Groupe de travail Réseau
Request for Comments : 4721
RFC rendue obsolète : 3012
RFC mise à jour : 3344
Catégorie : En cours de normalisation

C. Perkins, Nokia Research Center
P. Calhoun, Cisco Systems, Inc.
J. Bharatia, Nortel Networks
janvier 2007
Traduction Claude Brière de L'Isle

Extensions défi/réponse IPv4 mobile (révisée)

Résumé
IP mobile, tel que spécifié à l'origine, définit une extension d'authentification (l'extension Authentification de mobile étranger) par laquelle un nœud mobile peut s'authentifier auprès d'un agent étranger. Malheureusement, cette extension ne fournit à l'agent étranger aucune garantie directe que le protocole soit protégé des répétitions et elle ne permet pas l'utilisation de techniques existantes (comme le protocole d'authentification par dialogue à énigme (CHAP, *challenge handshake authentication protocol*)) pour l'authentification des ordinateurs portables.

Dans la présente spécification, on définit les extensions pour les annonces d'agent IP mobile et la demande d'enregistrement qui permet à un agent étranger d'utiliser un mécanisme de défi/réponse pour authentifier le nœud mobile.

De plus, le présent document met à jour la RFC 3344 en incluant une nouvelle extension d'authentification appelée extension d'authentification d'autorisation et de comptabilité (AAA) mobile. Cette nouvelle extension est fournie afin qu'un nœud mobile puisse fournir des accréditifs pour l'autorisation, en utilisant les éléments d'infrastructure AAA couramment disponibles. Cette extension d'activation d'autorisation PEUT coexister dans la même demande d'enregistrement que les extensions d'authentification définies pour l'enregistrement IP mobile par la RFC 3344. Le présent document rend obsolète la RFC 3012.

Table des Matières

1. Introduction

IP mobile définit l'extension Authentification de mobile étranger pour permettre à un nœud mobile de s'authentifier auprès d'un agent étranger. Un tel mécanisme d'authentification est essentiellement externe au fonctionnement principal de IP mobile, car l'agent étranger peut facilement acheminer les paquets de et vers un nœud mobile si le nœud mobile peut produire une adresse de rattachement légitime à l'agent étranger. Malheureusement, cette extension ne donne pas à l'agent étranger une garantie directe que le protocole soit protégé des répétitions et ne permet pas l'utilisation de CHAP [RFC1994] pour authentifier les ordinateurs portables. Dans la présente spécification, on définit des extensions pour les annonces d'agent IP mobile et la demande d'enregistrement qui permettent à un agent étranger d'utiliser un mécanisme de défi/réponse pour authentifier le nœud mobile. De plus, une extension d'authentification supplémentaire, l'extension d'authentification AAA mobile, est fournie afin qu'un nœud mobile puisse fournir des accréditifs pour l'autorisation en utilisant des éléments d'infrastructure AAA couramment disponibles. L'agent étranger peut être capable d'interagir avec une infrastructure AAA (en utilisant des protocoles qui sortent du domaine d'application du présent document) pour obtenir une indication sûre que le nœud mobile est autorisé à utiliser les ressources du réseau local.

1.1 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].

Le présent document utilise le terme Indice de paramètres de sécurité (SPI, *Security Parameters Index*) comme défini dans la spécification de base du protocole IP mobile [RFC3344]. Toutes les valeurs de SPI définies dans le présent document se réfèrent aux valeurs de SPI définies dans cette spécification.

La terminologie supplémentaire suivante est utilisée en plus de celle définie dans la [RFC3344] :

défi utilisé précédemment : le défi est un défi utilisé précédemment si le nœud mobile a envoyé le même défi à l'agent étranger dans une demande d'enregistrement précédente, et si cette demande d'enregistrement précédente a réussi à toutes les vérifications de validité effectuées par l'agent étranger. L'agent étranger peut n'être pas capable de garder trace de tous les défis utilisés précédemment, mais voir au paragraphe 3.2 les exigences minimales.

association de sécurité : une "association de sécurité de mobilité", comme définie dans la [RFC3344].

défi inconnu : tout défi d'un nœud mobile particulier dont l'agent étranger n'a pas gardé trace de l'avoir mis dans une de ses annonces d'agent récentes ou dans un message de réponse d'enregistrement à ce nœud mobile.

défi non utilisé : défi provenant du nœud mobile dans la demande d'enregistrement qui n'a pas été déjà accepté par l'agent étranger, c'est-à-dire, un défi qui n'est ni inconnu ni précédemment utilisé.

2. Extension de défi d'annonce d'agent IP mobile

Cette Section définit une nouvelle extension au protocole de découverte de routeur [RFC1256] à l'usage des agents étrangers qui ont besoin de produire un défi pour l'authentification de nœuds mobiles.

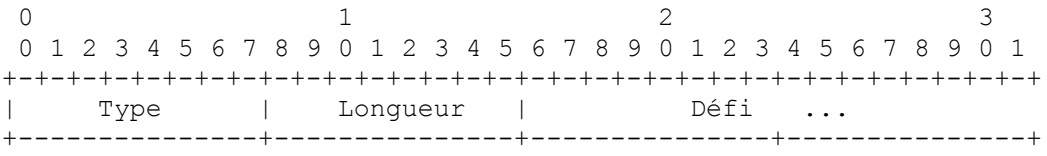

Figure 1 : Extension Défi

Type : 24

Longueur : longueur de la valeur de Défi en octets ; DEVRAIT être d'au moins 4.

Défi : valeur aléatoire qui DEVRAIT être d'au moins 32 bits.
L'extension Défi, illustrée à la Figure 1, est insérée dans les annonces d'agent par l'agent étranger afin de communiquer une valeur de défi précédemment non utilisée qui peut être utilisée par le nœud mobile pour calculer une authentification pour son prochain message de demande d'enregistrement. Le défi est choisi par l'agent étranger pour donner une assurance locale que le nœud mobile ne répète pas une demande d'enregistrement antérieure. Eastlake et al. [RFC4086] donnent plus d'informations sur la génération de nombres pseudo aléatoires dont l'utilisation convient comme valeurs pour le défi.

Noter que la mémorisation des différents défis reçus dans des annonces d'agent provenant de plusieurs agents étrangers est spécifique de la mise en œuvre et sort donc du domaine d'application de la présente spécification.

2.1 Traitement des annonces d'agent sollicitées

Lorsque un agent étranger génère une annonce d'agent en réponse à une sollicitation de routeur [RFC1256], certaines considérations supplémentaires peuvent entrer en jeu. Selon la spécification de base IP mobile [RFC3344], l'annonce d'agent résultante peut être en diffusion groupée ou en envoi individuel.

Si l'annonce d'agent sollicitée est en diffusion groupée, l'agent étranger NE DOIT PAS générer une nouvelle valeur de défi et mettre à jour sa fenêtre de défis annoncés mémorisés. Il doit plutôt réutiliser les valeurs les plus récentes d'annonce de défi de la CHALLENGE_WINDOW (Section 9).

Si l'annonce d'agent est renvoyée en envoi individuel au nœud mobile solliciteur, elle DOIT être traitée comme suit : si le défi envoyé le plus récemment en envoi individuel au nœud mobile solliciteur n'a pas été utilisé précédemment (comme défini au paragraphe 1.1) il DEVRAIT être répété dans la nouvelle annonce d'agent produite en envoi individuel. Autrement, un nouveau défi DOIT être généré et mémorisé comme plus récent défi produit au nœud mobile. La Section 12 expose ceci plus en détails.

3. Fonctionnement

Cette Section décrit les modifications au processus d'enregistrement IP mobile [RFC3344] qui peuvent arriver après la production par l'agent étranger d'une annonce d'agent IP mobile contenant le défi sur sa liaison locale. Voir à l'Appendice C la figure qui montre le flux de messages canoniques pour les messages relatifs au traitement par l'agent étranger des valeurs de défi.

3.1 Traitement des demandes d'enregistrement par le nœud mobile

Le comportement de retransmission pour les demandes d'enregistrement est identique à celui mentionné dans la spécification IP mobile [RFC3344]. Une demande d'enregistrement retransmise PEUT utiliser la même valeur de défi que celle donnée dans la demande d'enregistrement d'origine.

Chaque fois que l'annonce d'agent contient l'extension Défi, si le nœud mobile n'a pas une association de sécurité avec l'agent étranger, il DOIT alors inclure la valeur de défi dans une extension Défi de mobile étranger dans le message de demande d'enregistrement. Si par ailleurs, le nœud mobile n'a pas une association de sécurité avec l'agent étranger, il DEVRAIT inclure la valeur de défi dans son message de demande d'enregistrement.

Si le nœud mobile a une association de sécurité avec l'agent étranger, il DOIT inclure une extension Authentification de mobile étranger dans son message de demande d'enregistrement, conformément à la spécification de base IP mobile [RFC3344]. Lorsque la demande d'enregistrement contient l'extension Défi mobile étranger spécifiée à la Section 4, l'authentification de mobile étranger DOIT suivre l'extension Défi dans la demande d'enregistrement. Le nœud mobile PEUT aussi inclure l'extension Authentification AAA mobile.

Si les deux extensions Authentification de mobile étranger et Authentification AAA mobile sont présentes, l'extension Défi de mobile étranger DOIT précéder l'extension Authentification AAA mobile, et l'extension Authentification AAA mobile DOIT précéder l'extension Authentification de mobile étranger.

Si le nœud mobile n'a pas une association de sécurité avec l'agent étranger, le nœud mobile DOIT inclure l'extension Authentification AAA mobile comme défini à la Section 6, quand il inclut l'extension Défi de mobile étranger. De plus, le nœud mobile DEVRAIT inclure l'extension NAI [RFC2794] pour permettre à l'agent étranger de faire usage de l'infrastructure de vérification disponible qui l'exige. Le champ SPI de l'extension Authentification AAA mobile spécifie le secret et

l'algorithme (partagés entre le nœud mobile et l'infrastructure de vérification) qui doivent être utilisés pour effectuer l'authentification. Si la valeur de SPI est choisie comme CHAP_SPI (voir la Section 9) le nœud mobile spécifie alors l'authentification de style CHAP [RFC1994] utilisant MD5 [RFC1321].

Dans l'un et l'autre cas, l'extension Défi de mobile étranger suivie par une des extensions d'authentification spécifiées ci-dessus DOIT suivre l'extension Authentification de mobile de rattachement, si elle est présente.

Un nœud mobile PEUT inclure l'extension Authentification AAA mobile dans la demande d'enregistrement lorsque le nœud mobile s'enregistre directement auprès de son agent de rattachement (en utilisant une adresse d'entretien colocalisée). Dans ce cas, le nœud mobile utilise une valeur de SPI de CHAP_SPI (Section 8) dans l'extension Authentification, autorisation, et comptabilité de nœud mobile (Mobile-AAA, *Mobile Node-Authentication, Authorization, and Accounting*) et NE DOIT PAS inclure l'extension Défi de mobile étranger. Aussi, la protection contre la répétition pour la demande d'enregistrement est fourni dans ce cas par le champ Identification défini par la [RFC3344].

3.2 Traitement des demandes d'enregistrement par l'agent étranger

À réception de la demande d'enregistrement, si l'agent étranger a produit un défi au titre de ses annonces d'agent, et si il n'a pas une association de sécurité avec le nœud mobile, l'agent étranger DEVRAIT vérifier que l'extension Défi de mobile étranger existe, et qu'elle contient une valeur de défi précédemment inutilisée par le nœud mobile. Cela assure que le nœud mobile ne tente pas de répéter une annonce et une authentification antérieures. Dans ce cas, si la demande d'enregistrement ne comporte pas une extension Défi, l'agent étranger DOIT envoyer une réponse d'enregistrement avec le champ Code réglé à missing_challenge *(défi manquant)*.

Si un nœud mobile retransmet une demande d'enregistrement avec la même extension Défi, et si l'agent étranger a encore un enregistrement de demande d'enregistrement en cours au sujet du nœud mobile, l'agent étranger transmet alors à nouveau la demande d'enregistrement à l'agent de rattachement. L'agent étranger DEVRAIT vérifier que le nœud mobile est en fait en train d'effectuer une retransmission, en vérifiant que les champs pertinents de la demande retransmise (y compris, si présente, l'extension NAI de nœud mobile [RFC2794]) sont les mêmes que ceux représentés dans l'entrée de la liste de visiteurs pour la demande d'enregistrement en cours (paragraphe 3.7.1 de la [RFC3344]). Cette vérification NE DOIT PAS inclure le champ "Durée de vie restante de l'enregistrement en cours" ou "Identification", car ces valeurs vont probablement changer même pour les demandes qui sont de simples retransmissions et non de nouvelles demandes d'enregistrement. Dans toutes les autres circonstances, si l'agent étranger reçoit une demande d'enregistrement avec une extension Défi contenant une valeur de défi utilisée précédemment par ce nœud mobile, l'agent étranger DEVRAIT envoyer une réponse d'enregistrement au nœud mobile, contenant la valeur de code stale_challenge *(défi périmé)*.

L'agent étranger NE DOIT PAS accepter de défi dans la demande d'enregistrement sauf si c'était offert dans la dernière réponse d'enregistrement ou annonce d'agent en envoi individuel envoyée au nœud mobile ou annoncée comme une des dernières valeurs de défi CHALLENGE_WINDOW (voir la Section 9) insérée dans les annonces d'agent immédiatement précédentes. Si le défi n'est pas d'une des valeurs récemment annoncées, l'agent étranger DEVRAIT envoyer une réponse d'enregistrement avec la valeur de code de unknown_challenge *(défi inconnu)* (voir la Section 10). L'agent étranger DOIT conserver le dernier défi utilisé par chaque nœud mobile qui s'est enregistré en utilisant une des dernières valeurs de défi de CHALLENGE_WINDOW. Cette dernière valeur de défi peut être mémorisée au titre de l'enregistrement du nœud mobile. Voir aussi le paragraphe 3.2.1 sur l'utilisation possible d'un algorithme pour satisfaire cette exigence.

De plus, l'agent étranger DOIT vérifier qu'il y a une extension d'authentification soit de mobile étranger, soit de mobile AAA après l'extension Défi. Tout message d'enregistrement qui contient l'extension Défi sans l'une ou l'autre de ces extensions d'authentification DOIT être éliminé en silence. Si le message d'enregistrement contient une extension Authentification de mobile étranger avec un authentifiant incorrect qui échoue à la vérification, l'agent étranger PEUT envoyer une réponse d'enregistrement au nœud mobile avec la valeur de code "le nœud mobile a échoué à l'authentification" (voir la Section 10).

Si l'extension Authentification AAA mobile (voir la Section 6) est présente dans le message, ou si une extension Identifiant d'accès réseau (NAI, *Network Access Identifier*) est incluse pour indiquer que le nœud mobile appartient à un domaine administratif différent, l'agent étranger peut, pour mener à bien l'authentification du nœud mobile, entreprendre des actions qui sortent du domaine d'application de la présente spécification de protocole. Si le message d'enregistrement contient une extension Authentification AAA mobile avec un authentifiant incorrect qui échoue à la vérification, l'agent étranger PEUT envoyer une réponse d'enregistrement au nœud mobile avec la valeur de code fa_bad_aaa_auth. Si l'extension Authentification AAA mobile est présente dans la demande d'enregistrement, l'agent étranger NE DOIT PAS retirer l'extension Authentification AAA mobile ni l'extension Défi de mobile étranger de la demande d'enregistrement avant de la transmettre à l'agent de rattachement. L'Appendice C donne un exemple d'action qui pourrait être prise par un agent étranger.

Si il arrive que l'extension Défi soit authentifiée au moyen de l'extension Authentification de mobile étranger et si l'extension Authentification AAA mobile n'est pas présente, l'agent étranger PEUT retirer l'extension Défi de la demande d'enregistrement

sans perturber la valeur d'authentification utilisée pour le calcul. Si l'extension Authentification AAA mobile est présente et si il existe une association de sécurité entre l'agent étranger et l'agent de rattachement, l'extension Défi de mobile étranger et l'extension Authentification AAA mobile DOIVENT précéder l'extension d'authentification étranger-rattachement.

Si l'agent étranger retire l'extension Défi et l'authentification applicable du message de demande d'enregistrement, il DEVRAIT alors mémoriser le champ Identification du message de demande d'enregistrement au titre de ses informations de retraçage de ce nœud mobile particulier afin de protéger contre les répétitions.

3.2.1 Algorithme de traçage des défis utilisés par l'agent étranger

Si l'agent étranger tient une grande CHALLENGE_WINDOW, il devient plus important pour les besoins d'adaptabilité de comparer efficacement les défis entrants à l'ensemble des valeurs de défi qui ont été annoncées récemment. Cela peut être fait en gardant les valeurs de défi dans l'ordre des annonces, et d'utiliser le comportement obligatoire que les nœuds mobiles NE DOIVENT PAS utiliser les valeurs de défi qui ont été annoncées avant la dernière valeur de défi annoncée que le nœud mobile a tenté d'utiliser. Le pseudocode de l'Appendice E réalise cet objectif. La taillé maximale de mémorisation totale requise par cet algorithme est égale à Taille*(CHALLENGE_WINDOW + (2*N)), où N est le nombre actuel de nœuds mobiles pour lesquels l'agent étranger mémorise des valeurs de défi. Noter que chaque fois que la valeur de défi mémorisée n'est plus dans la CHALLENGE_WINDOW, elle peut être supprimée des listes de l'agent étranger, peut-être avec toutes les autres informations d'enregistrement pour le nœud mobile si il n'est plus enregistré.

On présume que l'agent étranger tient une matrice des défis annoncés, un enregistrement du dernier défi annoncé utilisé par un nœud mobile, et aussi un enregistrement du dernier défi fourni à un nœud mobile dans une réponse d'enregistrement ou dans une annonce d'agent en envoi individuel.

Pour satisfaire aux obligations de sécurité mentionnées à la Section 12, l'agent étranger DEVRAIT utiliser un des défis précédemment inutilisés déjà mémorisés, lors d'une réponse à une demande d'enregistrement ou sollicitation d'agent non authentifiée. Si aucun des défis déjà mémorisés n'est précédemment inutilisé, l'agent étranger DEVRAIT générer un nouveau défi, l'inclure dans la réponse, et le mémoriser dans la structure de données par mobiles.

3.3 Traitement par l'agent étranger des réponses d'enregistrement

L'agent étranger DEVRAIT inclure une nouvelle extension Défi de mobile étranger dans toute réponse d'enregistrement, réussie ou non. Si l'agent étranger inclut cette extension dans une réponse d'enregistrement réussie, l'extension DEVRAIT précéder une extension d'authentification de mobile étranger, si elle est présente. Supposons que la réponse d'enregistrement inclut une extension Défi provenant de l'agent de rattachement, et que l'agent étranger souhaite inclure une autre extension Défi avec la réponse d'enregistrement pour que le nœud mobile l'utilise. Dans ce cas, l'agent étranger DOIT supprimer l'extension Défi de l'agent de rattachement de la réponse d'enregistrement, ainsi que toute extension d'authentification étranger-rattachement, avant d'ajouter la nouvelle extension Défi à la réponse d'enregistrement.

Un exemple de situation où l'agent étranger PEUT omettre l'inclusion d'une extension Défi de mobile étranger dans la réponse d'enregistrement serait lorsque un nouveau défi a été envoyé récemment en diffusion groupée.

Si un agent étranger a des conditions dans lesquelles il omet l'inclusion d'une extension Défi de mobile étranger dans la réponse d'enregistrement, il DOIT quand même répondre avec une annonce d'agent contenant un défi précédemment inutilisé en réponse à une sollicitation d'agent ultérieure provenant du même nœud mobile. Autrement (lorsque lesdites conditions ne sont pas satisfaites) l'agent étranger DOIT inclure un défi précédemment inutilisé dans toute réponse d'enregistrement, réussie ou non.

Si l'agent étranger ne retire pas l'extension Défi de la demande d'enregistrement reçue du nœud mobile, l'agent étranger DEVRAIT alors mémoriser la valeur du défi au titre de la liste de demandes d'enregistrement en instance [RFC3344]. Aussi, si la réponse d'enregistrement venant de l'agent de rattachement n'inclut pas d'extension Défi, l'agent étranger NE DEVRAIT PAS rejeter la demande d'enregistrement. Si l'extension Défi est présente dans la réponse d'enregistrement, ce DOIT être la même valeur de défi que celle incluse dans la réponse d'enregistrement reçue de l'agent de rattachement, l'agent étranger DOIT insérer une extension Erreur d'agent étranger avec la valeur d'état de ha_wrong_challenge dans la réponse d'enregistrement envoyée au nœud mobile (voir la Section 10).

Un nœud mobile DOIT être prêt à utiliser un défi provenant d'une annonce d'agent en envoi individuel ou en diffusion groupée au lieu d'une retournée dans une réponse d'enregistrement, et il DOIT en solliciter une si il n'en a pas encire reçu soit dans une réponse d'enregistrement, soit dans une annonce récente.

Si l'agent étranger reçoit une réponse d'enregistrement avec la valeur de code ha_bad_aaa_auth, la réponse d'enregistrement avec cette valeur de code DOIT être relayée au nœud mobile. Dans le présent document, chaque fois que l'agent étranger est

obligé de rejeter une demande d'enregistrement, il DOIT mettre ce code dans le champ Code usuel de la réponse d'enregistrement, sauf si la réponse d'enregistrement a déjà été reçue de l'agent de rattachement. Dans ce cas, l'agent étranger DOIT préserver la valeur du champ Code établie par l'agent de rattachement et DOIT mettre son propre code de rejet dans le champ État de l'extension Erreur d'agent étranger (défini dans la [RFC4636]).

3.4 Traitement par l'agent de rattachement de l'extension Défi

Si l'agent de rattachement reçoit une demande d'enregistrement avec l'extension Défi de mobile étranger et si il reconnaît l'extension, l'agent de rattachement DOIT inclure l'extension Défi dans la réponse d'enregistrement. L'extension Défi DOIT être placée après l'extension Authentification de mobile de rattachement, et l'extension DEVRAIT être authentifiée par une extension Authentification étranger-rattachement.

L'agent de rattachement peut recevoir une demande d'enregistrement avec l'extension Authentification AAA mobile. Si l'extension Authentification AAA mobile est utilisée par l'agent de rattachement comme extension permettant l'autorisation et si la vérification échoue du fait d'un authentifiant incorrect, l'agent de rattachement PEUT rejeter la réponse d'enregistrement avec le code d'erreur ha_bad_aaa_auth.

Comme le type d'extension pour l'extension Défi est dans la gamme 128 à 255, l'agent de rattachement DOIT traiter une telle demande d'enregistrement même si il ne reconnaît pas l'extension Défi [RFC3344]. Dans ce cas, l'agent de rattachement va envoyer une réponse d'enregistrement à l'agent étranger qui n'inclut pas d'extension Défi.

3.5 Traitement par le nœud mobile des réponses d'enregistrement

Un nœud mobile peut recevoir le code d'erreur dans la réponse d'enregistrement provenant de l'agent étranger comme réponse à la demande d'enregistrement. Les codes d'erreur sont définis à la Section 10.

Dans tous les cas, si le nœud mobile tente de s'enregistrer à nouveau après une telle erreur, il DOIT utiliser une nouvelle valeur de défi dans un tel enregistrement, obtenue d'une annonce d'agent, ou d'une extension Défi à la réponse d'enregistrement qui contient l'erreur.

Dans le mode d'adresse d'entretien colocalisée, le nœud mobile reçoit une réponse d'enregistrement sans l'extension Défi et traite la réponse d'enregistrement comme spécifié dans la [RFC3344]. Dans ce cas, lorsque le nœud mobile inclut l'extension Authentification AAA mobile, la valeur de défi de 0 est recommandée pour le calcul d'authentifiant mentionné à la Section 8.

4. Extension Défi de mobile étranger

Cette section spécifie une nouvelle extension d'enregistrement IP mobile qui est utilisée pour satisfaire un défi dans une annonce d'agent. L'extension Défi au message Demande d'enregistrement est utilisée pour indiquer le défi que le nœud mobile tente de satisfaire.

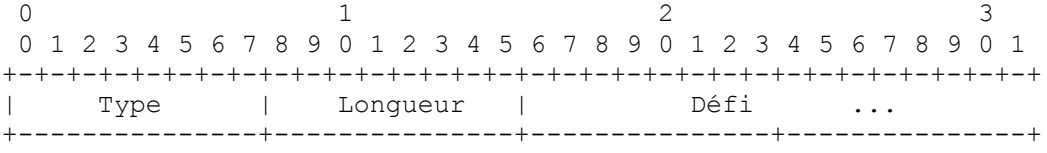

Figure 2 : Extension Défi de mobile étranger

Type : 132 (sautable). (Voir la [RFC3344]).

Longueur : Longueur de la valeur du défi.

Défi : le champ Défi est copié du champ Défi qui se trouve dans l'extension Défi reçue.

Supposons que le nœud mobile se soit enregistré avec succès en utilisant une des valeurs de défi parmi les valeurs de la CHALLENGE_WINDOW annoncée par l'agent étranger. Dans ce cas, dans toute nouvelle demande d'enregistrement, le nœud mobile NE DOIT PAS utiliser de valeur de défi annoncée par l'agent étranger avant la valeur de défi dans la dernière demande d'enregistrement du nœud mobile.

5. Extension généralisée d'authentification IP mobile

Plusieurs nouvelles extensions d'authentification ont été conçues pour divers messages de contrôle proposés pour des extensions à IP mobile. Une nouvelle extension d'authentification est nécessaire pour qu'un nœud mobile présente ses accréditifs à toute autre entité que celles déjà définies ; les seules entités définies dans la spécification IP mobile de base [RFC3344] sont l'agent de rattachement et l'agent étranger. L'objet de l'extension généralisée d'authentification définie ici est pour collecter les données pour toutes ces nouvelles applications d'authentification dans un seul type d'extension avec des sous types.

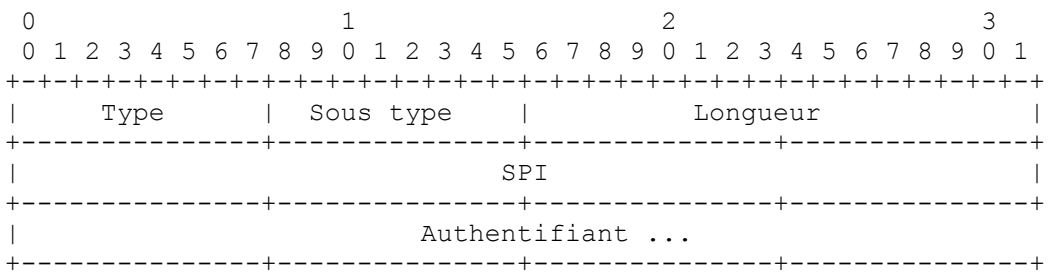

Figure 3 : Extension généralisée d'authentification IP mobile

Type : 36 (non sautable). (Voir la [RFC3344]).

Sous type : numéro alloué pour identifier la sorte de points d'extrémité ou les autres caractéristiques de la stratégie d'authentification particulière.

Longueur : 4 plus le nombre d'octets de l'authentifiant ; DOIT être d'au moins 20.

SPI : indice de paramètres de sécurité

Authentifiant : champ Authentifiant de longueur variable

Dans le présent document, un seul sous type est défini :
1 : sous type d'authentification AAA mobile (Hachage MD5 de code d'authentification de message (HMAC-MD5)) (voir la Section 6).

6. Sous type d'authentification AAA mobile

L'extension généralisée d'authentification avec le sous type 1 sera appelée extension Authentification AAA mobile. Le nœud mobile PEUT inclure une extension Authentification AAA mobile dans toute demande d'enregistrement. Cette extension PEUT coexister dans la même demande d'enregistrement avec les extensions d'authentification définies pour l'enregistrement IP mobile ([RFC3344]). Si le nœud mobile n'inclut pas une extension Authentification de mobile étranger, il DOIT alors inclure l'extension Authentification AAA mobile chaque fois que l'extension Défi est présente. Si les deux sont présentes, l'extension Authentification AAA mobile DOIT précéder l'extension Authentification de mobile étranger.

Si l'extension Authentification AAA mobile est présente, l'extension Authentification de mobile de rattachement DOIT apparaître avant l'extension Authentification AAA mobile. La réponse correspondante DOIT inclure l'extension Authentification de mobile de rattachement et NE DOIT PAS inclure l'extension Authentification AAA mobile.

L'algorithme par défaut pour le calcul de l'authentifiant est HMAC-MD5 [RFC2104] calculé sur les données suivantes, dans l'ordre indiqué :

Données IP mobile précédentes || Type, Sous type, Longueur, SPI

où le Type, Longueur, Sous type, et SPI sont comme le montre la Section 5. Les données IP mobile précédentes se réfèrent à la charge utile UDP (les données de demande d'enregistrement ou de réponse d'enregistrement) et toutes les extensions antérieures en entier. L'invocation de la fonction résultante, comme décrit dans la [RFC2104], serait :

hmac_md5(données, Longueur des données, Clé, Longueur de clé, authentifiant) ;

Chaque nœud mobile DOIT prendre en charge la capacité de produire l'authentifiant en utilisant HMAC-MD5 comme indiqué. Tout comme avec IP mobile, il doit être possible de configurer l'utilisation de tout SPI arbitraire de 32 bits parmi les SPI dans la gamme réservée de 0 à 255 pour le choix de cet algorithme par défaut.

7. SPI réservés pour IP mobile

IP mobile définit plusieurs extensions d'authentification à utiliser dans les demandes et réponses d'enregistrement. Chaque extension d'authentification porte un indice de paramètres de sécurité (SPI) qui devrait être utilisé pour indexer un tableau des associations de sécurité. Les valeurs dans la gamme de 0 à 255 sont réservées pour une utilisation spéciale. Une liste des numéros de SPI réservés est tenue par l'IANA à l'URL suivant : http://www.iana.org/assignments/mobileip-numbers

8. SPI pour serveurs AAA RADIUS

Certains serveurs AAA n'admettent qu'une seule association de sécurité et donc n'utilisent pas de numéro de SPI pour les extensions d'authentification IP mobile pour déterminer l'association de sécurité qui serait nécessaire pour vérifier les informations d'authentification incluses avec l'extension d'authentification.

Le numéro de SPI CHAP_SPI (voir la Section 9) est réservé pour indiquer la procédure qui suit pour calculer les données d'authentification (appelées "authentifiant") qui est utilisée aujourd'hui par de nombreux serveurs RADIUS [RFC2865].

Pour calculer l'authentifiant, appliquer MD5 [RFC1321] calculé sur les données suivantes, dans l'ordre indiqué :

> octet de poids fort de Défi || clé || MD5 (Données IP mobile précédentes || Type, Sous type (si présent), Longueur, SPI) || 237 octets de moindre poids du défi

où Type, Longueur, SPI, et éventuellement Sous type sont les champs de l'extension d'authentification utilisée. Par exemple, ces quatre champs seraient utilisés lorsque SPI == CHAP_SPI est utilisé avec l'extension généralisée d'authentification. En cas d'adresse d'entretien colocalisée, la valeur de défi de 0 est utilisée (voir le paragraphe 3.5). Comme le protocole RADIUS ne peut pas porter des attributs d'une longueur supérieure à 253, les données IP mobile précédentes, le type, le sous type (si présent), la longueur, et le SPI sont hachés en utilisant MD5. Finalement, les 237 octets de moindre poids du défi sont enchaînés. Si le défi a moins de 238 octets, cet algorithme inclut deux fois l'octet de poids fort dans le calcul mais assure que le défi est utilisé exactement tel quel. Aucun bourrage supplémentaire n'est utilisé pour augmenter la longueur du défi ; les données d'entrée peuvent faire moins de 237 octets de long.

9. Paramètres configurables

Chaque agent IP mobile qui prend en charge les extensions définies dans le présent document DEVRAIT être capable de configurer chaque paramètre du tableau suivant. Chaque entrée du tableau contient le nom du paramètre, la valeur par défaut, et le paragraphe du document dans lequel le paramètre paraît pour la première fois.

Nom du paramètre	Valeur par défaut	Section du document
CHALLENGE_WINDOW	2	3.2
CHAP_SPI	2	8

Tableau 1 : Paramètres configurables

Noter que CHALLENGE_WINDOW DEVRAIT être d'au moins 2. Cela rend beaucoup moins probable que des nœuds mobiles s'enregistrent en utilisant une valeur de défi qui soit en dehors de l'ensemble de valeurs admissibles par l'agent étranger.

10. Valeurs d'erreur

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

Nom d'erreur	Valeur	paragraphe du document
unknown_challenge	104	3.2
nœud mobile a échoué à l'authentification	67	3.2 ; voir aussi la [RFC3344]
missing_challenge	105	3.1, 3.2
stale_challenge	106	3.2
fa_bad_aaa_auth	108	3.2
ha_bad_aaa_auth	144	3.4
ha_wrong_challenge	109	3.2

Tableau 2 : Valeurs d'erreur

11. Considérations relatives à l'IANA

Ce qui suit est actuellement alloué par l'IANA pour la [RFC3012] et est applicable au présent document. L'IANA a enregistré ces valeurs au titre du présent document.

L'extension généralisée d'authentification IP mobile définie à la Section 5 est une extension d'enregistrement IP mobile. L'IANA a alloué une valeur de 36 à cette extension.

Un nouvel espace de numéros est à créer pour énumérer les sous types de l'extension généralisée d'authentification (voir la Section 5). Les nouveaux sous types de l'extension généralisée d'authentification, autres que le numéro (1) pour l'extension d'authentification AAA mobile spécifiée à la Section 6, doivent être spécifiés et approuvés par un expert désigné.

L'extension Défi de nœud mobile - agent étranger (MN-FA) définie à la Section 4, est une extension d'annonce de routeur comme défini dans la [RFC1256] et étendue dans la [RFC3344]. L'IANA a alloué une valeur de 132 à cette fin.

Les valeurs de code définies à la Section 10 sont des codes d'erreur comme défini dans la [RFC3344]. Elles correspondent aux valeurs d'erreur conventionnellement associées au rejet par l'agent étranger (c'est-à-dire, des valeurs dans la gamme de 64 à 127). La valeur de code 67 est une valeur préexistante qui est à utiliser dans certains cas avec l'extension définie dans la présente spécification. L'IANA a enregistré les valeurs définies à la Section 10.

Une nouvelle section pour énumérer les algorithmes identifiés par des SPI spécifiques dans la gamme de 0 à 255 a été ajoutée par l'IANA. Le numéro CHAP_SPI 2 discuté à la Section 8 est alloué dans cette gamme de numéros de SPI réservés. Les nouvelles allocations dans cette gamme réservée doivent être spécifiées et approuvées par le groupe de travail IP mobile. Le numéro de SPI 1 ne devrait pas être alloué sauf à l'avenir si le groupe de travail IP mobile décide que SKIP n'est pas important pour l'énumération dans la liste des numéros réservés. Le numéro de SPI 0 ne devrait pas être alloué.

De plus, les nouveaux codes d'erreur fa_bad_aaa_auth, ha_bad_aaa_auth, et ha_wrong_challenge sont définis par le présent document. Parmi eux, ha_wrong_challenge peut apparaître dans le code d'état de l'extension Erreur d'agent étranger, défini dans la [RFC4636].

12. Considérations sur la sécurité

Dans le cas où un nœud mobile malveillant tente de répéter l'authentifiant pour un vieux défi mobile étranger, l'agent étranger va le détecter, car l'agent vérifie toujours si il a annoncé le défi récemment (voir le paragraphe 3.2). Permettre aux nœuds mobiles qui ont des adresses IP ou des NAI différents d'utiliser la même valeur de défi ne représente pas une vulnérabilité pour la sécurité, car les données d'authentification fournies par le nœud mobile seront calculées sur des données différentes (l'adresse IP du nœud mobile va au moins varier).

Si l'agent étranger choisit une valeur de défi (voir la Section 2) avec moins de 4 octets, l'agent étranger DEVRAIT inclure la valeur du champ Identification dans les registres qu'il tient pour le nœud mobile. L'agent étranger peut alors déterminer si les messages d'enregistrement qui utilisent la valeur courte de défi sont en fait uniques et donc s'assurer qu'ils ne sont pas répétés à partir d'un enregistrement antérieur.

La Section 8 (SPI pour serveurs RADIUS AAA) définit une méthode de calcul du champ Authentifiant de l'extension généralisée d'authentification IP mobile, en utilisant MD5 d'une manière qui est cohérente avec RADIUS [RFC2865]. L'utilisation de MD5 dans la méthode décrite à la Section 8 est moins sûre que HMAC-MD5 [RFC2104] et DOIT être évitée chaque fois que possible.

Noter qu'un attaquant actif peut essayer d'empêcher la réussite des enregistrements en envoyant un grand nombre de sollicitations d'agent ou des demandes d'enregistrement fautives, dont chacune va causer la réponse de l'agent étranger avec un défi frais, invalidant le défi que le nœud mobile essaye actuellement d'utiliser. Pour empêcher de telles attaques, l'agent étranger NE DOIT PAS invalider les défis précédemment inutilisés lorsque il répond à des demandes d'enregistrements ou des sollicitations d'agent non authentifiées. De plus, l'agent étranger NE DOIT PAS allouer de nouvelles mémorisations lorsque il répond à de tels messages, car cela créerait aussi la possibilité d'un déni de service.

L'extension Défi spécifiée dans le présent document n'a pas besoin d'être utilisée pour le mode adresse d'entretien colocalisée. Dans ce cas, la protection contre la répétition est assurée par le champ Identification dans le message de demande d'enregistrement [RFC3344].

L'extension généralisée d'authentification IP mobile inclut un champ sous type qui est utilisé pour identifier les caractéristiques de la stratégie d'authentification particulière. Le présent document définir seulement un sous type, le sous type Authentification AAA mobile qui utilise HMAC-MD5. Si il est nécessaire à l'avenir de passer à un nouvel algorithme d'authentification de message, cela pourra se faire en définissant un nouveau sous type qui en utilisera un différent.

13. Remerciements

Les auteurs tiennent à remercier Pete McCann, Ahmad Muhanna, Henrik Levkowetz, Kent Leung, Alpesh Patel, Madjid Nakhjiri, Gabriel Montenegro, Jari Arkko, et les autres participants au groupe de travail MIP4 pour leurs commentaires utiles.

14. Références normatives

[RFC1256] S. Deering, éditeur, "Messages ICMP de découverte de routeur", septembre 1991.

[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992. *(Information)*

[RFC1994] W. Simpson, "Protocole d'authentification par mise en cause de la prise de contact en PPP (CHAP)", août 1996.

[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.

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

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

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

[RFC4636] C. Perkins, "Extension d'erreur d'agent étranger pour IPv4 mobile", octobre 2006. *(P.S.)*

Appendice A. Changements depuis la RFC 3012

Voici la liste des changements par rapport à la [RFC3012] :

- Il est recommandé à l'agent étranger d'inclure un défi dans chaque réponse d'enregistrement afin que le nœud mobile puisse se réenregistrer sans attendre une annonce.
- L'agent étranger DOIT enregistrer les valeurs de défi applicables utilisées par chaque nœud mobile.
- Il est interdit au nœud mobile d'utiliser les valeurs de défi qui ont été annoncées avant la dernière valeur de défi qui a été utilisée pour un enregistrement.

- o Les définitions de défi sont précisées.
- o La suggestion de programme est ajoutée en appendice.
- o L'option HMAC_CHAP_SPI est ajoutée pour l'extension généralisée d'authentification IP mobile. À réception, HMAC_CHAP_SPI, HMAC-MD5 est utilisé à la place de MD5 pour calculer l'authentifiant.
- o Ajout des codes d'erreur fa_bad_aaa_auth et ha_bad_aaa_auth pour rapporter les erreurs d'authentification causées lors du traitement de l'extension Authentification AAA mobile. Aussi, ajout du code d'erreur ha_wrong_challenge pour indiquer que la valeur du défi diffère dans la réponse d'enregistrement reçue de l'agent de rattachement par rapport à celle envoyée à l'agent de rattachement dans la demande d'enregistrement.
- o Le traitement de l'extension Authentification AAA mobile est précisé pour l'agent étranger et l'agent de rattachement
- o La coexistence de l'extension Authentification AAA mobile dans la même demande d'enregistrement est rendue explicite.
- o La situation dans laquelle l'agent étranger envoie missing_challenge est un peu précisée.
- o L'utilisation de l'extension Authentification AAA mobile est permise par le nœud mobile avec une adresse d'entretien colocalisée.
- o Ajout de la protection contre la réponse d'enregistrement et l'annonce d'agent erronées. Aussi, le traitement du défi est précisé si il est reçu dans l'annonce d'agent en diffusion groupée/envoi individuel.
- o Ajout de la référence de l'extension d'erreur d'agent étranger dans la section des références et mise à jour du texte pertinent au paragraphe 3.2 et la Section 11.

Appendice B. Infrastructure de vérification

Les extensions Défi dans cette spécification de protocole sont supposées être utiles pour aider l'agent étranger à gérer la connexité pour les nœuds mobiles visiteurs, même dans des situations où l'agent étranger n'a aucune association de sécurité avec le nœud mobile ni avec l'agent de rattachement du nœud mobile. Pour mener à bien la nécessaire authentification, il est prévu que l'agent étranger va avoir besoin de l'assistance de systèmes administratifs externes, qui se trouvent s'appeler des systèmes AAA. Pour les besoins du présent document, on appelle le support administratif externe "infrastructure de vérification". L'infrastructure de vérification est décrite pour justifier la conception des éléments de protocole définis dans le présent document et n'est pas strictement nécessaire pour le fonctionnement du protocole. L'agent étranger est libre d'utiliser tout moyen à sa disposition pour vérifier les accréditifs du nœud mobile. Il pourrait, par exemple, s'appuyer sur un protocole distinct entre l'agent étranger et l'agent de rattachement IP mobile et n'avoir besoin d'exiger aucune modification du nœud mobile.
Pour vérifier les accréditifs du nœud mobile, on suppose que l'agent étranger a accès à une infrastructure de vérification qui peut retourner une notification sécurisée à l'agent étranger que l'authentification a été effectuée, ainsi que le résultat de cette authentification. Cette infrastructure peut être visualisée comme le montre la Figure 4.

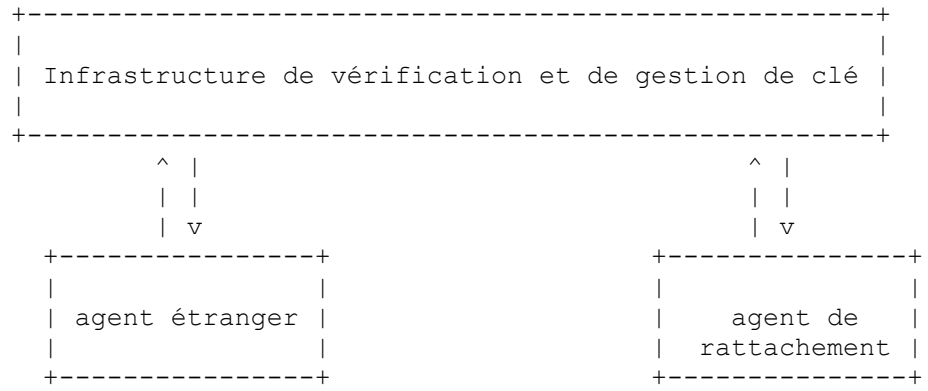

Figure 4 : Infrastructure de vérification

Après que k'agent étranger a obtenu l'authentification du défi, il PEUT passer l'authentification à l'infrastructure (non spécifiée ici) et attendre une réponse d'enregistrement. Si la réponse a un état positif (indiquant que l'enregistrement a été accepté) l'agent étranger accepte l'enregistrement. Si la réponse contient la valeur de code BAD_AUTHENTICATION (voir la Section 10) l'agent étranger prend les mesures indiquées pour les enregistrements rejetés.

L'observation importante que l'agent étranger et l'agent de rattachement doivent être équipés pour utiliser tout protocole exigé par l'infrastructure de vérification du défi et de gestion de clé montrée dans la figure est implicite.

Les messages de protocole pour traiter l'authentification au sein de l'infrastructure de vérification et l'identité de l'agent qui effectue la vérification du défi de l'agent étranger ne sont pas spécifiés dans le présent document, car ces opérations n'ont pas à être effectuer par une entité IP mobile.

Appendice C. Flux de messages pour le défi de FA avec l'extension AAA mobile

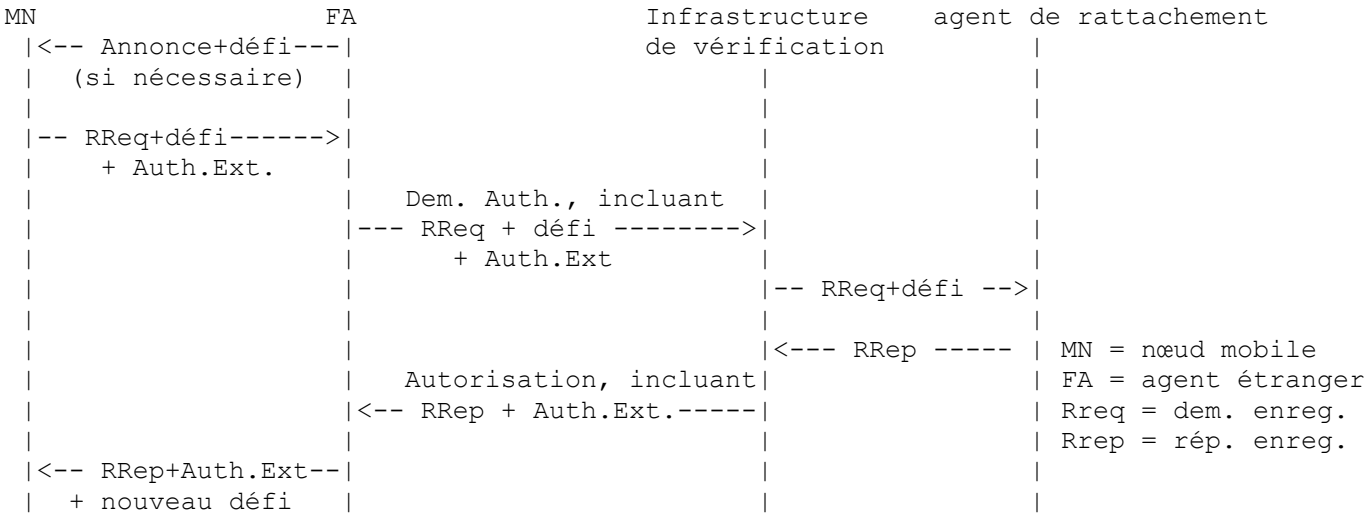

Figure 5 : Flux de messages pour défi de l'agent étranger

Dans la Figure 5, le flux de messages d'informations suivant est illustré :

1. L'agent étranger inclut une valeur de défi dans une annonce d'agent en envoi individuel, si nécessaire. Cette annonce PEUT avoir été produite après réception d'une sollicitation d'agent provenant du nœud mobile (non montrée sur la figure).

2. Le nœud mobile crée une demande d'enregistrement incluant la valeur de défi annoncée dans l'extension Défi, ainsi qu'avec une extension d'authentification AAA mobile.

3. L'agent étranger relaye la demande d'enregistrement à l'agent de rattachement spécifié par le nœud mobile ou à son infrastructure de vérification configurée localement (voir l'Appendice B) conformément à la politique locale.

4. L'agent étranger reçoit une réponse d'enregistrement avec les indications appropriées pour autoriser la connexité pour le nœud mobile.

5. L'agent étranger relaye la réponse d'enregistrement au nœud mobile, souvent avec une nouvelle valeur de défi à utiliser par le nœud mobile dans son prochain message de demande d'enregistrement.

Appendice D. Flux de messages pour défi d'agent étranger avec authentification MN-FA

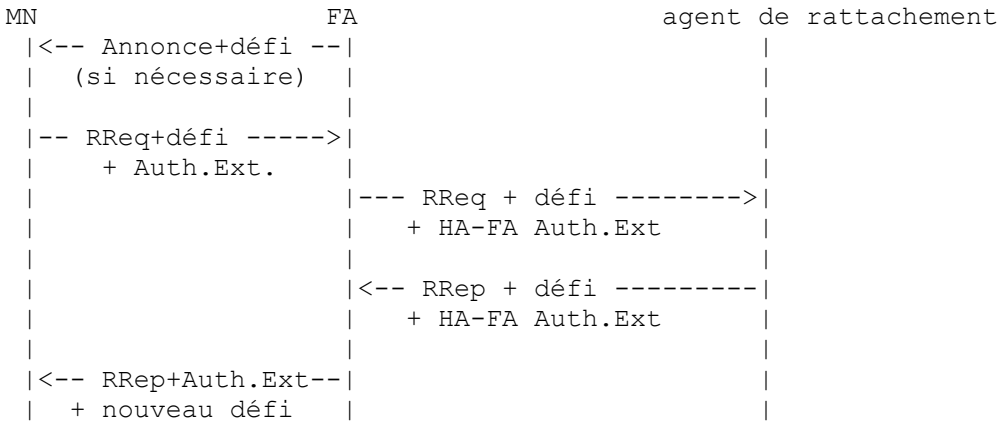

Figure 6 : Flux de messages pour défi d'agent étranger avec authentification MN-FA

Dans la Figure 6, le flux de messages d'informations suivant est illustré :

1. L'agent étranger diffuse une valeur de défi dans une annonce d'agent, si nécessaire. Cette annonce PEUT avoir été produite après réception d'une sollicitation d'agent de la part du nœud mobile (non montrée sur la figure).

2. Le nœud mobile crée une demande d'enregistrement incluant la valeur de défi annoncée dans l'extension Défi, avec une extension Authentification de mobile étranger.

3. L'agent étranger relaye la demande d'enregistrement à l'agent de rattachement spécifié par le nœud mobile.

4. L'agent étranger reçoit une réponse d'enregistrement avec les indications appropriées pour autoriser la connexité pour le nœud mobile.

5. L'agent étranger relaye la réponse d'enregistrement au nœud mobile, éventuellement avec une nouvelle valeur de défi à utiliser par le nœud mobile dans son prochain message de demande d'enregistrement. Si la réponse contient la valeur de code ha_bad_aaa_auth (voir la Section 10) l'agent étranger prend les mesures indiquées pour les enregistrements rejetés.

Appendice E. Exemple de pseudocode pour suivre les défis utilisés

```
current_chal := RegistrationRequest.challenge_extension_value
last_chal := mobile_node_record.last_used_adv_chal

if (current_chal == mobile_node_record.RegReply_challenge) {
   update (mobile_node_record, current_chal)
   return (OK)
}
else if (current_chal "among" VALID_ADV_CHALLENGES[]){
  if (last_chal "among" VALID_ADV_CHALLENGES[]) {
     if (current_chal is "before" last_chal) {
        send_error(STALE_CHALLENGE)
        return (FAILURE)
     }
     else {
        update (mobile_node_record, current_chal)
        return (OK)
     }
  }
  else {
     update (mobile_node_record, current_chal)
     return (OK)
  }
}
else {
  send_error(UNKNOWN_CHALLENGE);
}
```

Adresse des auteurs

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

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

Jayshree Bharatia
Nortel Networks
2221, Lakeside Blvd
Richardson, TX 75082
téléphone : +1 972-684-5767
mél : jayshree@nortel.com

Déclaration complète de droits de reproduction

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