5GC versus EPC

EFORT
http://www.efort.com

1. Introduction

Les réseaux cœur 4G et 5G doivent prendre en charge différentes fonctionnalités réseau telles que la gestion de la mobilité, la gestion de session, la gestion du SMS, la gestion de l'authentification, la gestion du routage/transfert des paquets IP du client, etc. L'architecture réseau EPC consistes en des entités de réseau où chaque entité de réseau gère une ou plusieurs fonctionnalités réseau. Les deux protocoles de signalisation utilisés par l'EPC sont DIAMETER pour les procédures AAA (Authentication, Authorization, Account) et GTPv2-C pour la gestion de session (établissement/libération de connexions PDN). L'architecture de réseau 5GC déployée dans un monde cloud telco consiste en des NFs virtualisées (Network Functions) élémentaires qui ne prennent en charge chacune qu'une seule fonctionnalité réseau. L'application 5GC se compose donc de petits services indépendants (appelés microservices dans le monde du cloud) qui communiquent entre eux via des APIs bien définies basées sur le protocole de signalisation HTTP/2. Le but de ce tutoriel est de décrire les entités de réseau EPC et les fonctions de réseau 5GC et le mapping entre ces entités et fonctions. Ce tutoriel considère que le lecteur connait l'architecture générale du réseau EPC. Le détail de l'architecture EPC est décrit dans plusieurs tutoriels EFORT disponibles à l'URL http://efort.com/index.php?PageID=5&l=fr

.

2. Réseau cœur 5G

La figure 1 montre l'architecture de haut niveau qui peut être utilisée comme modèle de référence pour le système 5G (5GS). Sont décrits les éléments UE, Réseau d 'accès, Réseau cœur 5G (5GC) et leurs points de référence.
N2: Point de référence pour le plan de contrôle entre le réseau d'accès et le réseau cœur 5G.
N3: Point de référence pour le plan usager entre le réseau d'accès et le réseau cœur 5G.
N1: Point de référence pour le plan de contrôle entre l'UE et le réseau cœur 5G.
N6: C'est le point de référence entre le réseau cœur 5G et le réseau de données (PDN, Packet data Network). Le réseau de données peut être un réseau de données public ou privé externe d'opérateur ou un réseau de données intra-opérateur, e.g., pour la fourniture de services IMS. Ce point de référence correspond à SGi dans le contexte EPC.

L 'UE ne peut dialoguer avec le 5GC que s 'il supporte le protocole NAS (Non-Access Stratum) N1.

Les RANs (Rado Access Networks) ne peuvent dialoguer avec le réseau cœur 5G (5GC) que s 'ils supportent les interfaces N2 (Plan contrôle) et N3 (Plan usager).
Les radios autorisées à s 'interfacer au 5GC sont LTE et ses évolutions (LTE-Advanced), New Radio 5G, WiFi (aussi bien WiFi trusted que WiFi untrusted). Les accès fixes peuvent aussi s 'interface au 5GC.
Dans le cas de l 'accès WiFi untrusted, un élément d 'interfonctionnement a été spécifié appelé N3IWF (Non-3GPP Interworking Function).
Dans le cas de l 'accès WiFi trusted, un élément d 'interfonctionnement a été spécifié appelé TNGF (Trusted Non-3GPP Gateway Function).
Dans le cas du réseaux d 'accès fixe tel que xDSL, FTTx ou câble, un élément d 'interfonctionnement a été spécifié et appelé W-AGF (Wireline Access Gateway Function).

Le réseau 5GC donne accès à des réseaux externes IP (e.g., Internet, Intranet, IMS) appelés Data Networks.
L'un des premiers drivers clés de la nouvelle architecture de réseau cœur 5G et des principes associés d'indépendance des technologies d'accès étaient de faire converger les opérations pour les différents types de technologies. Cela signifie qu'un fournisseur de services qui propose à la fois les services fixes et mobiles à ses clients pourrait à l'avenir faire appel à une seule équipe opérationnelle, un ensemble uniforme de solutions d'infrastructure et des processus opérationnels identiques dans les différentes offres de services. Si cela se produit, cela signifierait que le concept de «convergence fixe-mobile» serait enfin une réalité, souhait depuis longtemps des grands opérateurs de service pour réduire les CAPEX et OPEX.

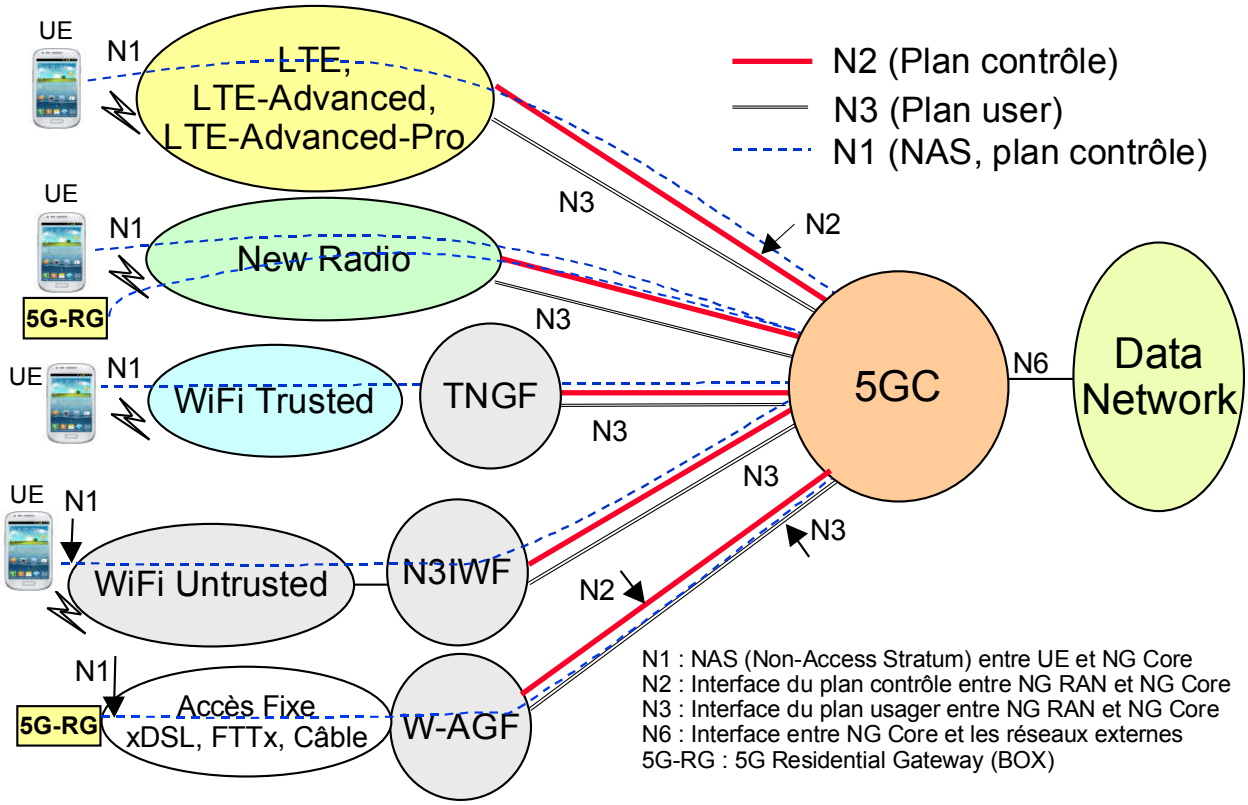


Figure 1 : Architecture du système 5G à un haut niveau

Pour les accès WiFi et les accès fixes, il est nécessaire de mettre en œuvre dans le réseau d 'accès des fonctions d 'interfonctionnement capables de supporter les interfaces de plan contrôle et de plan usager requises par le cœur de réseau 5G :

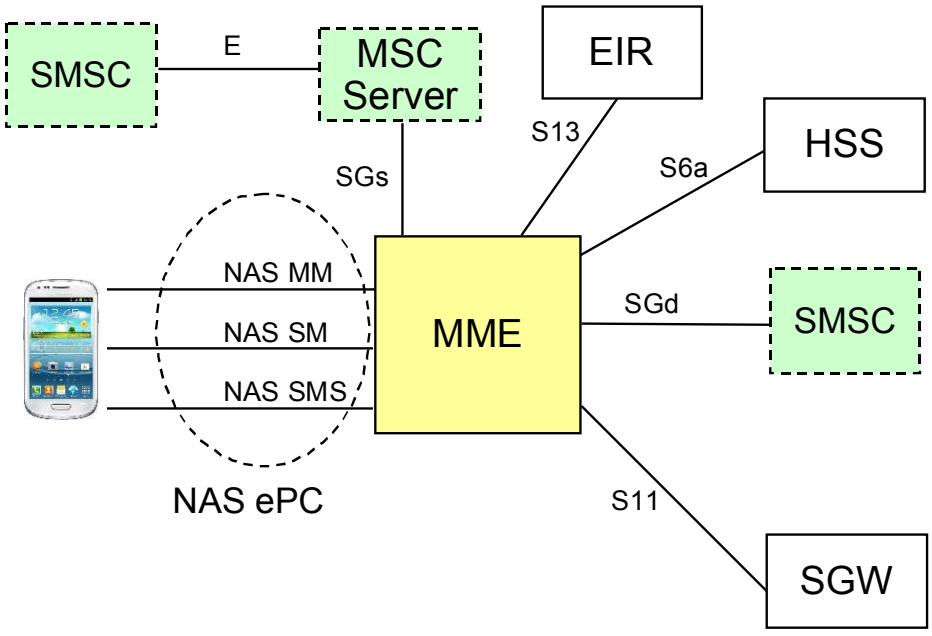
- N3IWF (Non-3GPP Interworking Function) : N3IWF est utilisé pour l 'accès WLAN non-trusted. N3IWF supporte les interfaces N2 et N3 vers le 5GC. L 'UE supporte l 'interface N1 avec le 5GC.
- TNGF (Trusted Non-3GPP Gateway Function) : TNGF est utilisé pour l 'accès WLAN trusted. N3IWF supporte les interfaces N2 et N3 vers le 5GC. L 'UE supporte l 'interface N1 avec le 5GC.
- W-AGF (Wireline Access Gateway Function) : W-AGF est utilisé pour l 'accès fixe tel que xDSL, FTTx ou câble. W-AGF supporte les interfaces N2 et N3 vers le 5GC. La Box fixe (RG, Residential Gateway) de nouvelle génération appelée 5G-RG supporte l 'interface N1 avec le 5GC. Pour les anciennes box fixes appelées alors FN-RG pour Fixed Network 5G, c 'est la fonction W-AGF qui supportera l 'interface N1 avec le 5GC.

Si la box est une box 5G considérée comme un UE, elle utilisera directement l 'accès 5G. On parle alors de Fixed Wireless Access (FWA) et ainsi l 'accès 5G remplace l 'accès filaire.

Mais il est aussi possible avec une box filaire (xDSL, FTTx ou câble) d 'utiliser le 5GC pour une convergence du cœur de réseau fixe et mobile avec le 5GC. Il s 'agit de Wireline Wireless Convergence (WWC). Une même BOX pourrait d'ailleurs être compatible à la fois par rapport aux accès fixe et mobile et ainsi agréger les débits des deux accès pour la transmission des données.

3. Fonctions de l'entité MME

Pour invoquer les procédures de réseau EPC telles que l 'attachement, le détachement, la mise à jour de changement de localisation, l 'établissement de connexions PDU, etc, l 'UE dispose du protocole de signalisation NAS EPC (Non Access Stratum) utilisé avec le MME. L 'eNodeB n 'est qu 'un relai de ces messages qu 'il n 'a pas à traiter.
Dans le réseau ePC, le MME reçoit et traite les messages de signalisation NAS MM (gestion de la mobilité), SM (gestion de session) et SMS (service de messagerie courte). Pour le NAS SMS, le MME utilise l'interface DIAMETER SGd pour envoyer et recevoir des SMS directement vers / depuis SMSC. Le MME peut aussi utiliser l 'interface SGs et relayer le SMS au MSC Server.
Pour les procédures MM nécessitant une authentification UE, le MME interagit avec le HSS via l'interface DIAMETER S6a pour obtenir les vecteurs d'authentification et effectuer l'authentification de l'UE. Par ailleurs le MME vérifie l'IMEI de l'UE auprès de l'EIR via l'interface DIAMETER S13. Une fois l 'authentification de l 'UE et la vérification de l 'IMEI réalisées avec succès, le MME obtient du HSS le profil de l 'usager. Ce profil contient la liste des APNs (Access Point Name) que l 'UE peut activer. Pour activer un APN, l 'UE échange avec le MME la signalisation NAS SM. Le MME dialogue alors avec le SGW via l 'interface S11 basée sur le protocole GTPv2-C pour mettre en œuvre la connectivité PDN .
Le MME traite donc les signalisation NAS MM, NAS SM et NAS SMS (si l'interface SGd est implantée).



Les interfaces S6a, S13, SGd sont basées sur DIAMETER
L 'interface E s 'appuie sur MAP
L 'interface SGs est basée sur SGS-AP.
L 'interface S11 est basée sur GTPv2-C.

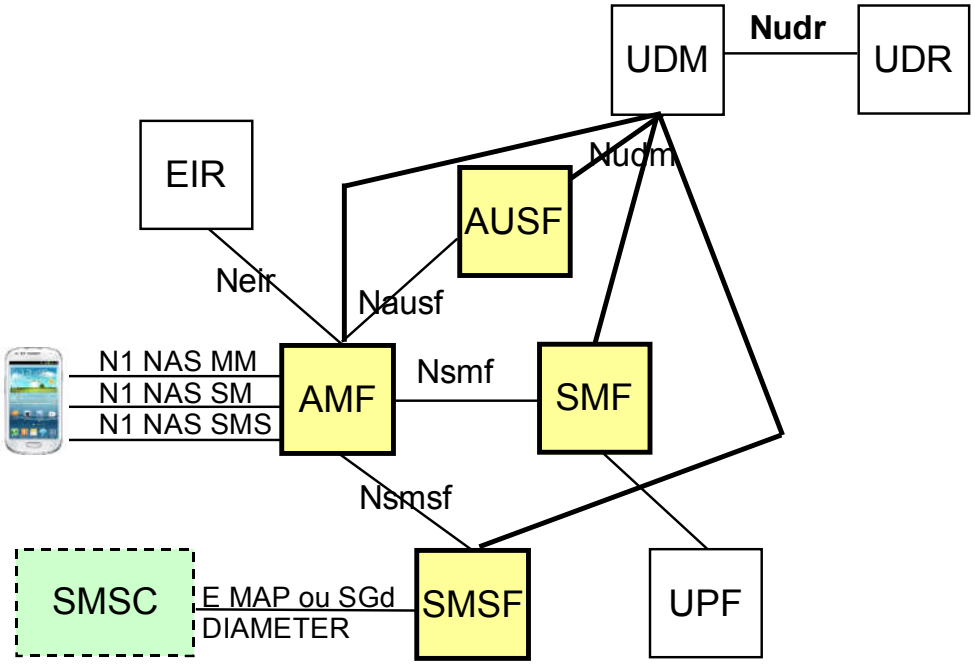
Figure 2 : Entité MME et ses interfaces

Le MME obtient auprès du HSS des données de souscription EPS (Evolved Packet System) relatives à un UE qui sont les suivantes :

- Des données de gestion de mobilité (RATs autorisés, TAIs autorisés, UE Usage Type)
- Des vecteurs d ’authentifications pour l ’authentification mutuelle avec l ’UE (Vecteurs E-UTRAN)
- Des données de gestion de session (APN Configuration data) afin d ’autoriser l ’UE à activer des APNs
- Des données de gestion SMS (TS21, TS22, SMS-barring info) si l ’architecture SMS in MME est implantée afin d ’autoriser l ’UE à envoyer et recevoir des SMSs.

4. Correspondance du MME dans le réseau cœur 5GC

Dans le contexte 5GC, la fonction AMF (Core Access and Mobility Management Function) termine l'interface NAS N1 avec l ’UE, reçoit / transmet toute la signalisation NAS de / vers l'UE. D'autre part, elle ne traite directement que la signalisation NAS MM et transmet la signalisation NAS SM à la fonction SMF (Session Management Function) et la signalisation NAS SMS à la fonction SMSF (Short Message Service Function).
De plus, toute signalisation NAS MM liée à l'authentification UE est transmise à la fonction AUSF (Authentification Server Function). L ’AUSF est la fonction qui obtient des vecteurs d'authentification à partir de l'UDM (Unified Data Management Function, base de données globale) et a la capacité de réaliser l'authentification de l'UE. L’AMF s’interface avec la fonction EIR pour vérifie l’identité IMEI. Chaque fonction de réseau du plan contrôle fournit une interface de service unique dans son rôle de fonction réseau serveur qui peut être invoquée par des fonctions réseau clientes si elles sont autorisées par la fonction réseau serveur. A titre d’exemple, la fonction UDM autorise les fonctions AUSF, AMF, SMF et SMSF à utiliser les services qu’elle propose via son interface de service appelée Nudm.
L ’UDM n ’est qu’un front-end qui accède aux données de souscription d ’un UE auprès de l ’UDR qui est un back-end. L’AMF, la SMF, la SMSF et l’UDM peuvent être considérées comme des microservices qui qui communiquent entre eux via des APIs HTTP/2 normalisées par 3GPP. La figure 3 décrit les fonctions 5GC qui réalisent les fonctionnalités de l’entité MME.



Authentication Server Function (AUSF)
Core Access and Mobility Management Function (AMF)
Session Management Function (SMF)
User plane Function (UPF)
Short Message Service Function (SMF)
Unified Data Management (UDM)
User Data Repository (UDR)

Figure 3 : Fonctions qui émulent le MME dans le réseau 5GC

Le MME est donc émulé par plusieurs fonctions du réseau cœur 5G suivantes :

- AMF pour la gestion de la mobilité de l 'UE
- AUSF pour l 'authentification de l 'UE
- SMF pour l 'obtention auprès de l 'UDM des données d 'APN à activer et d 'activation d 'APN
- SMSF pour la gestion des SMS sortants et entrants de l 'UE.

5. Fonctions de l'entité PGW

Les fonctions de l'entité PDN GW incluent :
• Interface vers les réseaux externes (Internet et intranets). Le PDN GW est l'entité qui termine le réseau mobile EPS et assure l'interface aux réseaux externes tels qu 'Internet et Intranets.
• Allocation de l'adresse IP de l'UE. Le PDN GW assigne à l'UE une adresse pour chaque APN qu 'active l 'UE. Le PDN GW peut allouer une adresse IPv4 ou IPv6.
• Interception légale. Le PDN GW est sur le chemin de signalisation pour l'établissement/la libération de bearer (PGW-C) et sur le chemin du média (paquets de données échangés par l'UE) (PGW-U). Il est donc un point stratégique pour l'interception légale des flux média et flux de contrôle relatifs à l 'établissement de bearers.
• Marquage des paquets dans les sens montant et descendant, e.g., positionnant le DiffServ Code Point sur la base du QCI (QoS Class Identifier) du bearer EPS associé. Cela permet d'associer des priorités aux flux de données au sens DiffServ. La QoS des flux IP de l 'UE est dictée par le PCRF via des politiques de QoS demandées par le PGW-C au PCRF lors de l 'établissement du bearer. Le PCRF lui-même obtient ces politiques de QoS auprès d 'une base de données de politiques appelée la SPR (Subscription Profile Repository).

• Taxation des flux de service montants et descendants (e.g. sur la base des règles de taxation fournies par le PCRF) ou sur la base de l'inspection de paquets définie par des politiques locales). Le PCRF indique pour chaque flux autorisé la QoS du flux et le type de taxation à appliquer au flux (taxation online ou taxation offline). Si la taxation est online, le PGW-C doit obtenir un crédit généralement sur la base du volume auprès de l 'OCS. Si la taxation est offline, le PGW-C doit soumettre des tickets de taxation à l 'OFCS.
Le PGW-C utilise des interfaces DIAMETER Gx, Gy et Gz avec le PCRF, l 'OCS et l 'OFCS respectivement.
Le PCRF utilise une interface DIAMETER Sp avec la SPR.
Le PGW-C utilise une interface Sxb basée sur le protocole PFCP (Packet Forwarding Control Protocol) pour contrôler le PGW-U.

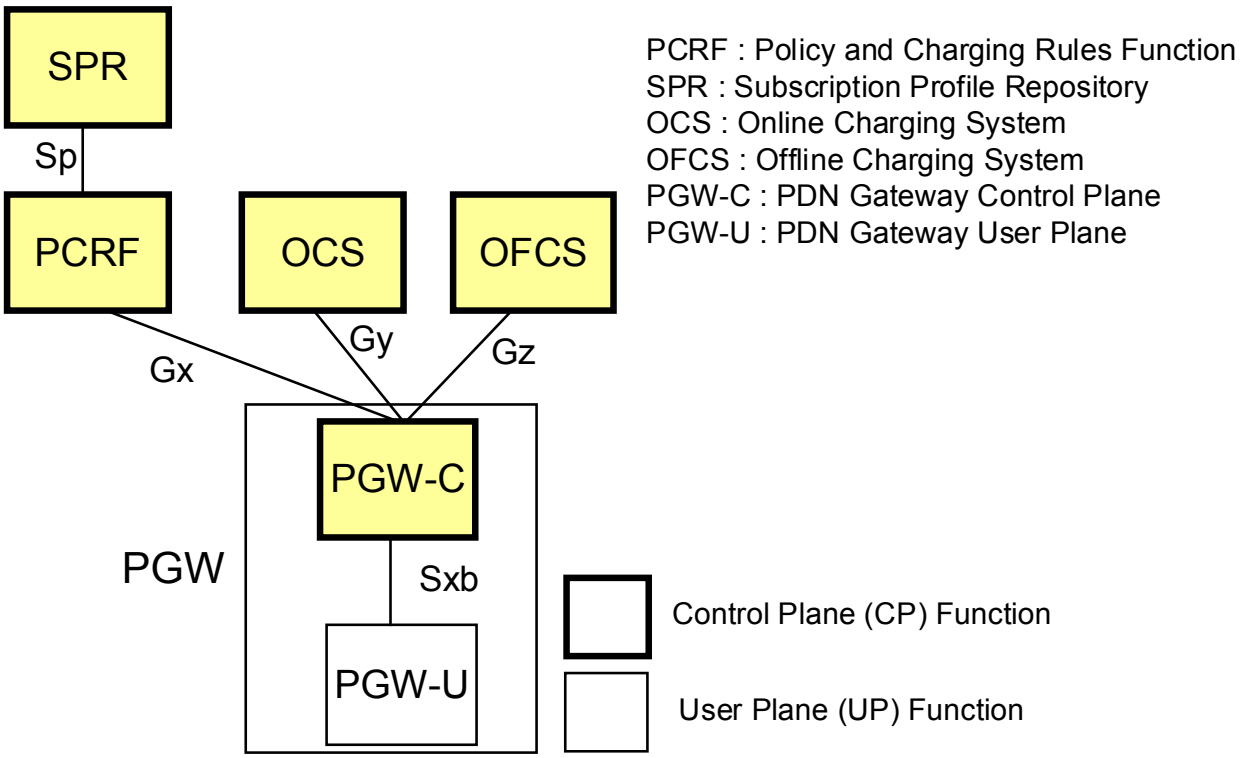


Figure 4 : Entité PGW et ses interfaces

6. Correspondance du PGW dans le réseau cœur 5G

En 5G, SMF/UPF correspond en 4G à PGW-C / PGW-U.
La SMF doit obtenir des politiques auprès de la fonction PCF et des crédits auprès de la fonction CHF.
Lorsque l'UE établit une session PDU (connectivité PDN), la fonction SMF reçoit la demande via l'AMF et invoque l'UDM afin d 'obtenir des informations relatives à la DNN (APN) que l'UE souhaite activer.
En 5G, les politiques sont stockées dans l'UDR, alors qu'en 4G, elles sont stockées dans une SPR.
La fonction AF peut utiliser l'interface PCF pour demander la mise en oeuvre de la qualité de service pour un flux IP donné (e.g., VoIP).
La PCF correspond au PCRF dans le réseau 4G. La CHF correspond à la fois à l'OCS et à l'OFCS dans le réseau 4G.

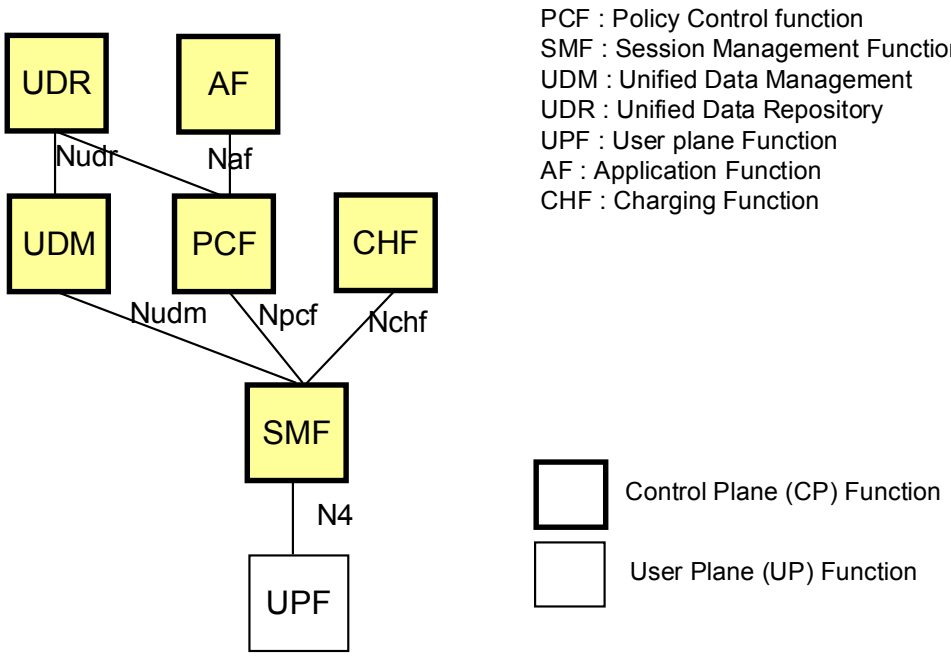


Figure 5 : Fonctions qui émulent le PGW et PCC dans le réseau 5GC

7. Accès WiFi untrusted connecté à l'EPC versus accès WiFi untrusted connecté au 5GC

L 'architecture ePC permet le rattachement depuis un accès WLAN non-trusted comme le montre la figure 6. 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 à la maison, dans un hotel, restaurant ou café.
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 ePC. L'interface utilisée est Swu basée sur IKEv2/IPSec.
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 6, le 3GPP AAA Server dispose d'une interface SWm avec l'ePDG.pour le transport sécurisé des informations d'authentification et d'autorisation.
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 tous 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 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 via l'interface S6a et par le 3GPP AAA Server via l'interface SWx auprès du HSS.
Dans le cas des accès 3GPP, c'est le MME 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 au SGW qui relaie la demande au PGW via l'interface S5/S8. Enfin le MME émet une requête S6a 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 à 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.

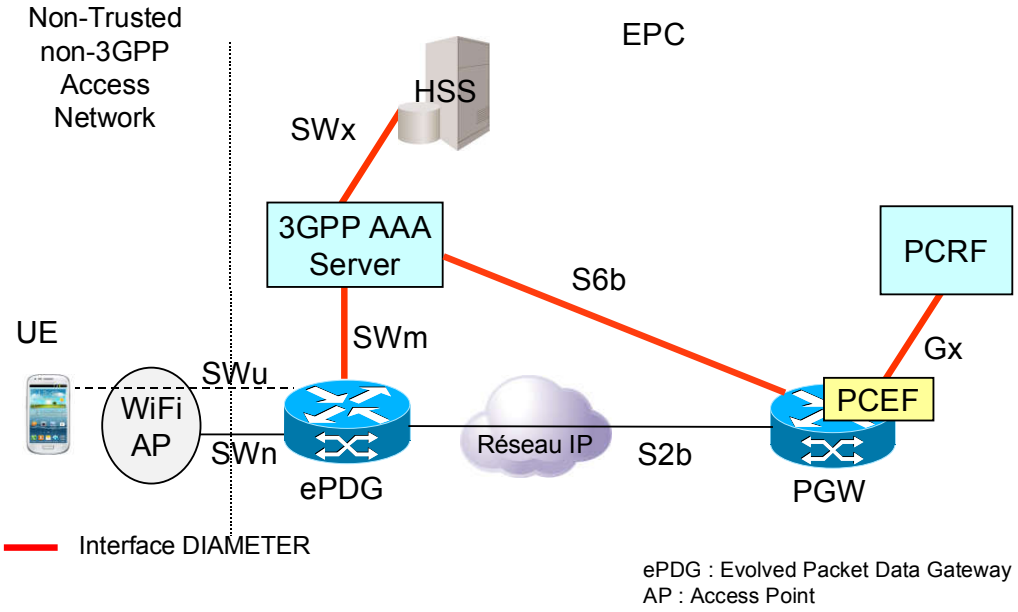


Figure 6 : Architecture WiFi non-trusted connecté à l'EPC

Dans le contexte de l 'accès WiFi untrusted connecté au 5GC, il n 'existe pas de fonction spécifique à l 'accès WiFi dans le réseau cœur 5G pour prendre en charge l 'UE.
En effet, le 3GPP AAA Server est émulé par les fonctions existantes du 5GC.
L 'ePDG devient une fonction d 'accès appelée N3IWF (Non 3GPP Interworking Function) et non pas une fonction cœur de réseau. Elle est vue comme un gNB (station de base 5G) avec l 'interface N2 vers l 'AMF et l 'interface N3 vers l 'UPF (Figure 7). Si l'accès WiFi est trusted, le TWAN devient la TNGF (Trusted WLAN Gateway Function).

L 'ePDG est émulé par la fonction N3IWF (Plan contrôle et Plan usager).
Le 3GPP AAA Server est émulé par plusieurs fonctions du réseau cœur 5G :

- AMF pour la gestion de la mobilité de l 'UE
- AUSF pour l 'authentification de l 'UE
- SMF pour l 'obtention auprès de l 'UDM des données d 'APN à activer et d 'activation d 'APN
- Le PGW est émulé par les fonctions SMF (Plan contrôle) et UPF (Plan usager).

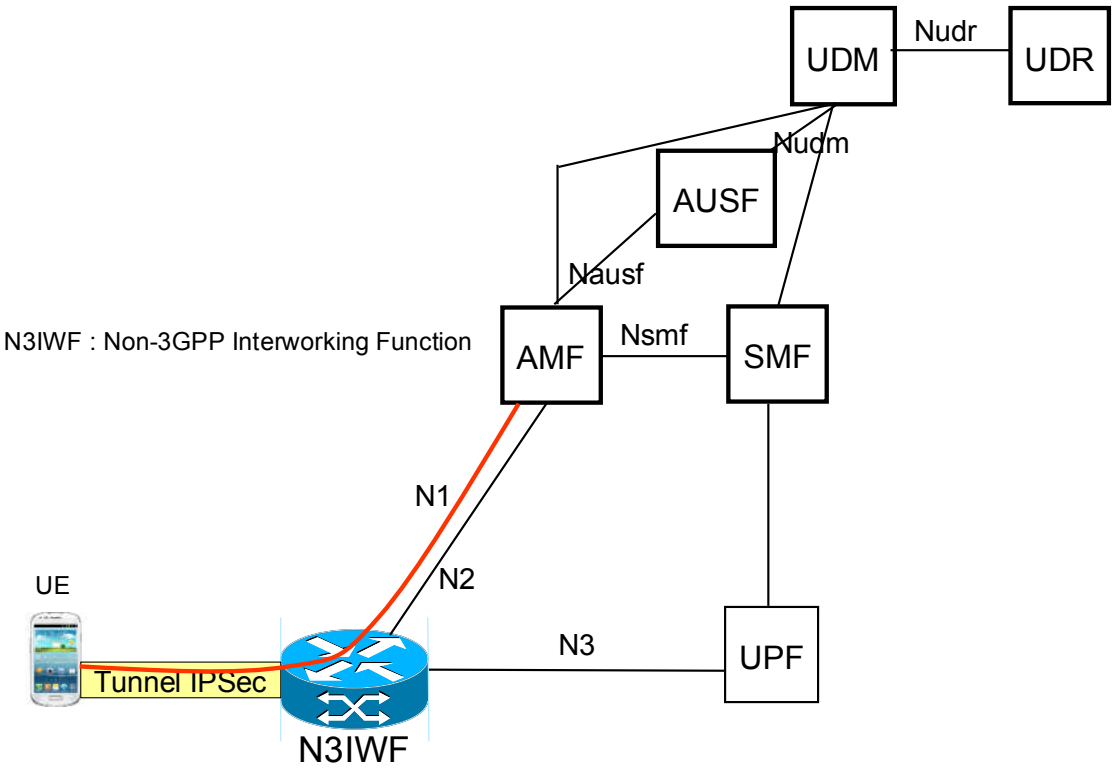


Figure 7 : Architecture WiFi non-trusted connecté au 5GC

8. Réseau de signalisation DIAMETER versus Réseau de signalisation HTTP/2

Dans le réseau EPC, pour des raisons de scalabilité et de simplicité de configuration, le mode quasi-associé est choisi par les opérateurs pour le transport de la signalisation DIAMETER. Un agent DIAMETER appelé DRA (DIAMETER Routing Agent) relie l 'ensemble des nœuds devant dialoguer entre eux via le protocole DIAMETER ; c'est le cas pour le MME, le HSS, l'EIR, le PGW/PCEF, le PCRF, l'OCS, etc. Ce même DRA route le trafic de signalisation DIAMETER entre ces nœuds. Tous les nœuds par défaut relaient leur signalisation à l 'agent DIAMETER qui dispose de toute l 'intelligence de routage. En Roaming, lorsque un nœud DIAMETER du réseau visité (e.g., MME) souhaite délivrer un message DIAMETER à un nœud présent dans le réseau nominal (e.g., HSS), l 'agent du réseau visité devient un DEA (DIAMETER Edge Agent). Le DEA est une fonction de l 'Agent DIAMETER qui joue le rôle d 'élément de frontière (border element) d 'un réseau EPC pour la signalisation DIAMETER et peut mettre en œuvre des fonctionnalités de masquage de la topologie et de firewalling. Ce DEA transfert la signalisation DIAMETER à un autre agent (international) appelé DRA qui dispose de la connectivité pour acheminer le trafic DIAMETER au réseau de destination dont le point d'entrée est un autre DEA (Figure 8).

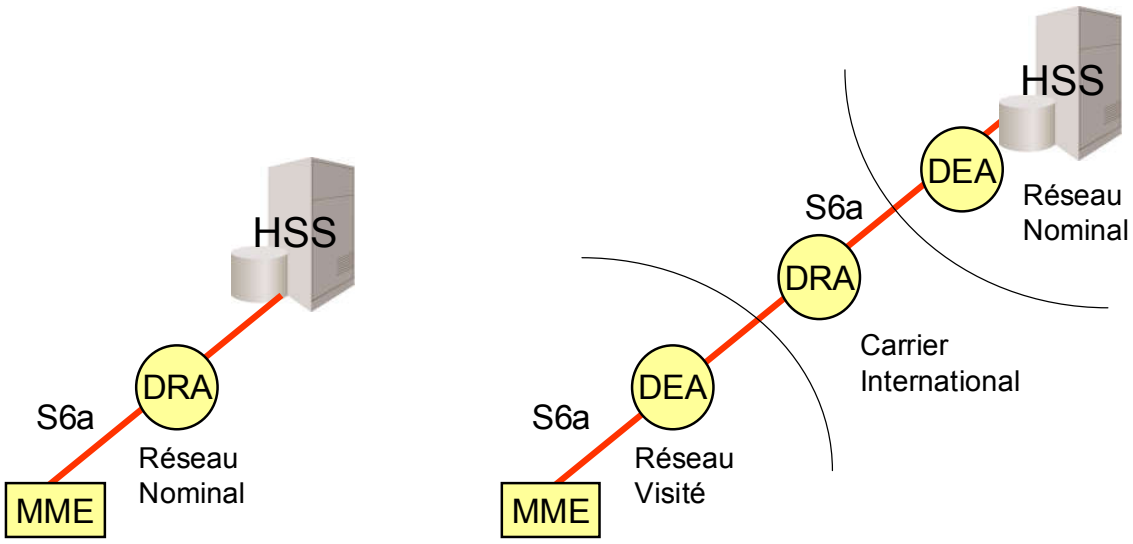


Figure 8 : Réseau de signalisation DIAMETER

Dans le contexte 5GC, un réseau de signalisation HTTP/2 (Figure 9) est mise en œuvre similaire au réseau de signalisation DIAMETER utilisé par l'EPC.
L'équivalent du DRA interne au réseau EPC est appelé SCP (Service Communication Proxy) et supporte les fonctionnalités suivantes :

- Routage des opérations de service HTTP/2 entre NF consommateur (e.g., AMF) et NF fournisseur (e.g., UDM).
- Partage de charge entre différentes instances de destination possibles (e.g,., différentes instances d'UDM)

Toutes les instances de fonction réseau créées dans le 5GC enregistrent leur profil NF auprès de la NRF (Network Registration Function). Le SCP invoque la NRF pour obtenir les profils des instances candidates qui indiquent notamment leur charge et ainsi permet au SCP de réaliser son opération de routage/partage de charge.
L'équivalent du DEA à l'interface entre réseaux EPC est appelé SEPP (Security Edge Protection Proxy) et supporte les fonctionnalités additionnelles suivantes par rapport au SCP :

- Masquage de la topologie pour sécuriser le plan de contrôle 5GC d 'un opérateur 5G vis à vis du monde externe.
- Firewall HTTP/2 pour filtrer tout le trafic HTTP/2 plan de contrôle entrant et sortant du réseau 5GC d 'un opérateur.

Par ailleurs, le carrier international dispose de ses propres proxy HTTP/2 appelés Proxy IPX (IP eXchange Network).

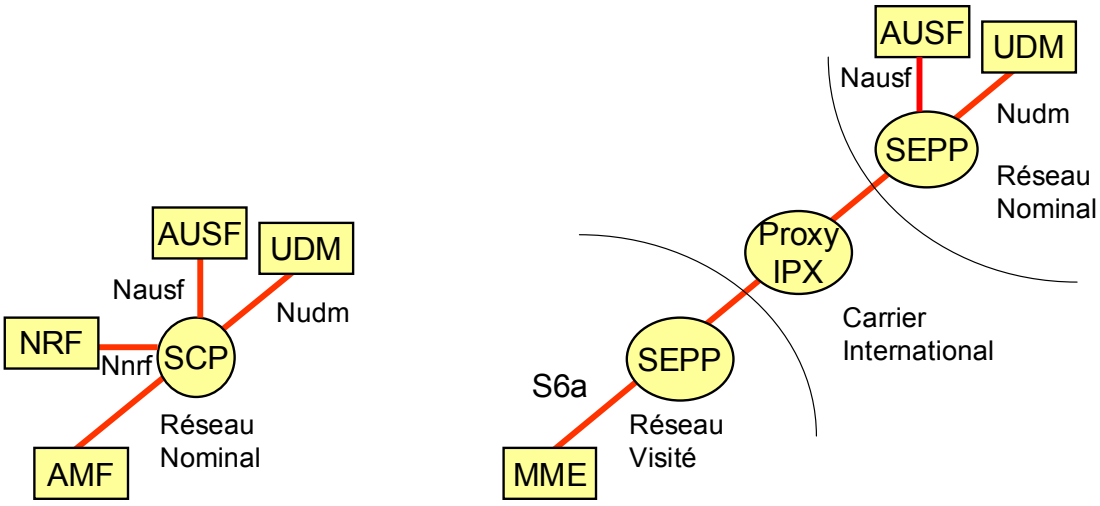


Figure 9 : Réseau de signalisation HTTP/2

9. SCEF versus NEF

Dans le contexte 4G, La fonction SCEF (Service Capability Exposure Function) représente la plate-forme de réseau qui offre des capacités de services réseau aux applications MTC (Machine Type Communication) via des APIs et s 'appuie sur l 'architecture du réseau mobile pour réaliser ces services (service de souscription/notification d 'événement, service de gestion de groupe, service de localisation, service de réveil de device, livraison de données non-IP, etc) (Figure 10).

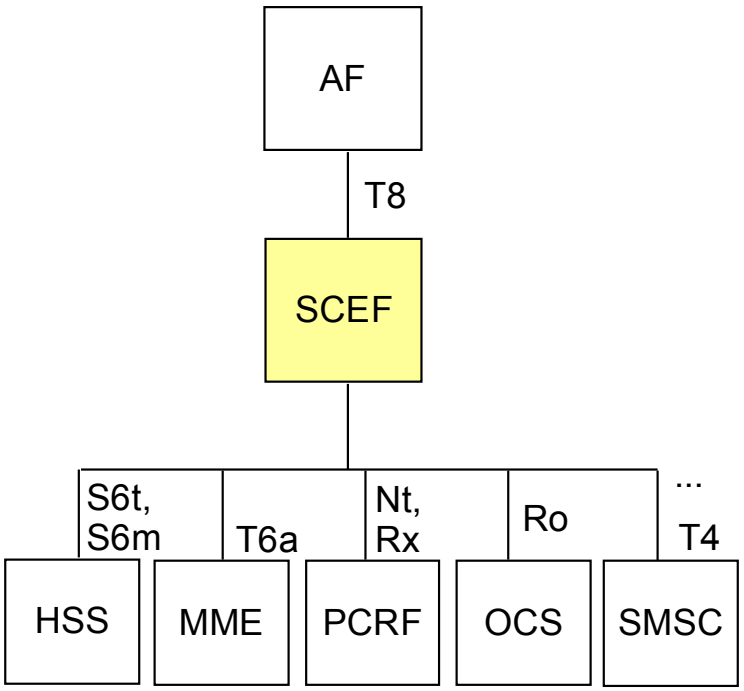


Figure 10 : Fonction SCEF EPC et ses interfaces

Pour rendre ses services via l 'interface de service Nnef (qui est la même interface de service HTTP que celle proposée par la SCEF appelée T8) exposée aux Application

Functions (AFs), la NEF utilise les services rendus par les fonctions de réseau telles que AMF, SMF, UDM, PCF, etc. (Figure 11).

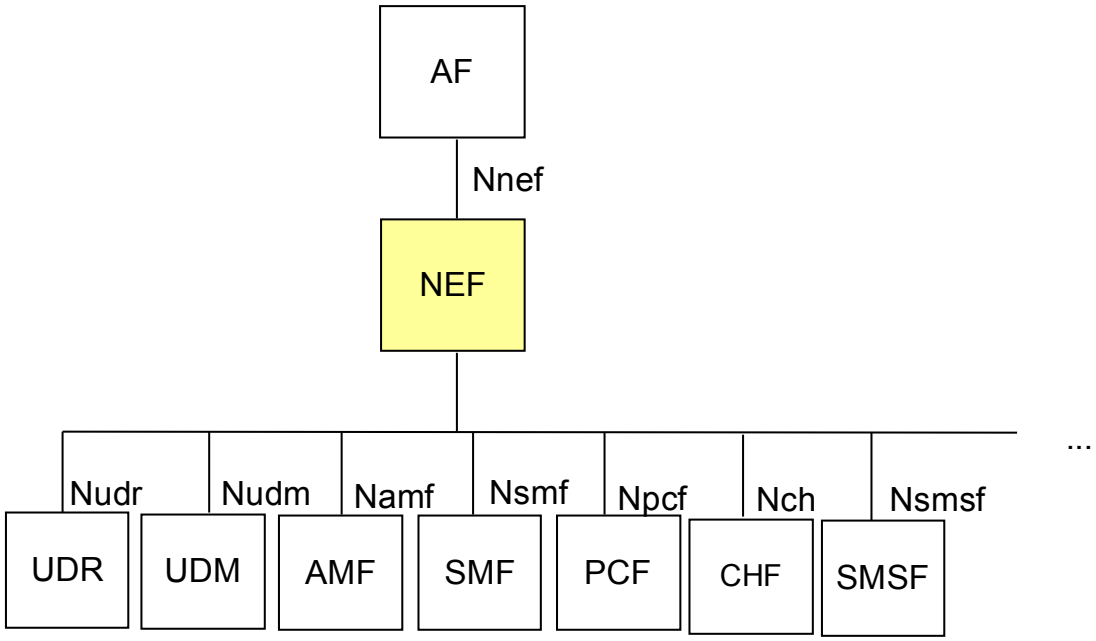


Figure 11 : Fonction NEF 5GC et ses interfaces

10. Mapping entre fonctions EPC et 5GC

Le tableau suivant montre la correspondance entre entités EPC et fonctions 5GC.

Fonction 5GC	**Entité EPC**
AMF	MME
AUSF	MME
SMSF	MME
5G-EIR	EIR
BSF	Policy DRA
CHF	OCS+OFCS
NEF	SCEF
PCF	PCRF
SEPP	DEA
SCP	DRA
SMF	MME+SGW-C/PGW-C
UDM	HSS
UDR	UDR/SPR
UPF	SGW-U/PGW-U
N3IWF	ePDG
TNGF	TWAN

NRF et W-AGF n ’ont pas d ’équivalence en 4G

La fonction BSF dans le 5GC permet de mettre en œuvre le binding de service. C ’est cette fonction qui permet à une fonction d ’AF d ’acheminer ses opérations de service HTTP/2 à la fonction PCF adéquate. Dans l’EPC, la fonction de binding de service est mise en œuvre dans le DRA (Policy DRA).

La formation EFORT « Réseau Cœur 5G » décrit l'architecture de réseau cœur 5G, les fonctions réseau associées, leurs interfaces de service, le réseau de signalisation http/2 associé au réseau cœur 5G ainsi que toutes les procédures offertes par le 5GC.
http://efort.com/index.php?PageID=21&l=fr&f_id=194&imageField.x=0&imageField.y=4