Groupe de travail Réseau
Request for Comments : 2977
Catégorie : Information

Traduction Claude Brière de L'Isle

S. Glass, Sun Microsystems
T. Hiller, Lucent Technologies
S. Jacobs, GTE Laboratories
C. Perkins, Nokia Research Center
octobre 2000

Exigences d'authentification, d'autorisation et de comptabilité pour IP mobile

Résumé
Les groupes de travail "IP mobile" et "Authentification, autorisation, et comptabilité" (AAA) cherchent actuellement à définir les exigences pour l'authentification, l'autorisation, et la comptabilité. Le présent document contient les exigences qui devraient être satisfaites par un service AAA pour aider à fournir les services IP mobile.

1. Introduction

Les clients obtiennent des services Internet en négociant un point de rattachement à un "domaine de rattachement", généralement auprès d'un fournisseur d'accès Internet (FAI), ou autre organisation à partir de laquelle sont faites, et satisfaites les demandes de service. Avec la popularité croissante des appareils mobiles a été généré un besoin croissant de permettre aux usagers de se rattacher à tout domaine convenant à leur localisation réelle. De cette façon, un client a besoin de l'accès à des ressources qui sont fournies par un domaine administratif différent de son domaine de rattachement (appelé un "domaine étranger"). Le besoin de service à partir d'un domaine étranger exige, dans de nombreux modèles, une autorisation, qui conduit directement à l'authentification, et bien sûr une comptabilité (d'où, "AAA"). Il y a des discussions sur la notion qui domine, ou est dérivée des autres, mais il y a accord sur le fait que les trois fonctions AAA sont étroitement interdépendantes.

Un agent dans un domaine étranger, qui est appelé à fournir l'accès à une ressource à un utilisateur mobile, va probablement demander ou exiger du client qu'il fournisse des accréditifs qui peuvent être authentifiés avant que l'accès aux ressources ne soit permis. La ressource peut être aussi simple qu'un conduit vers l'Internet, ou peut être aussi complexe qu'un accès à des ressources privées spécifiques au sein du domaine étranger. Les accréditifs peuvent être échangés de nombreuses façons différentes, qui sortent toutes du domaine d'application du présent document. Une fois authentifié, l'utilisateur mobile peut être autorisé à accéder aux services au sein du domaine étranger. Une comptabilité des ressources réelles peut alors être établie.

IP mobile est une technologie qui permet à un nœud réseau ("nœud mobile") de migrer de son réseau "de rattachement" à d'autres réseaux, au sein du même domaine administratif, ou dans d'autres domaines administratifs. La possibilité de mouvement entre domaines, qui exige les services AAA a créée une demande immédiate de conception et de spécification de protocoles AAA. Une fois disponibles, les protocoles et l'infrastructure AAA vont fournir l'incitation économique pour un déploiement à grande échelle de IP mobile. Le présent document identifie, décrit, et expose les exigences fonctionnelles et de performance que IP attend des protocoles AAA.

La description formelle de IP mobile se trouve dans les [RFC2002], [RFC2003], [RFC2004], [RFC2290].

Dans le présent document, on a tenté de montrer les exigences de façon progressive. Après avoir montré le modèle AAA de base pour IP mobile, on déduit les exigences comme suit :
- exigences fondées sur le modèle général
- exigences fondées sur la fourniture du service IP aux nœuds mobiles
- exigences dérivées de besoins spécifiques du protocole IP mobile.

Ensuite, on montre certains modèles AAA en rapport et on décrit les exigences déduites de ces modèles.

2. Terminologie

Le présent document utilise fréquemment les termes suivants en plus de ceux définis dans la [RFC2002] :

Comptabilité : acte de collecte des informations sur l'utilisation des ressources aux fins d'analyse de tendance, de vérification, de facturation, ou d'allocation des coûts.

Domaine administratif : un intranet, ou une collection de réseaux, ordinateurs, et bases de données sous une administration commune. Les entités informatiques opérant sous une administration commune peuvent être supposés partager les associations de sécurité créées administrativement.

Assistant *(Attendant)* : nœud conçu pour fournir l'interface de service entre un client et le domaine local.

Authentification : acte de vérifier une identité revendiquée, sous la forme d'une étiquette préexistante provenant d'un espace de noms mutuellement connu, comme origine d'un message (authentification de message) ou comme point d'extrémité d'un canal (authentification d'entité).

Autorisation : acte de déterminer si un droit particulier, comme l'accès à des ressources, peut être accordé au présentateur d'un accréditif particulier.

Facturation : acte de préparer une facture.

Courtier : agent intermédiaire, de confiance pour deux autres serveurs AAA, capable d'obtenir et fournir des services de sécurité de ces serveurs AAA. Par exemple, un courtier peut obtenir et fournir des autorisations, ou des assurances que les accréditifs sont valides.

Client : nœud qui souhaite obtenir des services d'un assistant au sein d'un domaine administratif.

Domaine étranger : domaine administratif, visité par un client IP mobile, et contenant l'infrastructure AAA nécessaire pour effectuer les opérations qui permettent les enregistrements IP mobile. Du point de vue de l'agent étranger, le domaine étranger est le domaine local.

Comptabilité inter domaines : c'est la collecte des informations sur l'utilisation des ressources par une entité dans un domaine administratif, pour les utiliser dans un autre domaine administratif. Dans la comptabilité inter domaines, les paques de comptabilité et les enregistrements de session vont normalement traverser les frontières administratives.

Comptabilité intra domaine : c'est la collecte des informations sur l'utilisation des ressources au sein d'un domaine administratif, pour les utiliser dans ce domaine. Dans la comptabilité intra domaine, les paquets de comptabilité ne traversent normalement pas les frontières administratives.

Domaine local : domaine administratif contenant l'infrastructure AAA d'intérêt immédiate pour un client IP mobile lorsque il est hors du domaine de rattachement.

Comptabilité en temps réel : cela implique le traitement des informations sur l'utilisation des ressources dans une fenêtre temporelle définie. Les contraintes de temps sont normalement imposées afin de limiter le risque financier.

Enregistrement de session : cela représente une récapitulation de la consommation de ressources d'un utilisateur sur une session entière. Les passerelles de comptabilité qui créent l'enregistrement de session peuvent le faire en traitant les événements de comptabilité intermédiaires.

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].

3. Modèle de base

Dans cette section, on tente de saisir les principales caractéristiques d'un modèle de base du fonctionnement des serveurs AAA qui semble avoir un bon soutien dans le groupe de travail IP mobile. Au sein de l'Internet, un client qui appartient à un domaine administratif (appelé le domaine de rattachement) a souvent besoin d'utiliser des ressources fournies par un autre domaine administratif (appelé le domaine étranger). Un agent dans le domaine étranger qui reçoit la demande du

client (on appelle cet agent "l'assistant") va probablement exiger que le client fournisse des accréditifs qui puissent être authentifiés avant de permettre l'accès aux ressources. Ces accréditifs peuvent être quelque chose que le domaine étranger comprend, mais dans la plupart des cas ils sont alloués, et compris seulement par le domaine de rattachement, et peuvent être utilisés pour établir des canaux sûrs avec le nœud mobile.

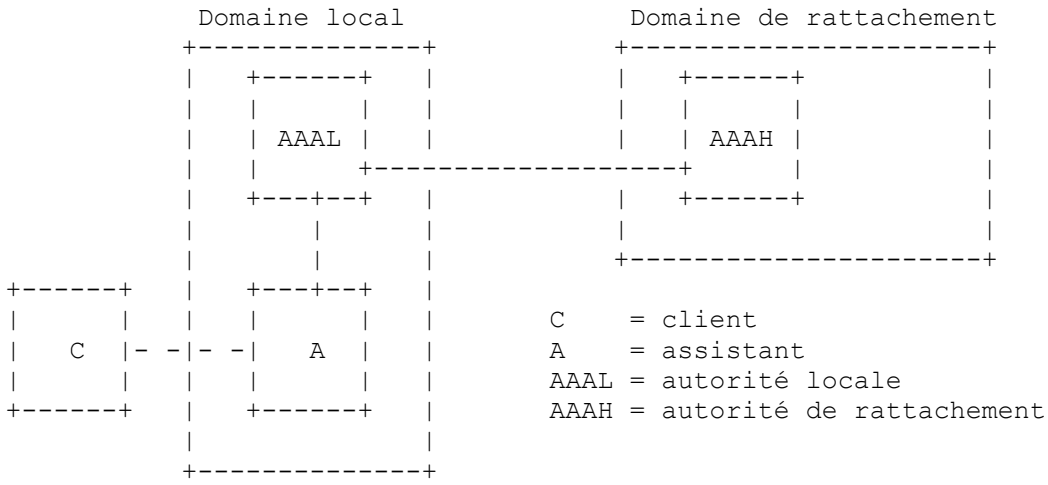

Figure 1 : Serveurs AAA dans le domaine local et le domaine de rattachement

Souvent, l'assistant n'a pas un accès direct aux données nécessaires pour achever la transaction. L'assistant est plutôt supposé consulter une autorité (normalement dans le même domaine étranger) afin de demander la preuve que le client a des accréditifs acceptables. Comme l'assistant et l'autorité locale font partie du même domaine administratif, ils sont supposés avoir établi, ou être capables d'établir pour la durée de vie nécessaire, un canal sûr pour les besoins de l'échange d'informations sensibles (d'accès) et de les garder secrètes à l'égard (au moins) du nœud mobile visiteur.

L'autorité locale (AAAL) elle-même peut n'avoir pas assez d'informations mémorisées en local pour effectuer la vérification des accréditifs du client. Au contraire de l'assistant, l'AAAL est cependant supposé être configuré avec assez d'informations pour négocier la vérification des accréditifs de client avec les autorités externes. Les autorités locales et externes devraient être configurées avec des relations de sécurité suffisantes et des contrôles d'accès pour qu'elles puissent, éventuellement sans avoir besoin d'autre agent AAA, négocier l'autorisation qui peut permettre au client d'avoir accès à une ou toutes les ressources demandées. Dans de nombreux cas ordinaires, l'autorisation dépend seulement de la sûreté de l'authentification des accréditifs du client.

Une fois que l'autorisation a été obtenue par l'autorité locale, et que l'autorité a notifié à l'assistant la réussite de la négociation, l'assistant peut fournir les ressources demandées au client.

Sur la figure, il peut y avoir de nombreux assistants pour chaque AAAL, et il peut y avoir de nombreux clients provenant de nombreux domaines de rattachement différents. Chaque domaine de rattachement fournit un AAAH qui peut vérifier les accréditifs provenant de clients administrés par ce domaine de rattachement.

Il y a un modèle de sécurité implicite dans la figure ci-dessus, et il est crucial d'identifier les associations de sécurité spécifiques supposées dans le modèle de sécurité.

D'abord, il est naturel de supposer que le client a une association de sécurité avec le AAAH, car c'est en gros ce que signifie que le client appartient au domaine de rattachement.

Ensuite, d'après le modèle illustré à la figure 1, il est clair que AAAL et AAAH doivent partager une association de sécurité, parce que autrement ils ne pourraient pas s'appuyer sur le résultat de l'authentification, les autorisations, ni même les données comptables qu'ils pourraient s'échanger. Exiger de telles relations de sécurité bilatérales est cependant finalement non adaptable ; le cadre AAA DOIT fournir des mécanismes plus adaptables, comme le suggère la Section 6.

Finalement, dans la figure, il est clair que l'assistant peut naturellement partager une association de sécurité avec l'AAAL. C'est nécessaire pour que le modèle fonctionne parce que l'assistant doit savoir si il est possible de permettre d'allouer les ressources locales au client.

Pour un exemple dans l'Internet d'aujourd'hui, on peut citer le déploiement de RADIUS [RFC2138] pour permettre aux clients d'ordinateurs mobiles d'avoir accès à l'Internet au moyen d'un FAI local. Le FAI veut s'assurer que le client mobile peut payer la connexion. Une fois que le client a fourni des accréditifs (par exemple, identification, données univoques, et

signature inimitable) le FAI vérifie la signature auprès de l'autorité de rattachement du client, et pour obtenir l'assurance que le client payera la connexion. Ici, la fonction de l'assistant peut être effectuée par le serveur d'accès réseau (NAS, *Network Access Server*) et les autorités locales et de rattachement peuvent utiliser les serveurs RADIUS. Les accréditifs permettant l'autorisation chez un assistant DEVRAIENT être inutilisables dans une future négociation sur le même assistant ou tout autre.

À partir de la description et l'exemple ci-dessus, on peut identifier plusieurs exigences.
- Chaque assistant local doit avoir une relation de sécurité avec le serveur AAA local (AAAL)
- L'autorité locale doit partager, ou établir de façon dynamique, une relation de sécurité avec les autorités externes qui sont capables de vérifier les accréditifs du client.
- L'assistant doit conserver l'état pour les demandes en cours du client pendant que l'autorité locale contacte l'autorité externe appropriée.
- Comme le nœud mobile peut ne pas nécessairement initier la connexité réseau de l'intérieur de son domaine de rattachement, il DOIT être capable de fournir des accréditifs complets, et donc inimitables sans avoir jamais été en contact avec son domaine de rattachement.
- Comme les accréditifs du nœud mobile doivent rester inimitables, les nœuds intervenants (par exemple, ni l'assistant ni l'autorité locale (AAAL) ni aucun autre nœud intermédiaire) NE DOIVENT PAS être capables d'apprendre des informations (secrets) qui pourraient leur permettre de reconstruire et réutiliser les accréditifs.

De cette dernière exigence, on peut voir les raisons de l'exigence naturelle que le client doit partager, ou établir de façon dynamique, une relation de sécurité avec l'autorité externe dans le domaine de rattachement. Autrement, il est techniquement infaisable (étant donné la topologie implicite du réseau) que le client produise des signatures inimitables qui puissent être vérifiées par l'AAAH. La Figure 2 illustre les associations de sécurité naturelles tirées du modèle proposé. Noter que, conformément à l'exposé de la Section 6, il peut y avoir, par accord mutuel entre AAAL et AAAH, un tiers inséré entre AAAL et AAAH pour les aider à arbitrer des transactions sûres d'une façon plus adaptable.

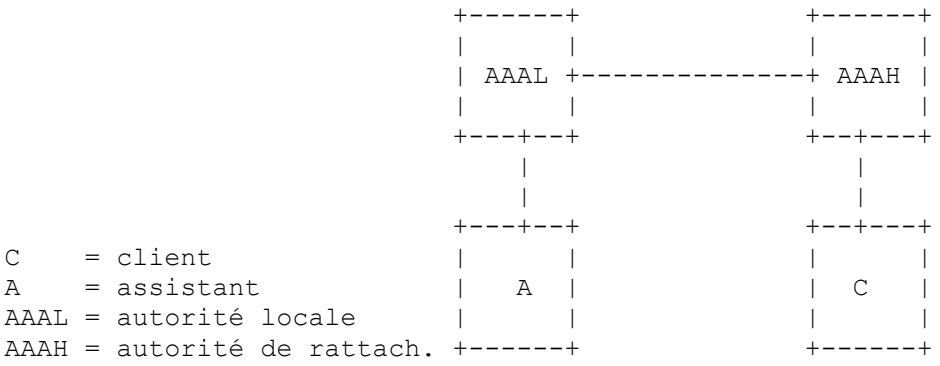

Figure 2 : Associations de sécurité

En plus des exigences mentionnées ci-dessus, on spécifie les exigences suivantes qui dérivent de l'expérience du fonctionnement des protocoles d'itinérance actuels.
- Il y a des scénarios dans lesquels un assistant va devoir gérer en même temps des demandes pour de nombreux clients.
- L'assistant DOIT protéger contre les attaques en répétition.
- L'équipement de l'assistant devrait être aussi peu coûteux que possible, car il sera répliqué aussi souvent que possible pour traiter autant de clients que possible dans le domaine étranger.
- Les assistants DEVRAIENT être configurés à obtenir l'autorisation d'un serveur local AAA (AAAL) de confiance pour les exigences de qualité de service posées par le client.

Les nœuds dans deux domaines administratifs séparés (par exemple, AAAH et AAAL) doivent souvent prendre des mesures supplémentaires pour vérifier l'identité de leur partenaire de communication, ou autrement pour garantir la confidentialité des données constituant la communication. Bien que ces considérations conduisent à d'importantes exigences de sécurité, comme mentionné ci-dessus dans le contexte de la sécurité entre serveurs, on considère que le choix exact des associations de sécurité entre les serveurs AAA sort du domaine d'application du présent document. Les choix ont peu de chances de dépendre de caractéristiques spécifiques du modèle général illustré à la Figure 1. D'un autre côté, les associations de sécurité nécessaires entre les entités IP mobile seront d'une importance capitale dans la conception d'une infrastructure AAA convenable pour IP mobile. Le modèle général montré ci-dessus est en général compatible avec les besoins de IP mobile. Cependant, quelques changements de base sont nécessaires dans le modèle de sécurité IP mobile, comme détaillé à la section 5.

Enfin, une récente discussion dans le groupe de travail IP mobile a indiqué que l'assistant DOIT être capable de mettre un terme au service au client sur la base d'une détermination de politique par le serveur AAAH ou AAAL.

3.1 Exigences d'itinérance du protocole AAA

On précise ici les exigences supplémentaires sur la base des problèmes découverts à travers l'expérience du fonctionnement des réseaux RADIUS d'itinérance existants. Le protocole AAA DOIT satisfaire ces exigences afin que les fournisseurs offrent un service robuste. Ces exigences ont été identifiées par TR45.6 au titre de sa collaboration avec le groupe de travail IP mobile.

- Prise en charge d'un mécanisme fiable de transport AAA.
  * Il doit y avoir un mécanisme efficace de retransmission et de reprise sur échec bond par bond afin que la fiabilité ne dépende pas seulement de la retransmission de bout en bout.
  * Ce mécanisme de transport sera capable d'indiquer à une application AAA qu'un message a été livré à la prochaine application AAA homologue ou qu'une fin de temporisation est intervenue.
  * La retransmission est contrôlée par le mécanisme fiable de transport AAA, et non par des protocoles de couche inférieure comme TCP.
  * Même si le message AAA est à transmettre, ou si les options ou la sémantique du message ne sont pas conformes au protocole AAA, le mécanisme de transport va accuser réception du message AAA par l'homologue.
  * Les accusés de réception DEVRAIENT pouvoir être portés dans les messages AAA.
  * Les réponses AAA doivent être livrés à temps pour que IP mobile n'arrive pas en fin de temporisation et retransmette.
- Transport d'un certificat numérique dans un message AAA, afin de minimiser le nombre d'allers retours associés aux transactions AAA. Note : Cette exigence s'applique aux applications AAA et non aux stations mobiles. Les certificats peuvent être utilisés par des agents de rattachement et étrangers pour établir une association de sécurité IPsec pour sécuriser les données tunnelées du nœud mobile. Dans ce cas, l'infrastructure AAA pourrait aider en obtenant l'état de révocation d'un tel certificat (soit en effectuant des vérifications en ligne, soit autrement en validant le certificat) afin que les agents de rattachement et étranger puissent éviter une coûteuse vérification en ligne du statut du certificat.
- Assurer l'intégrité du message et l'authentification de l'identité bond par bond (nœud AAA).
- Prise en charge des capacités de protection contre la répétition et facultativement de la non répudiation pour tous les messages d'autorisation et de comptabilité. Le protocole AAA doit fournir la capacité que les messages de comptabilité soient confrontés aux messages d'autorisation antérieurs.
- Prise en charge de la comptabilité via des accords bilatéraux et via des serveurs AAA courtiers assurant le rôle de chambre de compensation et de réconciliation entre réseaux desservants et de rattachement. Il y a un accord explicite que si le réseau privé ou le FAI de rattachement authentifie la station mobile qui demande le service, le réseau privé ou FAI de rattachement accepte alors aussi de s'ajuster avec le fournisseur de service de rattachement ou le courtier. La comptabilité en temps réel doit être prise en charge. Les horodatages doivent être inclus dans tous les paquets de comptabilité.

4. Exigences relatives à la connexité IP de base

Les exigences énumérées à la section précédente relèvent des relations entre les unités fonctionnelles, et ne dépendent pas de l'adressage réseau sous-jacent. D'un autre côté, de nombreux nœuds (mobiles ou simplement portables) sont programmés à recevoir des ressources spécifiques d'IP durant la phase d'initialisation de leur tentative de connexion à l'Internet.

On pose les exigences supplémentaires suivantes pour les services AAA afin de satisfaire de tels clients :
- Chaque serveur AAA DOIT être capable d'obtenir, ou de coordonner l'allocation d'une adresse IP convenable pour le consommateur, à sa demande.
- Les serveurs AAA DOIVENT être capables d'identifier le client par un moyen autre que son adresse IP.

La politique du domaine de rattachement peut imposer que l'agent de rattachement gère l'allocation d'une adresse IP pour le nœud mobile au lieu de l'AAAH . Les serveurs AAA DOIVENT être capables de coordonner l'allocation d'une adresse IP pour le nœud mobile au moins de cette façon.

Les serveurs AAA identifient aujourd'hui les clients en utilisant l'identifiant d'accès réseau (NAI, *Network Access Identifier*) [RFC2486]. Un nœud mobile peut s'identifier en incluant le NAI avec la demande d'enregistrement IP mobile [RFC2794]. Le NAI est de la forme "usager@domaine" ; il est univoque et convient bien pour une utilisation dans le modèle AAA illustré à la Figure 1. Utiliser un NAI (par exemple, "usager@domaine") permet au AAAL de déterminer facilement le domaine de rattachement (par exemple, "domaine") pour le client. Le AAAL et le AAAH peuvent tous deux utiliser le NAI pour indexer les enregistrements par l'identité spécifique du client.

5. AAA pour IP mobile

Les clients qui utilisent IP mobile requièrent des caractéristiques spécifiques de la part des services AAA, en plus des exigences déjà mentionnées au sujet des fonctionnalités de base AAA et qui sont nécessaires pour la connexité IP. Pour comprendre l'application du modèle général pour IP mobile, on considère le nœud mobile (MN) comme le client dans la Figure 1, et l'assistant comme l'agent étranger (FA). Si il se produit une situation où il n'y a pas d'agent étranger présent, par exemple, dans le cas d'un nœud mobile IPv4 avec une adresse d'entretien colocalisée ou un nœud mobile IPv6, la fonctionnalité équivalente à l'assistant sera fournie par l'entité d'allocation d'adresse, par exemple, un serveur DHCP. Une telle fonctionnalité d'assistant sort du domaine d'application du présent document. L'agent de rattachement, bien qu'important pour IP mobile, peut jouer un rôle durant l'enregistrement initial qui est subordonné au rôle joué par le AAAH. Pour une application à IP mobile, on modifie le modèle général (comme illustré à la Figure 3). Après l'enregistrement initial, le nœud mobile est autorisé à continuer à utiliser IP mobile au domaine étranger sans exiger d'autre engagement des serveurs AAA. Donc, l'enregistrement initial va probablement prendre plus de temps que les enregistrements IP mobiles ultérieurs.

Afin de réduire autant que possible les frais généraux de ce délai supplémentaire, il est important de réduire le temps pris pour les communications entre les serveurs AAA. Un composant majeur de cette latence de communications est le temps pris pour traverser les grandes zones de l'Internet qui vont probablement séparer le AAAL et le AAAH. Cela conduit à une motivation encore plus forte pour l'intégration des fonctions de AAA elles-mêmes, ainsi que l'intégration des fonctions de AAA avec l'enregistrement IP mobile initial. Afin de réduire le nombre de messages qui traversent le réseau pour l'enregistrement initial d'un nœud mobile, les fonctions de AAA dans le réseau visité (AAAL) et le réseau de rattachement (AAAH) ont besoin d'une interface avec l'agent étranger et l'agent de rattachement pour traiter le message d'enregistrement. La latence sera réduite par suite du traitement d'un enregistrement initial en conjonction avec l'AAA et les agents de mobilité IP mobile. Les enregistrements suivants sont cependant être traités conformément à la [RFC2002]. Une autre façon de réduire la latence en matière de comptabilité serait d'échanger de petits enregistrements.

Comme il y a de nombreux types différents de sous services que les assistants peuvent fournir aux clients mobiles, il DOIT y avoir des formats extensibles de comptabilité. De cette façon, les services spécifiques fournis peuvent être identifiés, ainsi que les supports de comptabilité si plus de services devaient être identifiés à l'avenir.

Le domaine de rattachement AAA et le domaine de rattachement HA du nœud mobile n'ont pas besoin de faire partie du même domaine administratif. Une telle situation peut se produire si l'adresse de rattachement du nœud mobile est fournie par un domaine, par exemple, un FAI que l'usager mobile utilise quand il est chez lui, et que l'autorisation et la comptabilité le sont par un autre domaine (spécialisé) par exemple, une société de carte de crédit. L'agent étranger envoie seulement les informations d'authentification du nœud mobile à l'AAAL, qui fait l'interfaces avec le AAAH. Après la réussite de l'autorisation du nœud mobile, l'agent étranger est capable de continuer la procédure d'enregistrement IP mobile. Un tel schéma introduit plus de retards si l'accès à la fonctionnalité AAA et au protocole IP mobile sont mis en séquence. Les enregistrements suivants seront traités conformément à la [RFC2002] sans autre interaction avec le AAA. C'est en fin de compte à une décision de politique qu'il revient de savoir s'il faut combiner ou séparer les données du protocole IP mobile et les messages AAA. Une séparation des données du protocole IP et des messages AAA ne peut réussir à se faire que si l'adresse IP de l'agent de rattachement du nœud mobile est fournie à l'agent étranger qui assume la fonction d'assistant.

Toutes les fonctions AAA et IP mobile nécessaires DEVRAIT être traitées durant une seule traversée de l'Internet. Cela DOIT être fait sans exiger que les serveurs AAA traitent les messages de protocole envoyés aux agents IP mobile. Les serveurs AAA DOIVENT identifier les agents IP mobile et les associations de sécurité nécessaire pour traiter l'enregistrement IP mobile, passer les données d'enregistrement nécessaires à ces agents IP mobile, et rester en dehors du processus d'acheminement et d'authentification particulier de l'enregistrement IP mobile.

Pour IP mobile, les serveurs AAAL et AAAH ont les tâches générales supplémentaires suivantes :
- permettre la [ré] authentification de l'enregistrement IP mobile,
- autoriser le nœud mobile (une fois que son identité a été établie) à utiliser au moins l'ensemble de ressources pour les fonctionnalités IP mobile minimales, plus potentiellement les autres services demandés par le nœud mobile,
- initier la comptabilité pour l'utilisation du service,
- utiliser les extensions de protocole AAA, spécifiquement pour inclure les messages d'enregistrement IP mobile au titre de la séquence d'enregistrement initial à traiter par les serveurs AAA.

Ces tâches, et les tâches résultantes plus spécifiques qui seront énumérées plus loin, sont traitées et expédiées avec avantage par les serveurs AAA montrés à la Figure 1 parce que ces tâches se présentent souvent ensemble et le traitement des tâches a besoin de l'accès aux mêmes données au même moment.

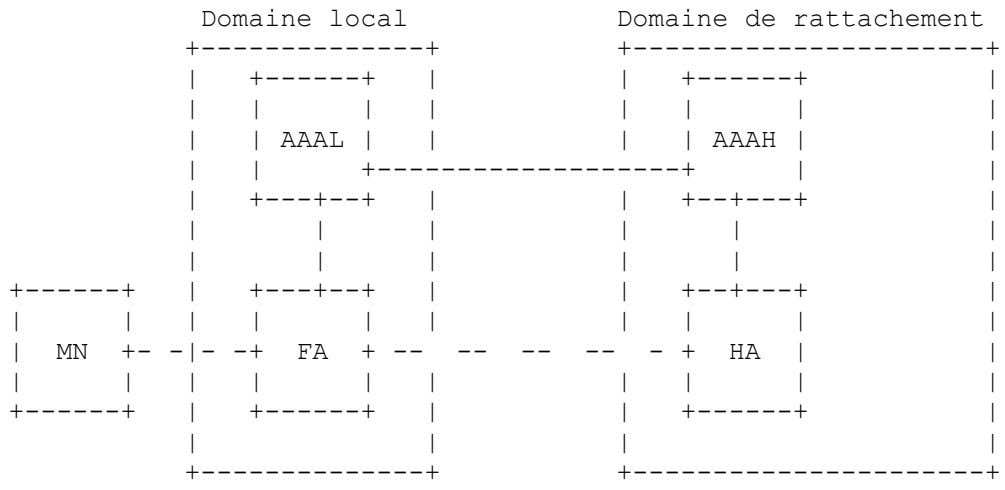

Figure 3 : Serveurs AAA avec agents IP mobile

Dans le modèle de la Figure 1, les transactions AAA initiales sont traitées sans avoir besoin de l'agent de rattachement, mais IP mobile exige que tous les enregistrements soient traités entre l'agent de rattachement (HA) et l'agent étranger (FA), comme montré par la ligne alternant tirés et espaces (en bas) sur la Figure 3. Cela signifie que durant l'enregistrement initial, quelque chose doit se produire pour permettre à l'agent de rattachement et à l'agent étranger d'effectuer les enregistrements IP mobile suivants. Après l'enregistrement initial, le AAAH et le AAAL de la Figure 3 ne seraient pas nécessaires, et les enregistrements IP mobile suivants suivraient seulement le chemin de contrôle inférieur entre l'agent étranger et l'agent de rattachement.

Toutes les données IP mobile qui sont envoyées par FA au AAAH à travers le AAAL DOIVENT être considérées comme opaques aux serveurs AAA. Les données d'autorisation nécessaires pour les serveurs AAA DOIVENT alors leur être livrées par l'agent étranger à partir des données fournies par le nœud mobile. L'agent étranger devient un agent de traduction entre le protocole d'enregistrement IP mobile et AAA.

Comme mentionné à la Section 3, les nœuds dans deux domaines administratifs séparés doivent souvent prendre des mesures supplémentaires pour garantir leur sécurité et confidentialité, ainsi que la sécurité et la confidentialité des données qu'ils échangent. Dans l'Internet d'aujourd'hui, de telles mesures de sécurité peuvent être fournies par l'utilisation de différents algorithmes. Certains s'appuient sur l'existence d'une infrastructure de clé publique [RFC2459] ; d'autres s'appuient sur la distribution de clés symétriques aux nœuds en communication [RFC1510]. Les serveurs AAA DEVRAIENT être capables de vérifier les accréditifs en utilisant l'un ou l'autre style dans leurs interactions avec les entités IP mobile.

Afin de permettre les enregistrements suivants, les serveurs AAA DOIVENT être capables d'effectuer des distributions de clé durant le processus initial d'enregistrement IP mobile pour tout domaine administratif.

Cette distribution de clé DOIT être capable de fournir les fonctions de sécurité suivantes :

- Identifier ou créer une association de sécurité entre MN et agent de rattachement (HA) ; il est exigé du MN qu'il produise les données de [ré] authentification pour l'extension d'authentification MN--HA, qui est obligatoire sur les enregistrements IP mobile.
- Identifier ou créer une association de sécurité entre nœud mobile et agent étranger, à utiliser avec les enregistrements suivants sur le même agent étranger, afin que l'agent étranger puisse continuer d'obtenir l'assurance que le même nœud mobile a demandé la poursuite de l'autorisation pour les services IP mobile.
- Identifier ou créer une association de sécurité entre agent de rattachement et agent étranger, à utiliser avec les enregistrements suivants sur le même agent étranger, afin que l'agent étranger puisse continuer d'obtenir l'assurance que le même agent de rattachement a continué de donner l'autorisation des services IP mobile au nœud mobile.
- Participer à la distribution de l'association de sécurité (et de l'indice de paramètre de sécurité (SPI, *Security Parameter Index*) aux entités IP mobile.
- Le serveur AAA DOIT aussi être capable de valider les certificats fournis par le nœud mobile et fournir des indications fiables à l'agent étranger.
- Le AAAL DEVRAIT accepter une indication de l'agent étranger sur la durée de vie acceptable pour ses associations de sécurité avec le nœud mobile et/ou l'agent de rattachement du nœud mobile. Cette durée de vie pour ces associations de sécurité DEVRAIT être un multiple entier de la durée de vie d'enregistrement offerte par l'agent étranger au nœud mobile. Ceci PEUT permettre la tenue de la réauthentification IP mobile sans qu'il soit besoin qu'elle ait lieu au niveau de AAA, raccourcissant ainsi le temps nécessaire au ré enregistrement du nœud mobile.
- Les serveurs AAA DEVRAIENT être capables de soumettre à condition leur acceptation de l'autorisation d'un

enregistrement IP mobile selon que l'enregistrement exige un service en diffusion ou en diffusion groupée pour le nœud mobile tunnelé à travers l'agent étranger.

- De plus, le tunnelage inverse peut aussi être une exigence nécessaire pour la connexité du nœud mobile. Donc, les serveurs AAA DEVRAIENT aussi être capables de conditionner leur acceptation de l'autorisation d'un enregistrement IP mobile au fait que l'enregistrement exige la prise en charge du tunnelage inverse au domaine de rattachement à travers l'agent étranger.

La durée de vie de toute association de sécurité distribuée par le serveur AAA pour être utilisée avec IP mobile DEVRAIT être assez longue pour éviter de trop fréquentes initialisations de la distribution de clés AAA, car chaque invocation de ce processus va probablement causer de longs délais entre les [ré] enregistrements [IP-RTP]. Les délais d'enregistrement dans IP mobile causent d'abandon de paquets et des perturbations notables du service. Noter que toute clé distribuée par AAAH à l'agent étranger et à l'agent de rattachement PEUT être utilisée pour initier l'échange de clé Internet (IKE, *Internet Key Exchange*) [RFC2409].

Noter de plus que le nœud mobile et l'agent de rattachement peuvent bien avoir une association de sécurité établie qui ne dépende d'aucune action de l'AAAH.

5.1 IP mobile avec adresses IP dynamiques

Selon la section 4, de nombreuses personnes aimeraient que leur nœud mobile soit identifié par son NAI, et obtenir une adresse de rattachement allouée de façon dynamique pour l'utiliser dans le domaine étranger. Ces personnes peuvent souvent n'être pas concernées par les détails de la façon dont leur ordinateur met en œuvre IP mobile, et peuvent bien sûr n'avoir aucune connaissance de leur agent de rattachement ou de toute association de sécurité sauf entre eux-mêmes et le AAAH (voix la Figure 2). Dans ce cas, les données de l'enregistrement IP mobile doivent être portées avec les messages AAA. Le domaine de rattachement AAA et le domaine de rattachement HA doivent faire partie du même domaine administratif.

IP mobile exige que l'adresse de rattachement allouée au nœud mobile appartienne au même sous réseau que l'agent de rattachement qui fournit le service au nœud mobile. Pour une utilisation efficace des adresses IP de rattachement, le AAAH DEVRAIT être capable de choisir un agent de rattachement à utiliser avec l'adresse de rattachement nouvellement allouée. Dans de nombreux cas, le nœud mobile va déjà connaître l'adresse de son agent de rattachement, même si le nœud mobile n'a pas déjà une adresse de rattachement existante. Donc, le AAAH DOIT être capable de coordonner l'allocation d'une adresse de rattachement avec un agent de rattachement qui peut être désigné par le nœud mobile.

Allouer une adresse de rattachement et un agent de rattachement au mobile donnerait une simplification supplémentaire des besoins de configuration pour le nœud mobile du client. Actuellement, dans la spécification IP mobile [RFC2002] un nœud mobile doit être configuré avec une adresse de rattachement et l'adresse d'un agent de rattachement, ainsi qu'avec une association de sécurité avec cet agent de rattachement. À l'opposé, les caractéristiques AAA proposées exigeraient seulement que le nœud mobile soit configuré avec son NAI et un secret partagé sûr à utiliser par le AAAH. L'adresse de rattachement du nœud mobile, l'adresse de son agent de rattachement, l'association de sécurité entre le nœud mobile et l'agent de rattachement, et même l'identité (nom DNS ou adresse IP) de l'AAAH peuvent toutes être déterminées dynamiquement au titre de l'enregistrement initial IP mobile auprès de l'agent de mobilité dans le domaine étranger (c'est-à-dire, un agent étranger avec des caractéristiques d'interface AAA). Néanmoins, le nœud mobile peut choisir d'inclure l'extension de sécurité MN-HA ainsi que les accréditifs AAA, et le modèle IP mobile et serveur AAA proposé DOIT fonctionner quand les deux sont présents.

La raison de toute cette simplification est que le NAI code l'identité du client ainsi que le nom du domaine de rattachement du client ; cela suit la pratique existante dans l'industrie pour la façon dont les NAI sont utilisés aujourd'hui (voir la Section 4). Le nom du domaine de rattachement est alors disponible pour être utilisé par l'AAA local (AAAL) pour localiser le AAA de rattachement qui dessert le domaine de rattachement du client. Dans le modèle général, le AAAL aurait aussi à identifier l'association de sécurité appropriée à utiliser avec cet AAAH. La Section 6 expose un moyen de réduire le nombre des associations de sécurité qui doivent être maintenues entre des paires de serveurs AAA comme le AAAL et l'AAAH qu'on vient de décrire.

5.2 Pare-feu et AAA

IP mobile a rencontré des difficultés de déploiement relatives à la traversée de pare-feu ; voir par exemple la [RFC2356]. Comme le pare-feu et le serveur AAA peuvent faire partie du même domaine administratif, on propose que le serveur AAA DEVRAIT être capable de produire des messages de contrôle et des clés au pare-feu à la frontière de son domaine administratif, qui vont configurer le pare-feu pour qu'il soit perméable aux enregistrements IP mobile et au trafic de données provenant du nœud mobile.

5.3 IP mobile avec agents de rattachement locaux

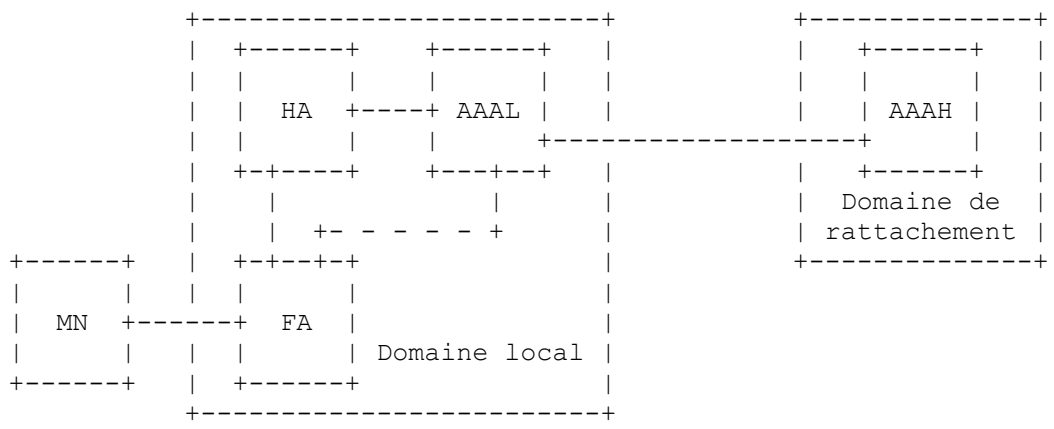

Figure 4 : Agent de rattachement alloué par l'AAAL

Dans certains modèles IP mobile, les nœuds mobiles s'amorcent sur des sous réseaux qui sont techniquement des sous réseaux étrangers, mais les services dont ils ont besoin sont locaux, et donc la communication avec le sous réseau de rattachement comme si ils résidaient sur le domaine de rattachement n'est pas nécessaire. Tant que le nœud mobile peut obtenir une adresse acheminable de l'intérieur du domaine courant (qu'il soit adressé publiquement, ou de façon privée) il peut utiliser IP mobile pour circuler autour de ce domaine, en appelant le sous réseau sur lequel il est connecté son rattachement temporaire. Cette adresse sera probablement allouée de façon dynamique sur demande du nœud mobile.

Dans de telles situations, lorsque le client veut utiliser une adresse IP allouée de façon dynamique et n'a aucune préférence pour la localisation du réseau de rattachement (ni géographique ni topologique) le serveur AAA local peut être capable d'offrir ce service d'allocation supplémentaire au client. Ensuite, l'agent de rattachement sera localisé dans le domaine local, qui va probablement offrir de plus courts délais pour les nouveaux enregistrements IP mobile.

À la Figure 4, l'AAAL a reçu une demande du nœud mobile pour allouer un agent de rattachement dans le domaine local. Le nouvel agent de rattachement reçoit des clés de l'AAAL pour permettre de futurs enregistrements IP mobile. D'après la figure, il est évident qu'une telle configuration évite les problèmes avec la protection du pare-feu aux frontières du domaine, comme ceux qui ont été décrits brièvement au paragraphe 5.2. D'un autre côté, cette configuration rend difficile au nœud mobile de recevoir des données de tout partenaire de communication dans le domaine administratif de rattachement du nœud mobile. Noter que, dans ce modèle, l'adresse de rattachement du nœud mobile est affiliée au domaine étranger pour les besoins d'acheminement. Donc, toute mise à jour dynamique au DNS, pour associer le nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name* [RFC1035]) de rattachement du nœud mobile avec sa nouvelle adresse IP, va exiger l'insertion d'une adresse IP étrangère dans la base de données du serveur DNS de rattachement.

5.4 IP mobile avec payements locaux

Comme le AAAL est supposé être capable d'allouer un agent de rattachement local sur demande, on peut faire une autre simplification. Dans les cas où le AAAL peut gérer toute fonction nécessaire d'autorisation en local (par exemple, si le client paye en espèces ou en carte de crédit) il n'est alors pas besoin d'un protocole ou infrastructure AAA pour interagir avec le AAAH. La configuration simple qui en résulte est illustrée à la Figure 5.

Dans ce modèle simplifié, on peut considérer que le rôle de l'AAAH est joué par un gouvernement national (dans le cas de payement en espèces) ou par un service d'autorisation de carte si le payement est par carte de crédit, ou quelque autre autorité acceptable par toutes les parties. Alors, le AAAL s'attend à ce que ces autorités externes garantissent la valeur représentée par les accréditifs de payement du client (espèces ou carte de crédit).

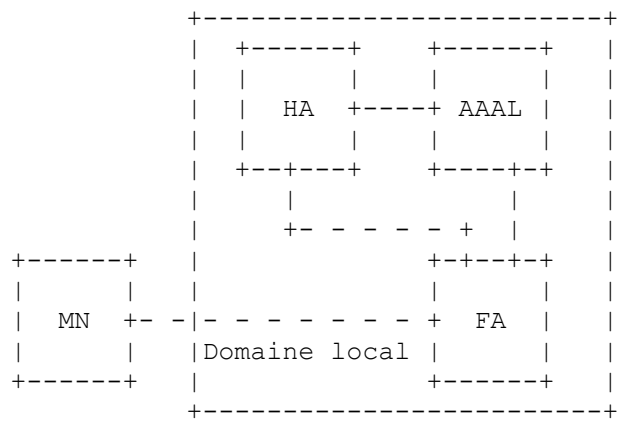

Figure 5 : Payement local pour services IP mobile locaux

Il y a probablement d'autres cas où l'accès aux ressources locales est accordé aux clients, ou l'accès à l'Internet, sans aucune charges du tout. De telles configurations peuvent se trouver dans les aéroports et autres zones communes où les clients d'affaires passent du temps. Le fournisseur de service peut trouver une rétribution suffisante dans la bonne volonté des clients, ou dans des annonces diffusées sur les portails Internet qui sont utilisés par les clients. Dans de telles situations, l'AAAL DEVRAIT quand même allouer un agent de rattachement, les clés appropriées, et l'adresse de rattachement du nœud mobile.

5.5 Transfert cellulaire rapide

Comme le mouvement d'une zone de couverture à une autre zone de couverture peut être fréquent dans les réseaux IP mobiles, il est impératif que la latence impliquée dans le processus de transfert inter cellulaire soit minimisée. Voir, par exemple, le document sur l'optimisation de chemin [RFC4449] sur une façon de le faire en utilisant les mises à jour de lien. Lorsque le nœud mobile entre dans un nouveau sous réseau visité, il serait souhaitable qu'il fournisse le NAI du précédent agent étranger. Le nouvel agent étranger peut utiliser ces informations pour contacter le précédent FA pour restituer les informations de clé de session du centre de distribution des clés, ou il peut tenter de restituer les clés depuis le AAAL. Si l'AAAL ne peut pas fournir les informations de clés nécessaires, la demande devra être envoyée à l'AAAH du nœud mobile pour restituer les nouvelles informations de clés. Après l'autorisation initiale, les autorisations ultérieures DEVRAIENT être faites en local au sein du domaine local.

Lorsque un MN se déplace dans un nouveau sous réseau étranger par suite d'un transfert inter cellulaire, il est alors servi par un FA différent, et l'AAAL de ce domaine peut contacter l'AAAL dans le domaine que le MN vient de quitter pour vérifier l'authenticité du MN et/ou obtenir les clés de session. Le nouvel AAAL desservant peut déterminer l'adresse de l'AAAL dans le domaine visité précédemment à partir des informations de NAI du FA précédent fournies par le MN.

6. Modèle du courtier

Le dessin de la Figure 1 montre une configuration dans laquelle l'autorité locale et l'autorité de rattachement doivent avoir une confiance mutuelle. Selon le modèle de sécurité utilisé, cette configuration peut causer une croissance exponentielle du nombre de relations de confiance, lorsque le nombre d'autorités AAA (AAAL et AAAH) augmente. Ceci a été identifié comme problème par le groupe de travail roamops [RFC2477], et toute proposition AAA DOIT résoudre ce problème. L'utilisation de courtiers résout beaucoup des problèmes d'adaptation associés à l'exigence de relations directes d'affaire/itinérance entre chacun des deux domaines administratifs. Afin de fournir des réseaux adaptables dans les réseaux très divers des fournisseurs de service dans lesquels il y a de nombreux domaines (par exemple, de nombreux fournisseurs de service et un grand nombre de réseaux privés) plusieurs couches de courtiers DOIVENT être prises en charge pour les deus modèles de courtier décrits.

L'intégrité ou la confidentialité des informations entre les domaines de rattachement et desservant peut être réalisée par des associations de sécurité bond par bond ou de bout en bout établies avec l'aide de l'infrastructure de courtier. Un courtier peut jouer le rôle de mandataire entre deux domaines administratifs qui ont des associations de sécurité avec le courtier, et relayer les messages AAA dans les deux sens en toute sécurité.

Autrement, un courtier peut aussi permettre aux deux domaines avec lesquels il a des associations, mais où les domaines eux-mêmes n'ont pas d'association directe, d'établir une association de sécurité, court-circuitant par là le courtier pour le transport des messages entre les domaines. Ceci peut être établi en faisant que le courtier relaye une clé secrète partagée par

les deux domaines qui essayent d'établir une communication sûre et qu'ensuite les domaines utilisent les clés fournies par le courtier pour établir une association de sécurité.

En supposant que l'AAAB accepte la responsabilité du payement au domaine desservant au nom du domaine de rattachement, le domaine desservant est assuré de recevoir les payements pour les services offerts. Cependant, le courtier de redirection va généralement exiger une copie des messages d'autorisation de la part du domaine de rattachement et des messages de comptabilité de la part du domaine desservant, afin que le courtier détermine si il veut accepter la responsabilité de l'autorisation et de l'utilisation des services. Si le courtier n'accepte pas une telle responsabilité pour une raison quelconque, il doit alors être capable de terminer le service à un nœud mobile dans le réseau desservant. Dans le cas om plusieurs courtiers sont impliqués, dans la plupart des situations, tous les courtiers doivent être en copie. Cela peut représenter une charge supplémentaire pour les agents étrangers et les AAAL.

Bien que ce mécanisme puisse réduire la latence dans le transit des messages entre les domaines après que le courtier a terminé son rôle, il peut y avoir de nombreux messages en plus par suite des copies supplémentaires des messages d'autorisation et de comptabilité aux courtiers impliqués. Il peut aussi y avoir une latence supplémentaire pour l'accès initial au réseau, en particulier lorsque une nouvelle association de sécurité doit être créée entre AAAL et AAAH (par exemple, venant de l'utilisation de ISAKMP). Ces délais peuvent devenir des facteurs importants pour les applications où la latence est critique.

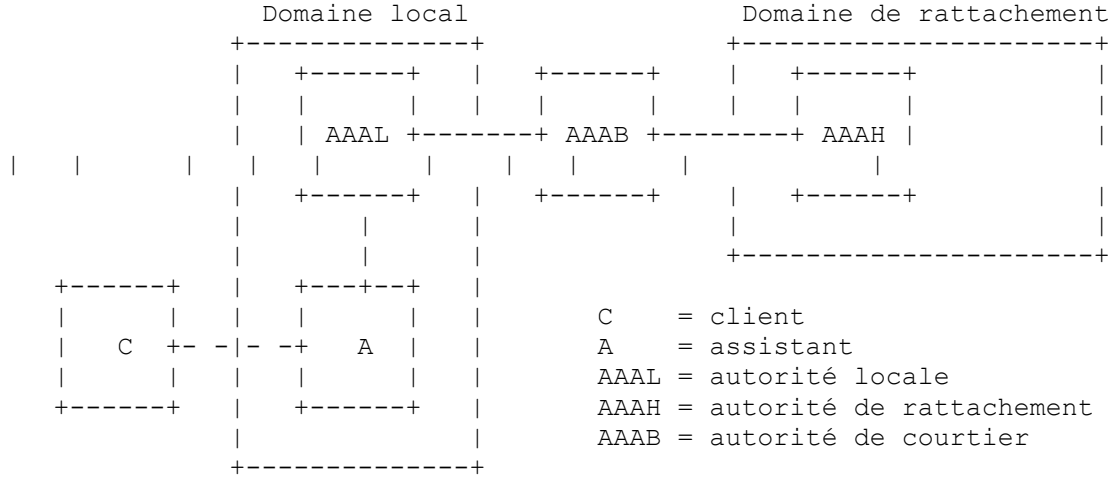

Figure 6 : Serveurs AAA utilisant un courtier

Le AAAB dans la figure 6 est le serveur d'autorité du courtier. Le courtier agit comme agent de règlement, assurant la sécurité et un point de contact central pour de nombreux fournisseurs de service et entreprises.

Le AAAB permet aux domaines local et de rattachement de coopérer sans exiger que chacun des réseaux ait une relation directe de sécurité ou d'affaire avec tous les autres réseaux. Donc, les courtiers offrent l'adaptabilité nécessaire pour gérer les relations de confiance entre des domaines réseau autrement indépendants. L'utilisation d'un courtier n'empêche pas de gérer des relations de confiance séparées entre domaines, mais cela n'offre pas une solution de remplacement à le faire. Tout comme avec le AAAH et l'AAAL (voir la Section 5) les données spécifiques des messages de contrôle IP mobile NE DOIVENT PAS être traitées par le AAAB. Tous les accréditifs ou les données de comptabilité à traiter par le AAAB doivent être présents dans les unités de message AAA, non extraites des extensions de protocole IP mobile.

Les exigences suivantes proviennent principalement de la [RFC2607], qui expose l'utilisation des courtiers dans le cas particulier d'autorisation pour des utilisateurs téléphoniques en itinérance.

- permettre la gestion de la confiance avec les domaines externes au moyen de courtiers AAA.
- fiabilité de la comptabilité. Les données comptables qui traversent l'Internet peuvent subir des pertes de paquets substantielles. Comme les paquets de comptabilité peuvent traverser un ou plusieurs point d'autorisation intermédiaires (par exemple, des courtiers) la retransmission est nécessaire à partir des points intermédiaires pour éviter de longs délais de bout en bout.
- sécurité de bout en bout. Le domaine local et le domaine de rattachement doivent être capables de vérifier les signatures au sein du message, même si le message est passé à travers un serveur d'autorité intermédiaire.
- comme le AAAH dans le domaine de rattachement PEUT envoyer des informations sensibles, comme des clés d'enregistrement, le courtier DOIT être capable de passer des données chiffrées entre les serveurs AAA.

Le besoin de sécurité de bout en bout résulte des attaques suivantes qui ont été identifiées lorsque des opérations par courtier utilisent RADIUS [RFC2138] (voir la [RFC2607] pour plus d'informations sur les attaques individuelles) :

+ édition de message
+ édition d'attributs
+ vol de secrets partagés
+ vol et modification des données comptables
+ attaques en répétition
+ capture de connexion
+ comptabilité frauduleuse

Ce sont de sérieux problèmes dont la persistance ne peut pas être admise dans un protocole et une infrastructure AAA acceptables.

7. Considérations sur la sécurité

Ceci est un document sur les exigences de AAA fondé sur IP mobile. Comme AAA se fonde sur la sécurité, la plus grande partie du présent document traite des considérations de sécurité que AAA DOIT faire au nom de IP mobile. Comme avec toute proposition de sécurité, ajouter des entités qui interagissent en utilisant des protocoles de sécurité crée de nouvelles exigences administratives pour maintenir les associations de sécurité appropriées entre les entités. Dans le cas des services AAA proposés, ces exigences administratives sont cependant naturelles, et déjà bien comprises dans l'Internet d'aujourd'hui à cause de l'expérience de l'accès réseau numéroté.

8. Considérations sur IPv6

La principale différence entre IP mobile pour IPv4 et IP mobile v6 est que dans IPv6 il n'y a pas d'agent étranger. La fonction d'assistant doit donc être localisée ailleurs. Les dépositaires logiques de cette fonction sont soit au routeur local, pour l'autoconfiguration d'adresse sans état, soit autrement au plus proche serveur DHCPv6, pour l'autoconfiguration d'adresse à états pleins. Dans ce dernier cas, il est possible qu'il y ait une relation étroite entre le serveur DHCPv6 et le AAALv6, mais on pense que les fonctions du protocole devraient quand même être tenues séparées.

Le MN-NAI serait également utile pour identifier le nœud mobile auprès du AAALv6 comme c'est décrit précédemment.

9. Remerciements

Merci à Gopal Dommety et Basavaraj Patil pour leur participation au sous comité IP mobile du groupe de travail AAA qui a formulé les exigences détaillées dans le présent document. Merci à N. Asokan pour ses commentaires pertinents sur la liste de diffusion mobile-ip. Une partie du texte du présent document a été tirée d'un projet dont Pat Calhoun était co-auteur. Patrik Flykt a suggéré du texte sur la façon de permettre que les fonctions du domaine de rattachement AAA soient séparées du domaine qui gère l'adresse de rattachement de l'ordinateur mobile.

Les exigences des paragraphes 5.5 et 3.1 ont été tirées d'un projet soumis par les membres du groupe de travail TR45.6 du TIA. Nous tenons à saluer le travail fait par les auteurs de ce projet : Tom Hiller, Pat Walsh, Xing Chen, Mark Munson, Gopal Dommety, Sanjeevan Sivalingham, Byng-Keun Lim, Pete McCann, Brent Hirschman, Serge Manning, Ray Hsu, Hang Koo, Mark Lipford, Pat Calhoun, Eric Jaques, Ed Campbell, et Yingchun Xu.

10. Références

[IP-RTP] Ramon Caceres et Liviu Iftode, "Improving the Performance of Reliable Transport Protocols in Mobile Computing Environments". IEEE Journal on Selected Areas in Communications, 13(5):850-- 857, juin 1995.

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par la* RFC6604)

[RFC1510] J. Kohl et C. Neuman, "Service Kerberos d'authentification de réseau (v5)", septembre 1993. *(Obsolète, voir* RFC6649)

[RFC2002] C. Perkins, éd., "Prise en charge de la mobilité sur IP", octobre 1996. (*Obsolète, voir* RFC3220) *(P.S.)*

[RFC2003] C. Perkins, "Encapsulation de IP dans IP", octobre 1996. (*MàJ par* RFC 3168, RFC 6864, Errata) *(P.S.)*

[RFC2004] C. Perkins, "Encapsulation minimale au sein de IP", octobre 1996. *(P.S.)*

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

[RFC2138] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Service d'authentification distante d'utilisateur appelant (RADIUS)", avril 1997. *(Remplace* RFC2058) (*Obsolète, voir* RFC2865) *(P.S.)*

[RFC2290] J. Solomon, S. Glass, "Option de configuration IPv4 mobile pour PPP IPCP", février 1998. (*MàJ par* RFC2794) *(P.S.)*

[RFC2356] G. Montenegro, V. Gupta, "Traversée de pare-feu SKIP de Sun pour IP mobile", juin 1998. *(Information)*

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2459] R. Housley, W. Ford, W. Polk et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de CRL pour l'Internet", janvier 1999. (*Obsolète, voir la* RFC3280) *(P.S.)*

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

[RFC2486] B. Aboba, M. Beadles, "Identifiant d'accès réseau", janvier 1999. (*Obsolète, voir* RFC4282) *(P.S.)*

[RFC2607] B. Aboba, J. Vollbrecht, "Chaînage de mandataire et mise en œuvre de politique dans l'itinérance", juin 1999.

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

[RFC4449] C. Perkins, "Sécurisation de l'optimisation de chemin IPv6 mobile avec une clé partagée statique", juin 2006.

11. Adresses

Le groupe de travail peut être contacté via ses présidents actuels :

Basavaraj Patil
Nokia
6000 Connection Drive
Irving, TX 75039
USA
téléphone : +1 972-894-6709
mél : Basavaraj.Patil@nokia.com

Phil Roberts
Motorola
1501 West Shure Drive
Arlington Heights, IL 60004
USA
téléphone : +1 847-632-3148
mél : QA3445@email.mot.com

Les questions relatives au présent mémoire peuvent être adressées à :

Pat R. Calhoun
Network et Security Center
Sun Microsystems Labs
15 Network Circle
Menlo Park, California 94025
USA
tél. : +1 650-786-7733
pcalhoun@eng.sun.com

Gopal Dommety
IOS Network Protocols
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
tél. : +1-408-525-1404
gdommety@cisco.com

Steven M. Glass
Sun Microsystems
1 Network Drive
Burlington, MA 01803
USA
tél. : +1-781-442-0504
steven.glass@sun.com

Charles E. Perkins
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
tél. : +1-650 625-2986
charliep@iprg.nokia.com

Stuart Jacobs
Secure Systems Dpt
GTE Laboratories
40 Sylvan Road
Waltham, MA 02451-1128
USA
tél. : +1 781-466-3076
mél : sjacobs@gte.com

Tom Hiller
Lucent Technologies
Rm 2F-218
263 Shuman Blvd
Naperville, IL 60566
USA
tél. : +1 630 979 7673
mél : tomhiller@lucent.com

Peter J. McCann
Lucent Technologies
Rm 2Z-305
263 Shuman Blvd
Naperville, IL 60566
USA
tél. : +1 630 713 9359
mél : mccap@lucent.com

Basavaraj Patil
Nokia
6000 Connection Drive
Irving, TX 75039
USA
tél. : +1 972-894-6709
mél : Basavaraj.Patil@nokia.com

12. Déclaration complète de droits de reproduction

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