Groupe de travail Réseau
Request for Comments : 4004
Catégorie : En cours de normalisation
août 2003
Traduction Claude Bière de L'Isle

P. Calhoun, Cisco Systems, Inc.
T. Johansson, Bytemobile Inc
C. Perkins, Nokia Research Center
T. Hiller, éditeur
P. McCann, Lucent Technologies

Application IPv4 Mobile Diameter

Résumé
Le présent document spécifie une application Diameter qui permet à un serveur Diameter d'authentifier, autoriser et collecter les informations de comptabilité pour les services IPv4 mobiles rendus à un nœud mobile. Combinée avec la capacité inter domaines du protocole de base, cette application permet aux nœuds mobiles de recevoir des services de la part des fournisseurs de service étrangers. Les messages de comptabilité Diameter seront utilisés par les agents étrangers et de rattachement pour transférer les informations d'utilisation aux serveurs Diameter.

Table des Matières

1. Introduction

IPv4 mobile [RFC3344] permet à un nœud mobile (MN, *Mobile Node*) de changer son point de rattachement à l'Internet tout en conservant son adresse de rattachement fixée. Les paquets dirigés sur l'adresse de rattachement sont interceptés par un agent de rattachement (HA, *Home Agent*) encapsulés dans un tunnel, et transmis au MN à son point de rattachement actuel. Facultativement, un agent étranger (FA, *Foreign Agent*) peut être déployé à ce point de rattachement, qui peut servir de point d'extrémité de tunnel et peut aussi assurer le contrôle d'accès pour la liaison réseau visitée. Dans ce rôle, le FA doit authentifier chaque MN qui peut se rattacher à lui, que le MN soit du même domaine administratif ou d'un domaine différent. Le FA doit vérifier que le MN est autorisé à se rattacher et utiliser des ressources dans le domaine étranger. Aussi, le FA doit fournir les informations au domaine administratif de rattachement sur les ressources utilisées par le MN pendant qu'il est rattaché au domaine étranger.

Les exigences d'authentification, autorisation et comptabilité (AAA, *Authentication, Authorization, et Accounting*) pour IPv4 mobile sont décrites en détails dans d'autres documents [RFC2977], [RFC3141]. Le présent document spécifie une application Diameter qui satisfait ces exigences. Cette application n'est pas transposable au protocole IPv6 mobile.

Les formats de message (par exemple, comme au paragraphe 5.1) sont spécifiés comme des listes de paires attribut-valeur (AVP, *Attribute-Value Pair*) utilisant la syntaxe décrite dans la [RFC2234]. Ceci inclut l'utilisation du symbole "*" pour noter zéro, une ou plusieurs occurrences d'une AVP.

Conventions utilisées dans le présent document
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 le BCP 14, [RFC2119].

1.1 Entités et relations

L'application Diameter IPv4 mobile prend en charge le HA et le FA en fournissant le service IPv4 mobile aux MN. Le HA et le FA agissent tous deux comme des clients Diameter. Les MN interagissent avec le HA et le FA en utilisant seulement IPv4 mobile et ne mettent donc pas en œuvre Diameter.

Le FA, lorsque présent, est toujours supposé exister dans le domaine administratif visité. Le HA peut être alloué de façon statique ou dynamique au MN dans le domaine administratif de rattachement ou peut être alloué de façon dynamique au MN dans un domaine administratif visité. Le domaine de rattachement contient un serveur AAA de rattachement (AAAH, *Home AAAA*) et le domaine visité contient un serveur AAA étranger (AAAF, *foreign AAA*). Lorsque le MN est "à la maison" (présent sur son réseau de rattachement) le AAAH et le AAAF peuvent être le même.

1.2 Associations de sécurité de mobilité

Le protocole IPv4 mobile de base [RFC3344] suppose l'existence d'une association de sécurité de mobilité (MSA, *Mobility Security Association*) entre le MN et le HA (MSA MN-HA). La MSA MN-HA est utilisée pour authentifier, en utilisant un algorithme de style chiffrement hachage, la demande d'enregistrement IP mobile qui est envoyée du MN au HA. Il est important d'authentifier les demandes d'enregistrement, car elles informent le HA sur l'adresse d'entretien actuelle du MN, qui est la destination des paquets tunnelés provenant du réseau de rattachement. Sans authentification, des attaquants malveillants seraient capables de rediriger des paquets n'importe où dans l'Internet. La MSA comporte un accord sur un indice de paramètre de sécurité (SPI, *Security Parameters Index*) (un nombre de 32 bits) qui va être utilisé pour se référer à la MSA, un algorithme qui sera utilisé pour calculer des hachages chiffrés sur les messages, et une clé secrète partagée. Pour permettre l'authentification d'un message, l'envoyeur ajoute une extension d'authentification IP mobile qui contient le SPI et le résultat de l'application du hachage chiffré sur le contenu antérieur entier du message. Le receveur vérifie l'extension d'authentification en examinant la MSA sur la base du SPI, en recalculant le hachage chiffré, et en vérifiant que le résultat est égal au contenu de l'extension d'authentification reçue.

Le protocole IPv4 mobile de base prend aussi en charge une MSA facultative entre MN et FA (MSA MN-FA). Si elle est disponible, la MSA MN-FA est utilisée par le FA pour authentifier chaque demande d'enregistrement qui passe à travers elle sur le chemin du HA. Bien qu'elle ne soit pas critique pour le fonctionnement du protocole de base, la MSA MN-FA est utile lorsque le FA doit connaître l'authenticité d'une demande d'enregistrement ; par exemple, lorsque il va générer des enregistrements de comptabilité pour une session. La MSA MN-FA pourra aussi être utile dans de futurs travaux sur l'optimisation du relais.

De même, IPv4 mobile prend en charge une MSA facultative entre FA et HA (MSA FA-HA). La MSA FA-HA est utile pour authentifier les messages entre FA et HA, comme lorsque le HA cherche à informer le FA qu'il a révoqué un enregistrement IP mobile.

Noter que la configuration des MSA qui implique des FA est substantiellement plus difficile que la configuration de celles entre le MN et le HA, parce que le MN et le HA sont souvent dans le même domaine administratif et que le MN va conserver le même HA pendant longtemps. À l'opposé, le MN va probablement rencontrer de nombreux FA au fil du temps et peut se trouver souvent lui-même dans des domaines administratifs étrangers.

Le protocole IPv4 mobile de base suppose que les MN sont identifiés par leurs adresses IP de rattachement statiques et que toutes les MSA sont préconfigurées de façon statique. L'application IPv4 mobile Diameter, avec les extensions [RFC2794], [RFC3012], [RFC3957], [RFC3846] au protocole IPv4 mobile de base, permet à un MN de recevoir de façon dynamique une adresse de rattachement et/ou un agent de rattachement lorsque il se connecte à l'Internet. Cet ensemble de spécifications prend aussi en charge la configuration dynamique des MSA MN-HA, MN-FA, et FA-HA. La configuration dynamique de ces relations est importante pour prendre en charge les déploiements dans lesquels le MN peut se rattacher à un réseau visité sans avoir avec lui de relation préétablie.

Initialement, le MN est supposé avoir une association de sécurité AAA de long terme seulement avec le AAAH. Cette association de sécurité est indexée par le NAI du MN, et, comme les MSA, comporte un accord sur un SPI, un algorithme, et une clé secrète partagée. Le MN entre dans un réseau visité et demande le service à un FA en envoyant une demande

d'enregistrement IPv4 mobile. Le FA contacte un AAAF dans son propre domaine administratif pour authentifier et autoriser la demande de service. Le AAAF et le AAAH peuvent établir une session Diameter directement l'un avec l'autre, comme via un Redirect Diameter, ou peuvent passer des messages via un réseau de mandataires Diameter. Lorsque le AAAF et le AAAH acheminent des messages de l'un à l'autre par des mandataires, plutôt que par une connexion directe, on suppose une confiance mutuelle. Les MN peuvent inclure leur identifiant d'accès réseau (NAI, *Network Access Identifier*) dans une demande d'enregistrement IPv4 mobile [RFC2794], qui sert, au lieu de l'adresse de rattachement, pour identifier le MN. Le NAI est utilisé pour acheminer les messages Diameter à l'AAAH correct. Cette utilisation du NAI est cohérente avec le modèle d'itinérance défini par le groupe de travail ROAMOPS [RFC2477], [RFC2607].

Le AAAH peut authentifier la demande d'enregistrement avec l'utilisation de l'association de sécurité MN-AAA [RFC3012]. Si l'authentification réussit, le AAAH génère alors et distribue les MSA au MN, HA, et FA. Pour chacune des paires de MSA qui impliquent le MN (c'est-à-dire, les MSA MN-HA/HA-MN et MN-FA/FA-MN) le AAAH génère un nom occasionnel et le hache ensuite avec la clé partagée MN-AAA pour déduire la clé de session pour la paire de MSA. Les noms occasionnels sont envoyés au HA qui les inclut dans la réponse d'enregistrement, ce qui permet au MN de déduire les mêmes clés [RFC3957]. En même temps, le AAAH doit distribuer les MSA MN-HA/HA-MN et FA-HA/HA-FA au HA et doit distribuer les MSA MN-FA/FA-MN et FA-HA/HA-FA au FA. Elles sont envoyées dans des AVP Diameter et doivent être sécurisées indépendamment en utilisant IPsec ou TLS entre le AAAH et le FA et entre le AAAH et le HA. Voir à la Section 8 plus d'informations sur la déduction et la distribution des clés.

Noter que les MSA dans IP mobile sont unidirectionnelles en ce que, par exemple, la MSA MN-HA (utilisée pour protéger le trafic du MN au HA) et la MSA HA-MN (utilisée pour protéger le trafic du HA au MN) peuvent utiliser des SPI, algorithmes, et secrets partagés différents. Ceci est vrai du protocole IP mobile de base en dépit de la pratique courante existante durant la configuration manuelle des MSA dans laquelle tous les paramètres sont établis à la même valeur dans les deux directions. Le présent document prend en charge l'utilisation de différents SPI dans chaque direction ; cependant, il ne prend en charge la distribution que d'une seule clé de session pour chaque paire de MSA entre deux nœuds. Les implications de sécurité de cela sont discutées à la Section 13. Le présent document ne cite parfois qu'une seule des deux MSA unidirectionnelles quand il se réfère à la distribution du seul secret partagé et à la paire de SPI pour la paire de MSA entre deux entités.

1.3 Relais

En plus de prendre en charge la déduction et le transport des MSA MN-HA, MN-FA, et FA-HA, cette application prend aussi en charge le relais MIPv4. Lorsque un MN se déplace d'un point de rattachement à un autre, le MN peut continuer la même session IPv4 mobile en utilisant son HA et son adresse de rattachement existants.

Le MN réalise ceci en envoyant une demande d'enregistrement IPv4 mobile à partir de son nouveau point de rattachement. Pour permettre qu'un seul ensemble d'enregistrements de comptabilité soit conservé pour la session entière, incluant les relais, il est nécessaire de permettre au AAAH de lier le nouvel enregistrement à la session préexistante. Pour permettre à la demande d'enregistrement IPv4 mobile d'être acheminée au même AAAH, le MN DEVRAIT inclure le NAI du AAAH [RFC3846] dans de tels réenregistrements. Aussi, pour aider le AAAH à acheminer les messages au HA existant du MN, le nœud mobile DEVRAIT inclure le MAI du HA [RFC3846] dans de tels réenregistrements. Si le nœud mobile ne prend pas en charge l'extension de NAI AAA IPv4 mobile [RFC3846], cette fonctionnalité n'est pas disponible.

1.4 Structure du document

Le reste de ce document est structuré comme suit. La Section 2 donne les définitions des acronymes. La Section 3 donne des exemples et des flux de messages qui illustrent les messages IPv4 mobile et Diameter qui se produisent lorsque un nœud mobile se rattache à l'Internet. La Section 4 définit les relations de cette application au protocole Diameter de base. La Section 5 définit les nouveaux codes de commandes. La Section 6 définit les nouveaux codes de résultat utilisés par cette application. La Section 7 définit l'ensemble des paires d'attribut valeur (AVP, *Attribute-Value-Pair*) obligatoires. La Section 8 donne une vue d'ensemble de la capacité de distribution de clés, et la Section 9 définit les AVP de distribution de clés. La Section 10 définit les AVP de comptabilité, et la Section 11 contient une liste de toutes les AVP et leur occurrence dans les commandes Diameter. Finalement, les Sections 12 et 13 donnent respectivement les considérations relatives à l'IANA et à la sécurité.

2. Acronymes

AAAH *(Authentication, Authorization, et Accounting Home)* : authentification, autorisation et comptabilité de rattachement
AAAF *(Authentication, Authorization, et Accounting Foreign)* : authentification, autorisation et comptabilité étrangères
AMA *(AA-Mobile-Node-Answer)* : réponse de nœud mobile AA

AMR *(AA-Mobile-Node-Request)* : demande de nœud mobile AA
ASR *(Abort-Session-Request)* : demande d'interruption de session
AVP *(Attribute Value Pair)* : paire attribut valeur
CoA *(Care-of-Address)* : adresse d'entretien
FA *(Foreign Agent)* : agent étranger
FQDN *(Fully Qualified Domain Name)* : nom de domaine pleinement qualifié
HA *(Home Agent)* : agent de rattachement
HAA *(Home-Agent-MIP-Answer)* : réponse d'agent de rattachement IP mobile
HAR *(Home-Agent-MIP-Request)* : demande d'agent de rattachement IP mobile
MN *(Mobile Node)* : nœud mobile
MSA *(Mobility Security Association)* : association de sécurité de mobilité
NAI *(Network Access Identifier)* : identifiant d'accès réseau
RRQ *(demande d'enregistrement)* : demande d'enregistrement
SPI *(Security Parameters Index)* : indice de paramètres de sécurité
STR *(Session-Termination-Request)* : demande de terminaison de session

3. Scénarios et flux de messages

Cette section présente quatre scénarios illustrant l'application IPv4 mobile Diameter et décrivant le fonctionnement de la distribution de clés.
Dans ce document, le rôle "d'accompagnateur" *(attendant, un nœud conçu pour fournir l'interface de service entre un client et le domaine local)* [RFC2977] est effectué soit par le FA (quand il est présent dans un réseau visité) soit par le HA (pour les nœuds mobiles colocalisés non enregistrés via un FA) et ces termes seront utilisés de façon interchangeable dans les scénarios qui suivent.

3.1 IPv4 mobile inter domaine

Lorsque un nœud mobile demande le service en produisant une demande d'enregistrement à l'agent étranger, l'agent étranger crée le message AA-Mobile-Node-Request (AMR) qui comporte les AVP définies à la Section 7. Les champs Adresse de rattachement, Agent de rattachement, NAI de nœud mobile, et autres qui sont importants sont extraits des messages d'enregistrement pour une possible inclusion comme AVP Diameter. Le message AMR est alors transmis au serveur Diameter local, appelé AAA-Foreign, ou AAAF.

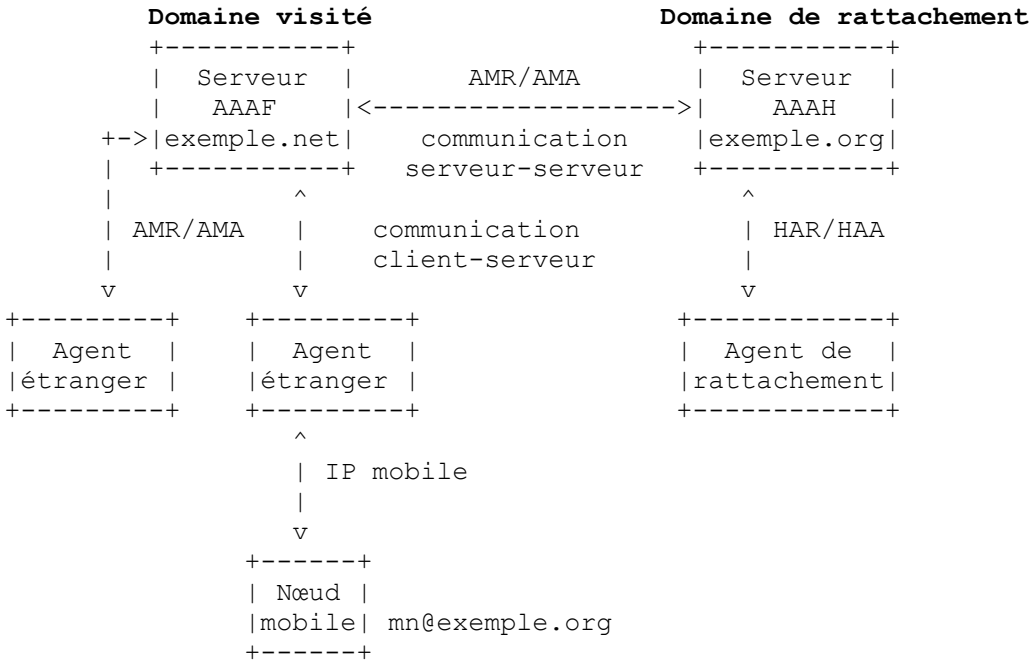

Figure 1 : Mobilité inter domaines

À réception de l'AMR, l'AAAF suit les procédures mentionnées dans la [RFC3588] pour déterminer si l'AMR devrait être traitée en local ou transmise à un autre serveur Diameter appelé le AAA de rattachement (AAAH, *AAA-Home*). La Figure 1 montre un exemple dans lequel un nœud mobile (mn@exemple.org) demande le service d'un fournisseur étranger

(exemple.net). La demande reçue par l'AAAF est transmise au serveur AAAH de exemple.org.

La Figure 2 montre les flux de messages impliqués lorsque l'agent étranger invoque l'infrastructure AAA pour demander qu'un nœud mobile soit authentifié et autorisé. Noter qu'il n'est pas exigé que l'agent étranger invoque les services AAA chaque fois qu'il reçoit une demande d'enregistrement de la part du mobile, mais plutôt lorsque l'autorisation antérieure de la part de l'AAAH arrive à expiration. Le moment d'arrivée à expiration de l'autorisation est communiqué au moyen de l'AVP Authorization-Lifetime *(durée de vie d'autorisation)* dans la réponse de nœud mobile AA (AMA, *AA-Mobile-Node-Answer*) (voir au paragraphe 5.2) provenant de l'AAAH.

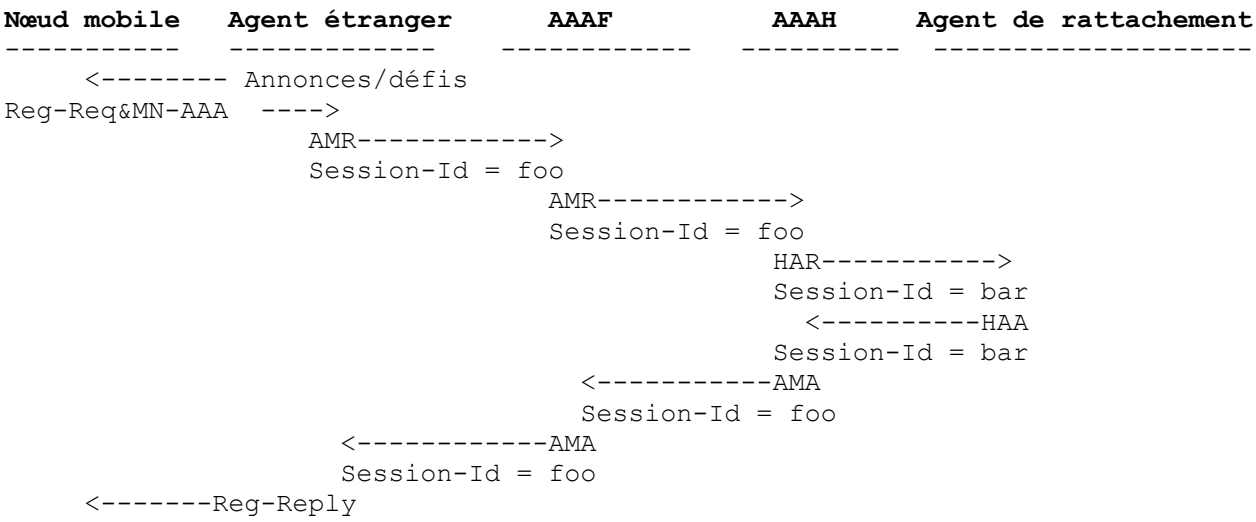

Figure 2 : Échange de messages IPv4 mobile/Diameter

L'agent étranger (comme le montre la Figure 2) PEUT fournir un défi *(challenge)* qui va donner un contrôle direct sur la protection contre la répétition dans le processus d'enregistrement IPv4 mobile, comme décrit dans la [RFC3012]. Le nœud mobile inclut le défi et l'extension d'authentification MN-AAA pour permettre l'autorisation par le AAAH. Si les données d'authentification fournies dans l'extension MN-AAA sont invalides, le AAAH retourne la réponse (AMA) avec l'AVP de code de résultat réglée à DIAMETER_AUTHENTICATION_REJECTED *(authentification Diameter rejetée)*.

Le scénario ci-dessus cause l'exposition des clés MN-FA et MN-HA aux agents Diameter tout le long du chemin Diameter. Si cela pose un problème, une approche plus sûre est d'éliminer le AAAF et les autres agents Diameter, comme montré à la Figure 3.

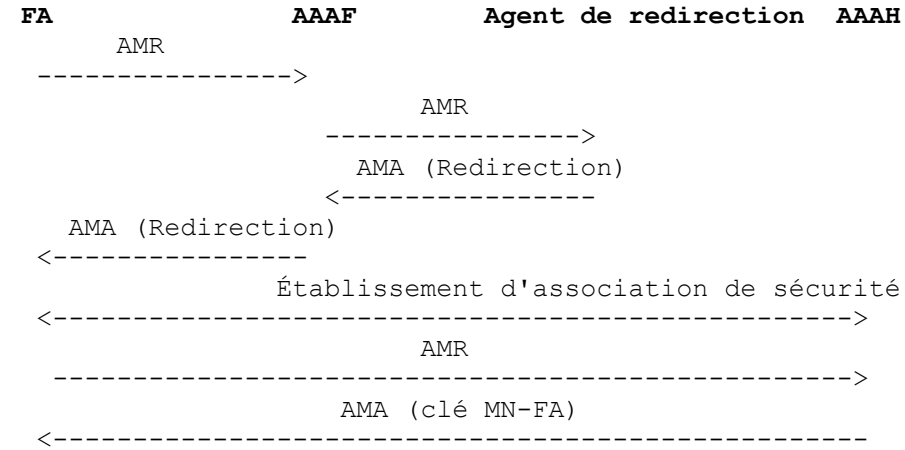

Figure 3 : Utilisation d'un serveur de redirection avec AMR/AMA

Dans la Figure 3, le FA établit une association de sécurité fondée sur TLS [RFC35461] ou IPsec [RFC2401] directement avec le AAAH et fait fonctionner l'échange d'AMR/AMA sur elle. Cela assure la sécurité de bout en bout pour les clés secrètes qui peuvent devoir être distribuées.

La Figure 4 montre l'interaction entre le AAAH et le HA avec l'aide d'un agent de redirection. Lorsque le AAAH et le HA sont dans le même réseau, il est probable que le AAAH va connaître l'adresse IP du HA, de sorte que le serveur de

redirection ne devrait pas être nécessaire ; cependant, il est quand même montré pour être complet. Le serveur de redirection va très probablement être utilisé dans le cas où le HA est alloué dans un réseau étranger (voir au paragraphe 3.2 les détails de l'allocation de HA dans les réseaux étrangers).

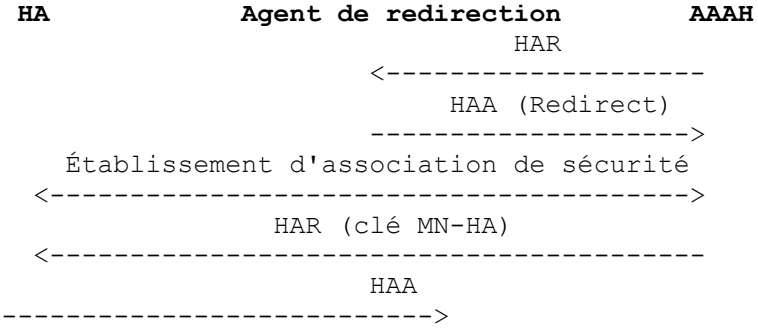

Figure 4 : Utilisation d'un serveur de redirection avec HAR/HAA

Comme dans la Figure 2, le FA de la Figure 3 va encore produire le défi et le mobile envoie le RRQ, etc. ; cependant, ces étapes ont été éliminées de la Figure 3 pour en réduire les dimensions. Le serveur de redirection élimine le AAAF et tous les autres agents Diameter de la vue des clés car elles sont transportées au FA et HA. Noter que les flux de messages des Figures 3 et 4 ne s'appliquent qu'à l'échange initial d'authentification et de clés. Les messages de comptabilité seraient quand même envoyés via des agents Diameter, et non via la connexion directe, sauf si la politique du réseau en décide autrement.

Un nœud mobile qui prend en charge l'extension NAI AAA [RFC3846], qui a été précédemment authentifié et autorisé, DOIT toujours inclure l'agent de rattachement alloué dans le sous type Identité HA de l'extension NAI AAA, et le serveur AAA de rattachement qui autorise dans le sous type Identité AAAH de l'extension NAI AAA, lors de la ré-authentification. Donc, dans le cas où l'AMR généré par le FA est pour une session qui a été précédemment autorisée, il DOIT inclure l'AVP Destination-Host *(hôte de destination)* avec l'identité du AAAH trouvée dans le AAAH-NAI, et l'AVP MIP-Home-Agent-Host *(hôte d'agent de rattachement MIP)* avec l'identité et le domaine du HA alloué trouvé dans le HA-NAI. Si, d'un autre côté, le nœud mobile ne prend pas en charge l'extension NAI AAA, le FA peut ne pas avoir l'identité du AAAH et l'identité et le domaine du HA alloué. Cela signifie que sans prise en charge de l'extension NAI AAA, le FA peut n'être pas capable de garantir que l'AMR sera destinée au même AAAH, qui a précédemment authentifié et autorisé le nœud mobile, car le FA peut ne pas savoir l'identité de l'AAAH.

Si l'authentification du nœud mobile a réussi, le AAAH détermine alors quel agent de rattachement utiliser pour la session. D'abord, le AAAH vérifie si un HA a été demandé par le MN en vérifiant l'AVP MIP-Home-Agent-Address et l'AVP MIP-Home-Agent-Host. Le domaine administratif qui possède le HA peut être déterminé à partir de la portion domaine de l'AVP MIP-Home-Agent-Host, ou en vérifiant le fanion Home-Agent-In-Foreign-Network *(agent de rattachement dans le réseau étranger)* de l'AVP MIP-Feature-Vector *(vecteur de caractéristiques MIP)* et la valeur de l'AVP MIP-Originating-Foreign-AAA *(AAA étranger générateur de MIP)*. Si le HA demandé appartient à un domaine administratif permis, le AAAH DEVRAIT utiliser ce HA pour la session. Autrement, le AAAH retourne la réponse (AMA) avec l'AVP de code de résultat réglée soit à DIAMETER_ERROR_NO_FOREIGN_HA_SERVICE *(erreur Diameter, pas de service de HA étranger)*, soit à DIAMETER_ERROR_HA_NOT_AVAILABLE *(erreur Diameter, HA non disponible)*.

Si le MN n'a pas demandé de HA particulier, un HA DOIT alors être alloué de façon dynamique. Dans ce cas, le MIP-Feature-Vector aura le fanion Home-Agent-Requested *(agent de rattachement demandé)* établi. Si le fanion Home-Address-Allocatable-Only-in-Home-Realm *(adresse de rattachement allouable seulement dans le domaine de rattachement)* n'est pas établi, et si le fanion Foreign-Home-Agent-Available *(agent de rattachement étranger disponible)* est établi, le AAAH DEVRAIT alors permettre au domaine étranger d'allouer le HA (voir au paragraphe 3.2) mais PEUT en allouer un lui-même dans le domaine de rattachement si la politique locale le décide. Si le fanion Home-Address-Allocatable-Only-in-Home-Realm est établi, le AAAH DOIT alors allouer un HA dans le domaine de rattachement au nom du MN. L'allocation du HA peut être faite de diverses façons, incluant en utilisant un algorithme d'équilibrage de charge pour égaliser la charge sur tous les agents de rattachement. L'algorithme réel utilisé et la méthode de découverte de l'agent de rattachement sortent du domaine d'application de la présente spécification.

Le AAAH envoie alors une demande d'agent de rattachement MIP (HAR, *Home-Agent-MIP-Request*) qui contient les données de message de demande d'enregistrement IPv4 mobile encapsulées dans l'AVP MIP-Reg-Request *(demande d'enregistrement MIP)* à l'agent de rattachement alloué ou demandé. Se référer à la Figure 4 si le AAAH n'a pas de chemin direct pour le HA. Le AAAH PEUT allouer une adresse de rattachement pour le nœud mobile, et l'agent de rattachement DOIT prendre en charge l'allocation d'adresse de rattachement. Dans le cas où le AAAH traite l'allocation d'adresse, il inclut l'adresse de rattachement dans une AVP MIP-Mobile-Node-Address *(adresse de nœud mobile MIP)* dans la HAR.

L'absence de cette AVP informe l'agent de rattachement qu'il doit effectuer l'allocation d'adresse de rattachement.

À réception de la HAR, l'agent de rattachement traite d'abord le message Diameter. L'agent de rattachement traite l'AVP MIP-Reg-Request et crée la réponse d'enregistrement, l'encapsulant dans l'AVP MIP-Reg-Reply. Dans la création de la réponse d'enregistrement, l'agent de rattachement DOIT inclure le NAI de HA et le NAI de AAAH, qui seront créés à partir des AVP Origin-Host et Origin-Realm de la HAR. Si une adresse de rattachement est nécessaire, l'agent de rattachement DOIT aussi en allouer une et inclure l'adresse dans la réponse d'enregistrement et dans l'AVP MIP-Mobile-Node-Address.

À réception de la HAA, le AAAH crée le message AA-Mobile-Node-Answer (AMA), qui inclut les mêmes Acct-Multi-Session-Id que contenus dans la HAA et les AVP MIP-Home-Agent-Address et MIP-Mobile-Node-Address dans le message AMA. Voir les Figures 3 et 4 sur l'utilisation de l'agent de redirection pour le transport sûr des messages HAA et AMA.

Voir au paragraphe 4.1 des informations sur la gestion des sessions et les identifiants de session par les entités Diameter IPv4 mobile.

3.2 Allocation d'agent de rattachement dans le réseau étranger

L'application IPv4 mobile Diameter permet à un agent de rattachement d'être alloué dans réseau étranger, comme exigé par les [RFC2977], [RFC3141]. Lorsque un agent étranger détecte que le nœud mobile a une adresse d'agent de rattachement égale à 0.0.0.0 ou 255.255.255.255 dans le message de demande d'enregistrement, il DOIT ajouter une AVP MIP-Feature-Vector avec le fanion Home-Agent-Requested réglé à un. Si l'adresse de l'agent de rattachement est réglée à 255.255.255.255, l'agent étranger DOIT régler le fanion Home-Address-Allocatable-Only-in-Home-Realm égal à un. Si l'adresse de l'agent de rattachement est réglée à 0.0.0.0, l'agent étranger DOIT régler le fanion Home-Address-Allocatable-Only-in-Home-Realm à zéro.

Lorsque le AAAF reçoit un message AMR avec le fanion Home-Agent-Requested réglé à un et avec le fanion Home-Address-Allocatable-Only-in-Home-Realm à zéro, le AAAF PEUT établir le fanion Foreign-Home-Agent-Available dans l'AVP MIP-Feature-Vector afin d'informer le AAAH qu'il a la volonté et la capacité d'allouer un agent de rattachement pour le nœud mobile. Lorsque il fait cela, l'AAAF DOIT inclure l'AVP MIP-Candidate-Home-Agent-Host et l'AVP MIP-Originating-Foreign-AAA. L'AVP MIP-Candidate-Home-Agent-Host contient l'identité (c'est-à-dire, une DiameterIdentity, qui est un FQDN) de l'agent de rattachement qui serait alloué au nœud mobile, et l'AVP MIP-Originating-Foreign-AAA contient l'identité de l'AAAF. L'AAAF envoie maintenant l'AMR au AAAH. Cependant, comme indiqué ci-dessus, l'utilisation d'agents Diameter entre le FA et l'AAAH exposerait la clé MN-FA. Si c'est estimé indésirable, on DEVRAIT utiliser l'approche du serveur de redirection pour communiquer l'AMR à l'AAAH. Cela fait que le FA communique l'AMR directement à l'AAAH via une association de sécurité.

Si le nœud mobile avec prise en charge de l'extension NAI AAA [RFC3846] qui a été précédemment autorisé par l'AAAH, a maintenant besoin d'être réauthentifié, et demande à conserver l'agent de rattachement alloué dans le réseau étranger, le nœud mobile DOIT inclure le NAI HA et le NAI AAAH dans la demande d'enregistrement au FA. À réception, le FA va créer l'AMR, incluant l'AVP MIP-Home-Agent-Address et l'AVP Destination-Host sur la base du NAI AAAH, et inclure l'AVP MIP-Home-Agent-Host sur la base du NAI de l'agent de rattachement. Si le AAAF autorise l'utilisation de l'agent de rattachement demandé, l'AAAF DOIT établir le bit Home-Agent-In-Foreign-Network dans l'AVP MIP-Feature-Vector.

Si le nœud mobile doit être réauthentifié mais ne prend pas en charge l'extension NAI AAA, il envoie une demande d'enregistrement sans NAI AAA ni NAI HA, même si il a été antérieurement autorisé par le AAAH et demande à conserver l'agent de rattachement alloué dans le réseau étranger. À réception, le FA va créer l'AMR, incluant l'AVP MIP-Home-Agent-Address. Si l'AAAF autorise l'utilisation de l'agent de rattachement demandé, et si il sait que l'agent est dans son propre domaine, l'AAAF DOIT établir le bit Home-Agent-In-Foreign-Network dans l'AVP MIP-Feature-Vector.

Lorsque l'AAAH reçoit un message AMR, il vérifie d'abord les données d'authentification fournies par le nœud mobile, conformément aux AVP MIP-Reg-Request et MIP-MN-AAA-Auth, et détermine si il autorise le nœud mobile. Si l'AMR indique que l'AAAF a offert d'allouer un agent de rattachement pour le nœud mobile (c'est-à-dire, si Foreign-Home-Agent-Available est établi dans l'AVP MIP-Feature-Vector) ou si l'AMR indique que l'AAAF a offert un agent de rattachement précédemment alloué au nœud mobile (c'est-à-dire, si Home-Agent-In-Foreign-Network est établi dans l'AVP MIP-Feature-Vector) l'AAAH doit alors décider si sa politique locale va permettre à l'utilisateur d'avoir ou conserver un agent de rattachement dans le réseau étranger. En supposant qu'il soit permis au nœud mobile de faire ainsi, l'AAAH détermine l'adresse IP du HA sur la base du FQDN du HA en utilisant le DNS ou en l'apprenant via une AVP MIP-Home-Agent-Address dans une réponse de redirection à une HAR (c'est-à-dire, si le serveur de redirection ajoute cette AVP à la HAA). Il envoie ensuite un message HAR à l'agent de rattachement en incluant l'AVP Destination-Host réglée à la valeur trouvée dans l'AVP MIP-Candidate-Home-Agent-Host ou MIP-Home-Agent-Host de l'AMR. Si le DNS est utilisé pour déterminer l'adresse IP du HA, on suppose que le HA a une adresse publique et que le DNS peut la résoudre.

Des considérations de sécurité peuvent exiger que le HAR soit envoyé directement de l'AAAH au HA sans utilisation d'agents Diameter intermédiaires. Cela exige qu'une association de sécurité soit établie entre le AAAH et le HA, comme a la Figure 4. Si aucune association de sécurité ne peut être établie, le AAAH DOIT retourner une AMA avec l'AVP Result-Code réglée à DIAMETER_ERROR_END_TO_END_MIP_KEY_ENCRYPTION *(erreur Diameter de chiffrement de clé MIP de bout en bout)*.

Si les agents Diameter sont utilisés (par exemple, si il n'y a pas de serveur de redirection) le AAAH envoie la HAR à l'AAAF générateur. Dans cette HAR, l'AVP Destination-Host est réglée à la valeur trouvée dans l'AVP MIP-Originating-Foreign-AAA de l'AMR, et l'AVP MIP-Home-Agent-Host ou MIP-Candidate-Home-Agent-Host trouvée dans l'AMR est copiée dans la HAR.

Donc, le AAAH DOIT toujours copier l'AVP MIP-Originating-Foreign-AAA provenant du message AMR dans le message HAR. Dans les cas où un autre AAAF reçoit la HAR, ce nouveau AAAF va envoyer la HAR au HA.

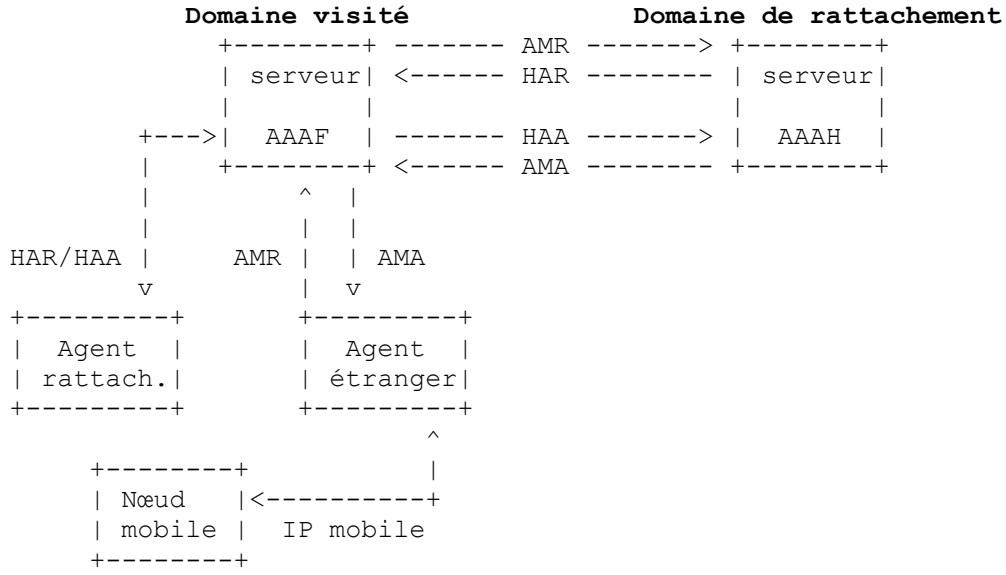

Figure 5 : Agent de rattachement alloué dans le domaine visité

À réception d'une HAA provenant de l'agent de rattachement dans le domaine visité, l'AAAF transmet la HAA au AAAH dans le domaine de rattachement. La AMA est alors construite et produite au AAAF et, finalement, au FA. Si le code de résultat indique le succès, la HAA et l'AMA DOIVENT inclure les AVP MIP-Home-Agent-Address et MIP-Mobile-Node-Address.

Si l'exposition des clés aux agents Diameter le long du chemin représente un risque de sécurité inacceptable, l'approche de redirection décrite par les Figures 3 et 4 DOIT être utilisée à la place.

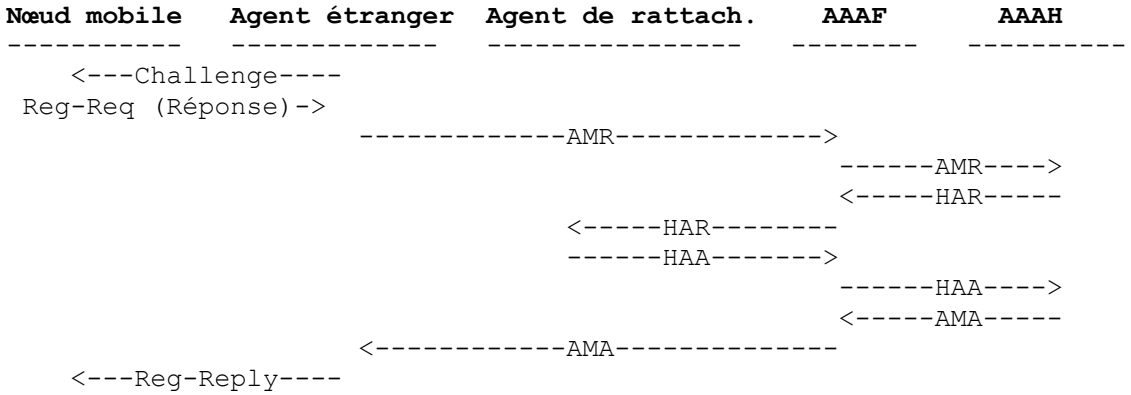

Figure 6 : Échange MIP/Diameter pour l'allocation de HA dans le domaine visité

Si le nœud mobile passe dans un autre réseau étranger, il PEUT demander à conserver le même agent de rattachement au sein de l'ancien réseau étranger ou demander d'en obtenir un nouveau dans le nouveau réseau étranger. Si le AAAH accepte

de fournir le service demandé, le AAAH aura à fournir des services pour les deux réseaux visités; par exemple, le rafraîchissement des clés.

3.3 Nœud mobile colocalisé

Si un nœud mobile s'enregistre auprès de l'agent de rattachement comme un nœud mobile colocalisé, aucun agent étranger n'est impliqué. Donc, lorsque l'agent de rattachement reçoit la demande d'enregistrement, un message AMR est envoyé au serveur AAAH local, avec le bit Co-Located-Mobile-Node établi dans l'AVP MIP-Feature-Vector. L'agent de rattachement inclut aussi l'AVP Acct-Multi-Session-Id (voir les paragraphes 4.1.1 et 4.1.2) dans l'AMR envoyée à l'AAAH, car l'AAAH peut trouver utile cet élément d'état de session ou ces information d'entrée d'enregistrement.

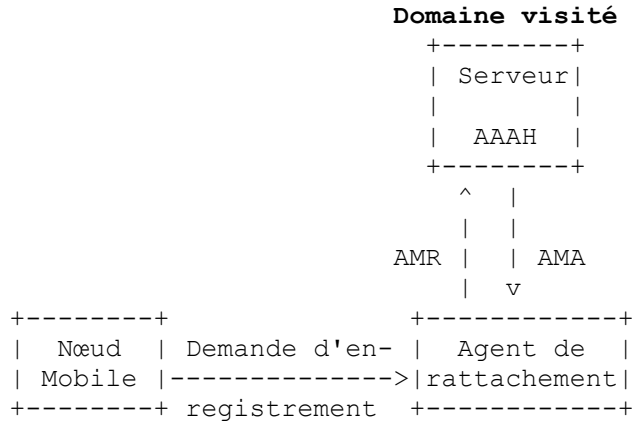

Figure 7 : Nœud mobile colocalisé

Si le bit MN-HA-Key-Requested a été établi dans le message AMR provenant de l'agent de rattachement, les clés de session de l'agent de rattachement et du nœud mobile seront présentes dans le message AMA.

La Figure 8 montre un diagramme de signalisation qui indique une façon sûre d'établir les associations de sécurité nécessaires lors de l'utilisation de serveur de redirection. Le AAA mandataire représente tout serveur AAA ou des serveurs que le HA peut utiliser. Ceci s'applique au réseau visité ou de rattachement.

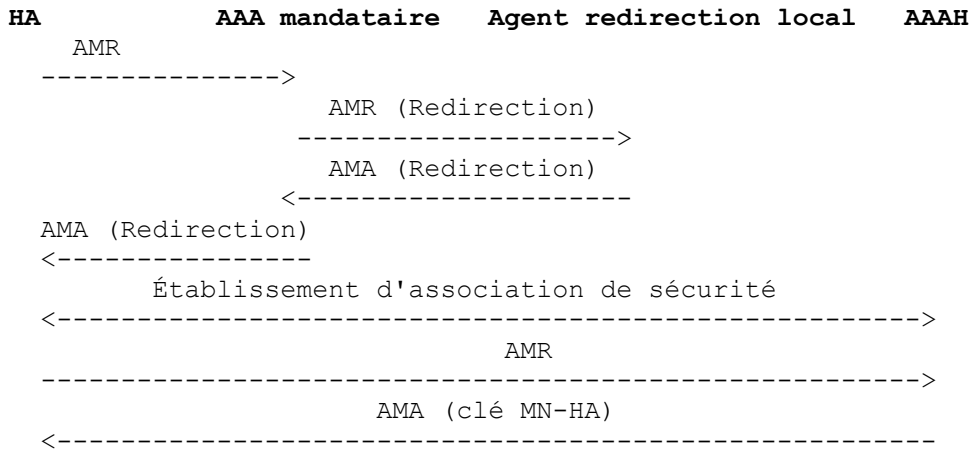

Figure 8 : Utilisation d'un serveur de redirection pour CoA et AMR/AMA colocalisés

3.4 Distribution de clé

Pour permettre l'adaptabilité des données sans fil à travers les domaines administratifs, il est nécessaire de minimiser le nombre d'associations de sécurité de mobilité préexistantes requis. Cela signifie que chaque agent étranger pourrait n'être pas obligé d'avoir une MSA préconfigurée avec chaque agent de rattachement sur l'Internet, et que le nœud mobile ne serait pas obligé d'avoir une MSA préconfigurée (comme défini dans la [RFC3344]) avec tout agent étranger spécifique. De plus, lorsque le nœud mobile demande une allocation dynamique d'agent de rattachement, il va probablement recevoir l'adresse d'un agent de rattachement pour lequel il n'a pas de MSA disponible.

L'application IPv4 mobile Diameter résout ce problème en incluant la fonction de distribution de clés, ce qui signifie qu'après l'authentification d'un nœud mobile, la phase d'autorisation inclut la génération de clés de session et de noms occasionnels. Précisément, trois clés de session et deux noms occasionnels sont générés :

- K1 : La clé de session MN-HA, qui va faire partie de la MSA entre le nœud mobile et l'agent de rattachement. La clé de session MH-HA est dérivée d'un nom occasionnel généré par AAA. Le nœud mobile obtient ce nom occasionnel dans la réponse d'enregistrement et génère cette clé en utilisant la même formule que AAA.

- K2 : La clé MN-FA, qui va faire partie de la MSA entre le nœud mobile et l'agent étranger. La clé MN-FA est dérivée d'un nom occasionnel généré par AAA. Le nœud mobile obtient ce nom occasionnel dans la réponse d'enregistrement et génère la clé MN-FA en utilisant la même formule que AAA.

- K3 : La clé FA-HA, qui va faire partie de la MSA entre l'agent étranger et l'agent de rattachement.

La même clé de session est utilisée dans les deux directions entre deux entités ; par exemple, le nœud mobile et l'agent étranger utilisent la même clé de session pour les extensions d'authentification de MN-FA et de FA-MN. Les implications de sécurité en sont examinées dans la Section 13. Cependant, les SPI peuvent être différents pour les extensions d'authentification de MN-FA et de FA-MN. Le SPI pour la MSA MN-FA est utilisé sur des messages envoyés du MN au FA, et le SPI pour la MSA FA-MN est utilisé dans les messages envoyés du FA au MN.

Toutes les clés et noms occasionnels sont générés par l'AAAH, même si un agent de rattachement est alloué de façon dynamique dans le réseau étranger.

La Figure 9 décrit les MSA utilisées pour l'intégrité des messages IPv4 mobile en utilisant les clés créées par le serveur Diameter.

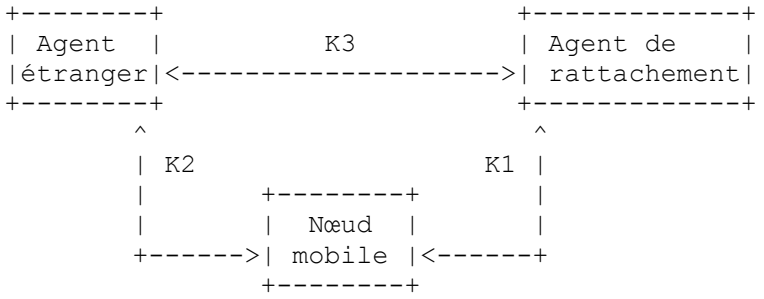

Figure 9 : Associations de sécurité de mobilité après la distribution des clés de session et des noms occasionnels

Les clés destinées à l'agent étranger et à l'agent de rattachement sont propagées aux agents de mobilité via le protocole Diameter. Si l'exposition de clés aux agents Diameter le long du chemin représente un risque de sécurité inacceptable, les clés DOIVENT alors être protégées par des association de sécurité IPsec ou TLS qui existent directement entre le HA et le AAAH ou le FA et le AAAF, comme expliqué ci-dessus.

Les clés destinées au nœud mobile DOIVENT aussi être propagées via le protocole IPv4 mobile et DOIVENT donc suivre les mécanismes décrits dans la [RFC3957]. Dans la [RFC3957], le nœud mobile reçoit un nom occasionnel pour chaque clé dont il a besoin, et le nœud mobile va utiliser le nom occasionnel et le secret partagé à long terme pour créer les clés (voir la Section 8).

Une fois les clés de session établies et propagées, les appareils de mobilité peuvent échanger directement les informations d'enregistrement, comme défini dans la [RFC3344], sans qu'il soit besoin de l'infrastructure Diameter. Cependant, les clés de session ont une durée de vie, après l'expiration de laquelle l'infrastructure Diameter DOIT être invoquée à nouveau si de nouvelles clés de session et de nouveaux noms occasionnels doivent être acquis.

4. Considérations sur le protocole Diameter

Cette section détaille les relations de l'application IPv4 mobile Diameter avec le protocole Diameter de base.

Le présent document spécifie Diameter Application-ID 2. Les nœuds Diameter qui se conforment à la présente spécification PEUVENT annoncer leur prise en charge en incluant la valeur de deux (2) dans l'AVP Auth-Application-Id ou Acct-Application-Id des commandes Capabilities-Exchange-Request et Capabilities-Exchange-Answer [RFC3588]. La

valeur de deux (2) DOIT être utilisée comme identifiant d'application (Application-Id) dans toutes les commandes AMR/AMA et HAR/HAA. La valeur de deux (2) DOIT être utilisée comme identifiant d'application dans toutes les commandes ACR/ACA, car cette application définit de nouvelles AVP obligatoires pour la comptabilité. La valeur de zéro (0) DEVRAIT être utilisée comme identifiant d'application dans toutes les commandes STR/STA et ASR/ASA, car elles sont définies dans le protocole Diameter de base et qu'aucune AVP obligatoire supplémentaire pour ces commandes n'est définie dans le présent document.

Étant donnée la nature de IPv4 mobile, la réauthentification ne peut être initiée que par un nœud mobile qui ne participe pas à l'échange de messages Diameter. Donc, la réauthentification à l'initiative du serveur Diameter ne s'applique pas à cette application, et les commandes RAR/RAA NE DOIVENT PAS être envoyées pour les sessions Diameter IPv4 mobile.

4.1 Gestion de session Diameter

Le AAAH et l'AAAF PEUVENT conserver l'état de session ou PEUVENT être sans état de session. Les agents AAA de redirection et de relais NE DOIVENT PAS conserver l'état de session. Le AAAH, l'AAAF, les mandataires et agents de relais DOIVENT conserver l'état de transaction.

La session d'un nœud mobile est identifiée via son identité dans les AVP User-Name, MIP-Mobile-Node-Address, et MIP-Home-Agent-machine, définies dans le protocole de base [RFC3588], comme étant utilisées sans modification pour la présente application. Cependant, comme le MN peut interagir avec plus d'un FA durant la vie de sa session, il est important que l'application IPv4 mobile Diameter distingue les deux parties de la session (un certain état au FA, un certain état au HA) et les gère de façon indépendante. Les sous paragraphes qui suivent détaillent cela.

4.1.1 Identifiants de session

Durant la création de l'AMR, le FA va choisir un identifiant de session. Durant la création de la HAR, le AAAH DOIT utiliser un identifiant de session différent de celui utilisé dans la AMR/AMA. Si le AAAH est à états pleins de session, il DOIT envoyer le même identifiant de session pour toutes les HAR initiées au nom de la session d'un certain nœud mobile. Autrement, si le AAAH est sans état de session, il va fabriquer un identifiant de session unique pour chaque HAR.

Lors de la première allocation du HA, il DOIT créer et inclure une AVP Acct-Multi-Session-Id dans la HAA retournée au AAAH. Cet identifiant sera conservé constant pour la durée de vie de la session IPv4 mobile, comme précisé au paragraphe suivant.

4.1.2 Gestion des sessions durant les relais IPv4 mobile

Étant donnée la nature de IPv4 mobile, un nœud mobile PEUT recevoir le service à partir de nombreux agents étrangers durant une certaine période. Cependant, le domaine de rattachement ne devrait pas voir ces relais comme des sessions différentes, car cela pourrait affecter les systèmes de facturation. De plus, les agents étrangers ne communiquent généralement pas entre eux, ce qui implique que les informations d'AAA ne peuvent pas être échangées entre ces entités.

Une demande d'enregistrement de relais provenant d'un nœud mobile va causer l'envoi par le FA d'une AMR à son AAAF. L'AMR va inclure un nouvel identifiant de session et PEUT être envoyée à un nouvel AAAF (c'est-à-dire, un AAAF différent de celui utilisé par le FA précédent). Cependant, l'AMR devra être reçue par l'AAAH auprès duquel l'usager est actuellement enregistré (éventuellement via le mécanisme de redirection décrit à la Figure 3).

Comme l'AAAH peut être sans état de session, il est nécessaire pour la HAR résultante reçue par le HA d'être identifiée comme continuation d'une session existante. Si le HA reçoit une HAR pour un nœud mobile avec un nouvel identifiant de session et si le HA peut garantir que cette demande est pour étendre un service existant, le HA DOIT alors être capable de modifier ses informations internes d'état de session pour refléter le nouvel identifiant de session.

Pour que la corrélation se fasse, les enregistrements de comptabilité doivent avoir une certaine communalité à travers les relais. Donc, l'agent de rattachement DOIT envoyer la même valeur d'AVP Acct-Multi-Session-Id dans toutes les HAA pour la session du mobile. C'est-à-dire, le HA génère un unique Acct-Multi-Session-Id lorsque il reçoit une HAR pour une nouvelle session et retourne cette même valeur dans toutes les HAA pour la session. Cette AVP Acct-Multi-Session-Id sera retournée à l'agent étranger par le AAAH dans l'AMA. Les agents étrangers et de rattachement DOIVENT tous deux inclure le Acct-Multi-Session-Id dans les messages de comptabilité, comme décrit à la Figure 10.

4.1.3 Terminaison de session Diameter

Suivant la présente spécification un agent étranger et un agent de rattachement PEUVENT s'attendre à ce que leurs serveurs

Diameter respectifs conservent les informations d'état de session pour chaque nœud mobile de leurs réseaux. Pour q'un serveur Diameter libère toutes les ressources allouées à un nœud mobile spécifique, ce serveur doit recevoir une demande de terminaison de session (STR, *Session-Termination-Request*) d'un agent de mobilité. Les agents de mobilité DOIVENT produire la demande de terminaison de session (STR) si la durée de vie d'autorisation est arrivée à expiration et si aucune demande d'enregistrement MIP suivante n'a été reçue.

Le AAAH DEVRAIT ne désallouer toutes les ressources qu'après que la STR est reçue de l'agent de rattachement. Cela assure qu'un nœud mobile qui se déplace d'un agent étranger à un autre (par exemple, par suite d'un transfert inter-cellulaire) ne cause pas la libération par le serveur Diameter de rattachement de toutes les ressources pour le nœud mobile. Donc, une STR d'un agent étranger libèrerait la session de l'agent étranger, mais pas l'état de session associé à l'agent de rattachement (voir la Figure 10).

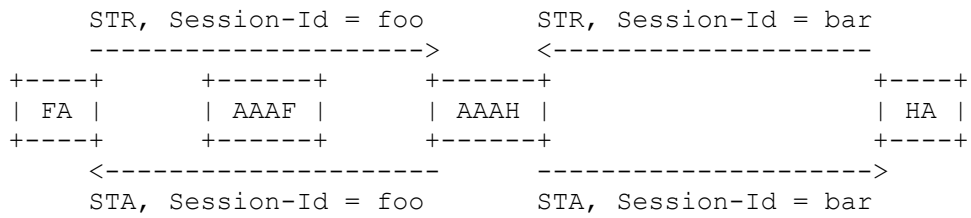

Figure 10 : Terminaison de session et identifiants de session

Lorsque il désalloue toutes les ressources du nœud mobile, le serveur Diameter de rattachement (et le serveur Diameter étranger dans le cas d'un HA alloué dans le réseau étranger) DOIT détruire toutes les clés de session qui pourraient être encore valides.

Dans le cas où l'AAAF souhaite terminer une session, son message Demande d'interruption de session (ASR, *Abort-Session-Request*) [RFC3588] DEVRAIT être envoyé au FA. De même, l'AAAH DEVRAIT envoyer son message à l'agent de rattachement.

5. Valeurs des codes de commandes

Cette section définit les codes de commandes [RFC3588] qui DOIVENT être acceptés par toutes les mises en œuvre de Diameter qui se conforment à la présente spécification. Les codes de commandes suivants sont définis :

Nom de commande	Abréviation	Code	Paragraphe
AA-Mobile-Node-Request	AMR	260	5.1
AA-Mobile-Node-Answer	AMA	260	5.2
Home-Agent-MIP-Request	HAR	262	5.3
Home-Agent-MIP-Answer	HAA	262	5.4

5.1 AA-Mobile-Node-Request

La demande de nœud mobile AA (AMR, *AA-Mobile-Node-Request*), indiquée par le réglage du champ Code de commande à 260 et le bit 'R' établi dans le champ Fanions de commandes, est envoyée par un accompagnateur (c'est-à-dire, l'agent étranger) agissant comme client Diameter, à un AAAF afin de demander l'authentification et l'autorisation d'un nœud mobile. L'agent étranger (ou l'agent de rattachement dans le cas d'un nœud mobile colocalisé) utilise les informations trouvées dans la demande d'enregistrement pour construire les AVP suivantes, à inclure au titre de l'AMR :

- Adresse de rattachement (AVP MIP-Mobile-Node-Address)
- Adresse de l'agent de rattachement (AVP MIP-Home-Agent-Address)
- NAI du nœud mobile (AVP User-Name [RFC3588])
- Demande de clé MH-HA (AVP MIP-Feature-Vector)Demande de clé MN-FA (AVP MIP-Feature-Vector)
- Extension d'authentification MN-AAA (AVP MIP-MN-AAA-Auth)
- Extension Défi d'agent étranger (AVP MIP-FA-Challenge)
- NAI d'agent de rattachement (AVP MIP-Home-Agent-Host)
- NAI de serveur AAA de rattachement (AVP Destination-Host [RFC3588])
- SPI d'agent de rattachement à agent étranger (AVP MIP-HA-to-FA-SPI)

Si l adresse de rattachement du nœud mobile est zéro, l'agent étranger ou de rattachement NE DOIT PAS inclure d'AVP MIP-Mobile-Node-Address dans l'AMR. Si l'adresse de l'agent de rattachement est zéro ou toute de uns, l'AVP MIP-Home-

Agent-Address NE DOIT PAS être présente dans l'AMR.

Si un agent de rattachement est utilisé dans un réseau visité, le AAAF PEUT établir le fanion Foreign-Home-Agent-Available dans l'AVP MIP-Feature-Vector dans le message AMR pour indiquer qu'il veut allouer un agent de rattachement dans le domaine visité.

Si l adresse de rattachement du nœud mobile est toute de uns, l'agent étranger ou de rattachement DOIT inclure une AVP MIP-Mobile-Node-Address réglée toute à un.

Si le nœud mobile inclut le NAI de l'agent de rattachement et le NAI du serveur AAA de rattachement [RFC3846], l'agent étranger DOIT inclure l'AVP MIP-Home-Agent-Host et l'AVP Destination-Host dans l'AMR.

Format de message

```
<AA-Mobile-Node-Request> ::= < En-tête Diameter : 260, REQ, PXY >
                             < Session-ID >
                             { Auth-Application-Id }
                             { User-Name }
                             { Destination-Realm }
                             { Origin-Host }
                             { Origin-Realm }
                             { MIP-Reg-Request }
                             { MIP-MN-AAA-Auth }
                             [ Acct-Multi-Session-Id ]
                             [ Destination-Host ]
                             [ Origin-State-Id ]
                             [ MIP-Mobile-Node-Address ]
                             [ MIP-Home-Agent-Address ]
                             [ MIP-Feature-Vector ]
                             [ MIP-Originating-Foreign-AAA ]
                             [ Authorization-Lifetime ]
                             [ Auth-Session-State ]
                             [ MIP-FA-Challenge ]
                             [ MIP-Candidate-Home-Agent-Host ]
                             [ MIP-Home-Agent-Host ]
                             [ MIP-HA-to-FA-SPI ]
                            * [ Proxy-Info ]
                            * [ Route-Record ]
                            * [ AVP ]
```

5.2 AA-Mobile-Node-Answer

La réponse de nœud mobile AA (AMA, *AA-Mobile-Node-Answer*), indiquée par le réglage à 260 du champ Code de commande et le bit 'R' à zéro dans le champ Fanions de commandes, est envoyée par l'AAAH en réponse au message AA-Mobile-Node-Request. Le nom d'utilisateur PEUT être inclus dans l'AMA si il est présent dans l'AMR. L'AVP Result-Code PEUT contenir une des valeurs définies à la Section 6, en plus des valeurs définies dans la [RFC3588].

Un message AMA avec l'AVP Result-Code réglé à DIAMETER_SUCCESS DOIT inclure l'AVP MIP-Home-Agent-Address, DOIT inclure l'AVP MIP-Mobile-Node-Address, et inclure l'AVP MIP-Reg-Reply si et seulement si le bit Co-Located-Mobile-Node n'était pas établi dans l'AVP MIP-Feature-Vector. L'AVP MIP-Home-Agent-Address contient l'agent de rattachement alloué au nœud mobile, tandis que l'AVP MIP-Mobile-Node-Address contient l'adresse de rattachement qui a été allouée. Le message AMA DOIT contenir les MIP-FA-to-HA-MSA et MIP-FA-to-MN-MSA si elles étaient demandées dans l'AMR et étaient présentes dans la HAR. Les AVP MIP-MN-to-HA-MSA et MIP-HA-to-MN-MSA DOIVENT être présentes si les clés de session étaient demandées dans l'AMR et si le bit Co-Located-Mobile-Node était établi dans l'AVP MIP-Feature-Vector.

Format de message

```
<AA-Mobile-Node-Answer> ::= < En-tête Diameter : 260, PXY >
                            < Session-Id >
                            { Auth-Application-Id }
                            { Result-Code }
```

```
                { Origin-Host }
                { Origin-Realm }
                [ Acct-Multi-Session-Id ]
                [ User-Name ]
                [ Authorization-Lifetime ]
                [ Auth-Session-State ]
                [ Error-Message ]
                [ Error-Reporting-Host ]
                [ Re-Auth-Request-Type ]
                [ MIP-Feature-Vector ]
                [ MIP-Reg-Reply ]
                [ MIP-MN-to-FA-MSA ]                    [ MIP-MN-to-HA-MSA ]
                [ MIP-FA-to-MN-MSA ]
                [ MIP-FA-to-HA-MSA ]
                [ MIP-HA-to-MN-MSA ]
                [ MIP-MSA-Lifetime ]
                [ MIP-Home-Agent-Address ]
                [ MIP-Mobile-Node-Address ]
               * [ MIP-Filter-Rule ]
                [ Origin-State-Id ]
               * [ Proxy-Info ]
               * [ AVP ]
```

5.3 Home-Agent-MIP-Request

Le AAA envoie la demande MIP d'agent de rattachement (HAR, *Home-Agent-MIP-Request*), indiquée par le réglage du champ Code de commande à 262 et le bit 'R' établi dans le champ Fanions de commandes, à l'agent de rattachement. Si l'agent de rattachement est à allouer dans un réseau étranger, la HAR est produite par le AAAH et transmise par le AAAF au HA si aucun serveur de redirection n'est impliqué. Si il y en a, la HAR est envoyée directement au HA via une association de sécurité. Si le message HAR ne comporte pas d'AVP MIP-Mobile-Node-Address, la demande d'enregistrement a 0.0.0.0 comme adresse de rattachement, et si la HAR est traitée avec succès, l'agent de rattachement DOIT allouer l'adresse du nœud mobile. Si, par ailleurs, le serveur AAA local de l'agent de rattachement alloue l'adresse de rattachement du nœud mobile, le serveur AAA local DOIT inclure l'adresse allouée dans une AVP MIP-Mobile-Node-Address.

Lorsque l'utilisation de clés de session est demandée par le nœud mobile, le AAAH DOIT les créer et les inclure dans le message HAR. Lorsque une clé de session FA-HA est demandée, elle sera créée et distribuée par le serveur AAAH.

Format de message

```
<Home-Agent-MIP-Request> ::= < En-tête Diameter : 262, REQ, PXY >
                < Session-Id >
                { Auth-Application-Id }
                { Authorization-Lifetime }
                { Auth-Session-State }
                { MIP-Reg-Request }
                { Origin-Host }
                { Origin-Realm }
                { User-Name }
                { Destination-Realm }
                { MIP-Feature-Vector }
                [ Destination-Host ]
                [ MIP-MN-to-HA-MSA ]
                [ MIP-MN-to-FA-MSA ]
                [ MIP-HA-to-MN-MSA ]
                [ MIP-HA-to-FA-MSA ]
                [ MIP-MSA-Lifetime ]
                [ MIP-Originating-Foreign-AAA ]
                [ MIP-Mobile-Node-Address ]
                [ MIP-Home-Agent-Address ]
               * [ MIP-Filter-Rule ]
                [ Origin-State-Id ]
```

* [Proxy-Info]
* [Route-Record]
* [AVP]

5.4 Home-Agent-MIP-Answer

En réponse à une Home-Agent-MIP-Request, l'agent de rattachement envoie la réponse MIP d'agent de rattachement (HAA, *Home-Agent-MIP-Answer*), indiquée par le réglage du champ Code de commande à 262 et le bit 'R' à zéro dans le champ Fanions de commandes, à son serveur AAA local. Le nom d'utilisateur PEUT être inclus dans la HAA si il est présent dans la HAR. Si l'agent de rattachement a alloué une adresse de rattachement au nœud mobile, l'adresse DOIT être incluse dans l'AVP MIP-Mobile-Node-Address. L'AVP Result-Code PEUT contenir une des valeurs définies à la Section 6 au lieu des valeurs définies dans la [RFC3588].

Format de message

<Home-Agent-MIP-Answer> ::= < Diameter Header: 262, PXY >
< Session-Id >
{ Auth-Application-Id }
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[Acct-Multi-Session-Id]
[User-Name]
[Error-Reporting-Host]
[Error-Message]
[MIP-Reg-Reply]
[MIP-Home-Agent-Address]
[MIP-Mobile-Node-Address]
[MIP-FA-to-HA-SPI]
[MIP-FA-to-MN-SPI]
[Origin-State-Id]
* [Proxy-Info]
* [AVP]

6. Valeur des AVP de code de résultat

Cette section définit les valeurs des nouveaux codes de résultat [RFC3588] qui DOIVENT être prises en charge par toutes les mises en œuvre Diameter qui se conforment à la présente spécification.

6.1 Défaillances transitoires

Les erreurs de la catégorie des défaillances transitoires sont utilisées pour informer un homologue que la demande n'a pas pu être satisfaite au moment de sa réception, mais qu'il serait possible qu'elle soit satisfaite à l'avenir.

DIAMETER_ERROR_MIP_REPLY_FAILURE : 4005
Ce code d'erreur est utilisé par l'agent de rattachement lorsque le traitement de la demande d'enregistrement a échoué.

DIAMETER_ERROR_HA_NOT_AVAILABLE : 4006
Ce code d'erreur est utilisé pour informer l'agent étranger que l'agent de rattachement demandé ne peut pas être alloué au nœud mobile pour le moment. L'agent étranger DOIT retourner une réponse d'enregistrement IPv4 mobile au nœud mobile avec un code d'erreur approprié.

DIAMETER_ERROR_BAD_KEY : 4007
Ce code d'erreur est utilisé par l'agent de rattachement pour indiquer au serveur Diameter local que la clé générée est invalide.

DIAMETER_ERROR_MIP_FILTER_NOT_SUPPORTED : 4008
Ce code d'erreur est utilisé par un agent de mobilité pour indiquer au serveur Diameter de rattachement que les règles de filtrage de paquet demandées ne peuvent pas être prises en charge.

6.2 Défaillances permanentes

Les erreurs qui entrent dans la catégorie des défaillances permanentes sont utilisées pour informer l'homologue que la demande a échoué et NE DEVRAIT PAS être tentée à nouveau.

DIAMETER_ERROR_NO_FOREIGN_HA_SERVICE : 5024
Cette erreur est utilisée par l'AAAF pour informer l'AAAH que l'allocation d'un agent de rattachement dans le domaine étranger n'est pas permise en ce moment.

DIAMETER_ERROR_END_TO_END_MIP_KEY_ENCRYPTION : 5025
Cette erreur est utilisée par l'AAAF/AAAH pour informer l'homologue que les clés de session IPv4 mobile demandées n'ont pas pu être livrées via une association de sécurité.

7. AVP obligatoires

Le tableau suivant décrit les AVP Diameter définies dans l'application IPv4 mobile, leurs valeurs de code d'AVP, types, et valeurs de fanions possibles, et si l'AVP PEUT être chiffrée.
Note du traducteur : Le texte suivant figurait dans la RFC3588 devant le même tableau ; cela explique le "P" de la colonne PEUT mais laisse le mystère entier pour le "V" de la colonne suivante, le "M" paraissant devoir être interprété comme "MUST". "Pour le générateur d'un message Diameter, "chiffrer" signifie que si un message contenant cette AVP doit être envoyé via un agent Diameter (mandataire, redirection ou relais) alors le message NE DOIT être envoyé que si il y a la sécurité de bout en bout entre le générateur et le receveur et si la protection de l'intégrité/confidentialité est offerte pour cette AVP OU si le générateur a une configuration de confiance locale qui indique que la sécurité de bout en bout n'est pas nécessaire. De même, pour le générateur d'un message Diameter, un "P" dans la colonne "PEUT" signifie que si un message contenant cette AVP doit être envoyé via un agent Diameter (mandataire, redirection ou relais) le message NE DOIT être envoyé que si il y a la sécurité de bout en bout entre le générateur et le receveur ou si le générateur a une configuration de confiance locale qui indique que le sécurité de bout en bout n'est pas nécessaire."

Pour des contraintes d'espace, on utilise la forme abrégée DiamIdent pour représenter DiameterIdentity.

				Règles des fanions d'AVP			
Nom d'attribut	Code d'AVP	§	Type de valeur	DOIT	PEUT	NE DOIT PAS	PEUT chiffrer
MIP-Reg-Request	320	7.1	OctetString	M	P	V	oui
MIP-Reg-Reply	321	7.2	OctetString	M	P	V	oui
MIP-MN-AAA-Auth	322	7.6	Grouped	M	P	V	oui
MIP-Mobile-Node-Address	333	7.3	Address	M	P	V	oui
MIP-Home-Agent-Address	334	7.4	Address	M	P	V	oui
MIP-Candidate-Home-Agent-Host	336	7.9	DiamIdent	M	P	V	non
MIP-Feature-Vector	337	7.5	Unsigned32	M	P	V	oui
MIP-Auth-Input-Data-Length	338	7.6.2	Unsigned32	M	P	V	oui
MIP-Authenticator-Length	339	7.6.3	Unsigned32	M	P	V	oui
MIP-Authenticator-Offset	340	7.6.4	Unsigned32	M	P	V	oui
MIP-MN-AAA-SPI	341	7.6.1	Unsigned32	M	P	V	oui
MIP-Filter-Rule	342	7.8	IPFilterRule	M	P	V	oui
MIP-FA-Challenge	344	7.7	OctetString	M	P	V	oui
MIP-Originating-Foreign-AAA	347	7.10	Grouped	M	P	V	oui
MIP-Home-Agent-Host	348	7.11	DiamIdent	M	P	V	non

7.1 AVP MIP-Reg-Request

L'AVP MIP-Reg-Request (Code d'AVP 320) est du type OctetString *(chaîne d'octets)* et contient la demande d'enregistrement IPv4 mobile [RFC3344] envoyée par le nœud mobile à l'agent étranger.

7.2 AVP MIP-Reg-Reply

L'AVP MIP-Reg-Reply (Code d'AVP 321) est du type OctetString et contient la réponse d'enregistrement IPv4 mobile [RFC3344] envoyée par l'agent de rattachement à l'agent étranger.

7.3 AVP MIP-Mobile-Node-Address

L'AVP MIP-Mobile-Node-Address (Code d'AVP 333) est du type Address et contient l'adresse IP de rattachement du nœud mobile.

7.4 AVP MIP-Home-Agent-Address

L'AVP MIP-Home-Agent-Address (code d'AVP 334) est du type Address et contient l'adresse IP d'agent de rattachement du nœud mobile.

7.5 AVP MIP-Feature-Vector

L'AVP MIP-Feature-Vector (code d'AVP 337) est du type Unsigned32 et est ajoutée avec les valeurs de fanion réglées par l'agent étranger ou par le AAAF possédé par le même domaine administratif que l'agent étranger. L'agent étranger DEVRAIT inclure l'AVP MIP-Feature-Vector au sein du message AMR qu'il envoie à l'AAAF.

Les valeurs de fanion actuellement définies incluent les suivantes :
1 : Mobile-Node-Home-Address-Requested (adresse de rattachement du nœud mobile demandée)
2 : Home-Address-Allocatable-Only-in-Home-Realm (adresse de rattachement allouable seulement dans le domaine de rattachement)
4 : Home-Agent-Requested (agent de rattachement demandé)
8 : Foreign-Home-Agent-Available (agent de rattachement étranger disponible)
16 : MN-HA-Key-Request (demande de clé MN-HA)
32 : MN-FA-Key-Request (demande de clé MN-FA)
64 : FA-HA-Key-Request (demande de clé FA-HA)
128 : Home-Agent-In-Foreign-Network (agent de rattachement dans réseau étranger)
256 : Co-Located-Mobile-Node (nœud mobile colocalisé)

Les fanions sont établis selon les règles suivantes.

Si le nœud mobile inclut une adresse de rattachement valide (c'est-à-dire, qui n'est pas égale à 0.0.0.0 ou 255.255.255.255) dans sa demande d'enregistrement, l'agent étranger règle le fanion Mobile-Node-Home-Address-Requested à zéro dans l'AVP MIP-Feature-Vector.

Si le nœud mobile règle le champ Agent de rattachement égal à 255.255.255.255 dans sa demande d'enregistrement, l'agent étranger règle les deux fanions Home-Agent-Requested et Home-Address-Allocatable-Only-in-Home-Realm à un dans l'AVP MIP-Feature-Vector.

Si le nœud mobile règle le champ Agent de rattachement égal à 0.0.0.0 dans sa demande d'enregistrement, l'agent étranger règle le fanion Home-Agent-Requested à un et met à zéro le fanion Home-Address-Allocatable-Only-in-Home-Realm dans l'AVP MIP-Feature-Vector.

Chaque fois que l'agent étranger règle le fanion Mobile-Node-Home-Address-Requested ou Home-Agent-Requested à un, il DOIT régler le fanion MN-HA-Key-Request à un. Le fanion MN-HA-Key-Request est aussi réglé à un si le nœud mobile inclut une extension "Demande généralisée de nom occasionnel de génération de clé MN-HA" [RFC3957], avec le sous type réglé à AAA.

Si le nœud mobile inclut une "Extension généralisée Demande de nom occasionnel de génération de clé MN-FA" [RFC3957] avec le sous type AAA (1) dans sa demande d'enregistrement, l'agent étranger règle le fanion MN-FA-Key-Request à un dans l'AVP MIP-Feature-Vector.

Si le nœud mobile demande un agent de rattachement dans le réseau étranger soit en réglant le champ Adresse de rattachement tout à un, soit en spécifiant un agent de rattachement dans le réseau étranger, et si l'AAAF autorise la demande, le AAAF DOIT régler le bit Home-Agent-In-Foreign-Network à un.

Si le AAAF veut et est capable d'allouer un agent de rattachement dans le réseau étranger, le AAAF règle le fanion Foreign-Home-Agent-Available à un.

Si l'agent de rattachement reçoit une demande d'enregistrement du nœud mobile indiquant que le MN agit comme nœud mobile colocalisé, l'agent de rattachement règle le bit Co-Located-Mobile-Node à un.

Si la politique locale de l'agent étranger lui permet de recevoir des clés de session AAA et si il n'a aucune clé FA-HA

existante avec l'agent de rattachement, l'agent étranger PEUT établir le fanion FA-HA-Key-Request.

L'agent étranger NE DOIT PAS établir les deux fanions Foreign-Home-Agent-Available et Home-Agent-In-Foreign-Network à un.

Lorsque le AAAF reçoit le message AMR, il DOIT d'abord vérifier que l'envoyeur était un agent étranger autorisé. Le AAAF effectue alors toutes les actions indiquées par le réglage des fanions d'AVP MIP-Feature-Vector. Le AAAF PEUT ensuite établir des fanions supplémentaires. Seul le AAAF peut établir à un les fanions Foreign-Home-Agent-Available et Home-Agent-In-Foreign-Network. Ceci est fait conformément aux politiques administratives locales. Lorsque l'AAAF a terminé le réglage des fanions supplémentaires conformément à sa politique locale, le AAAF transmet alors l'AMR avec l'AVP MIP-Feature-Vector éventuellement modifiée au AAAH.

7.6 AVP MIP-MN-AAA-Auth

L'AVP MN-AAA-Auth (code d'AVP 322) est du type Grouped et contient des données auxiliaires pour simplifier le traitement des données d'authentification dans la demande d'enregistrement IPv4 mobile [RFC3344], [RFC3012] par le serveur AAA cible. Sa valeur a la grammaire ABNF suivante :

```
MIP-MN-AAA-Auth ::= < En-tête d'AVP : 322 >
                    { MIP-MN-AAA-SPI }
                    { MIP-Auth-Input-Data-Length }
                    { MIP-Authenticator-Length }
                    { MIP-Authenticator-Offset }
                    * [ AVP ]
```

7.6.1 AVP MIP-MN-AAA-SPI

L'AVP MIP-MN-AAA-SPI (code d'AVP 341) est du type Unsigned32 et indique la MSA par laquelle le serveur AAA ciblé (AAAH) devrait tenter de valider l'authentifiant calculé par le nœud mobile sur les données de la demande d'enregistrement.

7.6.2 MIP-Auth-Input-Data-Length

L'AVP MIP-Auth-Input-Data-Length (code d'AVP 338) est du type Unsigned32 et contient la longueur, en octets, des données de la demande d'enregistrement (portion données de l'AVP MIP-Reg-Request) qui devraient être utilisées comme entrée à l'algorithme, comme indiqué par l'AVP MN-AAA-SPI, utilisée pour déterminer si les données d'authentifiant fournies par le nœud mobile sont valides.

7.6.3 AVP MIP-Authenticator-Length

L'AVP MIP-Authenticator-Length (code d'AVP 339) est du type Unsigned32 et contient la longueur de l'authentifiant à valider par le serveur AAA ciblé (c'est-à-dire, AAAH).

7.6.4 AVP MIP-Authenticator-Offset

L'AVP MIP-Authenticator-Offset (code d'AVP 340) est du type Unsigned32 et contient le décalage dans les données de la demande d'enregistrement, de l'authentifiant à valider par le serveur AAA ciblé (c'est-à-dire, AAAH).

7.7 AVP MIP-FA-Challenge

L'AVP MIP-FA-Challenge (code d'AVP 344) est du type OctetString et contient le défi annoncé par l'agent étranger au nœud mobile. Cette AVP DOIT être présente dans l'AMR si le nœud mobile utilise l'algorithme de calcul MN-AAA de style RADIUS [RFC3012].

7.8 AVP MIP-Filter-Rule

L'AVP MIP-Filter-Rule (code d'AVP 342) est du type IPFilterRule et donne les règles de filtrage qui doivent être configurées sur l'agent étranger ou de rattachement pour l'usager. Les règles de filtrage de paquet sont réglées par le AAAH en ajoutant une ou plusieurs AVP MIP-Filter-Rule dans la HAR si c'est destiné à l'agent de rattachement et/ou dans l'AMA si c'est destiné à l'agent étranger.

7.9 AVP MIP-Candidate-Home-Agent-Host

L'AVP MIP-Candidate-Home-Agent-Host (code d'AVP 336) est du type DiameterIdentity et contient l'identité d'un agent de rattachement dans le réseau étranger que l'AAAF propose d'allouer de façon dynamique au nœud mobile.

7.10 AVP MIP-Originating-Foreign-AAA

L'AVP MIP-Originating-Foreign-AAA (code d'AVP 347) est du type Grouped et contient l'identité de l'AAAF, qui produit la AMR au AAAH. L'AVP MIP-Originating-Foreign-AAA DOIT être utilisée seulement dans le cas où l'agent de rattachement est ou peut être alloué dans un domaine étranger. Si l'AVP MIP-Originating-Foreign-AAA est présent dans l'AMR, le AAAH DOIT la copier dans la HAR.

```
MIP-Originating-Foreign-AAA ::= < En-tête d'AVP : 347 >
                                 { Origin-Realm }
                                 { Origin-Host }
                                 * [ AVP ]
```

7.11 AVP MIP-Home-Agent-Host

L'AVP MIP-Home-Agent-Host (code d'AVP 348) est du type Grouped et contient l'identité de l'agent de rattachement alloué. Si l'AVP MIP-Home-Agent-Host est présent dans l'AMR, le AAAH DOIT la copier dans la HAR.

```
MIP-Home-Agent-Host ::= < En-tête d'AVP : 348 >
                         { Destination-Realm }
                         { Destination-Host }
                         * [ AVP ]
```

8. Distribution de clé

Le nœud mobile et les agents de mobilité utilisent des clés de session (c'est-à-dire, les clés de session MN-FA, FA-HA, et MN-HA) pour calculer les extensions d'authentification appliquées aux messages d'enregistrement MIP, comme défini dans la [RFC3344]. Si des clés de session sont demandées, le AAAH DOIT retourner les clés et les noms occasionnels après la réussite de l'authentification et l'autorisation du nœud mobile.

Les valeurs de SPI sont utilisées comme identifiants de clés, et chaque clé de session a sa propre valeur de SPI ; les nœuds qui partagent une clé peuvent avoir plusieurs SPI différents se référant tous à la même clé. Dans tous les cas, l'entité qui reçoit une extension d'authentification (c'est-à-dire, qui vérifie l'extension d'authentification) fournit à l'entité qui envoie l'extension d'authentification (c'est-à-dire, qui calcule l'extension d'authentification) la valeur du SPI à utiliser pour ce calcul. Noter que les clés dans ce modèle sont symétriques en ce qu'elles sont utilisées dans les deux directions, même si les SPI n'ont pas à être symétriques.

Le nœud mobile alloue les SPI à utiliser dans les associations de sécurité de mobilité FA-MN et HA-MN, via les extensions de demande de clé AAA IPv4 mobile [RFC3957]. L'agent de rattachement alloue les SPI pour les associations de sécurité de mobilité MN-HA et FA-HA. L'agent étranger choisit les SPI pour les associations de sécurité de mobilité MN-FA et HA-FA.

Une fois distribués les clés de session et les noms occasionnels, les enregistrements IPv4 mobile suivants n'ont pas besoin d'invoquer l'infrastructure AAA jusqu'à ce que les clés arrivent à expiration. Comme exigé par IPv4 mobile, ces enregistrements DOIVENT inclure l'extension d'authentification MN-HA. De même,les enregistrements suivants DOIVENT aussi inclure l'extension d'authentification MN-FA si la clé de session MN-FA a été générée et distribuée par AAA. C'est aussi vrai pour l'utilisation ultérieure des extensions d'authentification FA-HA.

8.1 Durée de vie d'autorisation contre durée de vie de clé MIP

L'application IPv4 mobile Diameter utilise deux temporisateurs : l'AVP Durée de vie d'autorisation *(Authorization-Lifetime)* [RFC3588] et l'AVP Durée de vie de MSA MIP *(MIP-MSA-Lifetime)*.

La durée de vie d'autorisation contient le nombre de secondes avant que le nœud mobile doive produire une autre demande

d'enregistrement MIP. Le contenu de l'AVP Durée de vie d'autorisation correspond au champ Durée de vie dans l'en-tête MIP [RFC3344].

L'AVP MIP-MSA-Lifetime contient le nombre de secondes avant l'arrivée à expiration des clés de session destinées aux agents de mobilité et au nœud mobile. Une valeur de zéro indique l'infini (pas de fin de temporisation). Si ce n'est pas zéro, la valeur de l'AVP MIP-MSA-Lifetime DOIT être au moins égale à celle de l'AVP Durée de vie d'autorisation.

8.2 Nom occasionnel contre clé de session

Comme décrit au paragraphe 3.4, l'AAAH génère les clés de session et les transmet à l'agent de rattachement et à l'agent étranger. L'AAAH génère les noms occasionnels qui correspondent aux mêmes clés et les transmet au nœud mobile. Lorsque il est nécessaire de protéger les clés de session et les SPI d'agents Diameter qui ne sont pas de confiance, des mécanismes de sécurité de bout en bout comme TLS ou IPsec sont nécessaires pour éliminer tous les agents Diameter entre le FA ou HA et le AAAH, comme mentionné ci-dessus.

Dans la [RFC3957], les associations de sécurité de mobilité sont établies via des noms occasionnels transmis au nœud mobile via IPv4 mobile. Pour fournir les noms occasionnels, le AAAH doit générer une valeur aléatoire [RFC4086] d'au moins 128 bits [RFC3957]. Le nœud mobile utilise alors le nom occasionnel pour déduire les clés de session MN-HA et MN-FA.

Plus de détails sur les procédures de création de clé de session MN-HA et MN-FA se trouvent dans la [RFC3957].

L'algorithme de hachage utilisé par le nœud mobile pour construire la clé de session doit être la même que celle utilisée par le AAAH dans la procédure de génération de clé de session. Le AAAH indique donc l'algorithme utilisé ainsi que le nom occasionnel.

La clé de session FA-HA et HA-FA est partagée entre le FA et HA. Le AAAH génère une valeur aléatoire [RFC4086] d'au moins 128 bits à utiliser comme cette clé de session.

Voir à la Section 9 les détails sur le format des AVP utilisées pour transporter les clés de session.

8.3 Distribution de clé de session de rattachement mobile

Si le nœud mobile n'a pas une clé de session MN-HA, le AAAH sera probablement la seule entité de confiance disponible au nœud mobile. Donc, le AAAH devra générer la clé de session MN-HA.

La distribution de la clé HA-MN (de session) au HA est spécifiée aux paragraphes 1.2 et 3.4. Le HA et l'AAAH établissent une association de sécurité (IPsec ou TLS) et transportent la clé sur elle. Si aucune association de sécurité n'existe entre l'AAAH et l'agent de rattachement et si on ne peut pas en établir une, le AAAH DOIT retourner une AVP Code de résultat avec DIAMETER_ERROR_END_TO_END_MIP_KEY_ENCRYPTION *(erreur Diameter de chiffrement de clé MIP de bout en bout)*.

Le AAAH doit aussi s'arranger pour que la clé soit livrée au nœud mobile. Malheureusement, le AAAH ne connaît que les messages et les AVP Diameter, et le nœud mobile ne connaît que les messages et extensions IPv4 mobile [RFC3344]. À cette fin, AAAH inclut l'AVP nom occasionnel MN-HA MIP dans une AVP MIP-MN-to-HA-MSA, qui est ajoutée à la HAR (pour IPv4 mobile de style adresse d'entretien par FA) ou à l'AMA (pour les messages IPv4 mobile colocalisé de style adresse d'entretien) et délivrée soit à un agent de rattachement local, soit à un agent de rattachement dans le réseau visité. Noter que le nœud mobile va utiliser le nom occasionnel pour créer la clé de session MN-HA en utilisant la clé MN-AAA qu'il partage avec le AAAH [RFC3957]. Le AAAH doit s'appuyer sur l'agent de rattachement (qui comprend aussi Diameter) pour transférer le nom occasionnel dans une extension IPv4 mobile "réponse généralisée de nom occasionnel de génération de clé MH-HA" [RFC3957] dans le message de réponse d'enregistrement. Le HA inclut les SPI proposés par le nœud mobile et l'agent de rattachement dans l'extension "demande généralisée de nom occasionnel de génération de clé MH-HA". L'agent de rattachement peut formater correctement le message de réponse et les extensions pour une livraison finale au nœud mobile. La réponse d'enregistrement résultante est ajoutée à l'AVP MIP-Reg-Reply de la HAA.

Le AAAH analyse le message HAA, le transforme en message AMA contenant une AVP MIP-Reg-Reply, et envoie le message AMA à l'agent étranger. L'agent étranger utilise alors cette AVP pour recréer un message de réponse d'enregistrement contenant l'extension "réponse généralisée de nom occasionnel de génération de clé MH-HA" pour la livrer au nœud mobile.

En résumé, le AAAH génère le nom occasionnel MN-HA, qui est ajouté à l'AVP MIP-MN-to-HA-MSA AVP, et une clé de

session, qui est ajoutée à l'AVP MIP-HA-to-MN-MSA. Ces AVP sont livrées à l'agent de rattachement dans des messages HAR ou AMA. L'agent de rattachement conserve la clé de session pour son propre usage et copie le nom occasionnel de l'AVP MIP-MN-to-HA-MSA dans l'extension "réponse généralisée de nom occasionnel de génération de clé MH-HA", qui est ajouté au message Réponse d'enregistrement IPv4 mobile. Ce message de réponse d'enregistrement DOIT aussi inclure l'extension d'authentification HA-MN, qui est créée en utilisant la clé de session HA-MN nouvellement créée. L'agent de rattachement inclut alors le message de réponse d'enregistrement et les extensions dans une AVP MIP-Reg-Reply comme partie du message HAA à renvoyer au serveur AAA.

La clé déduite par le MN du nom occasionnel de session MN-HA est identique à la clé de session HA-MN fournie au HA.

8.4 Distribution de clé de session de mobile étranger

Le nom occasionnel de session MN-FA est aussi généré par l'AAAH (sur demande) et ajouté à l'AVP MIP-MN-to-FA-MSA, qui est ajoutée à la HAR et copiée par l'agent de rattachement dans une extension "réponse généralisée de nom occasionnel de génération de clé MN-FA" [RFC3957] du message de réponse d'enregistrement IPv4 mobile. Le HA inclut aussi les SPI proposés par le nœud mobile et l'agent étranger dans l'extension "demande généralisée de nom occasionnel de génération de clé MN-FA". Le AAAH inclut la clé de session FA-MN dans l'AVP MIP-FA-to-MN-MSA dans l'AMA, pour qu'elle soit utilisée par l'agent étranger dans le calcul de l'extension d'authentification FA-MN.

La clé déduite par le MN du nom occasionnel de session MN-FA est identique à la clé de session FA-MN fournie au FA.

8.5 Distribution de la clé de session de rattachement étranger

Si l'agent étranger demande une clé de session FA-HA, il inclut aussi une AVP MIP-HA-to-FA-SPI dans l'AMR pour porter le SPI à utiliser à cette fin par l'agent de rattachement. Le AAAH génère la clé de session FA-HA, qui est identique à la clé de session HA-FA, et distribue cela au HA et au FA sur leurs associations de sécurité respectives en utilisant les AVP MIP-HA-to-FA-MSA et MIP-FA-to-HA-MSA. Le HA porte le SPI que le FA DOIT utiliser dans la HAA ; ceci est similaire à la façon dont le FA porte le SPI que le HA DOIT utiliser dans l'AMR. Le AAAH inclut ultérieurement ces SPI dans les AVP, respectivement, MIP-FA-HA-MSA et MIP-HA-FA-MSA, avec la clé de session. Voir aux Figures 2, 3, 4, et 6 les messages impliqués.

Noter que si plusieurs MN sont enregistrés sur la même paire de FA et HA, plusieurs associations de sécurité de mobilité seront alors distribuées. Cependant, une seule est nécessaire pour protéger le trafic de contrôle IP mobile entre FA et HA. Cela crée un niveau inacceptable d'état (c'est-à-dire, de mémoriser les deux SPI et la clé partagée pour chaque association de sécurité de mobilité FA-HA). Pour améliorer l'adaptabilité, le FA et le HA peuvent éliminer des associations de sécurité de mobilité FA-HA avant le moment où elles arriveraient réellement à expiration. Cependant, si une politique d'élimination appropriée n'est pas choisie, cela peut causer l'échec d'authentification de messages IP mobile en transit ou en attente dans des files d'attente.

Le FA DOIT toujours utiliser l'association de sécurité FA-HA qui a la dernière heure d'expiration lors du calcul des extensions d'authentification sur les messages sortants. Le FA PEUT éliminer des associations de sécurité de mobilité HA-FA 10 secondes après qu'une nouvelle association de sécurité de mobilité HA-FA arrive avec une heure d'expiration postérieure.

Le HA DEVRAIT utiliser l'association de sécurité de mobilité HA-FA qui a l'heure d'expiration la plus tardive lors du calcul des extensions d'authentification dans les messages sortants. Cependant, lorsque le HA reçoit une nouvelle association de sécurité de mobilité HA-FA avec une heure d'expiration postérieure, le HA DEVRAIT attendre 4 secondes que l'AMA soit transmise au FA avant d'utiliser la nouvelle association. Noter que le HA utilise toujours l'association de sécurité de mobilité provenant de la HAR lorsque il construit la réponse d'enregistrement IP mobile dans la HAA correspondante. Le HA PEUT éliminer une association de sécurité de mobilité FA-HA une fois qu'il a reçu un message authentifié par une association de sécurité de mobilité FA-HA avec une heure d'expiration postérieure.

9. AVP de distribution des clés

Le protocole IP mobile définit un ensemble d'associations de sécurité de mobilité partagées entre le nœud mobile, l'agent étranger, et l'agent de rattachement. Ces trois associations de sécurité mobile (MN-HA, MN-FA, et FA-HA) sont créées dynamiquement par l'AAAH et ont été précédemment décrites au paragraphe 3.4 et à la Section 8. Les serveurs AAA qui prennent en charge l'application IP mobile Diameter DOIVENT mettre en œuvre les AVP de distribution de clés définies dans le présent document.

Les noms des AVP de distribution de clés indiquent les deux entités qui partagent l'association de sécurité de mobilité. La première entité nommée dans le nom de l'AVP va utiliser l'association de sécurité de mobilité pour créer les extensions d'authentification en utilisant le SPI et la clé donnés. La seconde entité désignée dans le nom de l'AVP va utiliser l'association de sécurité de mobilité pour vérifier les extensions d'authentification des messages IP mobile reçus.

Par exemple, l'AVP MIP-MN-to-HA-MSA contient le nom occasionnel MN-HA, que le nœud mobile va utiliser pour déduire la clé MH-HA, et l'AVP MIP-HA-to-MN-MSA contient la clé MN-HA pour l'agent de rattachement. Noter que les associations de sécurité de mobilité sont unidirectionnelles ; cependant, cette application ne livre qu'une seule clé qui est partagée entre les deux associations de sécurité de mobilité unidirectionnelles qui existent entre les deux homologues. Les problèmes de sécurité relatifs à l'utilisation de la même clé dans chaque direction sont examinés à la Section 13. Les SPI sont cependant uniques pour chaque association de sécurité unidirectionnelle et sont choisis par l'homologue qui va recevoir les messages IP mobile authentifiés avec cette association de sécurité.

Le tableau qui suit décrit l'AVP Diameter définie dans l'application IP mobile et ses valeurs de code d'AVP, types, et valeurs de fanion possibles.

				Règles de fanion d'AVP			
Nom d'attribut	**Code d'AVP**	Paragraphe	Type de valeur	DOIT	PEUT	NE DOIT PAS	PEUT chiffrer
MIP-FA-to-HA-SPI	318	9.11	Unsigned32	M	P	V	oui
MIP-FA-to-MN-SPI	319	9.10	Unsigned32	M	P	V	oui
MIP-HA-to-FA-SPI	323	9.14	Unsigned32	M	P	V	oui
MIP-MN-to-FA-MSA	325	9.5	Grouped	M	P	V	oui
MIP-FA-to-MN-MSA	326	9.1	Grouped	M	P	V	oui
MIP-FA-to-HA-MSA	328	9.2	Grouped	M	P	V	oui
MIP-HA-to-FA-MSA	329	9.3	Grouped	M	P	V	oui
MIP-MN-to-HA-MSA	331	9.6	Grouped	M	P	V	oui
MIP-HA-to-MN-MSA	332	9.4	Grouped	M	P	V	oui
MIP-Nonce	335	9.12	OctetString	M	P	V	oui
MIP-Session-Key	343	9.7	OctetString	M	P	V	oui
MIP-Algorithm-Type	345	9.8	Enumerated	M	P	V	oui
MIP-Replay-Mode	346	9.9	Enumerated	M	P	V	oui
MIP-MSA-Lifetime	367	9.13	Unsigned32	M	P	V	oui

9.1 AVP MIP-FA-to-MN-MSA

L'AVP MIP-FA-to-MN-MSA (code d'AVP 326) est du type Grouped et contient la clé de session FA-MN. Cette AVP est convoyée au FA dans un message AMA. Le MN alloue le MIP-FA-to-MN-SPI. Le FA crée une extension d'authentification FA-MN en utilisant la clé de session et l'algorithme, et le MN vérifie cette extension en utilisant la même clé de session et algorithme. Le champ Données de cette AVP a la grammaire ABNF suivante :

```
MIP-FA-to-MN-MSA ::= < En-tête d'AVP : 326 >
                     { MIP-FA-to-MN-SPI }
                     { MIP-Algorithm-Type }
                     { MIP-Session-Key }
                    * [ AVP ]
```

9.2 AVP MIP-FA-to-HA-MSA

L'AVP MIP-FA-to-HA-MSA (code d'AVP 328) est du type Grouped et contient la clé de session FA-HA. Cette AVP est convoyée au FA dans un message AMA. Le HA alloue le MIP-FA-to-HA-SPI. Le FA crée l'extension d'authentification FA-HA en utilisant la clé de session et l'algorithme, et le HA vérifie cette extension en utilisant la même clé et algorithme. Le champ Données de cette AVP a la grammaire ABNF suivante :

```
MIP-FA-to-HA-MSA ::= < En-tête d'AVP : 328 >
                     { MIP-FA-to-HA-SPI }
                     { MIP-Algorithm-Type }
                     { MIP-Session-Key }
                    * [ AVP ]
```

9.3 AVP MIP-HA-to-FA-MSA

L'AVP MIP-HA-to-FA-MSA (code d'AVP 329) est du type Grouped et contient la clé de session de l'agent de rattachement, qui est partagée avec l'agent étranger. Cette AVP est convoyée au HA dans un message HAR. Le FA alloue le MIP-HA-to-FA-SPI. Le HA crée l'extension d'authentification HA-FA en utilisant la clé de session et l'algorithme, et le FA vérifie cette extension en utilisant la même clé de session et algorithme. Le champ Données de cette AVP a la grammaire ABNF suivante :

```
MIP-HA-to-FA-MSA ::= < En-tête d'AVP : 329 >
                     { MIP-HA-to-FA-SPI   }
                     { MIP-Algorithm-Type }
                     { MIP-Session-Key }
                    * [ AVP ]
```

9.4 AVP MIP-HA-to-MN-MSA

L'AVP MIP-HA-to-MN-MSA (code d'AVP 332) est du type Grouped, et contient la clé de session HA-MN. Cette AVP est convoyée au HA dans une HAR pour une adresse d'entretien de FA IPv4 mobile et dans une AMA pour une COA IPv4 mobile colocalisée. Le MN alloue le MIP-HA-to-MN-SPI. Le HA crée l'extension d'authentification HA-MN en utilisant la clé de session et l'algorithme, et le MN vérifie cette extension en utilisant la même clé et algorithme. Le champ d'AVP a la grammaire ABNF suivante :

```
MIP-HA-to-MN-MSA ::= < En-tête d'AVP : 332 >
                     { MIP-HA-to-MN-SPI   }
                     { MIP-Algorithm-Type }
                     { MIP-Replay-Mode }
                     { MIP-Session-Key }
                    * [ AVP ]
```

9.5 AVP MIP-MN-to-FA-MSA

L'AVP MIP-MN-to-FA-MSA (code d'AVP 325) est du type Grouped, et contient le nom occasionnel de session MN-FA, que le nœud mobile utilise pour déduire la clé de session MN-FA. Cette AVP est convoyée au HA dans un message HAR. Le FA alloue le MIP-MN-to-FA-SPI. Le MN crée l'extension d'authentification MN-FA en utilisant la clé de session et l'algorithme, et le FA vérifie cette extension en utilisant la même clé et algorithme.

L'agent de rattachement utilise cette AVP dans la construction de l'extension IP mobile "Réponse généralisée de nom occasionnel de génération de clé MN-FA" [RFC3957].

```
MIP-MN-to-FA-MSA ::= < En-tête d'AVP : 325 >
                     { MIP-MN-FA-SPI }
                     { MIP-Algorithm-Type }
                     { MIP-nom occasionnel }
                    * [ AVP ]
```

9.6 AVP MIP-MN-to-HA-MSA

L'AVP MIP-MN-to-HA-MSA (code d'AVP 331) est du type Grouped et contient le nom occasionnel de session MN-HA, que le nœud mobile utilise pour déduire la clé de session MN-HA. Cette AVP est convoyée au HA dans un message HAR pour l'adresse d'entretien de FA IPv4 mobile et dans une AMR pour une CoA IPv4 mobile colocalisée. Le HA alloue le MIP-MN-to-HA-SPI. Le MN crée l'extension d'authentification MN-FA en utilisant la clé de session et l'algorithme, et le HA vérifie cette extension en utilisant la même clé de session et algorithme.

L'agent de rattachement utilise cette AVP dans la construction de l'extension IP mobile "réponse généralisée de nom occasionnel de génération de clé MH-HA" [RFC3957].

```
MIP-MN-to-HA-MSA ::= < En-tête d'AVP : 331 >
                     { MIP-MN-HA-SPI }
                     { MIP-Algorithm-Type }
                     { MIP-Replay-Mode }
                     { MIP-nom occasionnel }
```

* [AVP]

9.7 AVP MIP-Session-Key

L'AVP MIP-Session-Key (code d'AVP 343) est du type OctetString et contient la clé de session pour l'extension d'authentification IPv4 mobile associée. Le HAAA choisit la clé de session.

9.8 AVP MIP-Algorithm-Type

L'AVP MIP-Algorithm-Type (code d'AVP 345) est du type Enumerated et contient l'identifiant d'algorithme pour l'extension d'authentification IPv4 mobile associée. Le HAAA choisit le type d'algorithme. Les valeurs suivantes sont actuellement définies :

2 : HMAC-SHA-1 [RFC2104]

9.9 MIP-Replay-Mode

L'AVP MIP-Replay-Mode (code d'AVP 346) est du type Enumerated et contient le mode de répétition de l'agent de rattachement pour authentifier le nœud mobile. Le HAAA choisit le mode de répétition.

Les valeurs suivantes sont acceptées (voir la [RFC3344] pour plus d'informations) :
1 : aucun
2 : horodatages
3 : noms occasionnels

9.10 AVP MIP-FA-to-MN-SPI

L'AVP MIP-FA-to-MN-SPI (code d'AVP 319) est du type Unsigned32, et contient l'indice de paramètres de sécurité (SPI, *Security Parameter Index*) que le FA et le MN utilisent pour se référer à l'association de sécurité de mobilité FA-MN. Le MN alloue le SPI, et il NE DOIT PAS avoir une valeur entre zéro (0) et 255, qui est l'espace de noms réservé défini dans la [RFC3344].

9.11 AVP MIP-FA-to-HA-SPI

L'AVP MIP-FA-to-HA-SPI (code d'AVP 318) est du type Unsigned32 et contient l'indice de paramètres de sécurité que FA et HA utilisent pour se référer à l'association de sécurité de mobilité FA-HA. Le HA alloue le SPI, et il NE DOIT PAS avoir une valeur entre zéro (0) et 255, qui est l'espace de noms réservé défini dans la [RFC3344].

9.12 AVP MIP-Nonce

L'AVP MIP-Nonce (code d'AVP 335) est du type OctetString et contient le nom occasionnel envoyé au nœud mobile pour l'extension d'authentification associée. Le nœud mobile suit les procédures de la [RFC3957] pour générer la clé de session utilisée pour authentifier les messages d'enregistrement IPv4 mobile. Le HAAA choisit le nom occasionnel.

9.13 AVP MIP-MSA-Lifetime

L'AVP MIP-MSA-Lifetime (code d'AVP 367) est du type Unsigned32 et représente la durée (en secondes) pendant laquelle la clé de session ou le nom occasionnel est valide. La clé de session ou le nom occasionnel associé, selon le cas, NE DOIT PAS être utilisé si la durée de vie est expirée ; si la durée de vie de la clé de session ou du nom occasionnel arrive à expiration alors que la session à laquelle il s'applique est toujours active, la clé de session ou nom occasionnel DOIT être changé ou la session d'association IPv4 mobile DOIT être terminée.

9.14 AVP MIP-HA-to-FA-SPI

L'AVP MIP-HA-to-FA-SPI (code d'AVP 323) est du type Unsigned32 et contient l'indice de paramètres de sécurité que HA et FA utilisent pour se référer à l'association de sécurité de mobilité HA-FA. Le FA alloue le SPI, et il NE DOIT PAS avoir une valeur entre zéro (0) et 255, qui est l'espace de noms réservé défini dans la [RFC3344].

10. AVP de comptabilité

10.1 Accounting-Input-Octets

L'AVP Accounting-Input-Octets (code d'AVP 363) est du type Unsigned64, et contient le nombre d'octets dans les paquets IP reçus de l'utilisateur. Cette AVP DOIT être incluse dans tous les messages Accounting-Request et PEUT être présente aussi dans les messages Accounting-Answer correspondants.

10.2 AVP Accounting-Output-Octets

L'AVP Accounting-Output-Octets (code d'AVP 364) est du type Unsigned64 et contient le nombre d'octets dans les paquets IP envoyés à l'utilisateur. Cette AVP DOIT être incluse dans tous les messages Accounting-Request et PEUT être présente aussi dans les messages Accounting-Answer correspondants.

10.3 AVP Acct-Session-Time

L'AVP Acct-Time (code d'AVP 46) est du type Unsigned32 et indique la longueur de la session actuelle en secondes. Cette AVP DOIT être incluse dans tous les messages Accounting-Request et PEUT être présente aussi dans les messages Accounting-Answer correspondants.

10.4 AVP Accounting-Input-Packets

L'AVP Accounting-Input-Packets (code d'AVP 365) est du type Unsigned64 et contient le nombre de paquets IP reçus de l'utilisateur. Cette AVP DOIT être incluse dans tous les messages Accounting-Request et PEUT être présente aussi dans les messages Accounting-Answer correspondants.

10.5 AVP Accounting-Output-Packets

L'AVP Accounting-Output-Packets (code d'AVP 366) est du type Unsigned64 et contient le nombre de paquets IP envoyés à l'utilisateur. Cette AVP DOIT être incluse dans tous les messages Accounting-Request et PEUT être présente aussi dans les messages Accounting-Answer correspondants.

10.6 AVP Event-Timestamp

L'AVP Event-Timestamp (code d'AVP 55) est du type Time et PEUT être incluse dans un message Accounting-Request pour enregistrer l'heure à laquelle cet événement s'est produit sur l'agent de mobilité, en secondes depuis le 1er janvier 1970, 00:00 UTC.

11. Tableaux d'occurrence des AVP

Les tableaux qui suivent présentent les AVP définies dans le présent document et leurs occurrences dans les messages Diameter. Noter que les AVP qui ne peuvent être présentes qu'au sein d'une AVP groupée ne sont pas représentées dans ce tableau.

Le tableau utilise les symboles suivants :
0 : l'AVP NE DOIT PAS être présente dans le message.
0+ : zéro, une ou plusieurs instances de l'AVP PEUVENT être présentes dans le message.
0 - 1 : zéro ou une instance de l'AVP PEUT être présente dans le message.
1 : une instance de l'AVP DOIT être présente dans le message.

11.1 Tableau des AVP de commande IP mobile

Le tableau de ce paragraphe se limite aux codes de commandes définis dans la présente spécification.

	Code de commande			
Nom d'attribut	**AMR**	**AMA**	**HAR**	**HAA**
Authorization-Lifetime	0-1	0-1	1	0

Auth-Application-Id	1	1	1	1
Auth-Session-State	0-1	0-1	1	0
Acct-Multi-Session-Id	0-1	0-1	0	0-1
Destination-Host	0-1	0	0-1	0
Destination-Realm	1	0	1	0
Error-Message	0	0-1	0	0-1
Error-Reporting-Host	0	0-1	0	0-1
MIP-Candidate-Home-Agent-Host	0-1	0	0-1	0
MIP-Home-Agent-Host	0-1	0	0-1	0
MIP-Originating-Foreign-AAA	0-1	0	0-1	0|
MIP-FA-Challenge	0-1	0	0	0|
MIP-FA-to-MN-MSA	0	0-1	0	0
MIP-FA-to-HA-MSA	0	0-1	0	0
MIP-HA-to-FA-MSA	0	0	0-1	0
MIP-HA-to-MN-MSA	0	0-1	0-1	0
MIP-MN-to-FA-MSA	0	0	0-1	0
MIP-MN-to-HA-MSA	0	0-1	0-1	0
MIP-FA-to-HA-SPI	0	0	0	0-1
MIP-HA-to-FA-SPI	0	0	0	0-1
MIP-FA-to-MN-SPI	0	0	0	0-1
MIP-MN-to-FA-SPI	0	0	0	0-1
MIP-HA-to-MN-SPI	0	0	0	0-1
MIP-MN-to-HA-SPI	0	0	0	0-1
MIP-Feature-Vector	0-1	0-1	1	0|
MIP-Filter-Rule	0	0+	0+	0|
MIP-Home-Agent-Address	0-1	0-1	0-1	0-1
MIP-MSA-Lifetime	0	0-1	0-1	0
MIP-MN-AAA-Auth	1	0	0	0
MIP-Mobile-Node-Address	0-1	0-1	0-1	0-1
MIP-Reg-Reply	0	0-1	0	0-1
MIP-Reg-Request	1	0	1	0
Origin-Host	1	1	1	1
Origin-Realm	1	1	1	1
Origin-State-Id	0-1	0-1	0-1	0-1
Proxy-Info	0+	0+	0+	0+
Redirect-Host	0	0+	0	0+
Redirect-Host-Usage	0	0-1	0	0-1
Redirect-Max-Cache-Time	0	0-1	0	0-1
Result-Code	0	1	0	1
Re-Auth-Request-Type	0	0-1	0	0
Route-Record	0+	0	0+	0
Session-Id	1	1	1	1
User-Name	1	0-1	1	0-1

11.2. Tableau des AVP de comptabilité

Le tableau de ce paragraphe est utilisé pour représenter quelles AVP définies dans ce document doivent être présentes dans les messages Accounting, comme défini dans la [RFC3588].

	Code de commande	
Nom de l'attribut	ACR	ACA
Accounting-Input-Octets	1	0-1
Accounting-Input-Packets	1	0-1
Accounting-Output-Octets	1	0-1
Accounting-Output-Packets	1	0-1
Acct-Multi-Session-Id	1	0-1
Acct-Session-Time	1	0-1
MIP-Feature-Vector	1	0-1
MIP-Home-Agent-Address	1	0-1
MIP-Mobile-Node-Address	1	0-1
Event-Timestamp	0-1	0

12. Considérations relatives à l'IANA

Cette section contient les espaces de noms qui ont été créés dans la présente spécification ou ont eu leurs valeurs allouées par des espaces de noms existants gérés par l'IANA.

12.1 Codes de commandes

Cette spécification alloue les valeurs 260 et 262 de l'espace de noms de code de commandes défini dans la [RFC3588]. Voir à la Section 5 l'allocation de l'espace de noms dans la présente spécification.

12.2 Codes d'AVP

Cette spécification alloue les valeurs 318 - 348 et 363 - 367 à partir de l'espace de noms de code d'AVP défini dans la [RFC3588]. Voir aux Sections 7, 9, et 10 les allocations de l'espace de noms dans la présente spécification.

12.3 Valeurs d'AVP de code de résultat

Cette spécification alloue les valeurs 4005 - 4008 et 5024 - 5025 à partir de l'espace de noms de valeur de l'AVP Result-Code (code d'AVP 268) défini dans la [RFC3588]. Voir à la Section 6 l'allocation de l'espace de noms dans la présente spécification.

12.4 Valeurs d'AVP de MIP-Feature-Vector

Il y a 32 bits dans l'AVP MIP-Feature-Vector (code d'AVP 337) qui sont disponibles pour allocation. Le présent document alloue les bits 1 - 9, comme mentionné au paragraphe 7.5. Les bits restants ne devraient être alloués que par action de normalisation [RFC2434].

12.5 Valeurs d'AVP de MIP-Algorithm-Type

Comme défini au paragraphe 9.8, l'AVP MIP-Algorithm-Type (code d'AVP 345) définit la valeur 2. Toutes les valeurs restantes, sauf zéro, sont disponibles pour allocation via un expert désigné [RFC2434].

12.6 Valeurs d'AVP de MIP-Replay-Mode

Comme défini au paragraphe 9.9, l'AVP MIP-Replay-Mode (code d'AVP 346) définit les valeurs 1 - 3. Toutes les valeurs restantes, sauf zéro, sont disponibles pour allocation via un expert désigné [RFC2434].

12.7 Identifiant d'application

Cette spécification utilise la valeur deux (2) pour l'espace de noms d'identifiant d'application défini dans la [RFC3588]. Voir plus d'informations à la Section 4.

13. Considérations sur la sécurité

La présente spécification décrit une application Diameter IPv4 mobile pour l'authentification et l'autorisation d'un nœud mobile IPv4 mobile. L'algorithme d'authentification utilisé dépend des transformations utilisées au sein du protocole IPv4 mobile, et de la [RFC3012]. La présente spécification, en conjonction avec la [RFC3957], définit aussi une méthode par laquelle le serveur Diameter de rattachement peut créer et distribuer les clés de session et les noms occasionnels à utiliser pour authentifier et protéger l'intégrité des messages d'enregistrement IPv4 mobile [RFC3344]. La distribution des clés est asymétrique, car la communication avec le nœud mobile se produit via le protocole IPv4 mobile [RFC3957], [RFC3344], alors que la communication avec l'agent de rattachement et l'agent étranger se produit via le protocole Diameter. Lorsque des agents Diameter qui ne sont pas de confiance sont présents, la sécurité de bout en bout DOIT être utilisée. La sécurité de bout en bout prend la forme d'associations de sécurité TLS ou IPsec entre le AAAH et le FA et entre le AAAH et le HA. Ces connexions seront authentifiées en utilisant des clés publiques et des certificats ; cependant, les identités qui apparaissent dans les certificats doivent être autorisées et liées à une session Diameter IPv4 mobile particulière avant que l'AAAH puisse commencer en toute sécurité la distribution des clés.

Noter que les connexions directes sont établies par suite de messages de redirection Diameter. Par exemple, dans la Figure 3, le FA obtient une réponse de redirection contenant l'AVP Redirect-Host de la part de l'AAAH. C'est l'identité qui devrait être confrontée au certificat présenté par l'AAAH lorsque la connexion sûre est établie. Dans ce cas, le réseau de mandataires Diameter et d'agents de redirection est de confiance pour la tâche de retourner l'identité d'AAAH correcte au FA.

Le AAAH doit aussi prendre une décision d'autorisation lorsque le FA établit la connexion. Si le AAAH et le serveur de redirection sont la même entité, le AAAH peut avoir observé et noté le message AMR original qui contenait l'identité du FA et peut ainsi autoriser l'établissement d'une connexion TLS ou IPsec à partir de la même entité. Autrement, le AAAH aura besoin de conserver une liste de tous les domaines visités autorisés (partenaires d'itinérance) et autoriser les connexions TLS ou IPsec sur la base de cette liste. Noter que l'établissement de la connexion n'est que la première étape, et le AAAH a une autre opportunité de refuser le service à réception du message AMR lui-même. À cette étape, le AAAH peut vérifier les AVP internes de l'AMR pour s'assurer que le FA est valide ; par exemple, il peut vérifier que l'adresse d'entretien IP mobile est égale à l'adresse IP utilisée comme point d'extrémité de la connexion TLS ou IPsec. Cependant, une telle politique empêcherait le FA d'utiliser des interfaces différentes pour les paquets AAA et de tunnel IP mobile et peut n'être pas désirable dans toutes les situations.

Un ensemble similaire de considérations s'applique à la connexion entre AAAH et HA lorsque ces entités sont dans des domaines administratifs différents. Cependant, les rôles sont ici inversés parce que c'est le AAAH qui contacte le HA via la HAR. L'identité du candidat HA est donnée au AAAH dans l'AMR, et le AAAH devrait s'attendre à recevoir la même identité dans les certificats de clé publique durant la négociation TLS ou IPsec. Le HA peut autoriser des connexions individuelles en agissant comme son propre serveur de redirection, ou il peut tenir une liste des partenaires d'itinérance de confiance.

Cette application crée et distribue une seule clé de session pour chaque paire de MSA entre deux entités ; par exemple, la même clé de session est utilisée pour la MSA MN-HA et la MSA HA-MN. Ceci est sûr du point de vue de la sécurité, car les clés de session ne sont utilisées qu'avec des fonctions de hachage chiffré pour générer les valeur d'authentifiant qui protègent l'intégrité de chaque message de contrôle IP mobile. Les messages IP mobile ont une protection incorporée contre la répétition avec l'utilisation d'horodatages ou de noms occasionnels [RFC3344], et, du fait de la nature du protocole, les demandes sont toujours différentes des réponses du point de vue binaire, au moins dans le code de type de message. Cela évite des problèmes qui pourraient se produire dans d'autres situations où un attaquant pourrait monter une attaque de répétition ou de réflexion si la même clé était utilisée (par exemple) pour chiffrer du trafic par ailleurs non protégé sur plus d'une branche de connexion dans le réseau.

Les noms occasionnels sont envoyés au nœud mobile, et ils sont utilisés pour générer les clés de session via la fonction unidirectionnelle HMAC-SHA-1. Parce que les noms occasionnels et les extensions d'authentification peuvent être observés par n'importe qui qui a accès à une copie en clair de la réponse d'enregistrement, la clé prépartagée entre le nœud mobile et le serveur Diameter de rattachement serait vulnérable à une attaque hors ligne de dictionnaire si elle ne contenait pas assez d'entropie. Pour empêcher cela, la clé prépartagée entre le nœud mobile et le serveur Diameter de rattachement DEVRAIT être une quantité choisie au hasard d'au moins 96 bits.

Comme la clé de session est déterminée par le secret à long terme et le nom occasionnel, le nom occasionnel DEVRAIT être temporairement et mondialement unique ; si le nom occasionnel devait être répété, la clé de session le serait aussi. Pour empêcher cela, il est fortement recommandé qu'un nom occasionnel soit une valeur aléatoire [RFC4086] d'au moins 128 bits. Le secret à long terme entre le MN et l'AAAH DOIT être rafraîchi périodiquement, pour se garder contre la récupération du secret à long terme due à la réutilisation du nom occasionnel ou d'autres facteurs. Ceci est réalisé par l'utilisation de mécanismes hors bande, qui ne sont pas spécifiés dans le présent document.

Noter qu'il n'est pas recommandé de régler la valeur de l'AVP MIP-MSA-Lifetime à zéro, car garder les clés de session pendant longtemps (sans les rafraîchir) augmente le niveau de vulnérabilité.

14 Références

14.1 Références normatives

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

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

[RFC2234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", novembre 1997. (*Obsolète, voir* RFC5234)

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la* RFC5226)

[RFC2486] B. Aboba, M. Beadles, "Identifiant d'accès réseau", janvier 1999. (*Obsolète, voir* RFC7542) *(P.S.)*

[RFC3012] C. Perkins, P. Calhoun, "Extensions de mise en cause/réponse pour IPv4 mobile", novembre 2000. (*Obs., voir* RFC4721) *(P.S.)*

[RFC3344] C. Perkins, éd., "Prise en charge de la mobilité IP pour IPv4", août 2002. (*Obsolète, voir* RFC5944) *(P.S.)*

[RFC3546] S. Blake-Wilson et autres, "Extensions à la sécurité de la couche Transport (TLS) ", juin 2003. *(Obsolète, voir la* RFC4366)

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

[RFC3846] F. Johansson, T. Johansson, "Extension IPv4 mobile pour le portages des identifiants d'accès réseau", juin 2004. *(P.S.)*

[RFC3957] C. Perkins, P. Calhoun, "Clés d'enregistrement d'authentification, d'autorisation, et de comptabilité (AAA) pour IPv4 mobile", mars 2005. *(P.S.)*

14.2 Références pour information

[RFC2477] B. Aboba, G. Zorn, "Critères pour l'évaluation des protocoles d'itinérance", janvier 1999. *(Information)*

[RFC2794] P. Calhoun, C. Perkins, "Extension d'identifiant d'accès à un réseau mobile IP pour IPv4", mars 2000. *(P.S.)*

[RFC2977] S. Glass, T. Hiller, S. Jacobs, C. Perkins, "Exigences d'authentification, d'autorisation et de comptabilité pour IP mobile", octobre 2000. *(Information)*

[RFC3141] T. Hiller et autres, "Exigences de données sans fil CDMA2000 pour AAA", juin 2001. *(Information)*

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005. (*Remplace* RFC1750) (BCP0106)

15. Remerciements

Les auteurs tiennent à remercier Nenad Trifunovic, Haseeb Akhtar, et Pankaj Patel de leur participation au groupe de lecture de document pré IETF, Erik Guttman de sa très utile proposition de texte, et Fredrik Johansson, Martin Julien, et Bob Kopacz de leur texte de contribution très utile.

Les auteurs voudraient aussi remercier les participants au groupe de travail TSG-X du 3GPP2 pour leurs précieux retours, et les personnes suivantes de leur contribution au développement du protocole : Kevin Purser, Thomas Panagiotis, Mark Eklund, Paul Funk, Michael Chen, Henry Haverinen, et Johan Johansson. Le texte sur le serveur de redirection général dû à Pasi Eronen a été emprunté à Diameter-EAP.

Pat Calhoun tient à remercier Sun Microsystems, car la plus grande partie des efforts mis à la production du présent document l'ont été pendant qu'il était leur employé.

Adresse des auteurs

Les questions sur le présent mémoire peuvent être adressées à :

Pat Calhoun
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA
téléphone : +1 408-853-5269
mél : pcalhoun@cisco.com

Tony Johansson
Bytemobile, Inc.
2029 Stierlin Court
Mountain View, CA 94043
téléphone : +1 650-641-7817
mél : tony.johansson@bytemobile.com

Charles E. Perkins
Nokia Research Center
313 Fairchild Drive
Mountain View, CA 94043
USA
téléphone : +1 650-625-2986
mél : Charles.Perkins@nokia.com

Tom Hiller
Lucent Technologies
1960 Lucent Lane
Naperville, IL 60566
USA
téléphone : +1 630-979-7673
mél : tomhiller@lucent.com

Peter J. McCann
Lucent Technologies
1960 Lucent Lane
Naperville, IL 60563
USA
téléphone : +1 630-713-9359
mél : mccap@lucent.com

Déclaration complète de droits de reproduction

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