

Groupe de travail Réseau
Request for Comments : 3911
 Catégorie : En cours de normalisation
 Traduction Claude Brière de L'Isle

R. Mahy, Airespace
 D. Petrie, Pingtel
 octobre 2004

En-tête "Join" du protocole d'initialisation de session (SIP)

Statut de ce mémoire

Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (2004).

Résumé

Le présent document définit un nouvel en-tête à utiliser avec les applications multiparties et les commandes d'appel SIP. L'en-tête Join est utilisé pour joindre logiquement un dialogue SIP existant à un nouveau dialogue SIP. Cette primitive peut être utilisée pour activer diverses caractéristiques, par exemple : "irruption", "déroulement de message" de style répondeur et "surveillance de centre d'appel". Noter que la définition de ces exemples de caractéristiques n'est pas normative.

Table des Matières

1. Introduction.....	1
2. Conventions.....	2
3. Applicabilité de la RFC2804 ("Raven").....	2
4. Comportement du serveur d'agent d'utilisateur à réception d'un en-tête Join.....	3
5. Comportement du client d'agent d'utilisateur à l'envoi d'un en-tête Join.....	4
6. Comportement du mandataire.....	4
7. Syntaxe.....	4
7.1 En-tête Join.....	4
7.2 Nouvelle étiquette d'option pour les en-têtes Require et Supported.....	5
8. Exemples d'utilisation.....	5
8.1 Join accepté et transmis à une conférence centrale.....	5
8.2 Join rejeté.....	8
9. Considérations sur la sécurité.....	8
10. Considérations relatives à l'IANA.....	9
10.1 Enregistrement de l'en-tête SIP "Join".....	9
10.2 Enregistrement de l'étiquette d'option SIP "join".....	9
11 Remerciement.....	9
12. Références.....	9
12.1 Références normatives.....	9
12.2 Références pour information.....	9
13. Adresse des auteurs.....	10
14. Déclaration complète de droits de reproduction.....	10

1. Introduction

Le présent document décrit un champ d'en-tête d'extension SIP [RFC3261] au titre du cadre d'architecture des applications SIP multi parties [RFC5850]. L'en-tête Join est utilisé pour joindre logiquement un dialogue SIP existant à un nouveau dialogue SIP. Ceci est particulièrement utile dans les environnements de commande d'appel d'homologue à homologue.

Une utilisation de l'en-tête "Join" est d'insérer un nouveau participant dans une conversation multimédia (qui peut être un appel à deux ou une conférence SIP [RFC4353]). Bien que cette fonctionnalité soit déjà disponible en utilisant la commande d'appel de tiers [RFC3725], de style commande d'appel, le modèle 3pcc exige un point de commande central qui peut n'être pas souhaité dans de nombreux environnements. À ce titre, une méthode pour effectuer ces mêmes primitives de commande

3. lorsque les attentes normales de l'envoyeur sont que les informations ne soient vues que par les receveurs ou des usagers obligés de garder confidentielles les informations,
4. lorsque le tiers agit délibérément pour cibler la transmission du premier usager, soit parce qu'il s'y intéresse, soit parce qu'il s'intéresse à la réception du second usager.

Précisément, le point 2 de cette définition ne s'applique pas à cette extension, car une partie est toujours informée d'une demande Join et peut même refuser de telles demandes. De plus, dans de nombreuses applications de cette primitive, certaine ou tous les autres point peuvent ne pas s'appliquer. Par exemple, dans de nombreux centres d'appel qui traitent des transactions financières, toutes les conversations sont enregistrées en pleine connaissance de cause et conformément aux attentes de toutes les parties concernées.

4. Comportement du serveur d'agent d'utilisateur à réception d'un en-tête Join

L'en-tête Join contient des informations utilisées pour se confronter à un dialogue SIP existant (call-id, to-tag, et from-tag). À réception d'un INVITE avec un en-tête Join, l'agent d'utilisateur (UA, *User Agent*) tente de confronter ces informations avec un dialogue confirmé ou précoce. Les paramètres to-tag et from-tag sont confrontés comme si c'étaient des étiquettes présentes dans une demande entrante. En d'autres termes, le paramètre to-tag est comparé à l'étiquette locale, et le paramètre from-tag est comparé à l'étiquette distante.

Si plus d'un champ d'en-tête Join est présent dans un INVITE, ou si un champ d'en-tête Join est présent dans une demande autre qu'un INVITE, l'UAS DOIT rejeter la demande avec une réponse 400 Mauvaise demande.

L'en-tête Join a une sémantique spécifique de commande d'appel. Si dans une même demande, deux champs d'en-tête, Join et un autre en-tête avec une sémantique contradictoire (par exemple un champ d'en-tête Replaces [RFC3891]) sont présents, la demande DOIT être rejetée avec une réponse 400 "Mauvaise demande".

Si le champ d'en-tête Join correspond à plusieurs dialogues, l'UA DOIT agir comme si aucune correspondance n'était trouvée.

Si aucune correspondance n'est trouvée, mais si l'URI de demande dans l'INVITE correspond à un URI de conférence, l'UAS DOIT ignorer l'en-tête Join et continuer à traiter l'INVITE comme si l'en-tête Join n'existait pas. Cela permet aux agents d'utilisateur qui reçoivent un INVITE avec un Join de rediriger la demande directement sur un URI de conférence.

Autrement, si aucune correspondance n'est trouvée, l'UAS rejette l'INVITE et retourne une réponse 481 L'appel/transaction n'existe pas. De même, si le champ d'en-tête Join correspond à un dialogue qui n'a pas été créé avec un INVITE, l'UAS DOIT rejeter la demande avec une réponse 481.

Si le champ d'en-tête Join correspond à un dialogue qui est déjà terminé, l'UA DEVRAIT décliner la demande avec une réponse 603 Refusée.

Si le champ d'en-tête Join correspond à un dialogue actif (nota bene : à la différence de l'en-tête Replaces, l'en-tête Join n'a pas de limitation d'utilisation avec les dialogues précoces) l'UA DOIT vérifier que l'initiateur du nouvel INVITE est autorisé à se joindre au dialogue correspondant. Si l'initiateur du nouvel INVITE a réussi à s'authentifier comme équivalent à l'utilisateur qui est rejoint, le Join est alors autorisé. Par exemple, si l'utilisateur rejoint et l'initiateur du dialogue qui se joint partagent les mêmes accreditifs pour l'authentification par résumé [RFC2617], ou si ils ont signé la demande de jonction avec S/MIME [RFC3851] avec la même clé privée et présentent le (même) certificat correspondant utilisé dans le dialogue d'origine, la jonction est alors autorisée.

Autrement, le mécanisme Referred-By [RFC3892] peut être utilisé par l'UAS pour vérifier qu'une demande Join a été envoyée au nom d'un autre participant dans le dialogue correspondant (dans ce cas, déclenché par une demande REFER). Si la demande Join contient un en-tête Referred-By qui correspond à l'utilisateur joint, l'UA DEVRAIT traiter le Join comme si il était autorisé par la partie jointe. L'en-tête Referred-By DOIT faire référence à un corps d'identité authentifié Referred-By correspondant, valide [RFC3893]. L'UA PEUT appliquer une autre politique locale pour autoriser le reste de la demande. En d'autres termes, l'UAS peut appliquer une politique différente au dialogue joint et au dialogue cible.

L'UA PEUT aussi tenir une liste des entités autorisées à qui il est permis de se joindre à tout dialogue ayant certaines caractéristiques (par exemple, tous les dialogues placés dans le contexte du centre d'appels de l'UA). De plus, l'UA PEUT utiliser d'autres mécanismes d'autorisation définis à cette fin dans des extensions en cours de normalisation. Par exemple, une extension pourrait définir un mécanisme pour affirmer des autorisations transitives d'une jonction.

Si l'autorisation réussit, l'UA tente d'accepter le nouvel INVITE, et alloue toutes les ressources de mixage ou de conférence nécessaires pour achever la jonction. Si l'UA ne peut pas accepter le nouvel INVITE (par exemple, il ne peut pas établir la

qualité de service ou le chiffrement requis, ou il a un support incompatible) l'UA DOIT retourner une réponse d'erreur appropriée et DOIT laisser inchangé le dialogue correspondant.

Un agent d'utilisateur qui accepte un en-tête Join a besoin d'établir des dialogues ou des conférences tels que l'UAC qui demande soit logiquement ajouté à l'espace de conversation associé au dialogue correspondant. Tout dialogue déjà logiquement associé au dialogue correspondant dans le même espace de conversation est inclus aussi. Pour une description détaillée des divers mécanismes de conférence qui pourraient être utilisés pour traiter un Join, prière de consulter le cadre de conférence SIP de la [RFC4353].

Si l'UAS a des ressources suffisantes pour traiter en local la demande Join, l'UAS DEVRAIT accepter la demande Join et effectuer le mélange ou la combinaison appropriée de supports. L'UAS PEUT plutôt réarranger les dialogues appropriés comme décrit ci-dessous sur la base d'une politique locale.

Si l'UAS n'a pas les ressources locales suffisantes pour traiter la demande, ou ne souhaite pas utiliser ces ressources locales, mais connaît d'autres ressources qui pourraient être utilisées pour satisfaire la demande (par exemple, un serveur de conférence centralisé) l'UA DEVRAIT créer une conférence en utilisant ces ressources (par exemple, INVITE le serveur de conférence pour obtenir un URI de conférence) rediriger le demandeur sur cette ressource, et demander que les autres participants au même espace de conversation utilisent cette ressource. L'UA PEUT utiliser tout mécanisme approprié pour faire passer les participants sur la nouvelle ressource (par exemple, une réponse 3xx, des réinvitations de commande d'appel de tiers, des demandes REFER, ou des réinvitations à un groupe de diffusion groupée). L'UA DEVRAIT n'utiliser que des mécanismes qui sont supposés être acceptables aux autres participants. Par exemple, l'UA NE DEVRAIT PAS tenter de passer les participants à un groupe de diffusion groupée sauf si l'UA peut raisonnablement s'attendre à ce que tous les participants puissent prendre en charge la diffusion groupée.

Si l'UAS est incapable de satisfaire la demande Join, il DOIT retourner une réponse 488 "Non acceptable ici".

5. Comportement du client d'agent d'utilisateur à l'envoi d'un en-tête Join

Un agent d'utilisateur qui souhaite ajouter son propre nouveau dialogue à un seul dialogue existant précoce ou confirmé et à tous dialogues ou conférences associés, peut envoyer à l'agent d'utilisateur cible une demande INVITE contenant un champ d'en-tête Join. L'UAC place les informations de Call-ID, to-tag, et from-tag pour le dialogue cible dans un seul champ d'en-tête Join et envoie le nouvel INVITE à la cible.

Si l'agent d'utilisateur reçoit une réponse de classe 300, et agit sur cette réponse en envoyant un INVITE à un contact dans la réponse, cette INVITE redirigée DOIT contenir le même en-tête Join qui était présent dans la demande d'origine. Bien que ceci soit inhabituel, cela permet que les demandes INVITE avec un en-tête Join soient redirigées avant d'atteindre l'UAS cible.

Noter que l'utilisation du mécanisme Join ne fournit pas de moyen pour correspondre à plusieurs dialogues, ni pour correspondre à un appel entier, une transaction entière, ou de suivre une chaîne de logique de mandataires qui se subdivise.

6. Comportement du mandataire

Les serveurs mandataires n'exigent pas de nouveau comportement pour prendre en charge cette extension. Ils passent simplement le champ d'en-tête Join de façon transparente comme décrit dans la spécification de SIP.

Noter qu'il est possible à un mandataire (en particulier lorsque il subdivise sur la base d'une logique de couche d'application, comme un visionnage des appelants ou un acheminement à un certain moment de la journée) de transmettre une demande INVITE qui contient un champ d'en-tête Join à un ensemble complètement orthogonal de contacts que la demande originale avait l'intention de remplacer. Dans ce cas, la demande INVITE avec le champ d'en-tête Join va échouer.

7. Syntaxe

7.1 En-tête Join

Le champ d'en-tête Join indique qu'un nouveau dialogue (créé par l'INVITE dans lequel le champ d'en-tête Join est contenu) devrait être joint à un dialogue identifié par le champ d'en-tête, et tous les dialogues ou conférences associés. C'est seulement un en-tête de demande, et qui n'est défini que pour les demandes INVITE. Le champ d'en-tête Join peut être chiffré au titre d'un chiffrement de bout en bout. Une seule valeur de champ d'en-tête Join peut être présente dans une demande SIP.

Le présent document ajoute l'entrée suivante au Tableau 3 de la [RFC3261]. Les ajouts à ce tableau sont toujours fournis pour les méthodes d'extension définies au moment de la publication du présent document. Ceci est fourni pour la facilité de lecture et n'est en aucune façon normatif. MESSAGE, SUBSCRIBE et NOTIFY, REFER, INFO, UPDATE, PRACK, et PUBLISH sont respectivement définis dans les [RFC2976], [RFC3262], [RFC3265], [RFC3311], [RFC3428], [RFC3515], et [RFC6914].

Champ d'en-tête	où	mandataire	ACK	BYE	CAN	INV	OPT	REG	MSG
Join	R		-	-	-	o	-	-	-
			SUB	NOT	REF	INF	UPD	PRA	PUB
Join	R		-	-	-	-	-	-	-

La spécification de syntaxe suivante utilise la forme Backus-Naur augmentée (BNF) décrite dans la [RFC2234].

Join = "Join" HCOLON callid *(SEMI join-param)

join-param = to-tag / from-tag / generic-param

to-tag = "to-tag" EQUAL token

from-tag = "from-tag" EQUAL token

Un en-tête Join DOIT contenir exactement une to-tag et exactement une from-tag, comme elles sont exigées pour une correspondance univoque de dialogue. Pour la compatibilité avec les dialogues initiés par les UA conformes à la [RFC2543], une to-tag de zéro correspond à la fois à une valeur de to-tag de zéro et à une to-tag nulle. De même, une from-tag de zéro correspond à la fois à une valeur de from-tag de zéro et à une from-tag nulle.

Exemples :

```
Join: 98732@sip.example.com
      ;from-tag=r33th4x0r
      ;to-tag=ff87ff
```

```
Join: 12adf2f34456gs5;to-tag=12345;from-tag=54321
```

```
Join: 87134@192.0.2.23;to-tag=24796;from-tag=0
```

7.2 Nouvelle étiquette d'option pour les en-têtes Require et Supported

La présente spécification définit une nouvelle étiquette d'option d'en-tête Require/Supported "join". Les UA qui prennent en charge l'en-tête Join DOIVENT inclure l'étiquette d'option "join" dans un champ d'en-tête Supported. Les UA qui veulent une notification explicite d'échec si Join n'est pas pris en charge peuvent inclure l'option "join" dans un champ d'en-tête Require.

Exemple :

```
Require: join, 100rel
```

8. Exemples d'utilisation

Les exemples non normatifs suivants ne sont pas destinés à énumérer toutes les possibilités d'usage de cette extension, mais plutôt seulement à fournir des exemples ou des idées. Pour d'autres exemples, prière de se reporter aux exemples de service de la [RFC5359].

8.1 Join accepté et transmis à une conférence centrale

```

A          B          C          conf
|          |  callid: 7@c  |          |
|          |  |          |          |
|          |  <-INVITE-----|          | *1
|          |  |-----200----->|          | *2
|          |  <-----ACK-----|          | *3
|          |  |<=====|          |
|          |  |          |          |
|  INVITE----->|          |          | *4

```

```

|Join: 7@c      |--INVITE----->| *5
|              |<----200-----| *6
|              |-----ACK----->|
|<----302-----|              | *7
|-----ACK----->|              |
|INVITE----->| *8
|<--200-----| *9
|---ACK----->|
|              |--REFER----->| *10
|              |<---202-----| |
|              |<--NOTIFY-----|--INVITE-*11->|
|              |-----200-----|<----200-*12--|
|              |<--NOTIFY-----|-----ACK----->|
|              |-----200----->|
|              |---BYE----->|
|              |<--200-----|
|              |              |
|<=====>| mixe ensemble
|              |<=====>| les trois sessions
|              |<=====>|

```

La conversation apparaît maintenant identique à celle mixée en local de l'exemple d'introduction. Les détails sur la façon dont Join est mis en œuvre sont transparents pour A. B pourrait à la place avoir utilisé une commande d'appel de tiers pour déplacer les sessions nécessaires.

Message *1: C -> B

```

INVITE sip:bob@example.org SIP/2.0
To: <bob@example.org>
From: <carol@example.org>;tag=xyz
Call-Id: 7@c.example.org
CSeq 1 INVITE
Contact: <sip:carol@c.example.org>

```

Message *2: B -> C

```

SIP/2.0 200 OK
To: <bob@example.org>;tag=pdq
From: <carol@example.org>;tag=xyz
Call-Id: 7@c.example.org
CSeq 1 INVITE
Contact: <sip:bob@b.example.org>

```

Message *3: C -> B

```

ACK sip:carol@c.example.org SIP/2.0
To: <bob@example.org>;tag=pdq
From: <carol@example.org>;tag=xyz
Call-Id: 7@c.example.org
CSeq 1 INVITE

```

Message *4: A -> B

```

INVITE sip:bob@b.example.org SIP/2.0
To: <sip:bob@example.org>
From: <sip:alice@example.org>;tag=iii
Call-Id: 777@a.example.org
CSeq: 1 INVITE
Contact: <sip:alice@a.example.org>
Join: 7@c.example.org;to-tag=xyz;from-tag=pdq

```

Message *5: B -> conf

```

INVITE sip:conf-factory@example.org SIP/2.0
To: <sip:conf-factory@example.org>
From: <sip:bob@example.org>;tag=abc
Call-Id: 999@b.example.org
CSeq: 1INVITE

```

Contact: <sip:bob@b.example.org>

Message *6: conf -> B

SIP/2.0 200 OK

To: <sip:conf-factory@example.org>;tag=def

From: <sip:bob@example.org>;tag=abc

Call-Id: 999@b.example.org

CSeq: 1 INVITE

Contact: <sip:conf456@conf-srv2.example.org>;isfocus

Message *7: B -> A

SIP/2.0 302 Moved Temporarily

To: <sip:bob@example.org>

From: <sip:alice@example.org>;tag=iii

Call-Id: 777@a.example.org

CSeq: 1 INVITE

Contact: <sip:conf456@conf-srv2.example.org>;isfocus

Message *8: A -> conf

INVITE sip:conf456@conf-srv2.example.org SIP/2.0

To: <sip:bob@example.org>

From: <sip:alice@example.org>;tag=iii

Call-Id: 777@a.example.org

CSeq: 2 INVITE

Contact: <sip:alice@a.example.org>

Join: 7@c.example.org;to-tag=xyz;from-tag=pdq

Message *9: conf ->A

SIP/2.0 200 OK

To: <sip:bob@example.org>;tag=jjj

From: <sip:alice@example.org>;tag=iii

Call-Id: 777@a.example.org

CSeq: 2 INVITE

Contact: <sip:conf456@conf-srv2.example.org>;isfocus

Message *10: B -> C

REFER sip:carol@c.example.org SIP/2.0

To: <carol@example.org>;tag=xyz

From: <bob@example.org>;tag=pdq

Call-Id: 7@c.example.org

CSeq: 1 REFER

Contact: <sip:bob@b.example.org>

Refer-To: <sip:conf456@conf-srv2.example.org>

Referred-By: <sip:bob@b.example.org>

Message *11: C -> conf

INVITE sip:conf456@conf-srv2.example.org SIP/2.0

To: <sip:conf456@conf-srv2.example.org>

From: <carol@example.org>;tag=mmm

Call-Id: 34343@c.example.com

CSeq: 1 INVITE

Contact: <sip:carol@c.example.com>

Referred-By: <sip:bob@b.example.org>

Message *12: C -> conf

SIP/2.0 200 OK

To: <sip:conf456@conf-srv2.example.org>

From: <carol@example.org>;tag=mmm

Call-Id: 34343@c.example.com

CSeq: 1 INVITE

Contact: <sip:conf456@conf-srv2.example.org>;isfocus

Referred-By: <sip:bob@b.example.org>

8.2 Join rejeté

```

A           B           C
|           | callid: 7@c |
|           |           |
|           | <===== > |
|           |           |
| INVITE-----> | *1   |
| Join: 7@c      |       |
| <-----486----- | *2   |
| -----ACK-----> |       |
|           |           |

```

Dans cet exemple B est occupé (il ne veut pas être dérangé) et ne souhaite donc pas ajouter A. B pourrait aussi décliner la demande avec une réponse 603.

Message *1: A -> B

```

INVITE sip:bob@b.example.org SIP/2.0
To: <sip:bob@example.org>
From: <sip:alice@example.org>;tag=iii
Call-Id: 777@a.example.org
CSeq: 1 INVITE
Contact: <sip:alice@a.example.org>
Join: 7@c.example.org;to-tag=xyz;from-tag=pdq

```

Message *2: B -> A

```

SIP/2.0 486 Busy
To: <sip:bob@example.org>
From: <sip:alice@example.org>;tag=iii
Call-Id: 777@a.example.org
CSeq: 1 INVITE

```

9. Considérations sur la sécurité

L'extension spécifiée dans le présent document change de façon significative la sécurité relative des appareils SIP. Actuellement dans SIP, même si un espion apprend les en-têtes Call-ID, To, et From d'un dialogue, il ne peut pas facilement modifier ou détruire ce dialogue si l'authentification par résumé ou l'intégrité de message de bout en bout est utilisée.

Cette extension peut être utilisée pour insérer ou surveiller un contenu potentiellement sensible dans une conversation multimédia. À ce titre, des invitations avec l'en-tête Join ne DOIVENT être acceptées que si l'homologue qui demande le remplacement a été correctement authentifié en utilisant un mécanisme SIP standard (Digest ou S/MIME) et autorisé à la jonction avec le dialogue cible. (Toutes les mises en œuvre SIP sont déjà obligées de prendre en charge l'authentification par résumé.) Les autorisations de jonction sont généralement configurées au titre de la politique locale comme des relations persistantes de longue durée.

Par exemple, les UA utilisés par les agents de centre d'appel peuvent être configurés avec une liste des identités qui peuvent joindre leurs appels (les superviseurs et tous les agents d'utilisateur de surveillance du centre d'appel). Autrement, les agents du centre d'appel peuvent s'appuyer sur des assertions d'autorisation transitives tirées d'une (plus courte) liste d'hôtes autorisés (par exemple, une autorité de certificat). Pour le visionnage de message de style répondeur, ceci est encore plus facile. On peut supposer que les usagers qui visionnent leurs messages ont déjà quelques accreditifs auprès de leur serveur de messagerie.

Les mécanismes pour obtenir les informations de dialogue nécessaires pour les en-têtes Join (Call-ID, to-tag, et from-tag) incluent des URI sur une page de la Toile, des abonnements à un paquetage d'événement approprié, et des notifications après une demande REFER. L'utilisation de mécanismes de sécurité de bout en bout pour la protection de l'intégrité et le chiffrement de ces informations est aussi RECOMMANDÉE.

La présente extension a été conçue pour tirer parti des futurs schémas de signature ou d'autorisation définis par des extensions en cours de normalisation. En général, les dispositifs de commande d'appel vont tirer un parti considérable de ces travaux.

La Section 4 décrit les mécanismes spécifiques de l'autorisation utilisant l'authentification par résumé et S/MIME (RFC3261) et Referred-by [RFC3892], les capacités actuellement disponibles dans SIP.

10. Considérations relatives à l'IANA

10.1 Enregistrement de l'en-tête SIP "Join"

Nom de l'en-tête : Join

Forme abrégée : aucune

Description normative : paragraphe 7.1 du présent document

10.2 Enregistrement de l'étiquette d'option SIP "join"

Nom de l'option : join

Description : Prise en charge de l'en-tête SIP Join

En-tête SIP définis : Join

Description normative : Le présent document

11 Remerciement

Merci à Robert Sparks, Alan Johnston, et Ben Campbell et à beaucoup d'autres membres du groupe de travail SIP pour leur soutien continu de la cause de la commande d'appel répartie dans SIP.

12. Références

12.1 Références normatives

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

[RFC2234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", novembre 1997. (*Obsolète, voir RFC5234*)

[RFC2617] J. Franks et autres, "Authentification HTTP : [Authentification d'accès de base et par résumé](#)", RFC 2617, juin 1999. (*DS.*)

[RFC3261] J. Rosenberg et autres, "SIP : [Protocole d'initialisation de session](#)", juin 2002. (*Mise à jour par RFC3265, RFC3853, RFC4320, RFC4916, RFC5393, RFC6665*)

[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

[RFC3851] B. Ramsdell, "Spécification du message d'extensions de messagerie Internet multi-objets/sécurisé (S/MIME) version 3.1", juillet 2004. (*Remplacée par RFC5751*)

12.2 Références pour information

[RFC2543] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP : protocole d'initialisation de session", mars 1999. (*Obsolète, voir RFC3261, RFC3262, RFC3263, RFC3264, RFC3265*) (*P.S.*)

[RFC2804] IAB, IESG, "[Politique de l'IETF en matière d'écoutes](#)", mai 2000. (*Information*)

[RFC2976] S. Donovan, "Méthode INFO pour SIP", octobre 2000. (*P.S., Remplacée par la RFC6086*)

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

- [RFC3265] A.B. Roach, "[Notification d'événement spécifique](#) du protocole d'initialisation de session (SIP)", juin 2002. (*MàJ par RFC6446*) (*Remplacée par la RFC6665*)
- [RFC3311] J. Rosenberg, "[Méthode UPDATE](#) du protocole d'initialisation de session (SIP) ", octobre 2002.
- [RFC3428] B. Campbell et autres, "[Extension de messagerie instantanée](#) pour le protocole d'initialisation de session (SIP) ", décembre 2002.
- [RFC3515] R. Sparks, "[Méthode Refer](#) du protocole d'initialisation de session (SIP)", avril 2003.
- [RFC3725] J. Rosenberg et autres, "Bonnes pratiques actuelles [pour la commande d'appel de tiers \(3pcc\)](#) dans le protocole d'initialisation de session (SIP)", avril 2004. ([BCP0085](#))
- [RFC3891] R. Mahy, B. Biggs, R. Dean, "[En-tête "Replaces"](#) du protocole d'initialisation de session (SIP)", septembre 2004. (*P.S.*)
- [RFC3892] R. Sparks, "[Mécanisme Referred-by](#) du protocole d'initialisation de session (SIP)", septembre 2004.
- [RFC3893] J. Peterson, "[Format de corps d'identité authentifiée](#) (AIB) du protocole d'initialisation de session (SIP)", septembre 2004.
- [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.*)
- [RFC4353] J. Rosenberg, "Cadre pour les conférences avec le protocole d'initialisation de session (SIP)", février 2006. (*Information*)
- [RFC4579] A. Johnston, O. Levin, "Commande d'appel du protocole d'initialisation de session (SIP) – Conférence pour agents d'utilisateur", août 2006. ([BCP0119](#))
- [RFC5359] A. Johnston et autres, "Exemples de services avec le protocole d'initialisation de session", octobre 2008. ([BCP0144](#))
- [RFC5850] R. Mahy, R. Sparks, J. Rosenberg, D. Petrie, A. Johnston, "Cadre de la commande d'appel et de l'utilisation multi-partie pour le protocole d'initialisation de session (SIP)", mai 2010. (*Information*)
- [RFC6914] J. Rosenberg, "SIMPLE rendu simple : vue d'ensemble des spécifications de l'IETF pour la messagerie instantanée et la présence avec le protocole d'initialisation de session (SIP)", avril 2013. (*Information*)

13. Adresse des auteurs

Rohan Mahy
Airespace
110 Nortech Parkway
San Jose, CA 95134
USA
mél : rohan@airespace.com

Dan Petrie
Pingtel
400 West Cummings Park, Suite 2200
Woburn, MA 01801
USA
mél : dpetrie@pingtel.com

14. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2004).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci-encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet

particulier.

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 le 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