3ème Année du cycle ingénieur
Brique RMOB
Trimestre 2

Encadrant M. Philippe MARTINS

Etude des procédures d'enregistrement et d'établissement de session en IMS

Avril 2006

Par

MROUEH Lina et LABAKY Elie

Sommaire

Table des Figures

Remerciement

On tient à remercier de tout cœur Monsieur Philippe Martins pour son encadrement et de nous avoir donné l'occasion de travailler sur un sujet novateur comme l'IMS.

Résumé

Ce projet consiste à faire l'étude de la procédure d'enregistrement et d'établissement de session dans les réseaux IMS.

Dans la première partie on présentera en gros l'architecture fonctionnelle de l'IMS ainsi que la gestion des identités et le types de cartes à puces utilisé. Puis on présentera le type de signalisation dans l'IMS. Ces informations forment les prés requis pour les parties suivantes.

Dans la deuxième et la troisième partie on expliquera en détail respectivement la procédure d'enregistrement et la procédure d'établissement de session.

Introduction

A nos jours les pratiques technologiques sont en train d'évoluer, tel que l'Internet mobile, la téléphonie mobile, le multimédia… Les opérateurs estiment l'émergence des nouveaux services multimédia qu'il faut fournir indépendamment du temps, du lieu et des méthodes d'accès à travers des équipements mobiles. En réalité, ni le réseau RTC, ni l'Internet ne correspondent aux besoins futurs. On entend beaucoup aujourd'hui de la téléphonie sur IP et de la vidéo sur IP souvent dans les accès xDSL ; donc on se dirige vers une convergence des réseaux des télécommunications. Or cette convergence nécessite un nouveau réseau qui est le NGN (Next Generation Network) qu'on peut appeler « New Generation Network » comme il n'est plus « Next ».

On envisage utiliser un même plan de transport pour offrir à la fois les services réseaux de données et les services télécoms comme la vidéo et la voix. Ceci nécessite le déploiement d'un réseau de transport commun donnant tous les types de QoS, ainsi que le développement d'une architecture de service commune et un plan contrôle.

De son coté l'IMS sera le plan contrôle de cette nouvelle infrastructure NGN où l'IP sera le plan transport. L'IMS est une architecture softswitch avec une couche service très évoluée ce qui permet de réaliser des services télécoms traditionnels et des nouveaux services multimédia. Avec l'architecture softswitch on a procédé à la rupture du lien étroit entre le plan transport (Matrice de commutation) et le plan de contrôle des commutateurs (Unité de contrôle). Dans IMS, le plan contrôle sera basé SIP avec un plan transport unifier IP. L'originalité d'IMS est le faite d'être transparent aux réseaux d'accès qui peuvent être des réseaux mobile (GSM, UMTS…) ou fixe (RTC, xDSL…) et ceci à travers une couche transport unique IP. Donc l'IMS sera le même réseau d'infrastructure pour les réseaux fixe et mobile et il assurerait une double convergence fixe/Mobile, circuit/paquet. Actuellement l'IMS est normalisé par le 3GPP comme une nouvelle évolution des réseaux mobiles.

La révolution majeure introduite par l'IMS dans le monde des télécommunications est le passage du mode « Visited Service Control » au « Home Service Control ». Ce nouveau paradigme permet à un terminal de rester attacher au même réseau nominal quelque soit le réseau visité et tous les services de l'utilisateur seront effectué et contrôlé par le réseau nominal sans aucun chargement de profil dans le réseau visité. Or dans l'ancienne approche on devait télécharger le profil de l'utilisateur du réseau nominal au réseau visité ainsi que des marques CAMEL par exemple pour que la plateforme de service du réseau nominal puisse manipuler les switch du réseau visité afin d'offrir le même service à l'utilisateur dans le réseau visité.

1. Présentation de l'architecture IMS

1.1. L'architecture fonctionnelle de l'IMS

Dans cette partie, on va faire une description synthétique des différents composants de l'architecture IMS :

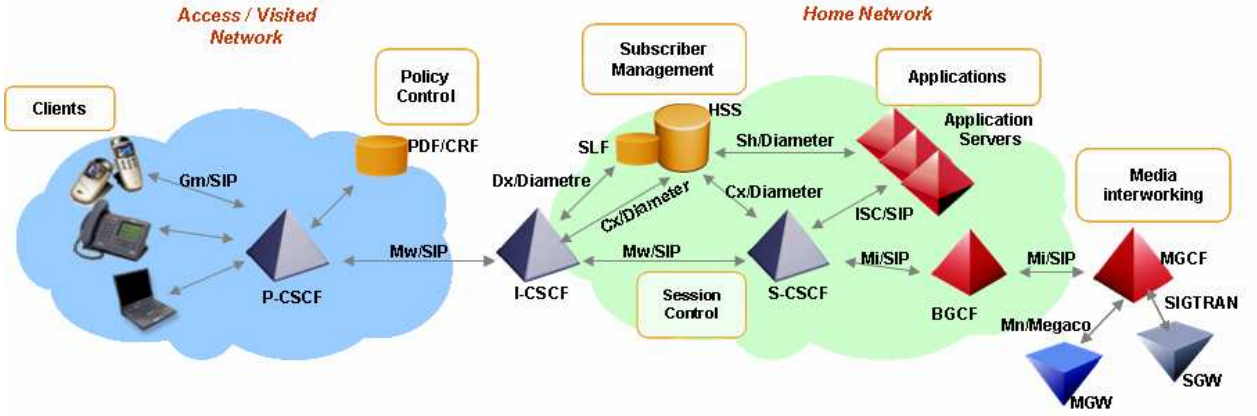

Figure 1.1.a : Architecture fonctionnelle IMS.

HSS : Home Subscriber Server

- Le HSS est l'équivalent du HLR de GSM.
- Elle contient toutes les informations nécessaires à un utilisateur pour ouvrir une session multimédia :
  - des informations sur la localisation de l'utilisateur.
  - le profil de l'utilisateur c'est à dire l'ensemble des services auxquels l'utilisateur est abonné.
  - L'adresse du S-CSCF alloué à l'utilisateur.
  - Des informations de sécurités.
- Le SLF est une base de données contenant pour chaque utilisateur le HSS correspondant dans le cas ou le réseau contient plusieurs HSS.

C-CSCF: Call/Session Control Function

Le C-CSCF est un serveur SIP qui traite la signalisation SIP en IMS. Il existe 3 types de C-CSCF :

P-CSCF: Proxy CSCF

Le P-CSCF est le premier point de contact usagers avec IMS : Toute la signalisation SIP du UE et vers le UE passe via le P-SCSF. Le P-CSCF est alloué à l'utilisateur dans la phase de registration et ne change pas durant toute la durée de registration. Le P-CSCF peut être localisé dans le home network, comme dans le visited network.

Les différentes fonctionnalités :

- Sécurité :
  - Il maintient des associations de sécurité IPsec entre lui et l'équipement terminal.
  - Authentification de l'utilisateur.
- Il maintient un cache local pour la localisation du S-SCSF associé à l'utilisateur.
- La compression / décompression des messages SIP.
- Le P-CSCF inclut les fonctionnalités du Policy Decision Function (PDF). Le PDF gére les exigences QoS pour les services et authorise l'allocation des ressources.
- La génération de CDRs (Call Detailed Record)→ taxation.

I-CSCF : Interrogating – CSCF

- L'I-CSCF est localisé dans le home network.
- Fait une première autorisation pour l'accès au réseau IMS.
- Pour une requête SIP, il contacte le HSS pour identifier le S-CSCF correspondant et renvoie les messages de cette session à ce S-CSCF (Protocole Diameter sur l'interface I-CSCF – HSS).
- Peut incluse une fonctionnalité de masquage de l'architecture du réseau de l'opérateur par rapport au réseau visité.

S-CSCF : Serving CSCF

Les fonctions réalisées par le S-CSCF pendant une session comprennent :

- Le S-CSCF est toujours localisé dans le home network.
- SIP Registrar : Il maintient l'association entre l'adresse IP du terminal et le SIP adresse de l'utilisateur (Public User Identity).
- Télécharger le profil de l'utilisateur de HSS :
  - A travers les « filter criteria », le S-CSCF envoi les requêtes SIP satisfaisant ces critères vers des serveurs d'applications correspondant au service demandé. De cette façon il fourni des services de type réseau intelligent (Signalisation d'intelligence).
  - Authentification, enregistrement.
- Service de translation : Consultation du DNS pour traduire le TEL-URI en SIP-URI.
- Il obtient l'adresse de l'I-CSCF dans le réseau destinataire lors de l'établissement de session.

Serveurs d'applications (AS)

Il y a 3 types de serveur qui agissent comme un serveur SIP du point de vue du réseau IMS.

- Serveur SIP d'application qui effectue des services IP multimédia basé SIP.
- OSA-SCS (Open Service Access – Service Capability Server): C'est une gateway OSA qui implémente l'API Parlay. Elle permet à des serveurs d'application tiers d'accéder au réseau IMS d'une façon sécurisé pour fournir des services aux utilisateurs.

- IMS-SSF (IP Multimedia Service Switching Function) : permet de réutiliser les services CAMEL développer pour les technologies GSM et GPRS. Donc une gsmSCF peut contrôler une session IMS grâce à ce serveur.

MRF : Media Ressource Function

- Le MRF est divisé en deux nœuds :
  - Signaling plane node : MRFC (Media Ressource Function Controller)
    - SIP user Agent : La MRFC interprète la signalisation SIP reçu via S-CSCF
  - Media Plane node : MRFP (Media Ressource Function Processor). La MRFP offre les ressources du plan usager qui sont demandés et commandés par la MRFC et réalise les fonctions suivantes :
    - Mixage des flux Media provenant du UE
    - Traitement du flux média (ex : transcodage audio, analyse du média).
    - Source de flux média (pour les annonces multimédia).

BGCF: Breakout Gateway Control Function

- Serveur SIP qui possède des fonctionnalités de routage lorsqu'il s'agit d'une session initié par un terminal IMS et destiné à un utilisateur dans un réseau commuté circuit (cas de PSTN, PLMN).
- Présente deux fonctionnalités essentielles :
  - Choisir le réseau approprié pour s'interfacer avec le domaine CS.
  - Ou choisir un Gateway (MGCF) si le passage vers le CS a eu lieu dans le même réseau que le BGCF.

PSTN/CS Gateway

Les PSTN gateways constituent une interface vers les réseaux commutés circuit. Cette interface présente plusieurs entités fonctionnelles suivant l'architecture Softswitch :

- **SGW : Signalling Gateway**

  C'est la fonction de transcodage de signalisation, qui permet grâce à SIGTRAN de transporter la signalisation SS7 sur IP, et d'avoir une interface NNI de signalisation avec les réseaux à commutation de circuits.
  - Effectue des conversions dans les protocoles de couche bas (Transport) transport : Remplace la couche de transport MTP de SS7 par SCTP (Stream Control Transmission Protocol) sur IP.
  - Conversion d'ISUP/MTP en ISUP/SCTP/IP.
- **MGCF/ Media Gateway Control Function**

  Elle permet de contrôler les MGW, et elle s'interface avec la SGW grâce à SIGTAN pour l'échange de la signalisation.
  - passerelle qui permet la communication entre IMS et les usagers dans le domaine de commutation de circuits CS.
  - Conversion de l'ISDN User Part (ISUP) ou le Bearer Independent Call Control (BICC) en protocole SIP.
- **MGW Meadi Gateway**
  - Interface pour le plan de données entre le réseau IMS/IP et les réseaux PSTN à commutation de circuit. (Transport de la voix).

- D'un côté, elle est capable d'envoyer et de recevoir flux IMS sur le protocole RTP Real-Time Protocol.
- D'un autre côté, utilise le PCM (Pulse Code Modulation) pour coder la voix et la transmettre sur des times slots au réseau CS.

- Fonction de transcodage quand le terminal IMS ne supporte pas le codesc utilisé par le CS. Par ex, Terminal IMS utilise AMR, tandis que le terminal PSTN utilise G711.

1.2. Gestion des identités en IMS

Comme dans tout type de réseau, il est impératif de pouvoir identifier les utilisateurs d'une façon unique de telle manière qu'ils soient joignables de n'importe quel réseau. Dans IMS il y a un nouveau concept d'identification par rapport à ce qui ce faisait dans les réseaux mobile tout en restant compatible avec. Cette identification peut paraître un peu étrange et compliqué mais elle fourni plus de flexibilité pour réaliser des nouveaux services. (La technique d'identification est prise de SIP)

1.2.1. Public User Identity

C'est une adresse publique qui permet d'identifier un utilisateur. L'opérateur attribut une ou plusieurs adresse publique pour chaque utilisateur IMS. C'est la grande nouveauté, ce qui permet à l'utilisateur de séparer son identité personnel, familiale et d'affaire pour générer des services différents. L'identité publique de l'utilisateur est l'équivalent du MSISDN en GSM, donc c'est une adresse de contacte qui permet de joindre un abonné, elle sert à router les messages SIP. La Public User Identity peut être sous deux formats :

- SIP URI : sous la forme « sip : premier.dernier@opérateur.com ». Il est aussi possible d'inclure un numéro de téléphone dans une SIP URI qui sera sous le format : « sip : +1-961-007-007@opérateur.com ; user=phone ».
- TEL URL : permet de représenter un numéro de téléphone dans un format international « tel : +1-961-007-007 ». Il est impossible de s'enregistrer avec un TEL URL, il faut toujours une SIP URI pour se faire. Mais le TEL URL est utilisé pour faire des appels entre le monde RTC et le monde IMS. Or en RTC les téléphones sont identifiés par des numéros et ne peuvent composer que des numéros. Donc l'opérateur IMS doit allouer à chaque utilisateur au moins une SIP URI et un TEL URL.

1.2. Private User Identity

On affecte une identité privée pour chaque utilisateur. Cette identité joue le même rôle que l'IMSI en GSM, elle permet d'authentifier l'abonné et pour l'enregistrement. Elle prend le format d'un « Network Access Identifier » qui est la suivante : « username@opérateur.com ». La Private User Identity est stockée dans la carte à puce.

1.2.3. Relations entre Public et Private User Identity

Dans le cas GSM/UMTS, la carte à puce stocke l'identité privée et au moins une identité publique. Le HSS contient pour chaque utilisateur son identité privée et la collection

d'identité publiques qui lui est attribué. Notons que dans le cas ou l'utilisateur utilise une carte GSM/UMTS qui ne contient pas ces informations, le terminal est capable de les construire à travers l'IMSI (Voire la procédure d'enregistrement par USIM). La relation entre l'utilisateur IMS et ces identités dans la Release 5 est montré par la figure suivante :

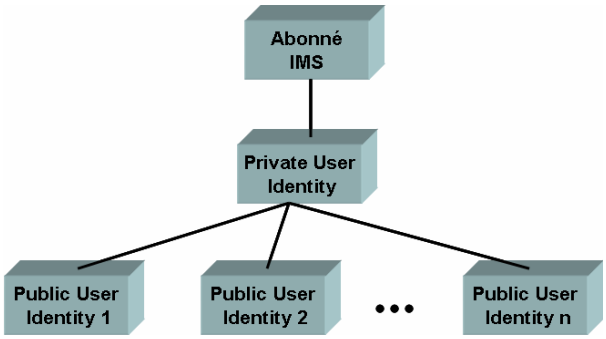

Figure 1.2.3.a : Relation entre l'identité privée et publiques en IMS 3GPP R5.

Dans l'IMS 3GPP Release 6, un abonné peut avoir plusieurs identités privées. Dans le cas de l'UMTS seulement une identité privée peut être contenu dans la carte à puce mais l'utilisateur peu avoir plusieurs cartes contenant chacune une identité privée différente. Il est encore possible d'utiliser simultanément la même identité publique avec plusieurs identités privées (deux cartes insérées dans deux terminaux différents).

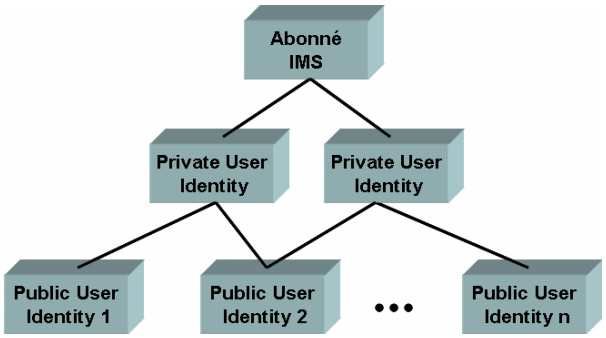

Figure 1.2.3.b : Relation entre l'identité privée et publiques en IMS 3GPP R6.

1.3. Les cartes USIM et ISIM

Dans chaque terminal, il y a une carte à puce appelée UICC (Universal Integrated Circuit Card). L'UICC est utilisé pour stocker des informations telles que l'état d'enregistrement, clefs d'authentifications, message et un carnet d'adresses. L'UICC contient plusieurs applications logiques qui peuvent être : la SIM, l'USIM et l'ISIM.

1.3.1. USIM (Universal Subscriber Identity Module)

Elle est utilisée pour l'accès au réseau UMTS en mode circuit ou paquet. Elle contient les paramètres suivants :

- IMSI : comme en GSM elle permet d'identifier l'utilisateur et l'authentifier. La Private user Identity est l'équivalent à l'IMSI mais en IMS.

- MSISDN : contient une ou plusieurs numéros de téléphone pour l'utilisateur. La Public User Identity est l'équivalent au MSISDN mais en IMS.
- CK (Ciphering Key) et IK (Integrity Key) : se sont les clefs de chiffrement et d'intégrité utilisés pour la sécurité de l'information sur l'interface radio.
- Long term secret : secret utilisé pour authentifier l'utilisateur et pour générer les clefs de chiffrement et d'intégrité utilisé entre le terminal et le réseau.
- SMS : Dans ce champ on va stocker les messages courts (reçu et envoyé avec leur état).
- SMS parameters : paramètres de configuration du service SMS (exemple : adresse du SMS centre).
- MMS user connectivity parameters : contient les paramètres de configuration du service MMS (exemple : adresse du MMS server et du MMS gateway).
- MMS user preferences : contient les préférences de l'utilisateur sur le service MMS comme le drapeau de rapport d'expédition.

1.3.2. ISIM (IMS Subscriber Identity Module)

Elle contient les paramètres utilisés pour l'identification et l'authentification de l'utilisateur ainsi que la configuration du terminal IMS. ISIM peut co-exister simultanément avec une USIM ou une SIM. Les paramètres essentiels contenus dans une ISIM sont :

- Private User Identity
- Public User Identity
- Home Network Domain URI : SIP URI du réseau nominal de l'utilisateur qui est unique dans la carte.
- Long-term secret : secret utilisé pour authentifier l'utilisateur et pour générer les clefs de chiffrement et d'intégrité utilisé entre le terminal et le réseau. Les messages SIP envoyés entre le terminal et le P-CSCF sont chiffrés et protégés par la clef d'intégrité.

1.4. Type de Signalisations en IMS

Dans tout type de réseau il y a toujours quatre types de signalisations ; dans IMS la signalisation est réaliser essentiellement par SIP :

- Signalisation d'enregistrement : c'est la signalisation par la qu'elle un terminal s'enregistre dans le réseau. Elle contient les procédures de téléchargement du profile et la gestion de la localisation. Cette signalisation est effectuée par la procédure d'enregistrement SIP (SIP REGISTER).
- Signalisation d'appel : c'est la signalisation par la qu'elle on établit une association de bout en bout entre les points d'extrémité désirant communiquer, c'est caractérisé par l'échange de référence. Ceci est réalisé en IMS grâce à la procédure d'établissement de session (SIP INVITE).
- Signalisation de connexion : c'est l'affectation d'un service support à un appel. De proche en proche on va réserver des ressources dans le réseau selon la QoS requise pour le service. Au niveau SIP cette signalisation est effectuée grâce aux entêtes SDP qui permettent de décrire le trafic et le ressources requis. Au niveau transport on utilise les mécanismes RSVP, DiffServ, MPLS pour faire la qualité de service dans le réseau IP.
- Signalisation d'intelligence : c'est la signalisation qui nous permet de faire un traitement substitutif par rapport au traitement d'appel normal. D'une façon similaire

aux réseaux intelligent de type RI (INAP) ou CAMEL, les services sont exécuter par l'équivalant aux plateformes de service qui sont des serveurs d'applications (AS). Un autre type de signalisation SIP est utilisé sur l'interface ISC entre les AS et les S-CSCF.

Comme SIP ne décrit pas le flux média on utilise en plus le protocole SDP (Session Description Protocol). SDP est transporté dans le cœur des messages SIP et il décrit les sessions multimédia en termes de codeur audio, vidéo, informations de session (bande requise, type de flux…) et adressage multicast…Ces informations seront exploitées pour faire la réservation de ressource dans le plan transport.

Certaines interfaces internes du réseau IMS utilisent la signalisation « Diameter » et nom pas SIP. C'est une application standardisé par le 3gpp qui permet d'interfacer différentes entité du réseau IMS. Les échanges Diameter sont toujours du type un message requête et une réponse associé. Les informations échangées dans ces messages sont mis dans des attributs appelés AVP (Attribute Value Pairs). Chaque interface Diameter a ces AVPs et ces commandes.

2. Procédure d'enregistrement dans IMS ➔ REGISTER

2.1. Préambule

Dans cette partie, on va expliquer le déroulement de la procédure d'enregistrement en IMS. C'est une procédure d'accès au réseau IMS qui permet à un terminal de se déclarer joignable de point de vue service IMS. Comme tout autre procédure d'accès (Mise à jour de localisation GSM, attachement GPRS…), le terminal sera authentifié par le réseau IMS et son profil sera chargé dans le S-CSCF nominal qui est une sorte de central de rattachement ou un MSC/VLR qui est alloué à l'utilisateur quelque soit sa localisation dans le monde. Le S-CSCF contient l'adresse du Proxy P-CSCF où le terminal est rattaché (équivalent à un BSC pour caricaturier).

Il faut garder à l'esprit que le réseau IMS est en dessus de tous types de réseaux qui peuvent servir à l'attachement du terminal au système IMS (GSM, GPRS, UMTS, WiMax, xDSL, RTC…). De plus toutes les procédures d'enregistrement, authentification et chargement de profiles qui se font au niveau IMS sont indépendantes des procédures dans les réseaux d'accès. La localisation géographique du terminal n'est plus importante car il sera toujours rattaché à son réseau nominal à travers le Proxy du réseau visité.

Afin d'expliquer la procédure, on va prendre l'hypothèse que le terminal est un terminal UMTS qui est dans son réseau nominal et que l'utilisateur s'attache au service IMS de son opérateur. Donc au préalable le mobile à déjà établit un contrat d'accès au service IMS de son opérateur UMTS. (C'est la même procédure si l'utilisateur est dans un réseau visité).

La procédure d'enregistrement se fait en plusieurs étapes :

1. Attachement au réseau UMTS.
2. Activation d'un Contexte PDP, avec obtention d'une adresse IPv6 et d'un APN qui donne une connexion vers le réseau IMS à travers une connectivité IPv6.
3. Découvert du P-CSCF.
4. Enregistrement IMS.
5. Souscription à l'état d'enregistrement du mobile « reg Event State ».

Concernant l'obtention d'une adresse IP, après que le mobile soit attaché au réseau UMTS, il demande l'ouverture d'un PDP contexte au SGSN demandant l'accès à un APN (Access Point Name) particulier et la connectivité à un réseau IPv6. L'APN désigne la connexion vers un réseau IMS. En fonction de cet APN et le type de connectivité le SGSN choisi le GGSN approprié et ouvre avec lui la suite du PDP contexte. Le GGSN va fournir au mobile un préfixe d'adresse IPv6 de 64bits (au lieu d'une adresse complète) et l'envoie dans la réponse à l'ouverture du PDP contexte. Le SGSN transmet d'une façon transparente le préfixe IPv6 au terminal qui lui va choisir aléatoirement un suffixe IPv6 de 64bits, pour former en tout, une adresse IPv6 de 128bits. Notons que si l'IP CAN n'est pas du type GPRS/UMTS, le terminal obtiendra une adresse IPv6 en utilisant probablement un protocole tel que le DHCPv6.

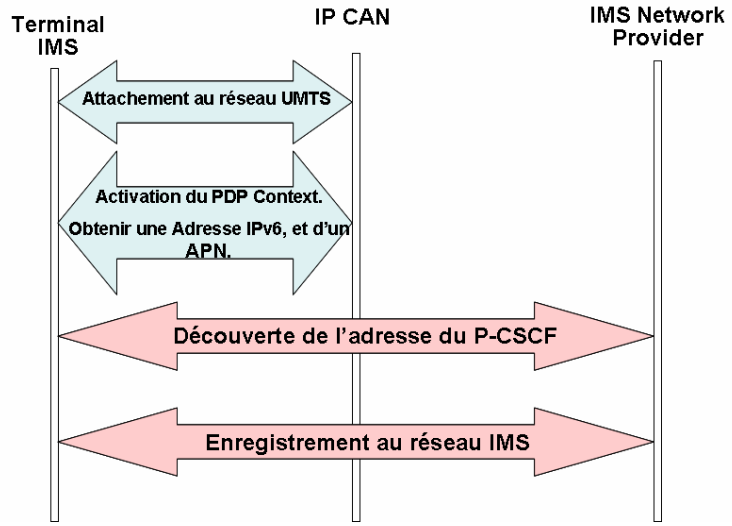

Figure 2.1.a : Procédure générale pour obtenir le service IMS.

2.2. Procédure d'enregistrement

La procédure d'enregistrement est constituée de plusieurs étapes. Tout d'abord le terminal doit obtenir l'adresse IP du P-CSCF cette procédure s'appel P-CSCF Discovery. Puis la procédure d'enregistrement au niveau IMS dans la qu'elle plusieurs fonctionnalité seront satisfaites.

2.2.1. Découverte du P-CSCF

Il y a deux façons pour obtenir l'adresse IP de P-CSCF :

- Intégré (Integrated) dans la procédure d'accès à l'IP CAN : Donc lors de l'établissement du PDP contexte le terminal obtiendra non seulement une adresse IPv6 et un APN mais aussi l'adresse du P-CSCF.
- La stand-alone, dans la qu'elle la découverte du P-CSCF se fait grâce à l'utilisation du DHCPv6 et du DNS.

Une fois un P-CSCF est alloué à un utilisateur il le sera toujours jusqu'à la prochaine découverte de P-CSCF. Et le terminal IMS n'a pas à s'inquiété si l'adresse du P-CSCF à changé car elle est fixe.

2.2.2. L'Enregistrement IMS (avec un ISIM)

Après avoir obtenu l'adresse du P-CSCF, le terminal envoie une requête SIP REGISTER. Cette procédure permet à l'utilisateur d'associer son URI publique à une URI qui contient l'adresse IP ou le host name de la machine où l'utilisateur est logué. En effet, l'URI publique ne permet pas la localisation de l'utilisateur car elle n'est pas routable, d'où la nécessité de l'associer à une adresse routable tel qu'une adresse IP.

On distingue deux façons pour faire l'enregistrement IMS. La différence réside dans la méthode d'authentification qui est appliqué. Or pour authentifier les utilisateurs le terminal devra être équipé par un UICC, qui peut inclure une application ISIM, USIM ou les deux.

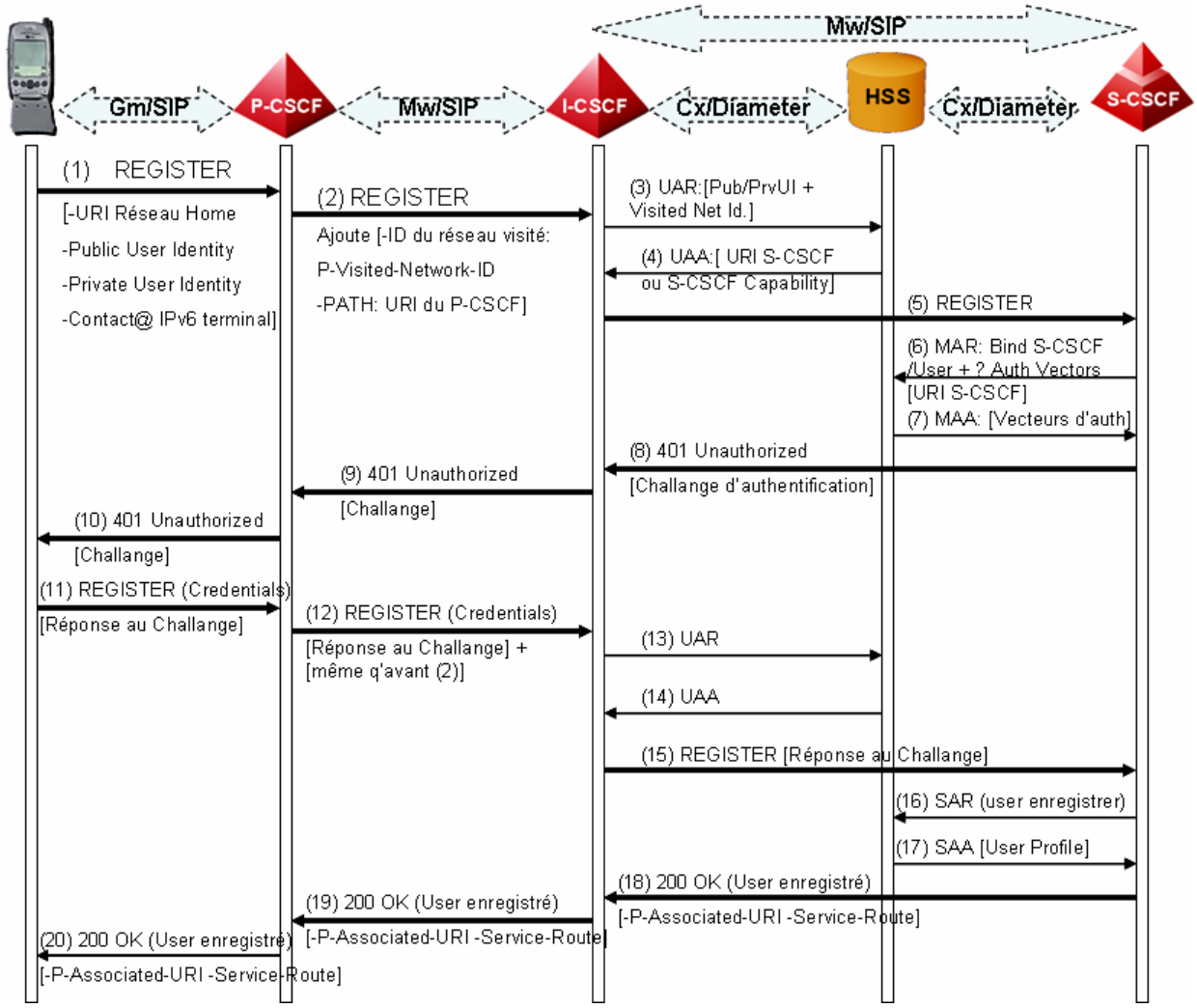

Figure 2.2.2.a : Procédure d'enregistrement.

La procédure d'enregistrement très similaire dans les deux cas même si quelque détail sont différents. On prendra dans un premier temps l'enregistrement utilisant une carte ISIM.

La procédure d'enregistrement permet de réaliser les fonctionnalités suivantes :

- Effectuer l'association entre une « Public User Identity » et une adresse IP de contacte.
- Le réseau nominal authentifie l'utilisateur.
- L'utilisateur authentifie son réseau nominal.

- Le réseau nominal IMS autorise l'enregistrement de l'utilisateur et l'utilisation des ressources IMS.
- Si le P-CSCF est localisé dans un réseau visité, le réseau nominal vérifie s'il y a un accord de roaming entre eux et en conséquence il autorise l'utilisation du P-CSCF.
- Le réseau nominal informe l'utilisateur des autres adresses qu'il lui a alloué.
- Le terminal IMS négocie avec le P-CSCF les mécanismes de sécurité à utilisé pour la signalisation qui suit. Ils établissent un ensemble de mécanismes de sécurité pour assurer l'intégrité des messages SIP envoyés.
- Le terminal IMS et le P-CSCF échangent leurs algorithmes de compression des entêtes SIP.

Afin de déclancher la procédure d'enregistrement, le terminal IMS extrait la Public User Identity, la Private User Identity et l'adresse du réseau nominale. Puis construit la requête SIP REGISTER et l'envoie au P-CSCF. Cette requête contient les paramètres suivant :

- Registration URI : SIP URI qui identifie le non de domaine du réseau nominal.
- Public User Identity : URI SIP qui représente l'identité de l'utilisateur sous enregistrement.
- Private User Identity : identité utilisé uniquement pour l'authentification.
- Contact address : URI SIP qui contient l'adresse IPv6 du terminal IMS pour joindre l'utilisateur.

Une fois la requête d'enregistrement est reçu par le P-CSCF il doit la relayer au I-CSCF du réseau nominal. En générale le P-CSCF peut ne pas être dans le réseau nominal de l'utilisateur. Donc il doit déterminer un point d'entré au réseau nominal qui est le I-CSCF, et ceci en faisant une requête DNS. Le P-CSCF insert dans l'entête SIP un champ « P-Visited-Network-ID » qui contient l'identifiant du réseau visité et un champ « Path » contenant son URI pour que le réseau nominal lui envoie les requêtes SIP destinées au mobil. Dans tous les cas les requêtes SIP passeront par le P-CSCF.

L'I-CSCF est un serveur « stateless » qui ne conserve aucun contexte d'enregistrement. En effet, l'I-CSCF peut varier d'une requête à une autre due au mécanisme de partage de charge DNS. Quand l'I-CSCF reçoit la requête d'enregistrement, il envoie une requête Diameter (UAR) au HSS qui répond par un (UAA). Le but de cet échange est de faire l'autorisation de l'utilisateur pour utiliser le réseau IMS et de voire s'il y a un S-CSCF alloué à l'utilisateur. Dans le Message UAR (User Authorization Request) l'I-CSCF envoie au HSS le Public User Identity, le Private User Identity et l'identificateur du réseau visité. Le HSS effectue les opérations suivantes :

- Vérifie que l'utilisateur défini par sa Public User Identity est un utilisateur légitime du système.
- Vérifie qu'il y a un accord de roaming avec le réseau visité.
- Fait une corrélation entre la Public User Identity et la Private User Identity pour des raisons d'authentification.
- Voit si il y a un S-CSCF alloué à l'utilisateur ou le I-CSCF doit choisir un.

La réponse du HSS sera dans le message UAA (User Authorization Answer), qui va contenir l'URI du S-CSCF qui a été déjà alloué à l'utilisateur. Dans le cas échéant (donc une première procédure d'enregistrement) le HSS envoie au I-CSCF un ensemble de capabilités que va utiliser le I-CSCF pour choisir le S-CSCF adéquat à l'utilisateur. Les capabilités sont divisé en deux catégories : capabilité obligatoire que le S-CSCF choisi doit au moins accomplir, et des capabilités optionnel que le S-CSCF peut ou pas les fournir. Ces capabilités

sont identifié par des entiers dont la sémantique est propriétaire à l'opérateur, l'interface Cx est interne. Le I-CSCF contient une table configurable qui à chaque S-CSCF dans le réseau elle lui associe les copabilités dont il est capable de fournir. De cette façon l'I-CSCF choisi le S-CSCF adéquat pour lui renvoyé la requête d'enregistrement.

Le S-CSCF reçoit la requête d'enregistrement et contacte le HSS pour deux raisons : le S-CSCF a besoin de télécharger les vecteur d'authentification pour authentifier l'utilisateur et enregistrer son URI dans le HSS pour que les requêtes suivantes concernant cet utilisateur soient rediriger vers lui. Le S-CSCF envoie un message Diameter MAR (Multimedia Authentication Request) sur l'interface Cx, pour demander les vecteur d'authentification du HSS et enregistre son URI dans le profile de l'utilisateur. Le HSS répond par un message MAA (Multimedia Authentication Answer) qui contient un ou plusieurs vecteurs d'authentification pour authentifier l'utilisateur.

Le S-CSCF crée un message « 401 Unauthorized » qui contient un défit dans l'entête « WWW-Authenticate » et l'envoie au terminal IMS. Ce message arrive au terminal IMS via un I-CSCF et le même P-CSCF. Le terminal détecte que ce message contient un défit, et répond par une nouvelle requête SIP REGISTER appelé « credentials » car elle contient une réponse à un défit. Le terminal extrait ou dérive les informations d'authentification de sa carte à puce (UICC) pour créer les « credentials ». De la même manière que la première requête REGISTER cette deuxième sera envoyée au P-CSCF qui va la relayer à l'I-CSCF. Il est très probable que le I-CSCF ne soit pas le même que le premier due au partage de charge. Donc l'I-CSCF fera la même procédure d'autorisation avec le HSS à travers les messages UAR et UAA, mais cette fois il va obtenir l'URI du S-CSCF qui a été alloué à l'utilisateur, donc la requête arrivera au même S-CSCF. Le S-CSCF vérifie la réponse au défit et si c'est correcte donc l'utilisateur est authentifié. Alors il informe le HSS que l'utilisateur est enregistré chez lui par un message Diameter SAR et demande le téléchargement du profile (ou du reste du profile) de l'utilisateur. Le HSS répond par le profile demandé au S-CSCF.

A ce stade là, le S-CSCF a stocké l'adresse URI de contacte de l'utilisateur qui lui permet de le rejoindre ainsi que la liste des « Path URI » qui permet de router les requêtes SIP vers l'utilisateur. (Les « Path URI » contiennent obligatoirement l'URI du P-CSCF et optionnellement les URI des I-CSCF).

A la fin le S-CSCF envoie une réponse 200 OK à l'utilisateur pour lui indiquer que la requête d'enregistrement est réussit. Cette requête contient un entête « P-Associated-URI » qui représente une liste d'URI alloué à l'utilisateur (qui identifient l'utilisateur). En plus on trouve un entête « Service-Route » qui contient une liste des URI des serveurs SIP qui seront utilisé pour router les requêtes SIP envoyé par le terminal, (l'URI du S-CSCF alloué à l'utilisateur est toujours présente dans cet entête). On note que l'utilisateur sera enregistré durent une période indiqué dans le paramètre « Expires » de l'entête « Contact ».

2.2.3. Enregistrement avec un USIM

Si on se place dans un contexte purement UMTS où le terminal n'a pas un ISIM mais plutôt un USIM. Dans ce cas l'utilisateur n'est pas capable d'obtenir une Private User Idententity, une Public User Identity et l'URI du réseau nominal. Mais le mobile dispose d'une IMSI, qui est un identifiant international unique pour l'utilisateur. Cet identifiant sera exploité pour que le terminal puisse construire une Private User Idententity temporaire, une Public User Identity temporaire et l'URI du réseau nominal. Ceci va permettre à l'utilisateur de construire une requête SIP REGISTER. Après l'enregistrement l'utilisateur obtiendra des Public User Identities qu'il utilisera dans les requêtes SIP suivante.

- Private User Identity temporaire : elle est toujours du format username@realm. L'IMSI sera l'username. Supposons qu'on a un IMSI=2483235551234, tel que le MCC=248, le MNC=323 et le MSIN=5551234. Donc la Parivate User Identity temporaire sera : « 2483235551234@323.248.imsi.3Gppnetwork.org ». La chaîne .imsi.3Gppnetwork.org est toujours fixe.
- Public User Identity temporaire : Elle a le même forma que la Parivate User Identity temporaire, mais précéder par la chaîne « sip : ».
  (« sip : 2483235551234@323.248.imsi.3Gppnetwork.org »).
- URI du réseau nominal : est obtenu en enlevant la parie user de la Public User Identity donc le format : « sip : 323.248.imsi.3Gppnetwork.org ».

La procédure d'enregistrement reste toujours la même, mais le contenu des messages sera différent. Et le S-CSCF va télécharger des vecteurs d'authentifications du HSS en ligne avec l'USIM, et l'authentification se fait comme en UMTS avec les quintuplés.

2.2.4. Les Messages SIP

1. (1) REGISTER :

```
REGISTER sip : home1.net SIP/2.0
Via : SIP/2.0/UDP [1080::8:800:200C:417A];comp=sigcomp;
     Branch=z9hG4bk9h9ab
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD;
                       Utran-cell-id-3gpp=C3559A3913B20E
From: <sip:alice@home1.net>;tag=s8732n
To: <sip:alice@home1.net>
Contact: <sip:[1080::8:800:200C:417A];comp=sigcomp>
          ;expires=600000
Call-ID: 23fi57lju
Authorization: Digest username= "alice_private@home1.net",
                Realm= "home1.net", nonce= "",
                Uri= "sip:home1.net", response= ""
Security-Client: ipsec-3gpp; alg=hmac-sha1-1-96;
                       Spi-c= 3929102; spi-s= 0293020;
                       Port-c: 3333; port-s=5059
Require: sec-agree
Proxy-Require : sec-agree
CSeq : 1 REGESTER
Supported: path
Content-Length: 0
```

- L'URI « home1.net » représente l'URI du réseau nominal vers le qu'elle la requête sera routé.
- Le champ « Via » contient l'adresse IPv6 que le terminal à obtenu durant l'activation du PDP Contexte.
- Le champ « P-Access-Network-Info » représente des informations concernant le type de réseau d'accès, dans notre cas c'est un réseau UMTS TDD.
- L'identité publique de l'utilisateur qui a émit cette requête est contenu dans le champ « From ». Cette identité peut être obtenue d'une ISIM ou une USIM.

- Le champ « To » contient aussi l'identité publique de l'utilisateur qui sera enregistré. Cette identité permet aux autres de reconnaître cet utilisateur. De même elle peut être obtenue d'une ISIM ou une USIM.
- Le champ « Contact » indique l'adresse IPv6 de l'utilisateur. C'est une adresse temporaire qui permet de joindre l'utilisateur, comme un point de contacte. Les requêtes destinées à cet utilisateur seront envoyé vers cette adresse. Le S-CSCF va stocker cette information.
- Le champ « Authorization » contient des informations d'authentifications. L'identité privée de l'utilisateur est dans le champ « username » (alice_private@home1.net). Le champ « Realm » contient le mon du réseau au l'utilisateur sera authentifier. Le champ « uri » est similaire au « Realm » car c'est obtenu du même champ de l'USIM ou l'ISIM.
- La partie « Security-Client » contient l'ensemble des algorithmes de sécurités que le terminal sait faire.
- Le champ « Supported » indique au récepteur de cette requête que le terminal supporte l'entête « Path ».

2. (5) REGISTER:

```
REGISTER sip : home1.net SIP/2.0
Via : SIP/2.0/UDP icscf1.home1.net; branch=z9hg4bkea1dof,
     SIP/2.0/UDP pcscf1.visited1.net; branch=z9hg4bkoh2qrz,
     SIP/2.0/UDP [1080::8:800:200C:417A];comp=sigcomp;
          Branch=z9hG4bk9h9ab
Max-Forwards: 68
P-Access-Network-Info: 3GPP-UTRAN-TDD;
                       Utran-cell-id-3gpp=C3559A3913B20E
From: <sip:alice@home1.net>;tag=s8732n
To: <sip:alice@home1.net>
Contact: <sip:[1080::8:800:200C:417A];comp=sigcomp>
          ;expires=600000
Call-ID: 23fi57lju
Authorization: Digest username= "alice_private@home1.net",
               Realm= "home1.net", nonce= "",
               Uri= "sip:home1.net", response= ""
               Integrity-protected="no"

Require: path
Supported: path
Path: <sip:term@pcscf1.visited1.net;lr>
P-Visited-Network-ID: "Visited 1 Network"
P-Charging-Vector: icid-value="W34h6dlg"
CSeq: 1 REGISTER
Content-Length: 0
```

- L'I-CSCF n'effectue aucune modification sur la requête d'enregistrement mais comme le P-CSCF il va ajouter son adresse dans la partie « Via ».
- Pour s'assurer que les requêtes SIP à destination du terminal passent toujours par lui, le P-CSCF ajoute son adresse dans le champ « Path ». Donc le S-CSCF saura où envoyer les requêtes.
- Le P-CSCF ajoute le champ « P-Visited-Network-ID », ce champ contient le nom de domaine ou une autre adresse qui permet d'identifier le réseau visité ou se trouve le P-CSCF.

- Le champ « Require » permet au récepteur de traiter correctement l'entête « Path ». Si le récepteur ne supporte pas cette adresse il génère une erreur 420 indiquant que le message à été routé par erreur en dehors du sous système IMS.
- Le P-CSCF ajoute aussi le champ « P-Charging-Vector » et alimente le paramètre « icid » par une valeur unique.
- Le P-CSCF enlève l'entête « Security-Client » et l'option « sec-agree » car il veut un entête vide.

3. (10) 401 UNAUTHORIZED

```
SIP/2.0 401 Unauthorized
Via : SIP/2.0/UDP [1080::8:800:200C:417A];comp=sigcomp;
     Branch=z9hG4bk9h9ab
From: <sip:alice@home1.net>;tag=s8732n
To: <sip:alice@home1.net>; tag=409sp3
Call-ID: 23fi57lju
WWW-Authenticate: Digest realm=”home1.net”,
          Nonce=”dcd98b7102dd2f0e8b11d0f600bfb0c093”,
          Algorithm=AKAv1-MD5
Security-Server: ipsec-3gpp; q=0.1; alg=hmac-sha1-1-96;
                     Spi-c= 909767; spi-s= 421909;
                     Port-c: 4444; port-s=5058
CSeq: 1 REGISTER
Content-Length: 0
```

- Le message « 401 Unauthorized » reçu par le P-CSCF est différent de celui-ci qui est envoyé au terminal par le P-CSCF. Or le message reçu par le P-CSCF contient en plus dans la partie « WWW-Authenticate » la clef d'intégrité IK et la clef de chiffrement CK, que le S-CSCF à mis. (Notons que le message du tableau ci-dessus est celui reçu par le terminal, et le terminal dérive IK et CK de son USIM comme en UMTS).
- Dans la partie « WWW-Authenticate » de ce message on trouve le défit envoyé par le S-CSCF pur authentifier l'utilisateur (nonce). Ce « nonce » est formé par la concaténation d'un AKA RAND, AKA AUTH et des données spécifiques au serveur.
- Dans le champ « Security-Server » on trouve le paramètre « q », qui indique qu'elle mécanisme de sécurité utiliser en premier. Dans notre cas le 0.1 indique l'IPSec.

4. (11) REGISTER (Credentials):

```
REGISTER sip : home1.net SIP/2.0
Via : SIP/2.0/UDP [1080::8:800:200C:417A];comp=sigcomp;
     Branch=z9hG4bk9h9ab
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD;
                     Utran-cell-id-3gpp=C3559A3913B20E
From: <sip:alice@home1.net>;tag=s8732n
To: <sip:alice@home1.net>
Contact: <sip:[1080::8:800:200C:417A];comp=sigcomp>
          ;expires=600000
Call-ID: 23fi57lju
Authorization: Digest username= “alice_private@home1.net”,
                Realm= “home1.net”,
                nonce= “dcd98b7102dd2f0e8b11d0f600bfb0c093”,
                Algorithm=AKAv1-MD5,
```

```
                Uri= “sip:home1.net”,
                Response= ”6629fae49393a0539740978507c4ef1”
Security-Verify: ipsec-3gpp; ; q=0.1; alg=hmac-sha1-1-96;
                     Spi-c= 909767; spi-s= 421909;
                     Port-c: 4444; port-s=5058
Require: sec-agree
Proxy-Require : sec-agree
CSeq : 2 REGESTER
Supported: path
Content-Length: 0
```

Ce message représente la réponse à la requête d'authentification émise par le S-CSCF.

- Le champ « Athorization » contient la réponse au défit déjà reçu par le terminal, dans le paramètre « Response ». et contient aussi l'identité privée de l'utilisateur, le « Realm », le « nonce », l' « URI » et les algorithmes. Se message est protéger par IPSec déjà négocié.
- Le champ « Security-Verify » contient l'accord sur les mécanismes de sécurité comme convenu dans le « Security-Server » du message précèdent.

5. (15) REGISTER

```
REGISTER sip : home1.net SIP/2.0
Via : SIP/2.0/UDP icscf1.home1.net; branch=z9hg4bkea1dof,
     SIP/2.0/UDP pcscf1.visited1.net; branch=z9hg4bkoh2qrz,
     SIP/2.0/UDP [1080::8:800:200C:417A];comp=sigcomp;
          Branch=z9hG4bk9h9ab
Max-Forwards: 68
P-Access-Network-Info: 3GPP-UTRAN-TDD;
                     Utran-cell-id-3gpp=C3559A3913B20E
From: <sip:alice@home1.net>;tag=s8732n
To: <sip:alice@home1.net>
Contact: <sip:[1080::8:800:200C:417A]:5059;comp=sigcomp>
          ;expires=600000
Call-ID: 23fi57lju
Authorization: Digest username= “alice_private@home1.net”,
                Realm= “home1.net”,
                nonce= “dcd98b7102dd2f0e8b11d0f600bfb0c093”,
                Algorithm=AKAv1-MD5,
                Uri= “sip:home1.net”,
                Response= ”6629fae49393a0539740978507c4ef1”
                Integrity-protected=”yes”
Require: path
Supported: path
Path: <sip:term@pcscf1.visited1.net;lr>
P-Visited-Network-ID: “Visited 1 Network”
P-Charging-Vector: icid-value=”W34h6dlg”
CSeq: 2 REGISTER
Content-Length: 0
```

C'est la réponse au défit reçu par le S-CSCF, il subit la même chose que le message (5) REGISTER en gardant le champ « Authorization ».

6. (20) 200 OK

```
SIP/2.0 200 OK
Via : SIP/2.0/UDP [1080::8:800:200C:417A]:5059;comp=sigcomp;
      Branch=z9hG4bk9h9ab
Path: <sip:term@pcscf1.visited1.net;lr>
Service-Route: <sip:orig@scscf1.home1.net;lr>
From: <sip:alice@home1.net>;tag=s8732n
To: <sip:alice@home1.net>; tag=409sp3
Call-ID: 23fi57lju
Contact: <sip:[1080::8:800:200C:417A]:5059;comp=sigcomp>
           ;expires=600000
CSeq: 2 REGISTER
Date : Wed, 04 April 2006 19:13:50 GMT
P-Associated-URI :<sip:alice-family@home1.net>
                  <sip:alice-business@home1.net>
                  <sip:+1-212-555-1234@home1.net;user=phone>
Content-Length: 0
```

Une fois l'authentification de l'utilisateur réussit, le S-CSCF envoie cette réponse au terminal qui contient :

- P-Associated-URI : qui contient une liste des URI alloué à l'utilisateur.
- Service-Route : Qui contient obligatoirement l'adresse du S-CSCF alloué à l'utilisateur ainsi qu'une liste optionnelle d'URI de serveurs SIP que le terminal peut utiliser pour envoyer ses requêtes.
- Le champ « Expires » indique la durée d'enregistrement du terminal.

2.2.5. Les Messages Diameter

Les messages suivants sont échangés sur l'interface Cx qui peut être entre l'I-CSCF et le HSS ou le S-CSCF et le HSS. Cette interface est caractérisée par l'application Diameter qui défini un ensemble de commandes (requête/réponse) pour l'interface Cx parmi les quelle figures ces messages.

1. (3) UAR/ (4) UAA:

Quand l'I-CSCF reçoit la requête SIP REGISTER, il envoie un message User-Authorization-Request au HSS pour les raisons suivante :

- Le HSS vérifie si la Public User Identity est attribué à un utilisateur légitime du système et que l'utilisateur ne doit pas être bloqué (Si son crédit est terminé).
- Le HSS vérifie encore s'il y a un accord de roaming avec le réseau visité où se trouve le P-CSCF. Ceci est important, car il permet au réseau du P-CSCF d'échanger des informations de facturation avec le réseau nominale.
- L'I-CSCF a besoin de savoir s'il y a un S-CSCF alloué à l'utilisateur pour lui renvoyer le message SIP REGISTER. Sinon l'I-CSCF recevra un ensemble de capabilité qui va lui permettre de choisir un.
- Le HSS va corréler la Public User Identity avec la Private User Identity, pour voir s'ils peuvent être utilisés ensemble pour authentifier l'utilisateur.

Le HSS répond par un User-Authorization-Answer à l'I-CSCF qui contient un Result-AVP (Result Attribute Value Paires) pour lui indiquer s'il continue la procédure

d'enregistrement ou pas. Si l'enregistrement est autorisé l'UAA contiendra aussi des AVP pour aider l'I-CSCF à déterminer ou choisir le S-CSCF.

2. (6) MAR/ (7) MAA:

Quand le S-CSCF reçoit le message d'enregistrement il doit authentifier l'utilisateur. Pour cela il doit télécharger les vecteurs d'authentification du HSS car pour une première fois le S-CSCF ne les à pas. Le S-CSCF envoie le message Multimedia-Auth-Request au HSS pour lui demander ces vecteurs et enregistre en même temps son URI dans le profile de l'utilisateur pour que d'autre CSCFs ou AS soit capable de savoir qu'elle est le S-CSCF alloué a cet utilisateur. Le HSS répond par les vecteurs dans le message Multimedia-Auth-Answer.

3. (16) SAR/ (17) SAA:

Une fois l'utilisateur authentifié, le S-CSCF envoie le message Server-Assignment-Request au HSS pour lui indiquer que l'utilisateur est enregistré chez lui et pour lui demander son profile complet (ou le reste de son profile). Le HSS répond par un message Server-Assignment-Answer contenant le profile demandé. Le S-CSCF peut aussi envoyer le massage SAR au HSS si l'utilisateur n'est plus enregistré pour garder le HSS au courrant de l'état d'enregistrement de l'utilisateur. Le HSS peut autoriser le S-CSCF de garder le profile de l'utilisateur et de lui rester affecter. Le HSS contrôle cette possibilité.

2.2.6. Souscription à l'état d'enregistrement du terminal « reg Event State »

Il est important d'informer l'utilisateur s'il est toujours joignable ou pas, c'est un besoin hérité du GSM, c'est-à-dire détecté si le service IMS est toujours disponible. La solution pour ce problème est d'utiliser une technique réseau intelligent sur événement, où on va souscrire le terminal IMS à un service qui lui permet de savoir son état d'enregistrement (registration-state), cette information est disponible dans le S-CSCF. Ceci consiste à mettre en place une supervision d'un événement (Enregistrement/désenregistrement) grâce au message SIP SUBSCRIBE, et pour informer l'occurrence de cet événement on utilise le NOTIFY.

Quand le terminal IMS termine son enregistrement, il envoie une requête SUBSCRIBE adressé pour la même Public User Identity déjà enregistré. Le S-CSCF reçoit cette requête et installe cette souscription. Le S-CSCF envoie une requête NOTIFY à l'utilisateur qui contient la liste des Public User Identity qui lui son affecté avec l'état d'enregistrement de chaque une. Maintenant le terminal sait avec qu'elle Public User Identity l'utilisateur est enregistré. Si l'état d'enregistrement de l'utilisateur change le S-CSCF va l'informer. De plus le P-CSCF va se souscrire à son tour à l'état d'enregistrement de l'utilisateur, de cette façon il sera informé en temps réelle sur l'état d'enregistrement de chaque Public User Identity.

Notons que d'autre entité peuvent souscrire à l'état d'enregistrement de l'utilisateur tel que les serveurs d'application afin de fournir des servir divers (ex : envoyé un message de bien venue à l'utilisateur).

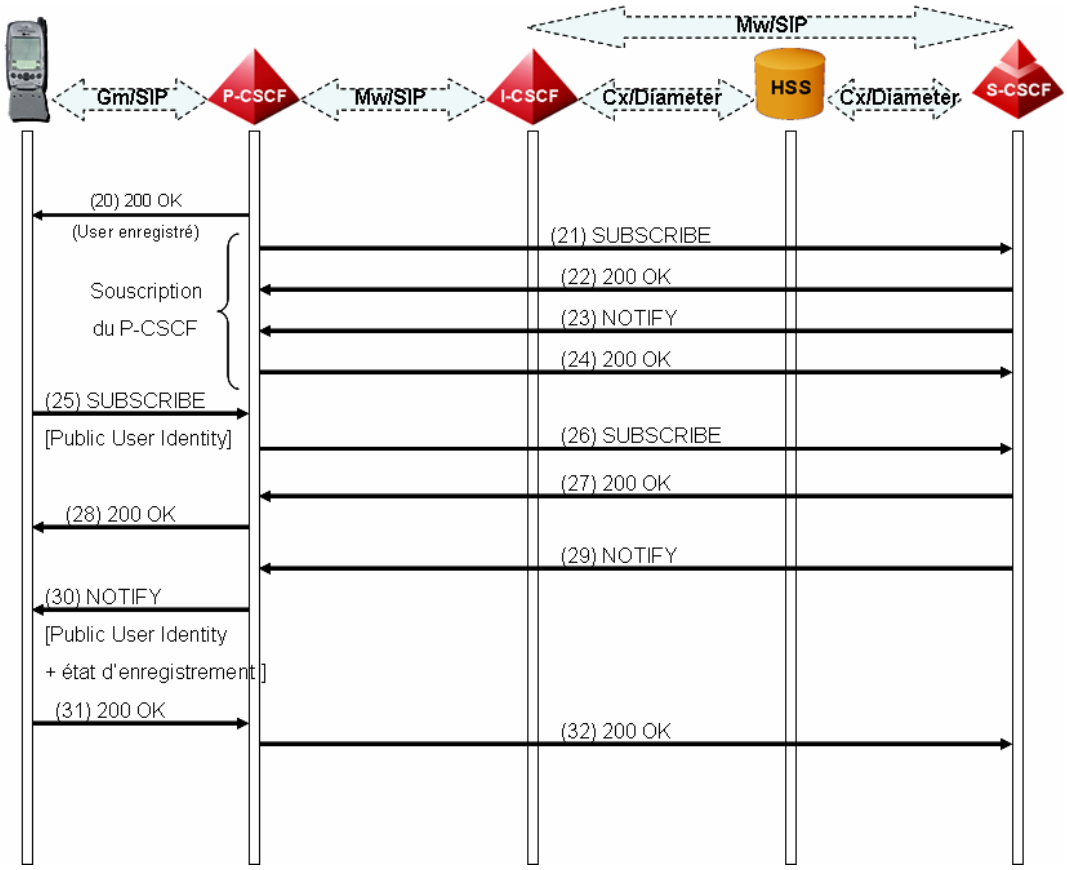

Figure 2.2.6.a : Souscription à l'état d'enregistrement (Suite de la procédure d'enregistrement).

3. Procédure d'établissement de session en IMS ➔ INVITE

Dans cette partie, on va décrire les messages échangés lors de l'établissement d'une session en IMS. Pour illustrer cette procédure, on va considérer un scénario où les 2 terminaux sont en cas de roaming. On va supposer alors que l'appelant (user1_public1@home1.net) possède un abonnement français et il est en roaming en Finland, et l'appelé (+1-212-555-2222) possède un abonnement allemand et il est en roaming aux Etats-Unis. Dans ce scénario, chacun des terminaux IMS, possède alors un réseau mère et un réseau visité. On suppose l'établissement d'une session de visiophonie entre des abonnées UMTS.
Dans la suite, on va suivre l'acheminement de l'appel étape par étape.

3.1. Etape 1 : Invite et Session Progress

La figure suivante représente l'étape 1 [Invite + Session Progress] des différents messages de signalisation échangés lors de l'établissement de session.

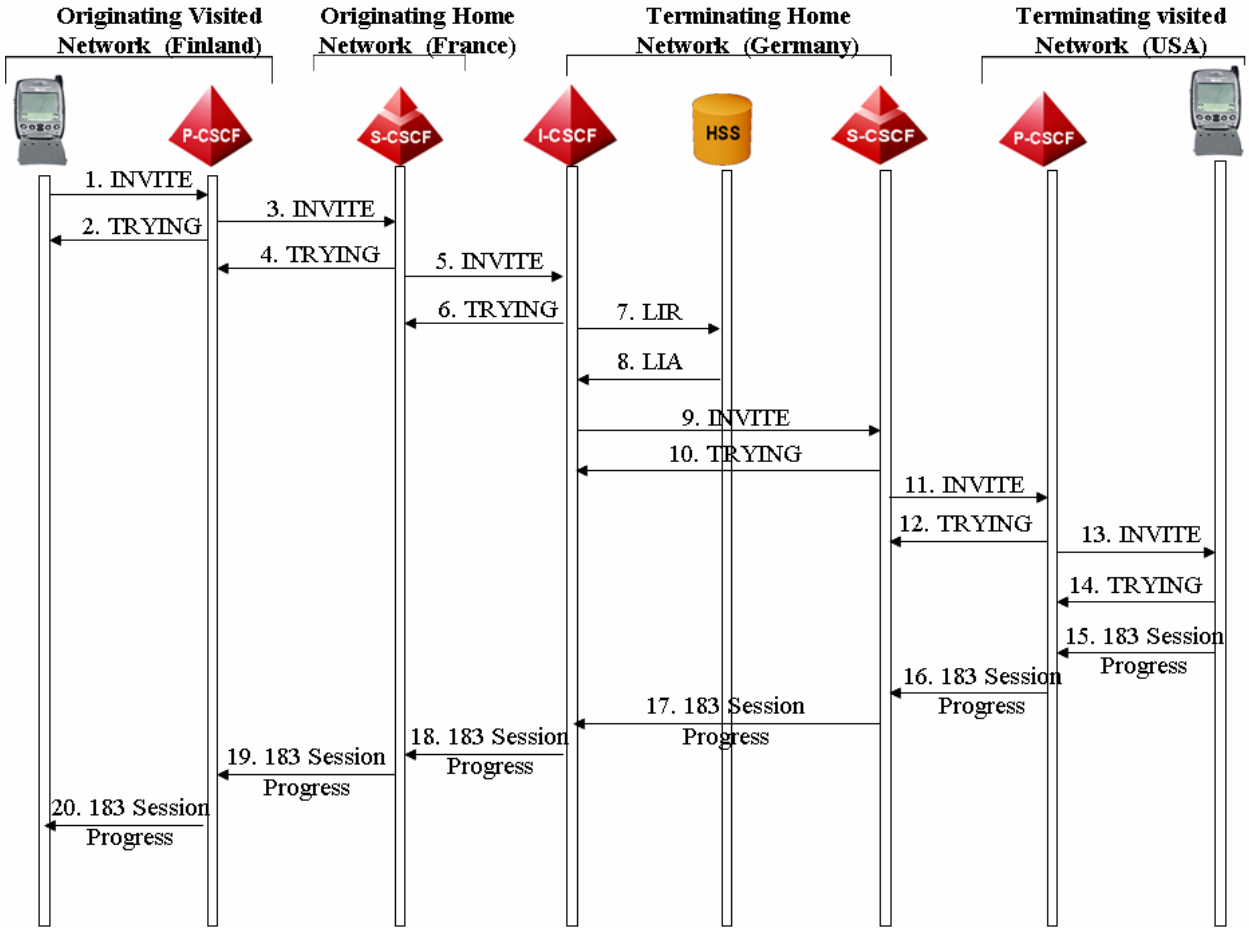

Figure 3.1.a : Invite + Session Progress

On va détailler par la suite les champs importants des messages SIP [Invite et Session Progress] échangés lors de la première étape.

(1) Invite : UE1 à P-CSCF1

L'UE1 envoie un *Invite request* au réseau pour établir une session multimédia.

```
INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
  port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

On va analyser les principaux champs de ce message :

- Request URI : Contient le TEL-URI Public User Identity de l'appelé (+ 1-212-555-2222).
- Via Header :
  - Contient l'adresse IPv6 (5555:aaa:bbb:ccc:ddd) et le numéro de port (1357) sur lequel le terminal IMS souhaite recevoir les réponses à cette requête.
  - Indique si le terminal est capable de recevoir des entêtes SIP compressé (SigComp : Compressed Signaling).
  - Indique le protocole de transport (UDP, TCP, SCTP) qui peut être utilisé (soit UDP dans notre cas).
- Route :
  - Contient l'adresse du P-CSCF : **p-cscf1.visited1.net** (d'après la Discovery Procedure) et la valeur du numéro de port (1357) du P-CSCF.
  - Contient la valeur du Service-Route Header obtenue lors de la registration, c'est à dire l'adresse du S-CSCF dans le réseau mère **s-cscf1.home1.net**.

- P-Preferred Identity : Chaque utilisateur peut avoir plusieurs Public User Identity. Pour cela, l'appelant doit indiquer quelle identité (user1_public1@home1.net) il va utiliser pour cette session.
- P-Access Network Info: Ce champ indique 2 types d'information sur l'accès:
  - Le type de la couche d'accès 2/3 utilisé par le terminal IMS (UMTS, WLAN, …), qui est dans notre cas un accès UMTS (UTRAN).
  - L'identité de la cellule radio auquel le terminal est connecté.
- SDP content : Ces champs décrivent la session ; Ils indiquent que c'est un offre SDP (Session Description Protocol) contenant le Bandwidth, ainsi que les caractéristiques pour chacun des codecs qu'il peut supporter pour cette session. Le vidéo streaming peut supporter 2 codecs (H.263 soit MPEG-4) et l'audio streaming peut supporter le codec AMR.
- Require : precondition indique que l'appelé doit répondre par un SDP answer.
- Privacy : = id si l'appelant veut cacher son identité, et = none dans le cas contraire.
- Security-Verify: Indique que la connexion entre le UE et le P-CSCF est chiffré, utilisation du protocole IP-Sec.

(3) Invite : P-CSCF 1 à S-CSCF 1

Ce message est utilisé pour transférer le message invite vers le next hop Destination indiqué dans le route Header du message précèdent c'est à dire vers le S-CSCF 1 (scscf1.home1.net).

```
INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
  SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

(SDP not modified and not shown)
```

On retrouve dans ce message les mêmes champs indiqués dans le message (1) avec les modifications suivantes :

- P-CSCF 1 ajoute son adresse SIP-URI (pcscf1.visted1.net) au Record- Route Header et au Via-Header. Ce Record Route ne contient pas le paramètre comp = sigcomp comme la requête est envoyé vers une interface non compressée.
- P-CSCF 1 enlève le Security-Verify Header, comme cette requête est envoyée vers le cœur du réseau. Il y aura pas par la suite besoin pour des connexions IP-Sec.
- P-Asserted-Identity: Le P-CSCF1 ajoute à la requête le champ P-Asserted-Identity et supprime le champ de P-Preferred-Identity header. Le P-Asserted-Identity doit

contenir une adresse SIP – URI valide (user1_public1@home1.net) pour l'utilisateur qui peut être égale au P-Preferred-Identity. Une fois, cette adresse est initialisée, le P-CSCF n'utilise plus l'adresse indiquée dans le champ From.

(5) – Invite: S-CSCF 1 vers I-CSCF 2

Le S-CSCF 1 attribué à l'UE 1 examine le P-Asserted-Identity pour identifier le l'utilisateur initiant l'appel. Pour cela, il télécharge le profil de l'utilisateur. Ce profil contient un critère important appelé "*Filter Criteria*".
Le « Filter Criteria » contient une collection de Triggers qui détermine si la requête doit passer par un ou plusieurs serveurs d'application pour fournir des services à l'utilisateur.
En effet, le S-CSCF n'exécute pas des services mais télécharge pour chaque utilisateur des filtres, qui sont une sorte de masque qu'il applique aux messages SIP, si le résultat est positif il envoie le message SIP a un serveur d'application pour exécuter un service. C'est la signalisation d'intelligence en IMS. Si non l'appel sera traité normalement par le S-CSCF comme dans notre cas.

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
  SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
  SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

(SDP not modified and not shown)
```

Le S-CSCF de l'UE1 est le premier nœud qui s'occupe de l'acheminement de l'appel vers le destinataire. Le S-CSCF analyse le champ Request-URI de la requête. Il existe deux types d'URI : SIP-URI et TEL-URI.

- Cas de TEL-URI: Qui correspond soit à un numéro de téléphone (+1-212-555-2222) appartenant soit à un réseau RTC ou GSM (Comme dans notre cas), soit à un utilisateur IMS. Dans ce cas, il sera traduit en un SIP-URL (user2_public1@home2.net). Pour cette translation d'adresse, le S-CSCF utilise les services du protocole ENUM-DNS, ou bien d'autres bases de données de translation correspondantes.

Une fois il connaît l'URI de l'appelé, le S-CSCF extrait le nom du domaine (home2.net) (user2_public2@home2.net) et effectue des requêtes DNS avec le DNS Server. Ces requêtes DNS échangés permettent de :

- Trouver les protocoles de transports supportés par le home2.net.
- Déterminer le ou les serveurs SIP (I-CSCF) dans le domaine home2.net.

Le S-CSCF 1 ajoute le TEL URI (+1-212-555-1111) correspondant au SIP URI (user1_public1@home1.net) dans le champ P-Asserted-Identity header pour que ce TEL URI

soit connu par le réseau de destination dans le cas où la requête INVITE était envoyée vers un MGCF. Il rajoute aussi son adresse (scscf1.home1.net) au record route et au via header.

(7-8) LIR et LIA

I-CSCF2 envoie une requête vers le HSS (contenant le public user identity : user2_public2@home2.net de l'appelé) pour trouver le S-CSCF2 correspondant à l'utilisateur appelé. HSS répond avec l'adresse du S-CSCF2.

(9) Invite: I-CSCF 2 vers S-CSCF 2

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1,
  SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
  SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
  SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home2.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

(SDP not modified and not shown)
```

On note ici que l'I-CSCF 2 n'ajoute pas son adresse au Record-Route header, comme il n'y a plus besoin de l'adresse de l'I-CSCF pour la signalisation une fois la session est établit, mais au via Header uniquement. L'I-CSCF 2 envoie le message vers le S-CSCF 2 (Route) obtenue dans les requêtes Diamater.

(11) Invite: S-CSCF 2 vers P-CSCF 2

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1,
  SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1,
  SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
  SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
  SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.visited2.net;lr>
Record-Route: <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type: application/sdp
Content-Length: (...)

(SDP not modified and not shown)
```

Le S-CSCF2 valide le profil de service de l'UE 2 et fait l'évaluation de son « Filter Criteria ». Il connaît aussi d'après la procédure de registration l'adresse de l'UE 2 et le next hop CSCF pour cet UE.

- Le S-CSCF 2 crée une nouvelle Request-URI dont le contenu est une adresse IPv6 qui est celle du Header contact fourni lors de l'enregistrement (5555 :eee :fff :aaa :bbb)
- Le S-CSCF 2 ajoute son adresse au Via Record Route (scscf2.home2.net).
- Route : Contient l'adresse du P-CSCF 2 (pcscf2.home2.net) stocké lors de la procédure de registration.
- P-Called-Party-ID: contient le Public User Identity de l'appelé et ses paramètres (user2_public2@home2.net).

(13) Invite : P-CSCF 2 vers UE 2

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1,
  SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1,
  SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1,
  SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
  SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
  SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>,
  <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
Privacy: none
P-Media-Authorization: 0020000100100101706466312e686f6d65312e6e6574000c02013331533134363231
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type: application/sdp
Content-Length: (...)

(SDP not modified and not shown)
```

- Le P-CSCF 2 ajoute son adresse URI (pcscf2.visited2.net) ainsi que le numéro de port négocié (8805) suivant les accords de sécurité via header et au record route.
- Il va router le message vers UE2 suivant l'adresse IPv6 indiqué dans Request_URI.
- Suivant la valeur de privacy indiqué dans le message 1, le P-Asserted-Identity sera supprimé ou pas.
  - Si privacy = id, le P-Asserted-Identity sera supprimé.
  - Privacy = none, le champ sera envoyé vers l'appelé.

(15) Session Progress: UE 2 vers P-CSCF 2

L'UE1 envoie une requête Invite à l'UE2 contenant un offer SDP indiquant l'adresse IP et les numéros de port sur lesquels l'UE1 veut recevoir le media stream, les codecs désirés et supportés pour chacun de ces media streams.

De plus, le SDP offre contient le champ require initialisé à precondition indiquant qu'il faut faire une réservation des ressources radio en avance.

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1,
  SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1,
  SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1,
  SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1,
  SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1,
  SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>,
  <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

Le SDP anser contient :

- Le media stream et le codec que l'appelé peut supporter pour cette session.
- Access Network Info : Le type d'accès.
- Contact: Contient le SIP URI avec l'adresse IP de l'UE 2 sur laquelle le destinataire souhaite recevoir le media streams. Il contient aussi comp=sigcomp parameter.
- SDP: Le SDP contient l'ensemble des codecs supportés par l'UE2. La confirmation de la QoS preconditions est nécessaire pour l'établissement de la session avec ces medias streams. L'UE2 peut accepter l'établissement de la session avec audio stream mais sans vidéo.
- Le SDP contient aussi un champ a=conf : qos indiquant que le destinataire UE2 souhaite recevoir une notification une fois l'UE1 a terminé le processus de réservation de ressources.

(16 … 20) Traitement de la Session Progress

La réponse Session Progress traverse l'ensemble des proxys traversés par Invite

- Au niveau de P-CSCF 2 :
  - P-Asserted-Identity: Le P-CSCF 2 prend la valeur du P-Called-Party-Id (user2_public1@home2.net (de l'appelé)) de la requête INVITE reçu précédemment et la met dans le champ P-Asserted-Identity de ce message.

- Record-Route: P-CSCF2 réécrit le champ Record-Route header tout en effaçant le numéro de port utilisé pour des associations de sécurité.

- Au niveau de S-CSCF 2 :
  - P-Asserted-Identity: S-CSCF2 ajoute le TEL URI (+1-212-555-2222) de l'appelé dans le champ P-Asserted-Identity.
- Au niveau de S-CSCF 1 :
  - Le S-CSCF 1 peut supprimer le P-Asserted-Identity si le champ Privacy du message (15) est initialisé à id.
- Au niveau de P-CSCF 1 :
  - Record-Route: P-CSCF1 réécrit le champ Record-Route header et ajoute le numéro de port utilisé pour des associations de sécurité.
- Le P-CSCF 1 envoie la réponse vers l'UE1.

3.2. Etape 2: Prack Request

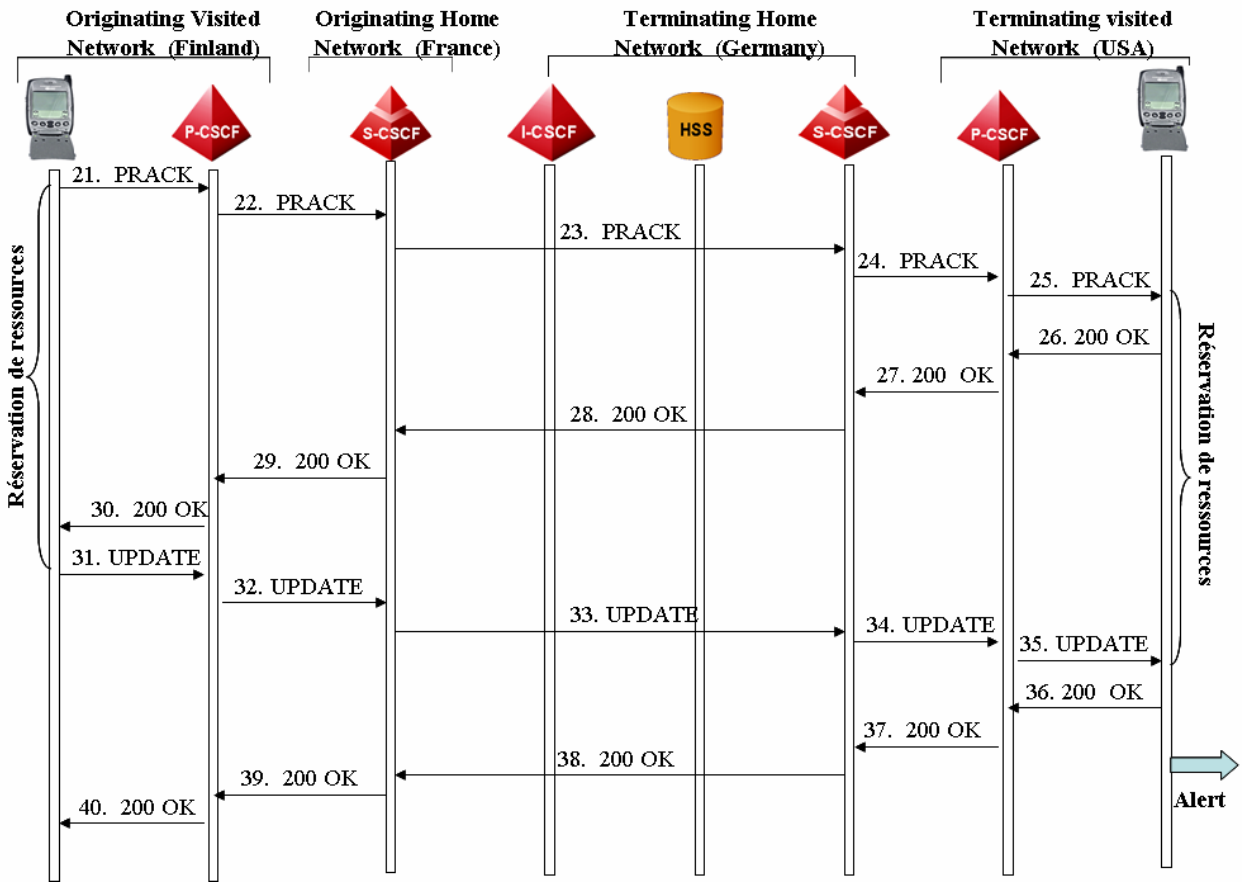

Figure 3.2.a : Suite de la procédure d'établissement de session.

(21 ... 25) L'UE1 Traite la réponse de la Session Progress : Prack

Comme l'UE1 peut supporter plusieurs codecs pour un media stream, le terminal a toujours tendance à réduire le nombre de codecs supportés par un media stream à un seul. Par exemple, pour le vidéo stream, le nombre de codecs négociés est deux (H.263 et MPEG-4).
L'UE1 doit choisir lequel des 2 codecs va être utilisé. Ceci aura un impact direct sur la gestion de la bande passante, Comme la réservation de ressources dépend du Bandwidth

associé au codec choisit. L'UE1 choisit un codec par flux (codec vidéo et codec audio AMR) et envoie une nouvelle offre SDP contenant le ou les codecs choisis. Par exemple, dans notre cas le terminal 1 choisit le H.263 comme codec pour la vidéo et l'AMR pour la voix. Cette nouvelle offre SDP sera envoyée dans le message PRACK.

En parallèle avec l'envoi de ce message PRACK, l'UE1 connaît déjà le BandWidth qui devra être alloué, il commence alors la **réservation des ressources radios.** Cette procédure nécessite un échange de message avec les nœuds radios et paquets (SGSN et GGSN si l'IP-CAN est un réseau GPRS ou UMTS).
La requête Prack est envoyée ensuite vers le path indiquée par Record Route Header.

(26 ... 40) L'UE2 Traite le Prack

Le message 200 Ok constitue la deuxième réponse à l'offre SDP de PRACK après celui de l'invite. Le SDP answer ne contient pas des paramètres à négocier mais plutôt une confirmation pour le codec et le media stream de cette session.
On note aussi que la réservation des ressources pour le terminal 2 commence à ce stade là.
Le SDP answer indique aussi que l'UE2 n'a pas reçu encore une notification que l'UE1 a terminé la procédure de réservation de ressources.
Ce message traverse les mêmes proxies que le message PRACK a traversés.

Une fois, l'UE1 a terminé la procédure de réservation de ressources, il envoie à l'UE2 un message de confirmation UPDATE contenant un nouvel offre SDP dans lequel l'UE1 met à jour le champ a=curr :qos local sendrecv indiquant que la réservation de ressources a été effectué au niveau de l'UE1.

L'UE2 doit répondre avec un SDP answer afin d'acquitter l'offre SDP de Update.

3.4. Etape 3: Alerter l'appelé

Avant que l'appelé soit alerté, l'UE2 doit vérifier si l'allocation des ressources a été faite des deux côtés de la session, pour cela deux conditions essentielles doivent être satisfaites:

- L'UE2 doit compléter la réservation de ses ressources.
- L'UE2 doit recevoir une confirmation que le l'UE1 a terminé la réservation de ses ressources (message UPDATE (31 … 35)).

Quand l'appelé est alerté, une réponse Ringing est générée et envoyée vers le terminal de l'appelant à travers le même ensemble de proxys. Cette réponse ne contient pas de SDP, puisque tous les paramètres ont étaient déjà négociés.
Due à la présence du champ *Require : 100rel*, Cette réponse doit être acquittée. Le terminal de l'appelant en recevant le Ringing va générer une tonalité ring-back (tonalité de retoure d'appel) sauvegardée localement, et va envoyer à l'appelé une réponse PRACK (comme aquittement du Ringing) sans offre SDP, ce dernier en recevant le PRACK envoie un 200 OK (comme aquittement du PRACK).
Quand l'appelé accepte l'appel, le terminal va envoyer un 200 OK comme acquittement pour la requête INVITE qu'il reçu de l'appelant. En recevant le message 200 Ok, le terminal de l'appelant commence à générer le trafic media, et il envoie en plus un ACK pour confirmer la réception du 200 OK.

L'établissement de la session est terminé et les deux utilisateurs peuvent commencer à générer leurs flux audio et vidéo. Ces flux en général sont envoyés de bout en bout via les routeurs de l'IPCAN.

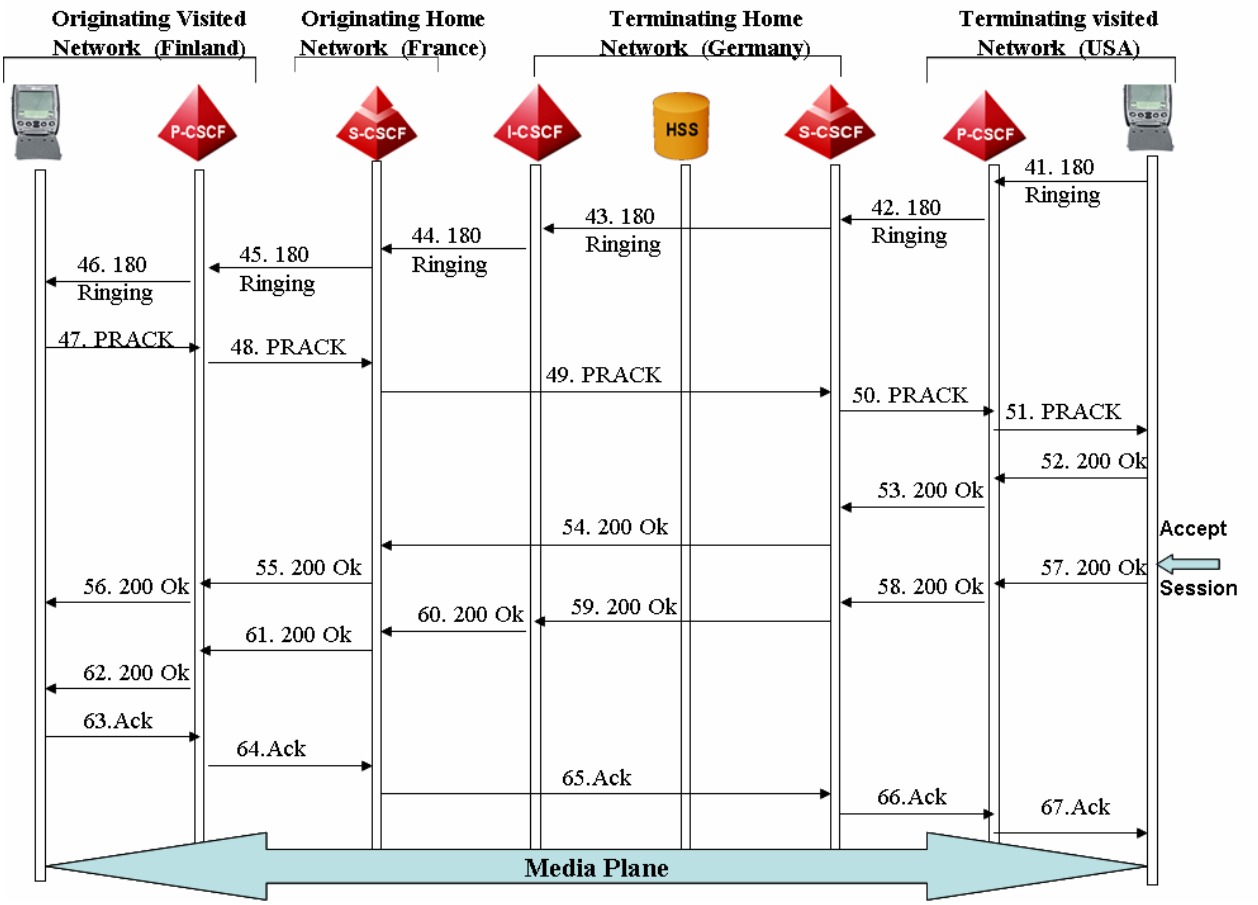

Figure 3.4.a : Suite de la procédure d'établissement de session.

Conclusion

Dans ce projet, on a analysé deux aspects fondamentaux de cette nouvelle technologie qui tend à remplacer l'infrastructure de contrôle dans les réseaux mobile. L'apport principal de l'IMS est le faite de pouvoir établir des sessions multimédia avec la fourniture de nouveaux services comme le Push to Talk, la messagerie instantanée jusqu'aux jeux vidéo…Mais pour faire des services très riche il faut que les réseaux d'accès IP assurent un débit élevé par utilisateur et une bonne réactivité. Actuellement les réseaux mobiles de troisième génération, telle que l'UMTS, ne fournissent pas un débit très élevé par utilisateur, donc pour vraiment faire des services multimédia d'une haute qualité il faut attendre l'émergence d'une nouvelle technologie radio. En plus le réseau IP de transport qui pourra être l'Internet doit fournir une qualité de service minimum pour véhiculer le trafic IMS. Là, on voit plusieurs problématiques qui apparaissent au niveau accès transport et même au niveau de la gestion de la mobilité de l'utilisateur quand il change de technologie d'accès.

Glossaire

ACK	Acknolage
AMR	Adaptative Multi Rate
API	Application Programming Interface
APN	Access Point Name
AS	Application Server
AVP	Attribute Value Pairs
BGCF	Breakout Gateway Control Function
CAMEL	Customized Application for Mobile network Enhanced Logic
C-CSCF	Call/Session Control Function
CDR	Call Detailed Record
CDRs	Call Detailed Record
CK	Ciphering Key
CS	Circuit Switching
DHCPv6	Dynamic Host Configuration Protocol version 6
DiffServ	Differenciated Services
DNS	Domain Name System
GPRS	General Packet Radio Service
GSM	Global System for Mobile
gsmSCF	GSM Service Control Function
HLR	Home Location Server
HSS	Home Subscriber Server
I-CSCF	Interrogating–CSCF
I-CSCF	Interrogating–CSCF
IK	Integrity Key
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IMS-SSF	IP Multimedia Service Switching Function
IMS-SSF	IP Multimedia Service Switching Function
INAP	Intelligent Network Application Part
IP	Internet Protocol
IP CAN	IP Connectivity Access Network
IP-Sec	Internet Protocol Security
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
ISIM	IMS Subscriber Identity Module
ISUP	ISDN User Part
LIA	Location Info Answer
LIR	Location Info Request
MAA	Multimedia Authentication Answer
MAR	Multimedia Authentication Request
MCC	Mobile Country Code
MGCF	Media Gateway Control Function
MGW	Meadi Gateway
MMS	Multimedia Message Service

MNC	Mobile Network Code
MPLS	Multi Protocol Label Switching
MRF	Media Ressource Function
MRF	Media Ressource Function
MRFC	Media Ressource Function Controller
MRFC	Media Ressource Function Controller
MRFP	Media Ressource Function Processor
MSIN	Mobile Station Identity Number
MSISDN	Mobile Subscriber ISDN Number
MTP	Message Transfer Part
NGN	Next Generation Network
OSA-SCS	Open Service Access – Service Capability Server
OSA-SCS	Open Service Access – Service Capability Server
PCM	Pulse Code Modulation
P-CSCF	Proxy-CSCF
P-CSCF	Proxy-CSCF
PDF	Policy Decision Function
PDF	Policy Decision Function
QoS	Quality of Service
RI	Réseau Intelligent
RSVP	Ressource Reservation Protocol
RTC	Réseau Téléphonique Commuté
RTP	Real-Time Protocol
SAA	Server Assignment Answer
SAR	Server Assignment Request
S-CSCF	Serving-CSCF
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SGW	Signalling Gateway
SIP	Session Initiation Protocol
SIP-URI	SIP Uniform Ressource Indentifier
SMS	Short Message Service
TCP	Transmision Control Protocol
TEL-URL	Telphone Uniform Ressource Locator
UAA	User Authorization Answer
UAR	User Authorization Request
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
VLR	Visitor Location Server
WLAN	Wireless Local Area Network
xDSL	x Digital Subscriber Line

Références

1. **The IP Multimédia Subsystem**, Gonzalo Camarillo et Miguel A. Garcia-Martin.

2. **Nouveaux Services Vocaux d'Entreprises**, Cours Claude Rigault, ENST 2005.

3. **RFC3261, SIP : Session Initiation Protocol**, J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, June 2002.

4. **3GPP TS 24.228 V5.13.0 June 2005**, Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP), and Session Description Protocol (SDP), Stage 3, Release 5.

5. **3GPP TS 29.229 V7.1.0 March 2006**, Cx and Dx interfaces based on the Diameter protocol, Protocol details, Release 7.

6. **Référence Internet :** www.tech-invite.com.

MROUEH Lina

3ème année du cycle ingénieur
Télécom Paris

mroueh@enst.fr

LABAKY Elie

3ème année du cycle ingénieur
Télécom Paris

labaky@enst.fr

Avril 2006