Groupe de travail Réseau
Request for Comments : 4916
RFC mise à jour : 3261
Catégorie : En cours de normalisation

J. Elwell
Siemens Enterprise Communications Limited
juin 2007
Traduction Claude Brière de L'Isle

Identité connectée dans le protocole d'initialisation de session (SIP)

Statut du présent mémoire

Le présent document spécifie un protocole de normalisation Internet pour la communauté Internet, et appelle à discussion et suggestions en vue de son amélioration. Prière de se reporter à l'édition en cours des "Internet Official Protocol Standards" (normes officielles de protocole de l'Internet) (STD 1) pour connaître l'état de la normalisation et le statut du présent protocole. La distribution du présent mémo n'est pas soumise à restrictions.

Résumé

Le présent document donne à un agent d'utilisateur (UA) du protocole d'initialisation de session (SIP, *Session Initiation Protocol*) qui reçoit une demande à formation de dialogue le moyen de fournir son identité à l'UA homologue grâce à une demande dans la direction inverse, et que cette identité soit signée par un service d'authentification. À cause du reciblage de la demande à formation de dialogue (qui change la valeur de l'URI de demande) l'UA qui la reçoit (le serveur d'agent d'utilisateur, UAS : *User Agent Server*) peut avoir une identité différente de celle du champ d'en-tête To. Le même mécanisme peut être utilisé pour indiquer un changement d'identité durant un dialogue, par exemple, à cause d'une action dans le réseau téléphonique public commuté (RTPC) derrière une passerelle. Le présent document met à jour de façon normative la RFC3261 (SIP).

Table des matières

1 Introduction

Le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) (RFC 3261 [1]) initialise des sessions mais fournit aussi des informations sur les identités des parties au deux extrémités d'une session. Les utilisateurs ont besoin de ces informations pour les aider à déterminer comment traiter les communications initialisées par SIP. L'identité de la partie qui répond à un appel peut différer de celle de la partie de l'appel initial pour diverses raisons telles qu'un renvoi d'appel, de la distribution des appels et de la prise d'appel. De plus, une fois qu'il a été répondu à un appel, une partie peut être remplacée par une partie différente avec une identité différente pour des raisons telles qu'un transfert d'appel, une mise en garde d'appel et sa reprise, etc. Bien que dans certains cas il puisse y avoir des raisons pour ne pas divulguer ces identités, il est souhaitable d'avoir un mécanisme qui fournisse ces informations.

Le présent document étend l'utilisation du champ d'en-tête From pour lui permettre de convoyer ce qui est couramment appelé les informations de "l'identité connectée" (l'identité de l'usager connecté) dans l'une et l'autre direction dans le contexte d'un dialogue initialisé par un INVITE existant. Il peut être utilisé pour convoyer :

- o l'identité de l'appelé à un appelant à l'appel duquel il est répondu ;
- o l'identité d'un appelé potentiel avant la réponse ; ou
- o l'identité d'un usager qui remplace l'appelant ou l'appelé à la suite d'un réarrangement d'appel tel qu'un transfert d'appel effectué au sein du RTPC ou au sein d'un agent d'utilisateur de boucle locale (B2BUA, *back-to-back user agent*) utilisant des techniques de commande d'appel de tierce partie.

Noter que l'utilisation des techniques SIP standard de transfert d'appel, qui impliquent la méthode REFER, conduisent à l'établissement d'un nouveau dialogue et donc appliquent un mécanisme normal pour l'identité de l'appelant et de l'appelé.

La fourniture de l'identité de la personne qui répond dans une réponse (communément appelée "identité de réponse") sort du domaine d'application du présent document.

Noter que même si l'identité devait être convoyée d'une manière ou d'une autre dans une réponse, il y aurait en général des difficultés à authentifier l'UAS. Fournir l'identité dans une demande séparée permet d'utiliser les techniques normales d'authentification.

2 Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la RFC2119 [2].

La présente spécification définit les termes supplémentaires suivants :

appelant : utilisateur de l'UA qui produit une demande INVITE pour initier un appel.

identité d'appelant : l'identité (adresse d'enregistrement) d'un appelant.

appelé : l'utilisateur de l'UA qui répond à un appel en produisant une réponse 2xx à une demande INVITE.

identité d'appelé : l'identité (adresse d'enregistrement) d'un appelé.

appelé potentiel : l'utilisateur de tout UA ciblé par une demande INVITE résultant en la formation d'un dialogue précoce, mais à cause du fourchement parallèle ou en série de la demande, pas nécessairement l'usager qui répond à l'appel.

usager connecté : tout usager impliqué dans un appel établi, incluant l'appelant, l'appelé ou tout usager qui remplace l'appelant ou l'appelé suite à un réarrangement d'appel tel qu'un transfert d'appel.

identité connectée : l'identité (adresse d'enregistrement) d'un usager connecté.

3 Vue générale de la solution

Une demande de mi-dialogue est utilisée pour fournir l'identité connectée. Le client d'agent d'utilisateur UAC, *User Agent Client*) pour cette demande insère son identité dans le champ d'en-tête From de la demande. Pour fournir l'authentification, le champ d'en-tête Identity (RFC4474 [3]) est inséré par un service d'authentification convenable sur le chemin de la demande de mi-dialogue. Sauf s'il est fourni à l'UAC, le service d'authentification est supposé être chez un mandataire qui

enregistre les chemins et est capable d'authentifier l'UAC.

Une demande dans la direction opposée à la demande INVITE avant ou au moment où il est répondu à l'appel peut indiquer respectivement l'identité de l'appelé potentiel ou de l'appelé. Une demande dans la même direction que la demande INVITE avant la réponse peut indiquer un changement d'appelant. Une demande dans l'une ou l'autre direction après la réponse peut indiquer un changement de l'usager connecté. Dans tous les cas, un dialogue (précoce ou confirmé) doit être établi avant qu'une telle demande puisse être envoyée.

Cette solution utilise la méthode UPDATE (RFC3311 [4]) pour la demande, ou dans certaines circonstances la méthode re-INVITE. Pour envoyer l'identité de l'appelé, l'UAS pour la demande INVITE envoie la demande UPDATE après l'envoi de la réponse 2xx à la demande INVITE et après avoir reçu une demande ACK. Pour envoyer l'identité de l'appelé potentiel, la RFC3262 [5] est supposée prise en charge. Dans ce cas, l'UAS pour la demande INVITE envoie la demande UPDATE après avoir reçu et répondu à une demande PRACK (ce qui arrive après l'envoi d'une réponse 1xx fiable à la demande INVITE). La demande UPDATE pourrait être utilisée aussi pour d'autres objets, par exemple, durant un dialogue précoce pour envoyer l'identité de l'appelé potentiel en même temps qu'une offre de protocole de description de session (SDP) pour des supports précoces. Pour indiquer un changement d'identité connectée durant un appel établi, la méthode UPDATE ou la méthode re-INVITE peuvent être utilisées. La méthode re-INVITE serait utilisée si nécessaire pour d'autres objets (par exemple, lorsque un B2BUA effectue un transfert en utilisant les techniques de commande d'appel par un tiers 3PCC, *Third Party Call Control*) il doit produire une demande re-INVITE sans offre SDP pour solliciter une offre SDP de la part de l'UA).

Cette solution implique de changer l'URI (mais pas les étiquettes) dans les champs d'en-tête To et From des demandes de mi-dialogue et leurs réponses, par rapport aux valeurs correspondantes dans la demande et la réponse de formation du dialogue. Changer les URI de champ d'en-tête To et From était envisagé au paragraphe 12.2.1.1 de la RFC3261 [1], qui dit :
"L'utilisation de l'URI provenant des champs To et From dans la demande originelle au sein des demandes ultérieures est faite pour la compatibilité amont avec la RFC2543, qui utilisait l'URI pour l'identification du dialogue. Dans la présente spécification, seules les étiquettes sont utilisées pour l'identification du dialogue. On s'attend à ce que l'obligation de refléter les URI d'origine de To et From dans les demandes à mi-dialogue soit déconseillé dans une révision future de la présente spécification."

Le présent document déconseille donc la répétition obligatoire des URI To et From originaux dans les demandes de mi-dialogue et leurs réponses, ce qui constitue un changement à la RFC3261 [1]. Le présent document ne prend aucune disposition pour les mandataires qui ne sont pas à même de tolérer un changement d'URI, car le changement d'URI a été attendu depuis longtemps. Pour satisfaire les besoins de tous les UA qui ne sont pas capables de tolérer un changement d'URI, une nouvelle étiquette d'option "from-change" est introduite pour fournir une indication positive de prise en charge dans le champ d'en-tête Supported. En envoyant une demande avec un changement de l'URI du champ d'en-tête From uniquement aux cibles qui ont indiqué la prise en charge de cette option, il n'est pas besoin d'envoyer cette étiquette d'option dans un champ d'en-tête Require.

En plus de la permission de changer l'URI du champ d'en-tête From durant un dialogue pour refléter l'identité connectée, le présent document exige aussi qu'un UA qui a reçu une identité connectée dans l'URI du champ d'en-tête From d'une demande de mi-dialogue utilise cet URI dans le champ d'en-tête To de toute demande de mi-dialogue ultérieure envoyée par cet UA.

En l'absence d'un service d'authentification convenable sur le chemin de la demande de mi-dialogue, l'UAS va recevoir une identité connectée non authentifiée (c'est-à-dire, sans un champ d'en-tête Identity correspondant). Les implications en sont exposées à la Section 7

4 Comportement

4.1 Comportement d'un UA qui produit une demande INVITE en dehors du contexte d'un dialogue existant

Lors de la production d'une demande INVITE, un UA conforme à la présente spécification DOIT inclure l'étiquette d'option "from-change" dans le champ d'en-tête Supported.

Noter que l'envoi de l'étiquette d'option "from-change" ne garantit pas que l'identité connectée sera reçue dans les demandes suivantes.

4.2 Comportement d'un UA qui reçoit une demande INVITE en dehors du contexte d'un dialogue existant

Après avoir reçu une demande INVITE, un UA conforme à la présente spécification DOIT inclure l'étiquette d'option "from-change" dans le champ d'en-tête Supported de toute réponse formatrice de dialogue.

Noter que l'envoi de l'étiquette d'option "from-change" ne garantit pas que l'identité connectée sera reçue dans le cas d'un changement d'appelant.

Après la formation d'un dialogue précoce, si l'étiquette d'option "from-change" a été reçue dans un champ d'en-tête Supported, l'UA PEUT produire une demande UPDATE (RFC3311 [4]) sur le même dialogue, sous réserve d'avoir envoyé une réponse provisoire fiable à la demande INVITE et d'avoir reçu et répondu à une demande PRACK. Après la formation d'un dialogue complet (après l'envoi d'une réponse finale 2xx à la demande INVITE), si l'étiquette d'option "from-change" a été reçue dans un champ d'en-tête Supported et si une demande UPDATE n'a pas été déjà envoyée dans le dialogue précoce, l'UA DOIT produire une demande UPDATE sur le même dialogue. Dans les deux cas, la demande UPDATE DOIT contenir l'identité de l'appelé (ou de l'appelé potentiel) dans l'URI du champ d'en-tête From (ou une identité anonyme si l'anonymat est exigé).

Noter que même si l'URI ne diffère pas de l'URI du champ d'en-tête To de la demande INVITE, l'envoi d'une nouvelle demande permet au service d'authentification de certifier l'authentification de cette identité et de confirmer à l'UA homologue que l'identité connectée est la même que celle de l'URI du champ d'en-tête To de la demande INVITE.

4.3 Comportement d'un UA dont l'identité change durant un dialogue établi à l'initiative de INVITE

Si l'étiquette d'option "from-change" a été reçue dans un champ d'en-tête Supported durant un dialogue initialisé par INVITE et si l'identité associée à l'UA change (par exemple, à la suite d'un transfert) par rapport à la dernière identité indiquée dans le champ d'en-tête From d'une demande envoyée par cet UA, l'UA DOIT produire une demande sur le même dialogue contenant la nouvelle identité dans l'URI du champ d'en-tête From (ou une identité anonyme si l'anonymat est exigé). Pour ce faire, l'UA DOIT utiliser la méthode UPDATE sauf si pour d'autres raisons la méthode re-INVITE est utilisée en même temps.

4.4 Comportement général d'UA

4.4.1 Envoi d'une demande à mi-dialogue

Lors de l'envoi d'une demande à mi-dialogue, un UA DOIT observer les exigences de la RFC4474 [3] en remplissant l'URI du champ d'en-tête From, et y inclure des dispositions pour réaliser l'anonymat.

Cela permettra à un service d'authentification sur le chemin de la demande de mi-dialogue d'insérer un champ d'en-tête Identity.

Lors de l'envoi d'une demande de mi-dialogue, un UA DOIT remplir l'URI de champ d'en-tête To avec la valeur actuelle de l'URI distant pour ce dialogue, et ceci est soumis à mise à jour conformément aux règles du paragraphe 4.4.2 du présent document plutôt que d'être fixé au commencement du dialogue comme établi dans la RFC3261 [1].

Après l'envoi d'une demande avec un URI de champ d'en-tête From révisé (c'est-à-dire, révisé par rapport à l'URI envoyé dans le champ d'en-tête From de la demande précédente de ce dialogue ou dans le champ d'en-tête To de la demande INVITE de formation de dialogue reçue si aucune demande n'a été envoyée) l'UA DOIT envoyer le même URI dans le champ d'en-tête From de toutes les demandes à venir sur le même dialogue, à moins que l'identité ne change à nouveau. Aussi, l'UA DOIT être prêt à recevoir l'URI révisé dans le champ d'en-tête To des demandes de mi-dialogue suivantes et DOIT aussi continuer d'être prêt à recevoir le vieil URI au moins jusqu'à ce qu'une demande contenant l'URI révisé dans le champ d'en-tête To ait été reçue.

La demande de mi-dialogue peut être rejetée conformément à la RFC4474 [3] si l'UAS n'accepte pas l'identité connectée. Si l'UAC reçoit une réponse 428, 436, 437, ou 438 à une demande de mi-dialogue, elle DEVRAIT considérer le dialogue comme terminé dans le cas d'une demande de terminaison de dialogue et DEVRAIT n'entreprendre aucune action dans le cas de toute autre demande.

Toute tentative de répétition de la demande ou d'envoi d'autre demande de mi-dialogue aura vraisemblablement la même réponse, car l'UA n'a aucun contrôle sur les actions du service d'authentification.

4.4.2 Réception d'une demande à mi-dialogue

Si un UA reçoit une demande de mi-dialogue de l'UA homologue, l'UA peut faire usage de l'identité dans l'URI du champ d'en-tête From (par exemple, en l'indiquant à l'usager). L'UA PEUT faire la distinction entre les identités signées et non signées. Dans le cas d'une identité signée, l'UA DEVRAIT invoquer un Vérificateur (voir au paragraphe 4.6) si il ne peut s'appuyer sur la présence d'un Vérificateur sur le chemin de la demande.

Si un UA reçoit une demande de mi-dialogue de la part de l'UA homologue dans laquelle l'URI du champ d'en-tête From diffère de celui reçu dans la demande précédente sur ce dialogue ou de celui envoyé dans le champ d'en-tête To de la demande INVITE d'origine et si l'UA envoie une réponse 2xx, l'UA DOIT mettre à jour l'URI distant pour ce dialogue, comme défini dans la RFC3261 [1]. Cela causera l'utilisation d'une nouvelle valeur dans le champ d'en-tête To des demandes suivantes qu'envoie l'UA, conformément aux règles du paragraphe 4.4.1. Si aucune autre réponse finale n'est envoyée, l'UA NE DOIT PAS mettre à jour l'URI distant pour ce dialogue.

4.5 Comportement du service d'authentification

Un service d'authentification DOIT se comporter conformément à la RFC4474 [3] pour traiter les demandes de mi-dialogue.

Noter que la RFC4474 reste muette sur le façon de se comporter si l'identité dans le champ d'en-tête From n'est pas une de celles que l'UAC est autorisé à affirmer, et donc c'est une affaire de politique locale de savoir s'il faut rejeter la demande ou la transmettre sans champ d'en-tête Identity. Les politiques peuvent être différentes pour une demande de mi-dialogue et pour les autres demandes.

Noter que quand les UA se conforment à cette spécification, le service d'authentification devrait (sous réserve des règles d'authentification normales) être capable d'authentifier l'envoyeur d'une demande comme étant l'entité identifiée dans le champ d'en-tête From et donc sera capable de fournir une signature pour cette identité. Ceci tranche sur la situation des UA qui ne prennent pas en charge la présente spécification, où le reciblage et les changements d'identité à mi-dialogue peuvent rendre le champ d'en-tête From inapproprié comme moyen d'identifier l'envoyeur de la demande.

4.6 Comportement du vérificateur

En traitant les demandes de mi-dialogue, un service d'authentification DOIT se comporter conformément à la RFC4474 [3] mise à jour comme indiqué ci-dessous.

La RFC4474 [3] établit que c'est une affaire de politique que de savoir s'il faut rejeter une demande avec une réponse 428 (Utiliser l'en-tête Identity) si il n'y a pas de champ d'en-tête Identity dans la demande. Un UA PEUT adopter une politique différente pour les demandes de mi-dialogue par rapport aux autres demandes.

4.7 Comportement du mandataire

Un mandataire qui reçoit une demande de mi-dialogue DOIT être prêt à ce que l'URI du champ d'en-tête To et/ou l'URI du champ d'en-tête From diffèrent de ceux qui apparaissent dans la demande et la réponse de formation du dialogue.

Un mandataire qui est capable de fournir un service d'authentification Service pour les demandes de mi-dialogue DOIT enregistrer la route si Supported: from-change est indiqué dans la demande de formation du dialogue reçue de l'UAC par le mandataire.

5 Exemples

Dans les exemples ci-dessous, plusieurs messages contiennent des lignes non coupées plus longues que 72 caractères. Elles sont marquées entre des étiquettes. La ligne entière se reconstruit en enchaînant directement toutes les lignes qui apparaissent entre les étiquette (en supprimant tous les retours à la ligne et les retours chariot).

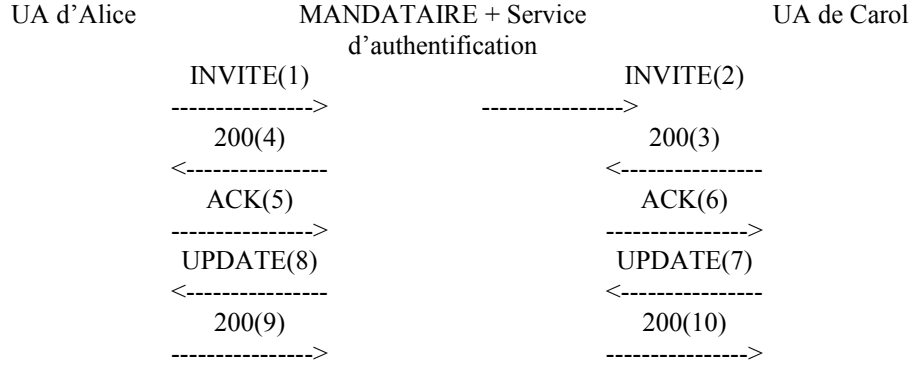
Dans les exemples, le domaine example.com est supposé avoir la clé privée suivante (rendue en format PEM). La clé privée est utilisée par le service d'authentification pour générer la signature dans le champ d'en-tête Identity.

-----DÉBUT DE CLÉ PRIVÉE RSA-----

MIICXQIBAAKBgQDPPMBtHVoPkXV+Z6jq1LsgfTELVWpy2BVUffJMPH06LL0cJSQOaIeVzIojzWtpauB7IylZKlAj
B5f429tRuoUiedCwMLKblWAqZt6eHWpCNZJ7lONcIEwnmh2nAccKk83Lp/VH3tgAS/43DQoX2sndnYh+g8522Pzwg7
EGWspzzwIDAQABAoGBAK0W3tnEFD7AjVQAnJNXDtx59Aa1Vu2JEXe6oi+OrkFysJjbZJwsLmKtrgttPXOU8t2mZpi
0wK4hX4tZhntiwGKkUPC3h9Bjp+GerifP341RMyMO+6fPgjqOzUDw+rPjjMpwD7AkcEcqDgbTrZnWv/QnCSaaF3xkU
GfFkLx5OKcRAkEA7UxnsE8XaT30tP/UUc51gNk2KGKgxQQTHopBcew9yfeCRFhvdL7jpaGatEi5iZwGGQQDVOVH
UN1H0YLpHQjRowJBAN+R2bvA/Nimq464ZgnelEDPqaEAZWaD3kOfhS9+vL7oqES+u5E0J7kXb7ZkiSVUg9XU/8Px
MKx/DAz0dUmOL+UCQH8C9ETUMI2uEbqHbBdVUGNk364CDFcndSxVh+34KqJdjiYSx6VPPv26X9m7S0OydTkSgs
3/4ooPxo8HaMqXm80CQB+rxbB3UlpOohcBwFK9mTrlMB6Cs9ql66KgwnlL9ukEhHHYozGatdXeoBCyhUsogdSU6/aS
AFcvWEGtj7/vyJECQQCCS1lKgEXoNQPqONalvYhyyMZRXFLdD4gbwRPK1uXKYpk3CkfFzOyfjeLcGPxXzq2qzuHz
GTDxZ9PAepwX4RSk-----FIN DE CLÉ PRIVÉE RSA-----

5.1 Envoi de l’identité connectée après la réponse à l’appel

Dans cet exemple, l’UA de Carol a été atteint par reciblage chez le mandataire et donc son identité (AoR) n’est pas égale à celle du champ d’en-tête To de la demande INVITE reçue (Bob). L’UA de Carol convoie l’identité de Carol dans le champ d’en-tête From d’une demande UPDATE. Le mandataire fournit aussi un service d’authentification et ajoute donc les champs d’en-tête Identity et Identity-Info à la demande UPDATE.



INVITE (1):

INVITE sip:Bob@example.com SIP/2.0
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@example.com>
From: Alice <sip:alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 1 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Supported: from-change
Contact: <sip:alice@ua1.example.com>
Content-Type: application/sdp
Content-Length: 154

v=0
o=UserA 2890844526 2890844526 IN IP4 ua1.example.com
s=Session SDP
c=IN IP4 ua1.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

INVITE (2):

INVITE sip:Carol@ua2.example.com SIP/2.0
Via: SIP/2.0/TLS proxy.example.com;branch=z9hG4bK776asdhds
<allOneLine>
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds8;received=192.0.2.
1

```
</allOneLine>
To: Bob <sip:bob@example.com>
From: Alice <sip:alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 1 INVITE
Max-Forwards: 69
Date: Thu, 21 Feb 2002 13:02:03 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Supported: from-change
Contact: <sip:alice@ua1.example.com>
Record-Route: <sip:proxy.example.com;lr>
<allOneLine>
Identity:
"xN6gCHR6KxGM+nyiEM13LcWgAFQD3lkni1DPkwgadxh4BB7G+VwY13uRv5hbCI2VSvKuZ4LYN0JNoe7v8VAzru
KMyi4Bi4nUghR/fFGBrpBSjztmfffLTp6SFLxo9XQSVrkm1O4c/4UrKn2ejRz+5BULu9n9kWswzKDNjlYlmmc="
</allOneLine>
Identity-Info: <https://example.com/example.cer>;alg=rsa-sha1
Content-Type: application/sdp
Content-Length: 154

v=0
o=UserA 2890844526 2890844526 IN IP4 ua1.example.com
s=Session SDP
c=IN IP4 ua1.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

200 (3):

SIP/2.0 200 OK
<allOneLine>
Via: SIP/2.0/TLS proxy.example.com;branch=z9hG4bK776asdhds;received=192.0.2.2
</allOneLine>
<allOneLine>
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds8;received=192.0.2.1
<allOneLine>
To: Bob <sip:bob@example.com>;tag=2ge46ab5
From: Alice <sip:alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Supported: from-change
Contact: <sip:carol@ua2.example.com>
Record-Route: <sip:proxy.example.com;lr>
Content-Type: application/sdp
Content-Length: 154

v=0
o=UserB 2890844536 2890844536 IN IP4 ua2.example.com
s=Session SDP
c=IN IP4 ua2.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

200 (4):

SIP/2.0 200 OK
<allOneLine>
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds8;received=192.0.2.1
</allOneLine>
To: Bob <sip:bob@example.com>;tag=2ge46ab5
```

From: Alice <sip:alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Supported: from-change
Contact: <sip:carol@ua2.example.com>
Record-Route: <sip:proxy.example.com;lr>
Content-Type: application/sdp
Content-Length: 154

v=0
o=UserB 2890844536 2890844536 IN IP4 ua2.example.com
s=Session SDP
c=IN IP4 ua2.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

ACK (5):

ACK sip:carol@ua2.example.com SIP/2.0
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds9
From: Alice <sip:Alice@example.com>;tag=13adc987
To: Bob <sip:Bob@example.com>;tag=2ge46ab5
Call-ID: 12345600@ua1.example.com
CSeq: 1 ACK
Max-Forwards: 70
Route: <sip:proxy.example.com;lr>
Content-Length: 0

ACK (6):

ACK sip:carol@ua2.example.com SIP/2.0
Via: SIP/2.0/TLS proxy.example.com;branch=z9hG4bK776asdhdt
<allOneLine>Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds9;received=192.0.2.1</allOneLine>
From: Alice <sip:Alice@example.com>;tag=13adc987
To: Bob <sip:Bob@example.com>;tag=2ge46ab5
Call-ID: 12345600@ua1.example.com
CSeq: 1 ACK
Max-Forwards: 69
Content-Length: 0

UPDATE (7):

UPDATE sip:Alice@ua1.example.com SIP/2.0
Via: SIP/2.0/TLS ua2.example.com;branch=z9hG4bKnashdt1
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 2 UPDATE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:15 GMT
Route: <sip:proxy.example.com;lr>
Contact: <sip:Carol@ua2.example.com>
Content-Length: 0

Noter que l'URI dans le champ d'en-tête From diffère de celui du champ d'en-tête To dans la demande/réponse INVITE. Cependant, l'étiquette est la même que dans la réponse INVITE.

UPDATE (8):

UPDATE sip:Alice@ua1.example.com SIP/2.0
Via: SIP/2.0/TLS proxy.example.com;branch=z9hG4bK776asdhdu

<allOneLine>
Via: SIP/2.0/TLS ua2.example.com;branch=z9hG4bKnashdt1;received=192.0.2.3
</allOneLine>
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 2 UPDATE
Max-Forwards: 69
Date: Thu, 21 Feb 2002 13:02:15 GMT
Contact: <sip:Carol@ua2.example.com>
<allOneLine>Identity:
"g8WJiVEzrbYum+z2lnS3pL+MIhuI439gDiMCHm01fwX5D8Ft5Ib9tewLfBT9mDOUSn6wkPSWVQfqdMF/QBPkpsIIR
OIi2sJOYBEMXZpNrhJd8/uboXMl9KRujDFQefZlmXV8dwD6XsPnMgcH8jAcaZ5aS04NyfWadIwTnGeuxko="</allOn
eLine>
Identity-Info: <https://example.com/cert>;alg=rsa-sha1
Content-Length: 0

200 (9):

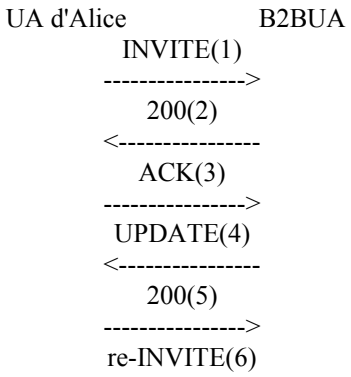
SIP/2.0 200 OK
<allOneLine>Via: SIP/2.0/TLS proxy.example.com;branch=z9hG4bK776asdhdu;received=192.0.2.2</allOneLine>
<allOneLine>Via: SIP/2.0/TLS ua2.example.com;branch=z9hG4bKnashdt1;received=192.0.2.3</allOneLine>
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 2 UPDATE
Contact: <sip:Alice@ua1.example.com>
Content-Length: 0

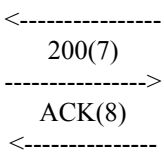
200 (10):

SIP/2.0 200 OK
<allOneLine>Via: SIP/2.0/TLS ua2.example.com;branch=z9hG4bKnashdt1;received=192.0.2.3</allOneLine>
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 2 UPDATE
Contact: <sip:Alice@ua1.example.com>
Content-Length: 0

5.2 Envoi de l’identité connectée durant l’appel

Dans cet exemple, un appel est établi entre Alice et Bob, où Bob (qui n’apparaît pas) se tient derrière un B2BUA. L’identité de Bob est convoyée par une demande UPDATE. Puis, le B2BUA exécute un transfert d’appel en utilisant des techniques de commande d’appel par tierce partie (3PCC) telles que décrites dans la RFC3725 [7] (par exemple, sous le contrôle d’une application cliquer pour numéroter). Il en résulte que Alice se trouve connectée à Carol (qui n’apparaît pas non plus), et une demande re-INVITE est produite, qui permet de renégocier la session. Le B2BUA fournit le service d’authentification et génère donc le champ d’en-tête Identity dans la demande re-INVITE pour fournir l’authentification de l’identité de Carol.





INVITE (1):

```
INVITE sip:Bob@example.com SIP/2.0
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@example.com>
From: Alice <sip:alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 1 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Supported: from-change
Contact: <sip:alice@ua1.example.com>
Content-Type: application/sdp
Content-Length: 154

v=0
o=UserA 2890844526 2890844526 IN IP4 ua1.example.com
s=Session SDP
c=IN IP4 ua1.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

200 (2)

```
SIP/2.0 200 OK
<allOneLine>Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds8;received=192.0.2.1</allOneLine>
To: Bob <sip:bob@example.com>;tag=2ge46ab5
From: Alice <sip:alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
Supported: from-change
Contact: <sip:xyz@b2bua.example.com>
Content-Type: application/sdp
Content-Length: 154

v=0
o=UserB 2890844536 2890844536 IN IP4 ua2.example.com
s=Session SDP
c=IN IP4 ua2.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

ACK (3)

```
ACK sip:xyz@b2bua.example.com SIP/2.0
Via: SIP/2.0/TLS ua1.example.com;branch=z9hG4bKnashds9
From: Alice <sip:Alice@example.com>;tag=13adc987
To: Bob <sip:Bob@example.com>;tag=2ge46ab5
Call-ID: 12345600@ua1.example.com
CSeq: 1 ACK
Max-Forwards: 70
Content-Length: 0
```

UPDATE (4)

```
UPDATE sip:alice@ua1.example.com SIP/2.0
Via: SIP/2.0/TLS b2bua.example.com;branch=z9hG4bKnashdt1
From: Bob <sip:Bob@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 2 UPDATE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:12 GMT
Contact: <sip:xyz@b2bua.example.com>
<allOneLine>Identity:
"AQFLSjCDRhO2eXlWmTajk99612hkJii9giDMWki5uT6qc4BrekywOUuObcwZI3qhJReZCN7ybMBNYFZ5yFXWdyet
4j3zLNCONU9ma+rs8ZOv0+z/Q3Z5cD26HrmitU+OCKWPLObaxbkGQry9hQxOmwRmlUgSjkeCEjgnc1iQc3E="</all
OneLine>
Identity-Info: <https://example.com/cert>;alg=rsa-sha1
Content-Length: 0
```

200 (5)

```
SIP/2.0 200 OK
<allOneLine>Via: SIP/2.0/TLS b2bua.example.com;branch=z9hG4bKnashdt1;received=192.0.2.2</allOneLine>
From: Bob <sip:Bob@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 2 UPDATE
Contact: <sip:Alice@ua1.example.com>
Content-Length: 0
```

re-INVITE (6)

```
INVITE sip:alice@ua1.example.com SIP/2.0
Via: SIP/2.0/TLS b2bua.example.com;branch=z9hG4bKnashdxy
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 3 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:03:20 GMT
Contact: <sip:xyz@b2bua.example.com>
<allOneLine>Identity:
"KCd3YLQHj51SlCQhFMnpQjmP6wHh7JGRO8LsB4v5SGEr/Mwu7j6Gpal8ckVM2vd1zqH/F4WJXYDlB525uuJm/fN3
O1A2xsZ9BxRkh4N4U19TL9I2Tok3U3kGg8To/6w1mEXpUQjo3OgNYqOBtawHuZI5nrOVaV3IrbQh1b2KgLo="</all
OneLine>
Identity-Info: <https://example.com/cert>;alg=rsa-sha1
Content-Length: 0
```

200 (7)

```
SIP/2.0 200 OK
<allOneLine>Via: SIP/2.0/TLS b2bua.example.com;branch=z9hG4bKnashdxy;received=192.0.2.2</allOneLine>
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 3 INVITE
Contact: <sip:Alice@ua1.example.com>
Content-Length: 154

v=0
o=UserA 2890844526 2890844526 IN IP4 ua1.example.com
s=Session SDP
c=IN IP4 ua1.example.com
t=0 0
```

m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

ACK (8)

ACK sip:alice@ua1.example.com SIP/2.0
Via: SIP/2.0/TLS b2bua.example.com;branch=z9hG4bKnashdxz
From: Carol <sip:Carol@example.com>;tag=2ge46ab5
To: Alice <sip:Alice@example.com>;tag=13adc987
Call-ID: 12345600@ua1.example.com
CSeq: 3 ACK
Max-Forwards: 70
Content-Length: 154

v=0
o=UserC 2890844546 2890844546 IN IP4 ua3.example.com
s=Session SDP
c=IN IP4 ua3.example.com
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

6 Considérations relatives à l'IANA

La présente spécification enregistre une nouvelle étiquette d'option SIP, conformément aux lignes directrices du paragraphe 27.1 de la RFC 3261 [1].

Le présent document définit l'étiquette d'option SIP "from-change".

La rangée suivante a été ajoutée au paragraphe "Option Tags" du registre des paramètres SIP :

Nom	Description	Référence|
from-change	Cette étiquette d'option est utilisée pour indiquer qu'un UA prend en charge les changements des URI dans les champs d'en-tête From et To durant un dialogue.	| [RFC4916]

7 Considérations pour la sécurité

La RFC4474 [3] expose assez en détails les considérations pour la sécurité qui se rapportent au champ d'en-tête Identity. Ces mêmes considérations s'appliquent lors de l'utilisation d'un champ d'en-tête Identity pour authentifier une identité connectée dans l'URI de champ d'en-tête From d'une demande de mi-dialogue.

Un URI de champ d'en-tête From reçu dans une demande de mi-dialogue pour lequel aucun champ d'en-tête Identity valide (ou un autre moyen d'authentification) n'a été reçu ni dans cette demande ni dans une demande antérieure dans ce dialogue ne peut pas être tenu pour de confiance (sauf dans des environnements très fermés) et est supposé être traité de la même façon qu'un champ d'en-tête From dans une demande d'initialisation de dialogue qui ne serait pas appuyé sur un champ d'en-tête Identity valide. Cependant, il est recommandé de ne pas rejeter une demande de mi-dialogue au motif que le champ d'en-tête Identity serait manquant (car cela interfèrerait avec le fonctionnement normal de l'appel). L'absence de champ d'en-tête Identity valide peut influencer les informations données à l'usager. Un UA peut libérer l'appel si la politique ou les choix de l'usager l'imposent.

Une identité connectée signée dans une demande de mi-dialogue (URI dans le champ d'en-tête From accompagné par un champ d'en-tête Identity valide) donne des informations sur l'UA homologue dans un dialogue. Dans le cas de l'UA qui était l'UAS dans la demande de formation du dialogue, cette identité n'est pas nécessairement la même que celle qui est dans le champ d'en-tête To de la demande de formation de dialogue. Cela, à cause du reciblage durant l'acheminement de la demande de formation de dialogue. Une identité connectée signée ne dit rien sur la légitimité d'un tel reciblage, mais reflète simplement le résultat de ce reciblage. Les informations d'historique (RFC4244 [8]) peuvent fournir des indications supplémentaires sur la façon dont l'usager connecté a été atteint.

De même, lorsqu'une identité connectée signée indique un changement d'identité durant un dialogue, elle n'apporte aucune information sur la raison d'un tel changement d'identité ni sur sa légitimité.

L'utilisation du schéma d'URI sips peut minimiser les chances des attaques dans lesquelles sont envoyées des informations d'identité connectée inappropriées, soit au moment de l'établissement de l'appel, soit pendant un appel.

L'anonymat peut être exigé par l'utilisateur d'un UA connecté. Pour l'anonymat, l'UA est supposé remplir l'URI dans le champ d'en-tête From d'une demande de mi-dialogue de la façon décrite dans la RFC4474 [3].

8 Remerciements

Merci à Francois Audet, Frank Derks, Steffen Fries, Vijay Gurbani, Cullen Jennings, Paul Kyzivat, Hans Persson, Jon Peterson, Eric Rescorla, Jonathan Rosenberg, Shida Schubert, Ya-Ching Tan, et Dan Wing pour leurs précieux commentaires.

9 Références

9.1 Références normatives

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley et E. Schooler, "SIP: Protocole d'initialisation de session", RFC3261, juin 2002.

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

[3] J. Peterson et C. Jennings, "Améliorations à la gestion d'identité authentifiée dans le protocole d'initialisation de session (SIP)", RFC4474, août 2006.

[4] J. Rosenberg, "Méthode UPDATE du protocole d'initialisation de session (SIP)", RFC3311, septembre 2002.

[5] J. Rosenberg et H. Schulzrinne, "Fiabilité des réponses provisoires dans le protocole d'initialisation de session (SIP)", RFC3262, juin 2002.

9.2 Références informatives

[6] M. Handley, H. Schulzrinne, E. Schooler et J. Rosenberg, "SIP : Protocole d'initialisation de session", RFC2543, mars 1999.

[7] J. Rosenberg, J. Peterson, H. Schulzrinne et G. Camarillo, "Bonnes practiques courantes pour la commande d'appel par un tiers (3pcc) dans le protocole d'initialisation de session (SIP)", RFC3725, juin 2002.

[8] M. Barnes, "Extension au protocole d'initialisation de session (SIP) pour la demande d'informations d'historique", RFC4244, novembre 2005.

Adresse de l'auteur

John Elwell
Siemens Enterprise Communications Limited
Technology Drive
Beeston, Nottingham NG9 1LA
UK
téléphone : +44 115 943 4989
mél : john.elwell@siemens.com

Déclaration de copyright

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

Remerciement

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