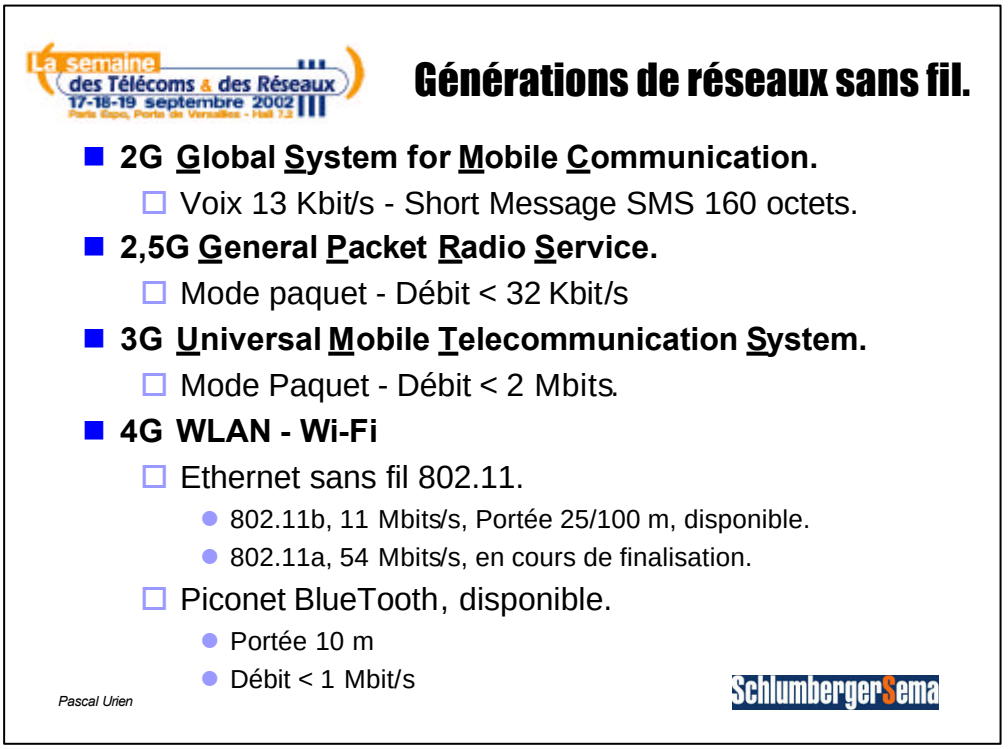
La carte WiFi,
un vecteur pour l'authentification des abonnés wireless,
et la facturation des services associés.

Pascal Urien, Directeur de Recherches SchlumbergerSema.
purien@slb.com

L'obtention de services téléphoniques ou télématiques en mode sans fil, est un besoin grandissant des utilisateurs qui désirent accéder de manière quasi permanente au réseau, sans avoir à initialiser une procédure de connexion. Le nombre de terminaux mobiles est estimé à 1 milliard d'unités en 2003 (source CISCO).



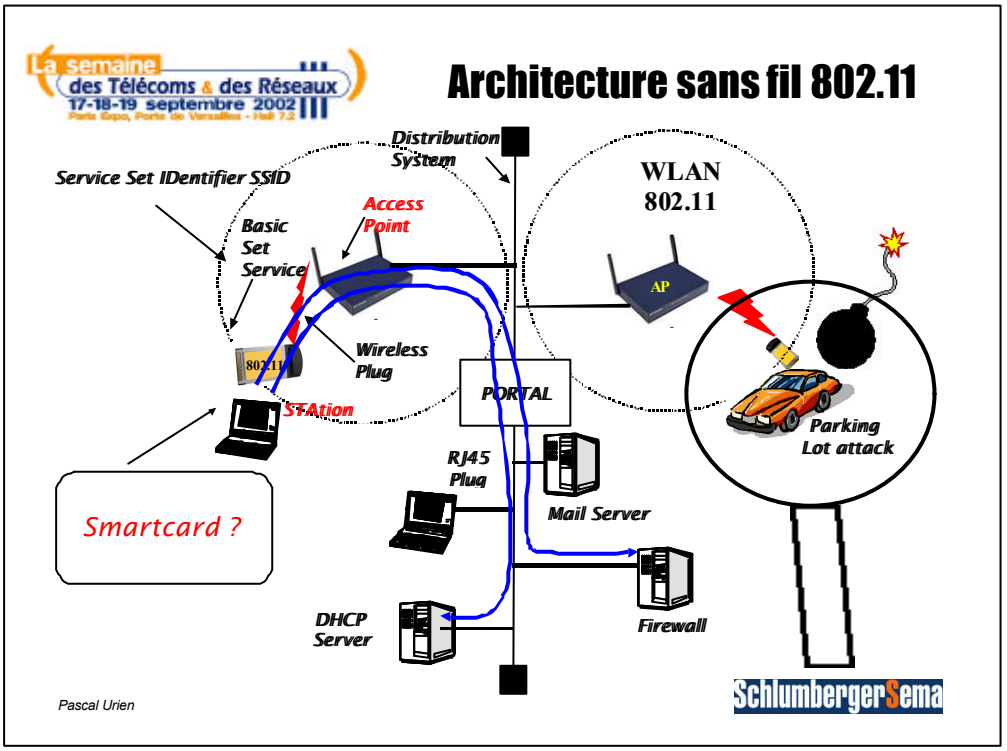
Schématiquement on peut distinguer quatre générations de réseaux mobiles,

- Le GSM, ou 2G disposant d'un canal voix de 13 kbit/s et des messages SMS de 160 octets (3,3 milliards[1] de SMS échangés en 2001 !)
- Le GPRS ou 2,5G, supportant un trafic en mode paquets de l'ordre de 32 kbit/s
- L'UMTS ou 3G, avec des débits estimés à 2 Mbits/s

[1] http://news.zdnet.fr/story/0,,t118-s2102365,00.html

- Les réseaux sans fils (4G) de moyenne (100 m, 802.11) ou faible (10 m, bluetooh) portée.

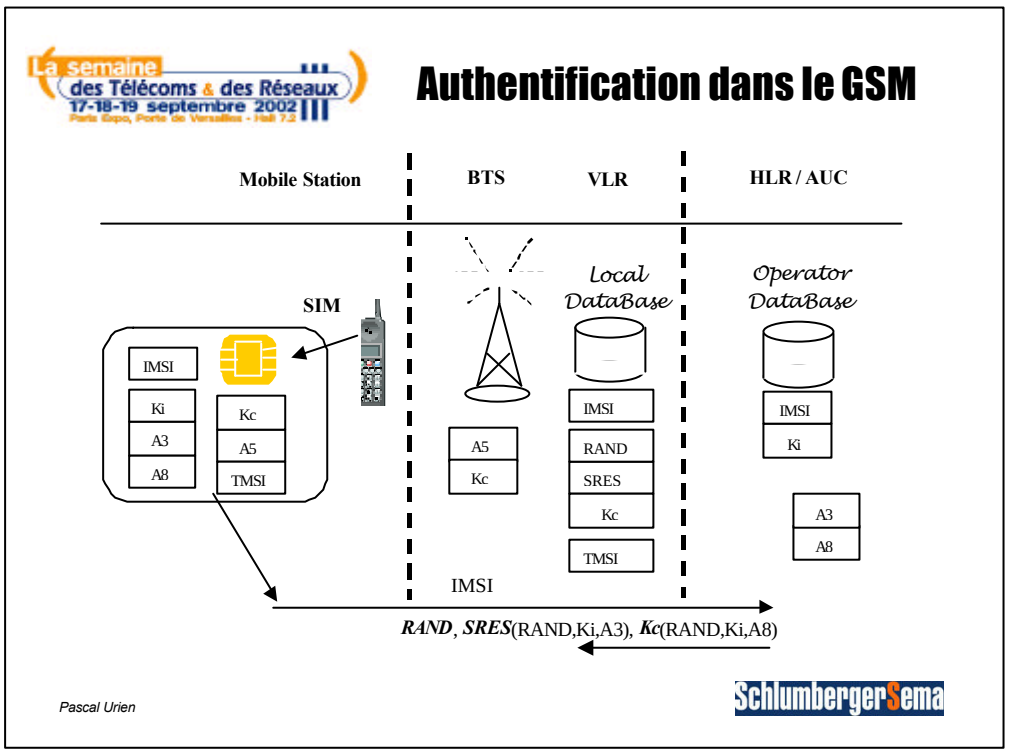
L'omniprésence d'équipements de connexion radio (WiFi, 802.11, …) intégrés prochainement à toutes les cartes mères des ordinateurs personnels (et bientôt aux puces informatiques), implique le déploiement d'architectures d'authentification dans l'internet de nouvelle génération, analogues à celles des réseaux GSM ou UMTS. Jusqu'à présent la sécurité des réseaux domotiques ou des intranets était réalisée par la restriction des accès aux personnes autorisées. A l'intérieur de l'entreprise l'usage du réseau est libre (par exemple pas d'authentification lors de l'obtention d'une adresse IP au moyen du protocole DHCP), en particulier pour permettre la connexion des ordinateurs portables.



La mise en œuvre de lien radio rend inefficace la politique traditionnelle du filtrage des entrées, puisqu'il devient possible d'accéder au réseau de l'entreprise à l'extérieur de ses locaux.

La première génération 802.11 a introduit un protocole de sécurité (WEP Wireless Equivalent Privacy) fournissant des mécanismes d'authentification (Share Key Authentication) mais également de confidentialité (chiffrement) et d'intégrité des informations échangées.

Ces fonctions utilisent un jeu de 4 clés fixes partagées entre la station et le point d'accès. Outre les faiblesses de WEP largement documentées[2] à travers le WEB, la gestion de l'authentification à partir de clés gérées par les points d'accès et les cartes WiFi est inadaptée pour des infrastructures comportant des milliers d'utilisateurs ou pour des clients de multiples réseaux (comment mettre à jour les clés ?).
Pour remédier à ces inconvénients le comité IEEE a défini la norme 801.x qui décrit une architecture centralisée, dans laquelle le processus d'authentification est réalisé entre le terminal sans fil et un serveur central, le point d'accès se comportant comme un simple relais entre ces deux entités.



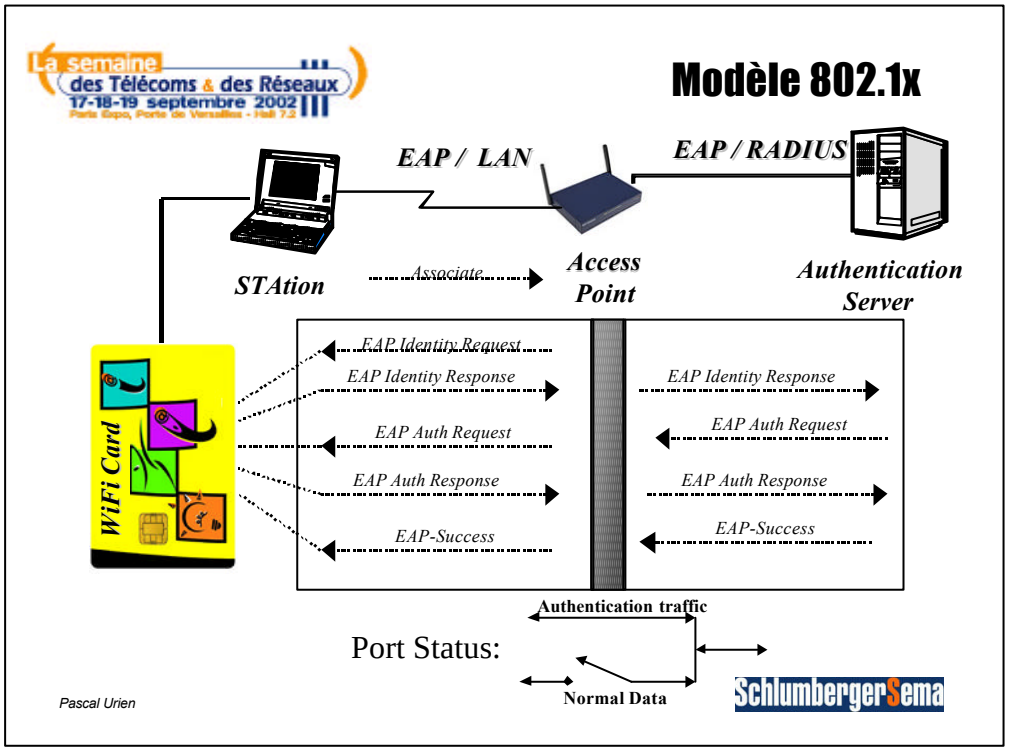
Ce schéma présente plusieurs analogies avec celui du GSM dont nous rappelons brièvement les principales caractéristiques. Le terminal stocke dans le module SIM l'identité de l'abonné (IMSI) et des procédures d'authentification. Avant d'établir une communication téléphonique il transmet son identité, via la station de base (BTS) vers le centre d'authentification de l'opérateur (AUC), qui génère alors un triplet (rand, sres, Kc) permettant d'une part à un système local (VLR) de vérifier l'identité du client (rand,sres) et d'autre part à la station de base de disposer d'une clé

[2] Revue du CNRS Sécurité Informatique n°40 juin 02 disponible en http://www.cnrs.fr/Infosecu/num40-sansFond.pdf

de chiffrement (Kc) pour le trafic vocal. L'authentification de l'abonné permet d'assurer la confidentialité des données échangées mais également d'établir ses droits et de facturer les services qu'il consomme (ce sont les fonctions AAA, Authentication Authorization Accounting en cours d'études à l'IETF).

En résumé l'architecture GSM comporte trois sous ensembles pour l'authentification,

- Le terminal muni d'une carte SIM, qui représente en fait l'opérateur.
- Un système local qui filtre/mesure les données émises par le terminal et vérifie l'identité du client.
- Un serveur central qui stocke le profil de l'abonné et réalise la facturation des services.



Le modèle 802.1x utilise également trois composants,

- Un terminal (désigné sous le terme **Supllicant**) associé à une carte réseau.
- Un système d'authentification, dit **Authenticator**, matérialisé par un point d'accès ou un HUB relié à un point d'accès. Cet élément filtre les paquets non authentifiés et peut réaliser des mesures de trafic.
- Un serveur d'authentification (**Authentication Server**) qui stocke le profil d'un utilisateur et ses paramètres d'identification. Le protocole RADIUS[3],

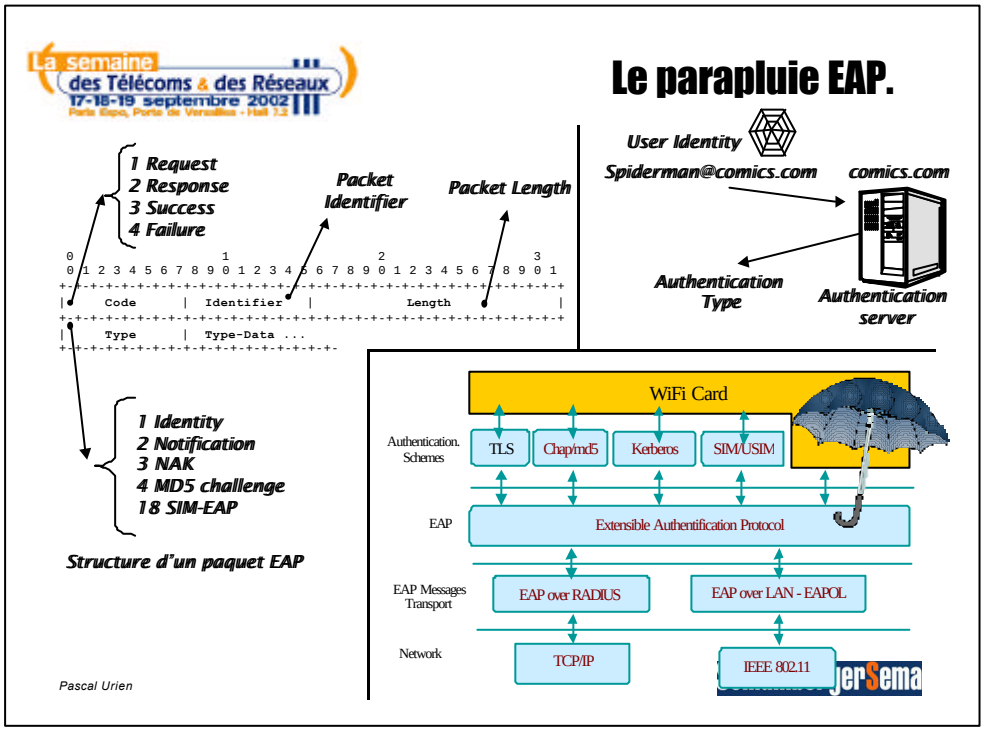
[3] "Remote Authentication Dial In User Service" rfc 2138 Avril 1997.

développé outre atlantique pour assurer une interopérabilité entre fournisseurs d'accès internet (ISP), réalise le transport des messages d'authentification.

Une des particularités de cette architecture est la mise en œuvre du protocole EAP[4] qui utilise quatre types de messages (Request, Response, Failure, Success), et supporte jusqu'à 255 méthodes d'authentification, citons par exemple,

- Un mécanisme challenge MD5, une empreinte est calculée à partir d'un nombre aléatoire et d'un secret partagé
- Le populaire protocole SSL (EAP TLS).
- Une adaptation de la version 5 du protocole Kerberos (IAKKERB).
- L'utilisation de cartes GSM SIM (EAP SIM), ou UMTS USIM (EAP AKA).

L'authentification du terminal est conduite avant l'obtention d'un adresse IP, en conséquence les paquets EAP sont acheminés par divers moyens, trames MAC (entre le terminal et AP) ou protocole routable RADIUS (entre AP et AS).



L'identité d'un utilisateur est réalisée à l'aide d'un identifiant, le NAI[5], dont la structure est analogue à celle d'une adresse de courrier électronique. La partie gauche est un login reconnu par le serveur d'authentification, dont l'adresse séparée par le caractère @, est indiquée par la partie droite.

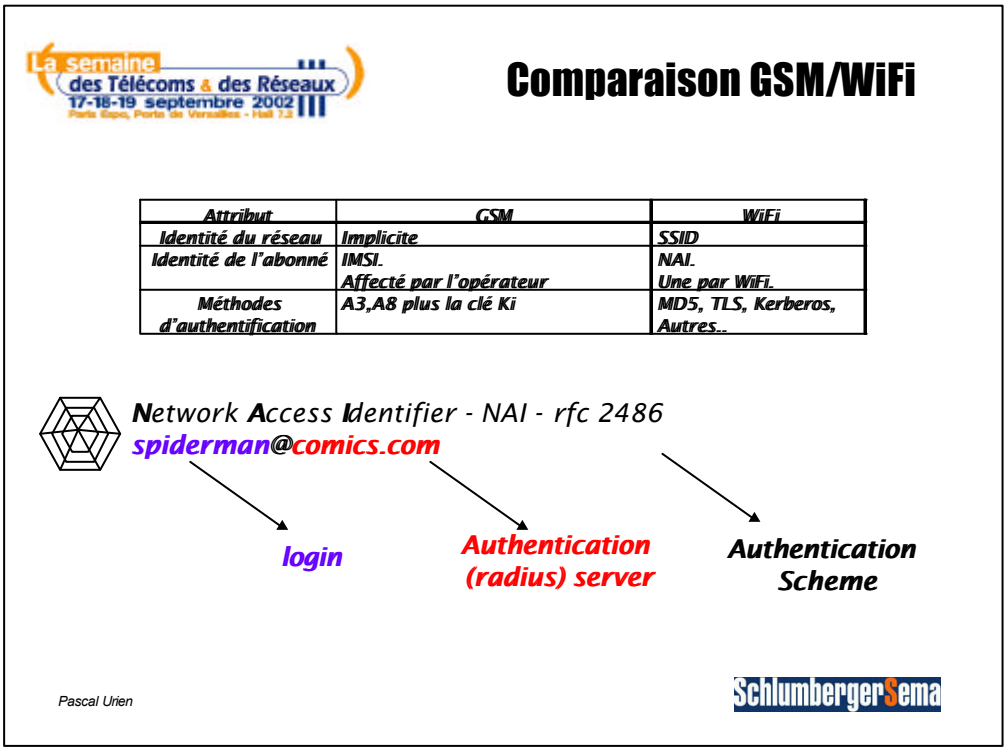
---

[4] "Extensible Authentication Protocol" rfc 2284 Mars 1998.

[5] "The Network Access Identifier" rfc 2486 Janvier 1999.

La profitabilité économique du GSM repose pour partie sur la robustesse des modules SIMs en charge de l'identification des abonnés. Parce que les ressources radio sont limitées (en comparaison des infrastructures câblées) et peuvent impliquer une gestion sécurisée des accès, nous proposons d'introduire des cartes à puces (WiFi card) dans les réseaux sans fils. Cette approche a l'avantage de reproduire le modèle éprouvé de la téléphonie mobile. Elle permettrait également d'introduire sur les réseaux de nouveaux services tels que paiements en ligne ou porte monnaie électronique.
La clé de voûte de ce concept est l'intégration du protocole EAP dans une nouvelle génération de cartes à puce. Ce protocole est déjà supporté par des comités de normalisation (IETF, IEEE…), des industriels (NOKIA, CISCO…), ou des fournisseurs de systèmes d'exploitation (Microsoft XP…).
Une rapide comparaison entre les réseaux GSM et 802.11 fait apparaître les points suivants,

- Une cellule WiFi est identifiée par un SSID, il paraît probable qu'un utilisateur accède à des services à partir de plusieurs réseaux 802.11
- Un abonné est donc associé à de multiples identités (c'est à dire des NAIs), sélectionnées en fonction du réseau visité.
- Chaque identité est authentifiée à l'aide d'un scénario particulier (GSM, Kerberos, …)

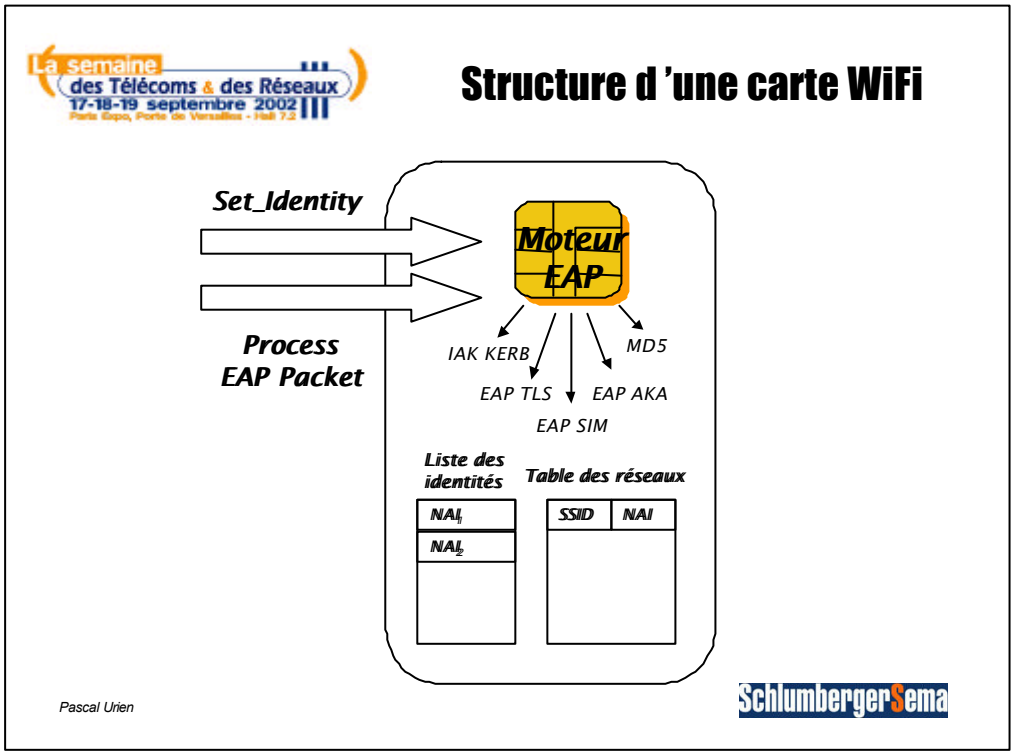


Schématiquement la structure des cartes WiFi comporte les éléments suivants,

- Une liste des identités (NAI) supportées par la carte.
- Une table optionnelle établissant une correspondance entre identifiant réseau et identifiant d'abonné.
- Une commande fixant l'identité courante de la carte.
- Une commande réalisant le traitement d'un paquet EAP et produisant la réponse associée.

Afin d'éviter un foisonnement de solutions propriétaires plusieurs initiatives de normalisation sont en cours,

- Un internet draft sera prochainement proposé à l'IETF, afin de décrire la structure des fichiers et commandes des cartes WiFi.
- Le javacard forum étudie une API EAP, destinée à faciliter le support du protocole EAP dans les cartes JAVA .



En conclusion nous soulignons que la définition de carte WiFi nous semble un prérequis pour le déploiement de service dans les environnements sans fils. L'IEEE a déjà défini les architectures matérielles indispensables à l'authentification des abonnés. Les modules WiFi permettront la diffusion de service adaptés à de telles infrastructures.