

Home Subscriber Server : Architecture, Interfaces et Evolutions

EFORT

<http://www.efort.com>

1 Introduction

Avec l'introduction du réseau 4G appelé EPS (Evolved Packet System), le HLR (Home Location Register) est réutilisé et renommé Home Subscriber Server (HSS). Le HSS est un HLR évolué et contient l'information de souscription pour GSM, GPRS, 3G, EPS et IMS (IP Multimedia Subsystem). IMS devient important lors de l'introduction de l'architecture VoLTE (Voice over LTE) via l'accès EPS.

A la différence de la 2G et de la 3G où les interfaces vers le HLR sont supportées par le protocole MAP (Mobile Application Part) transporté sur SS7 ou SIGTRAN, les interfaces du HSS s'appuient sur des applications du protocole DIAMETER transportées sur SCTP/IP, notamment S6a, S6d, SWx, Cx et Sh. DIAMETER est un protocole AAA (Authentication, Authorization & Accounting) pour des environnements IP tels que l'EPS et l'IMS.

Le HSS est une base de données qui est utilisée simultanément par les réseaux 2G, 3G, EPS et IMS appartenant au même opérateur. Il supporte donc les protocoles MAP (2G, 3G) et DIAMETER (EPS, IMS). Le but de ce tutoriel est de décrire les interface DIAMETER du HSS dans l'environnement EPS et de présenter la nouvelle structure HSS appelé UDC (User Data Convergence).

2 Fonctionnalités HSS

Le HSS consiste en les fonctionnalités suivantes :

- Fonctionnalité HSS IP Multimedia aussi appelée UPSF (User Profile Server Function) afin de fournir le support aux fonctions de contrôle de session IMS, telles que les I-CSCF et S-CSCF (Interface Cx basée sur DIAMETER) et contrôle de service (Interface Sh).
- Fonctionnalité HSS EPS nécessaire afin que les usagers EPS accèdent au domaine paquet ePC (Interface S6a/S6d).
- Fonctionnalité HSS pour l'accès non-3GPP à l'EPC (Evolved Packet Core) nécessaire afin de permettre à un 3GPP AAA Server d'obtenir du HSS les informations d'authentification pour authentifier l'utilisateur, ainsi que son profil d'utilisateur (Interface SWx). Un exemple d'accès non-3GPP est WLAN. Il est en effet possible d'accéder au cœur de réseau paquet ePC (Evolved Packet Core) depuis les accès 3GPP 2G, 3G (via le SGSN) et 4G ainsi que depuis les accès non-3GPP tels que WLAN.
- Fonctionnalité HLR/AuC requise pour le domaine PS (Interface Gr).
- Fonctionnalité HLR/AuC requise par le domaine circuit, s'il est nécessaire que les usagers accèdent au domaine circuit ou pour supporter le roaming dans des réseaux visités légitimes supportant le domaine circuit 2G/3G (Interfaces C, D).

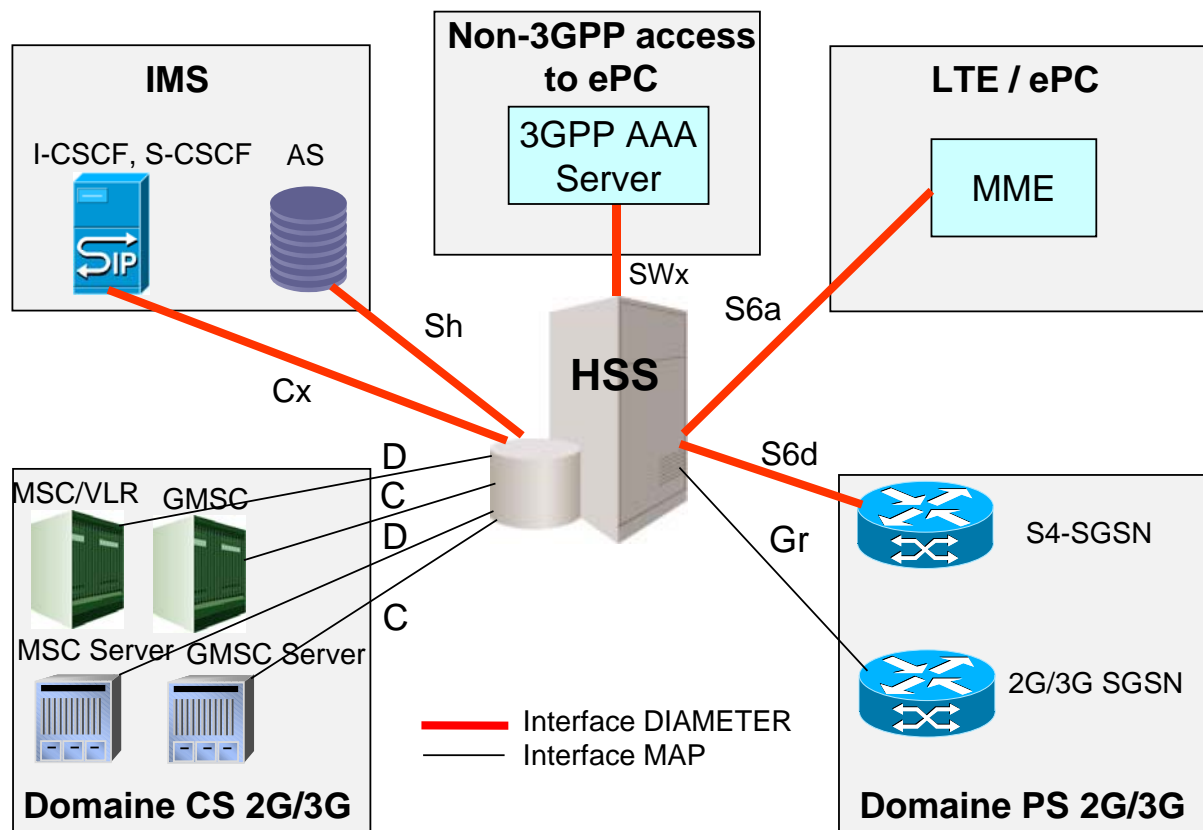


Figure 1 : Interfaces de l'entité HLR/HSS/UPSF

Un réseau nominal peut être supporté par un ou plusieurs HSSs. Le nombre est fonction du nombre d'utilisateurs mobiles, de la capacité du HSS et de l'organisation du HSS.

Le HSS prend en charge le stockage des informations suivantes de l'utilisateur :

- Identités privée et publiques de l'utilisateur
- Information de sécurité de l'utilisateur pour les aspects autorisation et authentification.
- Information de localisation de l'utilisateur. Le HSS supporte l'enregistrement de l'utilisateur et mémorise l'adresse du nœud réseau auquel il est rattaché.
- Le profil de l'utilisateur contenant entre autres les marques de service de l'utilisateur autorisant l'accès à ces services
- le HSS génère aussi des informations de sécurité utilisateur pour l'authentification mutuelle, le chiffrement et la protection de l'intégrité des données.

Lorsque l'utilisateur LTE est dans son réseau nominal, la couverture LTE peut être relativement limitée au début du déploiement de cette nouvelle technologie radio. C'est la raison pour laquelle le client LTE peut être amené à s'enregistrer au réseau mobile depuis une couverture 2G ou 3G. Son profil sera passé par le HSS au MME si l'utilisateur se rattache depuis une couverture LTE. Si la couverture de rattachement est 2G/3G, alors le nœud obtenant le profil de l'utilisateur auprès du HSS est le S4-SGSN. Le S4-SGSN a la capacité de terminer les sessions de données du client dans l'ePC (Evolved Packet Core) et non sur le GGSN afin de fournir une mobilité globale au client. Si l'utilisateur se rattache depuis sa couverture WiFi, le nœud obtenant le profil de l'utilisateur auprès du HSS est le 3GPP AAA server et non pas le MME ou S4-SGSN.

Lorsque la voix sur LTE (VoLTE) sera mise en œuvre, le S-CSCF est le composant de l'architecture IMS qui obtiendra le profil de l'utilisateur auprès de l'UPSF (User Profile Server Function). Par ailleurs les ASs peuvent obtenir de ce même UPSF les données de services permettant l'exécution des applications pour un client donné (e.g., numéro de renvoi d'appel).

Lorsque l'utilisateur est présent dans un réseau visité qui n'est que 2G/3G, alors le MSC Server et le 2G/3G SGSN obtiennent ses profils circuit et paquet respectivement auprès du HLR via l'interface légataire MAP et non pas DIAMETER. C'est la raison pour laquelle il est nécessaire de provisionner le HLR, le HSS et l'UPSF pour un client LTE donné.

Un produit HSS peut contenir les fonctionnalités HLR, HSS et UPSF.

Mis à part le HSS, les données de souscription pour les services de données d'un utilisateur sont stockées dans la SPR (Subscription Profile Repository) par APN (Access Point Name).

Des exemples de telles données sont :

- Un utilisateur dispose d'un abonnement data avec fair use de 3 Gigaoctets par cycle de facturation
- Un utilisateur est freemium (il n'a le droit d'accès via le réseau data mobile qu'aux communautés Facebook et Twitter)
- Un utilisateur est sujet au contrôle parental. Il ne peut donc pas accéder à n'importe quelle URL.
- Un utilisateur est autorisé à utiliser le service skype avec dégradation du flux correspondant
- Un utilisateur a souscrit au service TV mobile premium et peut utiliser le service TV mobile de manière illimitée sans impacter son fair use.

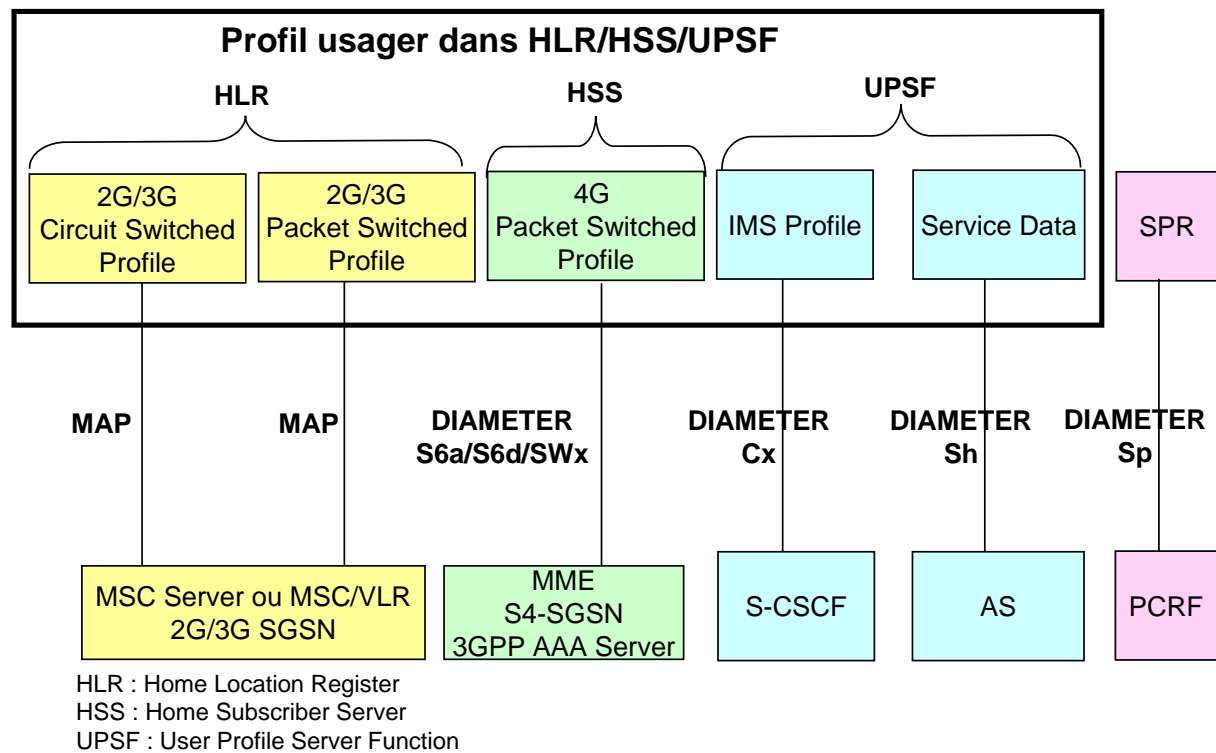


Figure 2 : Provisioning HSS pour un utilisateur LTE

3 Interface S6a/S6d

L'interface DIAMETER S6a/S6d permet à un client DIAMETER (i.e., MME ou S4-SGSN) et un serveur DIAMETER (i.e., HSS) :

- d'échanger l'information de localisation de l'utilisateur
- d'échanger l'information d'authentification de l'utilisateur
- de télécharger et traiter les changements des données de l'utilisateur stockées dans le serveur DIAMETER
- d'autoriser l'utilisateur à accéder à l'EPS.

Quatre procédures sont supportées par le HSS via l'interface S6a/S6d :

- Procédure de gestion de localisation. Cette procédure implique trois requêtes/réponses DIAMETER
 - Update-Location-Request/Answer (ULR/ULA) [MME/S4-SGSN→HSS]
 - Cancel-Location-Request/Answer (CLR/CLA) [HSS→MME/S4-SGSN]
 - Purge-UE-Request/Answer (PUR/PUA) [MME/S4-SGSN→HSS]
- Procédure de traitement de données usager avec deux requêtes/réponses associées
 - Insert Subscriber Data-Request/Answer (IDR/IDA) [HSS→MME/S4-SGSN]
 - Delete-Subscriber-Data-Request/Answer (DSR/DSA) [HSS→MME/S4-SGSN]
- Procédure d'authentification qui inclut une requête/réponse
 - Authentication-Information-Request/Answer (AIR/AIA) [MME/S4-SGSN→HSS]
- Procédure de correction de problèmes avec deux requêtes/réponses
 - Reset-Request/Answer (RSR/RSA) [HSS→MME/S4-SGSN]
 - Notify-Request/Answer (NOR/NOA) [MME/S4-SGSN→HSS]

3.1 Requêtes/réponses DIAMETER sur l'interface S6a/S6d

- Update-Location-Request/Answer (**ULR/ULA**) est utilisé entre le MME et le HSS et entre le S4-SGSN et le HSS afin de mettre à jour l'information de localisation dans le HSS. La procédure est invoquée par le MME ou le S4-SGSN et est utilisée afin:
 - D'informer le HSS au sujet de l'identité du MME ou du S4-SGSN auquel est actuellement rattaché l'utilisateur.
 - De fournir au MME ou au S4-SGSN les données de souscription de l'utilisateur.
- Cancel-Location-Request/Answer (**CLR/CLA**) est utilisé entre le HSS et le MME et entre le HSS et le S4-SGSN afin de supprimer le profil de l'utilisateur du MME ou du S4-SGSN. La procédure doit être invoquée par le HSS et est utilisée afin :
 - D'informer le MME ou le S4-SGSN de l'annulation de la souscription par l'utilisateur
 - D'informer le MME ou le S4-SGSN qu'une procédure de mise à jour a eu lieu, i.e., un changement de MME ou de S4-SGSN a eu lieu.
- Purge-UE-Request/Answer (**PUR/PUA**) est utilisé entre le MME et le HSS et entre le S4-SGSN et le HSS afin d'indiquer que le profil de l'utilisateur a été supprimé du MME ou du S4-SGSN car l'utilisateur est détaché depuis un certain temps.
- Insert Subscriber Data-Request/Answer (IDR/IDA) est utilisé entre le HSS et le MME et entre le HSS et le S4-SGSN dans les situations suivantes :
 - Suite à des changements dans la souscription de l'utilisateur
 - L'opérateur a appliqué des changements ou a retiré la marque "Operator Determined Barring" pour cet utilisateur.
- Delete-Subscriber-Data-Request/Answer (**DSR/DSA**) est utilisé par le HSS afin de supprimer toutes les données ou un sous-ensemble des données de souscription de l'utilisateur du MME ou du S4-SGSN.
- Authentication-Information-Request/Answer (**AIR/AIA**) est utilisé par le MME ou le S4-SGSN afin d'obtenir du HSS des vecteurs d'authentification.
- Reset-Request/Answer (**RSR/RSA**) est utilisé par le HSS après une réinitialisation afin d'indiquer au MME et au S4-SGSN qu'une faute s'est produite. Les MME et S4-SGSN doivent alors mettre à jour le HSS (via ULR/ULA) avec les informations de localisation des utilisateurs dont les profils sont pris en charge par ce HSS.
- Notify-Request/Answer (**NOR/NOA**) est utilisé par le MME ou le S4-SGSN afin d'informer le HSS :

- D'une mise à jour de l'information du terminal
- D'une assignation ou un changement de PDN GW pour une APN donnée.

4 Interface SWx

Les mêmes procédures que celles sur l'interface S6a/S6d sont présentes sur l'interface SWx.

- Procédure de gestion de localisation
 - Server-Assignment-Request/Answer (SAR/SAA) [3GPP AAA Server→HSS]
 - Registration-Termination-Request/Answer (RTR/RTA) [HSS→3GPP AAA Server]
- Procédure de prise en charge de données de souscription
 - Push-Profile-Request/Answer (PPR/PPA) [HSS→3GPP AAA Server]
- Procédure d'authentification
 - Multimedia-Authentication-Request/Answer (MAR/MAA) [3GPP AAA Server→HSS]
- Procédure de gestion des fautes
 - Utilise PPR/PPA et SAR/SAA

La procédure de gestion de localisation d'accès Non-3GPP sur l'interface SWx inclut les fonctionnalités suivantes :

- Enregistrement du 3GPP AAA Server : Ce dernier enregistre son adresse dans le HSS pour un usager donné lorsqu'un nouvel usager a été authentifié par le 3GPP AAA Server.
- Mise à jour du PDN GW et de l'APN : Le 3GPP AAA Server informe le HSS de l'identité du PDN GW (hostname) et l'APN utilisée pour un usager donné, ou pour informer le HSS que la paire <PDN GW, APN> n'est plus utilisée. Cet événement survient lorsqu'un default bearer est établi ou libéré.
- Obtention de l'identité du PDN GW et de l'APN : Le 3GPP AAA Server obtient du HSS l'identité du PDN GW et l'APN pour un usager donné qui dispose déjà de ses default bearers. Cet événement est observé lorsque l'UE était déjà enregistré via un accès 3GPP à l'ePC et se déplace sur un accès non-3GPP.
- Désenregistrement initié par le 3GPP AAA Server : Ce dernier peut se dissocier d'un usager donné et purger tout état d'enregistrement de l'UE dans le HSS. Cette procédure survient lorsque l'UE a été déconnecté de l'accès non-3GPP
- Désenregistrement initié par le HSS : Le HSS peut initier une procédure de désenregistrement afin de purger l'UE du 3GPP AAA Server. Cette procédure survient lorsque la souscription de l'UE a été annulée par l'opérateur ou pour d'autres raisons déterminées par l'opérateur. Par conséquent, le 3GPP AAA Server doit désactiver tout bearer de l'UE et détacher l'UE du réseau d'accès.

La procédure de prise en charge de données de souscription sur l'interface SWx inclut les fonctionnalités suivantes :

- Mise à jour du profil de l'utilisateur : Le HSS peut décider d'émettre le profil de l'utilisateur à un 3GPP AAA Server enregistré. Cette procédure survient lorsque le profil de l'utilisateur a été modifié dans le HSS; il est alors nécessaire de mettre à jour le 3GPP AAA Server.
- Demande du profil de l'utilisateur : Le 3GPP AAA Server demande le profil de l'utilisateur au HSS. Cette procédure est invoquée lorsque le profil de l'utilisateur est perdu ou doit être mis à jour par le 3GPP AAA Server.

4.1 Requêtes/réponses DIAMETER sur l'interface SWx

- MAR est utilisé par le 3GPP AAA Server afin d'obtenir les vecteurs d'authentification pour un usager donné auprès du HSS. La réponse MAA contient un ou plusieurs vecteurs d'authentification générés pour l'utilisateur.

- SAR est émis par le 3GPP AAA Server à l'entité HSS afin de mettre à jour dans le profil de l'utilisateur son 3GPP AAA Server courant. L'entité HSS répond par le message SAA en indiquant le nouvel état d'enregistrement de l'utilisateur ainsi que son profil d'utilisateur.
- L'annulation d'enregistrement de l'utilisateur par le réseau est réalisée à l'aide du message RTR émis par le HSS. Le 3GPP AAA Server l'acquiesce par une réponse RTA.
- Le message PPR est utilisé par le HSS afin de mettre à jour un profil d'utilisateur dans le 3GPP AAA Server. Ce message est acquiescé par le 3GPP AAA Server par une réponse PPA.
- La commande PPR est aussi utilisée par le HSS pour informer le 3GPP AAA Server que le HSS a été réinitialisé. Le 3GPP AAA Server doit alors mettre à jour le HSS (via SAR/SAA) avec les informations de localisation des utilisateurs dont les profils sont pris en charge par ce HSS.

5 Enregistrement de l'UE via le réseau EPS

L'UE souhaite s'enregistrer au réseau EPS (LTE + ePC). Cette procédure correspond à un attachement au réseau EPS qui conduira à l'authentification de l'UE, l'obtention de son profil EPS par le MME le prenant en charge, et à la création d'un default bearer permanent correspondant à une connectivité permanente IP (notamment pour accéder à Internet).

1. L'UE initie la procédure d'attachement en émettant une requête Attach au MME. L'UE utilise avec le MME un protocole de signalisation d'accès appelé EMM (EPS Mobility Management Protocol). Ce protocole est notamment traduit dans le cœur de réseau mobile en le protocole DIAMETER (Signalisation réseau).
2. Le MME obtient du HSS disposant du profil de l'UE, des vecteurs d'authentification à l'aide des commandes DIAMETER S6a Authentication Information Request/Answer.
3. Le MME soumet les couples RAND et AUTN à l'UE et escompte une réponse de l'UE contenant un résultat d'authentification égal à celui fourni par le HSS (RES). L'UE retourne la réponse au MME.
4. Le MME demande à l'UE de lui fournir son IMEI.
5. L'EIR, interrogé par le MME indique dans le message de retour si le terminal fait ou ne fait pas partie de la liste des équipements interdits (black list). L'interface DIAMETER S13 est utilisée entre le MME et l'EIR.
6. S6a : Le MME délivre une requête Update Location Request (adresse MME sous forme de hostname, IMSI) au HSS. S6b : Le HSS acquiesce la mise à jour de localisation par une réponse Update Location Answer au MME qui contient les données de souscription EPS de l'UE incluant la liste de tous les APNs que l'UE est en droit d'accéder, une indication sur l'APN par défaut, et les paramètres de QoS associés à chaque APN. Si le HSS rejette la procédure de mise à jour de localisation, alors le MME rejette la demande d'attachement de l'UE.
7. Le MME établit le premier default bearer pour l'UE.
8. Le MME retourne à l'UE une réponse EMM Attach Accept informant l'UE qu'il est accepté par le réseau. Cette réponse indique aussi à l'UE, l'APN qui a été activé et l'adresse IP assignée à l'UE pour cet APN.

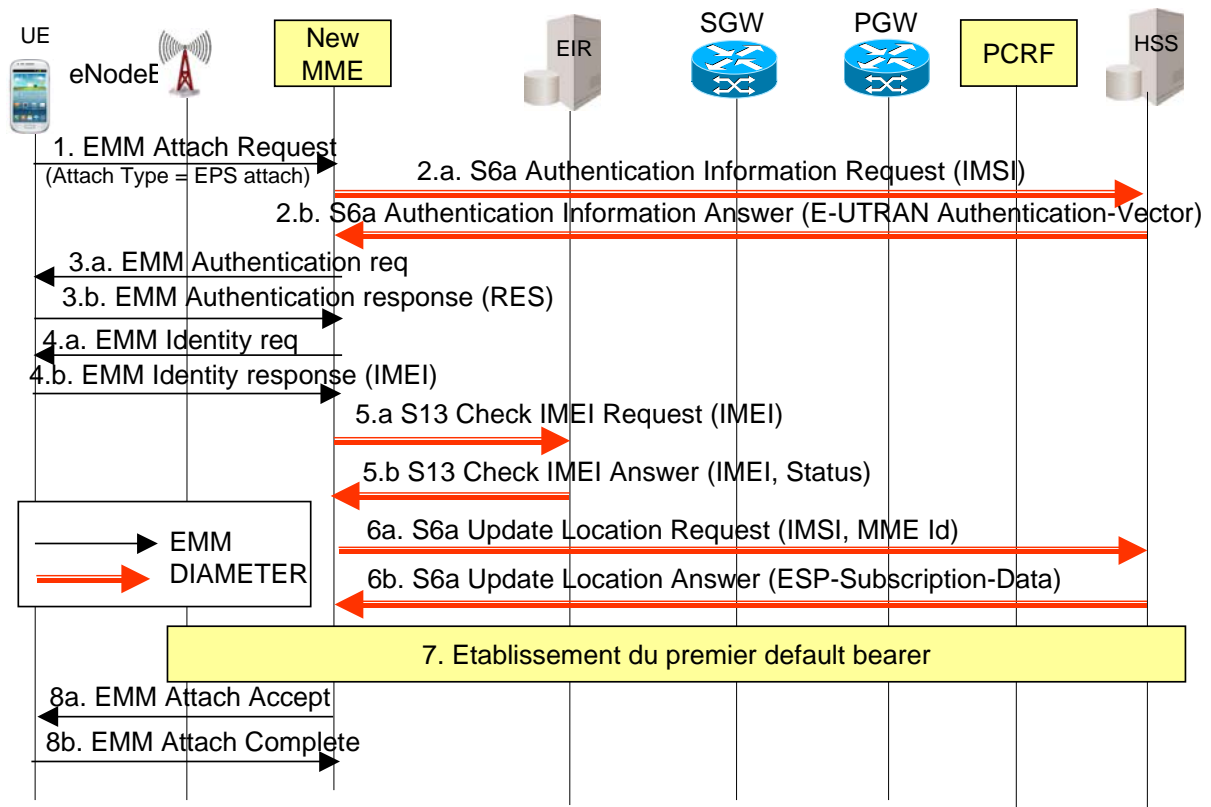


Figure 3 : Enregistrement de l'UE au réseau EPS

6 Structure HSS : UDC, UDR et FE

Le concept User Data Convergence (UDC) supporte une architecture en couche, en séparant le stockage des données de l'utilisateur de la logique d'application dans un système 3GPP. Ainsi les données de l'utilisateur sont stockées dans un répertoire de données logiquement unique appelé UDR (User Data Repository) permettant l'accès aux entités de réseau et de service, appelés front-ends (FEs).

Les éléments de réseau et de service doivent être conçus afin d'accéder aux données du profil de l'utilisateur à distance et sans stocker ses données en permanence localement.

L'architecture UDC peut très bien s'appliquer au HLR/HSS. UDR est un répertoire de données du point de vue des FEs. Un FE a accès uniquement aux données le concernant (vue de données d'application). L'UDR peut interagir avec plusieurs FEs exécutant la même logique d'application ou différentes logiques d'application. La structure interne de l'UDR est dépendante du fournisseur et les FEs ne sont pas sensés la connaître; L'UDR peut être centralisée ou distribuée sur différentes localisations ; elle peut être redondée, peut supporter des mécanismes de réplication, etc. Une transaction à l'UDR est mise en œuvre via une suite d'opérations qui font passer la base de données d'un état A - antérieur à la transaction - à un état B postérieur et des mécanismes permettent d'obtenir que cette suite soit à la fois atomique, cohérente, isolée et durable (ACID).

Un FE d'application exécute une logique d'application traitant de données de l'utilisateur stockées dans l'UDR (e.g., logique d'application HLR/HSS). Un FE d'application interagit avec les entités du système 3GPP via des interfaces 3GPP existantes. Ces interfaces (C, Gr, Cx, Sh, S6a, SWx...) doivent rester inchangées lors de l'introduction du concept UDC. Les FEs équivalents peuvent être regroupés dans un cluster de FEs afin de permettre la distribution des requêtes.

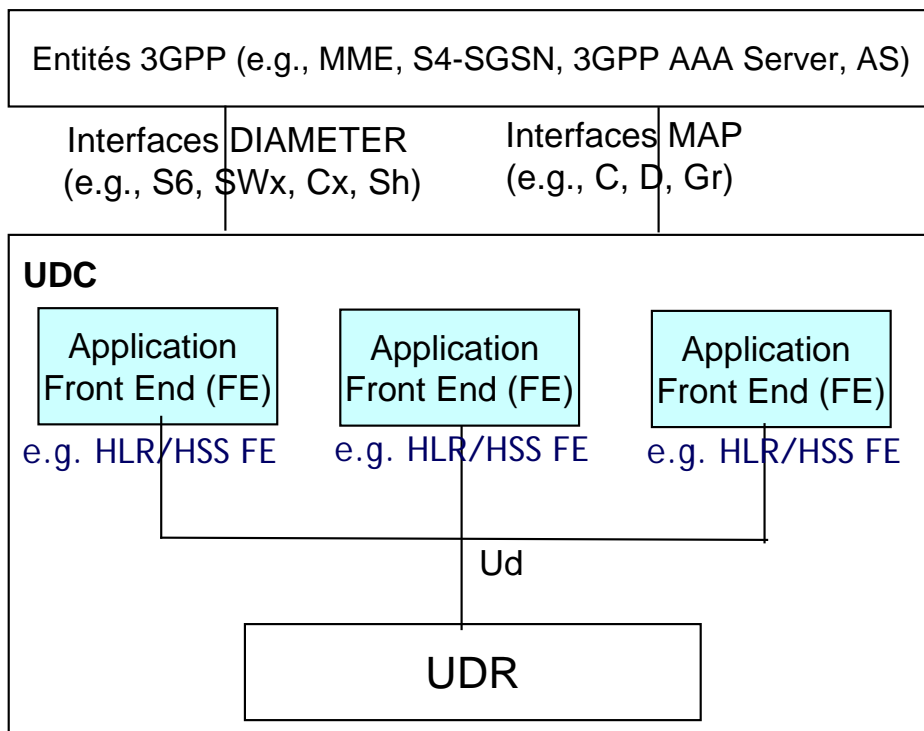


Figure 4 : Concept UDC

L'interface Ud utilise LDAP/TCP pour les procédures Ud Query, Create, Delete, Update.

- Ud Query correspond à LDAP Search.
- Ud Create correspond à LDAP Add.
- Ud Delete correspond à LDAP Delete.
- Ud Update correspond à LDAP Modify.

L'interface Ud utilise SOAP/HTTP pour les principes de Souscription/Notification.

L'application data view est un schéma LDAP.

Références

- 3GPP TS 29.272, Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol.
- 3GPP TS 29.273 Evolved Packet System (EPS); 3GPP EPS AAA interfaces
- 3GPP TS 29.335. User Data Convergence (UDC); User data repository access protocol over the Ud interface.
- 3GPP TS 29.002. Mobile Application Part (MAP) specification
- RFC 3588, P. Calhoun et al., Diameter Base Protocol, Sept 2003.