WiFi Calling :
Architecture de Réseau et de Service

EFORT
http://www.efort.com

1 Introduction

Avec l'arrivée du réseau mobile 4G qui est un réseau tout IP, les services voix/SMS ont d'abord été proposés en réutilisant le réseau circuit 2G/3G. Il s'agit de la solution Circuit Switched Fallback (CSFB). Or cette solution présente un ensemble de limitations qui militent pour offrir la voix sur IP directement depuis le réseau 4G. Il s'agit du service VoLTE successeur de CSFB. Le client peut continuer ses sessions data mobiles (sessions Internet) et en parallèle appeler ou être appelé. Le réseau cœur data mobile 4G a évolué pour supporter des accès non-3GPP de type WiFi ce qui permet à l'opérateur de densifier son réseau à moindre coût même en utilisant tout hotspot WiFi public (WiFi non trusted).
Le service WiFi Calling est certainement le principal service qui sera offert dans ce contexte d'accès WiFi connecté au réseau cœur 4G data mobile. D'ailleurs WiFi Calling et VoLTE partagent la même architecture de service, à savoir l'IMS, IP Multimedia Subsystem). Un opérateur avant le même IMS peut donc offrir les services VoLTE (Voice over IP over LTE), ViLTE (Video over IP over LTE), WiFi Calling et RCS (Rich Communication Suite).
Grâce à ce service, les utilisateurs n'auront plus à subir de restrictions en matière de voix dans les zones n'ayant pas de couverture mobile puisqu'ils peuvent désormais accéder aux services voix même à l'intérieur des bâtiments où la réception est mauvaise ou en cas de pic de trafic momentané. WiFi calling permet en effet, de faire transiter les appels vocaux mobiles par la connexion haut débit fixe via l'accès WiFi. Pour les opérateurs, cela se traduit par une diminution du taux de résiliation pour cause de couverture et capacité insuffisantes à l'intérieur des bâtiments.
Le but de ce tutoriel est de présenter l'ensemble des avantages du service WiFi calling et de montrer l'architecture associée à ce service.

2 Service WiFi Calling : Avantages

Le service WiFi Calling permet, en effet, de faire transiter les appels vocaux mobiles par la connexion haut débit fixe via l'accès WiFi. Parmi les avantages figurent :

- Appeler ou être appelé même sans couverture mobile ou lorsque la couverture mobile est de mauvaise qualité du moment qu 'une couverture WiFi est disponible.
- Client VoWiFi natif dans le terminal. Aucune application n 'est à installer. Il s'agit du même numéro MSISDN que dans le cas de la VoLTE
- Gestion de la mobilité et gestion du handover entre VoLTE et VoWiFi et vice versa. Par contre SR-VCC n 'est pas possible mais DR-VCC (Dual-Radio Voice Call Continuity) l 'est pour garantir la continuité de l'appel du monde VoWiFi au monde circuit mobile..
- Accéder à l 'ensemble des services de téléphonie, incluant les services complémentaires, le SMS, l 'USSD, l 'appel d 'urgence, les services CAMEL, le voice mail, via l 'architecture IMS commune avec VoLTE/ ViLTE.
- Remplacer la solution femtocell 3G ou 4G, à moindre coût, surtout pour les clients qui ne disposent pas de couverture mobile dans leur résidence avec l 'opérateur (C 'est la premier raison pour laquelle un client change d 'opérateur). L 'opérateur très souvent finance l 'équipement femtocell.

- Appeler avec des coûts de communication plus intéressants qu ’avec la radio mobile.

De nombreux mobiles du marché supportent déjà la fonctionnalité comme l’Iphone 5c, l’Iphone 5S, l’Iphone 6, l’Iphone 6S, le Samsung Galaxy S5, le Samsung Galaxy S6, le Samsung Galaxy S6 Edge, le Samsung Galaxy Note 4, le Sony Xperia Z3, etc.
Le fait qu ’iPhone supporte VoWiFi est un driver très important pour VoWiFi
Les premiers pays où VoWiFi sera déployé sont ceux avec une forte pénétration de smartphones et de hotsposts WiFi.

3 Architecture WiFi Calling

Pour le service WiFi Calling, les devices tels que l’Iphone avec iOS 8 considèrent toujours l ’accès WiFi comme « non-trusted » et établissent donc un tunnel Ipsec via l ’Internet public entre le device et l ’ePC d ’un opérateur mobile pour sécuriser les communications. Cela permet au device d ’utiliser n ’importe quel accès WiFi et établir et recevoir des appels et envoyer et recevoir des SMS en WiFi calling.
D ’un point de vue architectural, une entité dans le réseau ePC doit terminer le tunnel IPSec avec l’UE. Il s ’agit de l ’ePDG (Evolved Packet Data Gateway) qui partage l ’interface SWu avec l’UE. Le tunnel Ipsec est établi via l’échange de messages IKEv2 entre l’UE et l’ePDG. L’UE doit établir autant de tunnels Ipsec et d’adresses IP que d’APN qu’il souhaite activer.
Trois APNs concernent WiFi calling :

- APN IMS : via le tunnel Ipsec associé à cet APN, l’UE peut envoyer et recevoir le trafic SIP et le trafic voix sur IP.
- APN XCAP : via le tunnel Ipsec associé à cet APN, l’UE peut envoyer et recevoir des messages XCAP (XML Configuration Access Protocol) afin de configurer les données des services complémentaires.
- APN SOS : via le tunnel Ipsec associé à cet APN, l’UE peut envoyer et recevoir le trafic SIP et le trafic voix sur IP lié à un appel d’urgence.

Par ailleurs, l ’ePDG a une interface S2b afin de terminer les connectivités des usagers sur le PDN GW du réseau ePC. C ’est au niveau du PDN GW que les flux IP sont contrôlés avant d ’être délivrés au monde IP destinataire. L’interface S2b utilise le protocole de contrôle GTPv2-C pour établir/modifier/libérer des tunnels liés aux default/dedicated bearers, et le protocole du plan usager GTPv1-U permettant le transport des paquets IP sur les default et dedicated bearers.

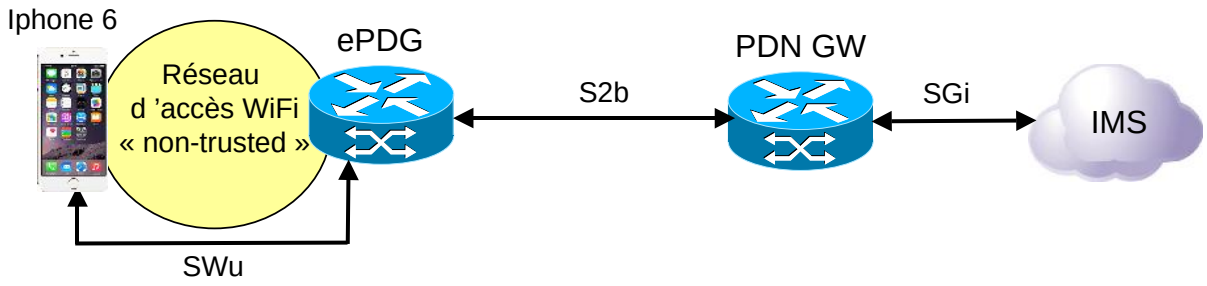


Figure 1 : Architecture d’accès WiFi untrusted à l’ePC

3.1 Architecture ePC pour un accès non-3GPP non-trusted avec S2b basé sur GTP

L ’architecture ePC permet le rattachement depuis un accès WLAN non-trusted comme le montre la figure 2. Non-trusted signifie par exemple que pour atteindre l’ePC, le réseau

d’accès non-3GPP (e.g., WiFi) utilise l’Internet. C’est le cas lorsque l’UE utilise un point d’accès WiFi dans un hotel, restaurant ou café.
Son architecture est similaire à celle de l’UMA/GAN, à savoir le déploiement d’une passerelle d’interconnexion, l ’ePDG (Evolved Packet Data Gateway).
Le mobile sous couverture WiFi établit un lien IP sécurisé avec l ’ePDG (via l’accès xDSL, FTTx ou câble) positionné directement dans le réseau cœur. L’interface utilisée est Swu basée sur IKEv2/IPSec.
Contrairement à l’UMA/GAN qui supporte indifféremment les modes "circuit" et "paquet", l ’accès non-3GPP à l ’EPC ne permet d’accéder qu’au mode "paquet". Les communications téléphoniques prise en charge par l ’opérateur ne deviennent alors possibles que grâce au déploiement d’une infrastructure de voix sur IP située dans le cœur du réseau (reposant sur le protocole SIP et l ’architecture de réseau et de services IMS).
Le 3GPP a normalisé les extensions du standard permettant un basculement des communications en cours de communication ("handover") entre un accès 3GPP et un accès non-3GPP tel que WLAN (WiFi).
A la figure ci-dessus, le 3GPP Server dispose d’une interface SWm avec l’ePDG.pour le transport sécurisé des informations d’authentification, d’autorisation et de taxation.
Pour le plan usager, les données de l’usager (flux IP) sont transmises via l’ePDG jusqu’au PGW en utilisant l’interface S2b. Comme dans le cas des accès 3GPP, le PGW sert de point d’ancrage pour le trafic de l’usager. L’interface SWm est une application DIAMETER.
L’interface S2b est basée soit sur GTPv2-C/GTP-v1U soit sur PMIP/GRE.
L’interface SWx permet au 3GPP AAA Server d’obtenir des vecteurs d’authentification ainsi que le profil non-3GPP (contenant les données de configuration de toutes les APNs autorisées pour l’UE) auprès du HSS.
L’interface S6b qui est une application DIAMETER, n’est pas utilisée lorsque les accès 3GPP s’interfacent à l’ePC. C’est l’interface S6a/S6d qui inclut alors la fonctionnalité de l’interface S6b. S6b est obligatoire lorsqu’un accès non-3GPP s’interface à l’ePC.
Lorsque l’opérateur permet l’interfonctionnement entre accès non-3GPP et ePC, le HSS doit toujours connaître les APNs actifs pour un UE donné et pour chaque APN actif, quel PDN GW termine l’APN. Ces informations sont mises à jour par le MME, le S4-SGSN et le 3GPP AAA Server auprès du HSS.
Dans le cas des accès 3GPP, c’est le MME/S4-SGSN qui interroge le DNS pour obtenir les adresses des PDN GWs candidats pour un APN à activer, puis qui choisit un PGW et qui demande l’établissement du tunnel réseau via l’interface S11/S4 au SGW qui relaie la demande au PGW via l’interface S5/S8. Enfin le MME/S4-SGSN émet une requête S6 Notify request pour informer le HSS de l’APN qui a été activé pour un UE donné, et de l’adresse du PGW qui termine cet APN.
Dans le cas de l’accès non-3GPP non-trusted, le 3GPP AAA server se contente de fournir les données de configuration d’APN à l’ePDG. L’ePDG interroge le DNS pour obtenir les adresses des PDN GWs candidats pour l’APN à activer, puis choisit un PGW et établit un tunnel réseau via l’interface S2b jusqu’au PGW. C’est le PGW qui informe le 3GPP AAA Server via l’interface S6b qu’un APN a été activé pour un UE donné et fournit son adresse de PGW qui termine cet APN. Le 3GPP AAA Server a son tour met à jour ces données auprès du HSS via l’interface SWx.

L’interface Gx entre PCEF et PCRF permet au PCEF d’obtenir des règles PCC auprès du PCRF pour l’APN activé.

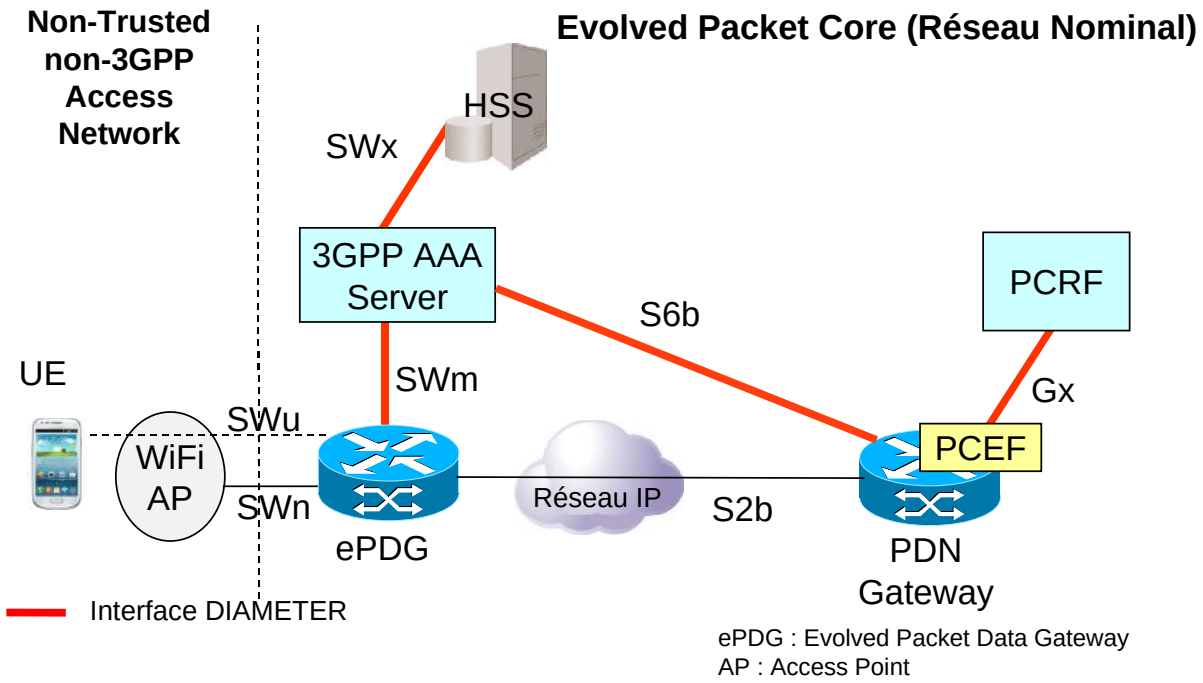
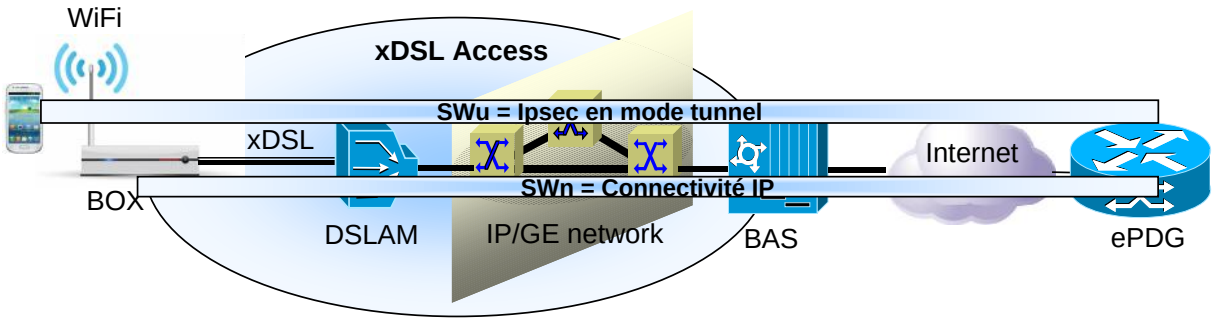


Figure 2: Architecture ePC pour un accès non-3GPP non-trusted avec S2b basé sur GTP

3.2 Accès non-3GPP non-trusted et son plan usager

La figure 3 montre un exemple d’accès non-3GPP non fiable. Il s ‘agit d’un client ayant souscrit un abonnement ADSL auprès d’un opérateur autre que son opérateur mobile. Le client dispose d’une box faisant office de point d’accès WiFi. Le trafic IP du client qui sera acheminé via cet accès non-3GPP non-fiable, doit être sécurisé entre l’UE et le point d’entrée du réseau ePC pour les accès non-3GPP non-trusted, à savoir, l’ePDG. Le client utilise donc le protocole IKEv2 pour établir un tunnel IPSec avec l’ePDG. Le trafic entre l’UE et l’ePDG est acheminé via le point d’accès WiFI typiquement dans la BOX, la paire de cuivre, le DSLAM, le backbone GE, le BAS et Internet à l’ePDG.



IAD : Integrated Access Device
DSLAM : DSL Access Multiplexer
DSL : Digital Subscriber Line
GE : Gigabit Ethernet
BAS : Broadband Access Server
ePDG : Evolved Packet Data Gateway

Figure 3 : Exemple d'accès non-3GPP non-trusted et son plan usager

3.3 Interface SWu : IPsec en mode tunnel

IPsec (Internet Protocol Security), défini par l'IETF comme un cadre de standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques, est un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP.
IPSec peut être utilisé en 2 modes différents : mode tunnel et mode transport. En Mode tunnel utilisé sur l 'interface SWu, tous les paquets IP originaux sont chiffrés/authentifiés et un nouvel en-tête IP est créé pour chaque paquet. Ce mode est utilisé pour les VPNs (Virtual Private Networks); il cache les caractéristiques du trafic.
En mode transport, l'en-tête original IP est utilisé tel qu'il est et le chiffrement concerne seulement les données du paquet IP

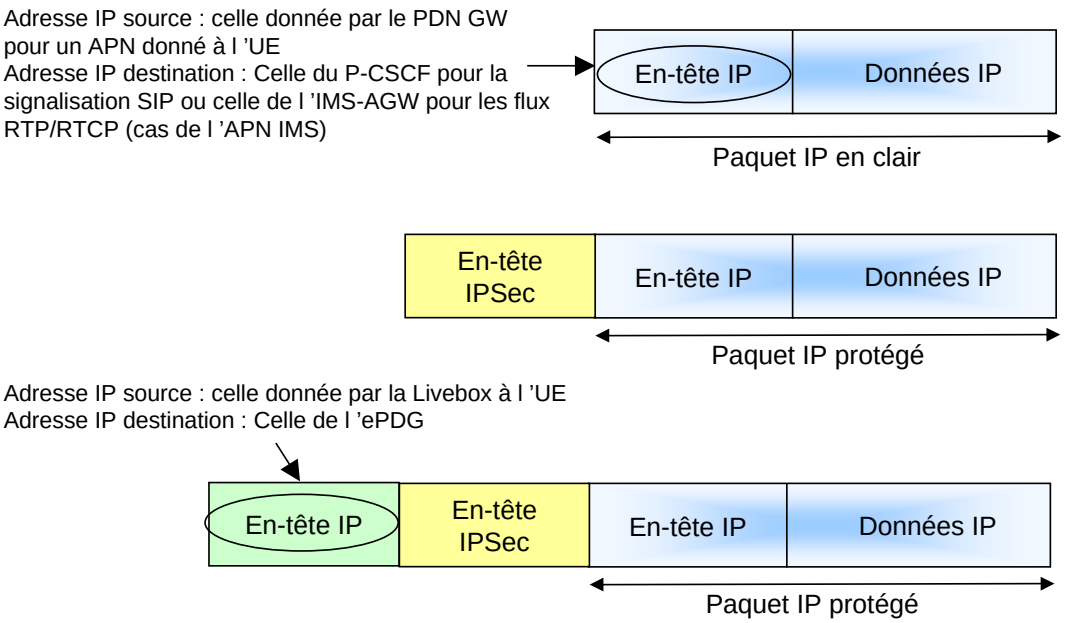


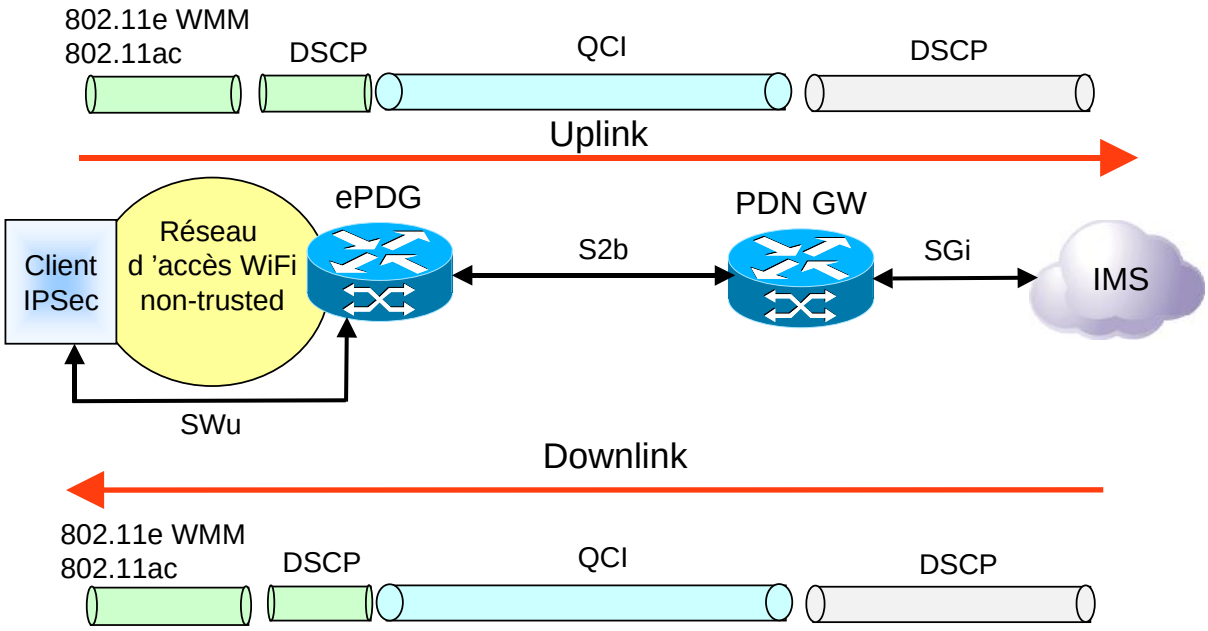
Figure 4 : Interface SWu : IPsec en mode tunnel

3.4 Qualité de service de bout en bout

La fonction Qualité de service Wi-Fi Multimedia (WMM) implantée dans 802.11e donne la priorité au trafic voix et vidéo sans fil au moyen de la liaison WiFi. La fonctionnalité Qualité de service WMM permet de donner la priorité aux paquets de données sans fil provenant de différentes applications en fonction de quatre catégories d'accès : voix, vidéo, interactive et background. Pour qu'une application bénéficie des avantages de la fonction Qualité de service WMM, cette dernière doit être activée à la fois sur l'application et sur le client qui l'exécute. Les applications propriétaires ne prenant pas le WMM en charge et les applications ne nécessitant pas la fonction Qualité de service sont assimilées à la catégorie Background, dont la priorité est inférieure à celle des catégories Voix et Vidéo. WMM est utilisé entre l 'UE et l 'AP WiFi.
Si L 'AP WiFi supporte WMM,

- il traduit WMM entre l 'UE et l 'AP en DSCP entre l 'AP et l 'ePDG pour les flux montants,
- il traduit DSCP entre l 'ePDG et le l 'AP en WMM entre l 'AP et l 'UE pour les flux descendants.

L 'ePDG traduit DSCP en QCI (Quality of Service Class Identifier) pour les flux montant et QCI en DSCP pour les flux descendants. 9 QCIs ont été définis par 3GPP. Dans le contexte VoWiFi, le defaut bearer de l 'APN IMS doit disposer d 'une QCI = 5 alors que le dedicated bearer qui transport le trafic voix sur IP a un QCI = 1. Pour un appel visio, deux dedicated bearers sont requis; l 'un pour le transport de la voix dont le QCI = 1 et l 'autre pour le transport de la vidéo dont le QCI = 2.
Le PDN GW retrouve le bearer associé au flux entrant.
Mis à part 802.11 WMM, il est aussi possible de considérer 802.11ac supporté notamment par la Livebox Play (LBv3) et la Freebox V6 Revolution. L 'Iphone 6, le Samsung Galaxy 4, le Samsung Galaxy Note par exemple le supportent aussi. Concernant cette norme WiFi ac, elle utilise exclusivement la bande des 5 GHz et s 'appuie sur la technique MIMO (Multiple Input, Multiple Output). Pour le moment, les appareils à cette norme utilisent une largeur de canal de 80 MHz mais il sera possible dans le futur d'aller jusqu'à 160 MHz pour doubler les débits. Avec un flux spatial (une antenne) en 80 MHz, on atteint déjà 433 Mbps et jusqu'à 1300 Mbps pour 3 flux spatiaux. Avec un smartphone compatible Wi-Fi 802.11ac et un unique flux spatial, le débit est pratiquement 10 fois plus élevé qu'en Wi-Fi 802.11g.



DSCP : Differentiated Services Code Point
WMM : WiFi Multi Media
QCI : Quality of Service Class Identitier

Figure 5 : QoS de bout en bout

3.5 Sessions DIAMETER après attachement de l 'UE

La figure 6 ci-dessus décrit l 'architecture de l 'accès non-3GPP non-trusted à l 'ePC. L 'UE établit un tunnel IPSec avec un ePDG auprès duquel il s 'attache; puis il est authentifié par le 3GPP AAA Server (via l 'PDG) qui a obtenu des vecteurs d 'authentification auprès du HSS. Le 3GPP AAA Server obtient ensuite auprès du HSS le profil non-3GPP de l 'usager contenant toutes les données de configuration d 'APNs autorisés. Le 3GPP AAA Server fournit à l 'ePDG les données de configuration du default APN ou de l 'APN demande par l 'UE via la signalisation IKEv2 qui permet d 'établir le tunnel IPSec, ceci, afin que l 'ePDG puisse l 'activer en établissant un tunnel réseau avec un PDN GW. C 'est l 'ePDG qui interroge le DNS pour identifier les PDN GWs candidats pour supporter l 'APN.
Un tunnel IPSec est établi et maintenu entre l 'UE et l 'ePDG.
Une session DIAMETER SWm est maintenue entre l 'ePDG et le 3GPP AAA Server tant que l 'APN est actif.
Une session DIAMETER Gx est maintenue entre le PCEF et le PCRF tant que l 'APN est actif.
Une session DIAMETER est maintenue entre le PGW et le 3GPP AAA Server tant que l 'APN est actif.
Aucune session DIAMETER n 'est maintenue entre le 3GPP AAA Server et le HSS.
Les sessions SWm et S6b seront libérées si :

- L 'UE ferme l 'APN en libérant le tunnel IPSec
- L 'UE se détache
- L 'UE réalise une mobilité de l 'accès non-3GPP à l 'accès 3GPP
- Le réseau a décidé de détacher l 'UE

La session Gx sera libérée si :

- L 'UE ferme l 'APN en libérant le tunnel IPSec
- L 'UE se détache
- Le réseau a décidé de détacher l 'UE

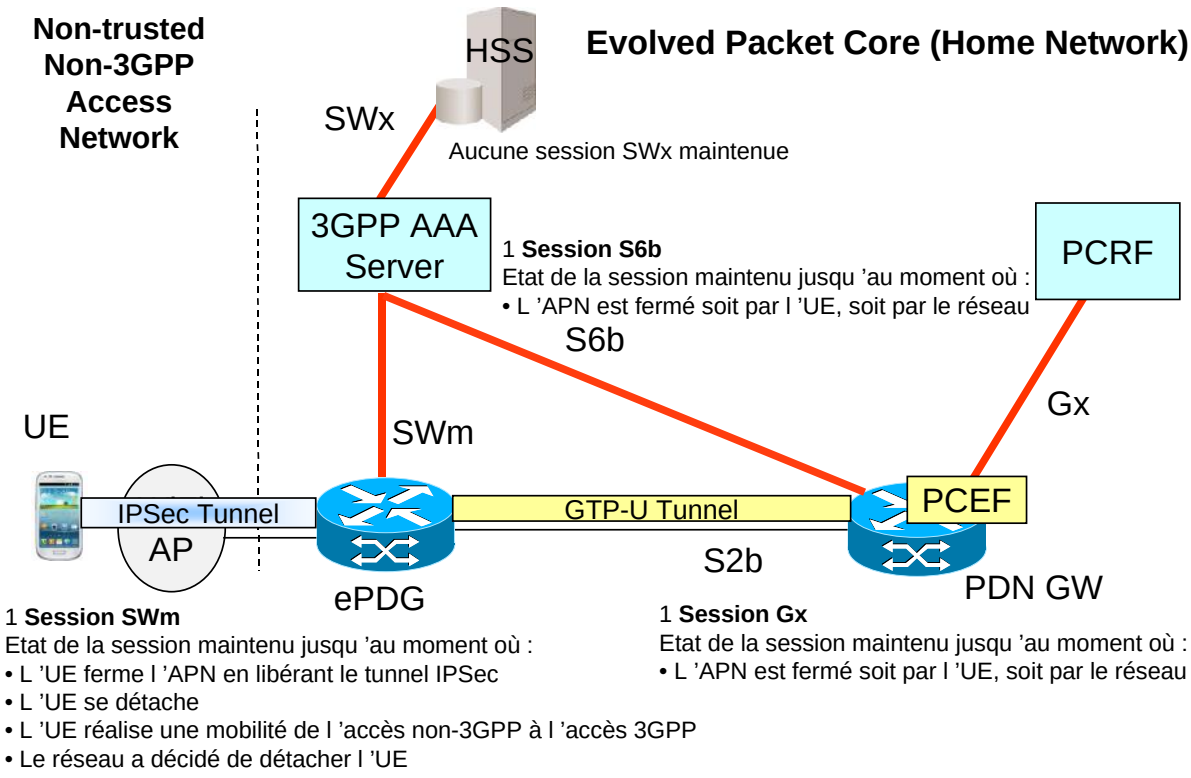


Figure 6 : Sessions DIAMETER après attachement de l 'UE

3.6 Sessions DIAMETER lorsque l 'UE active un APN supplémentaire

L 'UE décide d 'activer un autre APN. Il doit d 'abord ouvrir un second tunnel IPSec qu 'il partage avec le même ePDG. Il est alors authentifié par le 3GPP AAA Server pour le second APN a activer. Le 3GPP AAA Server fournit les données de configuration de l 'APN que l 'UE souhaite activer à l 'ePDG. Ce dernier établit un nouveau tunnel réseau avec un PDN GW. C 'est l 'ePDG qui interroge le DNS pour identifier le PGW.

Pour chaque APN actif (Figure 7) :

- Un tunnel IPSec est établi et maintenu entre l 'UE et l 'ePDG.
- Une session DIAMETER SWm est maintenue entre l 'ePDG et le 3GPP AAA Server
- Une session DIAMETER Gx est maintenue entre le PCEF et le PCRF
- Une session DIAMETER est maintenue entre le PGW et le 3GPP AAA Server
- Aucune session DIAMETER n 'est maintenue entre le 3GPP AAA Server et le HSS

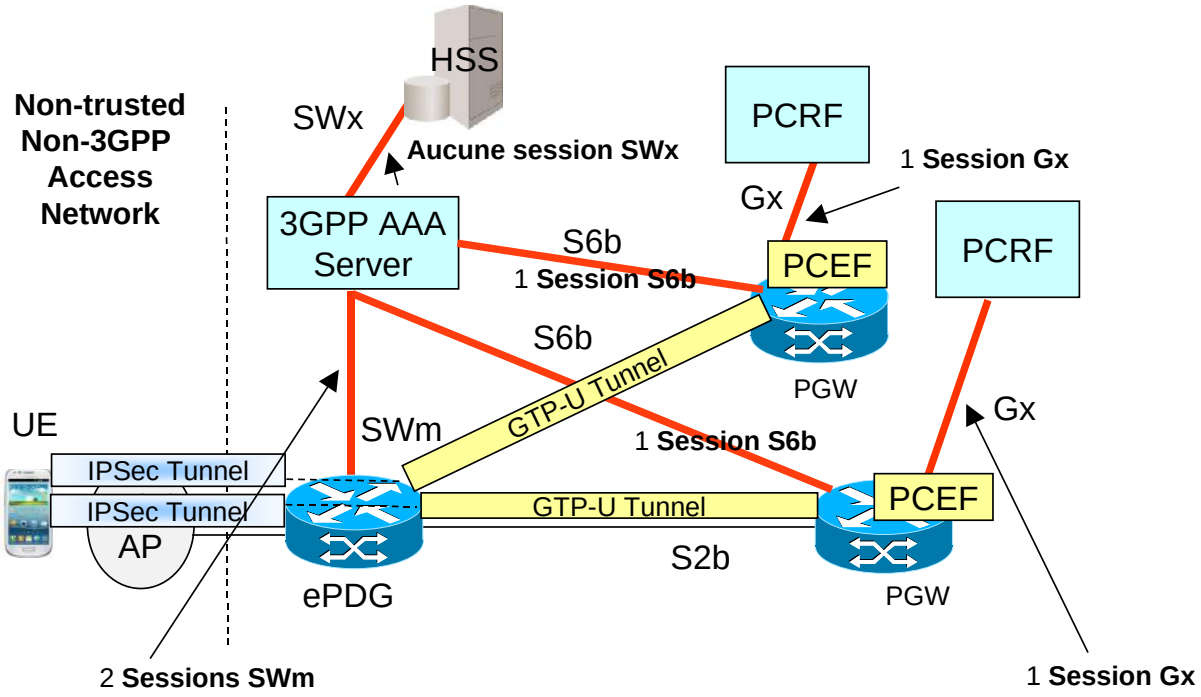


Figure 7 : Sessions DIAMETER lorsque l 'UE active un APN supplémentaire

4 WiFi calling et IMS

4.1 Enregistrement et établissement de session IMS

Une fois l'APN IMS activé, l'UE peut s'enregistrer au monde IMS.
Afin de s'enregistrer à l'IMS, l'UE doit émettre une requête SIP REGISTER à l'IMS. Le header P-Access-Network-Info doit indiquer le type d'accès (i.e., WiFi) et l'adresse MAC de l'AP WiFi (dans le champ i-wlan-node-id). Par exemple,
P-Access-Network-Info : IEEE-802.11;i-wlan-node-id="000cf1126028.
Dans le cas de l'accès LTE, l'UE s'enregistre à l'IMS en indiquant dans le header P-Access-Network-Info le type d'accès (i.e., E-UTRAN) et le numéro de cellule. Par exemple, P-Access-Network-Info : 3GPP-E-UTRAN-FDD; utran-cell-id-3gpp=208011D0FCE11.
Grâce à ce type d'information, l'opérateur peut établir des KPIs qui lui indiquent quel type de technologie d'accès a été utilisé par l'UE pour s'enregistrer.
Une fois l'UE enregistré, l'UE peut établir et recevoir des sessions IMS et d'envoyer et recevoir des SMS.
Dans le cas de WiFi Calling, des ressources additionnelles sont réservées entre l'ePDG et le PDN GW pour le transport de la voix sur IP. En effet, en plus du tunnel réseau entre l'ePDG et le PDN GW qui transporte le trafic SIP, il s'agit d'établir un tunnel réseau supplémentaire pour le transport de la voix sur IP sous forme de flux RTP. Ces deux tunnels sont associés à la même adresse IP de l'UE et au même APN IMS. Par contre entre l'UE et l'ePDG, le même tunnel IPSec est utilisé pour le transport de la signalisation SIP et le transport de la voix sur IP (flux RTP).

Dans le contexte VoLTE, il s'agit de réserver des tunnels différents entre l'UE et le Serving GW pour le transport de la signalisation SIP et de la voix sur IP, et des tunnels différents entre le Serving GW et le PDN GW pour le transport de la signalisation SIP et de la voix sur IP.

4.2 Services IMS pour WiFi Calling

WiFi Calling tout comme VoLTE en utilisant l'IMS doivent émuler les services du domaine circuit actuel et doivent donc fournir les services suivants :

- Les services complémentaires de la téléphonie (renvoi d 'appel, présentation du numéro, transfert d 'appel, signal d 'appel, restriction de la présentation du numéro, etc), incluant l 'USSD. Les services complémentaires et les services USSD sont mis en œuvre via le serveur d 'application MTAS (Multimedia Telephony Application Server)
- Le service SMS qui est mis en œuvre via un serveur d 'application appelé IP-SM-GW (IP Short Message Gateway) qui est un gateway de signalisation entre SIP et MAP et permet donc de relayer les SMS du monde IMS vers le SMSC ainsi réutilisant l 'architecture SMS existante.
- Les services CAMEL (prépayé, réseau privé virutel, etc). Les services CAMEL existants sont réutilisés en mettant en oeuvre un serveur d 'application appelé IM-SSF (IMS Service Switching Function) qui est un gateway de signalisation entre SIP et CAP relayant ainsi les appels aux plate-formes de service CAMEL existantes.
- Le service de continuité d 'appel si l 'usager perd la couverture WiFi pendant sa communication et ne peut basuler que sur la couverture 2G/3G. En effet, en 2G et 3G, c 'est le domaine circuit et le MSC Server qui prend en charge l 'appel. Le service de continuité d 'appel est mis en œuvre via un serveur d 'application appelé SCC (Service Centralization and Continuity) et le service associée s'appelle DR-VCC (Dual Radio Voice Call Continuity). Dans le cas de la VoLTE, le service s'appelle SR-VCC (Single Radio Voice Call Continuity).

La formation EFORT « Architectures d'Accès WiFi à l'ePC et Service VoWiFi Associé » fournit toutes les clés de compréhension du service WiFi calling, de son architecture et de sa mise en œuvre avec l'IMS.
http://efort.com/index.php?PageID=21&l=fr&f_id=180&imageField.x=1&imageField.y=3