Groupe de travail Réseau
Request for Comments : 3892
Catégorie : En cours de normalisation

R. Sparks, Xten
septembre 2004
Traduction Claude Brière de L'Isle

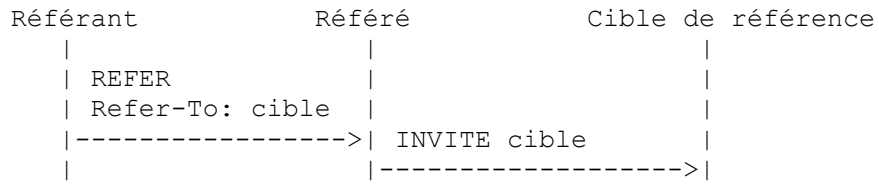
Mécanisme Referred-By du protocole d'initialisation de session (SIP)

Résumé
La méthode REFER du protocole d'initialisation de session (SIP, *Session Initiation Protocol*) fournit un mécanisme où une partie (le référant) donne à une seconde partie (le référé) un URI arbitraire à référencer. Si cet URI est un URI SIP, le référé va envoyer une demande SIP, souvent une INVITE, à cet URI (la cible de référence). Le présent document étend la méthode REFER, permettant au référant de fournir des informations sur la demande REFER à la cible de référence en utilisant le référé comme intermédiaire. Ces informations incluent l'identité du référant et l'URI auquel le référant se réfère. Le mécanisme utilise S/MIME pour aider à protéger ces informations contre un intermédiaire malveillant. Cette protection est facultative mais un receveur peut refuser d'accepter une demande si elle n'est pas présente.

Table des Matières

1. Généralités

La méthode SIP REFER [RFC3515] donne un mécanisme où une partie (le référant) fournit à une seconde partie (le référé) un URI arbitraire à référencer. Si cet URI est un URI SIP, le référé va envoyer une demande SIP, souvent une INVITE, à cet URI (la cible de référence). Rien de ce qui est fourni dans la [RFC3515] ne distingue cette demande référencée d'une autre demande que le référé pourrait avoir envoyée à la cible de référence.



Il y a des applications de REFER, telles que le transfert d'appel [RFC5589], où il est souhaitable de fournir à la cible de référence des informations particulières sur le référant et sur la demande REFER elle-même. Ces informations peuvent inclure, sans s'y limiter, l'identité du référant, l'URI référencé, et l'heure de la référence. La cible de référence peut utiliser ces informations pour décider si elle admet la demande référencée. Le présent document définit un ensemble de mécanismes pour fournir ces informations.

Tous les mécanismes de ce document impliquent de placer les informations dans la demande REFER que le référé copie dans la demande référencée. Cela établit nécessairement le référé comme un espion et place le référé en position de lancer des attaques par interposition sur ces informations.

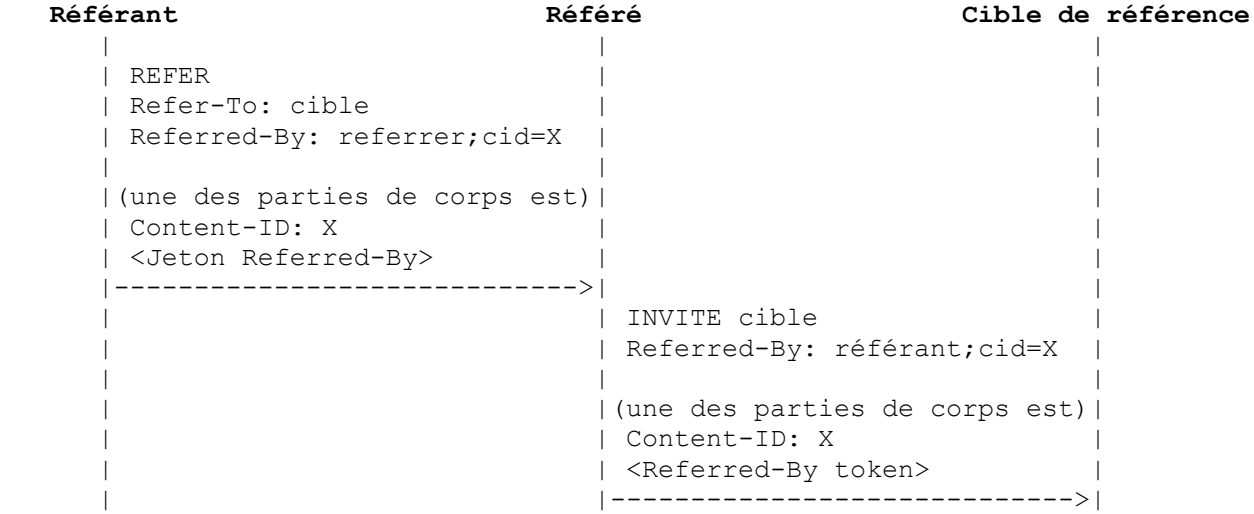
Au niveau le plus simple, le présent document définit un mécanisme pour porter l'identité du référant, exprimée comme un URI SIP dans un nouvel en-tête : Referred-By. La cible de référence peut utiliser cette information, même si elle n'a pas été protégée contre le référé, aux risques et avec les limitations précisées ici. Le document définit un mécanisme fondé sur S/MIME pour exprimer l'identité du référant et pour capturer d'autres informations sur la demande REFER, permettant à la cible de référence de détecter les altérations (et autres comportements indésirables) effectuées par le référé.

1.1 Notation des exigences

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC 2119].

2. Mécanisme Referred-By

La figure suivante résume comment les informations du Referred-By sont portées à la cible de référence. Le référant fournit un en-tête Referred-By avec une adresse d'enregistrement SIP *(address-of-record)* qui associe facultativement un jeton protégé par S/MIME qui reflète l'identité du référant et les détails de la demande REFER. Le référé copie cet en-tête et le jeton, si il est fourni, dans la demande déclanchée (montrée ci-dessous comme une INVITE).



2.1 Comportement du référant

Un UA qui envoie une demande REFER (un référant) PEUT fournir une valeur de champ d'en-tête Referred-By dans une demande. Une demande REFER NE DOIT PAS contenir plus d'une valeur de champ d'en-tête Referred-By.

Un référant PEUT inclure un jeton Referred-By dans une demande REFER. Une demande REFER qui contient un jeton Referred-By DOIT contenir une valeur de champ d'en-tête Referred-By avec une valeur de paramètre cid égale à l'identifiant de contenu *(Content-ID)* de la partie de corps qui contient le jeton.

Le référant va recevoir un NOTIFY avec un corps message/sipfrag [RFC3420] indiquant une réponse finale de 429 "Fournir l'identité du référant" à la demande référencée si la cible de référence exige un jeton Referred-By valide pour accepter la demande. Cela peut se produire lorsque aucun jeton n'est produit ou que le jeton fourni est invalide.

Le référant va recevoir une réponse 429 "Fournir l'identité du référant" au REFER si le référé exige la présence d'un jeton Referred-By pour accepter le REFER.

Si un référant souhaite tenter à nouveau de faire référence à un référé après avoir reçu une réponse 429 ou un NOTIFY contenant un 429, il PEUT soumettre une nouvelle demande REFER contenant un jeton Referred-By.

2.2 Comportement du référé

Un UA qui accepte une demande REFER (un référé) à un URI SIP (en utilisant le schéma sip: ou sips:) DOIT copier toute valeur de champ d'en-tête Referred-By et de jeton dans la demande référencée sans modification.

Un référé PEUT rejeter une demande REFER qui ne contient pas un jeton Referred-By avec une réponse 429 "Fournir l'identité du référant". Un référé NE DEVRAIT PAS rejeter une demande qui contient un jeton Referred-By chiffré avec une clé qu'il ne possède pas simplement parce qu'il ne peut pas déchiffrer le jeton. (Un scénario où un tel rejet serait approprié est lorsque le référé tente de rester anonymé (voir le paragraphe 6.1).) Noter que selon la [RFC3893], le référé devrait quand même être capable de vérifier la signature d'un tel jeton chiffré.

Un référé DEVRAIT présenter la même identité au référant et à la cible de référence.

2.3 Comportement de la cible de référence

Un UA qui reçoit une demande SIP non REFER PEUT inspecter la demande pour chercher un champ d'en-tête Referred-By et un jeton.

Si une valeur de champ d'en-tête Referred-By n'est pas présente, cet UA ne peut pas distinguer cette demande de toute autre que l'UA agissant comme référé pourrait avoir envoyé. Donc, l'UA va appliquer exactement les politiques d'admission et de traitement décrites dans la [RFC3261] à la demande.

Si une valeur de champ d'en-tête Referred-By est présente, l'UA receveur peut se considérer lui-même comme une cible de référence et PEUT appliquer des politiques d'admission supplémentaires sur la base du contenu du champ d'en-tête Referred-By et du jeton.

Le référé est en position de modifier le contenu de la valeur du champ d'en-tête Referred-By, ou d'en produire une fausse même si aucun REFER n'existe en fait. Si un tel comportement pouvait affecter la politique d'admission (incluant d'influencer l'utilisateur de l'agent en rendant un contenu trompeur) la cible de référence DEVRAIT exiger qu'un jeton Referred-By valide soit présent.

La cible de référence PEUT rejeter une demande si aucun jeton Referred-By n'est présent ou si le jeton est périmé en utilisant la réponse d'erreur 429 "Fournir l'identité du référant" définie à la Section 5. La réponse d'erreur 428 de la [RFC4475] n'est pas appropriée pour cet objet – il est nécessaire que la cible de référence demande un jeton d'authentification au référé.

Si aucun jeton Referred-By n'est présent, la cible de référence PEUT procéder au traitement de la demande. Si l'agent fournit des informations provenant de l'en-tête Referred-By à son utilisateur au titre du traitement de la demande, il DOIT notifier à l'utilisateur que les informations sont suspectes.

La cible de référence DOIT rejeter une demande par ailleurs bien formée mais qui a un jeton Referred-By invalide (voir la Section 4) avec une réponse d'erreur 429.

3. Champ d'en-tête Referred-By

Referred-By est un champ d'en-tête de demande comme défini dans la [RFC3261]. Il peut apparaître dans toute demande. Il porte un URI SIP qui représente l'identité du référant et, facultativement, le Content-ID *(identifiant de contenu)* d'une partie de corps (le jeton Referred-By) qui fournit une déclaration plus sûre de cette identité.

```
Referred-By  =  ("Referred-By" / "b") HCOLON referrer-uri *( SEMI (referredby-id-param / generic-param) )
referrer-uri = ( name-addr / addr-spec )
referredby-id-param = "cid" EQUAL sip-clean-msg-id
sip-clean-msg-id = LDQUOT dot-atom "@" (dot-atom / hôte) RDQUOT
dot-atom = atom *( "." atom )
atom     = 1*( alphanum / "-" / "!" / "%" / "*" / "_" / "+" / "'" / "`" / "~"   )
```

Comme le Content-ID apparaît comme une valeur de paramètre d'en-tête SIP qui doit se conformer à l'expansion de la valeur gen-value définie dans la [RFC3261], cette grammaire produit des valeurs dans l'intersection de l'expansion de gen-value et de msg-id d'après la [RFC2822]. Les guillemets qui entourent le sip-clean-msg-id DOIVENT être remplacés par des crochets angulaires gauche et droit pour déduire le Content-ID utilisé dans le corps MIME du message. Par exemple,

Referred-By: sip:r@ref.example;cid="2UWQFN309shb3@ref.example"

indique que le jeton est dans la partie de corps qui contient

Content-ID: <2UWQFN309shb3@ref.example>

Si le referrer-uri contient une virgule, un point d'interrogation, ou un point-virgule (par exemple, si il contient des paramètres d'URI) l'URI DOIT être inclus entre des crochets angulaires (< et >). Tout les paramètres d'URI sont contenus dans ces crochets. Si l'URI n'est pas inclus dans des crochets angulaires, tout paramètre délimité par un point-virgule est un paramètre d'en-tête, et pas un paramètre d'URI.

Le champ d'en-tête Referred-By PEUT apparaître dans toute demande SIP, mais il ne signifie rien pour ACK et CANCEL. Les mandataires n'ont pas besoin d'être capables de lire les valeurs de champ d'en-tête Referred-By et NE DOIVENT PAS les retirer ou les modifier.

La ligne suivante devrait être interprétée comme si elle apparaissait dans le Tableau 2 de la RFC3261.

Ch. d'en-tête	**où**	**mandataire**	**ACK**	**BYE**	**CAN**	**INV**	**OPT**	**REG**
Referred-By	R		-	o	-	o	o	o

4. Jeton Referred-By

Le jeton Referred-By est un corps d'identité authentifié comme défini par la [RFC3893]. Ce corps DOIT être identifié avec un champ Content-ID: de MIME [RFC2045].

Le sipfrag au sein d'un jeton Referred-By DOIT contenir des copies des champs d'en-tête Refer-To, Referred-By, et Date provenant de la demande REFER.

Le jeton NE DEVRAIT PAS contenir le champ d'en-tête Call-ID provenant de la demande REFER car cette information n'est pas utile pour la cible de référence et peut même être une fuite d'informations. Le jeton NE DEVRAIT PAS contenir le champ d'en-tête From provenant de la demande REFER car l'identité qui est revendiquée est représentée dans le champ d'en-tête Referred-By.

Le jeton PEUT contenir le champ d'en-tête To provenant de la demande REFER, mais il NE DEVRAIT PAS être inclus sauf si le référant a cryptographiquement identifié le référé. Certaines des façons dont cette authentification peut être réalisée incluent d'inspecter les certificats utilisés dans une association TLS entre le référant et le référé ou en chiffrant l'en-tête Refer-To dans la demande REFER en utilisant les techniques de chiffrement S/MIME détaillées dans la [RFC3261].

Lors de l'inspection des certificats utilisés pour établir les associations TLS, l'identité affirmée dans l'URI du champ d'en-tête To du jeton est comparée aux subjectAltNames du certificat du référé. Les schémas d'URI sip et sips DOIVENT être traités comme équivalents pour cette comparaison. Si l'URI est en correspondance exacte, la confiance dans l'authentification est élevée et le champ d'en-tête To PEUT être ajouté au jeton. Si les sujets du certificat contiennent seulement un nom d'hôte qui correspond à la portion nom d'hôte de l'URI, un avertissement de niveau application DEVRAIT être produit à l'agent

d'utilisateur du référant cherchant à obtenir le consentement de cet utilisateur avant d'inclure le champ d'en-tête To dans le jeton.

Inclure le champ d'en-tête To dans le jeton renforce significativement la revendication effectuée par le jeton, mais peut avoir des implications de confidentialité qui sont discutées au paragraphe 6.1.

Des champs d'en-tête et parties de corps supplémentaires PEUVENT être inclus dans le jeton.

Comme décrit dans la [RFC3893], un jeton Referred-By PEUT être chiffré ainsi que signé. Le subjectAltName du certificat utilisé pour ces opérations DEVRAIT correspondre exactement à l'identité revendiquée dans le referrer-uri dans le champ d'en-tête Referred-By dans le jeton.

4.1 Inspection de la cible de référence d'un jeton Referred-By

Une cible de référence DOIT traiter un jeton Referred-By avec une signature invalide comme un jeton invalide. Une cible DEVRAIT traiter un jeton avec une valeur de champ d'en-tête Date périmée comme invalide.

Une cible DEVRAIT vérifier que la demande qu'il reçoit correspond à la référence du champ d'en-tête Refer-To dans le jeton. Cette vérification DEVRAIT inclure au moins la méthode de la demande et toutes valeurs indiquées de champ d'en-tête de bout en bout. Noter que l'URI dans le champ d'en-tête Refer-To peut ne pas correspondre à l'URI de demande dans la demande reçue à cause d'un reciblage de la demande entre le référé et la cible de référence.

La cible DEVRAIT vérifier que l'identité dans le champ d'en-tête Referred-By dans le jeton correspond exactement au SubjectAltName provenant du certificat de signature, et rapporter les discordances à son utilisateur comme décrit dans la [RFC3893].

Si le jeton contient un champ d'en-tête To, la cible DEVRAIT vérifier que l'identité qu'il exprime correspond à celle du référant. Une façon de le vérifier est de confronter exactement l'identité dans le champ d'en-tête To du jeton au subjectAltName du certificat utilisé par le référé pour signer le aib qui protège la demande elle-même. La réponse 428 définie dans la [RFC4475] peut être utilisée pour demander un tel aib si il n'en est pas déjà un présent.

5. Réponse d'erreur 429 Fournir l'identité du référant

Le code de réponse d'erreur de client 429 est utilisé par une cible de référence pour indiquer que le référé doit fournir un jeton Referred-By valide. Comme exposé dans la section 2 sur les comportements, le référé va transmettre cette réponse d'erreur au référant dans un NOTIFY par suite du REFER. La phrase de texte suggérée pour la réponse d'erreur 429 est "Fournir l'identité du référant".

6. Considérations pour la sécurité

Le mécanisme défini dans la présente spécification s'appuie sur un intermédiaire (le référé) pour transmettre les informations du référant à la cible de référence. Cela établit nécessairement le référé comme un espion de ces informations et le positionne idéalement pour lancer des attaques par interposition utilisant ce mécanisme.

Un mandataire SIP est dans la même position. Protéger la messagerie SIP contre des mises en œuvre malveillantes de mandataire est discuté dans la [RFC3261]. À la différence d'un mandataire, l'agent du référé est un point d'extrémité. Les mandataires vont normalement être gérés et surveillés par les fournisseurs de service. Le comportement malveillant d'un mandataire a plus de chances d'être remarqué et d'avoir des répercussions négatives pour le fournisseur que n'en aurait le comportement malveillant d'un point d'extrémité. Le comportement d'un point d'extrémité peut être entièrement sous le contrôle d'un seul usager. Donc, il est plus facile pour un point d'extrémité qui agit comme référé de se comporter de façon malveillante qu'il ne l'est pour un mandataire qui fonctionne sous le contrôle d'un fournisseur de service.

La présente spécification utilise un mécanisme fondé sur S/MIME pour permettre à la cible de référence de détecter les manipulations des informations de Referred-By par le référé. L'utilisation de cette protection est facultative ! La communauté a affirmé qu'il y a des systèmes où la confiance dans la validité de ces informations est sans importance ou peut être établie par d'autres moyens. Toute mise en œuvre qui choisit de ne pas utiliser ce mécanisme facultatif devra fournir sa propre défense contre les risques suivants :

- Les informations de Referred-By vont très probablement influencer la politique d'admission de demande. Par exemple, elles peuvent être affichées à l'utilisateur de l'agent avec une indication "Cet appel vous a été transféré par X. L'acceptez vous ?". Un référé malveillant peut indûment influencer cette décision de politique en fournissant des informations de referred-by falsifiées. Cela inclut de revendiquer faussement avoir été référé en premier. (Le mécanisme S/MIME protège les informations par une signature, entravant la capacité du référé à injecter ou modifier des informations sans connaître la clé utilisée pour cette signature.)

- Un référé est par définition un espion des informations du referred-by. Des parties de ces informations peuvent être sensibles. (Le mécanisme S/MIME permet le chiffrement.)

- Le référé peut mémoriser toutes les informations de referred-by qu'il voit et les copier dans de futures demandes sans relation. (Le mécanisme S/MIME permet la détection des affirmations périmées en liant un horodatage à la signature et permet la détection de l'utilisation de demandes sans rapport en couvrant le champ d'en-tête Refer-To avec la signature.)

Les mécanismes de la présente spécification N'empêchent PAS le référé de supprimer TOUTES les informations de referred-by de la demande référencée. Une cible de référence ne peut pas détecter une telle suppression. Cela n'introduit pas de nouveaux problèmes car retirer toutes les informations de referred-by d'une demande référencée la transforme en une demande SIP ordinaire comme décrit dans la [RFC3261]. Donc, le référé ne gagne aucune nouvelle influence sur la logique de traitement de la cible de référence en retirant les informations du referred-by.

Les cibles de référence peuvent se protéger de la possibilité qu'un référé malveillant retire un jeton (laissant une identité non sûre dans le champ d'en-tête Referred-By) en utilisant la réponse d'erreur 429.

Les applications qui utilisent les mécanismes du présent document peuvent être capables de tirer parti des relations préexistantes entre les participants pour atténuer les risques de son utilisation. Dans certains scénarios de transfert, A a le choix de référer B à C ou de référer C à B. Si A et B ont une relation de confiance préexistante, conduire A à avoir plus confiance que B ne va pas se comporter de façon malveillante (B est l'assistant administratif de A, par exemple) référer B à C peut être plus raisonnable.

Ce mécanisme implique deux demandes SIP entre trois points d'extrémité, la demande REFER et la demande référencée. Le contenu de ces messages (incluant les informations du referred-by) est le sujet des considérations de sécurité et des mécanismes de protection documentés dans la [RFC3261].

Les mandataires entre les participants peuvent collecter les informations du referred-by et les réinsérer dans de futures demandes ou les rendre disponibles à des points d'extrémité hostiles. Les capacités de confidentialité de bout en bout discutées dans la [RFC3261] peuvent aider à réduire le risque d'exposition d'informations de referred-by sensibles à ces mandataires. Les possibilités d'abus dans des demandes ultérieures par des mandataires (ou des points d'extrémité sur qui ils font fuir des informations) entre le référé et la cible de référence sont identiques aux abus par le référé, et les considérations discutées pour un référé malveillant s'appliquent. Les possibilités d'abus dans des demandes ultérieures par des mandataires (ou des points d'extrémité auxquels ils communiquent les informations) entre le référant et le référé sont similaires à celles discutées pour la présentation des corps d'identité authentifiés dans la [RFC4475].

6.1 Identification du référé dans le jeton Referred-by

Pour une cible de référence, un jeton Referred-By affirme seulement que "l'identité exprimée par ce champ d'en-tête Referred-By a demandé à l'heure indiquée dans le champ d'en-tête Date que la demande indiquée par ce champ d'en-tête Refer-To soit envoyée". Cette assertion ne fait aucune revendication du tout sur à qui il a été demandé d'envoyer la demande. Ceci est suffisant pour permettre des politiques comme "Accepter toute demande référencée par Alice", mais pas "N'accepter les demandes provenant de Bob que si il peut prouver qu'Alice nous l'a référencé". Donc, il y a une opportunité pour une attaque de copier coller. Si Mallory voit qu'Alice nous référence Carol en utilisant un jeton minimal, il peut copier ce jeton dans sa propre demande (tant qu'elle correspond à ce qui est indiqué dans l'en-tête Refer-To incorporé) et il va nous apparaître comme si Alice nous avait référencé Mallory. Ce risque est bien atténué en protégeant le REFER qu'Alice envoie à Carol contre l'espionnage, en utilisant TLS ou les mécanismes S/MIME détaillés dans la [RFC3261].

Inclure le champ d'en-tête To de la demande REFER dans le jeton Referred-by permet le "N'accepter les demandes de Bob que si il peut prouver qu'Alice nous l'a référencé". Alice n'est contrainte d'ajouter cet en-tête au jeton que si elle est sûre qu'elle envoie la demande REFER à Bob. Nous, à notre tour, nous nous assurons que c'est Bob qui nous envoie la demande référencée, en plus de valider la signature du jeton d'Alice. L'attaque précédente de Mallory n'est pas efficace avec ce jeton.

Inclure le champ d'en-tête To dans le jeton Referred-By a cependant des implications sur la confidentialité. Carol, ci-dessus, peut souhaiter nous contacter de façon anonyme. Ce souhait ne sera pas exaucé si l'identité de Carol apparaît dans le jeton

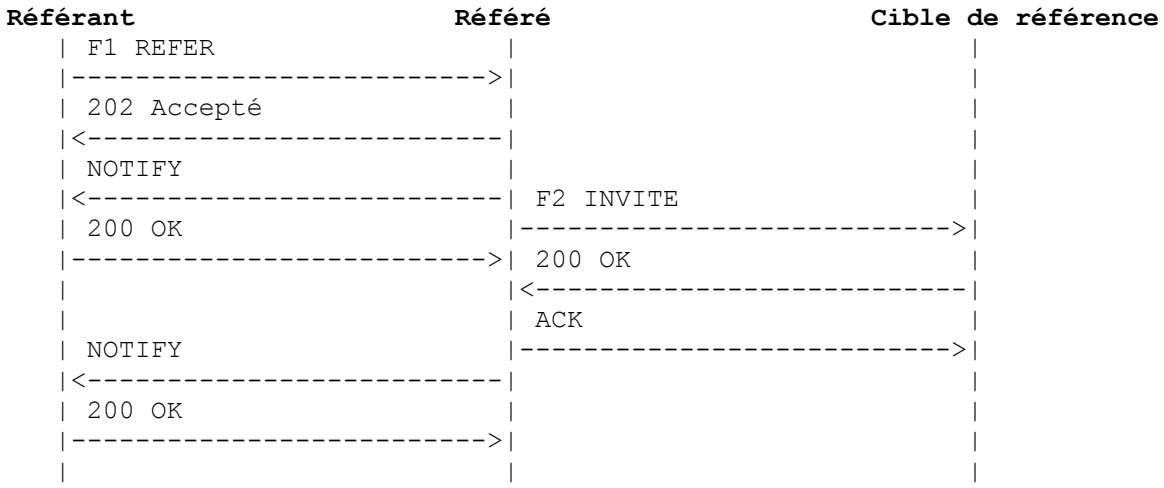
qu'Alice a créé. Si Alice a chiffré le jeton, Carol ne sera même pas informée de la fuite. Pour se protéger lorsque elle souhaite rester anonymé, Carol devra rejeter toutes les demandes REFER qui contiennent un jeton Referred-By qu'elle ne peut pas inspecter.

7. Exemples

7.1 REFER de base

Cet exemple montre le mécanisme Referred-By sécurisé appliqué à un REFER à un URI INVITE SIP.

Les détails ne sont montrés que pour les messages impliqués dans le mécanisme défini dans ce document.




```
F1 REFER sip:referee@referee.example SIP/2.0
  Via: SIP/2.0/UDP referrer.example;branch=z9hG4bK392039842
  To: sip:referee@referee.example
  From: sip:referrer@referrer.example;tag=39092342
  Call-ID: 2203900ef0299349d9209f023a
  CSeq: 1239930 REFER
  Max-Forwards: 70
  Contact: <sip:referrer.example>
  Refer-To: <sip:refertarget@target.example>
  Referred-By: <sip:referrer@referrer.example>
    ;cid="20398823.2UWQFN309shb3@referrer.example"
  Content-Type: multipart/mixed; boundary=unique-boundary-1
  Content-Length: (la valeur appropriée)

  --unique-boundary-1
  Content-Type: multipart/signed;
    protocol="application/pkcs7-signature";
    micalg=sha1; boundary=dragons39
  Content-ID: <20398823.2UWQFN309shb3@referrer.example>
  Content-Length: (la valeur appropriée)

  --dragons39
  Content-Type: message/sipfrag
  Content-Disposition: aib; handling=optional

  Date: Thu, 21 Feb 2002 13:02:03 GMT
  Refer-To: <sip:refertarget@target.example>
  Referred-By: <sip:referrer@referrer.example>
    ;cid="20398823.2UWQFN309shb3@referrer.example"

  --dragons39
  Content-Type: application/pkcs7-signature; name=smime.p7s
```

```
   Content-Transfer-Encoding: base64
   Content-Disposition: attachment; filename=smime.p7s;
     handling=required

   (la signature appropriée vient ici)

   --dragons39--
   --unique-boundary-1--

 F2 INVITE sip:refertarget@target.example SIP/2.0
   Via: SIP/2.0/UDP referee.example;branch=z9hG4bKffe209934aac
   To: <sip:refertarget@target.example>
   From: <sip:referee@referee.example>;tag=2909034023
   Call-ID: fe9023940-a3465@referee.example
   CSeq: 889823409 INVITE
   Max-Forwards: 70

   Contact: <sip:referee@referee.example>
   Referred-By: <sip:referrer@referrer.example>
     ;cid="20398823.2UWQFN309shb3@referrer.example"
   Content-Type: multipart/mixed; boundary=my-boundary-9
   Content-Length: (la valeur appropriée)

   --my-boundary-9
   Content-Type: application/sdp
   Content-Length: (la valeur appropriée)

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

   --my-boundary-9
   Content-Type: multipart/signed;
    protocol="application/pkcs7-signature";
    micalg=sha1; boundary=dragons39
   Content-ID: <20398823.2UWQFN309shb3@referrer.example>
   Content-Length: (la valeur appropriée)

   --dragons39
   Content-Type: message/sipfrag
   Content-Disposition: aib; handling=optional

   Date: Thu, 21 Feb 2002 13:02:03 GMT
   Refer-To: <sip:refertarget@target.example>
   Referred-By: <sip:referrer@referrer.example>
     ;cid="20398823.2UWQFN309shb3@referrer.example"

   --dragons39
   Content-Type: application/pkcs7-signature; name=smime.p7s
   Content-Transfer-Encoding: base64
   Content-Disposition: attachment; filename=smime.p7s;
     handling=required

   (la signature appropriée vient ici)

   --dragons39--
   --my-boundary-9--
```

7.2 REFER non sûr

Le flux pour cet exemple est le même que celui du paragraphe 7.1. Ici, le référant a opté pour ne pas inclure un jeton Referred-By, et la cible de référence veut accepter la demande référencée sans lui.

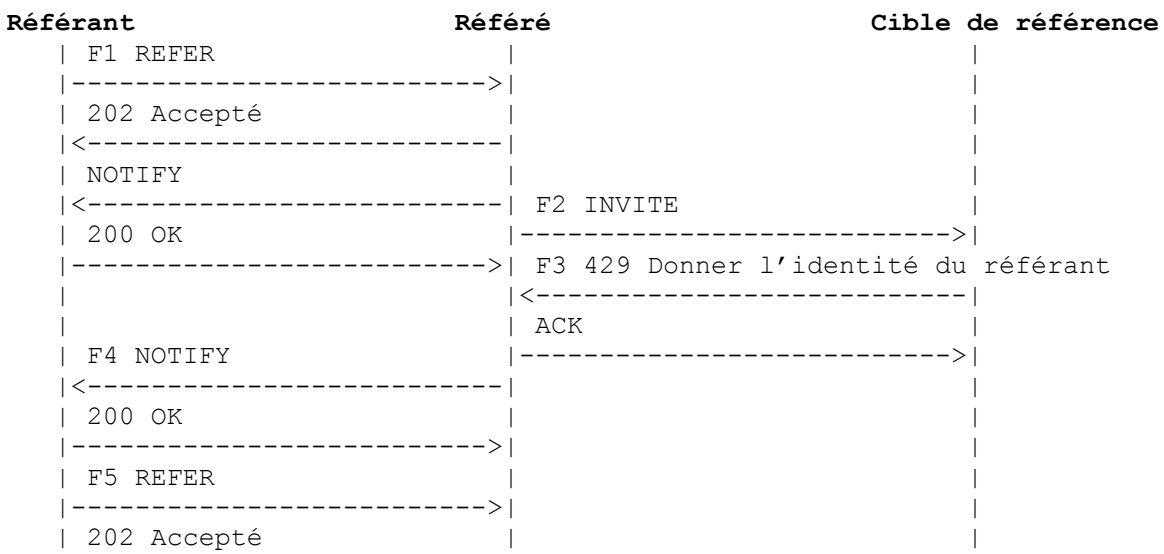
F1 REFER sip:referee@referee.example SIP/2.0
Via: SIP/2.0/UDP referrer.example;branch=z9hG4bK392039842
To: <sip:referee@referee.example>
From: <sip:referrer@referrer.example>;tag=39092342
Call-ID: 2203900ef0299349d9209f023a
CSeq: 1239930 REFER
Max-Forwards: 70
Contact: <sip:referrer.example>
Refer-To: <sip:refertarget@target.example>
Referred-By: <sip:referrer@referrer.example>
Content-Length: 0

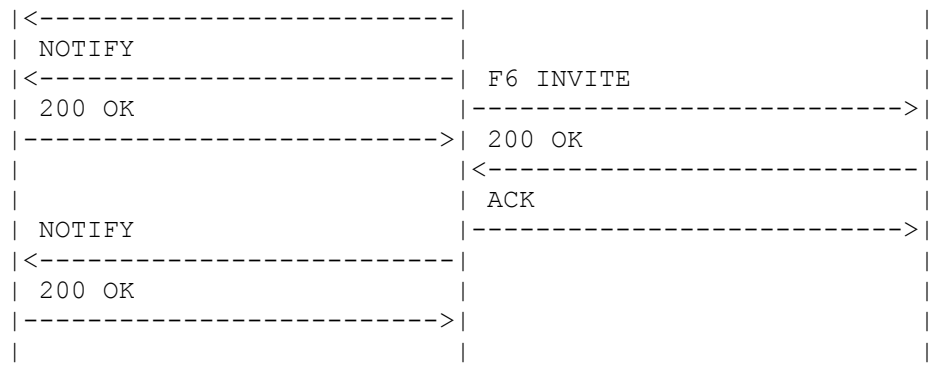
F2 INVITE sip:refertarget@target.example SIP/2.0
Via: SIP/2.0/UDP referee.example;branch=z9hG4bKffe209934aac
To: <sip:refertarget@target.example>
From: <sip:referee@referee.example>;tag=2909034023
Call-ID: fe9023940-a3465@referee.example
CSeq: 889823409 INVITE
Max-Forwards: 70
Contact: <sip:referee@referee.example>
Referred-By: <sip:referrer@referrer.example>
Content-Type: application/sdp
Content-Length: (la valeur appropriée)

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

7.3 Demande de l'identité du référant

À la différence de l'exemple du paragraphe 7.2, la cible de référence exige un jeton Referred-By pour accepter la demande référencée. Le référant choisit de fournir un jeton chiffré (noter que le bloc entouré d'astérisques représente le contenu chiffré). F1 et F2 sont identiques aux messages détaillés au paragraphe 7.2.





F3 SIP/2.0 429 Donner l'identité du référant
Via: SIP/2.0/UDP referee.example;branch=z9hG4bKffe209934aac
To: <sip:refertarget@target.example>;tag=392093422302334
From: <sip:referee@referee.example>;tag=2909034023
Call-ID: fe9023940-a3465@referee.example
CSeq: 889823409 INVITE
Content-Length: 0

F4 NOTIFY sip:referrer@referrer.example SIP/2.0
Via: SIP/2.0/UDP referee.example;branch=z9hG4bK2934209da390
To: <sip:referrer@referrer.example>;tag=39092342
From: <sip:referee@referee.example>;tag=199949923
Call-ID: 2203900ef0299349d9209f023a
CSeq: 3920390 NOTIFY
Event: refer;id=1239930
Subscription-State: terminated
Content-Type: message/sipfrag
Content-Length: (la valeur appropriée)

SIP/2.0 429 Donner l'identité du référant

F5 REFER sip:referee@referee.example SIP/2.0
Via: SIP/2.0/UDP referrer.example;branch=z9hG4bK98823423
To: <sip:referee@referee.example>
From: <sip:referrer@referrer.example>;tag=39092342
Call-ID: 2203900ef0299349d9209f023a
CSeq: 1239931 REFER
Max-Forwards: 70
Contact: <sip:referrer.example>
Refer-To: <sip:refertarget@target.example>
Referred-By: <sip:referrer@referrer.example>
;cid="20342EFXEI.390sdefn2@referrer.example"
Content-Type: multipart/mixed; boundary=unique-boundary-1
Content-Length: (la valeur appropriée)

--unique-boundary-1
Content-Type: multipart/signed;
protocol="application/pkcs7-signature";
micalg=sha1; boundary=boundary42
Content-ID: <20342EFXEI.390sdefn2@referrer.example>
Content-Length: (la valeur appropriée)

--boundary42
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m;
handling=required
Content-Length: (la valeur appropriée)

```
   ************************************************************
   * Content-Type: message/sipfrag                            *
   * Content-Disposition: aib; handling=optional              *
   *                                                          *
   * Date: Thu, 21 Feb 2002 13:02:03 GMT                     *
   * Refer-To: <sip:refertarget@target.example>               *
   * Referred-By: <sip:referrer@referrer.example>             *
   *    ;cid="20342EFXEI.390sdefn2@referrer.example"          *
   ************************************************************

   --boundary42
   Content-Type: application/pkcs7-signature; name=smime.p7s
   Content-Transfer-Encoding: base64
   Content-Disposition: attachment; filename=smime.p7s;
     handling=required

   (la signature appropriée vient ici)

   --boundary42--

F6 INVITE sip:refertarget@target.example SIP/2.0
   Via: SIP/2.0/UDP referee.example;branch=z9hG4bK3920390423
   To: <sip:refertarget@target.example>
   From: <sip:referee@referee.example>;tag=1342093482342
   Call-ID: 23499234-9239842993@referee.example
   CSeq: 19309423 INVITE
   Max-Forwards: 70
   Referred-By: <sip:referrer@referrer.example>
     ;cid="20342EFXEI.390sdefn2@referrer.example"
   Contact: <sip:referee@referee.example>
   Content-Type: multipart/mixed; boundary=my-boundary-9
   Content-Length: (la valeur appropriée)

   --my-boundary-9
   Content-Type: application/sdp
   Content-Length: (la valeur appropriée)

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

   --my-boundary-9
   Content-Type: multipart/signed;
     protocol="application/pkcs7-signature";
     micalg=sha1; boundary=boundary42
   Content-ID: <20342EFXEI.390sdefn2@referrer.example>
   Content-Length: (la valeur appropriée)

   --boundary42
   Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
     name=smime.p7m
   Content-Transfer-Encoding: base64
   Content-Disposition: attachment; filename=smime.p7m;
     handling=required
   Content-Length: (la valeur appropriée)

   ************************************************************
   * Content-Type: message/sipfrag                            *
   * Content-Disposition: aib; handling=optional              *
```

```
*                                   *
* Date: Thu, 21 Feb 2002 13:02:03 GMT                *
* Refer-To: <sip:refertarget@target.example>          *
* Referred-By: <sip:referrer@referrer.example>        *
*    ;cid="20342EFXEI.390sdefn2@referrer.example"     *
*********************************************************

--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s;
  handling=required

(la signature appropriée vient ici)

--boundary42--
--my-boundary-9--
```

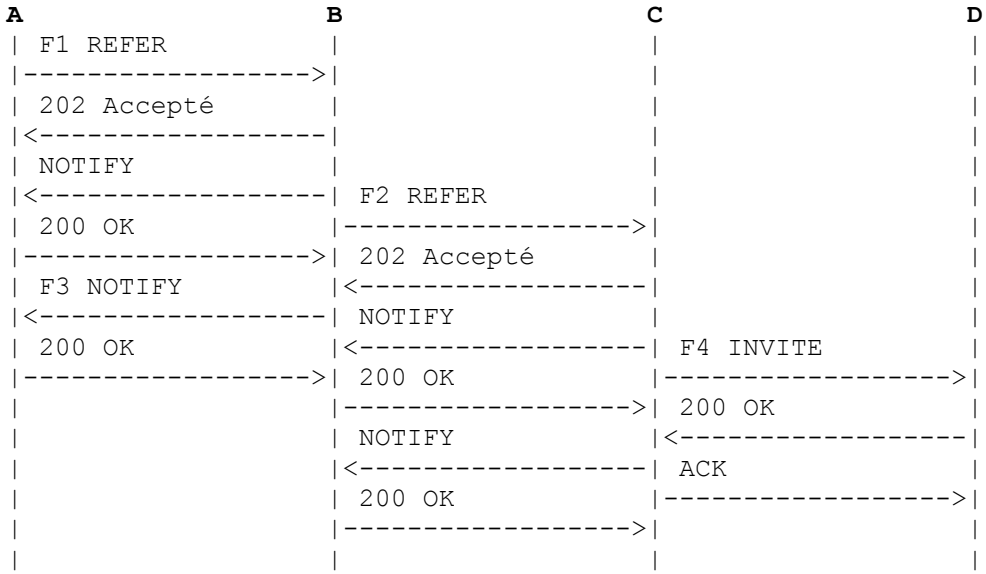
7.4 REFER incorporé

L'URI Refer-To peut être un URI SIP indiquant la méthode REFER. Considérons l'URI suivant que A utilise pour se référer à B pour envoyer une demande REFER à C qui se réfère à C pour envoyer un INVITE à D.

Noter que A fournit un jeton Referred-By qui est passé à travers B et C à D. En particulier, B ne fournit pas son propre jeton Referred-By à C. Noter aussi que A est notifié du résultat de la demande qu'il a déclenché à B (le REFER), non à C (le INVITE).

Refer-To: <sip:C.example;method=REFER?Refer-To="<sip:D.example>">

Cette référence va résulter en le flux suivant :




```
F1 REFER sip:B SIP/2.0
  Via: SIP/2.0/UDP A.example;branch=z9hG4bK3802394232
  To: <sip:B.example>
  From: <sip:A.example>;tag=23490234
  Call-ID: 2304098023@A.example
  CSeq: 2342093 REFER
  Max-Forwards: 70
  Contact: <sip:A.example>
  Refer-To: <sip:C.example;method=REFER?Refer-To="<sip:D>.example">
  Referred-By: <sip:A.example>;
    cid="23094202342.10123091233@A.example"
```

```
   Content-Type: multipart/mixed; boundary=unique-boundary-1
   Content-Length: (la valeur appropriée)

   --unique-boundary-1
   Content-Type: multipart/signed;
     protocol="application/pkcs7-signature";
     micalg=sha1; boundary=dragons39
   Content-ID: <23094202342.10123091233@A.example>
   Content-Length: (la valeur appropriée)

   --dragons39
   Content-Type: message/sipfrag
   Content-Disposition: aib; handling=optional

   Date: Thu, 21 Feb 2002 13:02:03 GMT
   Refer-To: <sip:C.example;method=REFER?Refer-To="<sip:D.example>">
   Referred-By: <sip:A.example>;
      cid="23094202342.10123091233@A.example"

   --dragons39
   Content-Type: application/pkcs7-signature; name=smime.p7s
   Content-Transfer-Encoding: base64
   Content-Disposition: attachment; filename=smime.p7s;
     handling=required

    (la signature appropriée vient ici)

   --dragons39--
   --unique-boundary-1--

F2 REFER sip:C.example SIP/2.0
   Via: SIP/2.0/UDP B.example;branch=z9hG4bK00239842
   To: <sip:C.example>
   From: <sip:B.example>;tag=2934u23
   Call-ID: 203942834@B.example
   CSeq: 8321039 REFER
   Max-Forwards: 70
   Contact: <sip:B.example>
   Refer-To: <sip:D.example>
   Referred-By: <sip:A.example>;
      cid="23094202342.10123091233@A.example"
   Content-Type: multipart/mixed; boundary=unique-boundary-1
   Content-Length: (la valeur appropriée)

   --unique-boundary-1
   Content-Type: multipart/signed;
     protocol="application/pkcs7-signature";
     micalg=sha1; boundary=dragons39
   Content-ID: <23094202342.10123091233@A.example>
   Content-Length: (la valeur appropriée)

   --dragons39
   Content-Type: message/sipfrag
   Content-Disposition: aib; handling=optional

   Date: Thu, 21 Feb 2002 13:02:03 GMT
   Refer-To: <sip:C.example;method=REFER?Refer-To="<sip:D.example>">
   Referred-By: <sip:A.example>;cid="23094202342.1012309123@A.example"

   --dragons39
   Content-Type: application/pkcs7-signature; name=smime.p7s
   Content-Transfer-Encoding: base64
   Content-Disposition: attachment; filename=smime.p7s;
```

```
    handling=required

   (la signature appropriée vient ici)

   --dragons39--
   --unique-boundary-1--

F3 NOTIFY sip:A.example SIP/2.0
   Via: SIP/2.0/UDP A.example;branch=z9hG4bK3802394232
   To: <sip:A.example>;tag=23490234
   From: <sip:B.example>;tag=5923020
   Call-ID: 2304098023@A.example
   CSeq: 29420342 NOTIFY
   Event: refer;id=2342093
   Subscription-State: terminated
   Max-Forwards: 70
   Contact: <sip:B.example>
   Content-Type: message/sipfrag
   Content-Length: (la valeur appropriée)

   SIP/2.0 202 Accepted

F4 INVITE sip:D.example SIP/2.0
   Via: SIP/2.0/UDP C.example;branch=z9hG4bK29348234
   To: <sip:D.example>
   From: <sip:C.example>;tag=023942334
   Call-ID: 23489020352@C.example
   CSeq: 1230934 INVITE
   Max-Forwards: 70
   Contact: <sip:C.example>
   Referred-By: <sip:A.example>;
      cid="23094202342.10123091233@A.example"
   Content-Type: multipart/mixed; boundary=unique-boundary-1
   Content-Length: (la valeur appropriée)

   --unique-boundary-1
   Content-Type: application/sdp
   Content-Length: (la valeuir appropriée)

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

   --unique-boundary-1
   Content-Type: multipart/signed;
     protocol="application/pkcs7-signature";
     micalg=sha1; boundary=dragons39
   Content-ID: <23094202342.10123091233@A.example>
   Content-Length: (la valeur appropriée)

   --dragons39
   Content-Type: message/sipfrag
   Content-Disposition: aib; handling=optional

   Date: Thu, 21 Feb 2002 13:02:03 GMT
   Refer-To: <sip:C.example;method=REFER?Refer-To="<sip:D.example>">
   Referred-By: <sip:A.example>;
      cid="23094202342.1012309123@A.example"
```

```
--dragons39
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s;
  handling=required

 (la signature appropriée vient ici)

--dragons39--
--unique-boundary-1--
```

8. Considérations relatives à l'IANA

Le présent document définit un nouveau champ d'en-tête SIP avec une forme compacte (respectivement Referred-By et b). Il définit aussi un nouveau code de réponse d'erreur du client SIP (429).

Les changements sont reflétés à :

La rangée suivante a été ajoutée à la section de champ d'en-tête (remplaçant la rangée existante pour Referred-By).

Nom d'en-tête	Forme compacte	Référence
Referred-By	b	[RFC3892]

La rangée suivante a été ajoutée à la section Code de réponse sous l'en-tête 4xx Échec de demande.

429 Fournir l'identité du référant	[RFC3892]

9. Contributeurs

Rohan Mahy a transposé le msg-id de la RFC2822 dans la définition de sip-clean-msg-id du présent document.

10. Références

10.1 Références normatives

[RFC2045] N. Freed et N. Borenstein, "Extensions de messagerie Internet multi-objets (MIME) Partie 1 : Format des corps de message Internet", novembre 1996. *(D. S., MàJ par* 2184, 2231, 5335.)

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

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

[RFC3420] R. Sparks, "message/sipfrag de type de support Internet", novembre 2002.

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

[RFC3893] J. Peterson, "Format de corps d'identité authentifiée (AIB) du protocole d'initialisation de session (SIP)", septembre 2004.

10.2 Références pour information

[RFC2822] P. Resnick, "Format de message Internet", avril 2001. *(Remplace la* RFC0822, STD 11, Remplacée par RFC5322)

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

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

11. Adresse de l'auteur

Robert J. Sparks
Xten
5100 Tennyson Parkway
Suite 1000
Plano, TX 75024
mél : RjS@xten.com

12. Déclaration complète de droits de reproduction

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