Groupe de travail Réseau
Request for Comments : 5627
Catégorie : Sur la voie de la normalisation

J. Rosenberg, Cisco Systems
octobre 2009
Traduction Claude Brière de l'Isle

Obtention et utilisation des URI d'agent d'utilisateur à acheminement mondial (GRUU) dans le protocole d'initialisation de session (SIP)

(La présente traduction incorpore l'errata 3173)

Résumé
Plusieurs applications du protocole d'initialisation de session (SIP, *Session Initiation Protocol*) exigent qu'un agent d'utilisateur (UA, *agent d'utilisateur*) construise et distribue un URI qui puisse être utilisé par tout le monde dans l'Internet pour acheminer un appel à cette instance d'UA spécifique. Un URI qui achemine à une instance d'UA spécifique est appelé un URI d'agent d'utilisateur mondialement acheminable (GRUU, *Globally Routable UA URI*). Le présent document décrit une extension à SIP pour obtenir un GRUU d'un registraire et pour communiquer un GRUU à un homologue au sein d'un dialogue.

Statut de ce mémoire
Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc5627

Table des Matières

1. Introduction

Dans le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) [RFC3261], l'unité de base de référence est l'adresse d'enregistrement(AOR, *Address Of Record*). Cependant, dans les systèmes SIP, un seul utilisateur peut avoir un certain nombre d'agents d'utilisateur (combinés téléphoniques, téléphones portables, comptes de messagerie vocale, etc.) qui sont tous référencés par la même AOR. Il y a un certain nombre de contextes dans lesquels il est désirable d'avoir un identifiant qui s'adresse à un seul agent d'utilisateur plutôt qu'au groupe d'agents d'utilisateur indiqué par une AOR.

Par exemple, considérons une application de transfert aveugle (voir la [RFC5589]). L'usager A parle à l'usager B. A veut transférer l'appel à l'usager C. Donc, A envoie un REFER à C. Ce REFER ressemble, en partie, à :

```
REFER sip:C@exemple.com SIP/2.0
From: sip:A@exemple.com;tag=99asd
To: sip:C@exemple.com
Refer-To: (URI that identifies B's UA)
```

Le champ d'en-tête Refer-To doit contenir un URI qui puisse être utilisé par l'utilisateur C pour passer un appel à l'utilisateur B. Cependant, cet appel a besoin d'être acheminé à l'instance d'UA spécifique que l'utilisateur B utilise pour parler à l'utilisateur A. Sinon, le service de transfert ne sera pas exécuté correctement. Par exemple, si A donne à C l'AOR de B, l'appel pourrait être acheminé à la boîte vocale de B au lieu du combiné téléphonique de B.

Afin de permettre cette fonctionnalité, l'utilisateur B fournit un URI spécifique de l'instance à l'utilisateur A dans l'en-tête Contact de leur échange SIP. Cet URI se réfère à l'agent d'utilisateur que B utilise actuellement, et il peut être déréférencé par l'agent d'utilisateur de C. Parce que l'utilisateur B ne sait pas à l'avance à qui l'utilisateur A va transférer l'appel, l'URI doit être utilisable par tous.

De nombreux clients actuels tentent de satisfaire au besoin d'un identifiant spécifique d'instance en utilisant des adresses IP explicites dans les valeurs qu'ils fournissent dans le champ d'en-tête Contact. Cependant, cela interagit mal avec les NAT et pare-feu, et en pratique, ces URI ne peuvent pas être utilisés par des clients externes arbitraires. L'usage des noms d'hôtes s'est révélé problématique pour des raisons similaires. De plus, de nombreux clients SIP n'ont pas ou ne peuvent pas obtenir du tout de nom d'hôte pour eux-mêmes.

La présente spécification décrit un mécanisme pour fournir un identifiant univoque d'agent d'utilisateur (UA, *User Agent*) qui est acheminable mondialement. Cet identifiant est appelé un URI d'agent d'utilisateur acheminable mondialement (GRUU, *Globally Routable User Agent*).

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].

La présente spécification définit les termes supplémentaires suivants :

Contact : le terme "contact", utilisé tout en minuscules, se réfère à un URI lié à une AOR et un GRUU au moyen d'un enregistrement. Un contact est généralement un URI SIP, et est lié à l'AOR et au GRUU par une demande REGISTER où il apparaît comme une valeur du champ d'en-tête Contact. L'URI contact identifie un UA spécifique.

Cible distante : le terme "cible distante" se réfère à un URI qu'un agent d'utilisateur utilise pour s'identifier pour la réception de demandes de mi-dialogue et hors dialogue. Une cible distante est établie en plaçant un URI dans le champ d'en-tête Contact d'une demande ou réponse formant dialogue et est mise à jour par des demandes ou réponses de rafraîchissement de cible.

Champ d'en-tête Contact : le terme "champ d'en-tête Contact", avec un C majuscule, se réfère au champ d'en-tête qui peut apparaître dans les demandes et réponses REGISTER, les demandes et réponse de redirection, ou de création de dialogue. Selon la sémantique, le champ d'en-tête Contact porte parfois un contact, et parfois une cible distante.

3. Vue d'ensemble du fonctionnement

L'idée de base derrière un GRUU est simple. Les GRUU sont produits par les domaines SIP et acheminent toujours vers un mandataire dans ce domaine. À son tour, le domaine maintient le lien entre le GRUU et l'instance d'UA particulière. Quand un GRUU est déréférencé lors de l'envoi d'une demande SIP, cette demande arrive au mandataire. Il transpose le GRUU en le contact pour l'instance d'UA particulière, et y envoie la demande.

3.1 Structure des GRUU

Un GRUU est un URI SIP qui a deux propriétés :
- o Il achemine à une instance d'UA spécifique.
- o Il peut être déréférencé avec succès par tout agent d'utilisateur sur l'Internet, pas juste ceux du même domaine ou réseau IP comme l'instance d'UA sur laquelle pointe le GRUU.

En principe, un GRUU peut être construit de toute façon que le domaine choisit, tant qu'il satisfait aux critères ci-dessus. Cependant, tous les GRUU contiennent le paramètre d'URI "gr" (avec ou sans une valeur) de sorte qu'un receveur de GRUU peut dire qu'il a ces deux propriétés.

En pratique, il y a deux différents types de GRUU :
1. Les GRUU qui exposent l'AOR sous-jacente,
2. Les GRUU qui cachent l'AOR sous-jacente.

3.1.1 GRUU qui exposent l'AOR sous-jacente

Dans de nombreux cas, il est désirable de construire le GRUU de telle façon que la transposition en AOR soit apparente. Par exemple, de nombreux agents d'utilisateur conservent les enregistrements d'appel, qui gardent trace des tentatives d'appel entrantes et sortantes. Si l'UA a fait un appel à un GRUU (peut-être par suite d'une demande de transfert) l'enregistrement d'appel va contenir le GRUU. Comme l'enregistrement d'appel est rendu à l'utilisateur, il serait utile d'être capable de présenter plutôt l'AOR à l'utilisateur, car l'AOR a une signification d'identifiant aux utilisateurs.

Ce type de GRUU est appelé un GRUU public. Il est construit en prenant l'AOR, et en y ajoutant le paramètre d'URI "gr" avec une valeur choisie par le registraire dans le domaine. La valeur du paramètre d'URI "gr" URI contient une représentation de l'instance d'UA. Par exemple, si l'AOR était "sip:alice@exemple.com", le GRUU pourrait être :

sip:alice@exemple.com;gr=kjh29x97us97d

Si un UA retire le paramètre d'URI "gr", le résultat est l'AOR. Comme de toutes façons, de nombreux systèmes ignorent les paramètres inconnus, un GRUU public va "ressembler" à l'AOR pour ces systèmes.

3.1.2 GRUU qui cachent l'AOR sous-jacente

Dans d'autres cas, il est désirable de construire un GRUU qui obscurcit l'AOR afin qu'elle ne puisse pas être extraite par un receveur du GRUU. Un tel GRUU est appelé un GRUU temporaire. La raison la plus évidente de le faire est de protéger la confidentialité de l'utilisateur. Dans un tel cas, le GRUU peut avoir un contenu quelconque pourvu qu'il satisfasse les exigences des paragraphes 3.1 et 5.4, et l'AOR ne peut pas être directement déterminée à partir du GRUU. Le GRUU va avoir le paramètre d'URI "gr", avec ou sans une valeur. Afin d'éviter de créer trop d'état chez le registraire, il est souvent désirable de construire des GRUU "sans état" protégés cryptographiquement en utilisant un algorithme comme celui décrit à l'Appendice A.

Un exemple de GRUU temporaire construit en utilisant un algorithme à états pleins va être :

sip:asd887f9dfkk76690@exemple.com;gr

3.2 Obtention d'un GRUU

Un agent d'utilisateur peut obtenir un GRUU d'une des différentes façons suivantes :
- o Au titre de sa transaction REGISTER.
- o En en construisant un en local, en utilisant l'adresse IP ou un nom d'hôte de l'instance d'agent d'utilisateur comme partie domaine de l'URI. Ils sont appelés des GRUU autonomes, et ne sont seulement réellement des GRUU que quand ils sont construits par des UA qui savent qu'ils sont accessibles mondialement en utilisant leur adresse IP ou nom d'hôte.
- o Via un mécanisme administratif spécifié en local.

Un UA qui veut obtenir un GRUU via sa demande REGISTER le fait en fournissant un identifiant d'instance dans le paramètre "+sip.instance" du champ d'en-tête Contact, défini dans la [RFC5626]. Par exemple :

```
Contact: <sip:callee@192.0.2.2>
;+sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>"
```

Le registraire détecte ce paramètre de champ d'en-tête et fournit deux GRUU dans la réponse REGISTER. L'un d'eux est un GRUU temporaire, et l'autre est le GRUU public. Ces deux GRUU sont retournés dans les paramètres, respectivement "temp-gruu" et "pub-gruu", du champ d'en-tête Contact dans la réponse. Par exemple :

```
<allOneLine>
Contact: <sip:callee@192.0.2.2>
;pub-gruu="sip:callee@exemple.com;gr=urn:
uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6"
;temp-gruu="sip:tgruu.7hs==
jd7vnzga5w7fajsc7-ajd6fabz0f8g5@exemple.com;gr"
;+sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>"
;expires=3600
</allOneLine>
```

Noter que l'étiquette <allOneLine> est utilisée comme défini dans la [RFC4475].

Quand un agent d'utilisateur rafraîchit cet enregistrement avant son expiration, le registraire va retourner le même GRUU public, mais va créer un nouveau GRUU temporaire. En dépit du fait que chaque rafraîchissement fournit à l'UA un nouveau GRUU temporaire, tous les GRUU temporaires appris des réponses REGISTER précédentes durant la vie d'un contact restent valides tant que (1) un contact avec cet identifiant d'instance reste enregistré, et (2) l'UA ne change pas le Call-ID dans sa demande REGISTER par rapport aux précédentes pour le même reg-id [RFC5626]. Quand le dernier contact pour l'instance expire, soit par désenregistrement explicite, soit par fin de temporisation, tous les GRUU temporaires deviennent invalides. De même, si un rafraîchissement de REGISTER pour un contact (ou, si la RFC 5626 est utilisée, pour un reg-id) change le Call-ID par rapport aux précédents rafraîchissements de REGISTER, tous les GRUU temporaires précédents sont invalidés. Quand l'agent d'utilisateur crée plus tard un nouvel enregistrement avec le même identifiant d'instance, le GRUU public est le même. Le GRUU temporaire va être nouveau (car il est avec des rafraîchissements) et il va être le seul GRUU temporaire valide pour l'instance jusqu'au prochain rafraîchissement, point auquel le second devient aussi valide. Par conséquent, les GRUU temporaires "s'accumulent" durant la vie d'un enregistrement.

3.3 Utilisation d'un GRUU

Une fois qu'un agent d'utilisateur obtient des GRUU du registraire, il les utilise de plusieurs façons. D'abord, il les utilise comme contenu du champ d'en-tête Contact dans les demandes et réponses non REGISTER qu'il émet (par exemple, une demande INVITE et une réponse 200 OK). Selon la [RFC3261], le champ d'en-tête Contact est supposé contenir un URI qui achemine à cet agent d'utilisateur. Avant cette spécification, il n'y avait pas de moyen de satisfaire réellement cette exigence. L'agent d'utilisateur va utiliser un de ses GRUU temporaires pour des appels anonymes, et utiliser son GRUU public autrement. Ensuite, l'UA peut utiliser le GRUU en tout endroit où il a besoin d'utiliser un URI qui se résout en lui-même, comme une page de la Toile

3.4 Déréferencement d'un GRUU

Parce qu'un GRUU est simplement un URI, un UA le déréférence exactement de la même façon qu'il le ferait de tout autre URI. Cependant, une fois que la demande a été acheminée au mandataire approprié, le comportement est légèrement différent. Le mandataire va transposer le GRUU en l'AOR et déterminer l'ensemble de contacts que l'instance d'UA particulière a enregistré. Le GRUU est alors transposé en ces contacts, et la demande est acheminée vers l'UA.

4. Comportement de l'agent d'utilisateur

Cette Section défini le comportement normatif des agents d'utilisateur.

4.1 Génération d'une demande REGISTER

Quand un UA conforme à la présente spécification génère une demande REGISTER (initiale ou rafraîchissement) il DOIT inclure le champ d'en-tête Supported dans la demande. La valeur de ce champ d'en-tête DOIT inclure "gruu" comme une des étiquettes d'option. Cela alerte le registraire pour le domaine que l'UA prend en charge le mécanisme de GRUU.

De plus, pour chaque contact pour lequel l'UA désire obtenir un GRUU, l'UA DOIT inclure une étiquette de caractéristique de support "sip.instance" (voir dans la [RFC5626]) comme caractéristique d'UA (voir la [RFC3840]) dont la valeur DOIT être l'identifiant d'instance qui identifie l'instance d'UA à enregistrer. Aucun de ces champs d'en-tête Contact NE DEVRAIT contenir de champ d'en-tête "pub-gruu" ou "temp-gruu". L'URI de contact NE DOIT PAS être équivalent, sur la base des règles d'égalité d'URI de la [RFC3261], à l'AOR dans le champ d'en-tête To. Si l'URI de contact est un GRUU, il NE DOIT PAS être un GRUU pour l'AOR dans le champ d'en-tête To.

Comme dans la [RFC3261], le Call-ID dans un rafraîchissement de REGISTER DEVRAIT être identique au Call-ID utilisé pour enregistrer précédemment un contact. Avec le GRUU, une considération supplémentaire s'applique. Si le Call-ID change dans un rafraîchissement de REGISTER, le serveur va invalider tous les GRUU temporaires associés à cette instance d'UA ; le seul valide va être le nouveau retourné dans cette réponse REGISTER. Quand la RFC 5626 est utilisée, cette règle s'applique aux reg-id : si le Call-ID change pour le rafraîchissement d'enregistrement pour un reg-id particulier, le serveur va invalider tous les GRUU temporaires associés à cette instance d'UA en bloc. Par conséquent, si un UA souhaite que ses GRUU temporaires obtenus précédemment restent valides, il DOIT utiliser le même Call-ID dans les rafraîchissements de REGISTER. Cependant, il PEUT changer le Call-ID dans un rafraîchissement si l'invalidation est l'objectif désiré.

Noter que, si des dialogues sont en cours qui utilisent un GRUU temporaire comme cible distante, et si un UA effectue un rafraîchissement d'enregistrement avec un changement de Call-ID, ces GRUU temporaires deviennent invalides, et l'UA ne va plus être accessible pour les messages de mi-dialogue suivants.

Si une instance d'UA essaye d'enregistrer plusieurs contacts pour la même instance pour des besoins de redondance, elle DOIT utiliser les procédures définies dans la [RFC5626].

Un UA qui utilise des GRUU peut quand même effectuer des enregistrements de tiers et peut inclure des contacts qui omettent le paramètre "+sip.instance" du champ d'en-tête Contact.

Si un UA souhaite garantir que la demande REGISTER n'est traitée que si le domaine prend en charge et utilise cette extension, il PEUT inclure un champ d'en-tête Require dans la demande avec une valeur qui contient l'étiquette d'option "gruu". Ceci s'ajoute à la présence du champ d'en-tête Supported, qui contient aussi l'étiquette d'option "gruu". L'utilisation de Proxy-Require n'est pas nécessaire et N'EST PAS RECOMMANDÉE.

4.2 Apprendre les GRUU des réponses REGISTER

Si la réponse REGISTER est un 2xx, chaque champ d'en-tête Contact qui contient le paramètre "+sip.instance" du champ d'en-tête Contact peut aussi contenir un paramètre "pub-gruu" et "temp-gruu" de champ d'en-tête Contact. Ces paramètres de champ d'en-tête portent respectivement le GRUU public et un GRUU temporaire pour l'instance d'UA. Un UA DOIT être prêt pour un champ d'en-tête Contact qui contient juste un "pub-gruu", juste un "temp-gruu", les deux ou aucun. Le GRUU temporaire va être valide pendant la durée de l'enregistrement (c'est-à-dire, avec des rafraîchissements) tandis que le GRUU public persiste à travers les enregistrements. L'UA va recevoir un nouveau GRUU temporaire à chaque réponse REGISTER réussie, tandis que le GRUU public va normalement être le même. Cependant, un UA DOIT être prêt à ce que le GRUU public change par rapport à un précédent, car la propriété de persistance n'est pas garantie avec une complète certitude. Si un UA a changé son Call-ID dans cette demande REGISTER par rapport à une demande REGISTER précédente pour le même contact ou reg-id, l'UA DOIT éliminer tous les GRUU temporaires appris par de précédentes réponses REGISTER. Un UA PEUT conserver zéro, un, quelques, ou tous les GRUU temporaires dont il est pourvu durant le temps pendant lequel au moins un contact ou reg-id est resté continuellement enregistré. Si un UA mémorise des GRUU temporaires pour les utiliser durant son enregistrement, il a besoin d'être certain que l'enregistrement ne s'arrête pas accidentellement à cause d'un biais d'horloge entre l'UA et le registraire. Par conséquent, l'UA DOIT rafraîchir son enregistrement de façon à ce que la transaction de rafraîchissement de REGISTER soit s'achève, soit arrive en fin de temporisation avant l'expiration de l'enregistrement. Pour les temporisateurs de transaction par défaut, ce serait au moins 32 secondes avant l'expiration, en supposant que l'expiration de l'enregistrement est supérieure à 64 secondes. Si l'expiration de l'enregistrement est de moins de 64 secondes, l'UA DEVRAIT rafraîchir son enregistrement à mi chemin de l'expiration.

Noter que quand la [RFC5626] est utilisée, et que l'UA utilise plusieurs flux pour les besoins de redondance, les GRUU temporaires restent valides tant qu'au moins un flux est enregistré. Donc, même si l'enregistrement d'un flux arrive à expiration, les GRUU temporaires appris précédemment restent valides.

Dans les cas où les registraires sont forcés de raccourcir les intervalles d'enregistrement, le paquetage d'événement d'enregistrement [RFC3680] est utilisé par les agents d'utilisateur pour apprendre ces changements. Un agent d'utilisateur qui met en œuvre à la fois la [RFC3680] et GRUU DOIT aussi mettre en œuvre les extensions à la [RFC3680] pour convoyer les informations sur le GRUU, comme défini dans la [RFC5628], car elles sont nécessaires pour garder la synchronisation de l'ensemble des GRUU temporaires entre l'UA et le registraire. Plus généralement, l'utilité des GRUU temporaires dépend de la synchronisation de l'UA et du registraire sur l'ensemble des GRUU temporaires valides à tout moment. Sans prise en charge de la [RFC3680] et de son extension pour GRUU, le client va rester synchronisé seulement pour autant qu'il se réenregistre toujours bien avant l'expiration de l'enregistrement. À côté des désenregistrements forcés, d'autres événements (comme des pannes du réseau, défaillances de connexion, et intervalles de rafraîchissement courts) peuvent conduire à de potentielles incohérences dans l'ensemble de GRUU temporaires valides. Pour cette raison, il est RECOMMANDÉ qu'un UA qui utilise des GRUU temporaires mette en œuvre la [RFC3680] et la [RFC5628].

Une réponse non 2xx à la demande REGISTER n'a pas d'impact sur les GRUU existants fournis précédemment à l'UA. Précisément, si une demande REGISTER réussie a précédemment fourni un GRUU à l'UA, un échec d'une demande ultérieure ne retire, supprime, ni n'invalide pas le GRUU.

Les parties utilisateur et hôte du GRUU apprises par l'UA dans la réponse REGISTER DOIVENT être traitées comme opaques par l'UA. C'est-à-dire que l'UA NE DOIT PAS les modifier tant soit peu. Un UA NE DOIT PAS modifier ou retirer des paramètres d'URI qu'il ne reconnaît pas. De plus, l'UA NE DOIT PAS ajouter, retirer, ou modifier des paramètres d'URI pertinents pour la réception et le traitement de demande chez le mandataire, incluant les paramètres d'URI transport, lr, maddr, ttl, user, et comp (voir la [RFC3486]). L'autre paramètre d'URI défini dans la [RFC3261], "method", ne va normalement pas être présent dans un GRUU livré par un registraire, et un UA PEUT ajouter un paramètre d'URI "method" au GRUU avant de le passer à une autre entité. De même, les paramètres d'URI définis dans la [RFC4240] et la [RFC4458] sont destinés à l'usage par l'UA. Ils ne vont pas être inclus dans le GRUU retourné par un registraire et PEUVENT être ajoutés par un UA qui souhaite fournir des services associés à ces paramètres d'URI.

Noter cependant que si un autre UA déréférence le GRUU, les paramètres vont être perdus chez le mandataire quand l'URI de demande est traduit en le contact enregistré, sauf si d'autres moyens sont fournis pour que les attributs soient livrés à l'UA. Des mécanismes pour une telle livraison sont actuellement le sujet d'une future activité de normalisation (voir "Livraison des URI de demande cibles aux agents d'utilisateur" [URI]).

4.3 Construction d'un GRUU par soi-même

De nombreux agents d'utilisateur (comme des passerelles du réseau téléphonique public commuté (RTPC) des serveurs de conférence, et des serveurs de supports) n'effectuent pas d'enregistrements, et ne peuvent pas obtenir de GRUU par ce mécanisme. Ces types d'agents d'utilisateur peuvent être publiquement accessibles. Cela signifierait que la politique du domaine est que les demandes peuvent venir de n'importe où dans l'Internet public et être livrées à l'agent d'utilisateur sans exiger de traitement par les mandataires intermédiaires dans le domaine. De plus, les politiques de pare-feu et de NAT administrées par le domaine permettraient de telles demandes dans le réseau. Quand un agent d'utilisateur est certain que

ces conditions sont satisfaites, un UA PEUT construire un GRUU autonome. Bien sûr, un agent d'utilisateur qui fait REGISTER, mais pour qui ces conditions sont de toutes façons satisfaites, PEUT aussi construire un GRUU autonome. Cependant, l'usage de GRUU obtenus par le registraire est plutôt RECOMMANDÉ.

Un GRUU autonome est celui dont la partie domaine est égale à l'adresse IP ou nom d'hôte de l'agent d'utilisateur. La partie utilisateur de l'URI SIP est choisie arbitrairement par l'agent d'utilisateur. Comme tous les autres GRUU, l'URI DOIT contenir le paramètre d'URI "gr", avec ou sans une valeur, indiquant qu'il est un GRUU.

Si un agent d'utilisateur ne s'enregistre pas, mais n'est pas publiquement accessible, il va avoir besoin d'obtenir un GRUU par d'autres moyens. Normalement, l'UA va être configuré avec un GRUU, le GRUU va être configuré dans le mandataire, et le mandataire va être configuré avec une transposition du GRUU en l'adresse IP (ou nom d'hôte) et accès de l'UA.

4.4 Utilisation de ses propres GRUU

Un UA DEVRAIT utiliser un GRUU quand il remplit le champ d'en-tête Contact des demandes et réponses formant dialogue et rafraîchissement de cible. En d'autres termes, un UA conforme à la présente spécification DEVRAIT utiliser un de ses GRUU comme sa cible distante. Cela inclut :

- la demande INVITE,
- une réponse 2xx ou 18x à un INVITE qui contient une étiquette To,
- la demande SUBSCRIBE (voir la [RFC3265])
- une réponse 2xx à un SUBSCRIBE qui contient une étiquette To,
- la demande NOTIFY,
- la demande REFER (voir la [RFC3515])
- une réponse 2xx à NOTIFY,
- la demande UPDATE,
- une réponse 2xx à UPDATE.

Les seules raisons de ne pas utiliser un GRUU seraient des considérations de confidentialité ; voir au paragraphe 10.3.

Quand il utilise un GRUU obtenu par un enregistrement, un UA DOIT avoir un enregistrement actif avant d'utiliser un GRUU, et DOIT utiliser un GRUU appris par cet enregistrement. Il NE DOIT PAS réutiliser un GRUU appris par un précédent enregistrement qui a expiré (en d'autres termes, obtenu quand il a enregistré un contact qui a expiré). L'UA PEUT utiliser soit le GRUU public soit un de ses GRUU temporaires fournis par son registraire. Un UA NE DOIT PAS utiliser un GRUU temporaire appris d'une réponse REGISTER dont le Call-ID diffère de celui de la plus récente demande REGISTER générée par l'UA pour la même AOR et identifiant d'instance (et, si la [RFC5626] est utilisée, le reg-id). Quand un UA souhaite construire une demande anonyme, comme décrit dans la [RFC3323], il DEVRAIT utiliser un GRUU temporaire. Voir au paragraphe 10.3 une discussion plus complète sur le niveau de confidentialité permis par les GRUU temporaires.

Selon la [RFC3261], un UA DEVRAIT inclure un en-tête Supported avec l'étiquette d'option "gruu" dans les demandes et réponses qu'il génère.

4.4.1 Considérations pour AOR multiples

Dans certains réseaux SIP, un agent d'utilisateur peut avoir plusieurs AOR, soit dans différents domaines, soit au sein du même domaine. Dans ce cas, des considérations supplémentaires s'appliquent.

Quand un UA envoie une demande, la demande va être envoyée "en utilisant" une de ses AOR. Cette AOR va normalement apparaître dans le champ d'en-tête From de la demande, et des accréditifs uniques de cette AOR vont être utilisés pour authentifier la demande. Le GRUU placé dans le champ d'en-tête Contact d'une telle demande DEVRAIT être celui qui est associé à l'AOR utilisée pour envoyer la demande. Dans les cas où l'UA utilise un URI tel (comme défini dans la [RFC3966]) pour remplir le champ d'en-tête From, l'UA a normalement une AOR SIP qui est traitée comme un alias pour l'URI tel. Le GRUU associé à cette AOR SIP DEVRAIT être utilisé dans le champ d'en-tête Contact.

Quand un UA reçoit une demande, le GRUU placé dans le champ d'en-tête Contact d'une réponse 2xx DEVRAIT être celui associé à l'AOR ou le GRUU auquel la demande a été le plus récemment ciblée. Il y a plusieurs façons de déterminer l'AOR ou le GRUU auquel une demande a été envoyé. Par exemple, si un UA a enregistré un contact différent pour chaque AOR (en utilisant une partie utilisateur différente de l'URI) l'URI de demande (qui contient ce contact) va indiquer l'AOR.

4.5 Déréférencement d'un GRUU

Un GRUU est identifié par la présence du paramètre d'URI "gr", et ce paramètre d'URI pourrait ou non avoir une valeur. Un UA qui souhaite envoyer une demande à un URI qui contient un GRUU sait que la demande va être livrée à une instance d'UA spécifique sans autre action de la part du demandeur.

Certains UA mettent en œuvre des mécanismes non standard de traitement d'URI qui compensent le fait que jusqu'à présent de nombreux URI de contact n'étaient pas acheminables mondialement. Comme tout URI contenant le paramètre d'URI "gr" est connu pour être acheminable mondialement, un UA NE DEVRAIT PAS appliquer de tels mécanismes quand un URI de contact contient le paramètre d'URI "gr".

Parce que l'identifiant d'instance est un paramètre de capacités de l'appelé, un UA pourrait être tenté d'envoyer une demande à l'AOR d'un utilisateur, et d'inclure un champ d'en-tête Contact Accept (défini dans la [RFC3841]) qui indique une préférence pour l'acheminement de la demande à un UA avec un identifiant d'instance spécifique. Bien que cela paraîtrait avoir le même effet que l'envoi d'une demande au GRUU, ce n'est pas le cas. Les préférences d'appelé exprimées dans le champ d'en-tête Contact Accept sont juste des préférences. Leur efficacité dépend de ce qu'un UA construise un champ d'en-tête Contact Accept qui interagit avec la logique de traitement du domaine pour une AOR, pour causer l'acheminement d'une demande sur une instance particulière. Étant donnée la variabilité de la logique d'acheminement dans un domaine (par exemple, un acheminement fondé sur le temps à seulement des contacts choisis) cela ne fonctionne pas pour de nombreuses politiques d'acheminement de domaines. Cependant, la présente spécification n'interdit pas à un client de tenter une telle demande, car il peut y avoir des cas où l'opération désirée est véritablement une demande d'acheminement préférentiel.

4.6 Rendu des GRUU sur une interface d'utilisateur

Quand on affiche un GRUU à un utilisateur à travers une interface d'utilisateur, il est RECOMMANDÉ que le paramètre d'URI "gr" soit retiré. Pour les GRUU publics, cela va produire l'AOR, comme désiré. Pour les GRUU temporaires, L'URI résultant va être probablement aléatoire. De futurs travaux pourraient fournir des mécanismes améliorés qui permettraient à un automate de savoir qu'un URI est anonymisé, et donc inapproprié à l'affichage.

5. Comportement du registraire

5.1 Traitement d'une demande REGISTER

Une demande REGISTER pourrait contenir un champ d'en-tête Require avec l'étiquette d'option "gruu" ; cela indique que le registraire doit comprendre cette extension afin de traiter la demande. Elle n'exige cependant pas que le registraire crée des GRUU.

Lorsque le registraire traite les contacts dans la demande REGISTER en accord avec les procédures de l'étape 7 du paragraphe 10.3 de la [RFC3261], il vérifie que chaque champ d'en-tête Contact dans le message REGISTER contient un paramètre de champ d'en-tête "+sip.instance". Si il est présent avec une expiration non à zéro, le contact est traité sur la base des règles du reste de cette section. Autrement, le contact est traité sur la base des règles normale de la [RFC3261].

Noter que le traitement d'une demande REGISTER contenant un champ d'en-tête Contact avec la valeur "*" et une expiration de zéro conserve la signification définie dans la [RFC3261] -- tous les contacts, pas seulement ceux qui ont un identifiant d'instance spécifique, sont supprimés. Comme décrit au paragraphe 5.4, cela supprime le lien de chaque contact) l'AOR et le lien de chaque contact à ses GRUU.

Si l'URI de contact est équivalent (sur la base de l'équivalence d'URI de la [RFC3261]) à l'AOR, le registraire DOIT rejeter la demande avec un 403, car cela causerait une boucle d'acheminement. Si l'URI de contact est un GRUU pour l'AOR dans le champ d'en-tête To de la demande REGISTER, le registraire DOIT rejeter la demande avec un 403, pour la même raison. Si le contact n'est pas un URI SIP, la demande REGISTER DOIT être rejetée avec un 403.

Ensuite, le registraire vérifie si il y a déjà un GRUU public valide pour l'AOR (présent dans le champ d'en-tête To de la demande REGISTER) et l'identifiant d'instance (présent comme contenu du paramètre "+sip.instance" du champ d'en-tête Contact). Si il n'y a pas de GRUU public valide, le registraire DEVRAIT construire un GRUU public à ce moment en accord avec les procédures du paragraphe 5.4. Le GRUU public DOIT être construit en ajoutant le paramètre d'URI "gr", avec une valeur, à l'AOR. Si le contact contenait un paramètre "pub-gruu" dans le champ d'en-tête Contact, le paramètre de champ d'en-tête DOIT être ignoré par le registraire. Un UA ne peut pas suggérer ou autrement fournir un GRUU public au registraire.

Ensuite, le registraire vérifie l'existence de contacts enregistrés à la même AOR, au même identifiant d'instance, et si le contact dans la demande REGISTER enregistre un flux [RFC5626], reg-id. Si il y en a au moins un, le registraire trouve celui qui a été le plus récemment enregistré, et examine la valeur du Call-ID associé à ce contact enregistré. Si il diffère de celui de la demande REGISTER, le registraire DOIT invalider tous les GRUU temporaires générés précédemment pour l'AOR et l'identifiant d'instance. Une conséquence de cette invalidation est que les demandes adressées à ces GRUU vont être rejetées par le domaine avec un 404 à partir de ce point.

Ensuite, le registraire DEVRAIT créer un nouveau GRUU temporaire pour l'AOR et l'identifiant d'instance avec les caractéristiques décrites au paragraphe 5.4. L'algorithme de construction de GRUU temporaire DOIT avoir les deux propriétés suivantes :

1. La probabilité que le GRUU temporaire soit égal à un autre GRUU qu'a créé le registraire DOIT être extrêmement petite.

2. Étant donnée une paire de GRUU, il DOIT être impossible de déterminer par le calcul si ils ont été produits pour le même AOR ou identifiant d'instance ou des AOR et identifiants d'instance différents.

Si le contact contenait un paramètre "temp-gruu" de champ d'en-tête Contact, le paramètre de champ d'en-tête DOIT être ignoré par le registraire. Un UA ne peut pas suggérer ou autrement fournir de GRUU temporaire au registraire.

5.2 Génération d'une réponse REGISTER

Quand on génère la réponse 200 (OK) à la demande REGISTER, les procédures de l'étape 8 du paragraphe 10.3 de la [RFC3261] sont suivies. De plus, pour chaque valeur de champ d'en-tête Contact placée dans la réponse, si le registraire a mémorisé un identifiant d'instance associé à ce contact, cet identifiant d'instance est retourné comme paramètre de champ d'en-tête Contact. Si la demande REGISTER contenait un champ d'en-tête Supported qui incluait l'étiquette d'option "gruu", et si le registraire a au moins un GRUU temporaire alloué à l'identifiant d'instance ID et l'AOR, le registraire DOIT ajouter un paramètre "temp-gruu" de champ d'en-tête Contact à ce champ d'en-tête Contact. La valeur du paramètre "temp-gruu" est une chaîne entre guillemets, et DOIT contenir le GRUU temporaire créé le plus récemment pour cette AOR et cet identifiant d'instance. De plus, si le registraire a un GRUU public alloué à l'identifiant d'instance et l'AOR (et si le client prend en charge les GRUU) le registraire DOIT ajouter un paramètre "pub-gruu" de champ d'en-tête Contact à ce champ d'en-tête Contact. La valeur du paramètre "pub-gruu" du champ d'en-tête Contact est le GRUU public.

Le registraire NE DEVRAIT PAS inclure d'étiquette d'option "gruu" dans le champ d'en-tête Require ou Supported de la réponse.

5.3 Fin de temporisation d'un enregistrement

Quand un contact enregistré expire (à cause d'une fin de temporisation ou d'un désenregistrement explicite) son lien à l'AOR est retiré comme d'habitude. De plus, ses liens à ses GRUU sont supprimés en même temps, par suite des relations décrites au paragraphe 5.4

Si, par suite de l'expiration du contact, un GRUU particulier n'a plus de contacts enregistrés qui lui soient liés, et si le GRUU est un GRUU temporaire, le GRUU DOIT être invalidé. Cela signifie que tous les GRUU temporaires accumulés sont invalidés une fois que le dernier contact pour un identifiant d'instance donné expire.

Si, cependant, le GRUU était un GRUU public, le registraire DEVRAIT continuer de traiter le GRUU comme valide. Par conséquent, les demandes suivantes ciblées sur le GRUU, avant le réenregistrement d'un contact au GRUU, DEVRAIENT retourner une réponse 480 (Temporairement indisponible). De plus, comme le GRUU reste valide, les règles du paragraphe 5.1 vont faire qu'il va être conservé quand un contact avec cet identifiant de instance est à nouveau enregistré à l'AOR.

Ces règles donnent à un GRUU public une propriété semi permanente. L'intention est que le registraire fasse tous ses efforts pour conserver la validité du GRUU aussi longtemps que AOR elle-même est connue au sein du domaine. L'exigence pour faire cela est du niveau DEVRAIT et non DOIT à cause de la difficulté de satisfaire une exigence de niveau DOIT ; des défaillances du registraire pourraient causer la perte de l'ensemble des GRUU valides, et la présente spécification exige que l'UA soit robuste dans ce cas. Ceci dit, il est possible qu'un GRUU public soit construit de telle façon qu'un registraire n'ait pas besoin de conserver d'état supplémentaire pour lui, et que le GRUU satisfasse encore les exigences décrites ici.

5.4 Création d'un GRUU

Ce paragraphe définit des comportements supplémentaires associés à la construction et maintenance d'un GRUU qui sont spécifiques d'un registraire. Ces règles ne s'appliquent pas aux GRUU autonomes ou aux GRUU non obtenus par un enregistrement.

Quand un registraire crée un GRUU, il est exigé qu'il tienne certaines informations associées au GRUU, sans considérer si il est un GRUU public ou temporaire. Chaque GRUU est associé à une seule AOR et un seul identifiant d'instance. Un registraire DOIT être capable de déterminer l'identifiant d'instance et l'AOR présentés avec un GRUU. De plus, le GRUU,

comme une AOR, se résout en zéro, un ou plusieurs contacts. Alors qu'une AOR se résout en tous les contacts enregistrés pour une AOR, un GRUU se résout seulement en les contacts dont l'identifiant d'instance correspond à celui associé au GRUU. Pour cette raison, un contact avec un identifiant d'instance est toujours lié à la fois à un GRUU et son AOR, jamais juste à une AOR ou juste un GRUU. Ceci est montré à la Figure 1. La figure montre trois contacts enregistrés à une seule AOR. Un des contacts a un identifiant d'instance de 1, et les deux autres ont un identifiant d'instance de 2. Il y a deux GRUU pour cette AOR. Un est associé à l'identifiant d'instance 1, et l'autre à l'identifiant d'instance 2. Le premier GRUU se résout seulement en les contacts dont l'identifiant d'instance est 1, et le second se résout seulement en les contacts dont l'identifiant d'instance est 2. Il va normalement y avoir plusieurs contacts pour un identifiant d'instance donné si un UA a eu une défaillance, a réamorcé, et s'est réenregistré avec le même identifiant d'instance, ou utilise les mécanismes de la [RFC5626] pour avoir plusieurs enregistrements pour la redondance. Si le contact pour l'identifiant d'instance 1 expire, l'AOR va se résoudre en deux contacts, mais le GRUU associé à l'identifiant d'instance 1 va se résoudre en zéro.

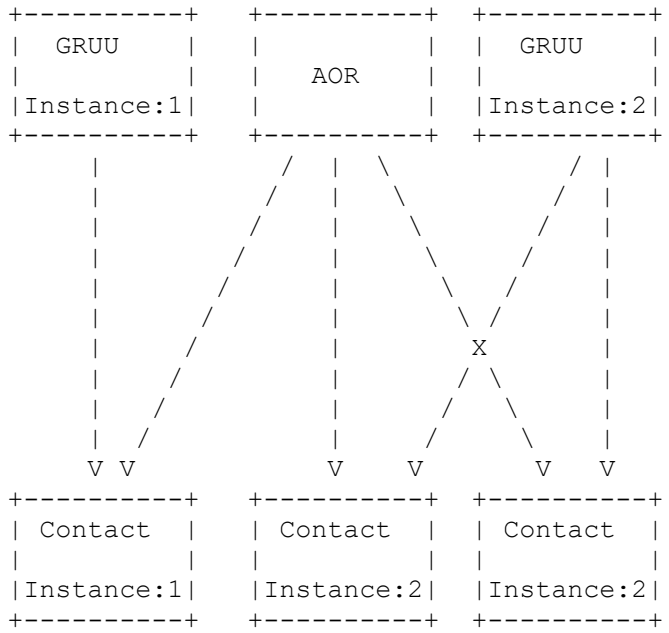

Figure 1

Il peut y avoir plusieurs GRUU avec le même identifiant d'instance et la même AOR. Bien sûr, la présente spécification exige que les registraires en tiennent plusieurs -- un qui est public, et plusieurs qui sont temporaires. Cependant, si deux GRUU sont associés à des AOR différentes ou différents identifiants d'instance, ou les deux, les GRUU DOIVENT être différents sur la base de la comparaison pour égalité d'URI. Un GRUU dans un domaine NE DOIT PAS être équivalent, sur la base de la comparaison d'URI, d'aucune AOR dans un domaine sauf pour celui associé au GRUU.

Un GRUU public va toujours être équivalent à l'AOR sur la base des règles d'égalité d'URI. La raison en est que les règles de la [RFC3261] causent que les paramètres d'URI qui sont dans un URI, mais pas dans l'autre, sont ignorés pour les besoins de la comparaison d'égalité. Comme un GRUU public diffère d'une AOR seulement par la présence du paramètre d'URI "gr", les deux URI sont équivalents sur la base de ces règles.

Une fois qu'un GRUU temporaire est construit, il DOIT être considéré valide par le registraire jusqu'à ce qu'il soit invalidé sur la base des règles décrites précédemment. Une fois qu'un GRUU public est construit, il DOIT être considéré valide pour la durée pendant laquelle l'AOR elle-même est valide. Une fois qu'une AOR n'est plus valide au sein d'un domaine, tous ses GRUU DOIVENT aussi être considérés invalides.

La présente spécification ne rend pas obligatoire de mécanisme particulier pour la construction du GRUU. Un exemple d'algorithmes pour les GRUU publics et temporaires qui fonctionnent bien est donné à l'Appendice A. Cependant, en plus des propriétés décrites au paragraphe 3.1, un GRUU construit par un registraire DOIT présenter les propriétés suivantes :

- La partie domaine de l'URI est une adresse IP présente dans l'Internet public, ou, si elle est un nom d'hôte, les procédures de résolution de la [RFC3263], une fois appliquées, résultent en une adresse IP sur l'Internet public.

- Quand une demande est envoyée au GRUU, il achemine à un mandataire qui peut accéder aux données d'enregistrement générées par le registraire. Un tel mandataire est appelé un mandataire d'autorité, défini dans la [RFC5626].

5.5 Prise en charge d'un événement d'enregistrement

La [RFC3680] définit un paquetage d'événements qui permet à un client d'apprendre les événements d'enregistrement chez le registraire. Ce paquetage permet aux registraires d'altérer de force les enregistrements (par exemple, de les raccourcir pour forcer un ré-enregistrement). Si un registraire prend en charge la [RFC3680] et GRUU, il DOIT aussi prendre en charge la [RFC5628].

6. Comportement du mandataire

Le comportement de mandataire est pleinement défini à la Section 16 de la [RFC3261]. Le traitement de GRUU impacte ce comportement en deux endroits – le ciblage de demande au mandataire d'autorité et l'enregistrement d'acheminement.

6.1 Ciblage de demande

Quand un mandataire reçoit une demande, possède le domaine dans l'URI de demande, et est supposé accéder à un service de localisation afin de calculer les cibles de demandes (comme spécifié au paragraphe 16.5 de la [RFC3261]) le mandataire examine l'URI de demande. Si il contient le paramètre d'URI "gr" mais n'est pas équivalent, sur la base de la comparaison d'URI, à un GRUU actuellement valide dans le domaine, il DEVRAIT être rejeté avec une réponse 404 (Non trouvé) ; c'est le même comportement qu'un mandataire présenterait pour tout autre URI dans le domaine qui n'est pas valide.

Si l'URI de demande contient le paramètre d'URI "gr" et est équivalent, sur la base d'une comparaison d'URI, à un GRUU qui est actuellement valide dans le domaine, le traitement se fait comme pour tout autre URI présent dans le service de localisation, comme défini au paragraphe 16.5 de la [RFC3261], sauf que le paramètre d'URI "gr" n'est pas supprimé au titre du processus de canonisation. C'est le cas pour les demandes hors dialogue ciblées sur le GRUU, et pour les demandes de mi-dialogue ciblées sur le GRUU (dans ce cas la demande entrante va avoir une valeur de champ d'en-tête Route contenant l'URI que le mandataire a utilisé pour l'acheminement d'enregistrement.).

Noter que le paramètre d'URI "gr" est conservé seulement pour les besoins de la découverte du GRUU dans le service de localisation ; si une correspondance est trouvée, l'URI de demande va être réécrit avec les contacts enregistrés, remplaçant le GRUU et son paramètre d'URI "gr". Le paramètre d'URI "gr" n'est pas porté plus loin dans l'URI de demande réécrit.

Si il n'y a pas de contact enregistré lié au GRUU, le serveur DOIT retourner une réponse 480 (Temporairement indisponible). Si il y en a plus d'un, il y a deux cas :

1. Le client utilise la [RFC5626] et enregistre plusieurs contacts pour la redondance. Dans ce cas, ces contacts contiennent des paramètres de champ d'en-tête Contact "reg-id", et les règles décrites à la Section 7 de la [RFC5626] pour choisir un seul contact enregistré s'appliquent.

2. Le client n'utilise pas la [RFC5626], et dans ce cas il va seulement y avoir plusieurs contacts avec le même identifiant d'instance si le client a réamorcé, redémarré, et ré-enregistré. Dans ce cas, ces contacts ne vont pas contenir le paramètre de champ d'en-tête Contact "reg-id". Le mandataire DOIT choisir le contact le plus récemment rafraîchi. Comme avec la RFC 5626, si une demande à cette cible échoue avec une réponse 408 (Demande périmée) ou 430 (Flux défaillant) le mandataire DEVRAIT réessayer avec le prochain contact le plus récemment rafraîchi. De plus, si la demande échoue avec une autre réponse, le mandataire NE DOIT PAS réessayer sur un autre contact pour cette instance.

Toutes les préférences d'appelant dans la demande (comme défini dans la [RFC3841]) DEVRAIENT être traitées par rapport aux contacts liés au GRUU.

Par nature, pour choisir un contact enregistré, le GRUU est traité exactement comme si il était l'AOR, mais seulement avec un sous ensemble des contacts liés à l'AOR.

Des considérations particulières s'appliquent au traitement de tous les en-têtes Path mémorisés dans l'enregistrement (voir la [RFC3327]). Si la demande reçue a des valeurs de champ d'en-tête Route au delà de celle pointant sur le mandataire d'autorité lui-même (cela va arriver quand la demande est une demande de mi-dialogue) l'URI de chemin DOIT être éliminé. Cela est permis par la [RFC3327] comme un sujet de politique locale ; l'usage des GRUU va exiger cette politique afin d'éviter des spirales d'appels et de probables échecs d'appel.

Un mandataire PEUT appliquer un autre traitement à la demande, comme l'exécution de caractéristiques de l'appelé, comme il pourrait le faire pour les demandes ciblées sur une AOR. Pour les demandes qui sont en dehors d'un dialogue, il est RECOMMANDÉ d'appliquer des types de fonctions de dissimulation, automatisées (comme d'écran de liste noire et de liste blanche) et interactives (comme des applications de réponse vocale interactive (IVR) qui confèrent avec l'utilisateur

pour déterminer si il accepte un appel). Dans de nombreux cas, la nouvelle demande se rapporte à un dialogue existant, et pourrait être une tentative de le joindre (en utilisant le champ d'en-tête Join défini dans la [RFC3911]) ou de le remplacer (en utilisant le champ d'en-tête Replaces défini dans la [RFC3891]). Quand la nouvelle demande se rapporte à un dialogue existant, l'UA va normalement prendre ses propres décisions d'autorisation ; outrepasser les services d'écran au mandataire d'autorité pourrait avoir un sens, mais doit être examiné avec attention par les concepteurs de réseau, car la capacité de le faire dépend du type spécifique de service d'écran.

Cependant, les services de transmission, comme de transmission d'appel, NE DEVRAIT PAS être fournis aux demandes envoyées à un GRUU. L'intention du GRUU est de cibler une instance d'UA spécifique, et c'est incompatible avec les opérations de transmission.

Si la demande est une demande de mi-dialogue, un mandataire DEVRAIT seulement appliquer les services qui sont significatifs pour les demandes de mi-dialogue, généralement parlant. Cela exclut les fonctions d'écran et de transmission.

De plus, une demande envoyée à un GRUU NE DEVRAIT PAS être redirigée. Dans de nombreuses instances, un GRUU est utilisé par un UA afin d'aider à la traversée des NAT et pare-feu, et une redirection pourrait empêcher cela de fonctionner.

6.2 Enregistrement d'acheminement

Il y a deux exigences distinctes pour l'enregistrement d'acheminement -- dans le domaine d'origine et dans le domaine de terminaison. Ces exigences évitent des spirales inutiles, et éventuellement problématiques, de demandes.

Si :
- o un mandataire d'autorité générateur reçoit une demande de formation de dialogue,
- o ET le champ d'en-tête Contact contient un GRUU dans le domaine du mandataire,
- o ET ce GRUU est valide dans le domaine du mandataire,
- o ET ce GRUU est associé à l'AOR correspondant à l'identité authentifiée du demandeur (en supposant qu'une telle authentification a été effectuée),
- o ET la demande contient un champ d'en-tête Record-Route,

alors le mandataire d'autorité DOIT enregistrer le chemin. Si toutes ces conditions sont vraies, sauf que le GRUU est associé à une AOR qui ne correspond pas à l'identité authentifiée du demandeur, il est RECOMMANDÉ que le mandataire rejette la demande avec une réponse 403 (Interdit).

Si :
- o un mandataire d'autorité de terminaison reçoit une demande de formation de dialogue,
- o ET l'URI de demande contient un URI dans le service de localisation (un GRUU ou une AOR),
- o ET le contact choisi pour envoyer la demande a un identifiant d'instance et est lié à un GRUU,
- o ET l'enregistrement contient un URI de chemin,

alors le mandataire d'autorité DOIT enregistrer le chemin.

Si un mandataire est dans le domaine d'origine ou de terminaison mais n'est pas un mandataire d'autorité, le mandataire PEUT enregistrer le chemin.

Si un mandataire dans le domaine de terminaison exige que les demandes de mi-dialogue passent à travers lui pour une raison quelconque (traversée de pare-feu, comptabilité, etc.) le mandataire DOIT encore enregistrer le chemin, et NE DOIT PAS supposer qu'un UA va utiliser son GRUU dans le champ d'en-tête Contact de sa réponse (ce qui causerait le passage des demandes de mi-dialogue à travers le mandataire sans enregistrer le chemin).

Les mises en œuvre devraient noter que, si un UA utilise un GRUU dans son contact, et si un mandataire s'insère lui-même dans le champ d'en-tête Path d'un enregistrement, ce mandataire va recevoir les demandes de mi-dialogue sans considération de si il enregistre les chemins ou non. La seule distinction est quel URI le mandataire va voir dans le champ d'en-tête Route supérieur des demandes de mi-dialogue. Si le mandataire enregistre les chemins, il va voir cet URI. Si il ne le fait pas, il va voir l'URI de chemin qu'il a inséré.

7. Grammaire

La présente spécification définit deux nouveaux paramètres de champ d'en-tête Contact ("temp-gruu" et "pub-gruu") en étendant la grammaire pour "contact-params" comme défini dans la [RFC3261]. Elle définit aussi un nouveau paramètre d'URI SIP ("gr") en étendant la grammaire pour "uri-parameter" comme défini dans la [RFC3261]. L'ABNF [RFC5234] est le suivant :

```
contact-params =/ temp-gruu / pub-gruu
temp-gruu = "temp-gruu" EQUAL quoted-string
pub-gruu = "pub-gruu" EQUAL quoted-string
uri-parameter =/ gr-param
gr-param = "gr" ["=" pvalue]                    ; défini dans la RFC 3261
```

Les chaînes entre guillemets pour temp-gruu et pub-gruu DOIVENT contenir un URI SIP. Cependant, elles sont codées comme toutes les autres chaînes entre guillemets et peuvent donc contenir des échappements de paire entre guillemets quand elles sont représentées de cette façon.

8. Exigences

La présente spécification a été créée afin de satisfaire les exigences suivantes :

REQ 1 : Quand un UA invoque un GRUU, il doit faire que la demande soit acheminée à l'instance d'UA spécifique à laquelle le GRUU se réfère.

REQ 2 : Il doit être possible qu'un GRUU soit invoqué de partout dans l'Internet, et faire que la demande soit acheminée de façon appropriée. C'est-à-dire, un GRUU ne doit pas être restreint à un domaine d'adressage spécifique.

REQ 3 : Il doit être possible à un GRUU d'être construit sans exiger que le réseau mémorise de l'état supplémentaire.

REQ 4 : Il doit être possible à un UA d'obtenir plusieurs GRUU qui acheminent chacun à cette instance d'UA. Par exemple, ceci est nécessaire pour prendre en charge une conférence ad hoc où une instance d'UA a besoin d'un URI différent pour chaque conférence qu'il héberge. Note : cette exigence n'est pas satisfaite par la présente spécification, et est traitée dans une spécification séparée (actuellement, "Livraison d'URI de demande cible aux agents d'utilisateur" [URI]).

REQ 5 : Quand un UA reçoit une demande envoyée à un GRUU, il doit être possible à l'UA de savoir le GRUU qui a été utilisé pour invoquer la demande. Ceci est nécessaire par suite de la REQ 4. Note : cette exigence n'est pas satisfaite par la présente spécification, et est traitée dans une spécification séparée (actuellement, "Livraison d'URI de demande cible aux agents d'utilisateur" [URI]).

REQ 6 : Il doit être possible à un UA d'ajouter du contenu opaque à un GRUU. Ce contenu n'est pas interprété ni altéré par le réseau, et est utilisé seulement par l'instance d'UA à laquelle le GRUU se réfère. Cela fournit un type de fonction de mouchard de base, qui permet à un UA de construire un GRUU avec l'état incorporé. Note : cette exigence n'est pas satisfaite par la présente spécification, et est traitée dans une spécification séparée (actuellement, "Livraison d'URI de demande cible aux agents d'utilisateur" [URI]).

REQ 7 : Il doit être possible à un mandataire d'exécuter des services et caractéristiques au nom d'une instance d'UA représentée par un GRUU. Par exemple, si un utilisateur a des caractéristiques de blocage d'appel, un mandataire pourrait vouloir appliquer ces caractéristiques de blocage d'appel aux appels faits au GRUU, en plus des appels faits à l'AOR de l'utilisateur.

REQ 8 : Il doit être possible à un UA dans un dialogue d'informer son homologue de son GRUU, et à l'homologue de savoir que l'URI représente un GRUU. Ceci est nécessaire pour les applications de conférence et de réutilisation de dialogue des GRUU, où les URI sont transférés dans un dialogue.

REQ 9 : Quand on transfère un GRUU selon la REQ 8, il doit être possible à l'UA qui reçoit le GRUU d'être assuré de son intégrité et de son authenticité.

REQ 10 : Il doit être possible à un serveur qui est d'autorité pour un domaine de construire un GRUU qui achemine à une instance d'UA liée à une AOR dans ce domaine. En d'autres termes, le mandataire peut construire un GRUU, lui aussi. Ceci est nécessaire pour l'application de présence.

9. Exemple de flux d'appel

Le flux d'appels suivant, illustré à la Figure 2, montre un enregistrement de base et l'établissement d'appel, suivis par un abonnement dirigé sur le GRUU. Il montre ensuite une défaillance de l'appelé, suivie par un ré-enregistrement. Les conventions de la [RFC4475] sont utilisées pour décrire la représentation de longues lignes de message.

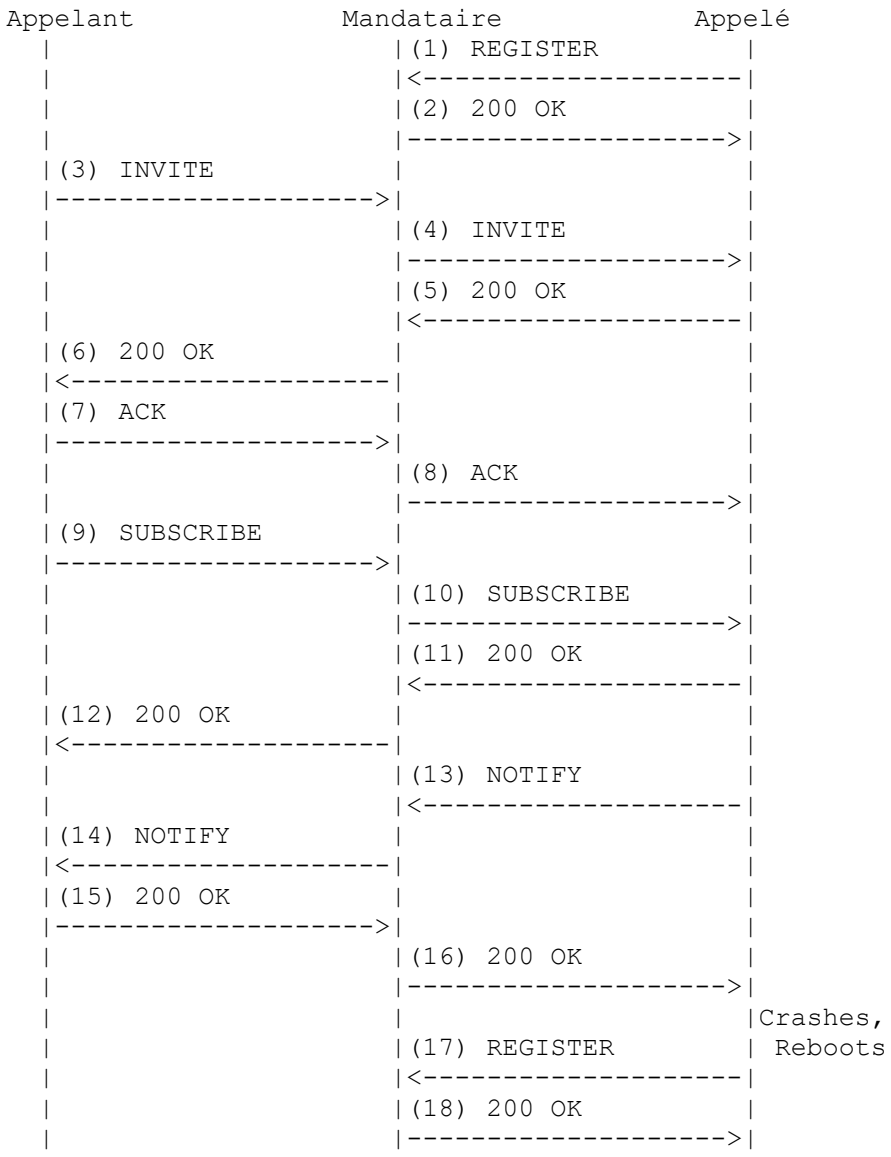

Figure 2

L'appelé prend en charge l'extension GRUU. À ce titre, son REGISTER (1) ressemble à :

```
REGISTER sip:exemple.com SIP/2.0
Via: SIP/2.0/UDP 192.0.2.1;branch=z9hG4bKnashds7
Max-Forwards: 70
From: Callee <sip:callee@exemple.com>;tag=a73kszlfl
Supported: gruu
To: Callee <sip:callee@exemple.com>
Call-ID: 1j9FpLxk3uxtm8tn@192.0.2.1
CSeq: 1 REGISTER
Contact: <sip:callee@192.0.2.1>
 ;+sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>"
Content-Length: 0
```

Le registraire alloue un GRUU temporaire et un GRUU public. La réponse REGISTER (message 2) ressemble à :

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.2.1;branch=z9hG4bKnashds7
From: Callee <sip:callee@exemple.com>;tag=a73kszlfl
To: Callee <sip:callee@exemple.com> ;tag=b88sn
Call-ID: 1j9FpLxk3uxtm8tn@192.0.2.1
CSeq: 1 REGISTER
<allOneLine>
Contact: <sip:callee@192.0.2.1>
```

```
;pub-gruu="sip:callee@exemple.com
;gr=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6"
;temp-gruu="sip:tgruu.7hs==jd7vnzga5w7fajsc7-ajd6fabz0f8g5@exemple.com;gr"
;+sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>"
;expires=3600
</allOneLine>
Content-Length: 0
```

Le champ d'en-tête Contact dans la réponse REGISTER contient le paramètre de champ d'en-tête Contact "pub-gruu" avec le GRUU public sip:callee@exemple.com;gr=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6, et le paramètre de champ d'en-tête "temp-gruu" avec le GRUU temporaire sip:tgruu.7hs==jd7vnzga5w7fajsc7-ajd6fabz0f8g5@exemple.com;gr. Tous deux sont des GRUU valides pour l'AOR et l'identifiant d'instance, et tous deux se traduisent en le contact sip:callee@192.0.2.1.

Le INVITE de l'appelant (message 3) est un SIP INVITE normal. Cependant, le 200 OK généré par l'appelé (message 5) contient maintenant un GRUU comme cible distante. L'UA a choisi d'utiliser son GRUU public.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP mandataire.exemple.com;branch=z9hG4bKnaa8
Via: SIP/2.0/UDP host.exemple.com;branch=z9hG4bK99a
From: Caller <sip:caller@exemple.com>;tag=n88ah
To: Callee <sip:callee@exemple.com> ;tag=a0z8
Call-ID: 1j9FpLxk3uxtma7@host.exemple.com
CSeq: 1 INVITE
Supported: gruu
Allow: INVITE, OPTIONS, CANCEL, BYE, ACK, SUBSCRIBE
Contact:<sip:callee@exemple.com;gr=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>
Content-Length: --
Content-Type: application/sdp
[Le SDP n'est pas montré]
```

Plus tard dans l'appel, l'appelant décide de s'abonner au paquetage d'événement du dialogue (défini dans la [RFC4235]) à cet UA spécifique. Pour ce faire, il génère une demande SUBSCRIBE (message 9) mais la dirige vers la cible distante, qui est un GRUU :

```
SUBSCRIBE sip:callee@exemple.com;gr=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6 SIP/2.0
Via: SIP/2.0/UDP host.exemple.com;branch=z9hG4bK9zz8
From: Caller <sip:caller@exemple.com>;tag=kkaz-
To: <sip:callee@exemple.com;gr=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>
Call-ID: faif9a@host.exemple.com
CSeq: 2 SUBSCRIBE
Supported: gruu
Event: dialogue
Allow: INVITE, OPTIONS, CANCEL, BYE, ACK, NOTIFY
Contact: <sip:caller@exemple.com;gr=hdg7777ad7aflzig8sf7>
Content-Length: 0
```

Dans cet exemple, l'appelant lui-même prend en charge l'extension GRUU et utilise son propre GRUU pour remplir sa cible distante.
Cette demande est acheminée au mandataire, qui procède à une recherche de localisation sur l'URI de demande. Elle est traduite en le contact pour cette instance, et ensuite mandatée à ce contact.

```
SUBSCRIBE sip:callee@192.0.2.1 SIP/2.0
Via: SIP/2.0/UDP mandataire.exemple.com;branch=z9hG4bK9555
Via: SIP/2.0/UDP host.exemple.com;branch=z9hG4bK9zz8
From: Caller <sip:caller@exemple.com>;tag=kkaz-
To: <sip:callee@exemple.com;gr=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>
Call-ID: faif9a@host.exemple.com
CSeq: 2 SUBSCRIBE
Supported: gruu
Event: dialogue
Allow: INVITE, OPTIONS, CANCEL, BYE, ACK, NOTIFY
Contact: <sip:caller@exemple.com;gr=hdg7777ad7aflzig8sf7>
Content-Length: 0
```

The SUBSCRIBE génère une réponse 200 (message 11) qui est suivie par un NOTIFY (messages 13 et 14) et sa réponse (messages 15 et 16). Un moment après la réception du message 16, la machine de l'appelé tombe en panne et récupère. Il obtient une nouvelle adresse IP, 192.0.2.2. Ignorant qu'il avait précédemment un enregistrement actif, il en crée un nouveau (message 17 ci-dessous). Noter que l'identifiant d'instance reste le même, car il persiste à travers les cycles de réamorçage :

```
REGISTER sip:exemple.com SIP/2.0
Via: SIP/2.0/UDP 192.0.2.2;branch=z9hG4bKnasbba
Max-Forwards: 70
From: Callee <sip:callee@exemple.com>;tag=ha8d777f0
Supported: gruu
To: Callee <sip:callee@exemple.com>
Call-ID: hf8asxzff8s7f@192.0.2.2
CSeq: 1 REGISTER
Contact: <sip:callee@192.0.2.2>;+sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>"
Content-Length: 0
```

Le registraire note qu'un contact différent, sip:callee@192.0.2.1, est déjà associé au même identifiant d'instance. Il enregistre aussi le nouveau et les retourne tous deux dans la réponse REGISTER. Tous deux ont le même GRUU public, mais le registraire a généré un second GRUU temporaire pour cette combinaison d' AOR et d'identifiant d'instance. Les deux contacts sont inclus dans la réponse REGISTER, et le GRUU temporaire pour chacun est le même -- le plus récemment créé pour l'identifiant d'instance et l'AOR. Le registraire génère alors la réponse suivante :

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.2.2;branch=z9hG4bKnasbba
From: Callee <sip:callee@exemple.com>;tag=ha8d777f0
To: Callee <sip:callee@exemple.com>;tag=99f8f7
Call-ID: hf8asxzff8s7f@192.0.2.2
CSeq: 1 REGISTER
<allOneLine>
Contact: <sip:callee@192.0.2.2>;pub-gruu="sip:callee@exemple.com;gr=urn:
uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6"
;temp-gruu="sip:tgruu.7hatz6cn-098shfyq193=ajfux8fyg7ajqqe7@exemple.com;gr"
;+sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>";expires=3600
</allOneLine>
<allOneLine>
Contact: <sip:callee@192.0.2.1>;pub-gruu="sip:callee@exemple.com;gr=urn:
uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6"
;temp-gruu="sip:tgruu.7hatz6cn-098shfyq193=ajfux8fyg7ajqqe7@exemple.com;gr"
;+sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>";expires=400
</allOneLine>
Content-Length: 0
```

L'UA n'a pas besoin de supprimer le contact enregistré périmé ; les règles de ciblage de demande du paragraphe 6.1 vont causer la livraison de la demande à la plus récente.

10. Considérations sur la sécurité

Les attaques dans les réseaux SIP qui utilisent des GRUU peuvent être divisées en attaques de l'extérieur (où un tiers essaye d'attaquer le système) et attaques de l'intérieur (où l'attaquant est un participant valide dans le système mais est malveillant). De plus, il y a des considérations de confidentialité sur l'utilisation des GRUU.

10.1 Attaques de l'extérieur

Il est important pour un UA d'être assuré de l'intégrité d'un GRUU donné dans une réponse REGISTER. Si le GRUU est altéré par un attaquant, le résultat pourrait être un déni de service (DoS) à l'UA. Par suite, il est RECOMMANDÉ qu'un UA utilise le schéma d'URI SIPS dans l'URI de demande quand il s'enregistre. Les mandataires et registraires DOIVENT prendre en charge l'URI SIPS et DOIVENT prendre en charge TLS. Cela ne représente pas de changement par rapport aux exigences de la [RFC3261].

L'exemple d'algorithme de construction de GRUU de l'Appendice A.1 ne tente pas de créer un GRUU qui cache l'AOR et l'identifiant d'instance associés au GRUU. En général, la détermination de l'AOR associée à un GRUU est considérée une

bonne propriété, car elle permet un suivi facile de la cible d'un appel particulier. Apprendre l'identifiant d'instance apporte peu à un attaquant. Pour s'enregistrer ou impacter autrement les enregistrements pour l'utilisateur, un attaquant aurait besoin d'obtenir les accréditifs de l'utilisateur. Connaître l'identifiant d'instance est insuffisant.

L'exemple d'algorithme de construction de GRUU de l'Appendice A.1 ne tente pas de créer un GRUU qui empêche les utilisateurs de deviner un GRUU sur la base de la connaissance de l'AOR et de l'identifiant d'instance. Un utilisateur qui est capable de faire cela va être capable de diriger une nouvelle demaande à une instance particulière. Cependant, la présente spécification recommande qu'un traitement de service (en particulier, les caractéristiques d'écran) soit donné aux demandes qui sont envoyées à un GRUU. Ce traitement va assurer que le GRUU ne fournit pas un accès dérobé aux attaquants pour contacter un utilisateur qui a essayé de bloquer l'attaquant.

10.2 Attaques de l'intérieur

En conséquence de la présente spécification, un UA va commencer à utiliser des GRUU dans les demandes de formation de dialogue et de rafraîchissement de cible et leurs réponses qu'il émet. Ces GRUU vont être passés à un autre UA (appelé le correspondant) qui les utilise alors dans les demandes qu'il émet.

Si un correspondant malveillant supprime le paramètre d'URI "gr", la demande va être acheminée au mandataire d'autorité. Si le GRUU était temporaire, la suppression du paramètre d'URI "gr" produit un URI qui n'est pas reconnu comme GRUU et n'est pas égal à une AOR. La demande va être rejetée. Si le GRUU était public, la suppression du paramètre d'URI "gr" aurait produit l'AOR. Donc, la demande est traitée comme un appel à l'AOR. Comme c'est un but désiré de permettre aux utilisateurs d'extraire l'AOR du GRUU, ce n'est pas une attaque, et l'appel va être traité normalement.

Un utilisateur malveillant dans le système pourrait essayer d'utiliser un GRUU pour lancer une attaque de DoS contre un autre UA SIP. Pour faire cela, il devrait attendre un appel de cet UA, et à partir de cet appel, observer son GRUU. Une fois le GRUU obtenu, l'UA lancerait une demande SIP à une entité, comme un serveur de présence, qui générerait de nombreuses demandes en retour à l'UA. Cependant, l'attaquant va utiliser le GRUU de la cible dans le champ d'en-tête Contact de cette demande SUBSCRIBE. Cela va causer la redirection du trafic vers la cible. Comme le GRUU est mondialement acheminable, ce trafic va plus probablement être livré à la cible que le trafic envoyé à son adresse IP. La présente spécification aide à atténuer cette attaque en exigeant que les mandataires valident que le GRUU dans le Contact d'une demande correspond à l'identité authentifiée de l'envoyeur de la demande. Cette vérification exige l'utilisation d'un mandataire sortant. SIP n'exige pas de mandataires sortants, et cela laisse une zone potentielle de vulnérabilité. Cependant, en pratique, presque tous les déploiements de SIP utilisent un mandataire sortant, et donc cette vulnérabilité a peu de chances de poser un problème.

10.3 Considérations de confidentialité

La [RFC3323] définit des mécanismes pour la confidentialité. Elle distingue la confidentialité fournie entre les réseaux et la confidentialité fournie par l'utilisateur. Dans la première, l'utilisateur demande des services de confidentialité au réseau en incluant un champ d'en-tête Privacy dans la demande. Dans la seconde, l'UA suit un ensemble de base de lignes directrices pour la construction de sa demande, de sorte qu'un certain niveau de confidentialité est assuré.

Les lignes directrices du paragraphe 4.1 de la [RFC3323] pour la confidentialité fournie par l'utilisateur demandent qu'un UA construise son champ d'en-tête Contact avec un URI qui omet la partie utilisateur, et utilise l'adresse IP ou le nom d'hôte de l'UA. Ces recommandations sont en conflit avec les règles définies dans la présente spécification, qui exige l'usage d'un GRUU dans le champ d'en-tête Contact.

Cependant, les GRUU temporaires fournis par le registraire peuvent être utilisés à la place du format d'URI de contact décrit dans la [RFC3323]. Un agent d'utilisateur va collecter le GRUU temporaire retourné dans chaque réponse REGISTER, et garder un petit nombre d'entre eux en antémémoire. Quand il fait ou reçoit un appel, un GRUU temporaire est utilisé pour remplir le champ d'en-tête Contact.

Un UA peut choisir d'utiliser le même GRUU temporaire dans chaque appel, ou il peut utiliser un GRUU temporaire différent dans chaque appel. Le choix dépend du niveau de confidentialité désiré :

- Un UA qui utilise le même GRUU temporaire pour chaque appel va permettre à un correspondant, sur la seule base de l'examen du champ d'en-tête Contact, de corréler les appels comme venant du même UA. Cela est aussi vrai pour les procédures de confidentialité fondées sur l'utilisateur de la [RFC3323], car l'adresse IP ou le nom d'hôte dans l'URI de contact fournissent une corrélation similaire.

- Un UA qui utilise un GRUU temporaire différent pour chaque appel ne va pas permettre à un correspondant, sur la seule base de l'examen du champ d'en-tête Contact, de corréler les appels comme venant du même UA.

- Dans les deux cas, sauf pour la confidentialité fournie par le réseau, les informations d'adresse et accès IP dans le protocole de description de session (SDP) (défini dans la [RFC4566]) vont permettre à un correspondant de corréler les appels comme venant du même UA.

- Dans les deux cas, si un utilisateur fait un appel, le correspondant va être capable de rappeler en dirigeant les demandes vers le GRUU dans le champ d'en-tête Contact. De même, les caractéristiques de transfert et de collecte des chiffres par les serveurs d'application réseau (voir la [RFC4730]) qui dépendent d'un contact avec la propriété de GRUU, vont aussi être possibles. Ces sortes de demandes entrantes vont être possibles jusqu'à ce que l'enregistrement pour cet UA expire. Un UA qui souhaite invalider son précédent GRUU temporaire afin de limiter l'accessibilité PEUT le faire en générant un rafraîchissement de REGISTER avec un identifiant d'appel qui diffère de ceux utilisés précédemment. Un UA NE DEVRAIT PAS faire expirer de force son enregistrement et ensuite se réenregistrer afin d'invalider un GRUU temporaire ; cela résulte en une brève période d'inaccessibilité et va souvent produire une charge excessive sur le réseau. Rafraîchir avec un nouvel identifiant d'appel est plus efficace et est vu comme la technique pour un contrôle grossier de la validité des GRUU temporaires. Un UA qui souhaite n'être pas dérangé par un rappel spécifique va devoir mettre en œuvre des procédures de traitement d'appel manuelles ou automatisées pour le rejeter. La présente spécification ne donne pas à l'UA la capacité d'invalider manuellement les GRUU temporaires individuels. Si un UA insiste pour ne recevoir aucune de ces demandes entrantes (incluant celles générées par les applications du réseau, comme celles utilisées pour collecter les chiffres) l'UA peut placer un non GRUU dans le champ d'en-tête Contact. Cependant, ceci n'est PAS RECOMMANDÉ. L'usage d'un GRUU couplé avec des caractéristiques de rejet d'appel automatique est bien supérieur.

- Tant qu'un GRUU temporaire est utilisé pour remplir le champ d'en-tête Contact, un correspondant ne va pas être capable de certifier d'information sur l'AOR ou l'identifiant d'instance de l'UA en inspectant le champ d'en-tête Contact. Cependant, sauf dans un service de confidentialité fourni par le réseau, l'adresse IP dans le SDP peut être utilisée pour déterminer les informations sur l'UA, comme sa localisation géographique et son FAI.

- Dans tous les cas, sans considération de si l'UA utilise un GRUU temporaire ou public dans le Contact, ni de si il utilise du tout de GRUU, et sans considération de si il invoque un service de confidentialité fourni par le réseau, un correspondant va être capable de déterminer le fournisseur de service SIP de l'UA.

11. Considérations relatives à l'IANA

La présente spécification définit deux nouveaux paramètres de champ d'en-tête Contact, un paramètre d'URI SIP, et une étiquette d'option SIP.

11.1 Paramètres de champ d'en-tête

La présente spécification définit deux nouveaux paramètres de champ d'en-tête, dans le registre créé par la [RFC3968].[2] Les informations requises sont les suivantes :

Champ d'en-tête dans lequel le paramètre peut apparaître : Contact
Nom du paramètre : pub-gruu
Valeurs prédéfinies : aucune
RFC de référence : RFC 5627

Champ d'en-tête dans lequel le paramètre peut apparaître : Contact
Nom du paramètre : temp-gruu
Valeurs prédéfinies : aucune
RFC de référence : RFC 5627

11.2 Paramètre d'URI

La présente spécification définit un nouveau paramètre d'URI SIP, selon le registre créé par la [RFC3969].

Nom du paramètre : gr
Valeurs prédéfinies : aucune
RFC de référence : RFC 5627

11.3 Étiquette d'option SIP

La présente spécification enregistre une nouvelle étiquette d'option SIP, selon les lignes directrices du paragraphe 27.1 de la

[RFC3261].

Nom : gruu

Description : cette étiquette d'option est utilisée pour identifier l'extension d'URI d'agent d'utilisateur mondialement acheminable (GRUU, *Globally Routable User Agent URI*). Quand elle est utilisée dans un en-tête Supported, elle indique qu'un agent d'utilisateur comprend l'extension. Quand elle est utilisée dans un champ d'en-tête Require d'une demande REGISTER, elle indique que le registraire n'est pas supposé traiter l'enregistrement sauf si il prend en charge l'extension GRUU.

12. Remerciements

L'auteur tient à remercier Eric Rescorla, Robert Sparks, Rohan Mahy, Paul Kyzivat, Alan Johnston, Ya-Ching Tan, Dale Worley, Jeroen van Bemmel, Vijay Gurbani, Andrew Allen, Alan Hawrylyshen, Francois Audet, Fredrik Thulin, Dean Willis, David Hancock, Keith Drage, et Cullen Jennings de leurs commentaires et contributions au présent travail.
Eric Rescorla a fourni le texte de l'introduction l'algorithme de construction de GRUU dans l'appendice.

13. Références

13.1 Références normatives

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

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

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

[RFC3265] A.B. Roach, "Notification d'événement spécifique du protocole d'initialisation de session (SIP)", juin 2002. (*MàJ par* RFC6446) (*Remplacée par la* RFC6665)

[RFC3327] D. Willis, B. Hoeneisen, "Champ d'en-tête d'extension du protocole d'initialisation de session (SIP) pour enregistrer des contacts non adjacents", décembre 2002. *(P.S.)*

[RFC3515] R. Sparks, "Méthode Refer du protocole d'initialisation de session (SIP)", avril 2003. *(MàJ par* RFC8217)

[RFC3840] J. Rosenberg, H. Schulzrinne et P. Kyzivat, "Indication des capacités d'agent d'utilisateur dans le protocole d'initialisation de session (SIP)", août 2004

[RFC3841] J. Rosenberg, H. Schulzrinne, P. Kyzivat, "Préférences de l'appelant pour le protocole d'initialisation de session (SIP)", août 2004. *(P.S.)*

[RFC3966] H. Schulzrinne, "L'URI tel pour les numéros de téléphone", décembre 2004. (*MàJ par* RFC5341) *(P.S.)*

[RFC3968] G. Camarillo, "Registre des paramètres de champ d'en-tête de l'IANA pour le protocole d'initialisation de session (SIP)", décembre 2004. (BCP0098)

[RFC3969] G. Camarillo, "Registre des paramètres d'identifiant de ressource uniforme (URI) de l'IANA pour le protocole d'initialisation de session (SIP)", décembre 2004. (BCP0099)

[RFC4566] M. Handley, V. Jacobson et C. Perkins, "SDP : Protocole de description de session", juillet 2006. *(P.S. ; remplacée par RFC8866)*

[RFC5234] D. Crocker, éd., P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", janvier 2008. (STD0068)

[RFC5626] C. Jennings, R. Mahy, F. Audet, éd., "Gestion des connexions initiées par le client dans le protocole d'initialisation de session (SIP)", octobre 2009. *(MàJ* RFC3261, RFC3327) *(P. S.)*

13.2 Références pour information

[RFC3323] J. Peterson, "Mécanisme de confidentialité pour le protocole d'initialisation de session (SIP)", novembre 2002.

[RFC3361] H. Schulzrinne, "Option du protocole de configuration dynamique d'hôte (DHCP-pour-IPv4) pour les serveurs du protocole d'initialisation de session (SIP)", août 2002. *(P.S.)*

[RFC3486] G. Camarillo, "Compression du protocole d'initialisation de session (SIP)", février 2003. (*MàJ par* RFC5049) *(P.S.)*

[RFC3608] D. Willis, B. Hoeneisen, "Champ d'en-tête d'extension du protocole d'initialisation de session (SIP) pour la découverte de chemin de service durant l'enregistrement", octobre 2003. *(P.S.)*

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

[RFC3911] R. Mahy, D. Petrie, "En-tête "Join" du protocole d'initialisation de session (SIP)", octobre 2004. *(P.S.)*

[RFC3891] R. Mahy, B. Biggs, R. Dean, "En-tête "Replaces" du protocole d'initialisation de session (SIP)", septembre 2004. *(P.S.)*

[RFC4235] J. Rosenberg et autres, "Paquetage d'événement de dialogue initié par INVITE pour le protocole d'initialisation de session (SIP)", novembre 2005. *(P.S.)*

[RFC4240] E. Burger et autres, "Services de base de support réseau avec SIP", décembre 2005. *(Information)*

[RFC4458] C. Jennings et autres, "URI du protocole d'initialisation de session (SIP) pour des applications comme la messagerie vocale et la réponse vocale interactive (IVR)", avril 2006. *(Information ; MàJ par* RFC8119)

[RFC4475] R. Sparks et autres, "Messages d'essais de résistance du protocole d'initialisation de session (SIP)", mai 2006. *(Info.)*

[RFC4730] E. Burger, M. Dolly, "Paquetage d'événement du protocole d'initialisation de session (SIP) pour stimulus par langage de balisage à pression de touche (KPML)", novembre 2006. *(P.S.)*

[RFC5589] R. Sparks, A. Johnston, éd., D. Petrie, "Contrôle du transfert d'appel dans le protocole d'initialisation de session (SIP)", juin 2009. (BCP0149)

[RFC5628] P. Kyzivat, "Extension de paquetage d'événement d'enregistrement pour les URI d'agent d'utilisateur mondialement acheminables (GRUU) du protocole d'initialisation de session (SIP)", octobre 2009. *(P. S.)*

[URI] Rosenberg, J., van Elburg, J., Holmberg, C., Audet, F., and S. Schubert, Ed., "Delivery Request-URI Targets to User Agents", Travail en cours, juin 2009.

Appendice A. Exemples d'algorithmes de construction de GRUU

Le mécanisme pour construire un GRUU n'est pas l'objet d'une spécification. Cet appendice donne un exemple qui peut être utilisé par un registraire pour construire un GRUU public et un GRUU temporaire. Bien sûr, d'autres sont permis, pour autant qu'il satisfont les contraintes définies pour un GRUU.

A.1 GRUU Public

L'approche de base pour construire un GRUU public est de prendre l'AOR et de placer la valeur réelle de l'identifiant d'instance dans le contenu du paramètre d'URI "gr".

A.2. GRUU temporaire

La présente spécification exige d'un registraire qu'il crée un nouveau GRUU temporaire sur chaque rafraîchissement d'enregistrement. Si un enregistrement a une très longue durée de vie, cela peut rapidement résulter en centaines ou même

milliers de GRUU temporaires créés et alloués à un UA. Par conséquent, il est important d'avoir un algorithme pour construire des GRUU temporaires qui n'exigent pas de mémorisation supplémentaire dont la taille croît avec le nombre de GRUU temporaires. L'algorithme suivant satisfait ce but.

Le registraire tient un compteur, I. Ce compteur de 48 bits est initialisé à zéro. Le compteur est mémorisé de façon persistante, en utilisant une base de données arrière ou autre technique similaire. Quand le registraire crée le premier GRUU temporaire pour une AOR particulière et un identifiant d'instance, le registraire note la valeur courante du compteur, I_i, et incrémente le compteur dans la base de données. Le registraire transpose alors I_i en l'AOR et identifiant d'instance en utilisant la base de données, une transposition de hachage persistante ou technologie similaire. Si l'enregistrement expire de telle façon qu'il n'y a plus aucun contact avec cet identifiant d'instance particulier lié au GRUU, le registraire supprime la transposition. De même, si les GRUU temporaires sont invalidés du fait d'un changement de l'identifiant d'appel, le registraire supprime la transposition courante de I_i à l'AOR et à l'identifiant d'instance, note la valeur courante du compteur I_j, et mémorise une transposition de I_j en l'AOR et l'identifiant d'instance. Sur la base de ces règles, la transposition de hachage va contenir une seule transposition pour chaque AOR et identifiant d'instance pour lesquel il y a un enregistrement actuellement valide.

L'usage d'un compteur dans un espace de 48 bits avec allocation séquentielle permet une représentation compacte de la clé de transposition de hachage, ce qui est important pour générer des GRUU de taille raisonnable. Le compteur commence à zéro quand le système est initialisé. La mémorisation persistante et fiable du compteur est exigée pour éviter un mauvais acheminement d'un GRUU à la mauvaise AOR et identifiant d'instance. De même, la mémorisation persistante de la transposition de hachage est exigée, même si le mandataire et le registraire redémarrent. Si la transposition de hachage est réinitialisée, tous les GRUU temporaires précédents deviennent invalides. Cela pourrait causer l'échec de dialogues en cours, ou l'échec de futures demandes vers un GRUU temporaire alors qu'elles ne le devraient normalement pas. La même transposition de hachage doit être accessible à tous les mandataires et registraires qui peuvent transmettre des demandes pour une AOR et identifiant d'instance particuliers.

Le registraire tient une paire de clés locales symétriques K_e et K_a. Elles sont régénérées chaque fois que le compteur est réinitialisé. Quand le compteur revient à zéro ou est réinitialisé, le registraire se souvient des vieilles valeurs de K_e et K_a pendant un certain temps. Comme la transposition de hachage elle-même, ces clés doivent être partagées à travers tous les mandataires et registraires qui peuvent servir les demandes d'une AOR et d'un identifiant d'instance particuliers.

Pour générer un nouveau GRUU temporaire, le registraire génère une valeur distinctive aléatoire de 80 bits D. Il calcule alors :

```
M = D || I_i
E = AES-ECB-Encrypt(K_e, M)
A = HMAC-SHA256-80(K_a, E)
Temp-Gruu-userpart = "tgruu." || base64(E) || base64(A)
```

où || note l'enchaînement, et AES-ECB-Encrypt représente le chiffrement AES en mode dictionnaire. M va faire 128 bits, produisant une valeur de E qui fait 128 bits et A qui fait 80 bits. Cela produit une partie utilisateur de 42 caractères.

Quand un mandataire reçoit une demande dont la partie utilisateur commence par "tgruu.", il extrait la portion restante, et la partage en 22 caractères (E') et les 14 caractères restants (A'). Il calcule alors A et E en effectuant un décodage base64 de A' et E' respectivement. Ensuite, il calcule :

```
Ac = HMAC-SHA256-80(K_a, E)
```

Si le compteur est revenu à zéro ou s'est réinitialisé, ce calcul est effectué avec le K_a actuel et le précédent. Si la ou les valeurs Ac qui sont calculées ne correspondent pas à la valeur de A extraite du GRUU, le GRUU est rejeté comme invalide. Ensuite, le mandataire calcule :

```
M = AES-ECB-Decrypt(K_e, E)
```

Si le compteur est revenu à zéro, ce calcul est fait en utilisant la valeur de K_e qui va avec la valeur de K_a, qui a produit un Ac valide dans la validation HMAC précédente. Les 80 bits de tête (le discriminant D) sont éliminés, laissant un indice I_i dans la transposition de hachage. Cet indice est recherché. Si il existe, le mandataire a maintenant l'AOR et l'identifiant d'instance correspondants à ce GRUU temporaire. Si il n'y a rien dans la transposition de hachage pour la clé I_i, le GRUU n'est plus valide et la demande est rejetée.

L'usage d'un compteur de 48 bits permet au registraire d'avoir jusqu'à un million d'AOR, avec 10 instances par AOR, et des cycles de 10 000 changements d'identifiants d'appel pour chaque instance pour la durée d'un seul enregistrement. Ces nombres reflètent une moyenne ; le système fonctionne bien si une AOR particulière a plus de 10 instances ou si une instance particulière passe par plus de 10 000 identifiants d'appel dans son enregistrement, pour autant que la moyenne

satisfasse ces contraintes.

Appendice B. Considérations de conception de réseau

La spécification GRUU fonctionne correctement sur la base de la logique mise en œuvre aux agents d'utilisateur et dans les mandataires d'autorité des deux côtés d'un appel. Par conséquent, il est possible de construire des déploiements de réseau dans lesquels les GRUU ne vont pas fonctionner correctement.

Une hypothèse importante faite par le mécanisme de GRUU est que, si une demande passe à travers des mandataires dans le domaine d'origine avant de visiter le domaine de terminaison, un de ces mandataires va être le mandataire d'autorité pour le client d'agent d'utilisateur (UAC, *User Agent Client*). Les administrateurs de réseaux SIP vont devoir s'assurer que cette propriété est conservée. Il y a plusieurs moyens de le faire :

1. Si les agents d'utilisateur prennent en charge le mécanisme de chemin de service [RFC3608], le registraire peut le mettre en œuvre et retourner un chemin de service qui pointe sur le mandataire d'autorité. Cela va causer le passage des demandes générées par l'agent d'utilisateur à travers le mandataire d'autorité.

2. Les agents d'utilisateur peuvent être configurés à ne jamais utiliser un mandataire sortant, et à envoyer les demandes directement au domaine de la partie terminale. Cette configuration n'est pas pratique dans de nombreux cas d'usage, mais est une solution à cette exigence.

3. Les agents d'utilisateur peuvent être configurés avec un mandataire sortant dans le même domaine que le mandataire d'autorité, et ce mandataire sortant transmet par défaut les demandes au mandataire d'autorité. Cela fonctionne très bien dans les cas où les clients ne sont pas en itinérance ; dans ces cas, le mandataire sortant dans un réseau visité peut être découvert dynamiquement par DHCP [RFC3361].

4. Dans les cas où le client découvre un mandataire sortant local via un mécanisme comme DHCP, et ne met pas en œuvre le mécanisme de chemin de service, l'UA peut être configuré à ajouter automatiquement un champ d'en-tête Route supplémentaire après le mandataire sortant, qui pointe sur un mandataire dans le réseau de rattachement. Ceci a le même effet net que le mécanisme de chemin de service, mais est réalisé par une configuration statique.

Adresse de l'auteur

Jonathan Rosenberg
Cisco Systems
Edison, NJ
USA

mél : jdrosen@cisco.com
URI : http://www.jdrosen.net