Groupe de travail Réseau
Request for Comments : 4740
Catégorie : Sur la voie de la normalisation

M. Garcia-Martin, éd., Nokia
M. Belinchon, Ericsson
M. Pallares-Lopez, Ericsson
C. Canales-Valenzuela, Ericsson
K. Tammi, Nokia

Traduction Claude Brière de L'Isle
novembre 2006

Application de Diameter au protocole d'initialisation de session (SIP)

Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.
(Cette traduction incorpore les errata 2246 et 6028).

Résumé

Le présent document spécifie l'application de Diameter au protocole d'initialisation de session (SIP, *Session Initiation Protocol*). C'est une application Diameter qui permet à un client Diameter de demander des informations d'authentification et d'autorisation. Cette application est conçue pour être utilisée en conjonction avec SIP et elle fournit à un client Diameter co-localisé avec un serveur SIP, la capacité de demander l'authentification des utilisateurs et l'autorisation de l'usage des ressources SIP à partir d'un serveur Diameter.

Table des matières

1. Introduction

Le présent document spécifie l'application de Diameter au protocole d'initialisation de session (SIP, *Session Initiation Protocol*). C'est une application Diameter qui permet à un client Diameter de demander des informations d'authentification et d'autorisation sur SIP à un serveur Diameter pour des services multimédia IP fondés sur SIP (voir la [RFC3261]). De plus, cette application Diameter SIP fournit au client Diameter des fonctions qui vont au delà des l'autorisation et authentification normales, comme la capacité de télécharger ou recevoir des profils d'utilsateur mis à jour, ou des fonctions rudimentaires d'acheminement qui peuvent aider un serveur SIP à trouver un autre serveur SIP alloué à l'utilisateur.

On suppose que le serveur SIP (comme un serveur SIP mandataire, registraire, serveur de redirection, ou autre) et le client Diameter sont co-localisés dans le même nœud, de sorte que le serveur SIP est capable de recevoir et traiter les demandes et réponses SIP. À son tour, le serveur SIP s'appuie sur l'infrastructure d'authentification, autorisation, et comptabilité (AAA) pour authentifier la demande SIP et autoriser l'usage de services SIP particuliers.

Le présent document donne les procédures de Diameter pour mettre en œuvre certaines fonctionnalités requises quand SIP est le protocole choisi pour initier et supprimer des sessions multimédia ou quand SIP est utilisé pour d'autres applications non relatives à une session. Cependant, le présent document ne rend obligatoire aucune transposition particulière des procédures de SIP aux procédures d'application Diameter SIP, ni aucune séquence particulière d'événements entre SIP et Diameter. Le présent document fournit des exemples utiles pour montrer l'interaction entre SIP et l'application Diameter SIP afin de réaliser la fonctionnalité désirée.

Cette application n'exige pas et est sans relation avec d'autres services d'authentification fournis par les applications de Diameter Mobile IPv4 [RFC4004] ou de serveur d'accès au réseau Diameter [RFC4005].

Cette application Diameter SIP est en relation lâche avec l'application de contrôle de crédit Diameter [RFC4006]. Bien que les deux applications soient indépendantes, l'application Diameter SIP est capable de fournir les adresses des serveurs de contôle de crédit qui vont mettre en œuvre l'application de contrôle de crédit Diameter [RFC4006].

La Section 5 discute les hypothèses et les configurations supposées par ce document. La Section 6 donne au lecteur les descriptions pour information des commandes et réponses de l'application Diameter SIP avec quelques lignes directrices sur leurs liens avec les procédures de SIP. L'annonce de cette application est spécifiée à la Section 7. La Section 8 fourni une description normative de toutes les nouvelles commandes Diameter définies par cette spécification. Cette application définit de nouvelles AVP. Elles sont décrites à la Section 9. Cette application étend les paires de valeur-attribut de code de résultat avec quelques nouvelles valeurs à la Section 10. Des informations supplémentaires sur l'authentification sont données à la Section 11.

2. Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans la [RFC2119] et indiquent les niveaux d'exigence pour les mises en œuvre conformes.

3. Définitions

Pour les besoins de ce document, le termes et définitions suivants s'appliquent :

Nœud : appareil adressable rattaché à un réseau informatique qui met en œuvre la fonction SIP, la fonction Diameter, ou une combinaison des deux.

Pour les besoins du présent document, les termes et définitions suivants de la [RFC3261] Section 6, s'appliquent :
- Adresse d'enregistrement (AOR, *Address-of-Record*)
- Mandataire sortant
- Mandataire
- Registraire
- Serveur (serveur SIP)
- Agent d'utilisateur (UA, *User Agent*)
- Client d'agent d'utilisateur (UAC, *User Agent Client*)
- Serveur d'agent d'utilisateur (UAS, *User Agent Server*)

Pour les besoins du présent document, les termes et définitions suivants de la [RFC3588] paragraphe 1.3, s'appliquent :
- Autorisation
- Authentification
- Paire Attribut-Valeur (AVP)
- Client Diameter
- Serveur Diameter
- Domaine de rattachement *(domaine de rattachement)*
- Agent de redirection
- Utilisateur

4. Acronymes

AKA *(Authentication and Key Agreement)* : authentification et accord de clé
LIR *(Location-Info-Request)* : Demande d'informations de localisation
LIA *(Location-Info-Answer)* : Réponse d'informations de localisation
MAR *(Multimedia-Auth-Request)* : Demande d'autorisation multimédia

MAA *(Multimedia-Auth-Answer)* : Réponse d'autorisation multimédia
PPR *(Push-Profile-Request)* : Demande de profil poussé
PPA *(Push-Profile-Answer)* : Réponse de profil poussé
RTR *(Registration-Termination-Request)* : Demande de terminaison d'enregistrement
RTA *(Registration-Termination-Answer)* : Réponse de terminaison d'enregistrement
SAR *(Server-Assignment-Request)* : Demande d'allocation de serveur
SAA *(Server-Assignment-Answer)* : Réponse d'allocation de serveur
SL *(Subscriber Locator)* : Localisateur d'abonné
UAR *(User-Authorization-Request)* : Demande d'autorisation d'utilisateur
UAA *(User-Authorization-Answer)* : Réponse d'autorisation d'utilisateur

5. Déclaration d'applicabilité

Le présent document suppose une architecture générale où un domaine de rattachement est composé d'un ou plusieurs nœuds qui mettent en œuvre des fonctions Diameter ou SIP. Les utilisateurs produisent des demandes SIP pour accéder aux ressources SIP. Pour chaque utilisateur particulier, le domaine de rattachement a besoin d'authentifier et autoriser l'usage de ces ressources et/ou du chemin au nœud approprié. On suppose que la base de données contenant les données relatives à l'utilisateur est située en dehors du nœud SIP qui demande l'autorisation. Les données qui appartiennent aux différents utilisateurs peuvent être mémorisées dans différents nœuds dans le domaine de rattachement, mais on suppose que toutes les données relatives à un utilisateur particulier sont mémorisées dans un seul nœud.

Note : Le fait que les données d'utilisateur sont mémorisées dans un seul point du réseau est central pour l'architecture. Cette restriction ne rend pas obligatoire une mise en œuvre particulière, par exemple, il est possible de mettre en œuvre des grappes de bases de données opérant en mode miroir pour fournir la redondance. La propriété exigée par la présente spécification est que les données d'utilisateur auxquelles le serveur Diameter a accès sont mémorisées de façon sûre dans ce qui est vu, d'un point de vue externe, comme une seule base de données d'utilisateur.

Le présent document permet plusieurs configurations du domaine de rattachement. Dans une configuration, un serveur SIP (mandataire, registraire, etc.) est alloué à un utilisateur pour les besoins de déclenchement et d'exécution des services. L'allocation du serveur SIP peut être faite dynamiquement, par exemple, au moment où l'utilisateur s'enregistre dans le réseau. Cette configuration exige d'un serveur SIP, normalement situé à la bordure du réseau, qu'il soit capable d'allouer un autre serveur SIP pour l'utilisateur et aussi qu'il prenne en charge l'acheminement des demandes et réponses SIP vers ce serveur SIP alloué. Le serveur SIP et les nœuds mettent en œuvre un client Diameter.

Dans une autre configuration, l'adresse d'un mandataire SIP de sortie est configurée (par des moyens qui sortent du domaine d'application de la présente spécification) dans l'agent d'utilisateur SIP. Le client Diameter de sortie dans le nœud mandataire SIP de sortie authentifie l'utilisateur, demande l'autorisation des demandes SIP, et effectue les activités de comptabilité.

6. Vue d'ensemble du fonctionnement

Cette Section donne une description pour information de la façon dont l'application Diameter SIP peut être utilisée avec SIP. Cette Section n'est pas destinée à rendre obligatoire un usage spécifique de l'application Diameter SIP ni une transposition spécifique entre les messages SIP et Diameter. On fournit une collection d'exemples qui montrent comment la fonction AAA requise peut être réalisée en conjonction avec SIP.

6.1 Architecture générale

L'application Diameter SIP peut être utilisée dans un environnement SIP où une interface à une infrastructure AAA est nécessaire pour authentifier et autoriser l'usage des ressources de SIP. Cette application fournit la prise en charge des agents d'utilisateur et mandataires SIP qui mettent en œuvre et utilisent l'authentification HTTP par résumé [RFC2617], qui est le mécanisme d'authentification rendu obligatoire par SIP [RFC3261]. L'application est extensible et, si le besoin s'en fait sentir, elle peut être étendue pour fournir la prise en charge d'autres mécanismes d'authentification ou des extensions pour l'authentification HTTP par résumé quand cela se produit.

Cette application fournit une prise en charge limitée des services de comptabilité comme suit : le serveur Diameter est capable de fournir les adresses des serveurs de comptabilité au client Diameter. La Figure 1 ci-dessous montre une vue

générale de l'intégration de l'architecture SIP dans l'architecture AAA.

Dans la Figure 1, il y a un ou plusieurs agents d'utilisateur SIP (UA) qui initient ou terminent le trafic SIP à travers un ou plusieurs serveurs SIP. Les deux serveurs SIP mettent en œuvre un client Diameter qui prend en charge l'application Diameter décrite dans cette spécification.

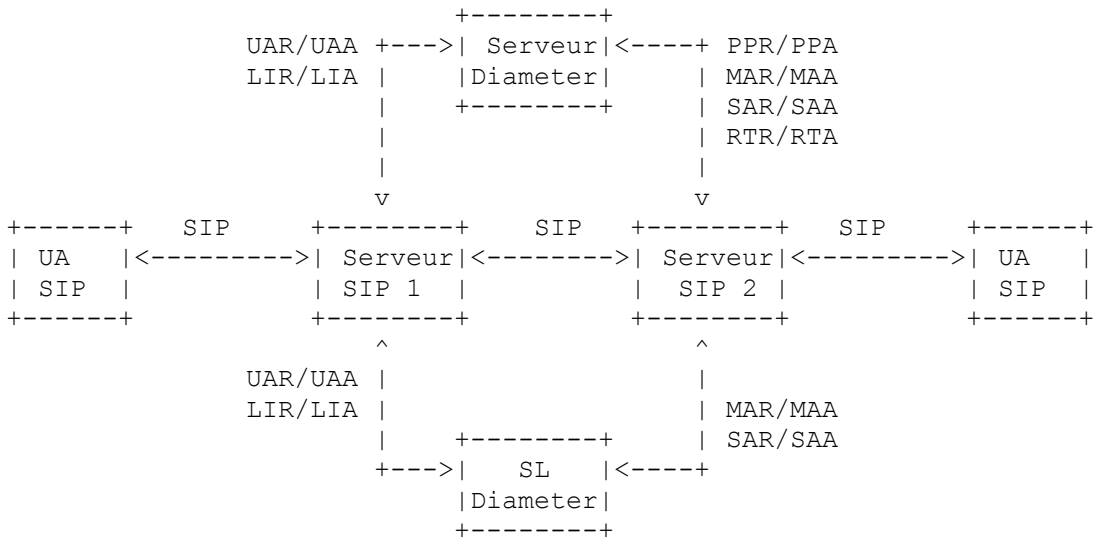


Figure 1 : Architecture de l'application Diameter pour SIP

Dans la Figure 1, on peut voir que le serveur SIP 1 envoie différentes commandes Diameter et reçoit des réponses différentes de celles envoyées et reçues par le serveur SIP 2. C'est parce que le serveur SIP 1 dans la Figure 1 est situé à la bordure d'un réseau, et sa principale tâche est de situer le serveur SIP 2. Le serveur SIP 2 demande et reçoit les données d'authentification et d'autorisation du serveur Diameter et n'est pas situé à la bordure du réseau.

Cette application Diameter suppose que toutes les données relevant d'un certain utilisateur sont mémorisées dans un seul serveur Diameter. Pour assurer la redondance, plusieurs serveurs Diameter peuvent être configurés de façon redondante, et dans ce cas, tous conservent les données synchronisées et opèrent de l'extérieur comme un seul serveur Diameter.

Par rapport au serveur SIP 1 de la Figure 1, l'application Diameter SIP fournit la prise en charge de l'existence d'un groupe de ces serveurs, normalement configurés à travers un ou plusieurs enregistrements du DNS qui pointent sur plusieurs hôtes (c'est une configuration normale dans les déploiements SIP courants). Il n'y a pas d'exigence que ces types de serveurs conservent l'état relatif à l'application Diameter SIP.

L'application Diameter SIP fournit la prise en charge d'une caractéristique qui permet à un domaine administratif de fournir une collection de serveurs SIP 2 (comme dans la Figure 1). Une fois que l'utilisateur s'est enregistré pour la première fois, un de ces serveurs SIP est choisi et toutes les demandes SIP relatives à l'utilisateur sont traitées par le même serveur SIP.

Le localisateur d'abonné (SL, *Subscriber Locator*) Diameter sert à localiser le serveur Diameter qui contient les données relatives à l'utilisateur. Sa fonction se fonde sur le mécanisme Diameter de redirection qui est décrit au paragraphe 6.8.

On devrait noter que le présent document ne rend obligatoire aucune architecture SIP/AAA particulière. Cependant, l'application Diameter SIP fournit la fonction nécessaire pour s'accommoder de toutes les différentes architectures où SIP et Diameter sont utilisés.

Les paragraphes qui suivent donnent une vue informative de l'application Diameter SIP, de ses commandes, et d'une possible interaction avec la signalisation SIP.

6.2 Authentification de l'utilisateur par le serveur Diameter

C'est le mécanisme générique pour authentifier les utilisateurs. Dans cette approche, on montre un exemple d'un réseau administratif où le serveur Diameter authentifie les demandes de l'utilisateur SIP. Ce pourrait être le cas d'un réseau de taille moyenne où le serveur Diameter garde des enregistrements d'utilisateur et authentifie les demandes SIP pour

effectuer une certaine transaction. On a choisi de montrer une demande SIP REGISTER dans l'exemple, mais le serveur SIP pourrait demander l'authentification de toute autre demande SIP.

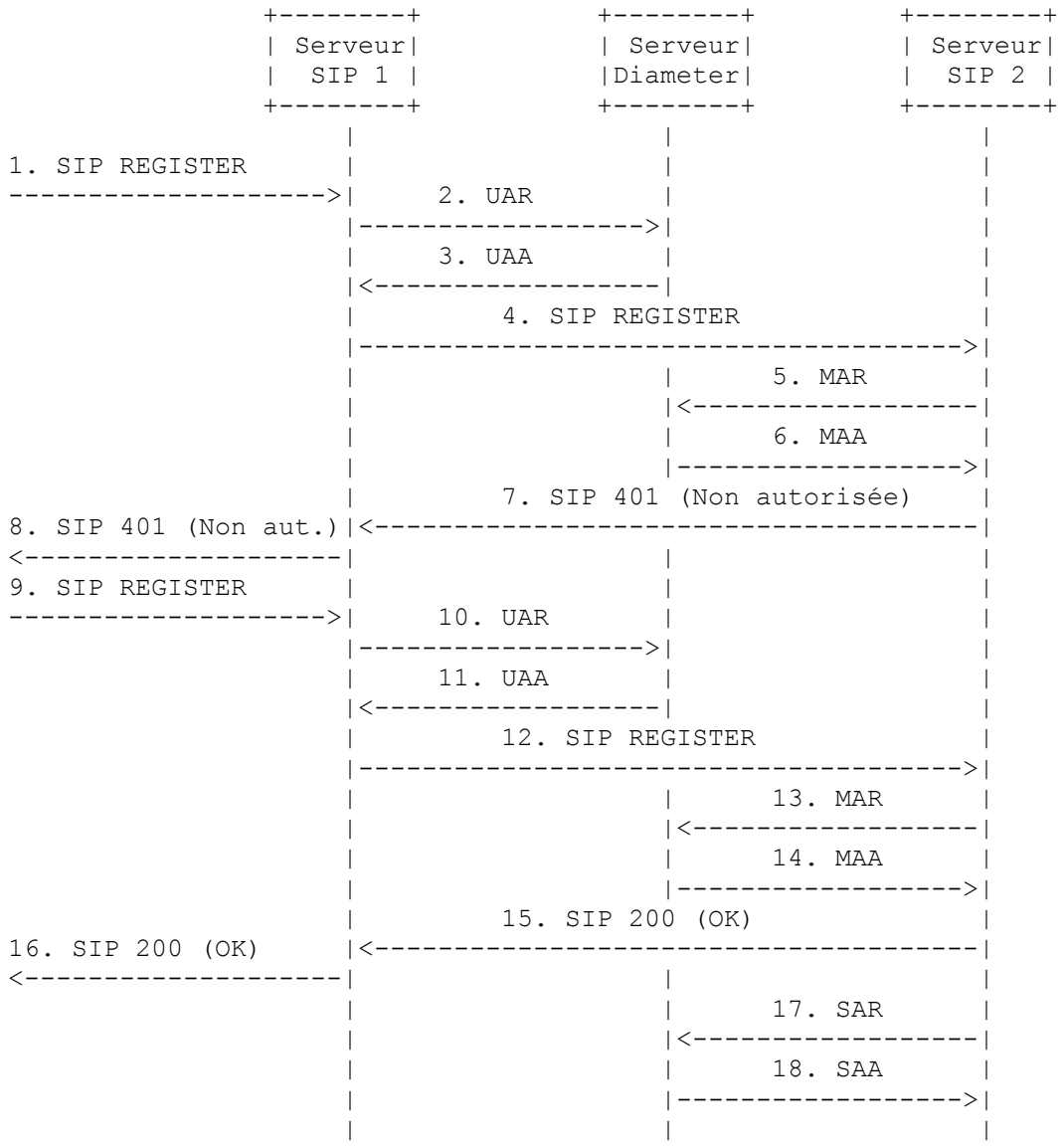


Figure 2 : Authentification effectuée dans le serveur Diameter

À la Figure 2, un client d'agent d'utilisateur SIP (UAC) envoie une demande SIP REGISTER (étape 1) au serveur SIP 1, qui reçoit la demande SIP. À la Figure 2, on suppose que ce serveur SIP est situé à la bordure du domaine administratif de rattachement. Le client Diameter dans le serveur SIP 1 contacte son serveur Diameter en envoyant un message Diameter Demande d'autorisation d'utilisateur (UAR, *User-Authorization-Request*) (étape 2) pour déterminer si cet utilisateur est admis à recevoir le service, et si oui, pour demander l'adresse d'un serveur SIP local capable de traiter cet utilisateur. Le serveur Diameter répond par un message Diameter Réponse d'autorisation d'utilisateur (UAA, *User-Authorization-Answer*) (étape 3) qui indique une liste des capacités que le serveur SIP 1 peut utiliser pour choisir le serveur SIP approprié (serveur SIP 2) et/ou un URI SIP ou SIPS pointant sur le serveur SIP 2.

Le serveur SIP 1 transmet la demande SIP REGISTER (étape 4) à un serveur SIP approprié (serveur SIP 2). Ensuite le client Diameter dans le serveur SIP 2 demande l'authentification d'utilisateur au serveur Diameter en envoyant un message Diameter Demande d'authentification multimédia (MAR, *Multimedia-Auth-Request*) (étape 5). Cette demande sert aussi à faire savoir au serveur Diameter l'URI SIP ou SIPS du serveur SIP 2, afin de retourner les demandes suivantes pour le même utilisateur au même serveur SIP 2. Le serveur Diameter répond par un message Diameter Réponse d'authentification multimédia (MAA, *Multimedia-Auth-Answer*) (étape 6) avec l'AVP Code de résultat réglé à la valeur AUTH_DIAMETER_MULTI_TOURS. Le serveur Diameter génère aussi un nom occasionnel et inclut un défi dans le message MAA. Le serveur SIP 2 utilise ce défi pour le transposer en l'en-tête WWW-Authenticate dans la réponse SIP 401

(Non autorisé) (étape 7) qui est renvoyée au serveur SIP 1 et ensuite à l'UAC SIP (étape 8).

Le serveur SIP 1 reçoit une demande SIP REGISTER suivante contenant les accréditifs de l'utilisateur (étape 9). Noter que le serveur SIP 1 n'a pas besoin de garder un état, et même plus, qu'il n'est pas garanti que la demande SIP arrive au même serveur SIP 1 ; il pourrait y avoir un groupe de serveurs SIP 1 opérant en configuration redondante. Le client Diameter dans le serveur SIP 1 contacte le serveur Diameter en envoyant un message Diameter UAR (étape 10) pour déterminer le serveur SIP alloué à l'utilisateur. Le serveur Diameter envoie l'URI SIP ou SIPS du serveur SIP 2 dans un message Diameter UAA (étape 11).

Ensuite le serveur SIP 1 transmet la demande SIP REGISTER au serveur SIP 2 (étape 12). Le serveur SIP 2 extrait les accréditifs de la demande SIP REGISTER. Le client Diameter dans le serveur SIP 2 envoie ces accréditifs dans un message Diameter MAR (étape 13) au serveur Diameter. À ce point, le serveur Diameter est capable d'authentifier l'utilisateur, et en cas de succès, retourne un message Diameter MAA (étape 14) avec l'AVP Code de résultat réglée à la valeur DIAMETER_RÉUSSI.

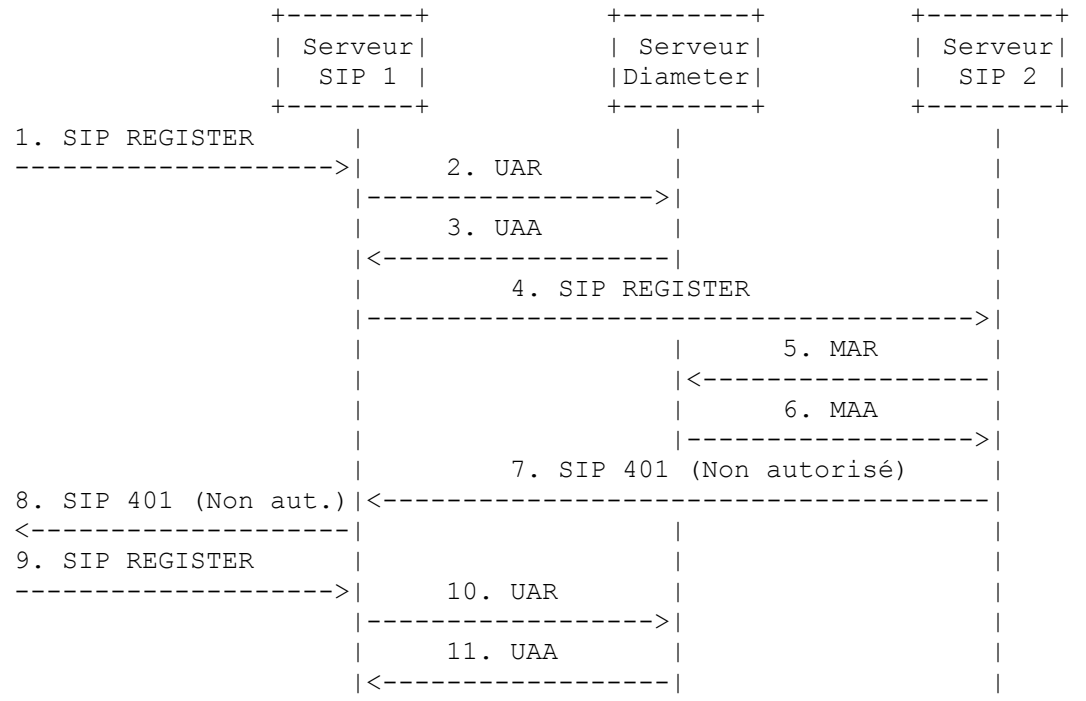
Ensuite, le serveur SIP 2 génère une réponse SIP 200 (OK) (étape 15) qui est transmise au serveur SIP 1 et finalement à l'UAC SIP (étape 16).

Si le client Diameter dans le serveur SIP 2 est intéressé à télécharger les informations de profil d'utilisateur ou est obligé de mémoriser l'adresse du serveur SIP dans le serveur Diameter, alors le client Diameter envoie un message Diameter SAR (étape 17) au serveur Diameter. Le serveur Diameter réplique avec un message Diameter SAA (étape 18) qui contient les informations de profil d'utilisateur demandées et l'accusé de réception de la mémorisation d'adresse du serveur SIP. Ces actions sont nécessaires quand le serveur SIP doit restituer un profil d'utilisateur utilisé pour fournir des services à l'usager desservi, ou quand le serveur SIP garde un état pour l'utilisateur, de sorte que le serveur Diameter a besoin de mémoriser l'adresse du serveur SIP.

6.3 Délégation de la vérification finale d'authentification au serveur SIP

Un opérateur avec une large base de serveurs SIP installée peut souhaiter minimiser le nombre d'allers-retours entre le client Diameter et le serveur Diameter. On fournit la prise en charge d'un mécanisme où le serveur Diameter délègue la vérification finale d'authentification au serveur SIP, économisant par là un aller-retour. Le paragraphe 14.1 discute les considérations de sécurité de ce scénario.

On notera que ce scénario n'est pas applicable quand le serveur Diameter est configuré à utiliser un algorithme de session MD5 (MD5-sess) parce que le serveur Diameter exige le nom occasionnel du client pour calculer le H(A1) avant de l'envoyer au client Diameter. Cependant, le nom occasionnel du client pourrait n'être pas disponible à ce moment.



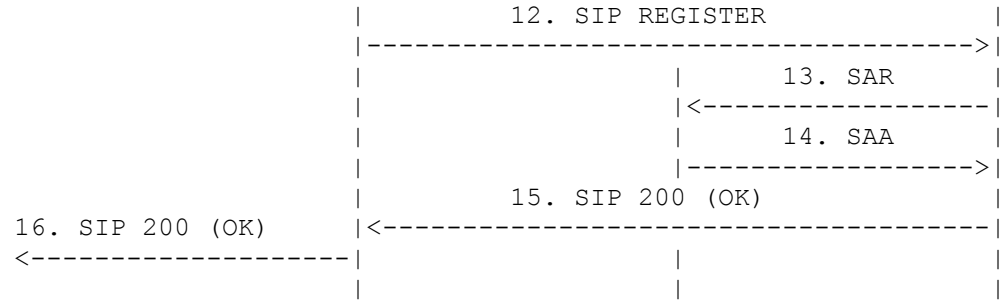


Figure 3 : Délégation d'authentification au serveur SIP

La Figure 3 montre un exemple où un serveur SIP est alloué dynamiquement à servir un agent d'utilisateur SIP avec le soutien du serveur Diameter. Ce peut être le cas de certaines architectures, comme celle du sous système de cœur de réseau multimédia du projet en partenariat de troisième génération (3GPP, *3rd Generation Partnership Project*).

Un premier serveur SIP reçoit une demande SIP REGISTER (étape 1) dont la cible est le domaine du réseau de rattachement. Dans la Figure 3, on suppose que ce serveur SIP est situé à la bordure du domaine administratif de rattachement. Le client Diameter dans ce serveur demande l'autorisation SIP au serveur Diameter de poursuivre l'enregistrement, en envoyant un message Diameter Demande d'autorisation d'utilisateur (UAR, *User-Authorization-Request*) (étape 2). Le message inclut, entre autres paires d'attribut-valeur (AVP, *Attribute-Value-Pair*) l'adresse d'enregistrement (AOR, *Address-Of-Record*) SIP qui est incluse dans la demande SIP REGISTER. Le serveur Diameter vérifie l'AOR SIP et, si c'est un utilisateur valide défini dans le réseau de rattachement, autorise la poursuite de l'enregistrement. Le serveur Diameter répond par un message Diameter Réponse d'autorisation d'utilisateur (UAA, *User-Authorization-Answer*) (étape 3) qui informe le client Diameter/serveur SIP du résultat de l'autorisation de l'utilisateur. En cas de réussite de l'autorisation, le message Diameter UAA indique l'adresse d'un serveur SIP local (le serveur SIP 2 dans la Figure 3) et/ou une liste des capacités que le serveur SIP 1 peut utiliser pour choisir un serveur SIP 2 approprié.

Quand l'autorisation réussit, le serveur SIP 1 transmet la demande SIP REGISTER (étape 4) au serveur SIP approprié (serveur SIP 2). Le client Diameter dans le serveur SIP 2 demande les paramètres d'authentification en envoyant un message Diameter Demande d'autorisation multimédia (MAR, *Multimedia-Auth-Request*) (étape 5) au serveur Diameter. Cette demande indique aussi au serveur Diameter l'URI SIP ou SIPS du serveur SIP 2, afin qu'il retourne les demandes suivantes du même utilisateur au même serveur SIP 2. Le serveur Diameter répond avec un message Diameter Réponse d'autorisation multimédia (MAA, *Multimedia-Auth-Answer*) (étape 6) qui inclut un nom occasionnel et tout le reste des paramètres nécessaires pour l'algorithme d'authentification désigné associé à l'utilisateur. Entre autres, le message MAA inclut une AVP Résumé HA1 qui contient H(A1) (comme défini dans la [RFC2617]) et qui permet au client Diameter de calculer la réponse attendue. Ensuite, le client Diameter peut comparer cette réponse attendue à la réponse au défi envoyé de l'UA SIP. L'absence de l'AVP Résumé HA1 dans la MAA indique que l'authentification et l'autorisation ont lieu dans le serveur Diameter, conformément au scénario décrit au paragraphe 6.2.

Le serveur SIP 2 crée une réponse SIP 401 (Non autorisé) (étape 7) sur la base du défi inclus dans le message MAA, incluant le matériel d'authentification nécessaire au client d'agent d'utilisateur SIP (UAC) pour inclure les accréditifs appropriés. Le serveur SIP 1 transmet la réponse SIP à l'UAC SIP (étape 8).

Le serveur SIP 1 reçoit la prochaine demande SIP REGISTER contenant les accréditifs de l'utilisateur (étape 9). Parce que le serveur SIP 1 n'a pas besoin de garder un état (et qu'il n'est pas garanti que la demande SIP arrive au même serveur SIP 1) le client Diameter du serveur SIP 1 contacte à nouveau le serveur Diameter en envoyant un message Diameter UAR (étape 10) pour déterminer le serveur SIP alloué à l'utilisateur. Le serveur Diameter envoie l'URI SIP ou SIPS du serveur SIP 2 dans un message Diameter UAA (étape 11).

Le serveur SIP 1 transmet la demande SIP REGISTER au serveur SIP 2 (étape 12). Le serveur SIP 2 valide les accréditifs en comparant la réponse fournie par l'UA SIP à la réponse attendue calculée par le serveur SIP 2 (sur la base du H(A1) reçu du serveur Diameter).

Si les accréditifs sont valides, le serveur SIP 2 envoie un message Diameter Demande d'allocation de serveur (SAR, *Server-Assignment-Request*) (étape 13) demandant au serveur Diameter de confirmer l'achèvement de la procédure d'authentification et de confirmer l'URI SIP ou SIPS du serveur SIP qui dessert actuellement l'utilisateur. Le message Diameter SAR sert aussi à demander que le serveur Diameter envoie le profil d'utilisateur au serveur SIP. Le serveur Diameter répond avec un message Diameter Réponse d'allocation de serveur (SAA, *Server-Assignment-Answer*) (étape 14). Si la valeur de l'AVP Code de résultat n'informe pas le serveur SIP 2 d'une erreur, le message SAA peut inclure zéro, une

ou plusieurs AVP Données d'utilisateur SIP contenant les informations dont le serveur SIP 2 a besoin afin de fournir un service à l'utilisateur.

Le serveur SIP 2 génère une réponse SIP 200 (OK) (étape 15) qui est transmise au serveur SIP 1 et finalement à l'UAC SIP (étape 16).

6.4 Demande d'authentification et d'autorisation par le serveur SIP

La Figure 4 décrit un scénario typique où un mandataire SIP sans état demande des informations d'authentification et d'autorisation à un serveur Diameter, pour fournir des services d'acheminement SIP à un agent d'utilisateur SIP. Le serveur mandataire SIP peut être configuré comme un mandataire SIP sortant, de sorte que toutes les demandes initiées par l'UA SIP traversent le mandataire SIP.

Selon la Figure 4, un agent d'utilisateur SIP envoie une demande SIP à son serveur mandataire SIP sortant. Dans ce cas, le message est une demande SIP INVITE (voir l'étape 1) mais ce pourrait être toute autre demande SIP. On suppose que cette demande SIP ne contient aucun accréditif pour l'instant. Le serveur mandataire SIP sortant a besoin d'authentifier et autoriser les services de mandataire offerts à l'utilisateur. Le client Diameter dans le serveur SIP envoie un message Demande d'autorisation multimédia (MAR, *Multimedia-Auth-Request*) (étape 2). Le serveur Diameter génère un nom occasionnel et envoie un message Réponse d'autorisation multimédia (MAA, *Multimedia-Auth-Answer*) (étape 3) qui inclut le nom occasionnel et le reste des données nécessaires au serveur SIP pour mettre au défi l'utilisateur, normalement avec une authentification par résumé HTTP indiquée dans le message MAA. Ces données permettent au serveur SIP de créer une réponse SIP 407 (Authentification de mandataire exigée) (étape 4) qui contient un défi. L'UA SIP crée une nouvelle demande INVITE (étape 5) qui contient les accréditifs. Le client Diameter dans le serveur SIP envoie les accréditifs au serveur Diameter dans un nouveau message MAR Diameter (étape 6). Le serveur Diameter valide les accréditifs et autorise la transaction SIP dans un message MAA Diameter (étape 7). Le serveur SIP transmet la demande SIP INVITE à sa destination (étape 8) selon les procédures SIP régulières. Finalement, l'établissement de session est confirmé par une réponse SIP 200 (OK) (étape 9) qui est transmise à l'UA SIP (étape 10). L'établissement de session est achevé.

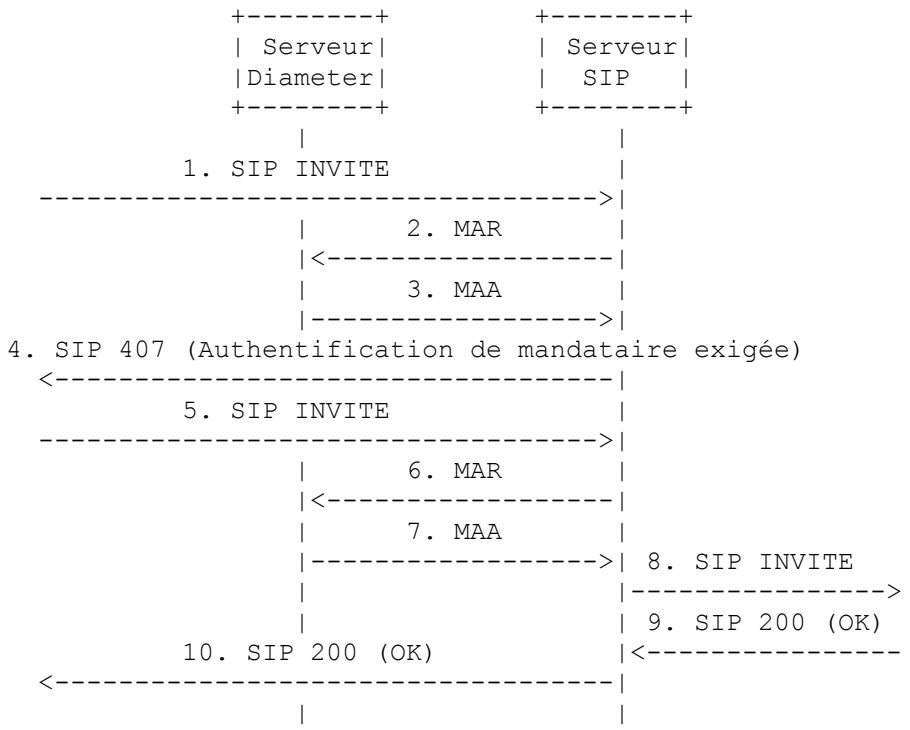


Figure 4 : demande d'autorisation par le serveur SIP

6.5 Localisation du receveur de la demande SIP

La Figure 5 montre le scénario où le serveur SIP 1 peut être configuré comme serveur mandataire SIP de bordure, traitant le trafic SIP à la bordure d'un réseau. Le serveur SIP 1 reçoit une demande SIP INVITE (étape 1). Le serveur SIP 1 a besoin de trouver l'adresse du serveur SIP 2, qui dessert le receveur de la demande SIP. Le client Diameter dans le serveur

SIP 1 envoie un message Diameter Demande d'informations de localisation (LIR, *Location-Info-Request* (LIR) (étape 2) au serveur Diameter. Le serveur Diameter répond par un message Diameter Réponse d'informations de localisation (LIA, *Location-Info-Answer*) (étape 3) qui contient l'URI SIP ou SIPS du serveur SIP 2. Le serveur SIP 1 transmet alors le SIP INVITE au serveur SIP 2 (étape 4). Le serveur SIP 2 transmet finalement le SIP INVITE à l'UAS approprié (étape 5).

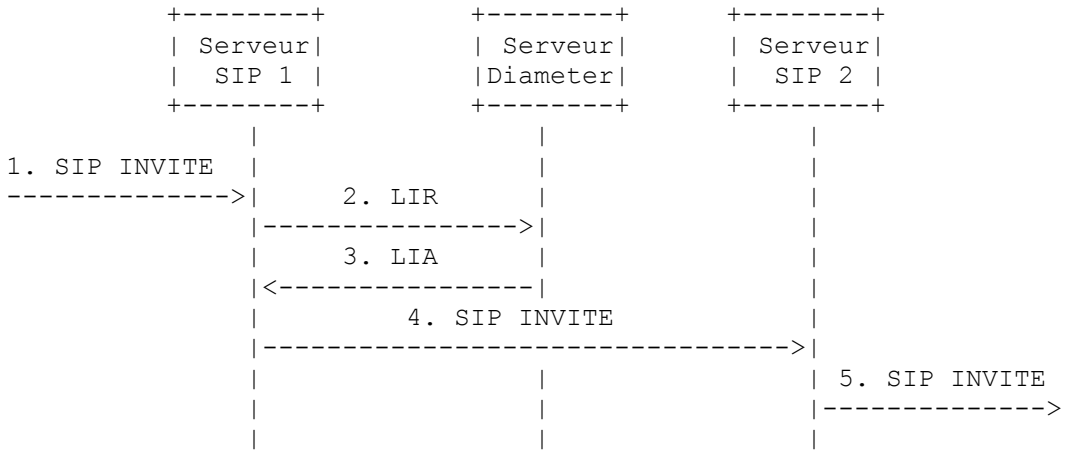


Figure 5 : Localisation du serveur SIP du receveur

Bien que l'exemple montre la connexion entre une demande SIP INVITE et le message Diameter LIR, toute demande SIP autre que REGISTER (comme SUBSCRIBE, OPTIONS, etc.) déclencherait le même message Diameter. (Une demande SIP REGISTER va déclencher un message Diameter UAR, comme indiqué aux Figures 2 et 3.)
Le scénario décrit dans ce paragraphe est aussi applicable dans le cas où un serveur SIP sortant n'est pas intéressé à authentifier l'utilisateur, mais est obligé de localiser un serveur SIP ultérieur pour acheminer les demandes SIP sortantes. Dans ce cas, le serveur SIP sortant est transposé en serveur SIP 1 comme le montre la Figure 5.

6.6 Mise à jour du profil d'utilisateur

L'application Diameter SIP donne un mécanisme pour qu'un serveur Diameter télécharge de façon asynchrone le profil d'un utilisateur à un serveur SIP chaque fois qu'il y a une mise à jour d'un tel profil. On notera que le serveur Diameter attache aussi le profil d'utilisateur au message Diameter Réponse d'allocation de serveur (SAA, *Server-Assignment-Answer*). Ceci est valide pour la plupart des situations quotidiennes ; cependant, l'administrateur peut décider de mettre à jour ou modifier le profil d'utilisateur pour un utilisateur particulier à cause, par exemple, de nouveaux services disponibles pour l'utilisateur. Cela peut impliquer des mécanismes qui sortent du domaine d'application de la présente spécification, comme une intervention humaine, dans le serveur Diameter. Dans cette situation, le serveur Diameter est capable de pousser le nouveau profil d'utilisateur dans le serveur SIP alloué à l'utilisateur.

Ce scénario est illustré à la Figure 6. Quand le profil d'utilisateur change, le serveur Diameter envoie un message Diameter Demande de pousser le profil (PPR, *Push-Profile-Request*) (étape 1) au client Diameter dans le serveur SIP alloué à cet utilisateur (le serveur SIP 2 dans les exemples). Le message Diameter PPR contient une ou plusieurs AVP Données d'utilisateur SIP, une AVP Nom d'utilisateur, et zero, une ou plusieurs AVP SIP-AOR. Le client Diameter dans le serveur SIP 2 accuse réception du message Diameter PPR en envoyant un message Diameter Réponse de profil poussé (PPA, *Push-Profile-Answer*) (étape 2) au serveur Diameter.

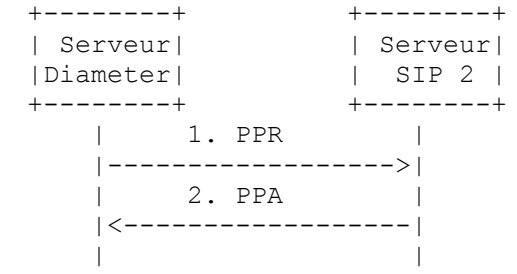


Figure 6 : le serveur Diameter pousse une mise à jour du profil d'utilisateur

6.7 Terminaison de l'état mou SIP

SIP peut créer des états mous dans les nœuds SIP sur la base d'événements comme des enregistrements SIP ou des abonnements à des événements SIP. Ces états sont périodiquement rafraîchis, et cessent d'exister si ils ne sont pas rafraîchis. De plus, une action administrative peut être effectuée pour terminer un état mou SIP, ou l'UA SIP peut explicitement terminer un état mou SIP.

Le protocole Diameter de base offre un mécanisme pour créer et supprimer les états dans les nœuds Diameter. Ces états sont appelés des sessions d'utilisateur Diameter. Le serveur Diameter décide si il utilise une session d'utilisateur Diameter comme mécanisme pour transposer un état mou SIP. Si le serveur Diameter décide d'utiliser des sessions d'utilisateur Diameter, la terminaison d'une session d'utilisateur Diameter implique la terminaison de l'état mou SIP correspondant (par exemple, enregistrement, souscription à un événement) et vice versa. Si le serveur Diameter n'utilise pas de sessions d'utilisateur Diameter, cette application Diameter SIP offre des commandes spécifiques pour gérer les états mous SIP. Les mises en œuvre conformes à la présente spécification DOIVENT prendre en charge les deux mécanismes de gestion de session.

On fournit la prise en charge des deux terminaisons de session initiées par le client Diameter et par le serveur Diameter. Selon que si les sessions Diameter sont utilisées ou non, la terminaison d'un état mou SIP peut être réalisée par une des méthodes suivantes :

- Quand le client Diameter (mandataire SIP) veut terminer l'état mou SIP et que les sessions d'utilisateur Diameter ne sont pas maintenues (c'est-à-dire, l'AVP État de session d'authentification a été précédemment réglé à PAS_D'ÉTAT_MAINTENu) le client Diameter DOIT envoyer un message Demande d'allocation de serveur (SAR) avec l'AVP Type d'allocation de serveur SIP (paragraphe 9.4) réglé à une des valeurs de désenregistrement : FIN_DE_TEMPORISATION_DÉSENREGISTREMENT, DÉSENREGISTREMENT_D'UTILISATEUR, FIN_DE_TEMPORISATION_DÉSENREGISTREMENT_MÉMORISER_NOM_SERVEUR, DÉSENREGISTREMENT_D'UTILISATEUR_MÉMORISER_NOM_SERVEUR, DÉSENREGISTREMENT_ADMINISTRATIF, DÉSENREGISTREMENT_TROP_DE_DONNÉES.

- Quand le client Diameter (mandataire SIP) veut terminer l'état mou SIP et que les sessions d'utilisateur Diameter sont maintenues (c'est-à-dire, l'AVP État de session d'authentification a été précédemment réglé à ÉTAT_MAINTAINU) le client Diameter DOIT envoyer un message Demande de terminaison de session (STR) selon les procédures régulières de la [RFC3588].

- Quand le serveur Diameter veut terminer l'état mou SIP et que les sessions d'utilisateur Diameter sont maintenues (c'est-à-dire, l'AVP État de session d'authentification a été précédemment réglé à PAS_D'ÉTAT_MAINTENU) le serveur Diameter DOIT envoyer un message Demande de terminaison d'enregistrement (RTR, *Registration-Termination-Request*) (voir le paragraphe 8.9).

- Quand le serveur Diameter veut terminer l'état mou SIP et que les sessions d'utilisateur Diameter sont maintenues (c'est-à-dire, l'AVP État de session d'authentification a été précédemment réglé à ÉTAT_MAINTAINU) le serveur Diameter DOIT envoyer un message Demande d'interruption de session (ASR, *Abort-Session-Request*) conformément aux procédures régulières de la [RFC3588].

6.8 Découverte de serveur Diameter

L'hypothèse de base de l'architecture du présent document est que toutes les données relatives à un utilisateur sont mémorisées dans un unique serveur Diameter. Contrairement à l'opinion générale, ceci ne crée pas un seul point de défaillance. On suppose que les serveurs Diameter sont configurés de façon redondante pour tenter d'atténuer le problème du point de défaillance unique.

Dans les grands réseaux, où le nombre d'utilisateurs peut être significativement élevé, il peut y avoir besoin d'adapter le nombre de serveurs Diameter. Toutes les données associées à un utilisateur sont cependant mémorisées dans un serveur Diameter (normalement, fonctionnant dans une configuration redondante) mais les données associées aux différents utilisateurs peuvent résider dans des serveurs Diameter différents.

Bien que cette configuration soit bien adaptable, elle introduit un nouveau problème, à savoir que étant donné en entrée l'AOR SIP de l'utilisateur, comment déterminer lequel des divers serveurs Diameter mémorise les données pour cet AOR SIP particulier. Ce problème est résolu en s'inspirant du mécanisme de redirection Diameter spécifié dans la [RFC3588]. On inclut dans l'architecture un nouveau nœud Diameter qui, pour les besoins de ce document, est appelé le localisateur d'abonné (SL, *Subscriber Locator*) Diameter. Le SL Diameter contient une base de données ou des tableaux

d'acheminement qui transposent les AOR SIP en URI de serveur Diameter. Un URI de serveur Diameter particulier pointe sur le serveur Diameter réel qui mémorise toutes les données relatives à un AOR SIP particulier, et par conséquent, de l'utilisateur qui possède l'AOR SIP. Le SL Diameter agit de façon similaire à l'agent de redirection Diameter, répartissant les demandes Diameter (par exemple, en fournissant l'URI de redirection dans la réponse). Le SL Diameter peut rediriger toutes les demandes relevant d'un utilisateur en réglant l'AVP Usage d'hôte de redirection à une valeur de TOUS_LES_UTILISATEURS, comme spécifé dans la [RFC3588].

Le SL Diameter peut être dupliqué dans différents nœuds le long du réseau, pour les besoins de la construction de l'adaptabilité et de la redondance. La base de données ou les tableaux d'acheminement doivent être cohérents entre tous ces différents SL Diameter, afin que des demandes Diameter égales produisent des réponses Diameter égales, quel que soit le SL Diameter qui traite la demande.

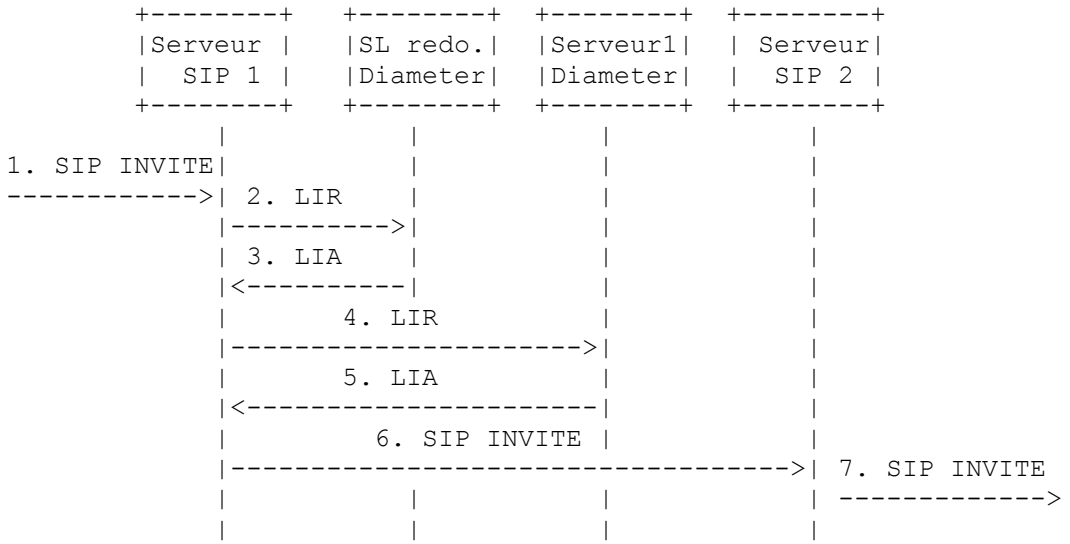


Figure 7 : Localisation d'un serveur Diameter. Le SL redirige les demandes

La Figure 7 montre un exemple de fonctionnement d'un SL Diameter agissant en mode redirection. Le serveur SIP 1 reçoit une demande INVITE (étape 1) adressée (dans l'URI de demande SIP) à un utilisateur pour lequel le client Diameter dans le serveur SIP 1 ne possède pas d'informations d'acheminement. En d'autres termes, le client Diameter dans le serveur SIP 1 ne connaît pas l'URI du serveur Diameter 1. Le client Diameter envoie un message LIR Diameter (étape 2) à tous les SL Diameter configurés dans le réseau. L'adresse de ces SL est supposée être pré-provisionnée dans le client Diameter. Le SL Diameter, sur la base du contenu de l'AVP SIP-AOR et de ses propres tableaux d'acheminement, détermine le serveur Diameter qui mémorise les informations allouées à cet utilisateur. Il construit ensuite un message Diameter LIA (étape 3) qui inclut une AVP Code de résultat réglée à INDICATION_DIAMETER_DE_REDIRECTION et une AVP Hôte de redirection dont la valeur est réglée à l'URI du serveur Diameter qui mémorise les informations relatives à un tel utilisateur. Ensuite, le client Diameter dans le serveur SIP 1 construit un nouveau message LIR (étape 4) adressé au serveur Diameter reçu dans l'AVP Hôte de redirection. Le reste de la procédure est comme décrit dans les paragraphes précédents.

7. Annonce de la prise en charge de l'application

Les mises en œuvre Diameter qui se conforment à la présente spécification DOIVENT annoncer sa prise en charge en includant une AVP Identifiant d'application d'autorisation dans les commandes Demande d'échange de capacités (CER, *Capabilities-Exchange-Request*) et Réponse d'échange de capacités (CEA, *Capabilities-Exchange-Answer*) conformément au protocole Diameter de base [RFC3588]. Cette AVP Identifiant d'application d'autorisation DOIT être réglée à la valeur de cette application Diameter SIP (le paragraphe 13.1 indique la valeur réelle allouée par l'IANA).

8. Codes de commandes d'application Diameter SIP

Toutes les mises en œuvre Diameter qui se conforment à la présente spécification DOIVENT mettre en œuvre et prendre en charge la liste des commandes Diameter du Tableau 1.

Nom de commande	Abréviation	Code	Paragraphe de référence
Demande d'autorisation d'utilisateur	UAR	283	8.1
Réponse d'autorisation d'utilisateur	UAA	283	8.2
Demande d'allocation de serveur	SAR	284	8.3
Réponse d'allocation de serveur	SAA	284	8.4
Demande d'informations de localisation	LIR	285	8.5
Réponse d'informations de localisation	LIA	285	8.6
Demande d'autorisation multimédia	MAR	286	8.7
Réponse d'autorisation multimédia	MAA	286	8.8
Demande de terminaison d'enregistrement	RTR	287	8.9
Réponse de terminaison d'enregistrement	RTA	287	8.10
Demande de profil poussé	PPR	288	8.11
Réponse de profil poussé	PPA	288	8.12

Table 1 : Codes de commande définis

Les paragraphes qui définissent les commandes contiennent le format de message pour cette commande particulière. Les formats de message inclus dans le présent document sont définis conformément au paragraphe 3.2 de la [RFC3588].

8.1 Commande Demande d'autorisation d'utilisateur (UAR)

La demande d'autorisation d'utilisateur (UAR, *User-Authorization-Request*) est indiquée par le code de commande réglé à 283 et le bit 'R' des fanions de commande établi. Le client Diameter dans un serveur SIP envoie cette commande au serveur Diameter pour demander l'autorisation pour l'agent d'utilisateur SIP d'acheminer une demande SIP REGISTER. Parce que la demande SIP REGISTER porte implicitement une permission de lier une AOR à une adresse de contact, le client Diameter utilise l'UAR Diameter comme première demande d'autorisation auprès du serveur Diameter pour autoriser l'enregistrement. Par exemple, le serveur Diameter peut vérifier que l'AOR est un utilisateur légitime du domaine.

Le client Diameter dans le serveur demande l'autorisation SIP pour une des valeurs possibles définies dans l'AVP Type d'autorisation d'utilisateur SIP (paragraphe 9.10).

Le nom d'utilisateur utilisé pour l'authentification de l'utilisateur est convoyé dans une AVP Nom d'utilisateur (définie dans le protocole de base Diameter [RFC3588]). La localisation du nom d'utilisateur d'authentification dans la demande SIP REGISTER varie selon le mécanisme d'authentification. Quand le mécanisme d'authentification est le résumé HTTP comme défini dans la [RFC2617], le nom d'utilisateur d'authentification se trouve dans la directive "username" de la valeur de champ d'en-tête Autorisation SIP. La présente application Diameter SIP fournit seulement la prise en charge de l'authentification HTTP par résumé dans SIP ; d'autres mécanismes d'authentification ne sont pas actuellement supportés.

L'URI SIP ou SIPS à enregistrer est porté dans l'AVP SIP-AOR (paragraphe 9.8). Normalement, cet URI SIP ou SIPS se trouve dans la valeur du champ d'en-tête To de la demande SIP REGISTER qui a déclenché le message Diameter UAR.

L'AVP Identifiant de réseau SIP visité indique le réseau qui fournit les services SIP (par exemple, la fonction de mandataire SIP ou toute autre sorte de services) à l'agent d'utilisateur SIP.

Le format de message de la commande UAR est comme suit :

```
<UAR> ::= < En-tête Diameter : 283, REQ, PXY >
            < Identifiant de session >
            { Identifiant d'application d'autorisation }
            { État de session d'autorisation }
            { Hôte d'origine }
            { Domaine d'origine }
            { Domaine de destination }
            { SIP-AOR }
            [ Hôte de destination ]
            [ Nom d'utilisateur ]
            [ Identifiant de réseau SIP visité ]
            [ Type d'autorisation d'utilisateur SIP ]
          * [ Informations de mandataire ]
```

* [Enregistrement de chemin]
* [AVP]

8.2 Commande Réponse d'autorisation d'utilisateur (UAA)

La Réponse d'autorisation d'utilisateur (UAA, *User-Authorization-Answer*) est indiquée par le code de commande réglé à 283 et le bit 'R' des fanions de commande réglé à zéro. Le serveur Diameter envoie cette commande en réponse à une commande Demande d'autorisation d'utilisateur (UAA) Diameter reçue précédemment. Le serveur Diameter indique le résultat de l'autorisation d'enregistrement demandée. De plus, le serveur Diameter peut indiquer une collection de capacités SIP qui aident le client Diameter à choisir un mandataire SIP pour l'AOR à enregistrer.

En plus des valeurs déjà définies dans la [RFC3588], l'AVP Code de résultat peut contenir une des valeurs définies au paragraphe 10.1.

Chaque fois que le serveur Diameter échoue à traiter le message Diameter UAR, il DOIT arrêter le traitement et retourner l'erreur pertinente dans le message Diameter UAA. Quand le processus est réussi, le serveur Diameter DOIT régler le code à DIAMETER_RÉUSSI dans le message Diameter UAA.

Si le serveur Diameter exige une valeur d'AVP Nom d'utilisateur pour traiter la demande Diameter UAR, mais si le message Diameter UAR ne contient pas de valeur d'AVP Nom d'utilisateur, le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à NOM_D'UTILISATEUR_DIAMETER_EXIGÉ (paragraphe 10.1.2) et la retourner dans un message Diameter UAA. À réception de ce message Diameter UAA avec la valeur d'AVP Code de résultat réglée à NOM_D'UTILISATEUR_DIAMETER_EXIGÉ, le serveur SIP demande normalement l'authentification en renvoyant une réponse SIP 401 (Non autorisé) ou SIP 407 (Authentification de mandataire exigée) à l'origine du message.

Quand la procédure d'autorisation réussit, le serveur Diameter construit un message Réponse d'autorisation d'utilisateur (UAA, *User-Authorization-Answer*) qui DOIT inclure (1) l'adresse du serveur SIP déjà alloué au nom d'utilisateur, (2) les capacités nécessaires au serveur SIP (client Diameter) pour choisir un autre serveur SIP pour l'utilisateur, ou (3) une combinaison des deux options précédentes.

Si le serveur Diameter a déjà connaissance d'un serveur SIP alloué à l'utilisateur, le message Diameter UAA contient l'adresse de ce serveur SIP.

Le message Diameter UAA contient les capacités requise par un serveur SIP pour déclencher et exécuter des services. La présence de ces capacités est exigée dans le message Diameter UAA à cause de la possibilité que le client Diameter (dans le serveur SIP) alloue un serveur SIP différent pour déclencher et exécuter les services pour cet utilisateur particulier.

Si une AVP Nom d'utilisateur est présente dans le message Diameter UAR, alors le serveur Diameter DOIT vérifier l'existence de l'utilisateur dans le domaine, c'est-à-dire, si la valeur de l'AVP Nom d'utilisateur est un utilisateur valide dans ce domaine. Si le serveur Diameter ne reconnaît pas le nom d'utilisateur reçu dans l'AVP Nom d'utilisateur, le serveur Diameter DOIT construire un message Diameter Réponse d'autorisation d'utilisateur (UAA, *User-Authorization-Answer*) et DOIT régler l'AVP Code de résultat à ERREUR_DIAMETER_UTILISATEUR_INCONNU.

Si une AVP Nom d'utilisateur est présente dans le message Diameter UAR, alors le serveur Diameter DOIT autoriser que cette valeur d'AVP Nom d'utilisateur soit capable d'enregistrer l'URI SIP ou SIPS inclus dans l'AVP SIP-AOR. Si cette autorisation échoue, le serveur Diameter doit régler l'AVP Code de résultat à ERREUR_DIAMETER_IDENTITÉS_NON_CORRESPONDANTES et l'envoyer dans un message Diameter UAA.

Note : la corrélation entre les valeurs d'AVP Nom d'utilisateur et SIP-AOR est exigée afin d'éviter l'enregistrement d'une SIP-AOR allouée à un autre utilisateur.

Si il y a une AVP Identifiant de réseau SIP visité dans le message Diameter UAR, et si la valeur de l'AVP Type d'autorisation d'utilisateur SIP reçue dans le message Diameter UAR est réglée à ENREGISTREMENT ou ENREGISTREMENT_ET_CAPACITÉS le serveur Diameter DEVRAIT alors vérifier si il est permis à l'utilisateur de circuler dans le réseau spécifié dans l'AVP Identifiant de réseau SIP visité dans le message Diameter UAR. Si il n'est pas permis à l'utilisateur de circuler dans ce réseau, le serveur Diameter AAA DOIT régler la valeur de l'AVP Code de résultat dans le message Diameter UAA à ERREUR_DIAMETER_ITINÉRANCE_NON_PERMISE.

Si l'AVP Type d'autorisation d'utilisateur SIP reçue dans le message Diameter UAR est réglée à ENREGISTREMENT ou ENREGISTREMENT_ET_CAPACITÉS, alors le serveur Diameter DEVRAIT vérifier si la valeur d'AVP SIP-AOR est

autorisée à s'enregistrer dans le domaine de rattachement. Lorsque l'AOR SIP n'est pas autorisée à s'enregistrer dans le domaine de rattachement, le serveur Diameter DOIT régler l'AVP Code de résultat à AUTORISATION_DIAMETER_REJETÉE et l'envoyer dans un message Diameter UAA.

Quand l'AVP Type d'autorisation d'utilisateur SIP n'est pas présente dans le message Diameter UAR, ou quand elle est présente et que sa valeur est réglée à ENREGISTREMENT, alors :

- Si le serveur Diameter n'a pas connaissance d'enregistrements précédents du nom de l'utilisateur (incluant des enregistrements d'autres AOR SIP allouées au même nom d'utilisateur) alors le serveur Diameter ne connaît aucun serveur SIP alloué à l'utilisateur. Dans ce cas, le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à PREMIER_ENREGISTREMENT_DIAMETER dans le message Diameter UAA, et le serveur Diameter DEVRAIT inclure les capacités de serveur SIP requises dans la valeur d'AVP Capacités de serveur SIP dans le message Diameter UAA. L'AVP Capacités de serveur SIP aide le client Diameter (serveur SIP) à choisir un serveur SIP approprié pour l'utilisateur, conformément aux capacités requises.

- Dans certains cas, le serveur Diameter a connaissance d'un serveur SIP alloué précédemment pour la même AOR SIP ou des AOR SIP différentes allouées au même nom d'utilisateur. Dans ces cas, la réallocation d'un nouveau serveur SIP peut ou non être nécessaire, selon les capacités du serveur SIP. Le serveur Diameter DOIT toujours inclure l'URI SIP du serveur SIP alloué dans l'AVP URI de serveur SIP du message UAA. Si le serveur Diameter ne retourne pas les capacités SIP, le serveur Diameter DOIT régler l'AVP Code de résultat dans le message Diameter UAA à ENREGISTREMENT_DIAMETER_SUIVANT. Autrement (c'est-à-dire, si le serveur Diameter inclut une AVP Capacités de serveur SIP) alors le serveur Diameter DOIT régler l'AVP Code de résultat dans le message Diameter UAA à CHOIX_DE_SERVEUR_DIAMETER. Alors le client Diameter détermine, sur la base des informations reçues, si il a besoin de choisir un nouveau serveur SIP.

Quand la valeur d'AVP Type d'autorisation d'utilisateur SIP reçue dans le message Diameter UAR est réglée à ENREGISTREMENT_ET_CAPACITÉS, le serveur Diameter DOIT alors retourner la liste des capacités dans la valeur d'AVP Capacités de serveur SIP du message Diameter UAA, il DOIT régler le Code de résultat à DIAMETER_RÉUSSI, et il NE DOIT PAS retourner une AVP URI de serveur SIP. L'AVP Capacités de serveur SIP permet au serveur SIP (client Diameter) de choisir un autre serveur SIP approprié pour invoquer et exécuter des services pour l'utilisateur, selon les capacités requises. Le serveur Diameter PEUT laisser vide la liste des capacités pour indiquer que tout serveur SIP peut être choisi.

Quand la valeur d'AVP Type d'autorisation d'utilisateur SIP reçue dans le message Diameter UAR est réglée à DÉSENREGISTREMENT, alors :

- Si le serveur Diameter a connaissance d'un serveur SIP alloué à l'AOR SIP qui se désenregistre, le serveur Diameter DOIT régler l'code d'AVP de résultat à DIAMETER_RÉUSSI et DOIT régler la valeur de l'AVP URI de serveur SIP au serveur SIP connu, et les retourner dans le message Diameter UAA.

- Si le serveur Diameter n'a pas connaissance d'un serveur SIP alloué à l'AOR SIP qui se désenregistre, il DOIT alors régler l'AVP Code de résultat dans le message Diameter UAA à ERREUR_DIAMETER_IDENTITÉ_NON_ENREGISTRÉE.

Le format de message de la commande UAA est comme suit :

```
<UAA> ::= < En-tête Diameter : 283, PXY >
          < Identifiant de session >
          { Identifiant d'application d'autorisation }
          { État de session d'autorisation }
          { Code de résultat }
          { Hôte d'origine }
          { Domaine d'origine }
          [ URI de serveur SIP ]
          [ Capacités de serveur SIP ]
          [ Durée de vie d'autorisation ]
          [ Période de grâce d'autorisation ]
          [ Hôte de redirection ]
          [ Usage d'hôte de redirection ]
          [ Redirect-Max-Cache-Time ]
        * [ Informations de mandataire ]
```

* [Enregistrement de chemin]
* [AVP]

8.3 Commande Demande d'allocation de serveur (SAR)

La commande Demande d'allocation de serveur (SAR, *Server-Assignment-Request*) est indiquée par le code de commande réglé à 284 et le bit 'R' des fanions de commande établi. Le client Diameter dans un serveur SIP envoie cette commande au serveur Diameter pour indiquer l'achèvement du processus d'authentification et pour demander que le serveur Diameter mémorise l'URI du serveur SIP qui dessert actuellement l'utilisateur. Les principales fonctions de la commande Diameter SAR sont d'informer le serveur Diameter de l'URI du serveur SIP alloué à l'utilisateur, et pour le mémoriser ou le supprimer du serveur Diameter. De plus, le client Diameter peut demander à télécharger le profil d'utilisateur ou une partie de lui.

Durant la procédure d'enregistrement, un serveur SIP est alloué à l'utilisateur. Le client Diameter dans le serveur SIP alloué DOIT inclure son propre URI dans l'AVP URI de serveur SIP du message Diameter Demande d'allocatio de serveur (SAR, *Server-Assignment-Request*) et l'envoyer au serveur Diameter. Le serveur Diameter prend alors connaissance de l'allocation du serveur SIP au nom d'utilisateur et de l'URI du serveur.

Le client Diameter dans le serveur SIP PEUT envoyer un message Diameter SAR pour d'autres raisons. Ces raisons sont identifiées dans la valeur de l'AVP Type d'allocation de serveur SIP *(SIP-Server-Assignment-Type)* (paragraphe 9.4). Par exemple, un client Diameter dans un serveur SIP peut contacter le serveur Diameter pour demander le désenregistrement d'un utilisateur, pour informer le serveur Diameter d'un échec d'authentification, ou juste pour télécharger le profil de l'utilisateur. Pour une description complète de toutes les valeurs de l'AVP Type d'allocation de serveur SIP, voir le paragraphe 9.4.

Normalement, la réception d'une demande SIP REGISTER dans un serveur SIP va déclencher l'envoi par le client Diameter dans le serveur SIP du message Diameter SAR. Cependant, si un serveur SIP reçoit une autre demande SIP, comme une INVITE, et si le serveur SIP n'a pas de profil d'utilisateur, le client Diameter dans le serveur SIP peut envoyer le message Diameter SAR au serveur Diameter afin de télécharger le profil d'utilisateur et faire connaître au serveur Diameter le serveur SIP alloué à l'utilisateur.

Le profil d'utilisateur est un élément d'information important qui dicte le comportement du serveur SIP quand il déclenche ou fournit des services pour l'utilisateur. Normalement le profil d'utilisateur est divisé en :
- o services à rendre à l'utilisateur quand il est enregistré et initie une demande SIP,
- o services à rendre à l'utilisateur quand il est enregistré et qu'une demande SIP destinée à cet utilisateur arrive au mandataire SIP,
- o services à rendre à l'utilisateur quand il n'est pas enregistré et qu'une demande SIP qui lui est destinée arrive au mandataire SIP.

L'AVP Type d'allocation de serveur SIP indique la raison pour laquelle le client Diameter (serveur SIP) a contacté le serveur Diameter. Si le client Diameter règle la valeur de l'AVP Type d'allocation de serveur SIP à ENREGISTREMENT, RÉ_ENREGISTREMENT, UTILISATEUR_NON_ENREGISTRÉ, PAS_D'ALLOCATION, ÉCHEC_D'AUTHENTIFICATION ou FIN_DE_TEMPORISATION_D'AUTHENTIFICATION, le client Diameter DOIT inclure exactement une AVP SIP-AOR dans le message Diameter SAR.

Le message SAR PEUT contenir zéro, une ou plusieurs AVP Type de données d'utilisateur SIP pris en charge. Chacune d'elles contient un type de données d'utilisateUr compris par le serveur SIP. Cela permet au client Diameter de donner une indication au serveur Diameter des différents formats de données d'utilisateur compris par le serveur SIP. Le serveur Diameter utilise ces informations pour choisir une ou plusieurs AVP Données d'utilisateur SIP qui vont être incluses dans le message SAA.

Le format de message de la commande SAR est comme suit :

<SAR> ::= < En-tête Diameter : 284, REQ, PXY >
< Identifiant de session >
{ Identifiant d'application d'autorisation }
{ État de session d'autorisation }
{ Hôte d'origine }
{ Domaine d'origine }
{ Domaine de destination }

{ Type d'allocation de serveur SIP }
{ Données d'utilisateur SIP déjà disponibles }
[Hôte de destination]
[Nom d'utilisateur]
[URI de serveur SIP]
* [Type de données d'utilisateur SIP pris en charge]
* [SIP-AOR]
* [Informations de mandataire]
* [Enregistrement de chemin]
* [AVP]

8.4 Commande Réponse d'allocation de serveur (SAA)

La commande Réponse d'allocation de serveur (SAA, *Server-Assignment-Answer*) est indiquée par le code de commande réglé à 284 et le bit 'R' des fanions de commande réglé à zéro. Le serveur Diameter envoie cette commande en réponse à une commande Demande d'allocation de serveur (SAR) précédemment reçue. La réponse peut inclure le profil d'utilisateur ou une de ses parties, si nécessaire.

En plus des valeurs déjà définies dans la [RFC3588], l'AVP Code de résultat peut contenir une des valeurs définies au paragraphe 10.1.

La valeur de l'AVP Code de résultat dans le message Diameter SAA peut indiquer un succès ou une erreur dans l'exécution de la commande Diameter SAR. Si la valeur de l'AVP Code de résultat dans le message Diameter SAA ne contient pas un code d'erreur, le message SAA PEUT inclure une ou plusieurs AVP Données d'utilisateur SIP qui contiennent normalement le profil de l'utilisateur, indiquant les services que le serveur SIP peut fournir à cet usager.

Le serveur Diameter PEUT inclure une ou plusieurs AVP Type de données d'utilisateur SIP pris en charge, dont chacune identifie un type de format de données d'utilisateur supporté dans le serveur Diameter. Si il n'y a pas de type commun de données d'utilisateur pris en charge entre le client Diameter et le serveur Diameter, le serveur Diameter DEVRAIT déclarer sa liste de types de données d'utilisateur supportés en incluant une ou plusieurs AVP Type de données d'utilisateur SIP pris en charge dans un message Diameter SAA. Cette indication est simplement pour des raisons de déboguage, car il n'y a pas de mécanisme de reprise sur défaillance qui permette au client Diameter de restituer le profil dans un format supporté.

Si le serveur Diameter exige une valeur d'AVP Nom d'utilisateur pour traiter la demande Diameter SAR, mais si le message Diameter SAR ne contenait pas de valeur d'AVP Nom d'utilisateur, le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à NOM_D'UTILISATEUR_DIAMETER_EXIGÉ (paragraphe 10.1.2) et la retourner dans un message Diameter SAA. À réception de ce message Diameter SAA avec la valeur de l'AVP Code de résultat réglée à NOM_D'UTILISATEUR_DIAMETER_EXIGÉ, le serveur SIP demande normalement l'authentification en générant une réponse SIP 401 (Non autorisé) ou SIP 407 (Authentification du mandataire exigée) en retour à l'origine du message.

Si l'AVP Nom d'utilisateur est incluse dans le message Diameter SAR, à réception du message Diameter SAR, le serveur Diameter DOIT vérifier l'existence de l'utilisateur dans le domaine, c'est-à-dire, que la valeur de l'AVP Nom d'utilisateur est un utilisateur valide dans ce domaine. Si le serveur Diameter ne reconnaît pas le nom d'utilisateur reçu dans l'AVP Nom d'utilisateur, il DOIT construire un message Diameter Réponse d'allocation de serveur (SAA) et DOIT régler l'AVP Code de résultat à ERREUR_DIAMETER_UTILISATEUR_INCONNU.

Ensuite le serveur Diameter DOIT autoriser que la valeur de l'AVP Nom d'utilisateur est un nom d'authentification valide pour l'URI SIP ou SIPS inclus dans l'AVP SIP-AOR du message Diameter SAR. Si cette autorisation échoue, le serveur Diameter doit régler l'AVP Code de résultat à ERREUR_DIAMETER_IDENTITÉS_NON_CORRESPONDANTES et l'envoyer dans un message Diameter Réponse d'allocation de serveur (SAA).

Après l'exécution réussie de la commande Diameter SAR, le serveur Diameter DOIT mettre à zéro le fanion "authentification en cours" et DEVRAIT passer l'URI SIP de serveur mémorisé temporairement à une mémorisation permanente.

Les actions du serveur Diameter à réception du message Diameter SAR dépendent de la valeur du type d'allocation de serveur SIP :

- Si la valeur de l'AVP Type d'allocation de serveur SIP dans le message Diameter SAR est réglée à ENREGISTREMENT ou RE_ENREGISTREMENT, le serveur Diameter DEVRAIT vérifier qu'il y a seulement une

AVP SIP-AOR. Autrement, le serveur Diameter DOIT répondre avec un message Diameter SAA avec la valeur d'AVP Code de résultat réglée à AVP_DIAMETER_TROP_DE_FOIS et NE DOIT PAS inclure d'AVP Données d'utilisateur SIP. Si il y a seulement une AVP SIP-AOR et si la valeur de l'AVP Données d'utilisateur SIP déjà disponibles est réglée à DONNÉES_D'UTILISATEUR_NON_DISPONIBLES alors le serveur Diameter DEVRAIT inclure une ou plusieurs données de profil d'utilisateur avec l'URI SIP ou SIPS (AVP SIP-AOR) et toutes les autres identités SIP associées à cette AVP dans la valeur de l'AVP Données d'utilisateur SIP du message Diameter SAA. En choisissant le type de données d'utilisateur, le serveur Diameter DEVRAIT prendre en compte les formats pris en charge au serveur SIP (AVP Type de données d'utilisateur SIP pris en charge dans le message SAR) et la politique locale. De plus, le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à DIAMETER_RÉUSSI dans le message Diameter SAA. Le serveur Diameter considère l'AOR SIP comme authentifiée et enregistrée.

- Si la valeur de l'AVP Type d'allocation de serveur SIP dans le message Diameter SAR est réglée à UTILISATEUR_NON_ENREGISTRÉ le serveur Diameter DOIT alors mémoriser l'adresse du serveur SIP incluse dans la valeur de l'AVP URI de serveur SIP. Le serveur Diameter va retourner l'adresse du serveur SIP dans les messages Diameter Réponse d'informations de localisation (LIA, *Location-Info-Answer*). Si la valeur de l'AVP Données d'utilisateur SIP déjà disponibles est réglée à DONNÉES_D'UTILISATEUR_NON_DISPONIBLES, le serveur Diameter DEVRAIT alors inclure une ou plusieurs données de profil d'utilisateur associées à l'URI SIP ou SIPS (AVP SIP-AOR) et les identités associées dans la valeur de l'AVP Données d'utilisateur SIP du message Diameter SAA. En choisissant le type de données d'utilisateur, le serveur Diameter DEVRAIT prendre en compte les formats pris en charge au serveur SIP (AVP Type de données d'utilisateur pris en charge dans le message SAR) et la politique locale. Le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à DIAMETER_RÉUSSI. Le serveur Diameter considère l'AOR SIP comme non enregistrée, mais avec un serveur SIP provisionné à déclencher et fournir des services pour des utilisateurs non enregistrés. Noter que dans le cas de UTILISATEUR_NON_ENREGISTRÉ (AVP Type d'allocation de serveur SIP) le serveur Diameter DOIT vérifier qu'il y a seulement une AVP SIP-AOR. Autrement, le serveur Diameter DOIT répondre au message Diameter SAR par un message Diameter SAA, et il DOIT régler la valeur de l'AVP Code de résultat à AVP_DIAMETER_TROP_DE_FOIS et NE DOIT PAS inclure d'AVP Données d'utilisateur SIP. Si l'AVP Nom d'utilisateur n'est pas présente dans le message Diameter SAR et si l'AOR SIP n'est pas connue du serveur Diameter, le serveur Diameter NE DOIT PAS inclure une AVP Nom d'utilisateur dans le message Diameter SAA et il DOIT régler la valeur de l"AVP Code de résultat à ERREUR_DIAMETER_UTILISATEUR_INCONNU.

- Si la valeur de l'AVP Type d'allocation de serveur SIP dans le message Diameter SAR est réglée à FIN_DE_TEMPORISATION_DÉSENREGISTREMENT, DÉSENREGISTREMENT_D'UTILISATEUR, DÉSENREGISTREMENT_TROP_DE_DONNÉES, ou DÉSENREGISTREMENT_ADMINISTRATIF, le serveur Diameter DOIT supprimer l'adresse du serveur SIP associée à toutes les AOR SIP indiquées dans chacune des valeurs d'AVP SIP-AOR incluses dans le message Diameter SAR. Le serveur Diameter considère toutes ces AOR SIP comme non enregistrées. Le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à DIAMETER_RÉUSSI dans le message Diameter SAA.

- Si la valeur de l'AVP Type d'allocation de serveur SIP dans le message Diameter SAR est réglée à FIN_DE_TEMPORISATION_DÉSENREGISTREMENT_DU_NOM_DE_SERVEUR_MÉMORISÉ ou DÉSENREGISTREMENT_DU_NOM_DE_SERVEUR_MÉMORISÉ_PAR_L'UTILISATEUR, le serveur Diameter PEUT garder l'adresse de serveur SIP associée aux AOR SIP incluses dans les valeurs d'AVP SIP-AOR du message Diameter SAR, même si les AOR SIP deviennent non enregistrées. Cette caractéristique permet à un serveur SIP de demander que le serveur Diameter reste un serveur SIP alloué pour ces AOR SIP (valeur d'AVP SIP-AOR) allouées au même nom d'utilisateur, et d'éviter l'allocation de serveur SIP. Le serveur Diameter DOIT considérer toutes ces AOR SIP comme non enregistrées. Si le serveur Diameter honore la demande du client Diameter (serveur SIP) de rester comme serveur SIP alloué, alors le serveur Diameter DOIT garder le serveur SIP alloué à ces AOR SIP affectées au nom d'utilisateur et DOIT régler la valeur de l'AVP Code de résultat à DIAMETER_RÉUSSI dans le message Diameter SAA. Autrement, quand le serveur Diameter n'honore pas la demande du client Diameter (serveur SIP) de rester comme serveur SIP alloué, le serveur Diameter DOIT supprimer le nom de serveur SIP alloué à ces AOR SIP et il DOIT régler la valeur de l'AVP Code de résultat à DIAMETER_RÉUSSI_NOM_DE_SERVEUR_NON_MÉMORISÉ dans le message Diameter SAA.

- Si la valeur de l'AVP Type d'allocation de serveur SIP dans le message Diameter SAR est réglée à PAS_D'ALLOCATION, le serveur Diameter DEVRAIT d'abord vérifier que la valeur de l'AVP URI de serveur SIP dans le message Diameter SAR est le même URI que celui alloué à la valeur d'AVP SIP-AOR. Si elles diffèrent, le serveur Diameter DOIT alors régler la valeur de l'AVP Code de résultat à DIAMETER_INCAPABLE_DE_SE_CONFORMER dans le message Diameter SAA. Autrement, si la valeur de l'AVP Données d'utilisateur SIP déjà disponibles est réglée à DONNÉES_D'UTILISATEUR_NON_DISPONIBLES, alors le serveur Diameter DEVRAIT inclure les données de profil d'utilisateur avec l'URI SIP ou SIPS (AVP SIP-AOR) et

toutes les autres identités SIP associées à cette AVP dans la valeur de l'AVP Données d'utilisateur SIP du message Diameter SAA. En choisissant le type de données d'utilisateur, le serveur Diameter DEVRAIT prendre en compte les formats pris en charge au serveur SIP (AVP Type de données d'utilisateur pris en charge dans le message SAR) et la politique locale.

o Si la valeur de l'AVP Type d'allocation de serveur SIP dans le message Diameter SAR est réglée à ÉCHEC_D'AUTHENTIFICATION ou FIN_DE_TEMPORISATION_D'AUTHENTIFICATION, le serveur Diameter DOIT vérifier qu'il y a exactement une AVP SIP-AOR dans le message Diameter SAR. Si le nombre d'occurrences de l'AVP SIP-AOR n'est pas exactement un, le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à AVP_DIAMETER_TROP_DE_FOIS dans le message Diameter SAA, et NE DEVRAIT PAS effectuer d'autre action. Si il y a exactement une AVP SIP-AOR dans le message Diameter SAR, le serveur Diameter DOIT supprimer l'adresse du serveur SIP alloué à l'AOR SIP affectée au nom de l'utilisateur, et le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à DIAMETER_RÉUSSI dans le message Diameter SAA. Le serveur Diameter DOIT considérer l'AOR SIP comme non enregistrée.

Le format de message de la commande SAA est comme suit :

```
<SAA> ::= < En-tête Diameter : 284, PXY >
          < Identifiant de session >
          { Identifiant d'application d'autorisation }
          { Code de résultat }
          { État de session d'autorisation }
          { Hôte d'origine }
          { Domaine d'origine }
        * [ Données d'utilisateur SIP ]
          [ Informations de comptabilité SIP ]
        * [ Type de données SIP pris en charge par l'utilisateur ]
          [ Nom d'utilisateur ]
          [ Période de grâce d'autorisation ]
          [ Durée de vie d'autorisation ]
          [ Hôte de redirection ]
          [ Usage d'hôte de redirection ]
          [ Redirect-Max-Cache-Time ]
        * [ Informations de mandataire ]
        * [ Enregistrement de chemin ]
        * [ AVP ]
```

8.5 Commande Demande d'informations de localisation (LIR)

La commande Demande d'informations de localisation (LIR, *Location-Info-Request*) est indiquée par le code de commande réglé à 285 et le bit 'R' des fanions de commande établi. Le client Diameter dans un serveur SIP envoie cette commande au serveur Diameter pour demander des informations d'acheminement, par exemple, l'URI du serveur SIP alloué à la valeur d'AVP SIP-AOR affectée aux utilisateurs.

Le format de message de la commande LIR est comme suit :

```
<LIR> ::= < En-tête Diameter : 285, REQ, PXY >
          < Identifiant de session >
          { Identifiant d'application d'autorisation }
          { État de session d'autorisation }
          { Hôte d'origine }
          { Domaine d'origine }
          { Domaine de destination }
          { SIP-AOR }
          [ Hôte de destination ]
        * [ Informations de mandataire ]
        * [ Enregistrement de chemin ]
        * [ AVP ]
```

8.6 Commande Réponse d'informations de localisation (LIA)

La commande Réponse d'informations de localisation (LIA, *Location-Info-Answer*) est indiquée par le code de commande réglé à 285 et le bit 'R' des fanions de commande réglé à zéro. Le serveur Diameter envoie cette commande en réponse à une commande Diameter LIR reçue précécdemment.

En plus des valeurs déjà définies dans la [RFC3588], l'AVP Code de résultat peut contenir une des valeurs définies au paragraphe 10.1. Quand le serveur Diameter trouve une erreur en traitant le message Diameter LIR, le serveur Diameter DOIT arrêter le traitement du message et répondre avec un message Diameter LIA qui inclut le code d'erreur approprié dans la valeur de l'AVP Code de résultat. Quand il n'y a pas d'erreur, le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à DIAMETER_RÉUSSI dans le message Diameter LIA.

Une des erreurs que le serveur Diameter peut trouver est que la valeur d'AVP SIP-AOR n'est pas un utilisateur valide dans le domaine. Dans ce cas, le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à ERREUR_DIAMETER_UTILISATEUR_INCONNU et la retourner dans un message Diameter LIA.

Si le serveur Diameter ne peut pas traiter la commande Diameter LIR, par exemple, à cause d'une erreur dans la base de données, le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à DIAMETER_INCAPABLE_DE_SE_CONFORMER et la retourner dans un message Diameter LIA. Le serveur Diameter NE DOIT PAS inclure d'AVP URI de serveur SIP ou Capacités de serveur SIP dans le message Diameter LIA.

Le serveur Diameter peut ou non avoir connaissance d'un serveur SIP alloué à la valeur d'AVP SIP-AOR incluse dans le message Diameter LIR. Si le serveur Diameter a connaissance d'un serveur SIP alloué à cet utilisateur particulier, le serveur Diameter DOIT inclure l'URI de ce serveur SIP dans l'AVP URI de serveur SIP et la retourner dans un message Diameter LIA. C'est la situation normale quand l'utilisateur est enregistré, ou qu'il est non enregistré mais qu'un serveur SIP est encore affecté à l'utilisateur.

Quand le serveur Diameter n'a pas connaissance d'un serveur SIP alloué à l'utilisateur (c'est normalement le cas quand l'utilisateur n'est pas enregistré) la valeur de l'AVP Code de résultat dans le message Diameter LIA dépend de si le serveur Diameter a connaissance que l'utilisateur a des services définis pour des utilisateurs non enregistrés :

- Les utilisateurs qui ont des services définis pour des utilisateurs non enregistrés peuvent exiger l'allocation d'un serveur SIP pour déclencher et peut-être exécuter ces services. Donc, quand le serveur Diameter n'a pas connaissance d'un serveur SIP alloué, mais que l'utilisateur a des services définis pour les utilisateurs non enregistrés, le serveur Diameter DOIT régler la valeur d'AVP Code de résultat à SERVICE_DIAMETER_NON_ENREGISTRÉ et la retourner dans un message Diameter LIA. Le serveur Diameter PEUT aussi inclure une AVP Capacités de serveur SIP pour faciliter au serveur SIP (client Diameter) le choix d'un serveur SIP approprié avec les capacités requises. L'absence de l'AVP Capacités de serveur SIP indique au serveur SIP (client Diameter) que tout serveur SIP est convenable pour être alloué à l'utilisateur.

- Les utilisateurs qui n'ont pas de service défini pour les utilisateurs non enregistrés n'exigent pas d'autre traitement. Le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à ERREUR_DIAMETER_IDENTITÉ_NON_ENREGISTRÉE et la retourner au client Diameter dans un message Diameter LIA. Le serveur SIP (client Diameter) peut retourner la réponse SIP appropriée (par exemple, 480 (Temporairement indisponible)) à la demande SIP d'origine.

Le format de message de la commande LIA est comme suit :

```
<LIA> ::= < En-tête Diameter : 285, PXY >
          < Identifiant de session >
          { Identifiant d'application d'autorisation }
          { Code de résultat }
          { État de session d'autorisation }
          { Hôte d'origine }
          { Domaine d'origine }
          [ URI de serveur SIP ]
          [ Capacités de serveur SIP ]
          [ Période de grâce d'autorisation ]
          [ Durée de vie d'autorisation ]
          [ Hôte de redirection ]
          [ Usage d'hôte de redirection ]
```

[Redirect-Max-Cache-Time]
* [Informations de mandataire]
* [Enregistrement de chemin]
* [AVP]

8.7 Commande Demande d'authentification multimédia (MAR)

La commande Demande d'authentification multimédia (MAR, *Multimedia-Auth-Request*) est indiquée par le code de commande réglé à 286 et le bit 'R' des fanions de commande établi. Le client Diameter dans un serveur SIP envoie cette commande au serveur Diameter pour demander que le serveur Diameter authentifie et autorise une tentative de l'utilisateur d'utiliser un service SIP (dans ce contexte, le service SIP peut être quelque chose d'aussi simple qu'une souscription SIP ou l'utilisation de services de mandataire pour une demande SIP).

La commande MAR peut aussi enregistrer le propre URI du serveur SIP auprès du serveur Diameter, afin que de futurs messages LIR/LIA puissent retourner cet URI. Si le serveur SIP agit comme registraire SIP (voir les exemples aus paragraphes 6.2 et 6.3) son client Diameter DOIT inclure une AVP URI de serveur SIP dans la commande MAR. Dans tous les autres cas (voir l'exemple du paragraphe 6.4) son client Diameter NE DOIT PAS inclure d'AVP URI de serveur SIP dans la commande MAR.

L'AVP Méthode SIP DOIT inclure le nom de la méthode SIP de la demande SIP qui a déclenché ce message Diameter MAR. Le serveur Diameter peut utiliser cette AVP pour autoriser des demandes SIP selon la méthode.

Le message Diameter MAR DOIT inclure une AVP SIP-AOR. L'AVP SIP-AOR indique la cible de la demande SIP. La valeur de l'AVP est extraite de différents endroits de la demande SIP, selon la sémantique de la demande SIP. Pour les messages SIP REGISTER, la valeur d'AVP SIP-AOR indique l'identité d'utilisateur publique prévue à enregistrer, et c'est l'URI SIP ou SIPS qui est dans la valeur du champ d'en-tête To (addr-spec selon la [RFC3261]) de la demande SIP REGISTER. Pour les autres types de demandes SIP, comme INVITE, SUBSCRIBE, MESSAGE, etc., la valeur de l'AVP SIP-AOR indique la destination prévue de la demande. Elle figure normalement dans l'URI de demande de la demande SIP. Extraire la valeur de l'AVP SIP-AOR du champ d'en-tête SIP approprié est de la responsabilité du client Diameter. Des extensions à SIP (nouvelles méthodes SIP ou nouvelle sémantique) peuvent exiger que l'AOR SIP soit extraite d'autres parties de la demande.

Si la demande SIP inclut des informations d'authentification, le client Diameter DOIT inclure le nom de l'utilisateur, extrait des informations d'authentification de la demande SIP, dans l'AVP Nom d'utilisateur.

Le format de message de la commande MAR est comme suit :

<MAR> ::= < En-tête Diameter : 286, REQ, PXY >
< Identifiant de session >
{ Identifiant d'application d'autorisation }
{ État de session d'autorisation }
{ Hôte d'origine }
{ Domaine d'origine }
{ Domaine de destination }
{ SIP-AOR }
{ Méthode SIP }
[Hôte de destination]
[Nom d'utilisateur]
[URI de serveur SIP]
[Nombre d'léments d'authentification SIP]
[Élément de données d'authentification SIP]
* [Informations de mandataire]
* [Enregistrement de chemin]
* [AVP]

8.8 Commande Réponse d'authentification multimédia (MAA)

La commande Réponse d'authentification multimédia (MAA, *Multimedia-Auth-Answer*) est indiquée par le code de commande réglé à 286 et le bit 'R' des fanions de commande réglé à zéro. Le serveur Diameter envoie cette commande en réponse à une commande Diameter MAR précédemment reçue.

En plus des valeurs déjà définies dans la [RFC3588], l'AVP Code de résultat peut contenir une des valeurs définies au paragraphe 10.1.

Si le serveur Diameter exige une valeur d'AVP Nom d'utilisateur pour traiter la demande Diameter MAR, mais si le message Diameter MAR ne contenait pas de valeur d'AVP Nom d'utilisateur, le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à NOM_D'UTILISATEUR_DIAMETER_EXIGÉ (voir le paragraphe 10.1.2) et la retourner dans un message Diameter MAA. Le serveur Diameter PEUT inclure une AVP Nombre d'éléments d'authentification SIP et une ou plusieurs AVP Élément de données d'authentification SIP avec des informations d'authentification (par exemple, un défi). À réception de ce message Diameter MAA avec la valeur d'AVP Code de résultat réglée à NOM_D'UTILISATEUR_DIAMETER_EXIGÉ, le serveur SIP demande normalement l'authentification en générant une réponse SIP 401 (Non autorisé) ou SIP 407 (Authentification de mandataire exigée) vers l'origine.

Si l'AVP Nom d'utilisateur est présente dans le message Diameter MAR, le serveur Diameter DOIT vérifier l'existence de l'utilisateur dans le domaine, c'est-à-dire, que la valeur de l'AVP Nom d'utilisateur est un utilisateur valide au sein du domaine. Si le serveur Diameter ne reconnaît pas le nom d'utilisateur reçu dans l'AVP Nom d'utilisateur, le serveur Diameter DOIT construire un message Diameter Réponse d'authentification multimédia (MAA, *Multimedia-Auth-Answer*) et DOIT régler l'AVP Code de résultat à ERREUR_DIAMETER_UTILISATEUR_INCONNU.

Si la valeur de l'AVP Méthodes SIP du message Diameter MAR est réglé à REGISTER et si une AVP Nom d'utilisateur est présente, alors le serveur Diameter DOIT autoriser cette valeur d'AVP Nom d'utilisateur pour qu'elle soit capable d'utiliser l'URI inclus dans l'AVP SIP-AOR. Si cette autorisation échoue, le serveur Diameter doit régler l'AVP Code de résultat à ERREUR_DIAMETER_IDENTITÉS_NON_CORRESPONDANTES et l'envoyer dans un message Diameter MAA.

Note : La corrélation entre les valeurs d'AVP Nom d'utilisateur et SIP-AOR est seulement exigée pour les demandes SIP REGISTER, pour empêcher un utilisateur d'enregistrer une AOR SIP allouée à un autre utilisateur. Dans d'autres types de demandes SIP (par exemple, INVITE) l'AOR SIP indique la destination prévue de la demande, plutôt que son origine.

Le serveur Diameter DOIT vérifier si le schéma d'authentification (valeur d'AVP Schéma d'authentification SIP) indiqué dans l'AVP groupée Élément de données d'authentification SIP est ou non pris en charge. Si ce schéma d'authentification n'est pas pris en charge, le serveur Diameter DOIT alors régler l'AVP Code de résultat à ERREUR_DIAMETER_SCHÉMA_D'AUTHENTIFICATION_NON_ACCEPTÉ et l'envoyer dans un message Diameter MAA.

Si l'AVP Nombre d'éléments d'authentification SIP est présent dans le message Diameter MAR, elle indique le nombre d'éléments de données d'authentification que le client Diameter demande. Il est RECOMMANDÉ que le serveur Diameter, quand il construit le message Diameter MAA, inclue un nombre d'AVP Élément de données d'authentification SIP qui soit un sous ensemble des éléments de données d'authentification demandées par le client Diameter dans la valeur de l'AVP Nombre d'éléments d'authentification SIP du message Diameter MAR.

Si l'AVP URI de serveur SIP est présente dans le message Diameter MAR, le serveur Diameter DOIT alors comparer le serveur SIP mémorisé (alloué à l'utilisateur) avec la valeur de l'AVP URI de serveur SIP (reçue dans le message Diameter MAR). Si elles ne correspondent pas, le serveur Diameter DOIT sauvegarder temporairement le serveur SIP nouvellement reçu alloué à l'utilisateur, et DOIT établir un fanion "Authentification en cours" pour l'utilisateur. Si elles correspondent, le serveur Diameter devra mettre à zéro le fanion "Authentification en cours" pour l'utilisateur.

Dans toutes les autres situations, si le traitement de la commande Diameter MAR est un succès et si le serveur Diameter a mémorisé l'URI de serveur SIP, le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à DIAMETER_RÉUSSI et la retourner dans un message Diameter MAA.

Si le traitement de la commande Diameter MAR est un succès, mais si le serveur Diameter n'a pas mémorisé l'URI de serveur SIP parce que l'AVP n'était pas présente dans la commande Diameter MAR, alors le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à :

1. DIAMETER_RÉUSSI_AUTH_ENVOYÉE_SERVEUR_NON_MÉMORISÉ, si le serveur Diameter envoie des accréditifs d'authentification pour créer un défi.

2. DIAMETER_RÉUSSI_NOM_DE_SERVEUR_NON_MÉMORISÉ, si le serveur Diameter a réussi à authentifier l'utilisateur et a autorisé le serveur SIP à poursuivre le traitement de la demande SIP.

Autrement, le serveur Diameter DOIT régler la valeur de l'AVP Code de résultat à DIAMETER_INCAPABLE_DE_SE_CONFORMER, et il NE DOIT PAS inclure d'AVP Élément de données d'authentification SIP.

Le format de message de la commande MAA est comme suit :

```
<MAA> ::= < En-tête Diameter : 286, PXY >
          < Identifiant de session >
          { Identifiant d'application d'autorisation }
          { Code de résultat }
          { État de session d'autorisation }
          { Hôte d'origine }
          { Domaine d'origine }
          [ Nom d'utilisateur ]
          [ SIP-AOR ]
          [ Nombre d'éléments d'authentification SIP ]
        * [ Élément de données d'authentification SIP ]
          [ Durée de vie d'autorisation ]
          [ Période de grâce d'autorisation ]
          [ Hôte de redirection ]
          [ Usage d'hôte de redirection ]
          [ Redirect-Max-Cache-Time ]
        * [ Informations de mandataire ]
        * [ Enregistrement de chemin ]
        * [ AVP ]
```

8.9 Commande Demande de terminaison d'enregistrement (RTR)

La commande Demande de terminaison d'enregistrement (RTR, *Registration-Termination-Request*) est indiquée par le code de commande réglé à 287 et le bit 'R' des fanions de commande établi. Le serveur Diameter envoie cette commande au client Diameter dans un serveur SIP pour indiquer au serveur SIP qu'une ou plusieurs AOR SIP doivent être désenregistrées. La commande permet à un opérateur d'annuler administrativement l'enregistrement d'un utilisateur d'un serveur Diameter centralisé.

Le serveur Diameter a la capacité d'initier le désenregistrement d'un utilisateur et d'informer le serveur SIP au moyen de la commande Diameter RTR. Le serveur Diameter peut décider si seulement une AOR SIP va être désenregistrée, ou une liste d'AOR SIP, ou toutes les AOR SIP allouées à l'utilisateur.

L'absence d'une AVP SIP-AOR dans le message Diameter RTR indique que toutes les AOR allouées à l'utilisateur identifié par l'AVP Nom d'utilisateur sont désenregistrées.

Le serveur Diameter DOIT inclure une valeur d'AVP Cause de désenregistrement SIP pour indiquer la raison du désenregistrement.

Le format de message de la commande RTR est comme suit :

```
<RTR> ::= < En-tête Diameter : 287, REQ, PXY >
          < Identifiant de session >
          { Identifiant d'application d'autorisation }
          { État de session d'autorisation }
          { Hôte d'origine }
          { Domaine d'origine }
          { Hôte de destination }
          { Cause de désenregistrement SIP }
          [ Domaine de destination ]
          [ Nom d'utilisateur ]
        * [ SIP-AOR ]
```

* [Informations de mandataire]
* [Enregistrement de chemin]
* [AVP]

8.10 Commande Réponse de terminaison d'enregistrement (RTA)

La commande Réponse de terminaison d'enregistrement (RTA, *Registration-Termination-Answer*) est indiquée par le code de commande réglé à 287 et le bit 'R' des fanions de commande réglé à zéro. Le client Diameter envoie cette commande en réponse à une commande Diameter RTR précédemment reçue.

En plus des valeurs déjà définies dans la [RFC3588], l'AVP Code de résultat peut contenir une des valeurs défines au paragraphe 10.1.

Si le serveur SIP (client Diameter) exige une valeur d'AVP Nom d'utilisateur pour traiter la demande Diameter RTR, mais si le message Diameter RTR ne contenait pas de valeur d'AVP Nom d'utilisateur, le client Diameter DOIT régler la valeur de l'AVP Code de résultat à NOM_D'UTILISATEUR_DIAMETER_EXIGÉ (voir le paragraphe 10.1.2) et la retourner dans un message Diameter RTA.

Le serveur SIP (client Diameter) applique le désenregistrement administratif à chacun des URI inclus dans chaque valeur d'AVP SIP-AOR, ou, si il n'y a pas d'AVP SIP-AOR présente dans la demande Diameter RTR, à tous les URI alloués à la valeur d'AVP Nom d'utilisateur.

La valeur de l'AVP Cause de désenregistrement SIP dans la commande Diameter RTR a un effet sur les actions effectuées au serveur SIP (client Diameter) :

- Si la valeur est réglée à TERMINAISON_PERMANENTE, alors l'utilisateur a terminé son enregistrement sur le domaine. Si l'information des parties intéressées (par exemple, les abonnés à l'événement "reg" [RFC3680]) sur le désenregistrement administratif est prise en charge par les procédures SIP, le serveur SIP (client Diameter) va le faire. Le client Diameter dans le serveur SIP NE DEVRAIT PAS demander un nouvel enregistrement de l'utilisateur. Le serveur SIP supprime l'état d'enregistrement des AOR désenregistrées.

- Si la valeur est réglée à NOUVEAU_SERVEUR_SIP_ALLOUÉ, le serveur Diameter informe le serveur SIP (client Diameter) qu'un nouveau serveur SIP a été alloué à l'utilisateur, pour une certaine raison. Le serveur SIP, si c'est pris en charge par les procédures SIP, va informer les parties intéressées (par exemple, les abonnés à l'événement "reg" [RFC3680]) du désenregistrement administratif à ce serveur SIP. Le client Diameter dans le serveur SIP NE DEVRAIT PAS demander un nouvel enregistrement de l'utilisateur. Le serveur SIP supprime l'état d'enregistrement des AOR SIP désenregistrées.

- Si la valeur est réglée à CHANGEMENT_DE_SERVEUR_SIP, le serveur Diameter informe le serveur SIP (client Diameter) qu'un nouveau serveur SIP doit être alloué à l'utilisateur, par exemple, parce que les capacités de l'utilisateur exigent un nouveau serveur SIP, ou pas assez de ressources dans le serveur SIP actuel. Si l'information des parties intéressées sur le désenregistrement administratif est prise en charge par les procédures SIP (par exemple, les abonnements à l'événement "reg" [RFC3680]), le serveur SIP le fait. Le client Diameter dans le serveur SIP NE DEVRAIT PAS demander un nouvel enregistrement de l'utilisateur. Le serveur SIP supprime l'état d'enregistrement des AOR SIP désenregistrées.

- Si la valeur est réglée à SUPPRIMER_LE_SERVEUR_SIP, le serveur Diameter informe le serveur SIP (client Diameter) que le serveur SIP ne sera plus lié dans le serveur Diameter à cet utilisateur. Le serveur SIP peut supprimer toutes les données relatives à l'utilisateur.

Le format de message de la commande RTA est comme suit :

<RTA> ::= < En-tête Diameter : 287, PXY >
< Identifiant de session >
{ Identifiant d'application d'autorisation }
{ Code de résultat }
{ État de session d'autorisation }
{ Hôte d'origine }
{ Domaine d'origine }
[Durée de vie d'autorisation]

[Période de grâce d'autorisation]
[Hôte de redirection]
[Usage d'hôte de redirection]
[Redirect-Max-Cache-Time]
* [Informations de mandataire]
* [Enregistrement de chemin]
* [AVP]

8.11 Commande Demande de profil poussé (PPR)

La commande Demande de profil poussé (PPR, *Push-Profile-Request*) est indiquée par le code de commande réglé à 288 et le bit 'R' des fanions de commande établi. Le serveur Diameter envoie cette commande au client Diameter dans un serveur SIP pour mettre à jour le profil d'utilisateur d'un utilisateur déjà enregistré dans ce serveur SIP ou les informations de comptabilité SIP. Cela permet à un opérateur de modifier les données d'un profil d'utilisateur ou les informations de comptabilité et de les pousser au serveur SIP où l'utilisateur est enregistré.

Chaque utilisateur a un profil d'utilisateur associé et d'autres informations de comptabilité. Le profil ou les informations de comptabilité peuvent changer dans le temps, par exemple, par l'ajout de nouveaux services à l'utilisateur. Quand le profil d'utilisateur ou les informations de comptabilité changent, le serveur Diameter envoie une commande Diameter Demande de profil poussé (PPR) au client Diameter dans un serveur SIP, afin de commencer à appliquer ces nouveaux services.

Une commande PPR PEUT contenir une AVP Informations de comptabilité SIP qui met à jour les adresses des serveurs de comptabilité. Les changements d'adresse des serveurs de comptabilité prennent effet immédiatement. Le client Diameter DEVRAIT clore toute session de comptabilité existante avec le serveur existant et commencer à fournir les informations de comptabilité au serveur de comptabilité nouvellement acquis.

Une commande PPR PEUT contenir zéro, une ou plusieurs valeurs d'AVP Données d'utilisateur SIP contenant le nouveau profil d'utilisateur. En choisissant le type de données d'utilisateur, le serveur Diameter DEVRAIT prendre en compte les formats supportés au serveur SIP (AVP Type de données d'utilisateur pris en charge envoyé dans un précédent message SAR) et la politique locale.

L'AVP Nom d'utilisateur indique l'utilisateur à qui le profil est applicable.

Le format de message de la commande tPPR est comme suit :

<PPR> ::= < En-tête Diameter : 288, REQ, PXY >
< Identifiant de session >
{ Identifiant d'application d'autorisation }
{ État de session d'autorisation }
{ Hôte d'origine }
{ Domaine d'origine }
{ Domaine de destination }
{ Nom d'utilisateur }
* [Données d'utilisateur SIP]
[Informations de comptabilité SIP]
[Hôte de destination]
[Durée de vie d'autorisation]
[Période de grâce d'autorisation]
* [Informations de mandataire]
* [Enregistrement de chemin]
* [AVP]

8.12 Commande Réponse de profil poussé (PPA)

La commande Réponse de profil poussé (PPA, *Push-Profile-Answer*) est indiquée par le code de commande réglé à 288 et le bit 'R' des fanions de commande réglé à zéro. Le client Diameter envoie cette commande en réponse à une commande Diameter Demande de profil poussé (PPR) précédemment reçue.

En plus des valeurs déjà définies dans la [RFC3588], l'AVP Code de résultat peut contenir une des valeurs définies au

paragraphe 10.1.

Si il n'y a pas d'erreur lors du traitement du message Diameter PPR reçu, le serveur SIP (client Diameter) DOIT télécharger le profil d'utilisateur reçu des valeurs d'AVP Données d'utilisateur SIP dans le message Diameter PPR et le mémoriser associé à l'utilisateur spécifié dans l'AVP Nom d'utilisateur.

Si le serveur SIP ne reconnaît pas ou ne prend pas en charge certaines des données transférées dans les valeurs d'AVP Données d'utilisateur SIP, le client Diameter dans le serveur SIP DOIT retourner un message Diameter PPA qui inclut une AVP Code de résultat réglée à la valeur ERREUR_DIAMETER_DONNÉES_D'UTILISATEUR_NON_SUPPORTÉES.

Si le serveur SIP (client Diameter) reçoit un message Diameter PPR avec une AVP Nom d'utilisateur AVP qui est inconnue, le client Diameter DOIT régler la valeur d'AVP Code de résultat à ERREUR_DIAMETER_UTILISATEUR_INCONNU et DOIT la retourner au serveur Diameter dans un message Diameter PPA.

Si le serveur SIP (client Diameter) reçoit dans la valeur d'AVP Contenu de données d'utilisateur SIP (de l'AVP groupée Données d'utilisateur SIP) plus de données qu'il ne peut accepter, il DOIT régler la valeur de l'AVP Code de résultat à ERREUR_DIAMETER_TROP_DE_DONNÉES et DOIT la retourner au serveur Diameter dans un message Diameter PPA. Le serveur SIP NE DOIT PAS remplacer le profil d'utilisateur existant par celui reçu dans le message PPR.

Si le serveur Diameter reçoit la valeur d'AVP Code de résultat réglée à ERREUR_DIAMETER_TROP_DE_DONNÉES dans un message Diameter PPA, il DEVRAIT forcer un nouveau réenregistrement de l'utilisateur en envoyant au client Diameter une commande Diameter Demande de terminaison d'enregistrement (RTR, *Registration-Termination-Request*) avec la valeur d'AVP Cause de désenregistrement SIP réglée à CHANGEMENT_DE_SERVEUR_SIP. Cela va forcer un réenregistrement de l'utilisateur et va déclencher le choix d'un nouveau serveur SIP.

Si le client Diameter n'est pas capable d'honorer la commande, pour toute autre raison, il DOIT régler la valeur de l'AVP Code de résultat à DIAMETER_INCAPABLE_DE_SE_CONFORMER et il DOIT la retourner dans un message Diameter PPA.

Le format de message de la commande PPA est comme suit :

```
<PPA> ::= < En-tête Diameter : 288, PXY >
          < Identifiant de session >
          { Identifiant d'application d'autorisation }
          { Code de résultat }
          { État de session d'autorisation }
          { Hôte d'origine }
          { Domaine d'origine }
          [ Hôte de redirection ]
          [ Usage d'hôte de redirection ]
          [ Redirect-Max-Cache-Time ]
        * [ Informations de mandataire ]
        * [ Enregistrement de chemin ]
        * [ AVP ]
```

9. AVP d'application Diameter SIP

Cette Section définit les nouvelles AVP utilisées dans cette application Diameter SIP. Les applications conformes à la présente spécification DOIVENT mettre en œuvre ces AVP.

Le Tableau 2 fait la liste des nouvelles AVP définies dans cette application Diameter SIP. Les abréviations suivantes sont utilisées dans la colonne Type de données :
DURI : URI Diameter
E : Énuméré
G : Groupé
OS : Chaîne d'octets
UTF8S : Chaîne UTF8
U32 : non signé 32 bits

Nom d'attribut	Code d'AVP	Référence	Type de données
Informations de comptabilité SIP	368	paragraphe 9.1	G
URI de serveur de comptabilité SIP	369	paragraphe 9.1.1	DURI |
URI de serveur de contrôle de crédit SIP	370	paragraphe 9.1.2	DURI|
URI de serveur SIP	371	paragraphe 9.2	UTF8S
Capacités de serveur SIP	372	paragraphe 9.3	G
Capacité SIP obligatoire	373	paragraphe 9.3.1	U32
Capacité SIP facultative	374	paragraphe 9.3.2	U32
Type d'allocation de serveur SIP	375	paragraphe 9.4	E
Élément de données d'authentification SIP	376	paragraphe 9.5	G
Schéma d'authentification SIP	377	paragraphe 9.5.1	E
Numéro d'élément SIP	378	paragraphe 9.5.2	U32
Authentification SIP	379	paragraphe 9.5.3	G
Autorisation SIP	380	paragraphe 9.5.4	G
Informations d'authentification SIP	381	paragraphe 9.5.5	G
Nombre d'léments d'authentification SIP	382	paragraphe 9.6	U32
Cause de désenregistrement SIP	383	paragraphe 9.7	G
Code de cause SIP	384	paragraphe 9.7.1	E
Informations de cause SIP	385	paragraphe 9.7.2	UTF8S
Identifiant de réseau SIP visité	386	paragraphe 9.9	UTF8S
Type d'autorisation d'utilisateur SIP	387	paragraphe 9.10	E
Type de données SIP pris en charge par l'utilisateur	388	paragraphe 9.11	UTF8S
Données d'utilisateur SIP	389	paragraphe 9.12	G|
Type de données d'utilisateur SIP	390	paragraphe 9.12.1	UTF8S
Contenu des données d'utilisateur SIP	391	paragraphe 9.12.2	OS|
Données d'utilisateur SIP déjà disponibles	392	paragraphe 9.13	E
Méthode SIP	393	paragraphe 9.14	UTF8S

Tableau 2 : AVP définies

Le Tableau 3 étend le tableau des AVP inclus au paragraphe 4.5 de la [RFC3588]. Le tableau indique les AVP Diameter définis dans cette application Diameter SIP, leurs valeurs de fanions possibles, et si l'AVP peut être chiffrée. Les acronymes 'M', 'P', et 'V' se réfèrent aux fanions d'AVP dont la sémantique est décrite au paragraphe 4.1 de la [RFC6733]. La valeur de la colonne "Chfr" est aussi décrite dans la [RFC3588].

Nom d'attribut	NE DOIT PAS	NE PEUT PAS	DOIT	Chfr
Informations de comptabilité SIP	M	P	V	N
URI de serveur de comptabilité SIP	M	P	V	N
URI de serveur de contrôle de crédit SIP	M	P	V	N
URI de serveur SIP	M	P	V	N
Capacités de serveur SIP	M	P	V	N
Capacité SIP obligatoire	M	P	V	N
Capacité SIP facultative	M	P	V	N
Type d'allocation de serveur SIP	M	P	V	N
Élément de données d'authentification SIP	M	P	V	N
Schéma d'authentification SIP	M	P	V	N
Numéro d'élément SIP	M	P	V	N
Authentification SIP	M	P	V	N
Autorisation SIP	M	P	V	N
Informations d'authentification SIP	M	P	V	N
Nombre d'éléments d'authentification SIP	M	P	V	N
Cause de désenregistrement SIP	M	P	V	N
Code de cause SIP	M	P	V	N
Informations de cause SIP	M	P	V	N
Identifiant de réseau SIP visité	M	P	V	N
Type d'autorisation d'utilisateur SIP	M	P	V	N
Type de données SIP pris en charge par l'utilisateur	M	P	V	N
Données d'utilisateur SIP	M	P	V	N
Type de données d'utilisateur SIP	M	P	V	N
Contenu des données d'utilisateur SIP	M	P	V	N

Données d'utilisateur SIP déjà disponibles	M	P	V	N
Méthode SIP	M	P	V	N

Table 3 : Sommaire des fanions des nouvelles AVP

9.1 AVP Informations de comptabilité SIP

L'AVP Informations de comptabilité SIP (code d'AVP 368) est de type Groupé, et contient les adresses Diameter des nœuds qui sont capables de collecter les informations comptables.

L'AVP Informations de comptabilité SIP est définie comme suit (selon la définition d'AVP Groupé de la [RFC3588]):

Informations de comptabilité SIP ::= < En-tête d'AVP : 368 >
* [URI de serveur de comptabilité SIP]
* [URI de serveur de contrôle de crédit SIP]
* [AVP]

9.1.1 AVP URI de serveur de comptabilité SIP

L'AVP URI de serveur de comptabilité SIP (code d'AVP 369) est du type URI Diameter. Cette AVP contient l'adresse d'un serveur Diameter qui est capable de recevoir des informations de session SIP relatives à la comptabilité.

9.1.2 AVP URI de serveur de contrôle de crédit SIP

L'AVP URI de serveur de contrôle de crédit SIP (code d'AVP 370) est du type URI Diameter. Cette AVP contient l'adresse d'un serveur Diameter qui est capable d'autoriser l'usage du contrôle de crédit en temps réel. L'application Contrôle de crédit Diameter [RFC4006] peut être utilisée pour cela.

9.2 AVP URI de serveur SIP

L'AVP URI de serveur SIP (code d'AVP 371) est du type Chaîne UTF8. Cette AVP contient un URI SIP ou SIPS (comme défini dans la [RFC3261]) qui identifie un serveur SIP.

9.3 AVP Capacités de serveur SIP

L'AVP Capacités de serveur SIP (code d'AVP 372) est du type Groupé. Diameter indique dans cette AVP les exigences pour une capacité SIP particulière, afin que le client Diameter (serveur SIP) soit capable de choisir un autre serveur SIP approprié pour desservir l'utilisateur.

L'AVP Capacités de serveur SIP permet à un client Diameter (serveur SIP) de choisir un autre serveur SIP pour déclencher ou exécuter des services pour l'utilisateur. Un utilisateur peut avoir activé certains services qui exigent la mise en œuvre de certaines capacités dans le serveur SIP qui déclenchent ou exécutent ces services. Par exemple, le serveur SIP qui déclenche ou exécute des services pour cet utilisateur peut avoir besoin de mettre en œuvre des servlets SIP [JSR-000116], le langage de traitement d'appel (CPL, *Call Processing Language*) [RFC3880], ou toute autre sorte de capacité. Ou peut-être que l'utilisateur appartient à un groupe d'utilisateurs privilégiés qui a un certain accord de qualité de service stricte qui exige un serveur SIP rapide. Les capacités requises ou recommandées pour un certain utilisateur sont convoyées dans l'AVP Capacités de serveur SIP. Quand il les reçoit, le client Diameter (serveur SIP) qui fait le choix du serveur SIP doit avoir les moyens de trouver les serveurs SIP disponibles qui satisfont aux capacités requises ou facultatives. De tel moyens sortent du domaine d'application de la présente spécification.

Noter que l'AVP Capacités de serveur SIP aide le client Diameter (serveur SIP) à produire un sous ensemble de tous les serveurs SIP disponibles pour être alloués à l'utilisateur dans le domaine de rattachement ; c'est le sous ensemble qui se conforme aux exigences de capacités par utilisateur. Normalement, ce sous ensemble va être formé de plus d'un seul serveur SIP, de sorte qu'une fois que le sous ensemble de ces serveurs SIP est identifié, il est possible que plusieurs instances de ces serveurs SIP existent, et dans ce cas, le client Diameter (serveur SIP) devrait choisir un serveur SIP particulier pour exécuter et déclencher les services pour cet utilisateur. Il est estimé qu'à ce point, le serveur SIP (client Diameter) va suivre les procédures de la [RFC3263] pour allouer un serveur SIP à l'utilisateur.

L'AVP Capacités de serveur SIP est défini comme suit (selon la définition d'AVP Groupé de la [RFC3588]) :

Capacités de serveur SIP ::= < En-tête d'AVP : 372 >
* [Capacité SIP obligatoires]
* [Capacité SIP facultatives]
* [URI de serveur SIP]
* [AVP]

9.3.1 AVP Capacités SIP obligatoires

L'AVP Capacités SIP obligatoires (code d'AVP 373) est du type Non signé32. La valeur représente une certaine capacité (ou ensemble de capacités) qui doit être satisfaite par le serveur SIP alloué à l'utilisateur.

La sémantique des différentes valeurs n'est pas normalisée, car c'est l'affaire du réseau administratif d'allouer sa propre sémantique dans son propre réseau. Chaque valeur doit représenter une seule capacité dans le réseau administratif.

9.3.2 AVP Capacités SIP facultatives

L'AVP Capacités SIP facultatives (code d'AVP 374) est du type Non signé32. La valeur représente une certaine capacité (ou ensemble de capacités) qui, facultativement, peut être satisfaite par le serveur SIP alloué à l'utilisateur.

La sémantique des différentes valeurs n'est pas normalisée, car c'est l'affaire du réseau administratif d'allouer sa propre sémantique dans son propre réseau. Chaque valeur doit représenter une seule capacité dans le réseau administratif.

9.4 AVP Type d'allocation de serveur SIP

L'AVP Type d'allocation de serveur SIP (code d'AVP 375) est de type Énuméré et indique le type de mise à jour de serveur effectuée dans une opération Diameter Demande d'allocation de serveur (SAR). Les valeurs suivantes sont définies :

- PAS_D'ALLOCATION (0) : le client Diameter utilise cette valeur pour demander le profil d'utilisateur d'une AOR SIP sans affecter l'état d'enregistrement de cette identité.

- ENREGISTREMENT (1) : premier enregistrement SIP d'une AOR SIP.

- RE_ENREGISTREMENT (2) : enregistrement SIP suivant d'une AOR SIP.

- UTILISATEUR_NON_ENREGISTRÉ (3) : le serveur SIP a reçu une demande SIP (par exemple, SIP INVITE) adressée à une AOR SIP qui n'est pas enregistrée.

- FIN_DE_TEMPORISATION_DÉSENREGISTREMENT (4) : la temporisation d'enregistrement SIP d'une identité a expiré.

- DÉSENREGISTREMENT_D'UTILISATEUR (5) : le serveur SIP a reçu une demande de désenregistrer une AOR SIP.

- FIN_DE_TEMPORISATION_DÉSENREGISTREMENT_MÉMORISER_NOM_SERVEUR (6) : le temporisateur d'enregistrement SIP d'une identité a expiré. Le serveur SIP garde mémorisées les données de l'utilisateur et demande au serveur Diameter de mémoriser l'adresse du serveur SIP.

- DÉSENREGISTREMENT_D'UTILISATEUR_MÉMORISER_NOM_SERVEUR (7) : le serveur SIP a reçu une demande de désenregistrement initiée par l'utilisateur. Le serveur SIP garde mémorisées les données de l'utilisateur et demande au serveur Diameter de mémoriser l'adresse du serveur SIP.

  DÉSENREGISTREMENT_ADMINISTRATIF (8) : le serveur SIP, pour des raisons administratives, a désenregistré une AOR SIP.

- ÉCHEC_D'AUTHENTIFICATION (9) : l'authentification d'un utilisateur a échoué.

- FIN_DE_TEMPORISATION_D'AUTHENTIFICATION (10) : le temporisateur d'authentification a expiré.

o DÉSENREGISTREMENT_TROP_DE_DONNÉES (11) : le serveur SIP a demandé des informations de profil d'utilisateur au serveur Diameter et a reçu un volume de données supérieur à ce qu'il peut accepter.

9.5 AVP Éléments de données d'authentification SIP

L'AVP Élément de données d'authentification SIP (code d'AVP 376) est du type Groupé et contient les informations d'authentification et/ou d'autorisation relatives à un utilisateur.

Quand le serveur Diameter utilise l'AVP groupée Élément de données d'authentification SIP pour inclure une AVP Authentification SIP, le serveur Diameter DOIT envoyer un maximum d'un élément de données d'authentification (par exemple, dans le cas où la demande SIP contenait plusieurs accréditifs). La Section 11 contient une discussion détaillée et normative du cas où une demande SIP contient plusieurs accréditifs.

L'AVP Élément de données d'authentification SIP est définie comme suit (selon la définition d'AVP Groupé de la [RFC3588]) :

```
Élément de données d'authentification SIP ::= < En-tête d'AVP : 376 >
                    { Schéma d'authentification SIP }
                    [ Numéro d'élément SIP ]
                    [ Authentification SIP ]
                    [ Autorisation SIP ]
                    [ Informations d'authentification SIP ]
                   * [ AVP ]
```

9.5.1 AVP Schéma d'authentification SIP

L'AVP Schéma d'authentification SIP (code d'AVP 377) est du type Énuméré et indique le schéma d'authentification utilisé dans les services d'authentification de SIP. La RFC 2617 identifie cette valeur comme "auth-scheme" (voir le paragraphe 1.2 de la [RFC2617]). La seule valeur acuellement définie est :

o RÉSUMÉ (0) pour indiquer l'authentification HTTP par résumé comme spécifé au paragraphe 3.2.1 de la [RFC2617]. Des travaux dérivés sont aussi considérés comme schéma d'authentification par résumé, tant que le "auth-scheme" est identifié comme résumé dans les en-têtes SIP portant l'authentification HTTP. Cela inclut, par exemple, l'authentification HTTP par résumé utilisant AKA [RFC3310].

Chaque directive (paramètre) HTTP Digest est transportée dans une AVP correspondante, dont le nom suit le schéma Digest-*. Les AVP Digest-* sont des attributs RADIUS importés de l'espace de noms d'extension RADIUS pour l'authentification par résumé [RFC4590] qui permet une transition en douceur entre les applications RADIUS et Diameter qui prennent en charge SIP. L'application Diameter SIP va une étape plus loin en groupant les AVP Digest-* dans les AVP groupées Authentification SIP, Autorisation SIP, et Informations d'authentfiication SIP qui correspondent aux champs d'en-tête SIP WWW-Authenticate/Proxy-Authentication, Authorization/Proxy-Authorization, et Authentication-Info, respectivement.

Note : Du fait que l'authentification HTTP par résumé [RFC2617] est le seul mécanisme d'authentification obligatoire dans SIP, le présent mémoire prend seulement en charge l'authentification HTTP par résumé et les travaux dérivés comme l'authentification HTTP par résumé utilisant AKA [RFC3310]. Des extensions au présent mémoire pourraient enregistrer de nouvelles valeurs et de nouvelles AVP pour fournir la prise en charge d'autres schémas d'authentification ou des extensions de l'authentification HTTP par résumé.

Note : Bien que la [RFC2617] définisse les schémas Basic et Digest pour l'authentification des demandes HTTP, la [RFC3261] importe seulement HTTP Digest comme mécanisme pour fournir l'authentification dans SIP.

Du fait des exigences de la syntaxe, l'authentification HTTP par résumé doit échapper les caractères guillemets dans les contenus des directives HTTP Digest. Quand on traduit les directives en AVP Digest-*, le client ou serveur Diameter supprime les guillemets lorsque ils sont présents, comme exigé par la syntaxe des attributs Digest-* définie dans "Extension RADIUS pour l'authentification par résumé" [RFC4590].

9.5.2 AVP Numéro d'élément SIP

L'AVP Numéro d'élément SIP (code d'AVP 378) est du type Non signé32 et est incluse dans une AVP groupée Élément de données d'authentification SIP dans les circonstances où il y a plusieurs occurrences d'AVP Élément de données d'authentification SIP et que l'ordre de traitement est important. L'AVP indique l'ordre dans lequel les éléments de données d'authentification SIP groupés devraient être traités. Les valeurs inférieures de l'AVP Numéro d'élément SIP indiquent que tout l'élément de données d'authentification SIP DEVRAIT être traité avant les autres AVP Élément de données d'authentification SIP qui contiennent des valeurs supérieures dans l'AVP Numéro d'élément SIP.

9.5.3 AVP Authentification SIP

L'AVP Authentification SIP (code d'AVP 379) est de type Groupé et contient une reconstruction des champs d'en-tête SIP WWW-Authenticate ou Proxy-Authentication spécifiés dans la [RFC2617] pour le schéma d'authentification HTTP par résumé. De plus, l'AVP peut inclure une AVP Digest-HA1 qui contient H(A1) (comme défini dans la [RFC2617]). H(A1) permet au client Diameter de créer une réponse attendue et de la comparer à la réponse Digest reçue de l'UA SIP.

L'AVP Authentification SIP est définie comme suit (selon la définition d'AVP Groupé de la [RFC3588]) :

```
Authentification SIP ::= < En-tête d'AVP : 379 >
                         { Digest-Realm }
                         { Digest-Nonce }
                         [ Digest-Domain ]
                         [ Digest-Opaque ]
                         [ Digest-Stale ]
                         [ Digest-Algorithm ]
                         [ Digest-Qop ]
                         [ Digest-HA1]
                        * [ Digest-Auth-Param ]
                        * [ AVP ]
```

9.5.4 AVP Autorisation SIP

L'AVP Autorisation SIP (code d'AVP 380) est de type Groupé et contient une reconstruction des champs d'en-tête SIP Autorisation ou Autorisation de mandataire spécifiés dans la [RFC2617] pour le schéma d'authentification HTTP par résumé.

L'AVP Autorisation SIP est définie comme suit (selon la définition d'AVP Groupé de la [RFC3588]) :

```
Autorisation SIP ::= < En-tête d'AVP : 380 >
                         { Digest-Username }
                         { Digest-Realm }
                         { Digest-Nonce }
                         { Digest-URI }
                         { Digest-Response }
                         [ Digest-Algorithm ]
                         [ Digest-CNonce ]
                         [ Digest-Opaque ]
                         [ Digest-Qop ]
                         [ Digest-Nonce-Count ]
                         [ Digest-Method]
                         [ Digest-Entity-Body-Hash ]
                        * [ Digest-Auth-Param ]
                        * [ AVP ]
```

9.5.5 AVP Informations d'authentification SIP

L'AVP Informations d'authentification SIP (code d'AVP 381) est de type Groupé et contient une reconstruction de l'en-tête SIP Informations d'authentification spécifié dans la [RFC2617] pour le schéma d'authentification HTTP par résumé.

L'AVP Informations d'authentification SIP est définie comme suit (selon la définition d'AVP Groupé de la [RFC3588]) :

```
Informations d'authentification SIP ::= < En-tête d'AVP : 381 >
                                        [ Digest-Nextnonce ]
                                        [ Digest-Qop ]
                                        [ Digest-Response-Auth ]
                                        [ Digest-CNonce ]
                                        [ Digest-Nonce-Count ]
                                       * [ AVP ]
```

Noter que, dans certains cas, l'AVP Digest-Response-Auth ne peut pas être calculée au serveur Diameter, mais doit être calculée au client Diameter (serveur SIP). Par exemple, si la valeur du paramètre Qualité de protection (qop) dans Digest est réglée à "auth-int", alors le paramètre response-digest (valeur de paramètre rspauth dans Digest) est calculé avec le hachage du corps de la réponse SIP, qui n'est pas disponible au serveur Diameter. Dans ce cas, le client Diameter (serveur SIP) doit calculer le response-digest une fois que le corps de la réponse SIP est calculé.

Donc, une valeur de "auth-int" dans l'AVP Digest-Qop de l'AVP Informations d'authentification SIP indique que le client Diameter (serveur SIP) DOIT calculer la valeur du paramètre Digest "rspauth" au client Diameter (serveur SIP).

9.5.6 AVP de résumé

Les AVP suivantes sont des attributs RADIUS définis dans les Extension RADIUS pour l'authentification par résumé [RFC4590] et importés par la présente spécification : Digest-AKA-Auts, Digest-Algorithm, Digest-Auth-Param, Digest-CNonce, Digest-Domain, Digest-Entity-Body-Hash, Digest-HA1, Digest-Method, Digest-Nextnonce, Digest-Nonce, Digest-Nonce-Count, Digest-Opaque, Digest-Qop, Digest-Realm, Digest-Response, Digest-Response-Auth, Digest-URI, Digest-Username, et Digest-Stale.

9.5.6.1 Considérations sur les AVP Digest-HA1

L'AVP Digest-HA1 contient la valeur, pré-calculée au serveur Diameter, de H(A1) comme défini dans la [RFC2617]. Le client Diameter peut utiliser H(A1) pour calculer la réponse Digest attendue, conformément à ce défi. Si l'UA SIP est en possession des accréditifs, la réponse calculée attendue et la réponse envoyée de l'UA SIP vont correspondre. Le serveur Diameter PEUT inclure cette AVP pour permettre et aider le serveur SIP à authentifier l'UA SIP.

Ce scénario n'est pas applicable quand le serveur Diameter est configuré à utiliser un algorithme de session MD5 (MD5-sess) parce que le serveur Diameter exige le nom occasionnel du client pour calculer le H(A1) avant de l'envoyer au client Diameter, et le nom occasionnel du client pourrait n'être pas disponible quand le calcul de H(A1) est fait. Donc, si l'authentification finale est déléguée au client Diameter, il est RECOMMANDÉ de configurer le serveur Diameter à utiliser des algorithmes différents de MD5-sess dans HTTP Digest.

Il appartient au serveur Diameter d'inclure une AVP Digest-HA1. Le serveur Diameter calcule le Digest H(A1) avec le nom d'utilisateur, le mot de passe, et le domaine (et nonce et cnonce, si applicable) en entrées, et il place le résultat dans la valeur de l'AVP Digest-HA1. Pour plus de détails sur le calcul de A1, voir au paragraphe 3.2.2.2 de la [RFC2617]. Le client Diameter peut calculer la réponse de Digest attendue avec H(A1) comme entrée, comme décrit au paragraphe 3.2.2 de la [RFC2617].

La Section 11 donne des détails normatifs sur l'usage de l'AVP Digest-HA1.

9.5.6.2 Considérations sur l'AVP Digest-Entity-Body-Hash

L'AVP Digest-Entity-Body-Hash *(hachage de corps d'entité de résumé)* contient un hachage du corps d'entité contenu dans le message SIP. Ce hachage est exigé par HTTP Digest avec la qualité de protection réglée à "auth-int". Les clients Diameter DOIVENT utiliser cette AVP pour transporter le hachage du corps d'entité quand HTTP Digest est le mécanisme d'authentification et que le serveur Diameter exige la vérification de l'intégrité du corps d'entité (par exemple, le paramètre qop réglé à "auth-int").

Les précisions décrites au paragraphe 22.4 de la [RFC3261] sur le hachage de corps d'entité vides s'appliquent à l'AVP Digest-Entity-Body-Hash.

9.5.6.3 Considérations sur l'AVP Digest-Auth-Param

L'AVP Digest-Auth-Param est le mécanisme par lequel le client Diameter et le serveur Diameter peuvent échanger de possibles paramètres d'extension contenus dans les en-têtes Digest qui ne sont pas compris par le client Diameter ou pour lesquels il n'y a pas d'AVP autonomes correspondantes. À la différence des AVP Digest-* mentionnés précédemment, Digest-Auth-Param contient non seulement la valeur, mais aussi le nom du paramètre, car il est inconnu du client Diameter. Le nœud Diameter DOIT insérer une combinaison paramètre/valeur Digest par valeur d'AVP. Si l'en-tête Digest contient plusieurs paramètres inconnus, alors la mise en œuvre Diameter DOIT répéter cette AVP et chaque instance DOIT contenir une combinaison paramètre/valeur Digest différente. Cette AVP correspond au paramètre "auth-param" défini au paragraphe 3.2.1 de la [RFC2617].

Exemple : supposons que le serveur Diameter veuille que le serveur SIP envoie un paramètre "foo" avec la valeur réglée à "bar", afin que le serveur SIP envoie cette combination dans un champ d'en-tête SIP WWW-Authenticate. Le serveur Diameter construit une AVP groupée Authentification SIP qui contient un Digest-Auth-Param dont la valeur est réglée à foo="bar". Alors le serveur SIP crée le champ d'en-tête WWW-Authenticate avec tous les paramètres de résumé (reçus dans les AVP Digest-*) et ajoute le paramètre foo="bar" à ce champ d'en-tête.

9.6 AVP Nombre d'léments d'authentification SIP

L'AVP Nombre d'éléments d'authentification SIP (code d'AVP 382) est de type Non signé32 et indique le nombre d'accréditifs d'authentification et/ou autorisation que le serveur Diameter a inclus dans un message Diameter.

Quand l'AVP est présente dans une demande, elle indique le nombre d'éléments de données d'authentification SIP que le client Diameter demande. Cela peut être utilisé, par exemple, quand le serveur SIP demande plusieurs accréditifs d'authentification précalculés. Dans le message de réponse, l'AVP Nombre d'éléments d'authentification SIP indique le nombre réel d'éléments que le serveur Diameter a inclus.

9.7 AVP Cause de désenregistrement SIP

L'AVP Cause de désenregistrement SIP (code d'AVP 383) est du type Groupé et indique la raison d'une opération de désenregistrement.

L'AVP Cause de désenregistrement SIP est définie comme suit (selon la définition d'AVP Groupé de la [RFC3588]) :

```
Cause de désenregistrement SIP ::= < En-tête d'AVP : 383 >
                                   { Code de cause SIP }
                                   [ Informations de cause SIP ]
                                  * [ AVP ]
```

9.7.1 AVP code de cause SIP

L'AVP Code de cause SIP (code d'AVP 384) est du type Énuméré et définit la raison du désenregistrement initié par le réseau. Les valeurs définies sont les suivantes :

- o TERMINAISON_PERMANENTE (0)
- o NOUVEAU_SERVEUR_SIP_ALLOUÉ (1)
- o CHANGEMENT_DE_SERVEUR_SIP (2)
- o SUPPRIMER_LE_SERVEUR_SIP (3)

9.7.2 AVP Informations de cause SIP

L'AVP Informations de cause SIP (code d'AVP 385) est du type Cghaîne UTF8 et contient des informations textuelles qui peuvent être rendues à l'utilisateur, sur la raison d'un désenregistrement.

9.8 AVP SIP-AOR

L'AVP SIP-AOR est un attribut RADIUS importé de l'espace de noms des extensions à RADIUS pour l'authentification par résumé [RFC4590], qui permet une transition en douceur entre les applications RADIUS et Diameter qui prennent en charge SIP. L'AVP SIP-AOR porte l'URI de l'utilisateur prévu relatif à la demande SIP (dont la localisation dans SIP peut

varier selon la demande SIP réelle et de si le serveur SIP agit sur Diameter du fait de demandes générées ou terminées dans SIP).

Le client Diameter (serveur SIP) utilise la valeur trouvée dans un URI de demande SIP ou une valeur de champ d'en-tête de la demande SIP de construire l'AVP SIP-AOR. Le choix d'un URI de demande ou d'un champ d'en-tête particulier pour créer la valeur de l'AVP SIP-AOR dépend de la sémantique du message SIP et de si le serveur SIP agit pour générer ou terminer les demandes. Par exemple, quand le serveur SIP reçoit une demande INVITE adressée à l'utilisateur desservi (par exemple, le serveur SIP reçoit une demande de terminaison de SIP) il transpose l'URI de demande SIP de la demande SIP en cette AVP. Cependant, quand le serveur SIP reçoit une demande INVITE générée par l'utilisateur desservi, il peut transposer les valeurs de P-Asserted-Identity ou du champ d'en-tête From en cette AVP. Si le serveur SIP agit comme registraire SIP, il transpose alors le champ d'en-tête To de la demande REGISTER en l'AVP SIP-AOR.

9.9 AVP Identifiant de réseau visité SIP

L'AVP Identifiant de réseau SIP visité (code d'AVP 386) est du type Chaîne UTF8. Cette AVP contient un identifiant qui aide le réseau de rattachement à identifier le réseau visité (par exemple, le nom de domaine du réseau visité) afin d'autoriser l'itinérance à ce réseau visité.

9.10 AVP Type d'autorisation d'utilisateur SIP

L'AVP Type d'autorisation d'utilisateur SIP (code d'AVP 387) est du type Énuméré et indique le type d'autorisation d'utilisateur effectuée dans une opération Autorisation d'utilisateur, c'est-à-dire, la commande Diameter Demande d'autorisation d'utilisateur (UAR, *User-Authorization-Request*). Les valeurs suivantes sont définies :

- ENREGISTREMENT (0) : cette valeur est utilisée pour l'enregistrement initial ou le réenregistrement. C'est la valeur par défaut.
- DÉSENREGISTREMENT (1) : cette valeur est utilisée pour le désenregistrement.
- ENREGISTREMENT_ET_CAPACITÉS (2) : cette valeur est utilisée pour l'enregistrement initial ou le réenregistrement quand le serveur SIP demande explicitement que le serveur Diameter obtienne des informations de capacités. Ces informations de capacités aident le serveur SIP à allouer un autre serveur SIP pour servir l'utilisateur.

9.11 AVP Type de données d'utilisateur SIP supportées

L'AVP Type de données d'utilisateur pris en charge (code d'AVP 388) est du type Chaîne UTF8 et contient une chaîne qui identifie le type de données d'utilisateur supporté (profil d'utilisateur, voir l'AVP Données d'utilisateur SIP (paragraphe 9.12)) dans le nœud. L'AVP peut être répétée, si le serveur SIP supporte plusieurs types de données d'utilisateur. En cas de répétition, le client Diameter devrait ordonner les différentes instances de cette AVP conformément à ses préférences.

Quand le client Diameter insère cette AVP dans un message SAR, cela permet au client Diameter de donner une indication au serveur Diameter sur les types de données d'utilisateur supportés par le serveur SIP. Le serveur Diameter, après inspection de ces AVP, va retourner une AVP Données d'utilisateur SIP (paragraphe 9.12) convenable du type indiqué dans l'AVP Type de données d'utilisateur SIP (paragraphe 9.12.1).

9.12 AVP Données d'utilisateur SIP

L'AVP Données d'utilisateur SIP (code d'AVP 389) est du type Groupé. Cette AVP permet au serveur Diameter de transporter des données spécifiques de l'utilisateur, comme un profil d'utilisateur, au serveur SIP (dans le client Diameter). Le serveur Diameter choisit un type de données d'utilisateur qui est compris par le serveur SIP dans le client Diameter, et a été indiqué dans une AVP Type de données d'utilisateur pris en charge. Dans le cas où le client Diameter a indiqué la prise en charge de plusieurs types de données d'utilisateur, le serveur Diameter DEVRAIT choisir le premier type supporté par le client.

L'AVP groupée Données d'utilisateur SIP contient une AVP Type de données d'utilisateur SIP qui indique le type de données d'utilisateur inclus dans l'AVP Contenu de données d'utilisateur SIP.

L'AVP Données d'utilisateur SIP est définie comme suit (selon la définition d'AVP Groupé de la [RFC3588]) :

Données d'utilisateur SIP ::= < En-tête d'AVP : 389 >

```
  { Type de données d'utilisateur SIP }
  { Contenu de données d'utilisateur SIP }
* [ AVP ]
```

9.12.1 AVP Type de données d'utilisateur SIP

L'AVP Type de données d'utilisateur SIP (code d'AVP 390) est du type Chaîne UTF8 et contient une chaîne qui identifie le type de données d'utilisateur inclus dans l'AVP Données d'utilisateur SIP (paragraphe 9.12).

Le présent document ne spécifie pas de convention pour caractériser le type de données d'utilisateur contenu dans l'AVP Données d'utilisateur SIP (paragraphe 9.12). Il est estimé que dans la plupart des cas, cette caractéristique va être utilisée dans des environnements contrôlés par un administrateur de réseau qui peut configurer le client et le serveur à allouer le même type de valeur au client et au serveur. Il est aussi RECOMMANDÉ que les organisations qui développent leur propre profil d'AVP Données d'utilisateur SIP (paragraphe 9.12) allouent un type sur la base de leur nom DNS canonique. Par exemple, l'organisation "exemple.com" peut définir plusieurs types de données d'utilisateur SIP et allouer les types "type1.dsa.exemple.com", "type2.dsa.exemple.com", et ainsi de suite. Cette convention évitera des conflits d'allocation de types d'AVP Données d'utilisateur SIP (paragraphe 9.12).

9.12.2 AVP Contenu des données d'utilisateur SIP

L'AVP Contenu de données d'utilisateur SIP (code d'AVP 391) est du type Chaîne d'octets. Les homologues Diameter n'ont pas besoin de comprendre la valeur de cette AVP.

L'AVP contient les données de profil d'utilisateur requises pour qu'un serveur SIP fournisse le service à l'utilisateur.

9.13 AVP Données d'utilisateur SIP déjà disponibles

L'AVP Données d'utilisateur SIP déjà disponibles (code d'AVP 392) est du type Énuméré et donne une indication au serveur Diameter sur si le client Diameter (serveur SIP) a déjà reçu la portion du profil d'utilisateur nécessaire afin de servir l'utilisateur. Les valeurs suivantes sont définies :

- DONNÉES_D'UTILISATEUR_NON_DISPONIBLES (0) : le client Diameter (serveur SIP) n'a pas les données dont il a besoin pour servir l'utilisateur.

- DONNÉE_D'UTILISATEUR_DÉJA_DISPONIBLES (1) : le client Diameter (serveur SIP) a déjà reçu les données dont il a besoin pour servir l'utilisateur.

9.14 AVP Méthode SIP

L'AVP Méthode SIP (code d'AVP 393) est du type Chaîne UTF8 et contient la méthode de la demande SIP qui a déclenché le message Diameter. Le serveur Diameter DOIT utiliser cette AVP seulement pour l'autorisation des demandes SIP, et NE DOIT PAS l'utiliser pour calculer l'authentification par résumé. Pour calculer l'authentification par résumé, le serveur Diameter DOIT utiliser à la place l'AVP Méthode de résumé.

10. Nouvelles valeurs pour les AVP existants

Cette Section définit les nouvelles valeurs que l'application Diameter SIP étend aux AVP déjà existantes.

10.1 Extension aux valeurs d'AVP Code de résultat

L'AVP Code de résultat est déjà définie dans la [RFC3588]. En plus des valeurs déjà définies dans la [RFC3588], l'application Diameter SIP définit les nouvelles valeurs d'AVP Code de résultat suivantes :

10.1.1 Valeurs d'AVP de code de résultat de succès

Un homologue Diameter utilise des valeurs d'AVP Code de résultat qui entrent dans la catégorie succès pour informer l'homologue distant qu'une demande s'est terminée par un succès.

- PREMIER_ENREGISTREMENT_DIAMETER 2003 : L'utilisateur n'était pas enregistré antérieurement. Le serveur Diameter a maintenant autorisé l'enregistrement.

- ENREGISTREMENT_DIAMETER_SUIVANT 2004 : L'utilisateur est déjà enregistré. Le serveur Diameter a maintenant autorisé le réenregistrement.

- SERVICE_DIAMETER_NON_ENREGISTRÉ 2005 : L'utilisateur n'est pas enregistré actuellement, mais le service demandé peut quand même être accordé à l'utilisateur.

- DIAMETER_RÉUSSI_NOM_DE_SERVEUR_NON_MÉMORISÉ 2006 : l'opération de demande a été traitée avec succès. Le serveur Diameter ne garde pas d'enregistrement de l'adresse du serveur SIP alloué à l'utilisateur.

- CHOIX_DE_SERVEUR_DIAMETER 2007 : le serveur Diameter a autorisé l'enregistrement. Un serveur SIP a déjà été alloué à l'utilisateur, mais il peut être nécessaire de choisir un nouveau serveur SIP pour l'utilisateur.

- DIAMETER_RÉUSSI_AUTH_ENVOYÉE_SERVEUR_NON_MÉMORISÉ 2008 : l'opération demandée a été exécutée avec succès. Le serveur Diameter envoie un certain nombre d'accréditifs d'authentification dans le message de réponse. Le serveur Diameter ne garde pas d'enregistrement du serveur SIP.

10.1.2 Valeurs d'AVP de code de résultat de défaillance transitoire

Un homologue Diameter utilise des valeurs d'AVP Code de résultat qui entrent dans la catégorie des défaillances transitoires pour informer l'homologue distant qu'une demande pourrait n'être pas satisfaite au moment où elle a été reçue, mais qu'elle PEUT être satisfaite par l'homologue Diameter à l'avenir.

- NOM_D'UTILISATEUR_DIAMETER_EXIGÉ 4013 : la demande Diameter ne contenait pas d'AVP Nom d'utilisateur, qui est exigé pour achever la transaction. L'homologue Diameter PEUT inclure une AVP Nom d'utilisateur et tenter à nouveau la demande.

10.1.3 Valeurs d'AVP de code de résultat de défaillance permanente

Un homologue Diameter utilise des valeurs d'AVP Code de résultat qui entrent dans la catégorie de défaillances permanentes pour informer l'homologue distant que la demande a échoué et ne devrait pas être tentée à nouveau.

- ERREUR_DIAMETER_UTILISATEUR_INCONNU 5032 : la valeur d'AVP SIP-AOR n'appartient pas à un utilisateur connu dans ce domaine.

- ERREUR_DIAMETER_IDENTITÉS_NON_CORRESPONDANTES 5033 : La valeur d'une des AVP SIP-AOR n'est pas allouée à l'utilisateur spécifié dans l'AVP Nom d'utilisateur.

- ERREUR_DIAMETER_IDENTITÉ_NON_ENREGISTRÉE 5034 : une interrogation sur des informations de localisation est reçue pour une AOR SIP qui n'a pas été enregistrée avant. L'utilisateur auquel appartient cette identité ne peut pas recevoir de service dans cette situation.

- ERREUR_DIAMETER_ITINÉRANCE_NON_PERMISE 5035 : l'itinérance de l'utilisateur n'est pas permise dans le réseau visité.

- ERREUR_DIAMETER_IDENTITÉ_DÉJA_ENREGISTRÉE 5036 : un serveur a déjà été alloué à l'identité à enregistrer et l'état d'enregistrement ne permet pas qu'il soit outrepassé.

- ERREUR_DIAMETER_SCHÉMA_D'AUTHENTIFICATION_NON_ACCEPTÉ 5037 : le schéma d'authentification indiqué dans une demande d'authentification n'est pas accepté.

- ERREUR_DIAMETER_DE_TYPE_D'ALLOCATION 5038 : l'adresse de serveur SIP envoyée dans la valeur de l'AVP URI de serveur SIP de la commande Diameter SAR est la même que celle actuellement allouée au nom d'utilisateur,

mais l'AVP Type d'allocation de serveur SIP n'est pas permise. Par exemple, l'utilisateur est enregistré et la demande d'allocation de serveur indique l'allocation pour un utilisateur non enregistré.

- ERREUR_DIAMETER_TROP_DE_DONNÉES 5039 : l'homologue Diameter dans le serveur SIP reçoit plus de données qu'il ne peut accepter. Le serveur SIP ne peut pas écraser les données déjà mémorisées.

- ERREUR_DIAMETER_DONNÉES_D'UTILISATEUR_NON_SUPPORTÉES 5040 : le serveur SIP informe le serveur Diameter que les données d'abonnement reçues contienent des informations qui n'ont pas été reconnues ou supportées.

11. Détails d'authentification

L'authentification d'un utilisateur peut survenir par divers mécanismes. Actuellement, l'authentification HTTP par résumé est prise en charge. L'authentification réelle est effectuée dans le serveur SIP ou le serveur Diameter.

Si le serveur Diameter veut assurer que l'authentification aura lieu dans le serveur Diameter (par opposition à une authentification déléguée ayant lieu au serveur SIP) il NE DOIT PAS inclure une AVP Digest-HA1 (au titre de l'AVP groupée Authentification SIP, qui à son tour fait partie de l'AVP Élément de données d'authentification SIP) dans un message MAA. Le serveur Diameter PEUT inclure une AVP précalculée Digest-HA1 dans le message MAA si il veut déléguer l'authentification de l'utilisateur au serveur SIP.

Noter que sur les systèmes où l'agent d'utilisateur SIP utilise aussi l'authentification HTTP par résumé [RFC2617] à l'intérieur de la sécurité de la couche transport (TLS, *Transport Layer Security*) [RFC4346], où seul le serveur mandataire SIP a un certificat, déléguer l'authentification au serveur SIP (en rendant le Digest-HA1 disponible au serveur SIP) pourrait réduire la charge sur le serveur Diameter.

Quand il demande l'authentification, le client Diameter indique dans la valeur de l'AVP Nombre d'éléments d'authentification SIP d'un message Diameter MAR combien d'accréditifs d'authentification sont demandés. Dans le message Diameter MAA, le serveur Diameter PEUT inclure plus d'une AVP Élément de données d'authentification SIP, mais elle n'est utile au client Diameter que si l'AVP Digest-Qop était réglée à "auth-int" (dans le message MAR) et si de futures authentifications vont avoir le même domaine. Quand on inclut plus d'une AVP Élément de données d'authentification SIP, le serveur Diameter DEVRAIT indiquer combien d'instances d'AVP Élément de données d'authentification SIP sont présentes avec l'AVP Nombre d'éléments d'authentification SIP. Ce nombre peut être différent de celui demandé dans le message Diameter MAR. Si plusieurs AVP Élément de données d'authentification SIP sont présentes, et si leur ordre est significatif, le serveur Diameter DOIT inclure une AVP Numéro d'éléments SIP dans chaque groupement pour indiquer l'ordre. L'AVP Schéma d'authentification SIP indique "Digest" et l'AVP Authentification SIP contient des données (normalement un défi d'une certaine sorte) que l'utilisateur peut utiliser pour son authentification. L'AVP groupée Autorisation SIP contient les AVP qui se conforment à la réponse attendue de l'utilisateur.

Si le serveur Diameter effectue l'authentification de l'utilisateur, le message Diameter MAR que le client Diameter envoie au serveur Diameter DOIT inclure tous les accréditifs d'authentification fournis par l'UA SIP (il pourrait y avoir plus d'un accréditif, par exemple, de domaines différents, d'authentification de mandataires, etc.). Chaque accréditif est inséré dans une AVP groupée Autorisation SIP (partie de l'AVP groupée Élément de données d'authentification SIP). Le client Diameter DOIT insérer une AVP Nombre d'éléments d'authentification SIP avec la valeur réglée au nombre d'accréditifs inclus. Si nécessaire, l'AVP Hachage de corps d'entité de résumé va contenir un hachage du corps, nécessaire pour effectuer l'authentification. Si l'authentification est un succès, le message Diameter MAA va contenir une AVP Code de résultat indiquant le succès, et si nécessaire, le serveur Diameter PEUT inclure une ou plusieurs AVP Élément de données d'authentification SIP pour fournir plus d'accréditifs d'authentification au serveur SIP. Si l'authentification est un échec à cause d'accréditifs manquants, le message Diameter MAA va inclure une AVP Élément de données d'authentification SIP avec les AVP Schéma d'authentification SIP et Authentification SIP contenant des données (normalement un défi d'une certaine sorte) que l'utilisateur peut utiliser pour s'authentifier lui-même.

Il y a des situations où une demande SIP traverse plusieurs mandataires, et chacun des mandataires demande à authentifier l'UA SIP. Dans cette situation, c'est un scénario valide qu'une demande SIP reçue à un serveur SIP contienne plusieurs jeux d'accréditifs. La directive "realm" dans HTTP est la clé que le client Diameter peut utiliser pour déterminer quel accréditif est applicable. Aussi, aucun des domaines peut n'intéresser le client Diameter, et dans ce cas, le client Diameter DOIT considérer qu'aucun accréditif (intéressant) n'a été envoyé. Dans tous les cas, un client Diameter DOIT envoyer zéro ou exactement un accréditif au serveur Diameter. Le client Diameter DOIT choisir l'accréditif sur la base de la directive "realm" dans le champ d'en-tête Autorisation/Autorisation de mandataire, et il DOIT correspondre au domaine du client

Diameter.

Il faut noter que les noms occasionnels sont toujours générés dans le serveur Diameter.

12. Migration depuis RADIUS

RADIUS offre la prise en charge de l'authentification HTTP par résumé dans les extensions à RADIUS pour l'authentification par résumé [RFC4590]. Un certain nombre d'AVP (les AVP Digest-*) de cette application Diameter SIP sont importées de l'espace de noms des attributs RADIUS, donc rendant douce la migration de RADIUS à Diameter.

Noter que les extensions à RADIUS pour l'authentification par résumé [RFC4590] fourissent une portée plus limitée que cette application Diameter SIP. Précisément, les extensions à RADIUS pour l'authentification par résumé fournissent simplement la prise en charge de l'authentification HTTP par résumé, tandis que l'application Diameter SIP fournit la prise en charge de la localisation de l'utilisateur, le téléchargement et la mise à jour du profil, etc.

Les paragraphes qui suivent discutent de plusieurs configurations dans lesquelles une passerelle traduit RADIUS en Diameter et vice versa.

12.1 Passerelle du client RADIUS à serveur Diameter

La passerelle transpose les messages Demande d'accès en demandes MAR. Si un message RADIUS Demande d'accès contient au moins un attribut Digest-*, la passerelle transpose tous les attributs Digest-* en les AVP d'une AVP Diameter Autorisation SIP, construit un message MAR, et l'envoie au serveur Diameter. Si le message RADIUS Demande d'accès ne contient aucun attribut Digest-*, alors le client RADIUS ne veut pas appliquer l'authentification HTTP par résumé, et dans ce cas, les actions à la passerelle sortent du domaine d'application de ce document.

Le serveur Diameter répond par un message MAA. Si le message MAA contient une AVP Code de résultat réglée à la valeur AUTH_DIAMETER_MULTI_TOURS et contient des paramètres de défi dans une AVP Authentification SIP, alors la passerelle traduit les AVP de l'AVP Authentification SIP et met les attributs RADIUS résultants dans un message Défi d'accès. Elle envoie le message Défi d'accès au client RADIUS.

Si le message MAA contient une AVP Informations d'authentification SIP et une AVP Réponse de résumé, la passerelle convertit ces AVP en les attributs RADIUS correspondants et construit un message RADIUS. Si l'AVP Code de résultat est DIAMETER_RÉUSSI, un Accès accepté est envoyé. Dans tous les autres cas, un Accès refusé est envoyé.

12.2 Passerelle du client Diameter au serveur RADIUS

Le client Diameter envoie un message Diameter MAR à la passerelle. Si le message MAR ne contient pas d'AVP Élément de données d'authentification SIP, la passerelle construit un message Demande d'accès et transpose les AVP AOR SIP et Méthode SIP en attributs RADIUS. La passerelle envoie le message Demande d'accès au serveur RADIUS, qui va répondre avec un Défi d'accès. La passerelle crée un message MAA avec une AVP Code de résultat réglée à AUTH_DIAMETER_MULTI_TOURS et transpose les attributs Digest-* en AVP Diameter dans une AVP Authentification SIP. La passerelle envoie le MAA résultant au client Diameter, qui va répondre avec une nouvelle MAR.

La passerelle vérifie les AVP Élément de données d'authentification SIP de ce MAR à la recherche d'une AVP où l'AVP Digest-Realm correspond à la valeur de domaine configuré en local. Elle prend les AVP de cette AVP Élément de données d'authentification SIP, les convertit en les attributs RADIUS correspondants et construit un message RADIUS Demande d'accès. La passerelle envoie le message Demande d'accès au serveur RADIUS. Si le serveur RADIUS répond par un message Accès accepté, la passerelle convertit les attributs RADIUS en AVP Diameter, construit un message MAA avec la valeur AVP Code de résultat réglée à DIAMETER_RÉUSSI et envoie ce message au client Diameter. Si le serveur RADIUS répond par un message Accès refusé, la passerelle convertit les attributs RADIUS en AVP Diameter, construit un message MAA avec une valeur d'AVP Code de résultat réglée à ERREUR_DIAMETER_ DENTITÉS_ NON_CORRESPONDANTES, et envoie ce message au client Diameter.

12.3 Limitations connues

Comme mentionné précédemment, il n'y a pas une correspondance à 100 % entre l'application Diameter SIP et les

extensions RADIUS pour l'authentification par résumé [RFC4590]. En particulier, les extensions RADIUS pour l'authentification par résumé [RFC4590] n'offrent pas de fonction équivalente aux messages Diameter UAR/UAA, SAR/SAA, LIR/LIA, RTR/RTA, et PPR/PPA définis par la présente spécification.

13. Considérations relatives à l'IANA

Le présent document sert de demande d'enregistrement par l'IANA d'un certain nombre d'éléments qui devraient être enregistrés dans le registre des paramètres AAA.

13.1 Identifiant d'application

Le présent document définit un identifiant d'application sur la voie de la normalisation qui entre dans l'espace de noms des adresses d'identifiant d'application défini par le paragraphe 11.3 de la [RFC3588]. Cet identifiant d'application a été enregistré dans le sous registre Identifiants d'application du registre des paramètres AAA avec les données suivantes :

Valeur d'identifiant	Nom	Référence
6	Application Diameter Protocole d'initialisation de session (SIP)	RFC 4740

13.2 Codes de commandes

Le présent document définit de nouvelles commandes standard dont les codes de commande sont à allouer dans l'espace d'adresses de codes de commande standard permanents défini au paragraphe 11;2.1 de la [RFC3588]. Ces codes de commande devraient être enregistrés dans le sous registre Codes de commandes du registre des paramètres AAA.

Le Tableau 1 de la Section 8 contient la liste détaillée des noms et valeurs de codes de commande qui font partie de cette application Diameter.

13.3 Codes d'AVP

Le présent document définit de nouvelles AVP standard, dont les codes d'AVP sont à allouer dans l'espace d'adresse des codes d'AVP défini au paragraphe 11.4 de la [RFC3588]. Ces codes d'AVP ont été enregistrés dans le sous registre Codes d'AVP du registre des paramètres AAA.

Le Tableau 2 de la Section 9 contient la liste détaillée des noms d'AVP et des codes d'AVP qui font partie de cette application Diameter.

13.4 Valeurs supplémentaires pour la valeur d'code d'AVP de résultat

Le présent document définit de nouvelles valeurs standard d'AVP Code de résultat à allouer dans l'espace d'adresse d'AVP Code de résultat défini dans la [RFC3588] paragraphe 14.4.1. La liste de ces valeurs figure dans la section AVP Code de résultat du sous registre Valeurs d'AVP spécifiques du registre des paramètres AAA.

Le paragraphe 10.1.1 fait la liste des nouvelles valeurs d'AVP Code de résultat qui entrent dans la catégorie succès, conformément à la [RFC3588] paragraphe 7.1.2.

Le paragraphe 10.1.2 fait la liste des nouvelles valeurs d'AVP Code de résultat qui entrent dans la catégorie défaillance transitoire, conformément à la [RFC3588] paragraphe 7.1.4.

Le paragraphe 10.1.3 fait la liste des nouvelles valeurs d'AVP Code de résultat qui entrent dans la catégorie défaillance permanente, conformément à la [RFC3588] paragraphe 7.1.5.

13.5 Création de la section Type d'allocation de serveur SIP dans le registre AAA

Le présent document définit une nouvelle AVP Type d'allocation de serveur SIP (paragraphe 9.4). Cette AVP est du type Énuméré. On définit un ensemble initial de valeurs qui devraient être enregistrées par l'IANA. L'IANA devrait créer une nouvelle section "Valeurs d'AVP Type d'allocation de serveur SIP" sous le sous registre Valeurs spécifiques d'AVP du

registre des paramètres AAA. La liste des valeurs initiales figure au paragraphe 9.4.

13.6 Création de la section Schéma d'authentification SIP dans le registre AAA

Le présent document définit une nouvelle AVP Schéma d'authentification SIP (paragraphe 9.5.1). Cette AVP est du type Énuméré. On définit actuellement une seule valeur qui devrait être enregistrée par l'IANA. L'IANA devrait créer une nouvelle section "Valeurs d'AVP Schéma d'authentification SIP" sous le sous registre Valeurs spécifiques d'AVP du registre des paramètres AAA. La liste initiale des valeurs est incluse au paragraphe 9.5.1.

13.7 Création de la section Code de cause SIP dans le registre AAA

Le présent document définit une nouvelle AVP Code de cause SIP (paragraphe 9.7.1). Cette AVP est du type Énuméré. On définit un ensemble initial de valeurs qui devraient être enregistrées par l'IANA. L'IANA devrait créer une nouvelle section "Valeurs d'AVP Code de cause SIP" sous le sous registre Valeurs spécifiques d'AVP du registre des paramètres AAA. La liste initiale des valeurs figure au paragraphe 9.7.1.

13.8 Création de la section Type d'autorisation d'utilisateur SIP dans le registre AAA

Le présent document définit une nouvelle AVP Type d'autorisation d'utilisateur SIP (paragraphe 9.10). Cette AVP est du type Énuméré. On définit un ensemble initial de valeurs qui devraient être enregistrées par l'IANA. L'IANA devrait créer une nouvelle section "Valeurs d'AVP Type d'autorisation d'utilisateur SIP" sous le sous registre Valeurs spécifiques d'AVP du registre des paramètres AAA. La liste initiale des valeurs figure au paragraphe 9.10.

13.9 Création de la section Données d'utilisateur SIP déjà disponibles dans le registre AAA

Le présent document définit une nouvelle AVP Données d'utilisateur SIP déjà disponibles (paragraphe 9.13). Cette AVP est du type Énuméré. On définit un ensemble initial de valeurs qui devraient être enregistrées par l'IANA. L'IANA devrait créer une nouvelle section "Valeurs d'AVP Données d'utilisateur SIP déjà disponibles" sous le registre Valeurs spécifiques d'AVP du registre des paramètres AAA. La liste initiale des valeurs figure au paragraphe 9.13.

14. Considérations sur la sécurité

Le présent mémoire ne décrit pas un protocole autonome, mais une application particulière pour le protocole Diameter [RFC3588]. Par conséquent, toutes les considérations sur la sécurité applicables à Diameter s'appliquent automatiquement au présent mémoire. En particulier, la Section 13 de la RFC 3588 s'applique au présent mémoire.

Cette application Diameter SIP permet à un client Diameter d'utiliser les propriétés d'authentification HTTP par résumé [RFC2617] en évaluant ou en envoyant au serveur Diameter les accréditifs fournis par un utilisateur. La discussion de l'authentification HTTP par résumé à la Section 4 de la [RFC2617] est aussi applicable au présent mémoire.

Cette application Diameter SIP permet aussi à un client Diameter d'utiliser les propriétés d'authentification HTTP par résumé en utilisant AKA [RFC3310] en évaluant ou en envoyant au serveur Diameter les accréditifs fournis par un utilisateur. La Section 5 de la [RFC3310] est aussi applicable au présent mémoire.

14.1 Vérification finale d'authentification chez le client Diameter/serveur SIP

L'application Diameter SIP peut être configurée à opérer dans un scénario où la vérification de l'authentification finale est effectuée dans le client Diameter (serveur SIP). Un certain nombre de problèmes de sécurité y sont associés ; tous sont des conséquences de l'exigence du transfert de H(A1) du serveur Diameter au client Diameter :

- o le client et le serveur Diameter doivent se faire confiance l'un l'autre, comme quand le client et le serveur appartiennent tous deux au même domaine administratif ;
- o pour éviter les espions, le protocole de transport entre le client et le serveur Diameter DOIT être sécurisé. La [RFC3588] spécifie TLS [RFC4346] et IPsec comme mécanismes possibles de protection du transport pour Diameter.

Du fait de ces considérations de sécurité, il est RECOMMANDÉ de configurer l'application Diameter SIP à opérer dans le mode où la vérification finale de l'authentification est effectuée au serveur Diameter.

15. Contributeurs

Les auteurs tiennent à remercier les contributeurs suivants qui ont fait de substantielles contributions à ce travail :
Pete McCann, Lucent
Jaakko Rajaniemi, Nokia
Wolfgang Beck (Deutsche Telekom AG) a fourni le texte de la Section 12, "Migration depuis RADIUS".

16. Remerciements

Les auteurs tiennent à remercier Tony Johansson et Kevin Purser de leur précieuse contribution au démarrage de cette application et à ses progrès continus. Les auteurs tiennent à remercier Daniel Warren, Jayshree Bharatia, Kuntal Chowdhury, Jari Arkko, Avi Lior, Wolfgang Beck, Ulrich Wiehe, Cullen Jennings, Anu Leinonen, Glen Zorn, German Blanco, Mikko Aittola, Bert Wijnen, et Sam Hartman de leur relecture et de leurs précieux commentaires.

L'application Diameter SIP se fonde sur l'application Diameter pour l'interface Cx du sous système multimédia IP du 3GPP [3GPP.29.229]. Les auteurs tiennent à remercier le groupe de travail 3GPP CN4 pour ce travail.

17. Références

17.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2617] J. Franks et autres, "Authentification HTTP : Authentification d'accès de base et par résumé", juin 1999. *(DS.)*

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* 3265, 3853, 4320, 4916, 5393, 6665, 8217, 8760)

[RFC3310] A. Niemi, J. Arkko, V. Torvinen, "Authentification de résumé dans le protocole de transfert Hypertext (HTTP) utilisant l'authentification et l'accord de clés (AKA)", septembre 2002. *(Information)*

[RFC3588] P. Calhoun et autres, "Protocole fondé sur Diameter", septembre 2003. (*Remplacée par la* RFC6733) *(P.S.)*

[RFC4590] B. Sterman et autres, "Extension à RADIUS pour l'authentification par résumé", juillet 2006.(*Obsolète, voir* RFC5090) *(P.S.)*

17.2 Références pour information

[3GPP.29.229] 3GPP, "Cx et Dx interfaces based on the Diameter protocol; Protocol details", 3GPP TS 29.229 5.12.0, juin 2006.

[JSR-000116] Java Community Process, "SIP Servlet API Specification 1.0 Final Release", JSR 000116, mars 2003.

[RFC3263] J. Rosenberg, H. Schulzrinne, "Protocole d'initialisation de session (SIP) : Localisation des serveurs SIP", juin 2002. (*Remplace* RFC2543) *(P.S. ; MàJ par* RFC7984, RFC8898)

[RFC3680] J. Rosenberg, "Paquetage d'événements du protocole d'initialisation de session (SIP) pour les enregistrements", mars 2004. *(P.S.)*

[RFC3880] J. Lennox, X. Wu, H. Schulzrinne, "Langage de traitement d'appel (CPL) : un langage pour le contrôle d'usager des services de téléphonie Internet", octobre 2004.

[RFC4004] P. Calhoun et autres, "Application IPv4 mobile Diameter", août 2005. *(P.S.)*

[RFC4005] P. Calhoun et autres, "Application de serveur d'accès au réseau Diameter", août 2005. *(P.S.) (Remplacée par* RFC7155)

[RFC4006] H. Hakala et autres, "Application Diameter de contrôle de crédit", août 2005. *(P.S.)*

[RFC4346] T. Dierks et E. Rescorla, "Protocole de sécurité de la couche Transport (TLS) version 1.1", avril 2006. *(Remplace* RFC2246 *; Remplacée par* RFC5246 *; MàJ par* RFC4366, 4680, 4681, 5746, 6176, 7465, 7507, 7919)

Adresse des auteurs

Miguel A. Garcia-Martin
Nokia
P.O. Box 407
NOKIA GROUP, FIN 00045
Finland
téléphone : +358 50 480 4586
mél : miguel.an.garcia@nokia.com

Maria-Carmen Belinchon
Ericsson
Via de los Poblados 13
Madrid 28033
Spain
téléphone : +34 91 339 3535
mél : maria.carmen.belinchon@ericsson.com

Miguel A. Pallares-Lopez
Ericsson
Via de los Poblados 13
Madrid 28033
Spain
téléphone : +34 91 339 4222
mél : miguel-angel.pallares@ericsson.com

Carolina Canales-Valenzuela
Ericsson
Via de los Poblados 13
Madrid 28033
Spain
téléphone : +34 91 339 2680
mél : carolina.canales@ericsson.com

Kalle Tammi
Nokia
P.O.Box 785
Tampere 33101
Finland
téléphone : +358 40 505 8670
mél : kalle.tammi@nokia.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.