IMS Avancé : Enregistrement et Authentification

EFORT
http://www.efort.com

Ce second tutoriel EFORT dédié à l'IMS présente les procédures d'enregistrement et d'authentification IMS. Avant de pouvoir utiliser les services du domaine IMS, tels qu'établir une session multimédia ou recevoir une demande de session, un usager doit s'enregistrer au réseau IMS. Puisque l'IMS supporte le « roaming », l'usager peut s'enregistrer depuis son réseau nominal où depuis n'importe quel réseau visité qui dispose d'un accord de roaming avec le réseau nominal. Le premier chapitre décrit les identités IMS nécessaires à l'enregistrement et l'authentification, i.e., identité privé et identité publique. Le second chapitre introduit la procédure d'enregistrement IMS. Le troisième chapitre détaille la procédure d'authentification IMS.

1 Identités pour l'enregistrement IMS

L'enregistrement à l'IMS requiert une identités privée et une identité publique. Trois types d'enregistrement sont à considérer :

1. Enregistrement d'un client mobile depuis un accès 3G ou 4G avec une carte USIM intégrant un module ISIM (IMS SIM Module)
2. Enregistrement d'un client mobile depuis un accès 3G ou 4G avec une carte USIM sans module ISIM (IMS SIM Module)
3. Enregistrement d'un client fixe sans USIM et ISIM.

1.1 Enregistrement de l 'usager disposant d'une USIM avec module ISIM

La référence à une souscription IMS est définie par un compte usager. La souscription IMS peut être utilisée depuis n 'importe quel équipement appelé UE (User Equipment) , pour des communications fixes ou mobiles.
Un usager doit avoir au moins une identité privée et au moins une identité publique.
L 'identité privée IMS (IMSI Private User Identity, IMPI) est une donnée usager permanente dans le HSS (Home Subscriber Server). Le format de l 'IMPI est de type username@realm de Network Address Identifier (NAI) tel que spécifié dans le RFC IETF 4282.
L 'IMSI peut être inclus dans la partie username si souhaité par l 'opérateur; le format de la partie realm étant alors : ims.mnc[MNC].mcc[MCC].3gppnetwork.org
Si l 'IMSI suivant est utilisé, 2080123456555 où MCC = 208, MNC = 01, et MSIN = 43567656, alors IMPI = 2080123456555@ims.mnc01.mcc208.3gppnetwork.org
autre IMPI possible: JohnCook_private@orange.fr
La Private User Identity n 'est pas une URI SIP.

L'identité publique d'usager (IMS Public User Identity, IMPU) est un nom de contact publié ou un numéro avec lequel adresser l'usager.
Plusieurs IMPUs peuvent exister par souscription IMS — par exemple, un numéro de téléphone (tel : +33672112445) et une adresse SIP URI (sip : JohnCook@orange.fr). L'opérateur de réseau IMS nominal assigne les identités IMPU.
Ces IDs sont des données permanentes de l'usager stockées dans la base de données HSS.
Des IMPUs peuvent être partagés par différents IMPIs avec la même souscription IMS. Une identité IMPU donnée peut être enregistrée simultanément sur différents UEs qui utilisent des IMPIs différents.

1.2 Enregistrement de l ’usager sans ISIM mais avec USIM

Un usager mobile peut s’enregistrer à l’IMS avec sa carte USIM sans que celle-ci possède de module ISIM. Une adresse privée temporaire et une adresse publique temporaire sont alors générées pour l’enregistrement IMS et ont le format : username@realm.
L ’IMSI doit être inclus dans la partie username; le format de la partie realm est : ims.mnc[MNC].mcc[MCC].3gppnetwork.org
Ex : IMSI = 2080143567656, où MCC = 208, MNC = 01, et MSIN = 43567656.
L ’identité privée est alors : 2080143567656@ims.mnc01.mcc208.3gppnetwork.org
L ’identité publique temporaire est identique à une adresse privée temporaire mais préfixée par « sip: » car il s ’agit d ’une URI SIP.
Dans notre exemple sa valeur est :
sip : 2080143567656@ims.mnc01.mcc208.3gppnetwork.org

Lorsqu ’un terminal IMS disposant d ’une USIM sans ISIM doit construire le nom de domaine de son réseau nominal qui est inclus dans le Request-URI de la requête SIP REGISTER, le terminal supprime la partie « user » de l ’identité publique temporaire. L ’URI du nom de domaine du réseau nominal est : sip: ims.mnc01.mcc208.3gppnetwork.org
Dans ce cas particulier, lorsque l ’usager s ’enregistre, l ’authentification sera basée sur l ’AKA 3G et non pas l ’AKA IMS.
L ’authentification IMS pour les clients mobiles est basée sur une clé partagée K qui est uniquement présente dans le HSS et dans l ’application ISIM de la carte USIM sur l ’UE. Comme le HSS ne communique jamais directement avec l ’UE, le S-CSCF réalise les procédures d ’authentification. Le vecteur d ’authentification (AV, Authentication Vector) est téléchargé par le S-CSCF à partir du HSS pendant l ’enregistrement. La procédure d’authentification est similaire à celle mise en œuvre dans les réseaux mobiles 3G sur la base du protocole AKA (Authentication and Key Agreement). La partie « authentication » de AKA permet de vérifier l ’identité de l ’usager alors que la partie « Key Agreement » permet de générer des clés qui sont ensuite utilisées pour le chiffrement du trafic de signalisation SIP entre l’UE et le P-CSCF et pour la protection de l ’intégrité de la signalisation SIP toujours entre l’UE et le P-CSCF.
Dans le cas d’un usager ne disposant pas de module ISIM, l’authentification s’appuiera sur l’AKA 3G et la clé K présents sur l’USIM. Si l’authentification réussit pendant la phase d’enregistrement l’usager obtient du réseau son identité ou ses identités publiques IMS (présentés dans le header P-Associated-URI de la réponse SIP 200 OK) .
Une fois la procédure d ’enregistrement finalisée, le terminal IMS dispose donc d ’un ensemble d ’identités publiques d ’usager pour par exemple établir des sessions IMS.

1.3 Enregistrement de l ’usager sans USIM et sans ISIM (i.e., enregistrement depuis un accès large bande fixe)

Dans ce cas précis, le nom d’utilisateur et le mot de passe utilisés par le modem (e.g., modem ADSL) pour l’authentification sur l’accès large bande fixe peuvent être réutilisés pour l’authentificaiton à l’IMS.
L ’authentification d ’accès HTTP avec la méthode Digest est la forme la plus simple d ’authentification dans le protocole SIP et concerne ce scénario.
Le mécanisme fait partie de la spécification SIP (RFC 3261) et doit être implanté obligatoirement dans les clients et serveurs SIP. Il s ’agit d ’une adaptation du même mécanisme utilisé pour l ’authentification au service Web.
Le mécanisme requiert un nom d ’utilisateur et un mot de passe. Le nom d ’utilisateur est considéré comme la Private User Identity. L ’authentification est toujours mutuelle. Le transport est assuré par TLS (Transport Layer Security).
L ’authentification d ’accès HTTP avec la méthode Digest est donc utilisée pour accéder à l ’IMS à travers des réseaux d ’accès non définis par 3GPP.

Nous avons montré que si l 'accès est 3GPP (e.g., 3G, 3G+, LTE/4G), l 'usager dispose d 'une USIM avec ou sans module ISIM. Alors le mécanisme d 'authentification est l 'authentification d 'accès HTTP avec la méthode Digest en utilisant AKA appelé simplement HTTP Digest AKA.

2 Enregistrement IMS

Avant de pouvoir utiliser les services du domaine IMS, tels qu'établir une session multimédia ou recevoir une demande de session, un usager doit s'enregistrer à l 'IMS. Que l'usager soit dans son réseau nominal ou dans un réseau visité, cette procédure fait intervenir un P-CSCF (Proxy- Call Stateful Control Function). L'usager dans un réseau d'accès 3G+ découvre l'adresse de l'entité P-CSCF en activant le contexte PDP nécessaire pour l'échange de messages de signalisation SIP. Le message d'acceptation d'activation de contexte PDP contient l'adresse IP allouée à l'UE (User Equipment) et l'adresse du P-CSCF. Tous les messages de signalisation émis par L'UE ou à destination de l'UE sont relayés par le P-CSCF ; l'UE n'a jamais la connaissance des adresses des autres CSCFs (i.e., I-CSCF et S-CSCF). L'entité P-CSCF est dans le réseau visité si l'usager souhaitant s'enregistrer est dans un réseau visité alors que les entités I-CSCF (Interrogating CSCF) et S-CSCF (Serving CSCF) sont toujours présentes dans le réseau nominal de l'usager, ainsi que le HSS. Les entités P-CSCF, I-CSCF, S-CSCF et HSS ont été décrites dans le tutoriel IMS d'EFORT (http://www.efort.com/r_tutoriels/IMS_EFORT.pdf).

Grâce à l'enregistrement SIP :

- Le HSS est notifié de la localisation courante de l'UE par rapport au domaine IMS et met à jour le profil de l'usager correspondant,
- L'usager est authentifié avant de pouvoir accéder aux services du domaine IM,
- Le domaine IMS nominal de l'usager sélectionne un S-CSCF approprié qui invoquera les services de l'UE auprès de serveurs d'application, et ce, grâce au profil de l'usager retourné par le HSS au S-CSCF sélectionné (i.e., ASSI). Le S-CSCF peut être assimilé à l'entité SSP de l'architecture du Réseau Intelligent.

La figure 1 décrit les différentes étapes de la procédure d'enregistrement IMS.

1. Un message SIP REGISTER est émis par l'UE au P-CSCF.
2. Le P-CSCF le relaye à l'entité I-CSCF du réseau nominal de l'usager s'enregistrant. Le réseau nominal peut être identifié à partir de l'URL SIP de l'usager s'enregistrant ou à partir de son IMSI. Le nom de domaine de l'adresse SIP de l'UE s'enregistrant peut être résolu par le DNS en une adresse IP d'une entité I-CSCF du domaine IMS nominal. L'entité I-CSCF joue le rôle de point d'entrée pour les messages de signalisation SIP provenant d'autres réseaux.
3. L'entité I-CSCF interroge le HSS (Home Subscriber Server) à travers l'interface Cx supportée par le protocole DIAMETER (Requête UAR : User Authorization Request). Le HSS est le HLR avec de nouvelles capacités pour supporter le domaine IMS. Le HSS est indépendant de l'accès de telle sorte que des opérateurs peuvent réutiliser le domaine IMS pour d'autres technologies d'accès telles que xDSL (Digital Subscriber Line), le câble ou FTTH. Le message UAR émis contient le nom du domaine nominal, le nom du domaine visité et l'identité de l'UE.
4. Le HSS retourne les informations d 'autorisation de l'usager et les capacités obligatoires et optionnelles du S-CSCF à sélectionner (Réponse UAA : User Authorization Answer). ces informations serviront d'entrées à sa fonction de sélection d'un S-CSCF.
5. L 'I-CSCF vérifie si l 'usager est autorisé à s'enregistrer à partir du réseau visité et dans le cas positif, l'I-CSCF relaye la méthode SIP REGISTER au S-CSCF identifié. L'entité S-

CSCF a plus de fonctionnalités que les P-CSCF et I-CSCF. L'opérateur peut disposer de plusieurs S-CSCFs avec des capacité différentes et sélectionner celui approprié pour rendre le service demandé.

6. L ’entité S-CSCF demande des informations d ’authentification de l ’usager au HSS (MAR : Multimedia authentication request)
7. Le HSS retourne les informations d’authentification par une réponse MAA (Multimedia Authentication Answer) au S-CSCF.

8.9. 10. L’entité S-CSCF retourne à l’usager une réponse négative d’enregistrement contenant d’une part une valeur random (RAND) à utiliser par son module ISIM pour calculer un résultat d’authentification usager et d’autre part un résultat d’authentification réseau (AUTN) permet au réseau IMS de s’authentifier auprès de l’usager. Notons que l’authentification IMS est mutuelle.

11. L ’usager renvoie une demande d ’enregistrement au P-CSCF. Cette deuxième demande d’enregistrement contient un résultat d’authentification usager (RES).
12. Le P-CSCF route le message REGISTER à un S-CSCF du domaine nominal de l ’usager.
13. et 14. Idem 3 et 4.
15. Le message REGISTER est routé de l ’I-CSCF au S-CSCF.
16. L'entité S-CSCF après avoir vérifié les informations d ’authentification de l ’usager, émet une requête SAR (Server Assignment Request) au HSS afin que ce dernier mette à jour le profil de l'usager avec le nom du S-SCSF qui le sert.
17. Le HSS retourne une réponse SAA (Server Assignment Answer) à l'entité S-CSCF, contenant le profil de l'usager. Ce profil consiste en les informations de souscription par l'usager à des services. Le S-CSCF doit par ailleurs stocker le nom / l'adresse du P-CSCF courant de l'usager afin de lui délivrer directement des demandes d'établissement de session entrantes concernant cet usager.
18. Le S-CSCF invoque des services éventuels tels que le service de Présence.

19., 20. et 21. Une réponse 200 OK est retournée par le S-CSCF à l'entité I-CSCF qui le relaye au P-CSCF qui le délivre à UE.

L ’IMS est basé sur plusieurs relations de sécurité. Deux d ’entre elles influencent la signalisation SIP : « authentification entre l ’usager et le réseau », et « L ’association de sécurité (SA, Security Association) entre l ’UE et le P-CSCF ».
Les procédures d ’authentification et d ’établissement de SA dans l ’IMS sont directement liées aux procédures d ’enregistrement SIP.

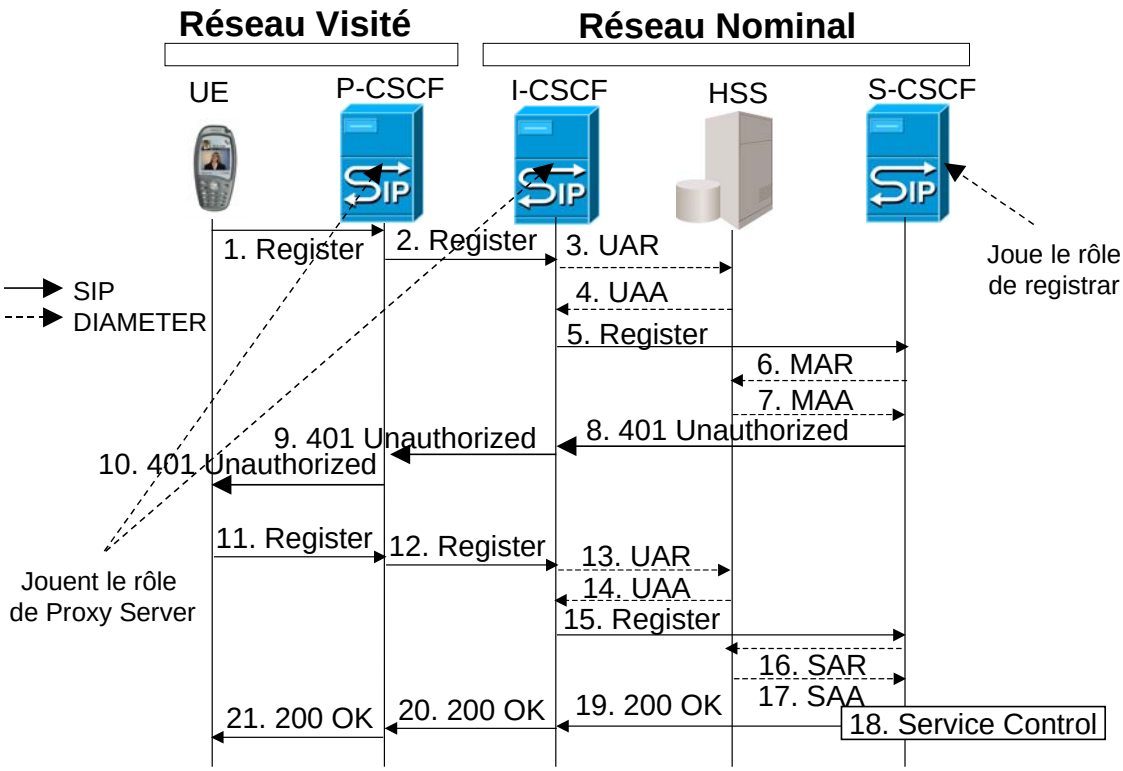


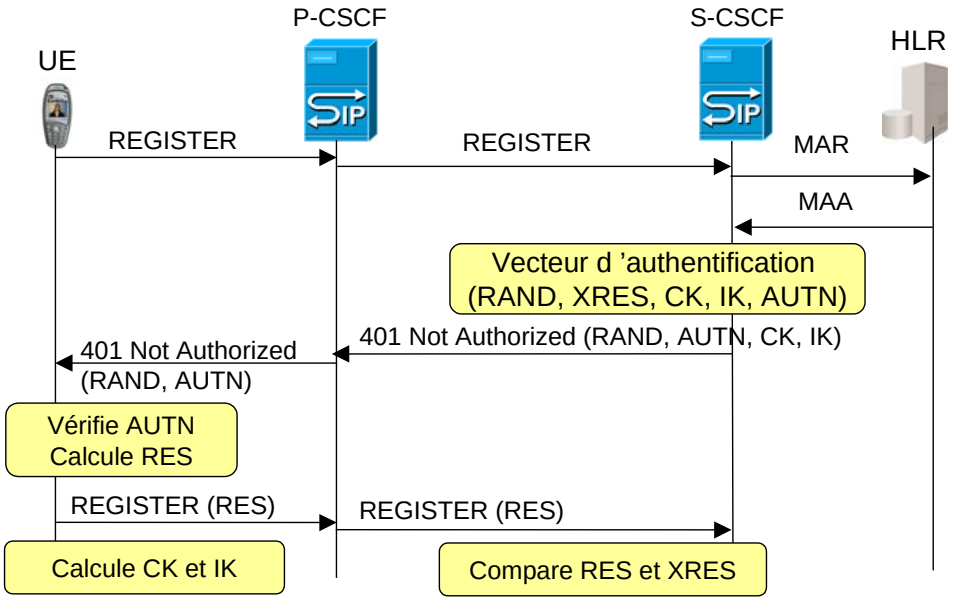
Figure 1 : Enregistrement IMS

3 Authentification IMS et Procédure AKA

Lorsque le S-CSCF reçoit la requête REGISTER de l 'UE, il télécharge les AV (Authentication Vector) à partir du HSS (Figure 2).
Un AV ne contient pas la clé secrète. Cette dernière n 'est présente que sur l 'ISIM (IMS SIM Module) et le HSS.
Les paramètres présents dans l 'AV sont :

- RAND – le challenge (non aléatoire généré par le HSS) qui sert en tant qu'un des paramètres d'entrée pour générer les 4 autres paramètres de l 'AV.
- XRES – Le résultat attendu, utilisé par le réseau pour l 'authentification de l 'ISIM de l 'UE.
- AUTN – Le jeton d 'authentification utilisé par l 'ISIM pour l 'authentification réseau.
- CK – La clé de chiffrement. Cette clé sert au chiffrement de la signalisation SIP échangée entre l'UE et le P-CSCF. Au delà du P-CSCF, la signalisation n'est pas chiffrée.

- IK – La clé d 'intégrité. Cette clé sert à la protection de l'intégrité de la signalisation SIP échangée entre l'UE et le P-CSCF. Au delà du P-CSCF, l'intégrité de la signalisation SIP n'est pas protégée.



Procédure AKA appliquée à IMS

Pour obtenir les vecteurs d'authentification, le S-CSCF émet la requête DIAMETER Multimedia-Auth Request (MAR) au HSS. Cette requête contient :

- < Diameter Header: 303, REQ, PXY, 16777216 >
- L 'AVP 'Session-Id' (263), positionné à scscf1.orange.fr; 1123347722;122
- L'AVP ' Vendor-Specific-Application-Id ' AVP (260) indiquant le Vendor-ID (i.e.,10415), et de manière optionnelle Authentication-Application-Id (16777216) et Accounting-Application-Id.
- L'AVP ' Auth-Session-State ' AVP (277) indiquant qu'aucun état n'est maintenu (i.e., No_State_Maintained).
- L 'AVP 'Public-Identity' (600), indiquant la public user identity qui est enregistrée, i.e., l 'URI contenue dans le header ' To ' de la requête REGISTER: 'sip:JohnCook@orange.fr;
- L 'AVP 'User-Name' AVP (1) positionné à la valeur de la private identity de John Cook, i.e., 'JohnCook_private@orange.fr ';
- L 'AVP 'Server-Name' (602) positionné à la valeur de l 'URI SIP du S-CSCF réalisant la commande MAR, i.e. 'sip:scscf1.orange.fr';
- L 'AVP 'SIP-Number-Auth-Items' (607) positionné à la valeur '5', indiquant que le S-CSCF souhaite télécharger 5 vecteurs d 'authentification consécutifs pour cet usager,
- L 'AVP 'SIP-Auth-Data-Item' (612), incluant le schéma d 'authentification SIP 'SIP-Authentication-Scheme'
- L ' AVP 'Origin-Host' (264) positionné à l 'adresse du S-CSCF, i.e. 'scscf1.orange.fr';
- L 'AVP 'Origin-Realm' (296) positionné au nom de domaine du réseau de l 'opérateur dans lequel est présent le S-CSCF, i.e., ' orange.fr ',
- L 'AVP 'Destination-Realm' (283) correspondant au nom de domaine du HSS, i.e. 'orange.fr',
- L 'AVP 'Destination-Host' (293) positionné à l 'adresse du HSS, i.e., 'hss1@orange.fr', qui sera pré-configurée au niveau du S-CSCF si le réseau nominal ne possède qu 'un seul HSS.

Après avoir reçu la commande MAR, le HSS vérifie d 'abord si le S-CSCF est autorisé à télécharger des données d 'authentification relatives à Mary Taylor. Comme le S-CSCF est autorisé, le HSS retourne une réponse DIAMETER Multimedia-Auth Answer (MAA) au S-CSCF, contenant :

- < Diameter Header: 303, PXY, 16777216 >
- L 'AVP 'Session-Id' (263), positionné à scscf1.orange.fr; 1123347722;122
- L'AVP ' Vendor-Specific-Application-Id ' AVP (260) indiquant le Vendor-ID (i.e.,10415), et de manière optionnelle Authentication-Application-Id (16777216) et Accounting-Application-Id.
- L'AVP ' Auth-Session-State ' AVP (277) indiquant qu'aucun état n'est maintenu (i.e., No_State_Maintained).
- L ' AVP 'Origin-Host' (264) positionné à l 'adresse du HSS, i.e., 'hss1.orange.fr';
- L 'AVP 'Origin-Realm' (296) positionné au nom de domaine du réseau de l 'opérateur dans lequel est présent le HSS, i.e., ' orange.fr ',
- L 'AVP 'Public-Identity' (608) positionné à la même valeur que celle reçue dans la commande MAR, i.e., public user identity, sip:JohnCook@orange.fr'
- L 'AVP 'User-Name' (1) positionné à l 'identité privée de John Cook : JohnCook_private@orange.fr'
- L 'AVP 'SIP-Number-Auth-Items' (607) positionné à la valeur '5', indiquant que le HSS a retourné 5 vecteurs d 'authentification à S-CSCF;
- L 'AVP 'SIP-Auth-Data-Item' (612), incluant 5 fois les AVPs suivants (un par vecteur d 'authentification) :
  - L 'AVP 'SIP-Item-Number' (613) positionné à la valeur '1' pour le premier vecteur d 'authentification (et incrémentée de 1 pour les 4 autres vecteurs d 'authentification), cette séquence indiquant l 'ordre dans lequel utiliser les vecteurs
  - L 'AVP 'SIP-Authentication-Scheme' AVP (608) positionné à la valeur 'Digest-AKAv1-MD5'
  - L 'AVP 'SIP-Authenticate' (609) incluant :
    - La valeur random (RAND);
    - Le jeton d 'authentification réseau (AUTN);
  - L 'AVP 'SIP-Authorization' (610) incluant le résultat attendu (XRES);
  - L 'AVP 'Confidentiality-Key' (625) incluant la clé de confidentialité (CK);
  - L 'AVP 'Integrity-Key' (626) incluant la clé d 'intégrité (IK);
- L 'AVP 'Result-Code' (268) positionné 'DIAMETER SUCCESS' (2001), indiquant que la requête a été exécutée avec succès.

Sur la base des données dans le quintuplé d 'authentification, le S-CSCF retourne une réponse 401 Unauthorized contenant le header WWW-Authenticate et renseigne ce header de la manière suivant comme montré à la figure ci-dessus :

• dans le champs « nonce », sont présents les paramètres RAND et AUTN qui étaient présents dans l 'AVP SIP-Authenticate de la réponse DIAMETER MAA.
Ces deux valeurs ont une longueur de 32 bits et 64 bits respectivement.

• dans le champ « algorithm » la valeur présente est 'AKAv1-MD5' comme présent dans l 'AVP SIPAuthentication-Scheme dans la réponse MAA et qui identifie le mécanisme 3GPP AKA;

• dans les champs ik et ck sont présents les clés d 'intégrité et de chiffrement respectivement comme présentes dans les AVPs Confidentiality-Key et Integrity-Key de la réponse MAA. Ces deux champs ne font pas partie de la définition à l 'origine du header WWW-Authenticate header, comme défini dans le RFC 3261.

Après avoir reçu la réponse SIP 401 (Unauthorized), le P-CSCF doit supprimer en les mémorisant les champs ik et ck du header WWW-Authenticate header, avant de relayer cette réponse à l 'UE.

S-CSCF → I -CSCF (Message 8) et I-CSCF → P-CSCF (Message 9)

SIP/2.0 401 Unauthorized
WWW-Authenticate: Digest realm= « orange.fr »,
nonce=A34Cm+Fva37UYWpGNB34JP, algorithm=AKAv1-MD5,
ik="0123456789abcdeedcba987654321021",
ck="9876543210abcdeedcba012345678944"

RAND et AUTN

P-CSCF → UE (Message 10)

SIP/2.0 401 Unauthorized
WWW-Authenticate: Digest realm= « orange.fr »,
nonce=A34Cm+Fva37UYWpGNB34JP, algorithm=AKAv1-MD5,

RAND et AUTN

A partir du paramètre AUTN reçu, l 'application ISIM sur l 'UE de John Cook découvre qu 'il s 'agit bien du réseau nominal de John Cook qui a envoyé la réponse 401 (Unauthorized).
Il peut dériver de l 'AUTN que le SQN (sequence number) est valide.
Les paramètres RAND et AUTN reçus ainsi que la clé K permettent à l 'ISIM de générer RES, CK et IK et les passe à l 'UE.
L 'UE renvoie une seconde requête SIP REGISTER qui inclut un header « Authorization » incluant entre autres les champs suivants :

- le champ « username » qui inclut l 'identité privée de John Cook,
- le champ « nonce » qui est retourné avec la même valeur que celle reçue dans le header WWW-Authenticate de la réponse SIP 401 (Unauthorized);
- le champ « response » qui inclut le challenge d 'authentification RES dérivé à partir de K et de RAND par l 'application ISIM.

L 'ISIM calcule aussi les clés CK et IK qui sont par ailleurs connues par le P-CSCF (ce dernier les a reçu du S-CSCF dans le message 9). Sur la base de ces clé et d 'autres informations, l 'UE et le P-CSCF établissent des SAs (Secure Associations) IPSec, utilisées par l 'UE pour envoyer la seconde requête REGISTER.

REGISTER sip:orange.fr SIP/2.0
Authorization: Digest username= "JohnCook_private@orange.fr",
realm= "orange.fr",
nonce=A34Cm+Fva37UYWpGNB34JP, algorithm=AKAv1-MD5,
uri="sip:orange.fr",
response="6629fae49393a05397450978507c4ef1"

Lorsque le S-CSCF reçoit le message REGISTER (Message 15), il compare le champ « response » avec le paramètre XRES deu vecteur d'authentification correspondant. Si les valeurs de ces deux informations sont égales, alors l'authentification de l'UE a réussi.

Le but de la formation « IMS Avancé » d'EFORT est de présenter en détail les procédures d'enregistrement, d'établissement de session, d'invocation de services et de taxation IMS. Les protocoles SIP et DIAMETER impliqués dans ces procédures sont décrits dans le contexte IMS et leur usage présenté à l'aide de traces.