Accès Non-3GPP à l'ePC
Architecture et Interfaces

EFORT
http://www.efort.com

Le but de ce tutoriel est de présenter l'interfonctionnement entre WLAN (accès non 3GPP) au réseau cœur paquet 4G appelé Evolved Packet Core (ePC). L'offload du trafic de l'accès mobile à WiFi en est une des principales raisons. L'offload vise à décharger une partie du trafic de données des utilisateurs du réseau mobile de l'opérateur sur un réseau filaire via les cellules WiFi. Ce détournement du signal vise à répondre à la demande exponentiellement croissante de consommation de l'Internet mobile. Par ailleurs cette solution permet l'authentification par l'opérateur mobile du client WiFi qui permet à ce dernier d'accéder à ses services mobiles depuis l'accès WiFi (TV mobile, MMS, voix sur IP avec IMS, RCS, etc.). Enfin la gestion de la mobilité 4G/WiFi est prise en compte ce qui permet au client de conserver son adresse IP et donc ses sessions de données en changeant de technologie d'accès. Le tutoriel décrit les architectures d'interfonctionnement entre accès non 3GPP (e.g., WLAN) fiable ou non fiables et le réseau ePC ainsi que les interfaces associées.

1 Comportement de l'UE vis à vis des accès non-3GPP

Lorsqu'un opérateur recherche une solution d'offload data des accès 3GPP (e.g. 2G, 3G/3G+ et LTE), les réseaux d'accès WLAN sont souvent utilisés comme alternative. L'interfonctionnement entre les accès non-3GPP tels que WLAN et le réseau cœur ePC a été défini dés le départ dans la Release R8 3GPP ainsi que la mobilité et la continuité de session data mobile entre accès non-3GPP et accès 3GPP. Par contre la R8 ne permet à l'UE de n'être actif que sur un accès à la fois, soit l'accès 3GPP, soit l'accès non-3GPP tel que WLAN afin d'offrir la continuité de session. Par ailleurs, en R8, si le terminal est connecté via WLAN, le trafic est toujours routé via le PDN GW dans l'ePC. Il est possible que l'UE soit directement connecté via WLAN à Internet par exemple, mais ce type de mode de fonctionnement sorte du cadre des spécifications R8.
Depuis la R10, 3GPP définit les mécanismes permettant la connexion simultanée sur plusieurs accès. Par ailleurs la R10 spécifie explicitement le cas où le terminal se connecte via l'accès WLAN et route son trafic directement sans traverser l'ePC.
Une connectivité multi-accès en R10 peut être fournie selon trois modes de fonctionnement :

- **MAPCON (Multi-access PDN Connectivity)** : L'UE peut disposer d'une ou plusieurs connexions PDN sur l'accès 3GPP et une ou plusieurs connexions PDN sur l'accès non-3GPP. La mobilité de chaque connexion PDN entre l'accès 3GPP et l'accès non-3GPP est aussi supportée.
- **IFOM (IP Flow Mobility)** : L'UE a la capacité à disposer d'une connexion PDN sur les deux accès 3GPP et non-3GPP simultanément et à choisir via quel accès router chaque flux IP individuellement. La mobilité pour chaque flux IP entre les accès 3GPP et non-3GPP est supportée.
- **NSWO (Non-seamless WLAN offload)** : Il s'agit de la capacité de router un trafic sur l'accès non-3GPP (e.g., WLAN) sans traverser l'ePC. Les flux ne sont donc pas ancrés sur un PDN GW de l'ePC. La mobilité (continuité de session IP) entre WLAN et 3GPP n'est pas supportée.

1.1 MAPCON

Un UE disposant de la capacité MAPCON est un UE capable de transférer et recevoir des flux sur différentes connexions PDN actives simultanément sur différents réseaux d'accès.

Dans un but d'utiliser MAPCON, l'UE doit essayer de se connecter à différentes APNs simultanément via différents réseaux d'accès uniquement si le réseau supporte ces connectivités simultanées. L'UE détermine si le réseau supporte MAPCON si l'UE est provisionné avec cette information ou a reçu des politiques de routage inter système par APN via l'ANDSF (cf. 1.4).
Dans l'exemple de la figure 1, l'UE établit la connexion PDN pour l'APN Internet via l'accès non-3GPP (WLAN) et la connexion PDN pour l'APN IMS via l'accès 3GPP (LTE).

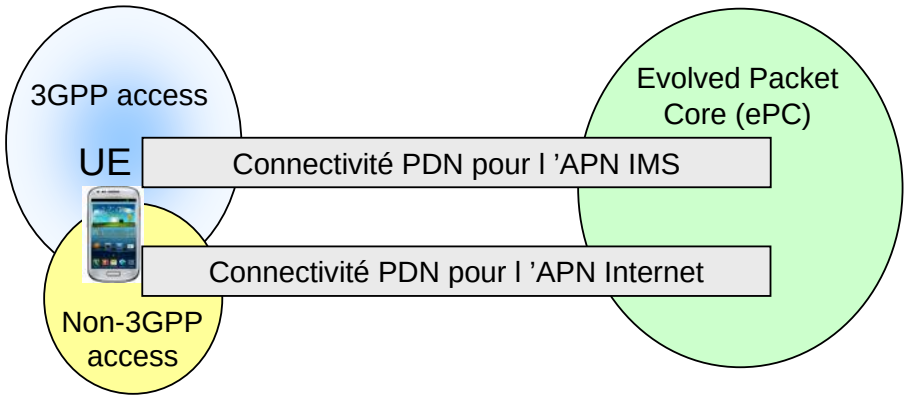


Figure 1 : Mode de fonctionnement MAPCON

1.2 IFOM

Un usager dispose d'une session multimédia avec un correspondant. Il s'agit d'une session de visiophonie constituée de deux flux IP, flux audio conversationnel et flux vidéo conversationnel. Pendant cette session multimédia, l'usager navigue sur le WEB (QoS best effort) et regarde occasionnellement des vidéos (QoS streaming). Plus tard pendant la session multimédia, l'usager initie une session FTP avec un serveur de sauvegarde (QoS best effort). Sur la base de politiques d'opérateur via la fonction ANDSF (cf. 1.4), les flux audio et vidéo conversationnels sont routés via l'accès 3GPP alors que les flux de streaming vidéos, WEB et FTP sont routés via l'accès non-3GPP.
Avec IFOM, si l'UE est sous couverture des deux accès 3GPP et non-3GPP, il doit être possible pour l'UE de communiquer via les différents accès simultanément pour une même connexion PDN; bien entendu, l'UE doit est autorisé par souscription à avoir un comportement relatif à la méthode IFOM. Il est possible de distribuer les flux vers/à partir de l'UE entre les différents accès disponibles sur la base des caractéristiques des flux IP et les capacités des accès disponibles, grâce aux préférences de l'usager et les politiques opérateur.
Par exemple, lorsque les deux accès 3GPP et WLAN sont disponibles, les flux IP dont les exigence de QoS sont fortes ne sont pas routés sur l'accès WLAN, afin d'éviter toute perte de service. L'opérateur doit pouvoir définir des politiques pour le contrôle et le routage des flux IP entre les accès disponibles. Chaque politique doit inclure une liste d'accès préférés.

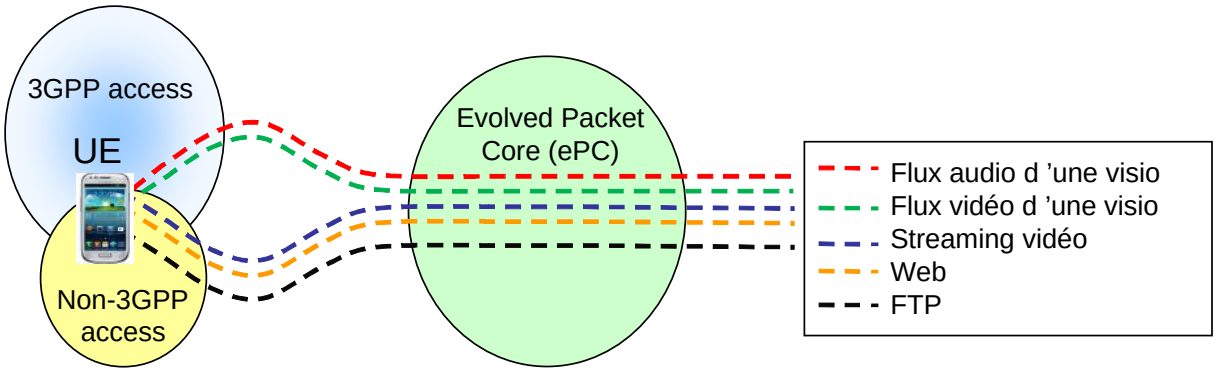


Figure 2 : Mode de fonctionnement IFOM

1.3 NSWO

NSWO (Non-seamless WLAN offload) est une capacité optionnelle d'un UE à être connecté sur les accès WLAN et 3GPP simultanément et router des flux IP spécifiques via l'accès WLAN sans traverser l'ePC. Ces flux IP sont identifiés via des préférences usagers et via des politiques qui peuvent être pré-configurées statiquement par l'opérateur sur l'UE ou dynamiquement positionnées par l'opérateur via la fonction ANDSF (Access Network discovery and Selection Function) (cf. 1.4). Pour ces flux IP, l'UE utilise l'adresse IP locale allouée par le réseau d'accès WLAN. La préservation de cette adresse IP n'est pas possible entre les accès WLAN et 3GPP.

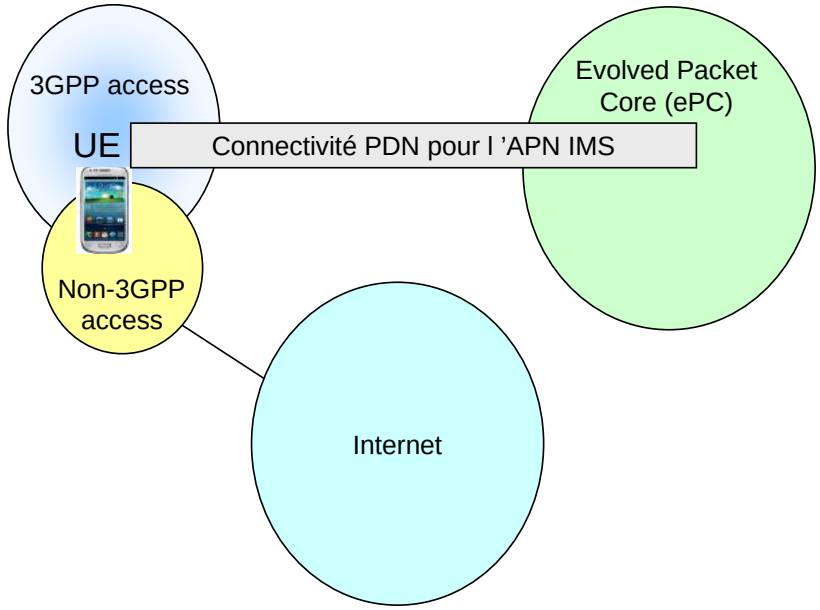


Figure 3 : Mode de fonctionnement NSWO

1.4 ANDSF

La fonction ANDSF (Access Network Discovery and Selection Function) est une fonction intelligente de sélection entre accès 3GPP et accès non-3GPP. L'ANDSF est une entité de réseau optionnelle. Elle fournit des informations utiles à l'UE et notamment les politiques définies par l'opérateur afin de guider les décisions de sélection de réseau.
L'ANDSF est localisée dans le réseau de l'opérateur en tant qu'entité indépendante et dispose d'une interface unique S14 afin de fournir à l'UE les information de sélection de réseau et les politiques associées.

Les informations fournies par l'ANSDF peuvent l'être en mode push ou pull. L'UE peut soumettre une demande à l'ANDSF et recevoir en retour les informations correspondantes (mode pull) ou l'ANDSF de son propre chef pousse les informations aux UEs concernés (mode push). Ces informations et politiques fournies par l'ANDSF sont utilisées par l'UE pour découvrir les réseaux dans son voisinage qui sont disponibles (incluant les réseaux non-3GPP) et pour comprendre comment ces réseaux doivent être priorisés par l'UE dans les décisions de sélection de réseau (e.g., quand, où , et pour quel trafic IP un SSID WiFi doit être préféré à un accès 3GPP).

2 Architecture ePC pour un accès non-3GPP non-fiable

L 'architecture ePC permet le rattachement depuis un accès WLAN non fiable (untrusted) comme le montre la figure 4. Non-fiable signifie par exemple que pour atteindre l'ePC, le réseaux d'accès non-3GPP 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 coeur. 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 par exemple sur le protocole SIP, voire sur l'architecture 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 4, 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 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 actives pour un UE et pour chaque APN active 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 PGW 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 PGW 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 (Policy and Charging Control) auprès du PCRF pour l'APN activé. Ces règles permettront au PCEF de contrôler les différents flux IP envoyés et reçus par l'UE dans un but de policy and charging control.

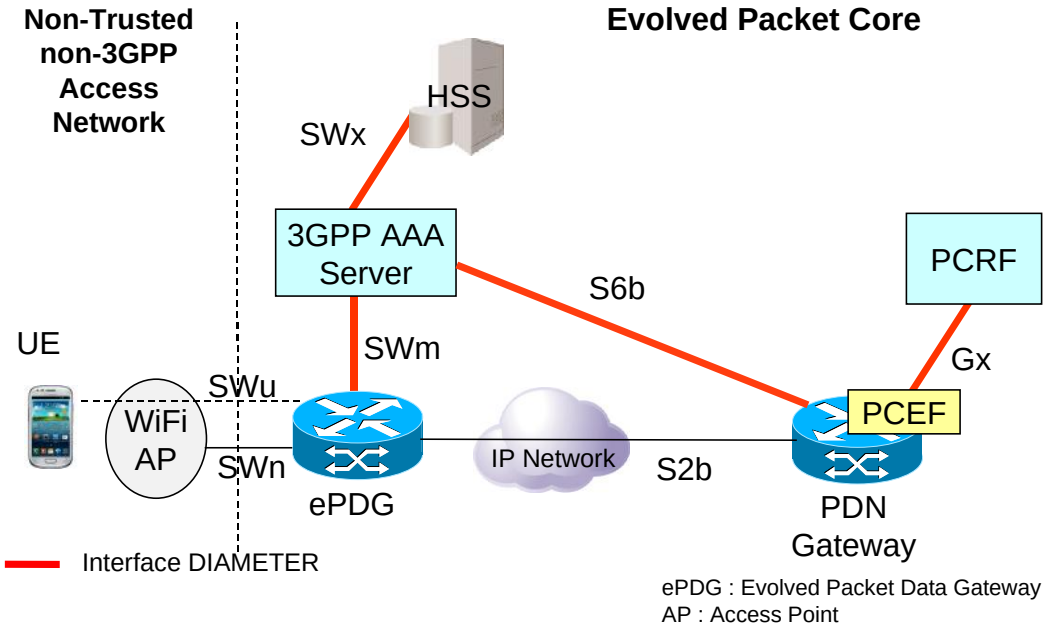
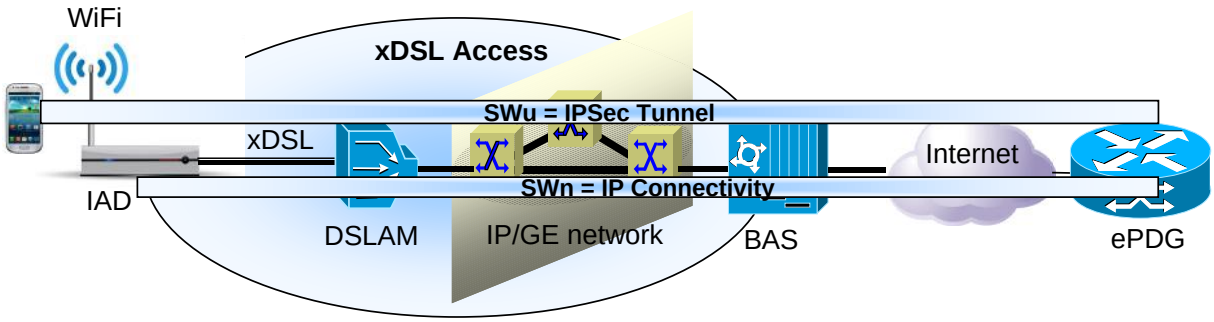


Figure 4 : Architecture ePC pour un accès non-3GPP non-fiable

La figure 5 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-fiable, 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, 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 5 : Exemple d'accès non-3GPP non-fiable avec son plan usager

3 Architecture ePC pour un accès non-3GPP fiable

L'architecture réseau fournissant la connectivité IP à l'ePC en utilisant un accès de type non-3GPP trusted, e.g., un accès WLAN typiquement contrôlé par l'opérateur mobile lui-même est décrite à la figure 6.

Le 3GPP Server dispose d'une interface STa avec le réseau d'accès trusted (TWAN, Trusted Wireless Access Network) pour le transport sécurisé des informations d'authentification, d'autorisation et de taxation.

Pour le plan usager, les données de l(usager sont transmises via le TWAN jusqu'au PGW en utilisant l'interface S2a. Comme dans le cas des accès 3GPP, le PGW sert de point d'ancrage pour le trafic de l'uager. L'interface STa est une application DIAMETER. L'interface S2a 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.

Comme dans le cas de l'accès non-3GPP non-trusted, l'interface S6b est présente entre le PGW et le 3GPP AAA Server.

Les fonctions de l 'entité TWAN sont décrites à la figure 7. Il s'agit de :

- Un réseau d 'accès (WLAN Access Network) qui inclut un ensemble de points d 'accès (AP) WLAN.
- Une entité Trusted WLAN Access Gateway (TWAG) qui termine l 'interface S2a avec le PGW. Elle termine aussi une connexion logique point à point avec l 'UE via le réseau d 'accès WLAN permettant l 'échange des flux IP sortant et entrants de l 'UE.
- Une entité Trusted WLAN AAA Peer (TWAP) qui termine l 'interface STa avec le 3GPP AAA Server. Toutes les données d 'authentification sont échangées entre l 'UE et le 3GPP AAA Server via l 'entité TWAP. Par ailleurs, l 'entité TWAP obtient du 3GPP AAA Server toutes les données de configuration des APNs souscrites par l 'UE.

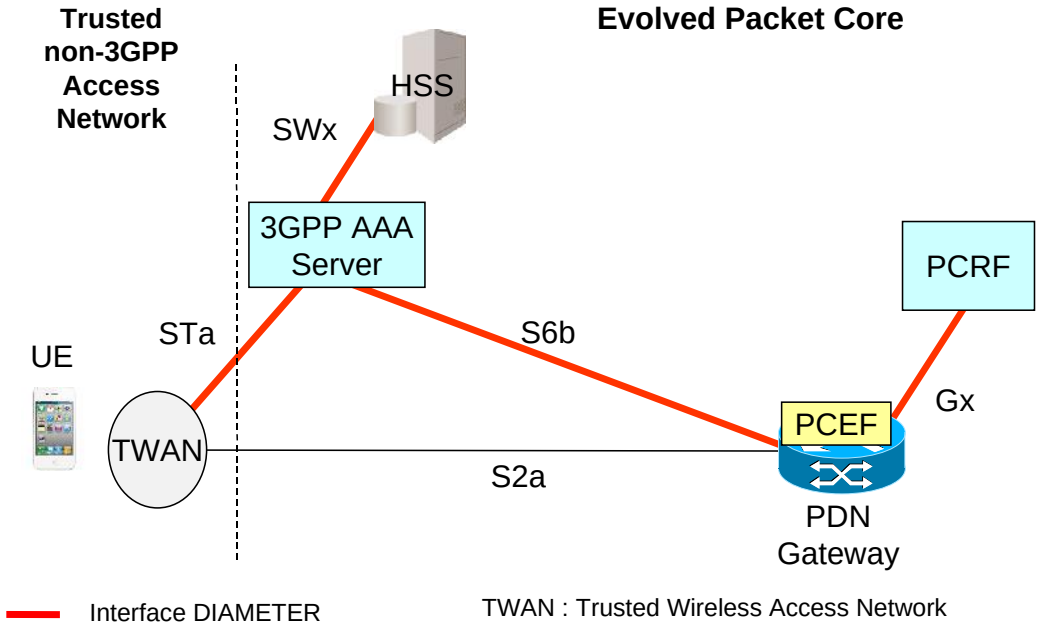


Figure 6 : Architecture ePC pour un accès non-3GPP fiable

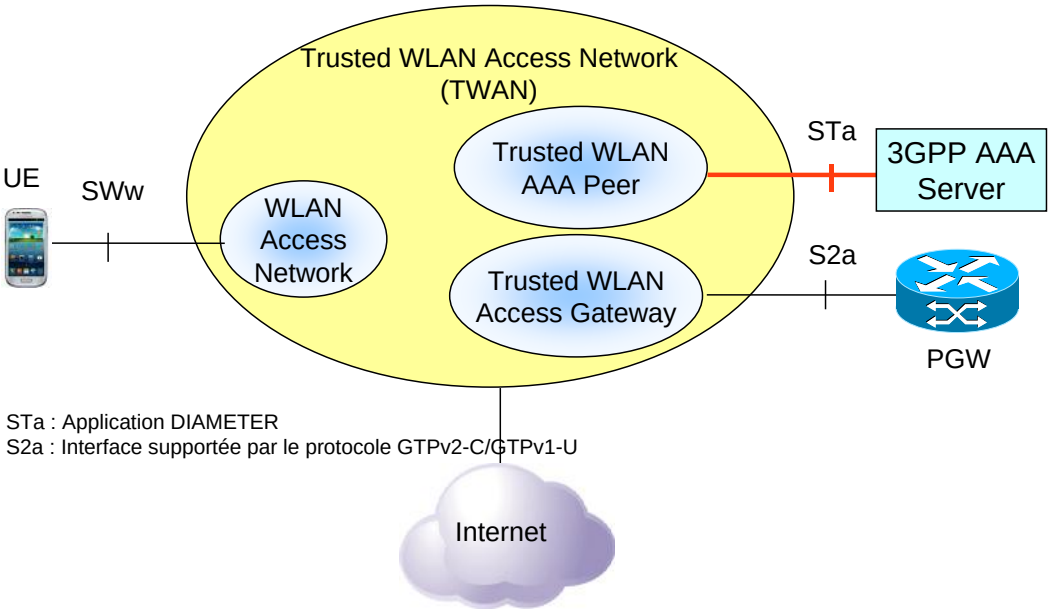


Figure 7 : Fonctions de l'entité TWAN

Références

3GPP TS 29.273, Evolved Packet System (EPS); 3GPP EPS AAA interfaces.

3GPP TS 24.302, Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3.

3GPP TR 23.852, Study on S2a Mobility based on GPRS Tunnelling Protocol (GTP) and Wireless Local Area Network (WLAN) access to the Enhanced Packet Core (EPC) network.

3GPP TR 23.861, Network based IP flow mobility.

3GPP TS 23.401, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.

3GPP TS 33.402, Security aspects of non-3GPP accesses.

3GPP TS 24.234, WLAN User Equipment (WLAN UE) to network protocols; Stage 3.

3GPP TS 23.327, Mobility between 3GPP-Wireless Local Area Network (WLAN) interworking and 3GPP systems.

La formation EFORT « Accès non-3GPP à l'ePC, Scénarii, architectures, interfaces et services associés » fournit toutes les clés de compréhension de l'interfonctionnement des accès non-3GPP (e.g., WLAN) à l'ePC dans un but d'offload de la data mobile.

http://efort.com/index.php?PageID=21&l=fr&f_id=108&imageField.x=5&imageField.y=6