Groupe de travail Réseau
Request for Comments : 3957
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

C. Perkins, Nokia Research Center
P. Calhoun, Airespace

mars 2005

Clés d'enregistrement d'authentification, d'autorisation, et de comptabilité (AAA) pour IPv4 mobile

Résumé
Les serveurs d'authentification, d'autorisation et de comptabilité (AAA, *Authentication, Authorization, and Accounting*) tels que RADIUS et DIAMETER, sont utilisés au sein de l'Internet d'aujourd'hui pour assurer des services d'authentification et d'autorisation pour les appels commutés des ordinateurs. IP mobile pour IPv4 exige une forte authentification entre le nœud mobile et son agent de rattachement. Lorsque le nœud mobile partage une association de sécurité AAA avec son serveur AAA de rattachement, il est cependant possible d'utiliser cette association de sécurité AAA pour créer des associations de sécurité de mobilité dérivées entre le nœud mobile et son agent de rattachement, et encore entre le nœud mobile et l'agent étranger qui offre actuellement la connexité au nœud mobile. Le présent document spécifie des extensions aux messages d'enregistrement IP mobile qui peuvent être utilisés pour créer des associations de sécurité de mobilité entre le nœud mobile et son agent de rattachement, et/ou entre le nœud mobile et son agent étranger.

Table des Matières

1. Introduction

Les serveurs AAA, tels que RADIUS [RFC2865] et DIAMETER [RFC3588], sont utilisés dans l'Internet d'aujourd'hui pour fournir des services d'authentification et d'autorisation pour les appels commutés des ordinateurs. De tels services seront probablement précieux pour les nœuds mobiles qui utilisent IP Mobile pour IPv4 [RFC3344], lorsque les nœuds

tentent de se connecter dans des domaines étrangers à des serveurs AAA. Dans le présent document, IP mobile pour IPv4 est appelé "IPv4 mobile" ou juste "IP mobile" pour abréger, car aucune confusion n'est possible avec d'autres versions. Les exigences pour les interactions entre AAA et IP mobile sont précisées dans la [RFC2977] ; ce document décrit une infrastructure qui permet aux serveurs AAA d'authentifier et autoriser les demandes d'accès réseau des nœuds mobiles. Voir aussi l'Appendice A. La demande d'enregistrement IP mobile est considérée comme une demande d'accès au réseau. Il est alors possible d'augmenter les fonctionnalités des agents de mobilité IP mobile afin qu'ils puissent faire la traduction entre les messages d'enregistrement IP mobile et les messages utilisés au sein de l'infrastructure AAA, comme décrit dans la RFC 2977. Les agents de mobilité et les serveurs AAA qui se conforment aux exigences de la RFC 2977 peuvent être considérés comme des entités réseau appropriées pour prendre en charge les types de message spécifiés dans ce document. Prière de consulter la [RFC2977] pour les détails.

La présente spécification utilise une seule association de sécurité AAA pour créer les associations de sécurité de mobilité dérivées. Une association de sécurité de mobilité dans la présente spécification est une connexion simple qui sert à authentifier le trafic de contrôle MIPv4 entre un nœud mobile (MN, *mobile node*) et un agent de rattachement (HA, *home agent*) et/ou un MN et un agent étranger (FA, *foreign agent*). Une association de sécurité de mobilité est identifiée par ses deux points d'extrémité, comme une adresse IP de MN et une adresse IP de HA, et un indice de paramètre de sécurité (SPI, *Security Parameter Index*). Deux nœuds peuvent avoir une ou plusieurs associations de sécurité de mobilité établies entre chacun d'eux ; cependant, normalement il n'y a pas de raison d'avoir plus d'une association de sécurité de mobilité entre deux nœuds.

Le présent document spécifie des extensions aux messages d'enregistrement IP mobile qui peuvent être utilisées pour créer des associations de sécurité de mobilité entre le MN et le FA et/ou le MN et le HA sur la base de l'association de sécurité AAA entre le MN et le serveur AAA. Ces nouvelles associations de sécurité de mobilité peuvent alors être utilisées pour calculer les données d'authentification nécessaires pour les extensions d'authentification utilisées dans les messages de contrôle IP mobile.

On suppose que l'association de sécurité entre le nœud mobile et son serveur AAA a été configurée de façon appropriée pour que le serveur AAA puisse fournir le matériel de chiffrement à utiliser comme base de la ou des associations de sécurité de mobilité nécessaires entre le nœud mobile et ses agents de mobilité éventuels.

Les serveurs AAA utilisent normalement un identifiant d'accès réseau (NAI, *Network Access Identifier*) [RFC2486] pour identifier de façon univoque le nœud mobile ; l'adresse de rattachement du nœud mobile n'est pas toujours nécessaire pour assurer cette fonction. Donc, il est possible qu'un nœud mobile s'authentifie lui-même, et soit autorisé à se connecter au domaine étranger, sans avoir d'adresse de rattachement. Cependant, pour que IP mobile fonctionne, le nœud mobile est obligé d'avoir une adresse de rattachement et une association de sécurité de mobilité [RFC3344] avec son agent de rattachement. Lorsque le paquet de réponse d'enregistrement IP mobile est authentifié par l'extension d'authentification MN-AAA [RFC3012], le nœud mobile peut vérifier que le matériel de chiffrement contenu dans les extensions a été produit par le serveur AAA, et donc peut être fiablement utilisé pour créer des associations de sécurité de mobilité avec l'agent de rattachement et/ou l'agent étranger.

On suppose aussi que les entités AAA impliquées (c'est-à-dire, le AAAH, le AAAL, et les dispositifs d'interface AAA des agents étrangers et des agents de rattachement) ont toutes les moyens, qui sortent du domaine d'application du présent document, d'échanger des clés. Les extensions de ce document sont destinées à fonctionner avec toute suite de protocoles AAA qui permet un tel échange, pour autant qu'elle satisfasse aux exigences spécifiées dans la [RFC2977]. Un tel protocole AAA est défini dans le cadre Diameter [RFC4004].

2. Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

AAA : authentification, autorisation, et comptabilité (voir la [RFC3127]).

entité AAA : nœud réseau qui traite les messages AAA conformément aux exigences des protocoles AAA (voir la [RFC3127]).

association de sécurité AAA : association de sécurité entre une entité AAA et un autre nœud nécessitant les services de cette entité AAA. Dans ce document, toutes les associations de sécurité AAA sont entre un nœud mobile et son serveur AAA de rattachement (AAAH). Une association de sécurité AAA de nœud mobile avec son serveur AAA de rattachement (AAAH) peut se fonder soit sur l'adresse IP du nœud mobile, soit sur son NAI [RFC2486]. La

clé est appelée une "clé AAA" dans la présente spécification.

clé : nombre, gardé secret. Seuls les nœuds en possession de la clé ont un espoir d'utiliser la transformation de sécurité pour obtenir des résultats corrects.

Nom occasionnel de génération de clé *(Key Generation Nonce)* : données de nom occasionnel utilisées pour les besoins d'une création de clé.

association de sécurité de mobilité : une association de sécurité de mobilité est une connexion unidirectionnelle qui applique les services de sécurité au trafic de contrôle MIPv4 de la RFC 3344 entre un MN et un HA (ou un MN et un FA) en utilisant les extensions d'authentification de la RFC 3344. Une association de sécurité de mobilité est identifiée de façon univoque par les adresses IP de source et de destination de l'homologue et un SPI. Deux nœuds peuvent avoir une ou plusieurs associations de sécurité de mobilité ; cependant, normalement, il n'y a pas de raison d'avoir plus d'une association de sécurité de mobilité entre deux nœuds, sauf comme condition transitoire durant des événements de changement de clé.

clé d'enregistrement : clé utilisée dans l'association de sécurité de mobilité MN-FA ou MN-HA. Une clé d'enregistrement n'est normalement utilisée qu'une fois ou un très petit nombre de fois, et seulement pour des besoins de vérification d'un petit volume de données d'authentification.

algorithme de sécurité : ensemble de règles d'utilisation de données d'entrée et d'une clé secrète pour produire des données à utiliser dans des protocoles de sécurité.

SPI *(Security Parameters Index)* : indice des paramètres de sécurité. Le SPI est une valeur arbitraire de 32 bits qui aide à l'identification d'une association de sécurité AAA, IP, ou de mobilité.

Les autres termes sont utilisés comme défini dans la spécification IP mobile de base [RFC3344]. De plus, afin de simplifier la discussion, on a utilisé le terme "extension" plutôt que "sous type de l'extension généralisée" dans de nombreux cas. Ainsi, par exemple, au lieu d'utiliser la phrase "le nom occasionnel de génération de clé MN-FA provenant du sous type AAA de l'extension généralisée de réponse de nom occasionnel de génération de clé MN-FA", on va plutôt utiliser la phrase "le nom occasionnel de génération de clé MN-FA provenant de l'extension AAA".

3. Généralités sur les opérations avec les extensions de nom occasionnel de génération de clé

Lorsque un nœud mobile dépend d'une infrastructure AAA pour obtenir l'autorisation de la connexité réseau et de l'enregistrement IP mobile, il peut ne pas avoir d'association de sécurité de mobilité préexistante avec son agent de rattachement, ou avec l'agent étranger qui contrôle l'accès au réseau étranger. Les extensions définies dans le présent document permettent à une entité AAA de fournir aux nœuds mobiles le matériel de chiffrement à utiliser comme base de son association de sécurité de mobilité avec les agents mobiles. L'entité AAA qui va agir sur ces extensions fait partie de l'infrastructure AAA, et est normalement identifiée au sein du domaine étranger par des méthodes qui sortent du domaine d'application de la présente spécification (voir l'Appendice A).

Le matériel de chiffrement peut être demandé par le nœud mobile dans de nouvelles extensions (définies ci-dessous) pour des messages de demande d'enregistrement IP mobile, et fourni au nœud mobile dans des extensions aux messages de réponse d'enregistrement IP mobile. Autrement, le serveur AAA PEUT fournir du matériel de chiffrement non sollicité via les agents de mobilité aux nœuds mobiles ; le nœud mobile DOIT alors calculer de nouvelles clés et mettre à jour ou créer son association de sécurité de mobilité pertinente. La méthode par laquelle le matériel de chiffrement est fourni aux agents de mobilité eux-mêmes sort du domaine d'application du présent document, et va dépendre des détails particuliers de l'architecture de sécurité pour les serveurs AAA dans les domaines étrangers et de rattachement (voir la RFC 2977 et l'Appendice A). Pour les besoins du présent document, on suppose qu'il y a une infrastructure AAA convenable disponible pour les agents de rattachement et étrangers, et que le nœud mobile a bien une association de sécurité AAA avec au moins un serveur AAA dans son domaine de rattachement.

Lorsque un nœud mobile voyage loin de son rattachement, il peut n'avoir pas d'association de sécurité de mobilité avec son agent de rattachement, peut-être parce qu'il n'a pas encore une adresse de rattachement [RFC2794]. Le protocole et les messages dans le présent document sont destinés à faciliter les opérations suivantes qui peuvent se produire entre le nœud mobile, l'agent étranger, l'agent de rattachement, et les serveurs AAA dans le domaine visité (local) (Authentification, Autorisation et comptabilité locale ou AAAL) et dans le domaine de rattachement (Authentification, Autorisation, et comptabilité de rattachement ou AAAH). Dans les séquences de messages suivantes, les seuls flux de messages spécifiés dans ce document sont les demandes d'enregistrement entre le nœud mobile et l'agent étranger, et les réponses d'enregistrement entre l'agent étranger et le nœud mobile. Les autres messages décrits ici résultent de l'action présumée des

entités AAA comme décrit dans la RFC 2977. Voir aussi l'Appendice B.

1. Si le nœud mobile n'a pas d'association de sécurité de mobilité avec l'agent étranger, il DEVRAIT inclure une extension Demande de nom occasionnel de génération de clé MN-FA (voir le paragraphe 6.1) au titre de la demande d'enregistrement qu'il envoie à l'agent étranger.

2. Si le nœud mobile n'a pas d'association de sécurité de mobilité avec l'agent de rattachement, il DOIT ajouter une extension Demande de nom occasionnel de génération de clé MN-HA (voir le paragraphe 6.3) au titre de la demande d'enregistrement qu'il envoie à l'agent étranger.

3. Si une ou plusieurs extensions Demande de nom occasionnel de génération de clé AAA ont été ajoutées, le nœud mobile DOIT ajouter l'extension Authentification MN-AAA à sa demande d'enregistrement.

4. Par l'action de l'agent étranger, qui est présumé être aussi une entité AAA, les demandes de clés et les données d'authentification du nœud mobile sont transférées au serveur local AAA (AAAL), normalement après leur reformatage pour qu'elles tiennent dans les messages AAA appropriés, ce qui sort du domaine d'application de ce document.

5. Après la vérification des informations au sein de l'extension d'authentification MN-AAA par le serveur AAA dans le domaine de rattachement (AAAH), il génère alors aussi le matériel de chiffrement qui a été demandé par le nœud mobile, pour les associations de sécurité de mobilité nécessaires.

6. Les clés respectives pour les associations de sécurité de mobilité sont distribuées à l'agent de rattachement et à l'agent étranger via le protocole AAA.

7. Le nœud mobile reçoit le message Réponse d'enregistrement de l'agent étranger.

8. Si une extension Demande de nom occasionnel de génération de clé MN-HA provenant de AAA est présente dans le message Demande d'enregistrement, le nœud mobile DOIT alors créer ou mettre à jour son association de sécurité de mobilité avec l'agent de rattachement indiqué dans la réponse d'enregistrement correspondante, en utilisant la clé calculée à partir du matériel de chiffrement dans l'extension Nom occasionnel de génération de clé MN-HA provenant de AAA. Dans ce cas, si aucune extension Réponse de nom occasionnel de génération de clé MN-HA n'est présente, le nœud mobile DOIT éliminer la réponse d'enregistrement.

9. En utilisant son association de sécurité de mobilité (peut-être de création nouvelle) avec l'agent de rattachement, le nœud mobile authentifie le message Réponse d'enregistrement en vérifiant les données d'authentification dans l'extension Authentification de rattachement mobile. Si la vérification échoue, le MN DOIT éliminer la réponse d'enregistrement et la nouvelle association de sécurité de mobilité, revenant à l'ancienne association de sécurité de mobilité avec l'agent de rattachement, si il en est un.

10 Si la réponse d'enregistrement réussit l'authentification et contient une extension Nom occasionnel de génération de clé MN-FA provenant de AAA (voir le paragraphe 6.2) le nœud mobile génère la clé d'enregistrement en utilisant le nom occasionnel de génération de clé fourni, conformément à son association de sécurité AAA avec l'AAA. La clé d'enregistrement résultante est utilisée pour établir l'association de sécurité de mobilité du nœud mobile avec son agent étranger, et est utilisée pour calculer les données d'authentification utilisées dans l'extension d'authentification de mobile étranger.

Si la vérification de l'extension Authentification de mobile étranger échoue, et si l'extension Réponse de nom occasionnel de génération de clé MN-FA n'était pas protégée par une autre extension d'authentification valide, le MN DOIT éliminer la nouvelle association de sécurité de mobilité, revenant à l'ancienne association de sécurité de mobilité avec l'agent étranger, si il en est un.

Toute réponse d'enregistrement qui contient l'extension Nom occasionnel de génération de clé MN-HA provenant de AAA DOIT aussi contenir une extension Authentification de mobile de rattachement suivante, créée en utilisant la clé MN-HA générée. De façon similaire, une réponse qui contient l'extension Nom occasionnel de génération de clé MN-FA provenant de AAA DOIT aussi contenir une extension Authentification de mobile étranger suivante, créée en utilisant la clé d'enregistrement.

4. Associations de sécurité de mobilité

Les associations de sécurité de mobilité entre les entités IP mobile (nœuds mobiles, agents de rattachement, agents étrangers) contiennent les informations nécessaires de clé de chiffrement et un moyen pour identifier la transformation

cryptographique qui utilise la clé pour produire les informations d'authentification qui sont présentes dans l'extension Authentification de mobile de rattachement ou l'extension Authentification de mobile étranger. Afin que le nœud mobile utilise le matériel de chiffrement créé par le serveur AAA, le nœud mobile doit aussi être capable d'identifier et choisir la transformation cryptographique appropriée qui utilise la clé pour produire l'authentification.

Les identifiants de transformations sont les mêmes que ceux utilisés dans IPsec. Il sont dans le tableau qui donne la liste des algorithmes d'authentification admissibles comme valeurs pour le "type d'attribut" (5) (c'est-à-dire, "Algorithme d'authentification") une des classifications du tableau des types d'attribut pour "Attributs des associations de sécurité IPsec". Voir à http://www.iana.org/assignments/isakmp-registry la liste complète des types d'attribut et autres attributs pour les associations de sécurité IPsec.

Les associations de sécurité de mobilité partagées entre nœuds mobiles et agents de rattachement exigent aussi une méthode de protection contre la répétition. Le tableau qui suit contient les méthodes de détection de répétition prises en charge.

Méthode de répétition	**Nom**	**Référence**
0, 1	réservé	
2	Horodatage	[RFC3344]
3	Nom occasionnel	[RFC3344]
4 à 65 535	non alloué	

5. Création de nom occasionnel de génération de clé et déduction de clé

Cette section contient les procédures suivies pour la création du nom occasionnel de génération de clé par les serveurs AAA, et les procédures de déduction de clé utilisées par les nœuds mobiles. Noter que les serveurs AAA vont aussi livrer les clés aux agents de mobilité (agent de rattachement, agent étranger) via le protocole AAA. Les serveurs AAA qui suivent ces procédures vont produire des résultats qui peuvent être compris par les nœuds mobiles. Les agents de mobilité vont de bon gré transcrire les résultats dans les extensions IP mobile appropriées.
L'exemple qui suit utilise HMAC-SHA1 [RFC2104]. Tous les nœuds mobiles et agents de mobilité qui mettent en œuvre IP mobile [RFC3344] et qui mettent en œuvre les extensions spécifiées dans le présent document DOIVENT mettre en œuvre HMAC-SHA1 [RFC3344]. D'autres codes d'authentification de message ou fonctions de hachage chiffrées PEUVENT aussi être utilisés. L'algorithme utilisé est configuré au titre de l'association de sécurité AAA entre le MN et le serveur AAAH, qui est à son tour indexé par le SPI AAA.

Les étapes suivantes sont effectuées sur le serveur AAAH :

1. Le serveur AAA identifie le nœud mobile. Si le champ NAI est présent dans la demande d'enregistrement, le NAI est alors utilisé comme identifiant de nœud mobile. Autrement, le champ Adresse de rattachement de la demande d'enregistrement est utilisé.

2 Le serveur AAA génère une valeur aléatoire [RFC1750] d'au moins 128 bits à utiliser comme nom occasionnel de génération de clé.

3. Le serveur AAA insère la valeur aléatoire dans l'extension Réponse de nom occasionnel de génération de clé dans le champ "Nom occasionnel de génération de clé".

Les étapes suivantes sont effectuées par le nœud mobile (ici || représente l'enchaînement) :

1. Le nœud mobile calcule :
   clé = HMAC-SHA1 (clé AAA, {Nom occasionnel de génération de clé || Identifiant de nœud mobile })
   Ici le Nom occasionnel de génération de clé provient de l'extension dans la réponse d'enregistrement, et l'identifiant de nœud mobile est le NAI du MN, s'il est présent dans la demande d'enregistrement, ou autrement l'adresse de rattachement provenant de la demande d'enregistrement.

2 Le nœud mobile crée la ou les associations de sécurité de mobilité, en utilisant la clé résultante et les autres informations pertinentes dans l'extension Nom occasionnel de génération de clé.

La clé secrète utilisée dans le calcul du HMAC-SHA1 est indiquée par l'association de sécurité AAA indexée par le SPI AAA, qui a été précédemment configuré comme base de l'association de sécurité AAA entre le nœud mobile et le serveur AAA pour créer le matériel de chiffrement.

6. Extensions de génération de clé

Cette section définit les nouvelles extensions aux demandes et réponses d'enregistrement IP mobile [RFC3344].

6.1 Extension généralisée Demande de nom occasionnel de génération de clé MN-FA

La Figure 1 illustre l'extension généralisée Demande de nom occasionnel de génération de clé MN-FA (en abrégé Demande KeyGen MN-FA).

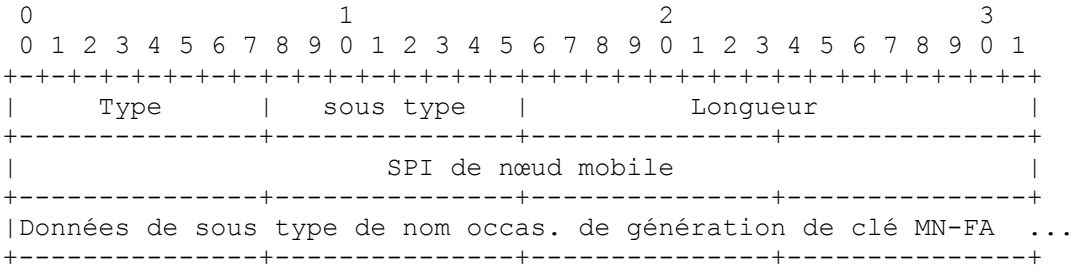

Figure 1 : Extension généralisée Demande de nom occasionnel de génération de clé MN-FA IP mobile

Type : 40 (non sautable) (voir la [RFC3344] et la section 8)

sous type : numéro alloué pour identifier la façon dont les données de sous type de demande de nom occasionnel de génération de clé MN-FA sont à utiliser lors de la génération de la clé d'enregistrement.

Longueur : le champ Longueur de 16 bits indique la longueur de l'extension. Il est égal au nombre d'octets dans les données de sous type de demande de nom occasionnel de génération de clé MN-FA plus 4 (pour le champ SPI de nœud mobile).

SPI de nœud mobile : Indice de paramètres de sécurité que va allouer le nœud mobile pour l'association de sécurité de mobilité créée pour utiliser avec la clé d'enregistrement.

Données de sous type de demande de nom occasionnel de génération de clé MN-FA : Données nécessaires pour porter la création de la clé d'enregistrement au nom du nœud mobile.

La demande KeyGen MN-FA définit un ensemble d'extensions, identifié par un sous type, qui peut être utilisé par un nœud mobile dans un message de demande d'enregistrement IP mobile pour demander qu'une autre entité crée une clé d'enregistrement à utiliser par le nœud mobile avec son nouvel agent étranger.

Le présent document définit le sous type 1 pour la demande de génération de clé MN-FA de AAA (en abrégé Demande KeyGen MN-FA AAA). La demande KeyGen MN-FA AAA a un champ Données de sous type de longueur zéro et DOIT apparaître dans la demande d'enregistrement avant l'extension Authentification MN-AAA.

6.2 Extension généralisée Réponse de nom occasionnel de génération de clé MN-FA

L'extension généralisée Réponse de nom occasionnel de génération de clé MN-FA (en abrégé Réponse KeyGen MN-FA) fournit le matériel de chiffrement demandé par l'extension Demande KeyGen MN-FA. La Figure 2 illustre le format de l'extension généralisée Réponse de nom occasionnel de génération de clé MN-FA.

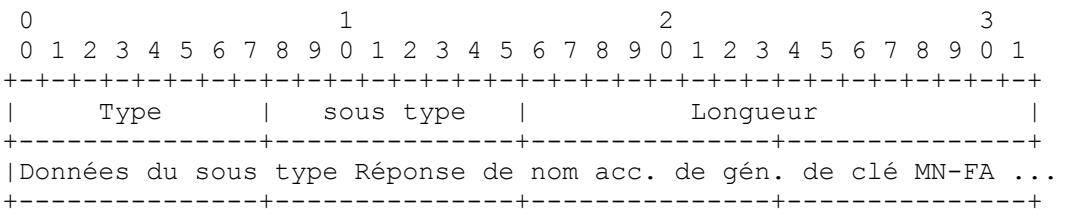

Figure 2 : Extension généralisée Réponse de nom occasionnel de génération de clé MN-FA IP mobile

Type : 41 (non sautable) (voir la [RFC3344] et la Section 8)

sous type : numéro alloué pour identifier la façon dont les données de sous type de réponse de nom occasionnel de génération de clé MN-FA vont être utilisées pour obtenir la clé d'enregistrement.

Longueur : Le champ de 16 bits Longueur est égal au nombre d'octets dans les données de sous type Réponse de nom occasionnel de génération de clé MN-FA.

Données de sous type Réponse de nom occasionnel de génération de clé MN-FA : copie codée du matériel de chiffrement, avec toutes les autres informations nécessaires pour que le receveur crée l'association de sécurité de mobilité désignée.

Pour chaque sous type, le format des données de sous type Réponse de nom occasionnel de génération de clé MN-FA doit être défini séparément conformément à la méthode particulière requise pour établir l'association de sécurité de mobilité.

Pour le sous type défini dans le présent document, le nom occasionnel de génération de clé MN-FA fourni dans les données pour un sous type de cette extension peut venir par suite d'une demande qui a été envoyée en utilisant un sous type de l'extension généralisée Demande de nom occasionnel de génération de clé MN-FA. Dans ce cas, le SPI à utiliser quand on emploie l'association de sécurité de mobilité définie par la clé d'enregistrement est le même que celui donné dans la demande d'origine. Une fois que le nœud mobile a créé l'association de sécurité de mobilité avec l'agent étranger, en utilisant la transformation indexée par le SPI AAA, il mémorise cette association de sécurité de mobilité indexée par le SPI FA dans sa liste des associations de sécurité mobile.

Si l'agent étranger reçoit une réponse d'enregistrement qui n'a pas d'extension Réponse de nom occasionnel de génération de clé MN-FA, et si il n'a pas d'association de sécurité de mobilité existante avec le nœud mobile, l'agent étranger PEUT changer la valeur de code de la réponse d'enregistrement en MISSING_MN_FA (voir la Section 7) causant effectivement l'échec de l'enregistrement.

Le présent document définit le sous type 1 de la Réponse KeyGen MN-FA pour l'extension Nom occasionnel de génération de clé MN-FA de AAA (en abrégé Réponse KeyGen MN-FA AAA) montrée à la Figure 3.

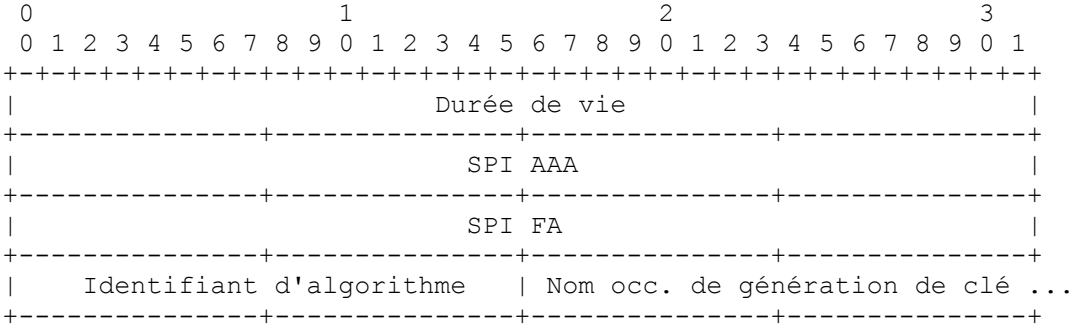

Figure 3 : Données spécifiques du sous type de nom occasionnel de génération de clé MN-FA de AAA

Durée de vie : ce champ indique la durée (en secondes) pendant laquelle le matériel de chiffrement utilisé pour créer la clé d'enregistrement est valide.

SPI AAA : valeur opaque de 32 bits, qui indique le SPI que le nœud mobile doit utiliser pour déterminer la transformation à utiliser pour établir l'association de sécurité de mobilité entre le nœud mobile et son agent étranger éventuel.

SPI FA : SPI pour l'association de sécurité de mobilité avec le FA que le nœud mobile crée en utilisant le nom occasionnel de génération de clé.

Identifiant d'algorithme : ce champ indique la transformation à utiliser (mémorisée au titre de l'association de sécurité de mobilité avec l'agent étranger, et choisie parmi les valeurs dans le tableau des "Algorithmes d'authentification " cité à la Section 4) pour les calculs futurs d'extension d'authentification de mobile étranger.

Nom occasionnel de génération de clé : valeur aléatoire [RFC1750] d'au moins 128 bits.

L'extension Réponse KeyGen MN-FA AAA DOIT apparaître dans la réponse d'enregistrement avant l'extension Authentification de mobile étranger.

Le nom occasionnel de génération de clé est fourni par le serveur AAA pour être utilisé par le nœud mobile lors de la

création de la clé d'enregistrement, qui est utilisée pour sécuriser les futurs enregistrements IP mobile avec le même agent étranger.

6.3 Extension généralisée Demande de nom occasionnel de génération de clé MN-HA

La Figure 4 illustre l'extension généralisée de demande de nom occasionnel de génération de clé MN-HA (en abrégé Demande KeyGen MN-HA).

Type : 42 (non sautable) (voir la [RFC3344] et la Section 8)

sous type : numéro alloué pour identifier la façon dont les données de sous type de nom occasionnel de génération de clé MN-HA sont à utiliser lors de la génération de la clé d'enregistrement.

Longueur : le champ Longueur de 16 bits indique la longueur de l'extension. Il est égal au nombre d'octets dans la demande de nom occasionnel de génération de clé MN-HA.

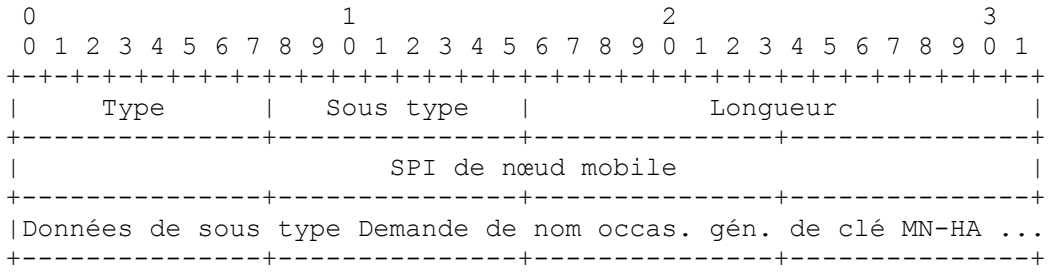

Figure 4 : Extension généralisée Demande de nom occasionnel de génération de clé MN-HA IP mobile

Sous type : données plus 4 (pour le champ SPI de nœud mobile).

SPI de nœud mobile : indice de paramètres de sécurité que le nœud mobile va allouer pour l'association de sécurité de mobilité créée pour utiliser avec la clé d'enregistrement.

Données de sous type de demande de nom occasionnel de génération de clé MN-HA : données nécessaires pour porter la création de la clé MN-HA au nom du nœud mobile.

L'extension Demande KeyGen MN-HA définit un ensemble d'extensions, identifiées par sous type, qui peut être utilisé par un nœud mobile dans un message de demande d'enregistrement IP mobile pour demander qu'une autre entité crée une clé MN-HA à utiliser par le nœud mobile avec le nouvel agent de rattachement du nœud mobile.

Le présent document définit le sous type 1 pour le nom occasionnel de génération de clé MN-HA à partir d'une demande AAA (en abrégé Demande KeyGen MN-HA). La demande KeyGen AAA MN-HA a un champ Données de sous type de longueur zéro et DOIT apparaître dans la demande d'enregistrement avant l'extension Authentification MN-AAA.

6.4 Extension généralisée Réponse de nom occasionnel de génération de clé MN-HA

L'extension généralisée Réponse de nom occasionnel de génération de clé MN-HA (en abrégé KeyGen MN-HA) fournit le matériel de chiffrement demandé dans l'extension Demande KeyGen MN-HA. La Figure 5 illustre le format de l'extension généralisée Réponse de nom occasionnel de génération de clé MN-HA.

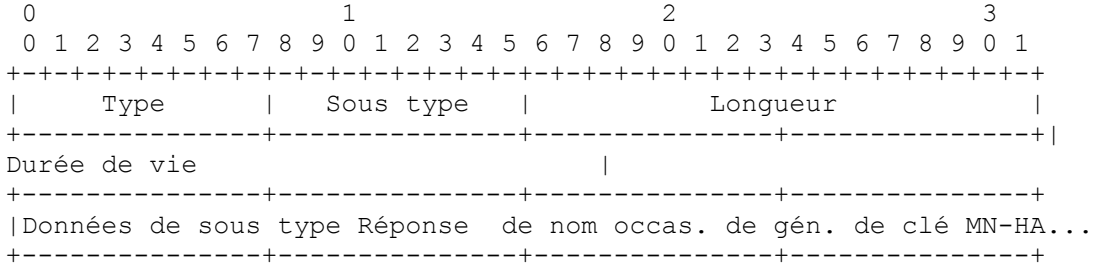

Figure 5 : Extension généralisée Réponse de nom occasionnel de génération de clé MN-HA IP mobile

Type : 43 (non sautable) (voir la [RFC3344] et la Section 8)

Sous type : numéro alloué pour identifier la façon dont les données de sous type de réponse de nom occasionnel de génération de clé MN-HA sont à utiliser pour obtenir la clé MN-HA.

Longueur : le champ Longueur de 16 bits indique la longueur de l'extension. Il est égal au nombre d'octets dans les données de sous type de réponse de nom occasionnel de génération de clé MN-HA plus 4 (pour le champ Durée de vie).

Durée de vie : ce champ indique la durée (en secondes) pendant laquelle la clé MN-HA est valide.

Données de sous type de réponse de nom occasionnel de génération de clé MN-HA : données utilisées pour déduire la clé MN-HA, ainsi que toutes les autres informations nécessaires pour que le nœud mobile crée l'association de sécurité de mobilité désignée avec l'agent de rattachement.

Pour chaque sous type, le format de Données de sous type de réponse de nom occasionnel de génération de clé MN-HA doit être défini de façon séparée conformément à la méthode particulière requise pour établir l'association de sécurité de mobilité.

Le présent document définit le sous type 1 de Réponse KeyGen MN-HA pour l'extension Nom occasionnel de génération de clé MN-HA provenant de AAA (en abrégé Réponse KeyGen MN-HA AAA) montrée à la Figure 6.

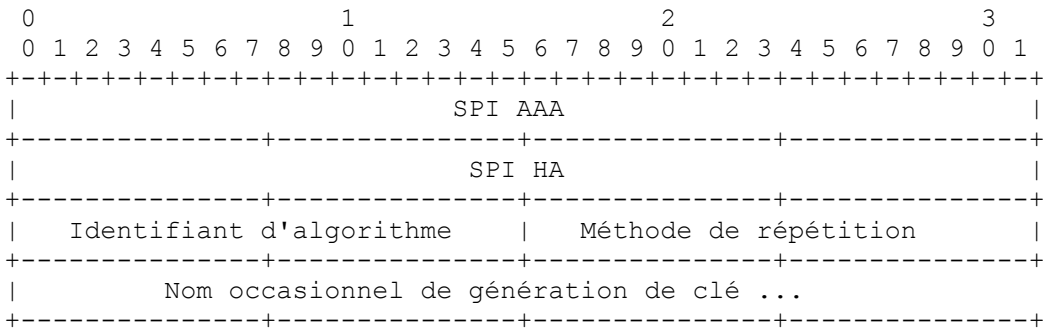

Figure 6 : Données spécifiques du sous type de nom occasionnel de génération de clé MN-HA provenant de AAA

SPI AAA : valeur opaque de 32 bits, qui indique le SPI que le nœud mobile doit utiliser pour déterminer la transformation à utiliser pour établir l'association de sécurité de mobilité entre le nœud mobile et son agent de rattachement.

SPI HA : SPI pour l'association de sécurité de mobilité au HA que le nœud mobile crée en utilisant le nom occasionnel de génération de clé.

Identifiant d'algorithme : ce champ indique la transformation à utiliser pour les futurs calculs de l'extension d'authentification de mobile de rattachement (voir la Section 4).

Méthode de répétition : ce champ contient la méthode de répétition à utiliser pour les futurs messages d'enregistrement (voir la Section 4).

Nom occasionnel de génération de clé : valeur aléatoire [RFC1750] d'au moins 128 bits.

Les données spécifiques de sous type Réponse KeyGen MN-HA AAA sont montrées à la Figure 6. Le nœud mobile calcule la clé MN-HA en utilisant le nom occasionnel de génération de clé fourni par le serveur AAA. Le calcul se fait en utilisant la clé partagée entre le nœud mobile et le serveur AAA qui a été configurée précédemment pour sécuriser toutes ces exigences de communication avec le serveur AAA qui sera contacté dans l'infrastructure AAA (voir l'Appendice A). La clé MN-HA est destinée à être utilisée par le nœud mobile pour sécuriser les futurs enregistrements IP mobile avec son agent de rattachement. L'extension Réponse KeyGen MN-HA AAA DOIT apparaître dans la réponse d'enregistrement avant l'extension Authentification MN-HA.

Une fois que le nœud mobile a créé la clé MN-HA, en utilisant la transformation spécifiée dans le SPI AAA, il mémorise les informations de sécurité HA indexées par le SPI HA dans sa liste des associations de sécurité mobile. Le nœud mobile utilise le champ Données d'identification de la réponse d'enregistrement comme données initiales de synchronisation avec l'agent de rattachement.

7. Valeurs d'erreur

Chaque entrée du tableau suivant contient le nom de la valeur de code [RFC3344] à retourner dans une réponse d'enregistrement, la valeur de ce code, et le paragraphe dans lequel l'erreur est mentionnée dans la présente spécification.

Nom d'erreur	Valeur	Paragraphe
MISSING_MN_FA	107	6.2

8. Considérations relatives à l'IANA

Le présent document définit quatre nouvelles extensions (voir la Section 6) tirées de l'espace de numérotation (non sautable) défini pour les extensions d'enregistrement IP mobile définies dans la [RFC3344] tel qu'étendu dans la [RFC2356]. Les valeurs de ces extensions sont :

Nom	Valeur	Paragraphe
MN-FA-KeyGen Request	40	6.1
MN-FA-KeyGen Reply	41	6.2
MN-HA-KeyGen Request	42	6.3
MN-HA-KeyGen Reply	43	6.4

L'IANA a créé et tiendra un nouveau registre pour les sous types Demande/Réponse KeyGen. Le contenu initial du registre est une seule entrée pour les sous types définis dans le présent document:

Nom	Valeur	Section
Demande/Réponse KeyGen de AAA	1	6

Les nouveaux sous types pour ces deux registres sont alloués par action de normalisation comme défini dans la [RFC2434].

L'IANA a alloué une valeur de code pour l'erreur MISSING_MN_FA, mentionnée à la Section 7. Cette valeur a été prise dans l'espace des valeurs d'erreur conventionnellement associé au rejet par l'agent étranger (c'est-à-dire, 64 à 127).

L'IANA a créée et tiendra un espace de noms pour identifiant de méthode de répétition. La présente spécification utilise 2 et 3 ; toutes les valeurs autres que zéro (0) et (1) sont disponibles pour être allouées, moyennant révision et approbation par un expert désigné [RFC2434].

9. Considérations sur la sécurité

Les extensions du présent document sont destinées à fournir le niveau approprié de sécurité aux entités IP mobile (nœud mobile, agent étranger, et agent de rattachement) pour calculer les données d'authentification nécessaires pour les extensions d'authentification utilisées avec les messages d'enregistrement IP mobile. Les associations de sécurité de mobilité résultant de l'utilisation de ces extensions n'offre pas un niveau de sécurité supérieur à celui qui est déjà implicite dans l'utilisation de l'association de sécurité AAA entre le nœud mobile et le AAAH. Afin de priver tout adversaire de la possibilité de jouir d'un temps illimité pour analyser et casser le secret de l'association de sécurité AAA entre le nœud mobile et le serveur AAA, cette association de sécurité AAA DOIT être rafraîchie périodiquement.

Le provisionnement et le rafraîchissement de la clé AAA dans le MN et le serveur AAA sort du domaine d'application du présent document.

Comme les extensions de réponse définies dans la présente spécification ne portent que des noms occasionnels de génération de clé, qui sont utilisés pour déduire des clés,elles n'exposent aucune donnée qui pourrait être utilisée dans une attaque visant à récupérer la clé partagée entre le nœud mobile et l'AAA. Les auteurs estiment que la présente spécification n'introduit aucune nouvelle faiblesse de sécurité.

10. Remerciements

Merci à Fredrik Johansson, Tom Hiller, et aux membres de l'IESG pour leur commentaires utiles. Merci particulièrement à Tom Hiller qui a contribué par de nombreuses améliorations rédactionnelles aux dernières révisions de ce document.

11. Références

11.1 Références normatives

[RFC1750] D. Eastlake 3rd et autres, "Recommandations d'aléa pour la sécurité", décembre 1994. *(Info., remplacée par la* RFC4086)

[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.

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

[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* RFC4282) *(P.S.)*

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

11.2 Références pour information

[RFC2865] C. Rigney et autres, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", juin 2000. (*MàJ par* RFC2868, RFC3575, RFC5080) *(D.S.)*

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

[RFC3127] D. Mitton et autres, "Authentification, autorisation et comptabilité : évaluation du protocole", juin 2001. *(Info.)*

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

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

Appendice A. Infrastructure AAA

Dans cet appendice, on tente de saisir les principales caractéristiques d'un modèle de base du fonctionnement des serveurs AAA qui sont nécessaires pour la compréhension de l'utilisation des extensions d'enregistrement IP mobile décrites dans le présent document. Ces informations ont été adaptées de l'exposé de la [RFC2977].

Au sein de l'Internet, un nœud mobile 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 étranger qui traite la demande d'enregistrement du nœud mobile va vraisemblablement exiger que le nœud mobile fournisse des accréditifs qui puissent être authentifiés avant de lui permettre l'accès aux ressources. Ces accréditifs peuvent être fournis au titre de l'extension Authentification Mobile-AAA [RFC3012], s'appuyant sur l'existence d'une infrastructure AAA comme celle décrite dans cette section, et aussi décrite dans la [RFC2977] et la [RFC3012]. De tels accréditifs sont normalement gérés par des entités du domaine de rattachement du nœud mobile. Ils peuvent aussi être utilisés pour établir des communications sécurisées avec le nœud mobile et l'agent étranger, or entre le nœud mobile et son agent de rattachement si nécessaire.

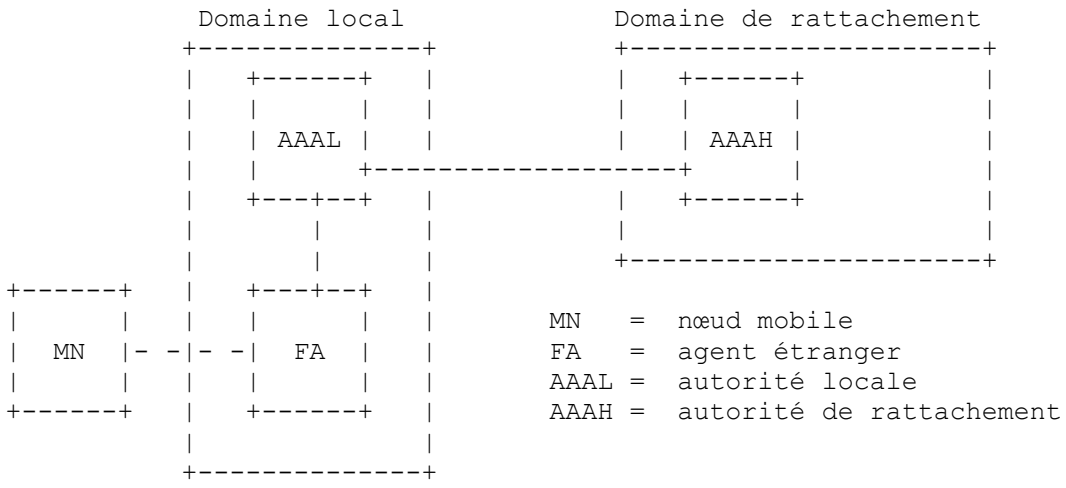

Figure 7 : Serveurs AAA dans le domaine local et le domaine de rattachement

L'agent étranger n'a souvent pas d'accès direct au données nécessaires pour vérifier les accréditifs. On attend plutôt de l'agent étranger qu'il consulte une autorité (normalement dans le même domaine étranger) afin de demander la preuve que le nœud mobile a des accréditifs acceptables. Comme l'agent étranger et l'autorité locale (AAAL) font partie du même domaine administratif, on s'attend à ce qu'ils aient établi, ou soient capables d'établir pour la durée de vie nécessaire, un canal sûr afin d'échanger des informations sensibles (d'accès) et de les garder confidentielles à l'égard (au moins) du nœud mobile visiteur.

L'autorité locale (AAAL) elle-même peut n'avoir pas assez d'informations mémorisées localement pour mener à bien la vérification des accréditifs du nœud mobile. À la différence de l'agent étranger, cependant, l'AAAL est supposé être configuré avec assez d'informations pour négocier la vérification des accréditifs du nœud mobile avec son domaine de rattachement. Les domaines de rattachement et étrangers devraient être configurés avec des associations de sécurité IP (c'est-à-dire, IPsec) et des contrôles d'accès suffisants pour qu'ils puissent négocier l'autorisation, et aussi permettre au nœud mobile d'acquérir des associations de sécurité de mobilité avec les agents de mobilité au sein du domaine étranger. Pour les besoins des échanges de clé spécifiés dans le présent document, l'autorisation est supposée ne dépendre que de l'authentification sûre des accréditifs du nœud mobile.

Une fois que l'autorisation a été obtenue par l'autorité locale, et que l'autorité a notifié à l'agent étranger le succès de la négociation, l'agent étranger peut livrer la réponse d'enregistrement au nœud mobile avec le matériel de chiffrement.

Dans la Figure 7, il peut y avoir de nombreux nœuds mobiles provenant de nombreux différents domaines de rattachement. Chaque domaine de rattachement fournit un AAAH qui peut vérifier les accréditifs originaires des nœuds mobiles administrés par ce domaine de rattachement. Il y a un modèle de sécurité implicite dans la Figure 7, et il est crucial d'identifier les associations de sécurité spécifiques supposées par le modèle de sécurité. Ces associations de sécurité IP sont illustrée à la Figure 8, et sont considérées comme des associations de sécurité de durée de vie relativement longue.

D'abord, il est naturel de supposer que le nœud mobile a une association de sécurité AAA avec le AAAH, car c'est en gros ce que signifie pour le nœud mobile appartenir au domaine de rattachement.

Ensuite, d'après le modèle illustré à la Figure 7, il est clair que AAAL et AAAH doivent partager une association de sécurité IP, parce que autrement, ils ne pourraient pas s'appuyer sur les résultats de l'authentification, des autorisations, ni même des données de comptabilité qui pourraient être échangées entre eux. Exiger de telles associations de sécurité IP bilatérales n'est cependant pas adaptable en fin de compte ; le cadre AAA doit fournir des mécanismes plus adaptables, mais les méthodes par lesquelles un tel modèle de courtage serait créé sortent du domaine d'application du présent document. Voir plus de détails dans la [RFC2977].

Finalement, d'après la Figure 7, il est clair que l'agent étranger peut naturellement partager une association de sécurité IP avec l'AAAL. C'est nécessaire afin que le modèle fonctionne parce que l'agent étranger doit avoir un moyen pour découvrir ce qu'il est permis d'allouer des ressources locales au nœud mobile, et de plus de transmettre toute réponse d'enregistrement réussie au nœud mobile.

La Figure 8 illustre les associations de sécurité IP qu'on comprend à partir de notre proposition de modèle. Noter qu'il peut y avoir, par accord mutuel entre AAAL et AAAH, un tiers inséré entre AAAL et AAAH pour les aider à arbitrer les transactions sécurisées de façon plus adaptable. Le modèle de courtier qui a été conçu pour permettre un tel traitement de tiers n'a pas d'incidence sur les extensions IP mobile spécifiées dans le présent document, et donc aucune description n'en

est fournie ici ; voir les détails dans la [RFC2977].

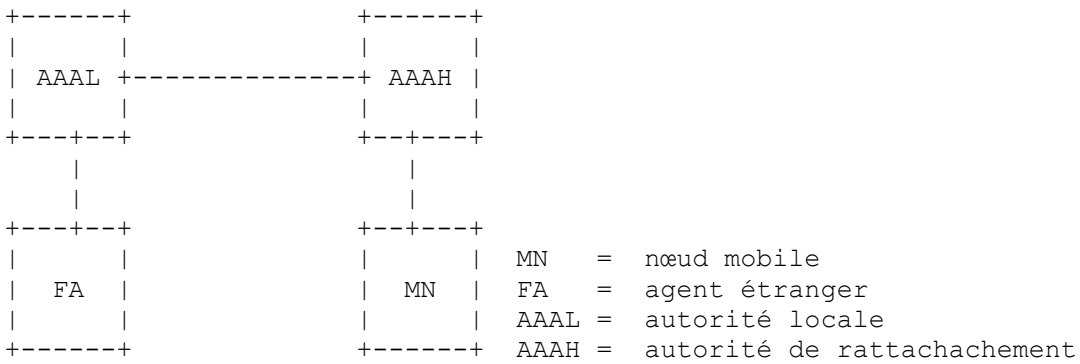

Figure 8 : Associations de sécurité IP

Les nœuds qui sont dans deux domaines administratifs séparés (par exemple, AAAH et AAAL) doivent souvent passer par des étapes supplémentaires pour vérifier l'identité de leurs partenaires de communication, ou garantir autrement la confidentialité des données qui constituent la communication. Bien que ces considérations conduisent à des exigences de sécurité importantes, comme mentionné ci-dessus dans le contexte de la sécurité entre les serveurs, on considère que le choix exact des associations de sécurité IP entre les serveurs AAA sort du domaine d'application du présent document. Les choix ont peu de chances de dépendre de IP mobile, ou d'une caractéristique spécifique du modèle général illustré à la Figure 7. D'un autre côté, les associations de sécurité de mobilité nécessaires entre les entités IP mobile sont d'une importance cruciale dans la conception des extensions de déduction de clés dans le présent document.

Un autre détail mérite d'être mentionné. L'association de sécurité de mobilité à établir entre le nœud mobile et l'agent étranger doit être communiquée à l'agent étranger ainsi qu'au nœud mobile. Les exigences suivantes figurent dans le mécanisme utilisé par l'infrastructure AAA pour effectuer la distribution de clé :

- Le AAAH doit établir de fortes clés de session fraîches.
- Le mécanisme doit conserver l'indépendance de l'algorithme, permettant la distribution de l'identification de l'algorithme d'authentification avec les clés.
- Le mécanisme doit inclure la détection des répétitions.
- Le mécanisme doit authentifier toutes les parties, incluant les serveurs AAA, le FA et le HA.
- Le mécanisme doit assurer l'autorisation du client, du FA, et du HA.
- Le mécanisme ne doit pas s'appuyer sur des mots de passe en clair.
- Le mécanisme doit assurer la confidentialité des clés de session.
- Le mécanisme doit désigner les clés de session de façon univoque.
- Le mécanisme doit être tel que la compromission d'un seul FA et HA ne puisse pas compromettre une autre partie du système, incluant les clés de session et les clés à long terme.
- Le mécanisme doit lier la ou les clés à un contexte approprié.
- Le mécanisme ne doit pas exposer les clés à des entités autres que le AAAH et FA (ou HA dans le cas de distribution de clé au HA).

La façon dont la clé est distribuée à l'agent étranger (ou l'agent de rattachement) est supposée être traitée au titre du traitement du protocole AAA entre le AAAH et le AAAL, et le traitement ultérieur du protocole AAA entre le AAAL et l'agent étranger. Ce traitement sort du domaine d'application du présent document, mais doit satisfaire aux exigences ci-dessus.

Appendice B. Flux de messages pour demander et recevoir des clés d'enregistrement

Dans cette section, on montre les flux de messages pour demander et recevoir une clé d'enregistrement à l'infrastructure AAA, décrite dans l'Appendice A. Les valeurs de défi, comme spécifiées dans la [RFC3012], peuvent être ajoutées aux messages d'annonce et d'enregistrement pour une protection supplémentaire contre la répétition, mais ne sont pas illustrées ici.

La Figure 9 illustre les flux de messages pour le cas où le nœud mobile demande explicitement le matériel de chiffrement pour créer les clés d'enregistrement.

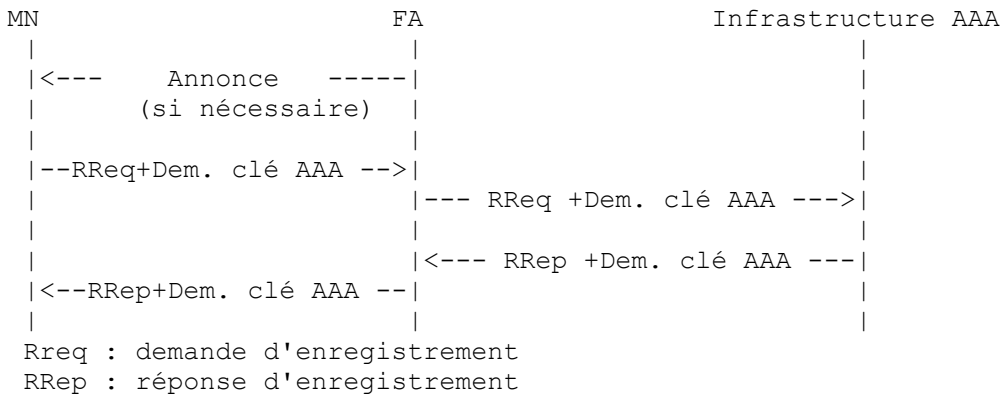

Figure 9 : Flux de messages pour demander et recevoir le nom occasionnel de génération de clé

Dans la Figure 9, les flux de messages suivants sont illustrés :

1. L'agent étranger diffuse une annonce d'agent. Cette annonce PEUT avoir été produite après avoir reçu une sollicitation d'agent de la part du nœud mobile (non montré sur la figure).

2. Le nœud mobile crée une demande d'enregistrement incluant la Demande KeyGen MN-HA AAA et/ou la Demande KeyGen MN-FA AAA, comme nécessaire, avec une extension Authentification permettant l'autorisation comme exigé par IP mobile [RFC3344].

3. L'agent étranger relaye la demande d'enregistrement et/ou la ou les demandes de clé à son infrastructure AAA configurée localement (voir l'Appendice A) conformément à la politique locale.

4. L'agent étranger reçoit une réponse AAA avec les indications appropriées pour autoriser la connexité pour le nœud mobile. Avec cette Réponse AAA, l'agent étranger peut aussi recevoir le matériel de chiffrement par une méthode sûre appropriée pour les communications entre lui et son infrastructure AAA locale. À ce point, si l'agent étranger n'a pas relayé la demande d'enregistrement, il la transmet directement à l'agent de rattachement et attend une réponse d'enregistrement (non montrée sur la figure).

5. L'agent étranger relaye la réponse d'enregistrement au nœud mobile, avec les nouvelles extensions Réponse KeyGen AAA à utiliser par le nœud mobile pour établir les associations de sécurité de mobilité avec les agents de mobilité pertinents (agent étranger et/ou agent de rattachement).

La Figure 10 illustre les flux de messages pour le cas où le nœud mobile reçoit du matériel de chiffrement non sollicité de l'infrastructure AAA.

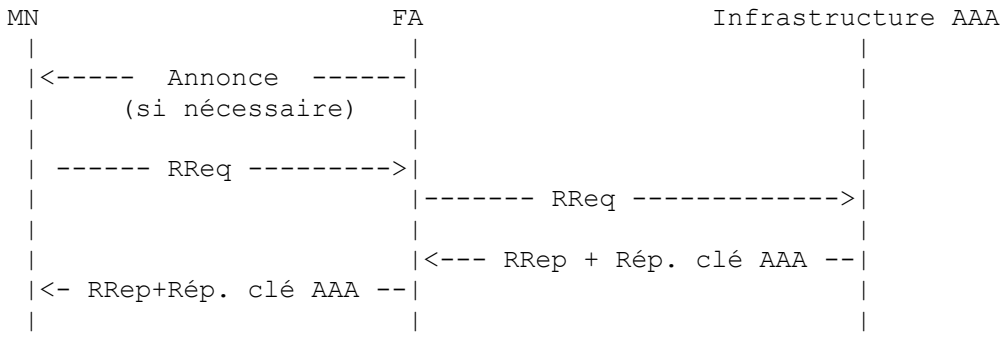

Figure 10 : Flux de messages pour la réception de nom occasionnel de génération de clé non sollicité

Dans la Figure 10, les flux de messages suivants sont illustrés :

1. L'agent étranger diffuse une annonce d'agent. Cette annonce PEUT avoir été produite après la réception d'une sollicitation d'agent de la part du nœud mobile (non montrée sue la figure).

2. Le nœud mobile crée une demande d'enregistrement incluant une extension d'authentification permettant l'autorisation comme exigé par IP mobile [RFC3344].

3. L'agent étranger envoie une Demande AAA (contenant éventuellement la demande d'enregistrement) à son infrastructure AAA configurée localement (voir l'Appendice A) conformément à la politique locale.

4. L'agent étranger reçoit une Réponse AAA avec les indications appropriées pour autoriser la connexité pour le nœud mobile. Avec cette Réponse AAA, l'agent étranger peut aussi recevoir le matériel de chiffrement par une méthode sûre appropriée pour les communications entre lui et son infrastructure AAA locale. À ce point, si l'agent étranger n'a pas relayé la demande d'enregistrement, il la transmet directement à l'agent de rattachement et attend une réponse d'enregistrement (non montrée sur la figure).

5. L'agent étranger relaye la réponse d'enregistrement au nœud mobile, avec les nouvelles extensions Réponse KeyGen à utiliser par le nœud mobile pour établir les associations de sécurité de mobilité avec les agents de mobilité pertinents (agent étranger et/ou agent de rattachement).

Adresse des auteurs

Charles E. Perkins
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
téléphone : +1 650 625-2986
Fax : +1 650 625-2502
mél : charles.perkins@nokia.com

Pat R. Calhoun
Airespace, Inc.
110 Nortech Parkway
San Jose, CA 95134
USA
téléphone : +1 408 635 2000
Fax : +1 408 635 2020
mél : pcalhoun@airespace.com

Déclaration complète de droits de reproduction

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