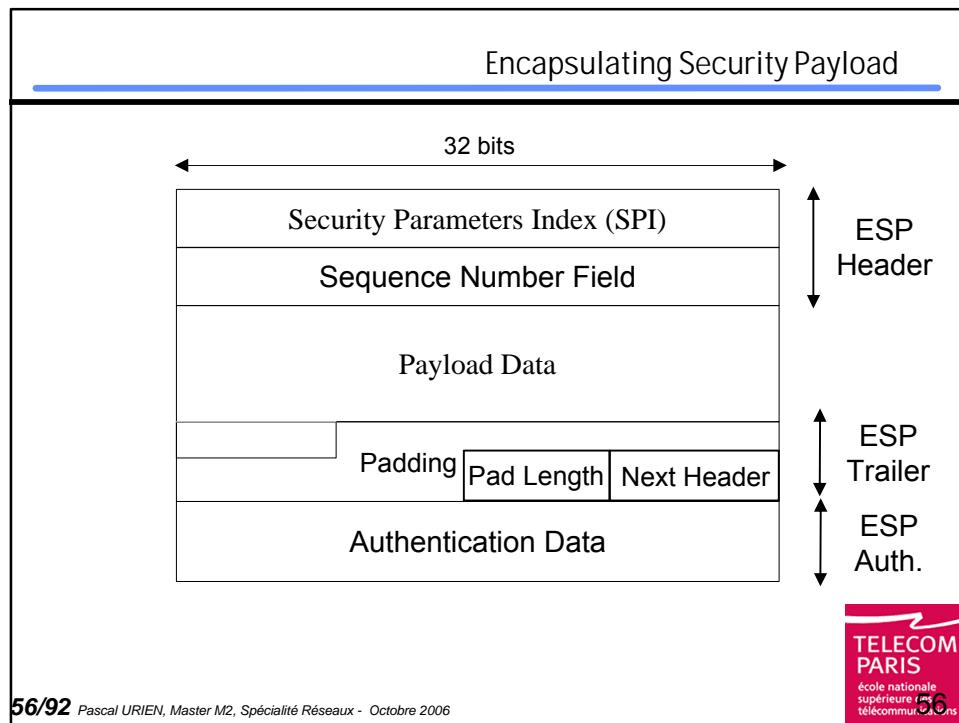
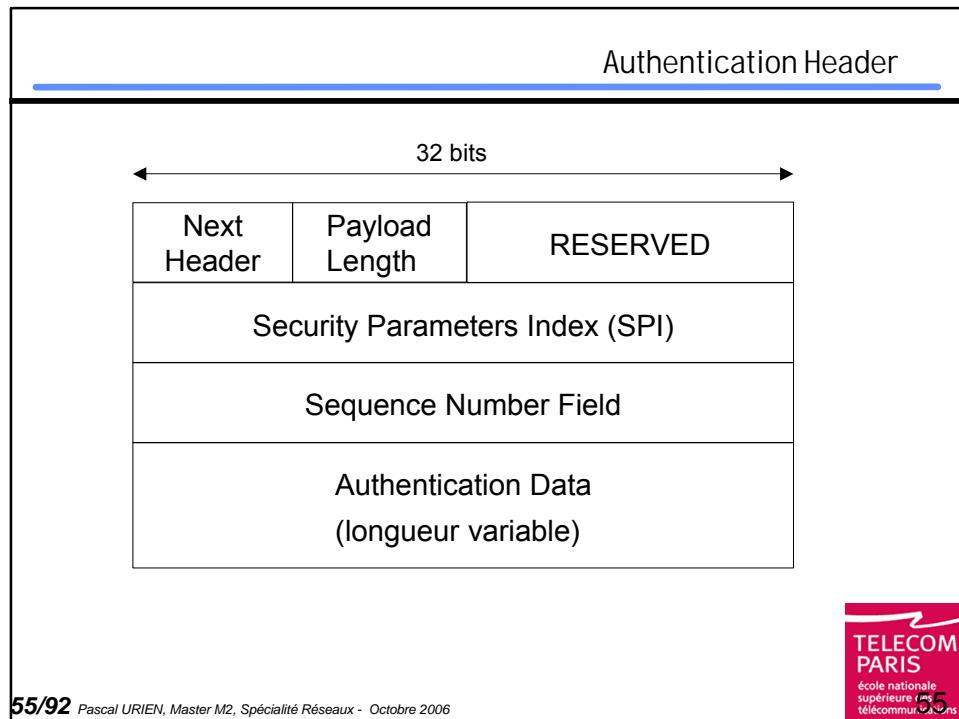


Modes IPSEC

- ⊕ En tête d'authentification AH
 - Cet en tête contient le résultat d'une fonction cryptographique calculée sur le datagramme IP, et utilisant une clé secrète d'authentification. Certains champs du datagramme (*TTL* - ipv4, ou *Hop Limit* Ipv6) ne sont pas pris en compte dans ce calcul (dans ce cas leur valeur est considérée égale à zéro).
 - Une clé dissymétrique permet de réaliser la non répudiation.
 - L'algorithme par défaut est MD5, qui utilise une clé symétrique et donc n'offre pas la non répudiation.
 - L'émetteur calcule un *message digest* qui porte sur le paquet IP (en tête incluse) tel qu'il sera reçu par le destinataire, ce qui signifie que les paquets IP dont l'en-tête finale n'est pas connue à priori ne peuvent pas être authentifiés par cette méthode.
 - Il y a deux modes possibles pour appliquer le mécanismes AH :
 - mode tunnel (ajout d'un nouvel en-tête IP)
 - mode transport (conservation de l'en-tête IP d'origine)
- ⊕ Encapsulation sécuritaire des données (ESP)
 - ESP garantit l'intégrité, l'authentification et la confidentialité des datagrammes IP. Il réalise cette fonction en encapsulant le datagramme IP, ou seulement le protocole véhiculé par IP (TCP, UDP...). La quasi totalité des données est chiffrée, et un en-tête non chiffré est ajouté à l'en-tête du paquet IP.
 - Il y a deux modes possibles pour appliquer ESP :
 - mode transport (conservation de l'en-tête IP d'origine)
 - mode tunnel (ajout d'un nouvel en-tête IP)

54/92 Combinaison AH et ESP
Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006





ISAKMP

- Internet Security Association and Key Management Protocol
- Ce protocole sert à :
 - l'établissement
 - la modification
 - la suppression
 - des Associations de Sécurité

ISAKMP

- ISAKMP comprend deux phases :
 - l'établissement d'une SA ISAKMP
 - authentification des tiers, génération des clefs,
 - échanges ISAKMP
 - la négociation des paramètres d'une SA pour un mécanisme donné (AH ou ESP par exemple)
 - le trafic de cette phase est sécurisé par la SA ISAKMP
- NB : Une SA ISAKMP est bidirectionnelle

Messages et Blocs

- Il existe 13 types de blocs :

■ SA	<i>Security Association</i>
■ P	<i>Proposal</i>
■ T	<i>Transform</i>
■ KE	<i>Key Exchange</i>
■ ID	<i>Identification</i>
■ CERT	<i>Certificate</i>
■ CR	<i>Certificate Request</i>
■ HASH	<i>Hash</i>
■ SIG	<i>Signature</i>
■ NONCE	<i>Nonce</i>
■ N	<i>Notification</i>
■ D	<i>Delete</i>
■ VID	<i>Vendor ID</i>



59/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

ISAKMP

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



60/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

ISAKMP

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

61/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



ISAKMP

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

62/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



ISAKMP

- A partir des blocs précédents, le protocole ISAKMP définit des types d'échanges (*Exchange Types*).
 - Il y a 5 types d'échanges par défaut :
 - Base Exchange
 - Identity Protection Exchange
 - Authentication Only Exchange
 - Aggressive Exchange
 - Informational Exchange

■ Notation

- **HDR** = entête du paquet ISAKMP
- **SA** = blocs SA + P + T

Base Exchange

Initiator

HDR, SA, NONCE

Attributs
négociés

Responder

Sélection des
attributs de SA

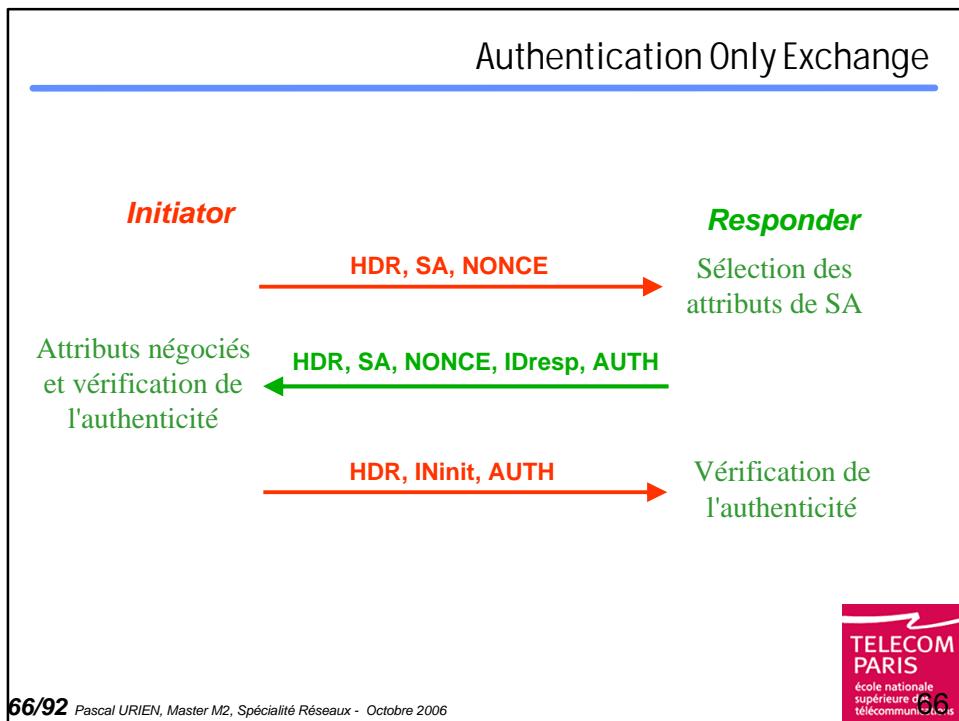
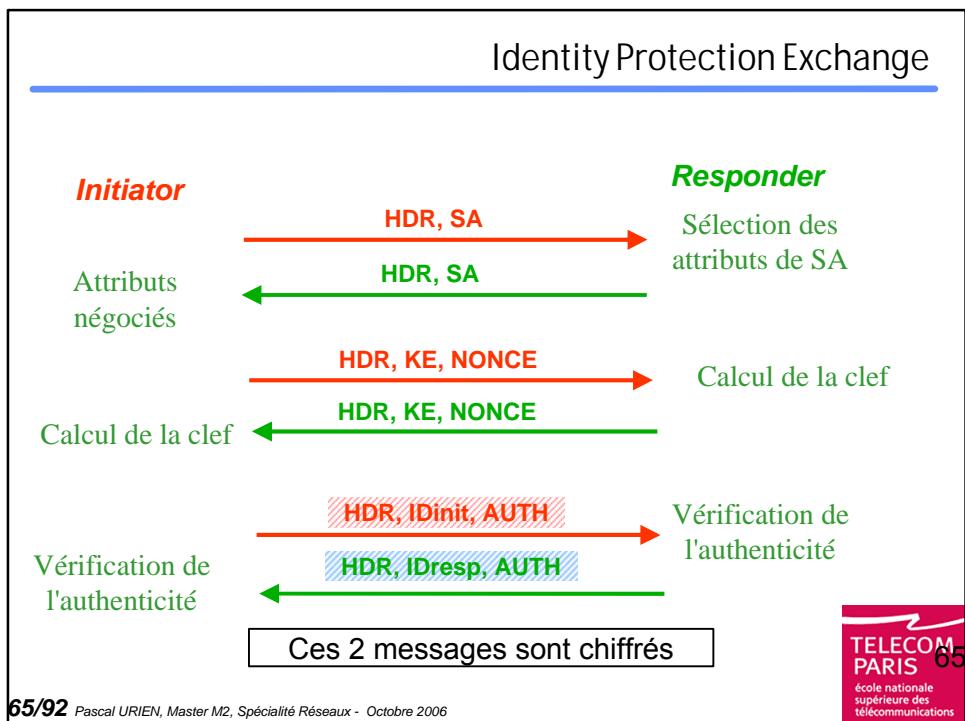
Vérification de
l'authenticité

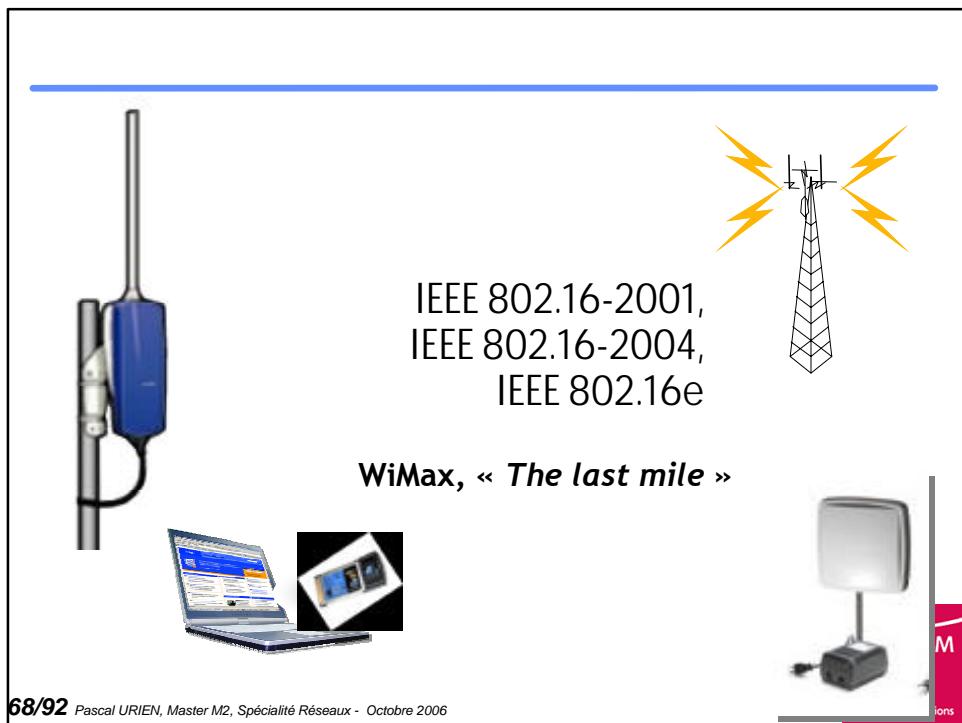
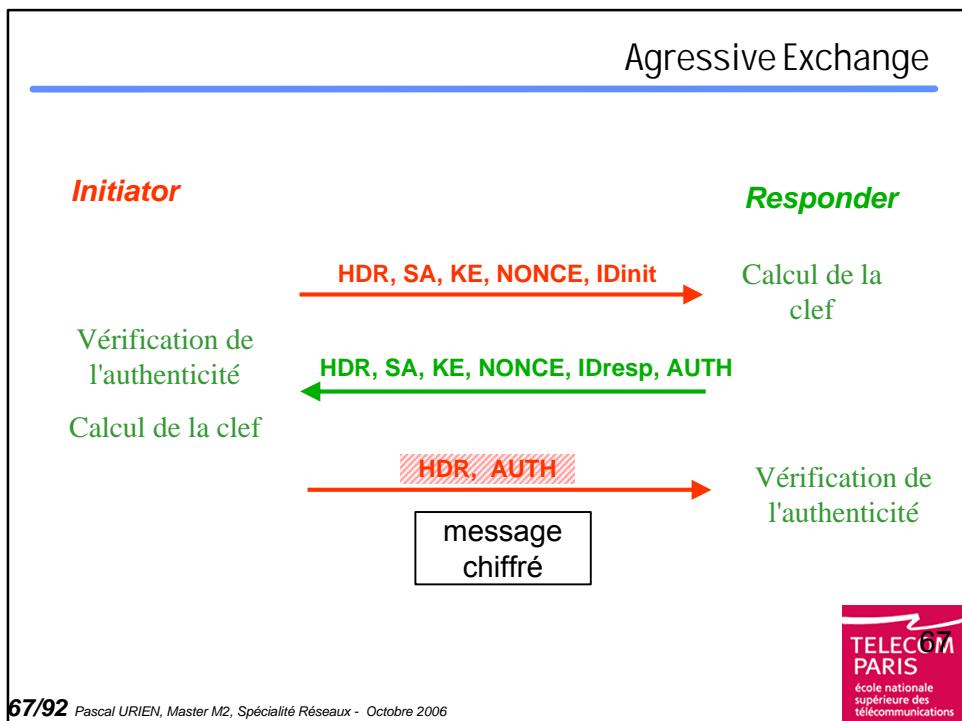
Vérification de
l'authenticité

HDR, SA, NONCE

HDR, KE, IDinit, AUTH

HDR, KE, IDresp, AUTH





Normes

Norme	IEEE 802.16-2001	IEEE 802.16-2004	IEEE 802.16e
Disponible	Décembre 2001	Octobre 2004	Février 2006
Bandé	10 - 66 GHz	2-11 GHz	< 6 GHz
Débit	32-134 Mbits dans des canaux de 28MHz	Jusqu'à 75 Mbits dans des canaux de 20MHz	Jusqu'à 15 Mbits dans des canaux de 5 MHz
Technique de Modulation	QPSK, 16QAM, 64QAM	OFDM 256 sous porteuses OFDMA 2048 sous porteuses	S-OFDMA
Mobilité	Fixe	Fixe, Nomade	Grande Mobilité
Largeur des canaux	20, 25 et 28 MHz	Variable 1.5 à 20 MHz	Identique à 802.16-2004 des sous canaux UL
Rayon de la cellule	2-5 km	7-10 km Maximum 50 km	2-5 km

69/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Marchés

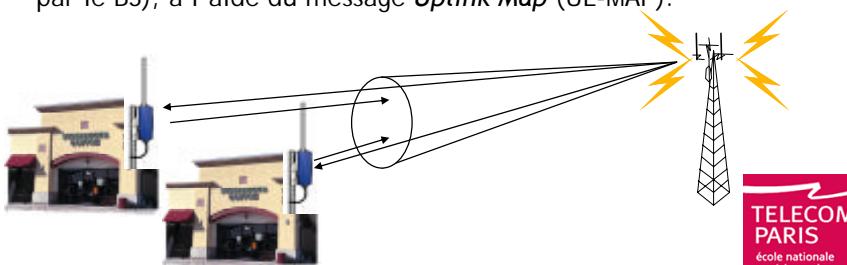
- ⊕ En premier lieu la fourniture de services de téléphonie en mode sans fil tels que T1 en Europe (2,048 Mbits/s) ou E1 (2,000 Mbits/s) aux Etats-Unis ; c'est une opportunité de prestations alternatives aux offres des opérateurs téléphoniques classiques, utilisant une infrastructure câblée.
- ⊕ Le haut 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*)

70/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



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).



71/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

TELECOM
PARIS
école nationale
supérieure des
télécommunications

Méthodes d'Accès Radio

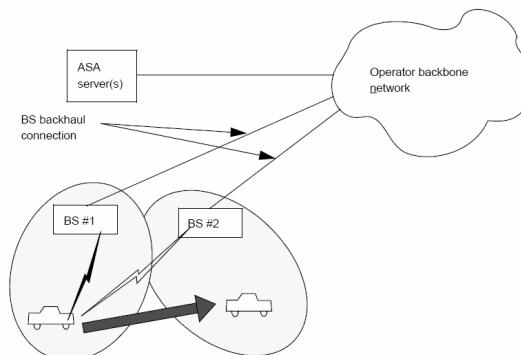
- ⊕ Une voie est organisée en une série de rafales (*bursts*), chacune d'entre elle étant identifiée par un code DIUC (*Downlink Interval Usage Code*) ou UIUC (*Uplink Interval Usage Code*), et caractérisée par des paramètres de modulation et de codage radio spécifiques, permettant d'obtenir des débits 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.

72/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

TELECOM
PARIS
école nationale
supérieure des
télécommunications

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.



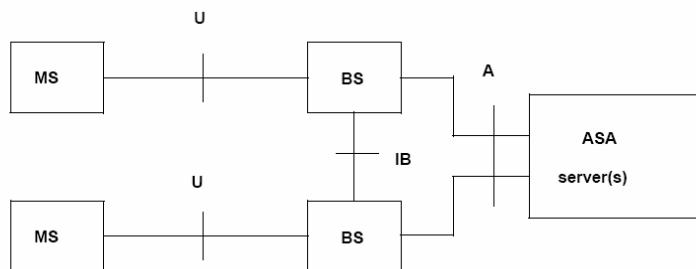
73/92 Pascal URIEN, Master M2



La sécurité IEEE 802.16e

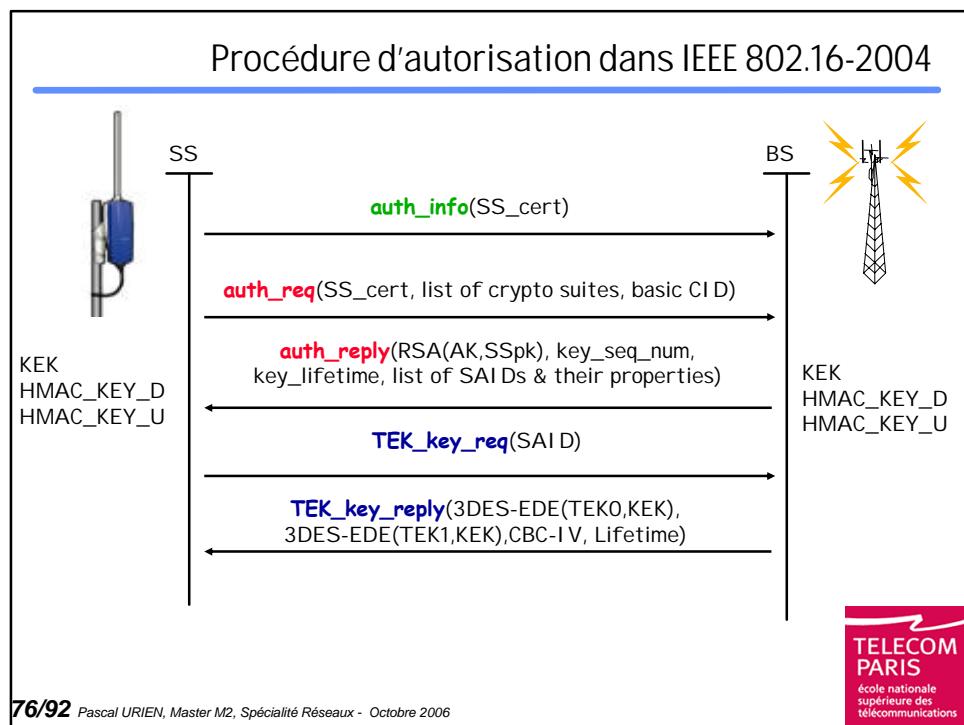
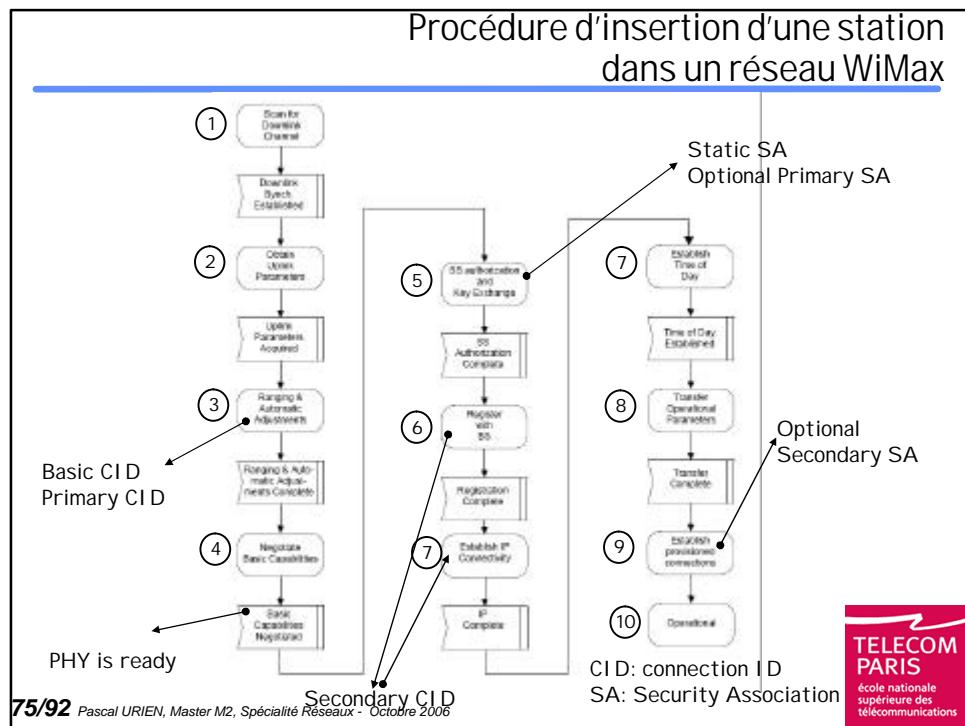
- L'architecture du réseau comporte des stations mobiles (*mobile station, MS*), communiquant avec des stations de base (*Base Station BS*). Ces dernières sont reliées à un réseau d'opérateur (*Operator Backbone Network*) qui possède généralement un centre d'authentification et d'autorisation (*Authentication 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. Enfin l'interface A achemine des paquets d'authentification entre stations de base et serveurs ASAs



74/92 P





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) ;
- deux clés de signature de 160 bits pour les liaisons descendantes et montantes, associées à un algorithme HMAC ;
- une clé de signature de 160 bits pour les infrastructures MESH.

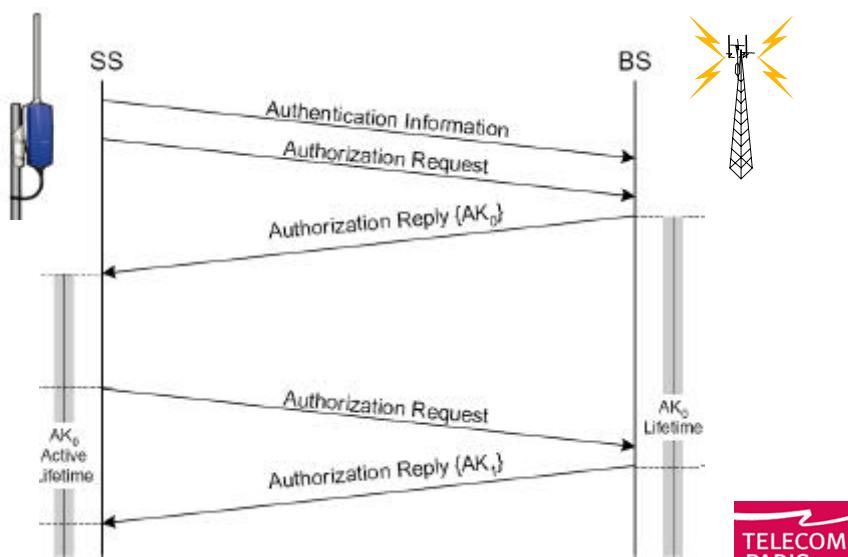
Données

- 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.

77/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



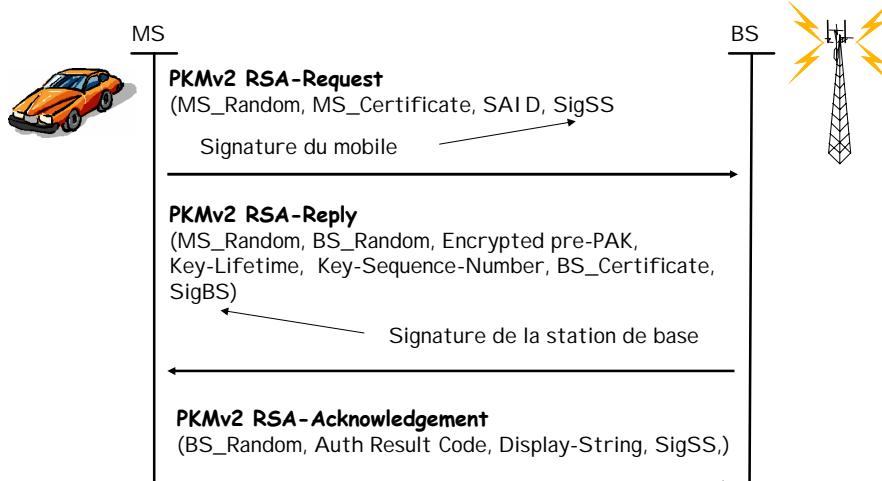
La distribution des clés TEKs (Traffic Encryption Key)



78/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



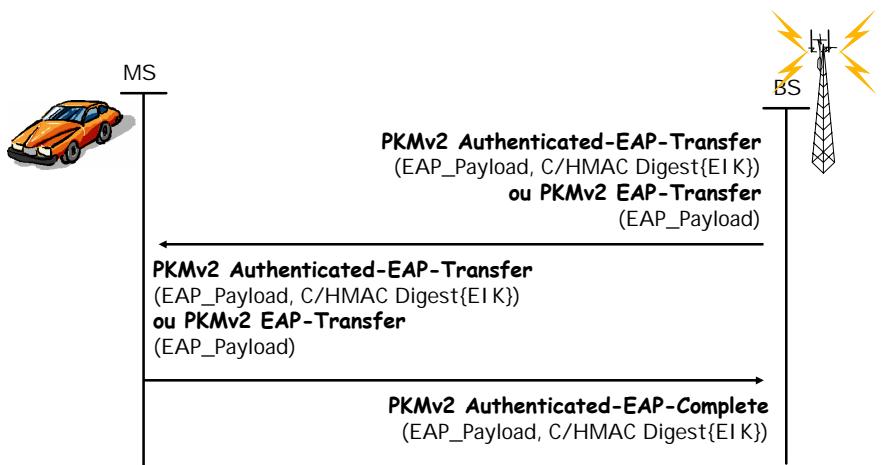
PKMv2 - RSA



79/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



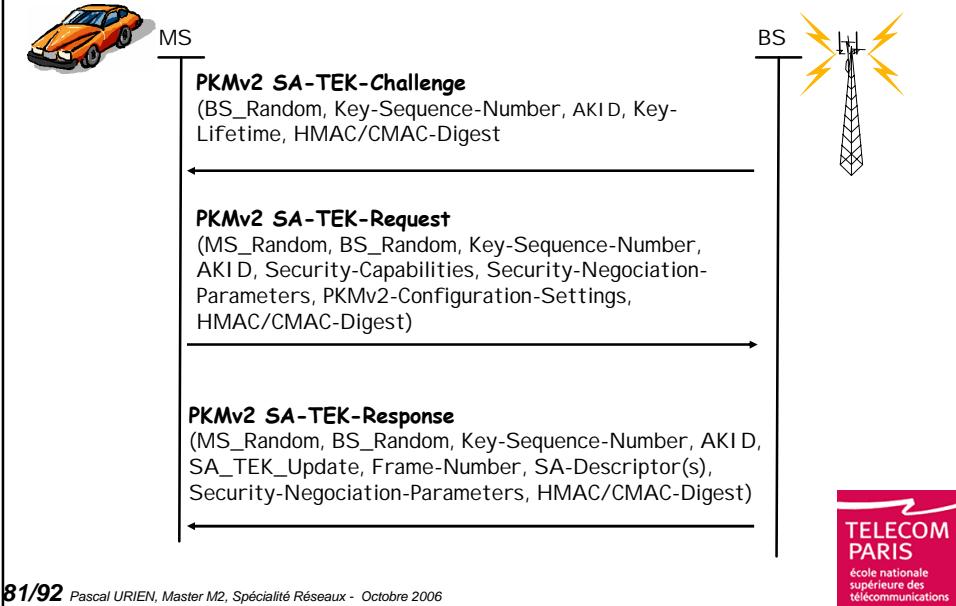
PKMv2 – EAP (Simple)



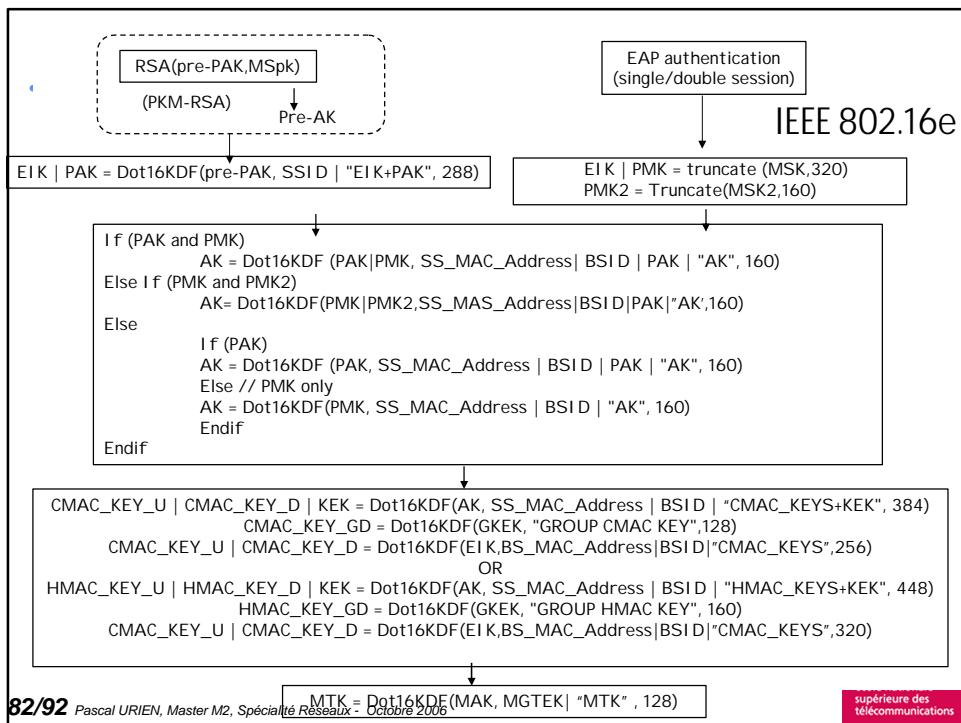
80/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



PKMv2 - SA-TEK 3-ways handshake



81/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



82/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006

PKI

83/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



RSA

- ➊ Soit n un produit de deux nombres premiers $n = pq$
- ➋ Soit e un entier inversible modulo $\varphi(n)$
 - Il est premier avec $\varphi(n) = (q-1)(p-1)$
 - Il existe d tel que $d \equiv 1 \pmod{\varphi(n)}$.
- ➌ Clé publique (e, n) , clé privée (d, n)
- ➍ Si M est inversible modulo n (premier avec n) $M^{\varphi(n)+1} \equiv 1 \pmod{n}$ (théorème de Fermat) et donc
 - $M^{ed} = M^{\varphi(n)+1} = M \pmod{n}$
- ➎ Si M n'est pas inversible modulo n
 - $M \equiv 0 \pmod{p}$, ou $M \equiv 0 \pmod{q}$
 - Si $M \not\equiv 0 \pmod{p}$, M est inversible modulo q , $M^{\varphi(q)} \equiv 1 \pmod{q}$,
 $\varphi(n) = \varphi(p) \cdot \varphi(q)$
 - $M^{\varphi(n)} \equiv 1 \pmod{q}$
 - $M^{ed} \equiv M \pmod{q}$
 - $M^{ed} \equiv 0 \pmod{p}$
 - D'où l'on déduit (théorème chinois) $M^{ed} \equiv M \pmod{(pq)}$

84/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



RSA

- La solution de $a x = 1 \text{ mod } n$ peut être trouvée à l'aide d'un algorithme d'Euclide étendu.

Si, a et b ont un diviseur commun d ($a > b$) alors $a-b$ et $a-2b$ sont divisibles par d.

On choisit le plus grand k tel que $a-kb = r$ ($r \geq 0$), soit $a = kb + r$.

Si $r=0$ alors a est divisible par b

Sinon on recommence l'algorithme avec b et r

Le PGCD est le dernier reste non nul.

- Exemple $a=522, b=453$

$$522-453 = 69$$

$$453-69 = 39$$

$$69-39=30$$

$$39-30=9$$

$$30-3.9=3$$

$3-3=0$, 3 est le PGCD(522,453)

- Exemple de calcul de clés RSA

$$p=47, q=59, n=pq = 2773, (p-1)(q-1)=2668$$

17 est premier avec $(p-1)(q-1)$

on cherche d 17 = 1 modulo 2668

$$\text{PGCD}(17,2668)=1, 1 = a u + b v, v \text{ est la solution}$$

$$2668=a$$

$$17=b$$

$$2668-156.17 = 2668 - 2652 = 16 = a - 156 b$$

$$17-16 = 1, b - (a - 156 b) = 1, 157 b - a = 1, \text{ d'où } d = 157$$

85/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



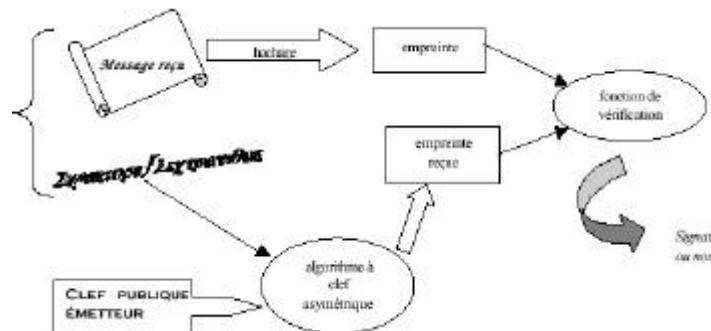
Signature

- D une fonction à sens unique

- M une suite de symbole (octets)

- La signature de M est le chiffrement de l'empreinte de M ($\text{Digest}(M)$) par une clé généralement asymétrique (clé privée RSA),

$$\text{Signature} = \text{Digest}(M)^{\text{PrivateExp}} \text{ modulo modulus}$$



86/92 Pascal



Certificat

- ⊕ C'est l'ensemble constitué par une suite de symbole (document M) et une signature.
- ⊕ Le format de certificat le plus courant est X509 v2 ou v3. La syntaxe utilisée est l'ASN.1 (*Abstract Syntax Notation One*).

87/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



X509

```
Certificate ::= SEQUENCE {
    certificateInfo CertificateInfo,
    signatureAlgorithm AlgorithmIdentifier,
    signature BIT STRING }

Certificate ::= SIGNED SEQUENCE {
    version [0] Version DEFAULT v1988,
    serialNumber CertificateSerialNumber,
    signature AlgorithmIdentifier,
    issuer Name,
    validity Validity,
    subject Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo }
    Certificate ::= SEQUENCE {
        tbsCertificate      TBSCertificate,
        signatureAlgorithm AlgorithmIdentifier,
        signatureValue     BIT STRING }
```

88/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



X509 v3

```
Certificate ::= SEQUENCE {
    tbsCertificate      TBSCertificate,
    signatureAlgorithm AlgorithmIdentifier,
    signature           BIT STRING }

TBSCertificate ::= SEQUENCE {
    version            [0] EXPLICIT Version DEFAULT v1,
    serialNumber       CertificateSerialNumber,
    signature          AlgorithmIdentifier,
    issuer             Name,
    validity           Validity,
    subject             Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID     [1] IMPLICIT UniqueIdentifier OPTIONAL,
                        -- If present, version shall be v2 or v3
    subjectUniqueID   [2] IMPLICIT UniqueIdentifier OPTIONAL,
                        -- If present, version shall be v2 or v3
    extensions         [3] EXPLICIT Extensions OPTIONAL
                        -- If present, version shall be v3
}
```

89/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Public Key Infrastructure

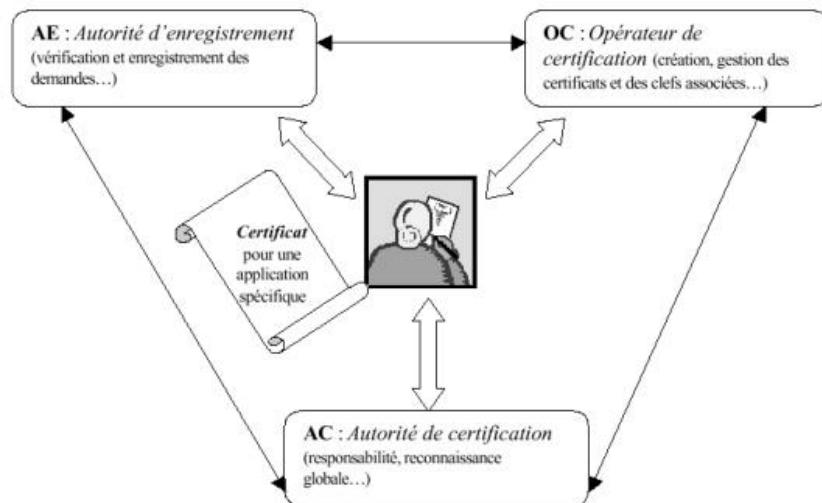
Les principales fonctions réalisées par une architecture PKI pour la gestion des certificats se résument ainsi :

- Enregistrement de demande et vérification des critères pour attribution d'un certificat : l'identité du demandeur est vérifiée ainsi que le fait qu'il soit bien en possession de la clef privée associée
- Création des certificats
- Diffusion des certificats entraînant publication des clefs publiques
- Archivage des certificats pour assurer la sécurité et la pérennité
- Renouvellement des certificats en fin de période de validité
- Suspension de certificats : elle peut être utile si le propriétaire estime ne pas avoir besoin temporairement de son certificat ; cependant cette fonction n'est pas aisée à mettre en œuvre ; elle est essentiellement administrative et il n'existe pas de standard d'implémentation
- Révocation de certificats : sur date de préemption, perte, vol ou compromission de clefs
- Création et publication (au sens gestion) des listes de révocation des certificats ; il y aura révocation du certificat dans les cas suivants : date de fin de validité atteinte, clef privée divulguée, perdue (donc impossibilité de lire les objets rendus confidentiels) ou compromise. Il n'existe aucun protocole standard qui permette de faire la révocation automatiquement, on a donc forcément recours à des moyens administratifs. Ceux-ci doivent être implantés avec un maximum de sécurité (le demandeur de la révocation doit en particulier prouver qu'il est bien le propriétaire de la clef publique ou privée devenue inutilisable). Les listes de révocation doivent d'une part être protégées pour éviter toute corruption, d'autre part être accessibles en permanence et le plus à jour possible (notion de temps réel). Pour un fonctionnement correct, cette fonction nécessite une synchronisation des horloges de tous les acteurs concernés par les listes de révocation.
- Délegation de pouvoir à d'autres entités reconnues de confiance Toute communauté peut créer sa propre infrastructure PKI, dans ce cas une étude de faisabilité est nécessaire en s'appuyant sur de nombreux critères.

90/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



PKI



91/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



Standards PKCS

- PKCS « *Public-Key Cryptography Standards* » est un ensemble de standards pour la mise en place des IGC, coordonné par RSA ; ces standards définissent les formats des éléments de cryptographie :
 - PKCS#1 : RSA Cryptography Specifications Version 2 (*RFC 2437*)
 - PKCS#2 : inclus dans PKCS#1
 - PKCS#3 : Diffie-Hellman Key Agreement Standard Version 1.4
 - PKCS#4 : inclus dans PKCS#1
 - PKCS#5 : Password-Based Cryptography Standard Version 2
 - PKCS#6 : Extended-Certificate Syntax Standard Version 1.5
 - PKCS#7 : Cryptographic Message Syntax Standard Version 1.5 (*RFC2315*)
 - PKCS#8 : Private-Key Information Syntax Standard Version 1.2
 - PKCS#9 : Selected Attribute Types Version 2.0
 - PKCS#10 : Certification Request Syntax Version 1.7 or Certificate Signing Request (CSR) (*RFC 2314*)
 - PKCS#11 : Cryptographic Token Interface Standard Version 2.10
 - PKCS#12 : Personnal Information Exchange Syntax Standard Version 1.0
 - PKCS#13 : Elliptic Curve Cryptography Standard Version 1.0
 - PKCS#14 : Pseudorandom Number Generation Standard Version 1.0
 - PKCS#15 : Cryptographic Token Information Format Standard Version 1.0

92/92 Pascal URIEN, Master M2, Spécialité Réseaux - Octobre 2006



La sécurité des réseaux sans fil 802.11



Introduction

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 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 (les «switchs»).

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*).

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 configuration¹, il est très facile d'accéder à l'intranet d'une entreprise depuis un port d'accès.

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)

¹ RFC 2131, Chapter 7 - Security Considerations, «...Therefore, DHCP in its current form is quite insecure».

IEEE 802.11

Un réseau 802.11 (voir figure 1) est un ensemble de cellules de base (BSS, *Basic Set Service*), chacune d'entre elles comportant un point d'accès (*Access Point*, AP) matérialisé par un dispositif d'émission réception analogue aux stations de base du GSM. L'ensemble de ces cellules (c'est à dire les APs) est relié par une infrastructure de communication fixe (*Distribution System DS*), qui incorpore en particulier un portail (*Portal*) assurant l'interface avec un réseau local (Ethernet) classique.

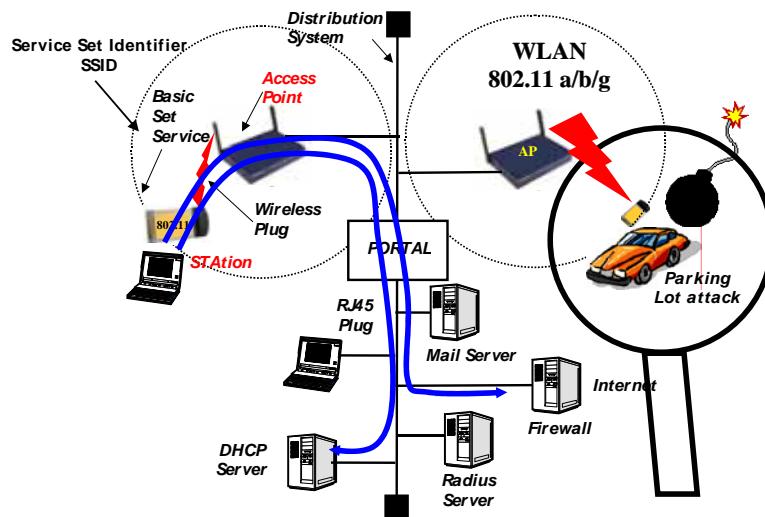


Figure 1. Une architecture typique 802.11

La norme 802.11 [IEEE Std 802.11, 1999] définit un protocole de sécurité radio, le WEP². Son principe consiste à chiffrer les trames (voir figure 2) à l'aide de l'algorithme RC4 et d'une clé, obtenue par la concaténation d'un secret partagé (de 40 ou 104 bits) et d'un index transporté en clair dans chaque paquet (un champ de 24 bits, noté IV).

² Wireless Equivalent Privacy

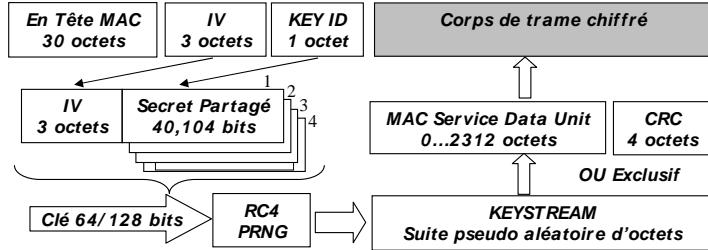


Figure 2. Le protocole WEP.

RC4 réalise le chiffrement des données en mode flux octets (*stream cipher*), à partir d'une clé de longueur comprise entre 8 et 2048 bits il génère (à l'aide d'un *pseudo random generator* PRNG) une suite d'octets pseudo aléatoire nommée *KeyStream*. Cette série d'octets (Ksi) est utilisée pour chiffrer un message en clair (Mi) à l'aide d'un classique protocole de Vernam, réalisant un ou exclusif (xor) entre Ksi et Mi (Ci = Ksi xor Mi).

Le WEP présente de nombreuses failles de sécurité [Borisov *et al.* 2001], en voici un bref résumé,

- Le nombre de *KeyStream* est limité à 16 millions (2^{24}). Un pirate peut facilement générer des trames, enregistrer leur forme chiffrée puis déduire et stocker les *KeyStream* identifiés par leur index *IV*.
- L'intégrité des trames est assurée par le chiffrement du CRC. Cette fonction étant linéaire par rapport à l'opération *ou exclusif*³ il est possible de modifier un bit dans une trame chiffrée tout en recalculant une valeur correcte du CRC, c'est la technique d'attaque dite *bit flipping*.
- L'attaque démontrée par Fluhrer [Fluhrer *et al.*, 2001] permet de recouvrir un secret partagé de 104 bits après l'émission d'approximativement quatre millions de trames chiffrées. Elle utilise des valeurs IV dites *résolvantes*, de la forme (3+B,255,N) avec B un octet du secret partagé et N une valeur quelconque comprise entre 0 et 255. Environ 60 valeurs résolvantes suffisent à retrouver un octet du secret partagé. Un rapide calcul montre que l'on obtient une valeur résolvante toutes les 2^{16} trames, soit 60 occurrences après environ 4 millions (2^{22}) de paquets.
- De manière optionnelle l'authentification est réalisée par une méthode de défi (nommée *Shared Authentication*), le point d'accès délivre un nombre

³ Soit T1 et T2 deux trames de même longueur, $\text{CRC}(T1 \text{ exor } T2) = \text{CRC}(T1) \text{ exor } \text{CRC}(T2)$.

aléatoire, la station chiffre cette valeur. Cette méthode est inefficace car réjouable, l'attaquant enregistre le couple (aléa, aléa chiffré) d'où il déduit la valeur du *KeyStream* associé à un index *IV*. Il peut utiliser ces paramètres pour chiffrer correctement un nouveau défi.

En raison des problèmes évoqués précédemment, il est fortement conseillé de changer la clé WEP fréquemment, par exemple tous les 10,000 trames. Cependant cette technique ne garantit pas l'intégrité de l'information et les attaques *bit flipping* restent possibles.

Une particularité du protocole 802.11 est que l'authentification est obligatoire avant toute association avec un point d'accès. Une station sans fil se trouve en conséquence dans l'un des trois états suivants,

- Non-Authentifié et Non-Associé
- Authentifié et Non-Associé
- Authentifié et Associé.

Lorsque la station ne souhaite pas utiliser une méthode (*Shared Authentication*) basée sur WEP, elle dispose d'une procédure volontaire sans aucun élément de sécurité, baptisée *Open Authentication*.

Une difficulté de déploiement d'une architecture basée sur WEP est la nécessité de partager un même secret entre station et point d'accès. Cette contrainte freine considérablement le passage à l'échelle; elle souligne l'importance de la disponibilité d'une infrastructure de distribution des clés telle que par exemple définie par la norme 802.1X [IEEE Std 802.1X, 2001].

IEEE 802.1X

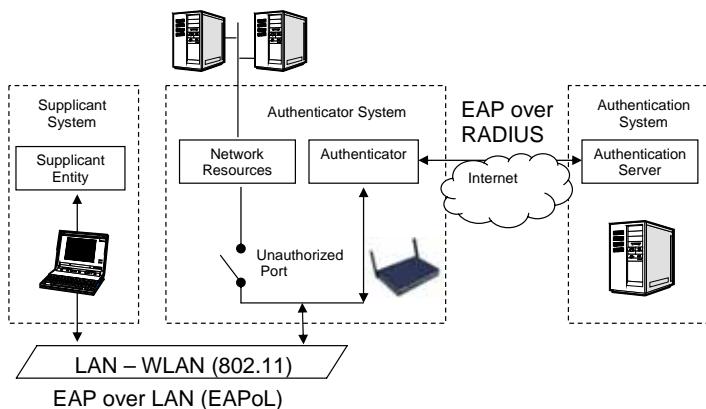


Figure 3. L'architecture 802.1X

Le protocole IEEE 802.1X (ou *Port Based Network Access Control*) était initialement conçu pour la gestion sécurisée des accès des réseaux (câblés) à base de commutateurs de paquets (*switchs*). L'idée centrale est de bloquer le flux de données d'un utilisateur non authentifié. Ce modèle s'appuie sur trois entités fonctionnelles (voir figure 3),

- Le ***Supplicant***, un terminal informatique désirant utiliser les ressources offertes par un réseau de communication.
- L'***Authenticator***, le système qui contrôle un port d'accès au réseau. Le flux de données du supplicant est divisé en deux classes, la première comprend les trames utilisées par le protocole d'authentification EAP⁴, la deuxième regroupe les autres paquets, qui sont bloqués lorsque le port se trouve dans l'état *non autorisé*. En cas de succès du processus d'authentification, le port passe à l'état authentifié et offre un libre passage à toutes les trames.
- Le ***serveur d'authentification*** (RADIUS⁵), il réalise la procédure d'authentification avec le supplicant. Durant cette phase l'*Authenticator* n'interprète pas le dialogue entre ces deux entités, il agit comme un simple relais passif.

Le protocole EAP est la clé de voûte de cette approche. Il est tour à tour encapsulé dans des trames MAC 802 (EAPoL⁶) ou par le protocole RADIUS qui est routable (puisque transporté par IP et UDP).

Schématiquement l'insertion d'un terminal sans fil dans un environnement 802.1X se déroule de la manière suivante,

- Dans un premier temps la station s'authentifie puis s'associe à un point d'accès, identifié par son SSID (une chaîne de 32 caractères au plus).
- La station émet alors périodiquement (toutes les 30 secondes) une trame EAPoL-Start.
- Le point d'accès transmet un message EAP-Request.Identity au *Supplicant* qui produit en retour une réponse (EAP-Response.Identity) comportant l'identité (*EAP-ID*) du terminal sans fil.
- A partir de ce paramètre le point d'accès déduit l'adresse (IP) du serveur d'authentification et transmet à ce dernier le message EAP-Response.Identity encapsulé dans une requête RADIUS.
- Dès lors des messages EAP (requêtes et réponses) sont échangés entre serveur RADIUS et *Supplicant*, le point d'accès ne jouant qu'un rôle passif de relais.

⁴ EAP – Extensible Authentication Protocol, RFC 2284, March 1998

⁵ RADIUS, Remote Authentication Dial In User Service, RFC 2865, June 2000

⁶ EAPoL - EAP Over LAN

- Le serveur RADIUS indique le succès ou l'échec de cette procédure grâce à un message *EAP-Success* ou *EAP-Failure*. En fonction de cette information le port transite à l'état autorisé ou non autorisé.

A la fin d'un scénario d'authentification réussi *Supplicant* et serveur d'authentification calculent une clé baptisée ***Unicast Key***. Ce paramètre est en fait un secret partagé entre les deux entités. Dans l'environnement Microsoft cette valeur représente un couple de clés⁷ (2 fois 32 octets) *MS-MPPE-Send-Key* et *MS-MPPE-Recv-Key*. Une clé dite ***Global Key*** est transportée (entre point d'accès et *Supplicant*) de manière sécurisée dans une trame EAPoL-Key, chiffrée et signée à l'aide de la clé *Unicast*. Grâce au protocole RADIUS le serveur d'authentification transmet la clé *Unicast* au point d'accès. Ce dernier choisit alors une clé globale (la clé WEP) et la délivre au *Supplicant*.

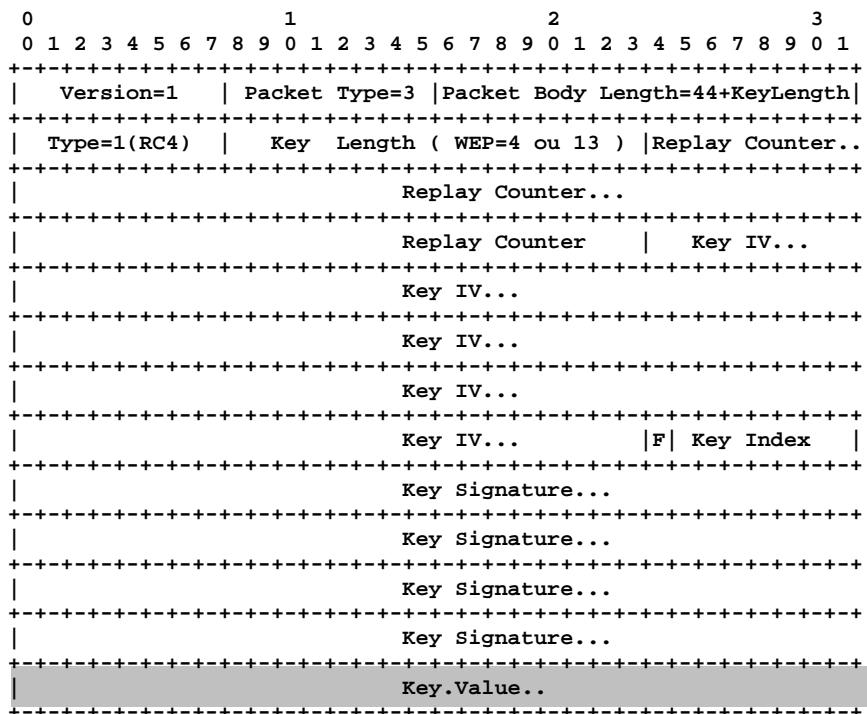


Figure 4. Format d'un descripteur EAPoL RC4.

⁷ Ces attributs sont définis dans la RFC 2548, *Microsoft Vendor-specific RADIUS Attributes*, March 1999.

La figure 4 présente le format d'un descripteur EAPoL-Key⁸. Le champ *ReplayCounter* (8 octets) s'interprète comme un horodatage au format NTP⁹; le paramètre *IV* est un nombre aléatoire cryptographique de 16 octets. La clé distribuée (*KeyValue*) est chiffrée au moyen de l'algorithme RC4 et d'une clé de 48 octets (16+32) obtenue par la concaténation des attributs *IV* et *MS-MPPE-Recv-Key*. L'ensemble du descripteur est signé (*KeySignature*) au moyen d'un HMAC-MD5¹⁰ (16 octets) dont la clé est *MS-MPPE-Send-Key*. Le drapeau (F) indique si la clé transportée est globale (F=1) ou *unicast*.

EAP

Le problème de la gestion de la mobilité des utilisateurs est devenu critique dès lors que les internautes ont massivement utilisé des modems et le protocole PPP pour accéder aux ressources offertes par leur ISP (*Internet Service Provider*). Les systèmes d'exploitation ont donc intégrés des fonctionnalités renforçant la sécurité des nomades, telles que :

- L'authentification des utilisateurs par des méthodes de défi par exemple CHAP¹¹, MSCHAP¹², MSCHAPv2¹³.
- Le chiffrement des trames PPP, par exemple par à l'aide de l'algorithme MPPE¹⁴.
- Des méthodes de calcul¹⁵ des clés de chiffrement (*MS-MPPE-Recv-Key* et *MS-MPPE-Send-Key*)
- La distribution¹⁶ de telles clés par le protocole RADIUS.

Le besoin de comptabilité avec des infrastructures d'authentification diversifiées et la nécessité de disposer de secrets partagés dans ces environnements multiples ont naturellement conduit à la genèse du protocole EAP, capable de transporter des méthodes d'authentification indépendamment de leurs particularités.

⁸ D'après draft-congdon-radius-8021x-29.txt, April 2003

⁹ Network Time Protocol, RFC 1305, March 1992

¹⁰ Keyed-Hashing for Message Authentication, RFC 2104, February 1997

¹¹ PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994, August 1996.

¹² Microsoft PPP CHAP Extensions, RFC 2433, October 1998.

¹³ Microsoft PPP CHAP Extensions, Version 2, RFC 2759, January 2000

¹⁴ Microsoft Point-To-Point Encryption (MPPE) Protocol, RFC 3078, March 2001

¹⁵ Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE), RFC 3079, March 2001

¹⁶ Microsoft Vendor-specific RADIUS Attributes, RFC 2548, March 1999.

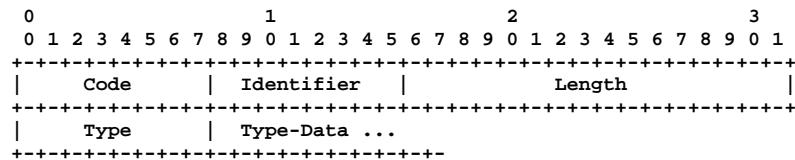


Figure 5. Format d'un message EAP

Le protocole EAP fournit un cadre peu complexe pour le transport de protocoles d'authentification; un message (voir figure 5) comporte un en tête de cinq octets et des données optionnelles. Il existe quatre types de messages identifiés par un code (1 octet), requête (1=request), réponse (2=response), succès (3=Success) et échec (4=Failure). Chaque message est étiqueté à l'aide d'un nombre *Identifier* compris entre 0 et 255, l'étiquette d'une réponse est égale à celle de la requête correspondante. La longueur totale du message, codée sur deux octets, est comprise entre 4 et 65535. Le champ type (compris entre 0 et 255) désigne le protocole d'authentification transporté ou des opérations particulières :

- Type=1, message relatif à l'identité (*Identity*)
- Type=3, notification d'un erreur (*NAK*).
- Type=4, protocole d'authentification à base de défis MD5 (EAP-MD5)
- Type = 13, transport de TLS (EAP-TLS)
- Type = 18 méthode d'authentification basée sur une carte SIM (EAP-SIM)
- Type = 26, transport de MSCHAPv2.

L'identité de l'utilisateur est indiquée par la valeur *EAP-ID* associée au message *EAP-Response.Identity*. Lorsque ce paramètre est similaire à une adresse de courrier électronique (NAI¹⁷) le point d'accès interprète la partie gauche (avant le caractère @) comme un *login* utilisateur et la partie droite comme le nom de domaine d'un serveur RADIUS.

Une session d'authentification (voir figure 6) est initiée par le point d'accès grâce au message *EAP-Request.Identity*. Elle se poursuit par une suite de requêtes et de réponses (*EAP-Request.Type* et *EAP-Response.Type*), relatives à un type (scénario d'authentification) particulier et échangés entre le serveur RADIUS et le *Supplicant*. Elle se termine par un message *EAP-Success* ou *EAP-Failure*.

¹⁷ The Network Access Identifier, RFC 2486, June 1999

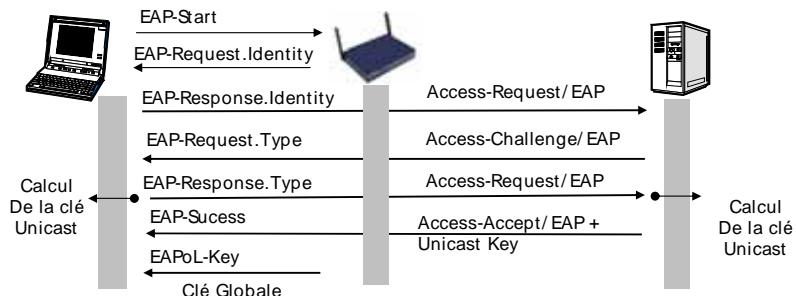


Figure 6. Une session typique d'authentification

Un des points faibles du protocole EAP est le déni de service [Mishra et al, 2002], un pirate peut écouter une session EAP et émettre à l'intention du *Supplicant* un message *EAP-Failure*. Cependant il ne pourra pas obtenir la clé globale délivrée par le message *EAPoL-Key* parce que cette dernière est chiffrée et signée par la clé unicast dont il ne connaît pas la valeur.

Nous allons à présent examiner brièvement trois types de méthodes d'authentification liées à des environnements différents.

EAP-MSCHAPv2

Dans l'univers Microsoft la sécurité d'un ordinateur personnel est fortement corrélée au mot de passe de son utilisateur. Ce dernier n'est jamais stocké en clair dans la mémoire de la machine. A partir d'un mot de passe on calcule une empreinte MD4 de 16 octets, mémorisée par le système hôte. Cette valeur, parfois nommée clé NT ou *NtPasswordHash* est complétée par cinq octets nuls. On obtient ainsi 21 octets interprétés comme une suite de trois clés DES (de 56 bits chacune). La méthode MSCHAPv1 est une authentification simple, le serveur d'authentification produit un nombre aléatoire de 8 octets, l'authentifié utilise ses trois clés DES pour chiffrer cet aléa, ce qui génère une réponse de 24 octets. MSCHAPv2 est une extension du protocole précédent, le serveur d'authentification délivre un nombre aléatoire de 16 octets (*AuthenticatorChallenge*), le Supplicant calcule une valeur de 8 octets à partir de cette valeur, d'un aléa (*PeerChallenge*) qu'il génère et du nom de l'utilisateur (*login*). Ce paramètre est chiffré de manière analogue à MSCHAPv1 par la clé NT et l'on obtient une valeur de 21 octets. Dans une plateforme Microsoft un annuaire stocke le nom des utilisateurs et leur mot de passe.

EAP-SIM

Les opérateurs de téléphonie mobiles utilisent une carte à puce SIM pour identifier et facturer un abonné. Cette dernière stocke l'identité de l'utilisateur (IMSI) et une clé secrète notée Ki. Le réseau authentifie un client à l'aide d'un triplet RAND (16 octets) SRES (4 octets) et Kc (8 octets). RAND est un nombre aléatoire généré par le serveur d'authentification. L'algorithme cryptographique A3/A8 associé à la clé Ki et appliqué à la valeur d'entrée RAND fournit une valeur de 96 bits, qui représente la concaténation des attributs SRES et KC. SRES est interprété comme une signature prouvant l'identité de l'utilisateur et KC est utilisé pour le chiffrement de la conversation téléphonique. Parce que les opérateurs envisagent de prolonger le réseau GPRS par des *hotspots* Wi-Fi ils proposent un protocole d'authentification EAP-SIM¹⁸, basé sur la carte SIM et se déroulant schématiquement de la manière suivante :

- L'identité (*EAP-ID*) est obtenue par la concaténation du caractère '1' de la valeur exprimée en ASCII de l'IMSI (une suite de chiffres) du caractère '@' et du nom de domaine de l'opérateur (*EAP_ID == 1IMSI@operator.com*)
- Le Supplicant génère un nombre aléatoire (NONCE)
- Le serveur RADIUS délivre une suite de valeurs RANDi, ce message est signé par une empreinte (digest) prenant en compte la valeur NONCE
- Le Supplicant calcule les valeurs SRESi et KCi. Il prouve sa connaissance de SRESi en incluant une empreinte, prenant en compte les valeurs SRESi, dans le message de réponse. Le nombre NONCE et les attributs KCi sont utilisés pour le calcul de la clé Unicast.

Grâce à la technologie EAP-SIM les opérateurs de téléphonie peuvent utiliser leur base de données clients (*Host Location Register*) pour assurer la facturation des services sans fil.

EAP-TLS

Le transport de messages TLS pose essentiellement un problème de segmentation. La taille d'un enregistrement TLS est d'au plus 16384 octets, le protocole RADIUS limite sa charge utile à 4096 octets et de surcroît la taille des trames 802.11 est limitée à 2312 octets. EAP-TLS¹⁹ supporte en conséquence un mécanisme de segmentation des enregistrements. Contrairement à l'usage courant de TLS mettant en œuvre une authentification (simple) du serveur, EAP-TLS utilise une authentification

¹⁸ H. Haverinen, J. Salowey , EAP SIM Authentication, draft-haverinen-pppext-eap-sim-11.txt June 2003

¹⁹ PPP EAP TLS Authentication Protocol, RFC 2716, October 1999.

mutuelle entre serveur RADIUS et *Supplicant* (voir figure 7). Ce dernier doit donc disposer d'un certificat X509 et d'une clé privée afin de prouver son identité.

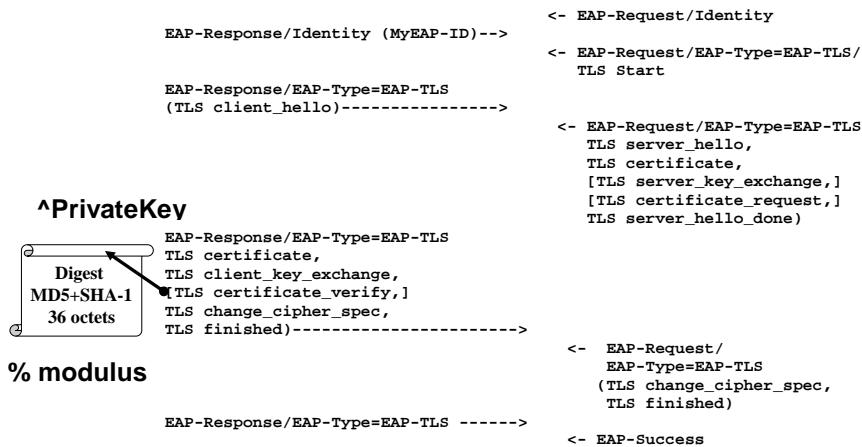


Figure 7. Le protocole EAP-TLS

L'usage d'une clé privée par le *Supplicant* soulève le problème critique de la sécurité requise par stockage et de la mise en œuvre d'un tel composant. Dans les plateformes informatiques usuelles cette sécurité est assurée par des mots de passe permettant de déchiffrer et d'utiliser la clé privée. La carte à puce constitue une alternative à cette méthode, lorsque la sécurité de la plateforme informatique est jugée insuffisante.

Vers la carte à puce EAP

Dans la section précédente nous avons évoqué l'usage de cartes à puce pour des réseaux liés aux opérateurs de téléphonie mobiles (cartes SIM), ou utilisant des infrastructures à clés publiques (PKI). Cette technologie a permis aux opérateurs d'exploiter leur réseau en limitant très fortement le nombre de fraudes (et par conséquent d'assurer une rentabilité financière); elle est également le support légal de la signature électronique reconnue par de nombreux pays.

La carte à puce EAP est un projet décrit par un *draft IETF*²⁰, auquel participent les principaux industriels de ce secteur, qui propose de traiter directement le protocole EAP dans la puce sécurisée. Bien que cette liste ne soit pas exhaustive les principales applications visées sont EAP-SIM et EAP-TLS.

Schématiquement une carte EAP [Urien2 et al, 2003] assure quatre services de base (voir figure 8),

- La gestion de multiples identités. Le porteur de la carte peut utiliser plusieurs réseaux sans fil. Chacun d'entre eux nécessite un triplet d'authentification, EAP-ID (la valeur délivrée dans le message EAP-Response.Identity), EAP-Type (le type de protocole d'authentification supporté par le réseau), et les crédits cryptographiques c'est-à-dire l'ensemble des clés ou paramètres utilisés par un protocole particulier (EAP-SIM, EAP-TLS, MSCHAPv2...). Chaque triplet est identifié par un nom (l'identité) dont l'interprétation peut être multiple (SSID, nom d'un compte utilisateur, mnémonique, ...)
- L'affectation d'une identité à la carte, en fonction du réseau visité.
- Le traitement des messages EAP.
- Le calcul de la clé *unicast* en fin de session d'authentification et sa mise à disposition pour le terminal désirant accéder aux ressources du réseau sans fil.

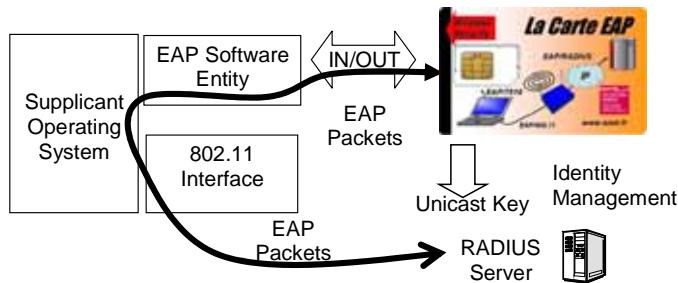


Figure 8. La carte à puce EAP

²⁰ P.Urien, A.J. Farrugia, G.Pujolle, M.Groot, J.Abellan “EAP support in smartcards“, draft-urien-eap-smartcard-06.txt, September 2004.

RADIUS

Outre Atlantique les fournisseurs de services internet (ISP) utilisent fréquemment des *pools* de modem installés dans les centraux téléphoniques urbains. Cette infrastructure, permettant des accès bon marché est baptisée point de présence ou POP (*point of presence*). Plutôt que de dupliquer et de mettre à jour dans chaque POP la base donnée des comptes clients, les ISPs ont déployé une architecture centralisée, assurant la gestion à distance de leurs clients (*roaming*) et s'appuyant sur trois niveaux fonctionnels

- L'utilisateur muni d'un login et d'un mot de passe (un *supplicant* en fait)
- Le Network Access Server (NAS). Cette entité contrôle l'ensemble des modems et assure l'interface avec le serveur d'authentification, elle est analogue à un *authenticator 802.1X*.
- Le serveur RADIUS, jouant le rôle d'un serveur d'authentification 802.1X.

Ce dernier système assure l'interface avec la base de données gérant les comptes utilisateurs. Le dialogue d'authentification usuellement basé sur les protocoles PAP ou CHAP et relayé par le NAS entre utilisateur et serveur d'authentification.

Le NAS réalise un pont applicatif entre les protocoles PAP ou CHAP (transportés par PPP) et le serveur RADIUS. Par exemple, dans le cas de PAP il transmet au serveur RADIUS, à des fins de vérification, l'identité de l'utilisateur et son mot de passe. Le serveur RADIUS indique au NAS le succès ou l'échec de cette opération. Le NAS mesure également le temps d'utilisation du service par le client et transmet une requête de facturation lorsque ce dernier quitte le POP.

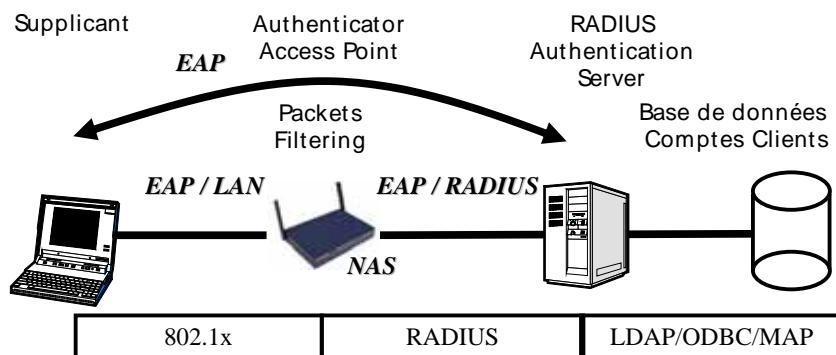


Figure 9.RADIUS et base de données clients.

Le transport²¹ quasi transparent du protocole EAP par RADIUS, permet de mettre en place une architecture générique, indépendante des méthodes d'authentification utilisées par les ISPs.

La sécurité des échanges RADIUS est assurée à l'aide d'un secret partagé entre serveur d'authentification et NAS. Le NAS produit des messages *Access-Request* comportant un nombre aléatoire de 16 octets, nommé *Authenticator*. La réponse du serveur RADIUS est l'un des trois messages suivants, *Access-Challenge*, *Access-Reject* ou *Access-Success*. Ces derniers sont signés par une empreinte MD5, le *Response Authenticator* calculée à partir du contenu du message, de l'aléa *Authenticator* et du secret partagé. Afin d'éviter des attaques du type « man in the middle », les requêtes RADIUS (délivrées par le NAS) sont signées par l'attribut *Message-Authenticator*, un HMAC²² du message dont la clé est égale au secret RADIUS.

En résumé la sécurité du protocole RADIUS repose sur l'algorithme MD5; certaines architectures s'appuient sur IPSEC pour renforcer la sécurité du lien avec le serveur d'authentification.

Bien que non standardisées, l'interface entre le serveur RADIUS et la base de donnée des comptes clients (SGBD, annuaire LDAP, autre...) est un point essentiel. Dans certain cas ces deux entités sont logées par la même machine; des locaux sécurisés sont cependant nécessaires pour éviter le pillage des données critiques. Lorsque la base cliente et le serveur RADIUS sont distants un lien sécurisé est nécessaire (SASL²³, SSL/TLS, IPSEC ...).

IEEE 802.11i

Nous avons précédemment souligné les faiblesses du protocole WEP. La norme 802.11x définit un cadre pour l'authentification mais ne spécifie de manière détaillée la méthode de distribution des clés. D'autre part le *Supplicant* ne participe pas au calcul de la clé globale, il n'y a pas de procédure de mutuelle authentification entre *Supplicant* et point d'accès mettant à profit l'existence d'un secret partagé (la clé *unicast*).

Le groupe de travail IEEE 802.11i [IEEE Std 802.11i/D5.0, 2003] étudie une architecture destinée à combler ces lacunes. Bien que ce standard ne soit encore pas encore finalisé, un comité industriel a déjà édité une

²¹ Ce transport est décrit dans la RFC 2869, RADIUS extensions, June 2000

²² Keyed-Hashing for Message Authentication, RFC 2104, February 1997

²³ Simple Authentication and Security Layer (SASL), RFC 2222, October 1997

recommandation (WPA²⁴) basée sur un sous ensemble de ce standard émergeant.

Nous classerons les apports de la norme IEEE 802.11i en trois catégories, définition de multiples protocoles de sécurité radio, éléments d'information permettant de choisir l'un d'entre eux et nouvelle méthode distribution de clés.

Le standard s'appuie sur les réseaux sans fil 802.11 et utilise 802.1x pour l'authentification et le calcul d'une clé maître nommée PMK (*Pairwise Master Key*). Cependant dans le cas du mode *adhoc*, cette clé baptisée PSK (*Pre Shared Key*) est distribuée manuellement. La hiérarchie des clés cryptographiques est présentée par la figure 10.

Protocoles de sécurité radio

Trois protocoles de sécurité sont proposés,

- WEP, importé de la norme 802.11 originale.
- TKIP (*Temporal Key Integrity Protocol*), le successeur de WEP. Il met en œuvre l'algorithme de chiffrement RC4, et ajoute à chaque SDU²⁵ MAC une signature de 64 bits baptisée MIC (*Message Integrity Code*). La clé RC4 (128 bits) est calculée à partir d'un compteur de 48 bits (*Transmit Sequence*) transmis en clair dans chaque trame et d'une clé TK (*Temporal Key*).
- CCMP (Counter-Mode/CBC-MAC), utilise l'algorithme de chiffrement AES en mode CCM et une signature MIC. Les paramètres de chiffrement (bloc initial...) sont déduits d'un compteur de 48 bits (*Packet Number*) transmis en clair dans chaque trame et d'une clé TK.

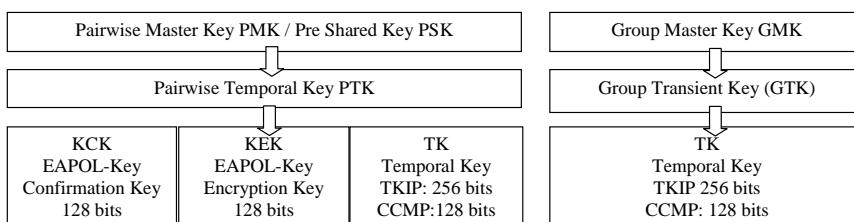


Figure 10. Hierarchy des clés 802.11i

²⁴ Wi-Fi Protected Access, Version 2.0, April 29, 2003

²⁵ Service Data Unit

Eléments d'information

Un point d'accès diffuse dans ses trames *Beacon* ou *Probe* des éléments d'information (IE, *Information Element*) afin de notifier au *Supplicant* les indications 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 inséré dans sa demande d'association.

Distribution des clés

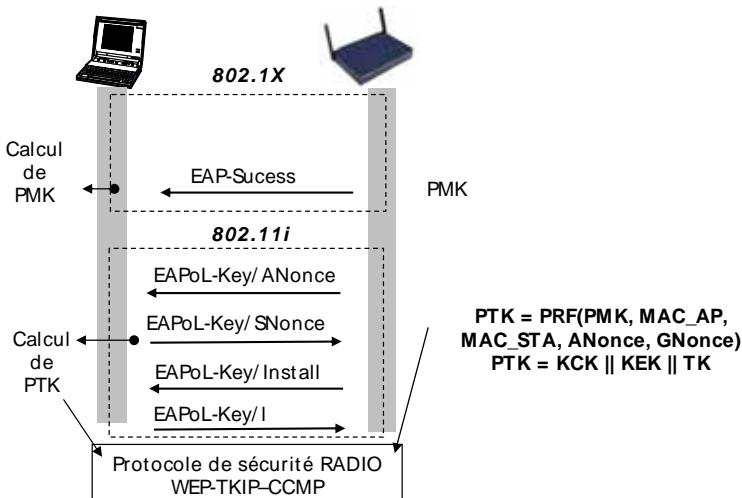


Figure 11 le protocole à quatre passes 802.11i.

A la fin de la procédure d'authentification le *Supplicant* et le serveur d'authentification partagent une clé PMK. Cette valeur est délivrée au point d'accès via le protocole RADIUS. A l'aide d'un protocole à quatre passes (*4-way Handshake*), transporté par des trames EAPoL-Key (voir figure 11) le supplicant et le point d'accès déduisent une clé PTK. Cette valeur est

calculée par la fonction PRF (*Pseudo Random Function*) avec comme arguments d'entrée des nombres aléatoires (ANonce et SNonce) fournis par le *supplicant* et le point d'accès, le secret partagé PMK et les adresses MAC du point d'accès et du *Supplicant*.

PTK= PRF(PMK, “Pairwise key expansion”, MAC_AP, MAC_STA, ANonce, SNonce)

La valeur PTK se décompose en plusieurs sous clés, KCK qui assure la signature des messages EAPoL-Key, KEK associée au chiffrement de la clé GMK, et TK utilisée pour la sécurité des trames de données.

Le point d'accès dispose d'une clé de groupe GMK. Un protocole à deux passes (*2-way handshake*) permet de délivrer la valeur GMK (chiffrée par KEK) et de déduire à l'aide d'un nombre aléatoire GNonce une clé temporaire de groupe GTK

GTK= PRF(GMK, “Group key expansion”, MAC_AP, GNonce).

Une approche verticale.

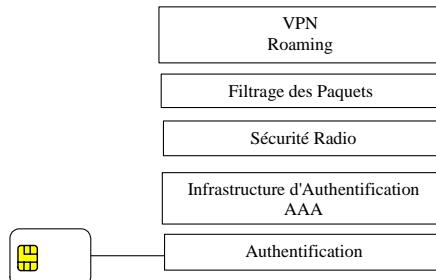


Figure 12 : Modèle à cinq couches de la sécurité des réseaux 802.11.

Nous avons récemment introduit [Urien1 et all, 2003] un modèle à cinq niveaux décrivant l'architecture de sécurité des environnements sans fil 802.11. Nous rappelons ici brièvement les éléments du modèle.

La **procédure d'authentification**. C'est la clé de voûte d'une infrastructure sécurisée. Il y a deux choix de base. 1-L'utilisateur connaît ses clés d'authentification (symétriques, asymétriques...), et les protège à l'aide de mot de passe (par exemple, de manière analogue au logiciel libre openssl une clé RSA privée est chiffrée par un triple DES, dont les clés sont déduites d'une phrase). 2-L'utilisateur ne connaît pas ses clés d'authentification qui sont la propriété du prestataire de service. Une carte à puce par exemple,

difficile à cloner, réalise après renseignement d'un code PIN, les calculs d'authentification.

L'infrastructure d'authentification. La norme 802.1x recommande l'usage de serveur RADIUS. L'authentification peut être conduite par un serveur situé dans le domaine visité ou à l'extérieur de ce dernier. De manière analogue à PGP, cette architecture établit un cercle de confiance, grâce auquel un message d'authentification est relayé par plusieurs serveurs, liés les uns aux autres par des associations de sécurité.

La sécurité radio. Elle assure la confidentialité, l'intégrité et la signature des paquets. Ces services sont délivrés par des protocoles tels que WEP ou TKIP ou CCMP normalisés par le comité IEEE 802. Ils utilisent des clés (chiffrement, signature trames), déduites d'une clé maître, au terme de la procédure d'authentification.

Le filtrage des paquets. La fiabilité de cette opération repose sur la signature des paquets (à l'aide de clés déduites de l'authentification). Grâce à ce mécanisme, les trames qui pénètrent dans le système de distribution sont sûres (pas de risque de *spoofing*), les systèmes de filtrages (point d'accès ou portail) gèrent les priviléges des paquets IP (destruction des paquets illicites) et par exemple peuvent réaliser et facturer des services de QoS.

L'accès à des services distants (*roaming*) que nous désignons génériquement sous l'appellation services VPN (Virtual Private Network). Par exemple, on mettra en oeuvre des liens sécurisés (inter domaine) à l'aide des protocoles IPSEC ou SSL.

Conclusion

Dans cet article nous avons présenté les architectures de sécurité qui sont en cours de déploiement ou de définition pour les réseaux 802.11. Compte tenu de l'engouement du marché sur l'IP sans fil, il est très probable que ces technologies deviennent des standards incontournables et jouent un rôle prépondérant dans l'informatique enfouie, qui ne pourra se développer sans normes de sécurité éprouvées.

Bibliographie

Arbaugh, W., Shankar, N. and Wan J.Y.C., "Your 802.11 Wireless Network has No Clothes", Department of Computer Science, University of Maryland, College Park, March 2001, <http://www.cs.umd.edu/~waa/wireless.pdf>.

Borisov N, GoldBerg I, Wagner D, "Intercepting Mobile Communications: The Insecurity of 802.11", Proceeding of the Eleventh Annual International Conference on Mobile Computing And Network, p180, July 16-21, 2001.

Fluhrer S, Mantin I, Shamir A, "Weakness in the key scheduling algorithm of RC4", 8th Annual Workshop on Selected Areas in Cryptography, August 2001.

IEEE Std 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", 1999.

IEEE Std 802.1X, "Standards for Local and Metropolitan Area Networks: Port Based Access Control", June 14, 2001

IEEE Std 802.11i/D5.0, "Draft Supplement to standard for Telecommunications and Information Exchange, Between Systems LAN/MAN Specific Requirements Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security", August 2003

Mishra A, Arbaugh W, "An Initial Security Analysis of the IEEE 802.1X standard". February. 2002

Urien P, Pujolle G, "Architecture sécurisée par cartes à puces, pour des réseaux sans fil sûrs et économiquement viables", GRES'2003, février 2003 Fortaleza Brésil.

Urien P, Loutrel M, "The EAP Smartcard, a tamper resistant device dedicated to 802.11 wireless networks, ASWN 2003", Third workshop on Applications and Services in Wireless Networks, Berne Suisse Juillet 2003